Networking documentation

La mise en réseau fait partie intégrante de la plateforme SDDC (Software Defined Datacenter), et Windows Server 2016 fournit de nouvelles technologies SDN (Software Defined Networking) nouvelles et améliorées pour vous aider à passer à une solution SDDC entièrement réalisée pour votre organisation.

About networking

VUE D'ENSEMBLE

Scénarios de mise en réseau pris en charge par Windows Server

NOUVEAUTÉS

Nouveautés de la mise en réseau

RÉFÉRENCE

Bibliothèques Windows Server

Contenu supprimé windows Server 2003/2003 R2

Mise en réseau SDN (Software Defined Networking)

VUE D'ENSEMBLE

Mise en réseau définie par logiciel (SDN)

Network Controller

Équilibrage de charge logicielle (SLB) pour SDN

Passerelle RAS pour SDN

Virtualisation de fonction réseau

Vue d'ensemble du pare-feu du centre

DÉPLOYER

Déployer une infrastructure SDN à l'aide de scripts

Networking Technologies

VUE D'ENSEMBLE

BranchCache

Guide du réseau principal

DirectAccess

Système de noms de domaine (DNS)

Protocole DHCP (Dynamic Host Configuration Protocol)

Virtualisation de réseau Hyper-V

Hyper-V commutateur virtuel

Gestion des adresses IP (IPAM)

Équilibrage de la charge réseau (NLB)

Networking Technologies

VUE D'ENSEMBLE

Serveur de stratégie réseau

Network Shell (Netsh)

Réglage des performances du sous-système réseau

Stratégie de qualité de service (QoS)

Service de noms Internet Windows (WINS)

Remote Access

Mise en réseau de conteneurs Windows

Réseau privé virtuel (VPN)

RÉFÉRENCE

Proxy d'application web dans Windows Server 2016

Guide de déploiement vpn Always On d'accès à distance

High-Performance Networking

VUE D'ENSEMBLE

High-Performance Networking

Scénarios de réseau pris en charge par Windows Server

29/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Cette rubrique fournit des informations sur les scénarios pris en charge et non pris en charge, que vous pouvez appliquer ou non avec cette version de Windows Server 2016.

> ⓘ **Important**
>
> Pour tous les scénarios de production, utilisez les derniers pilotes matériels signés de votre fabricant d'ordinateurs (OEM) ou votre fabricant de matériel d'origine.

Scénarios réseau pris en charge

Cette section comprend des informations sur les scénarios réseau pris en charge par Windows Server 2016, et inclut les catégories de scénario suivantes.

- Scénarios SDN (Software-Defined Networking)
- Scénarios de plateforme réseau
- Scénarios de serveur DNS
- Scénarios IPAM avec DHCP et DNS
- Scénarios d'association de cartes réseau
- Scénarios SET (Switch Embedded Teaming)

Scénarios SDN (Software-Defined Networking)

Vous pouvez utiliser la documentation suivante pour déployer des scénarios SDN avec Windows Server 2016.

- Déployer une infrastructure SDN (Software Defined Networking) avec des scripts

Pour plus d'informations, consultez Réseaux SDN (Software-Defined Networking).

Scénarios basés sur le Contrôleur de réseau

Les scénarios basés sur le Contrôleur de réseau vous permettent d'effectuer les opérations suivantes :

- Déployer et gérer une instance multinœud du Contrôleur de réseau. Pour plus d'informations, consultez Déployer le Contrôleur de réseau à l'aide de Windows PowerShell.
- Utiliser le Contrôleur de réseau pour définir par programmation une stratégie réseau à l'aide de l'API REST Northbound.
- Utiliser le Contrôleur de réseau pour créer et gérer des réseaux virtuels avec la virtualisation de réseau Hyper-V, à l'aide de l'encapsulation NVGRE ou VXLAN.

For more information, see Network Controller.

Scénarios NFV (Network Function Virtualization)

Les scénarios NFV vous permettent d'effectuer les opérations suivantes :

- Déployer et utiliser un équilibreur de charge logiciel pour distribuer le trafic sortant (Northbound) et entrant (Southbound).
- Déployer et utiliser un équilibreur de charge logiciel pour distribuer le trafic interne (Eastbound-Westbound) pour les réseaux virtuels créés avec la virtualisation de réseau Hyper-V.
- Déployer et utiliser un équilibreur de charge logiciel NAT pour les réseaux virtuels créés avec la virtualisation de réseau Hyper-V.
- Déployer et utiliser une passerelle de redirection L3 (Couche 3)
- Déployer et utiliser une passerelle VPN (réseau privé virtuel) pour les tunnels IPsec de site à site (IKEv2)
- Déployer et utiliser une passerelle GRE (Generic Routing Encapsulation).
- Déployer et configurer le routage dynamique et le routage de transit entre les sites à l'aide du protocole BGP (Border Gateway Protocol).
- Configurer la redondance M+N pour les passerelles L3 (Couche 3) de site à site ainsi que pour le routage BGP.
- Utiliser le Contrôleur de réseau pour spécifier les listes ACL sur les réseaux virtuels et les interfaces réseau.

Pour plus d'informations, consultez Virtualisation de fonction réseau.

Scénarios de plateforme réseau

Pour les scénarios de cette section, la fonctionnalité d'association de cartes réseau Windows Server prend en charge l'utilisation des pilotes certifiés Windows Server 2016. Vérifiez auprès du fabricant de vos cartes d'interface réseau si vous disposez des mises à jour de pilotes les plus récentes.

Les scénarios de plateforme réseau vous permettent d'effectuer les opérations suivantes :

- Utiliser une carte d'interface réseau convergée pour regrouper le trafic RDMA et Ethernet à l'aide d'une seule carte réseau.
- Créer un chemin de données à faible latence en utilisant Packet Direct, activé dans le commutateur virtuel Hyper-V, et une seule carte réseau.
- Configurer SET pour répartir les flux de trafic SMB Direct et RDMA entre deux cartes réseau au maximum.

Pour plus d'informations, consultez Accès direct à la mémoire à distance (Remote Direct Memory Access, RDMA) et association commutée/intégrée (Switched-Embedded Teaming, SET).

Scénarios de commutateur virtuel Hyper-V

Les scénarios de commutateur virtuel Hyper-V vous permettent d'effectuer les opérations suivantes :

- Créer un commutateur virtuel Hyper-V avec une carte d'interface réseau virtuelle RDMA (accès direct à la mémoire à distance)
- Créer un commutateur virtuel Hyper-V avec SET (Switch Embedded Teaming) et des cartes d'interface réseau virtuelles RDMA
- Créer une association SET dans le commutateur virtuel Hyper-V
- Gérer une association SET à l'aide des commandes Windows PowerShell

Pour plus d'informations, consultez Accès direct à la mémoire à distance (Remote Direct Memory Access, RDMA) et association commutée/intégrée (Switched-Embedded Teaming, SET)

Scénarios de serveur DNS

Les scénarios de serveur DNS vous permettent d'effectuer les opérations suivantes :

- Spécifier la gestion du trafic par géolocalisation à l'aide de stratégies DNS

- Configurer un DNS Split-Brain à l'aide de stratégies DNS
- Appliquer des filtres aux requêtes DNS à l'aide de stratégies DNS
- Configurer l'équilibrage de charge des applications à l'aide de stratégies DNS
- Spécifier des réponses DNS intelligentes en fonction de l'heure de la journée
- Configurer des stratégies de transfert de zone DNS
- Configurer des stratégies de serveur DNS pour les zones intégrées AD DS (Active Directory Domain Services)
- Configurer la limitation du taux de réponse
- Spécifier l'authentification DNS des entités nommées (DANE)
- Configurer la prise en charge des enregistrements inconnus dans DNS

Pour plus d'informations, consultez les rubriques Nouveautés du client DNS dans Windows Server 2016 et Nouveautés du serveur DNS dans Windows Server 2016.

Scénarios IPAM avec DHCP et DNS

Les scénarios IPAM vous permettent d'effectuer les opérations suivantes :

- Découvrir et administrer les serveurs DNS et DHCP ainsi que l'adressage IP dans plusieurs forêts Active Directory fédérées
- Utiliser IPAM pour une gestion centralisée des propriétés DNS, notamment les zones et les enregistrements de ressources.
- Définir des stratégies précises de contrôle d'accès en fonction du rôle, et déléguer des utilisateurs ou des groupes d'utilisateurs IPAM pour gérer l'ensemble des propriétés DNS spécifiées.
- Utiliser les commandes Windows PowerShell pour IPAM afin d'automatiser la configuration du contrôle d'accès pour DHCP et DNS.

  For more information, see Manage IPAM.

Scénarios d'association de cartes réseau

Les scénarios d'association de cartes réseau vous permettent d'effectuer les opérations suivantes :

- Créer une association de cartes réseau dans une configuration prise en charge
- Supprimer une association de cartes réseau
- Ajouter des cartes réseau à l'association de cartes réseau dans une configuration prise en charge
- Supprimer des cartes réseau de l'association de cartes réseau

> ⓘ **Notes**
>
> Avec Windows Server 2016, vous pouvez utiliser l'association de cartes réseau dans Hyper-V. Toutefois, dans certains cas, les files d'attente de machines virtuelles ne sont pas activées automatiquement sur les cartes réseau sous-jacentes quand vous créez une association de cartes réseau. Si cela se produit, utilisez la commande Windows PowerShell suivante pour vérifier que les files d'attente de machines virtuelles sont activées sur les adaptateurs membres de l'association de cartes réseau : `Set-NetAdapterVmq -Name <NetworkAdapterName> -Enable`

Scénarios SET (Switch Embedded Teaming)

SET est une autre solution pour l'association de cartes réseau, que vous pouvez utiliser au sein des environnements qui incluent Hyper-V et la pile SDN (Software-Defined Networking) dans Windows Server 2016. La technologie SET intègre certaines fonctionnalités d'association de NIC dans le commutateur virtuel Hyper-V.

Pour plus d'informations, consultez Accès direct à la mémoire à distance (Remote Direct Memory Access, RDMA) et association commutée/intégrée (Switched-Embedded Teaming, SET)

Scénarios réseau non pris en charge

Les scénarios réseau suivants ne sont pas pris en charge dans Windows Server 2016.

- Réseaux virtuels de locataires basés sur un VLAN.
- IPv6 n'est pas pris en charge dans la couche sous-jacente ou la superposition.

Configurer les options de protocoles sécurisés pour WinHTTP

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10

Ce guide pratique vous montre comment utiliser l'entrée de Registre `DefaultSecureProtocols` pour choisir les protocoles des services HTTP Windows (WinHTTP).

L'entrée de Registre `DefaultSecureProtocols` vous permet de spécifier les protocoles SSL à utiliser quand l'indicateur `WINHTTP_OPTION_SECURE_PROTOCOLS` est utilisé. Le paramètre permet aux applications créées d'utiliser l'indicateur WinHTTP par défaut pour appliquer les protocoles TLS les plus récents ou bloquer les anciens protocoles SSL de manière native sans nécessiter de mises à jour de l'application.

Prérequis

- Calculez la valeur de `DefaultSecureProtocols` avec WINHTTP_OPTION_SECURE_PROTOCOLS.
- Vérifiez que votre compte dispose de droits d'administration sur le système.
- Vérifiez que PowerShell est installé.

Configurer DefaultSecureProtocols

Sélectionnez le type d'architecture à ajouter et définir l'entrée de Registre `DefaultSecureProtocols` :

x86

1. Ouvrez une invite PowerShell avec élévation de privilèges.
2. Pour créer et définir la clé de Registre `DefaultSecureProtocols`, exécutez la commande suivante et remplacez `{value}` par la valeur `DefaultSecureProtocols` que vous avez sélectionnée dans Calculer la valeur.

   PowerShell

```
Get-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\WinHttp" | New-ItemProperty -Name "DefaultSecureProtocols" -
Value "{value}"
```

3. Redémarrez la machine, ou redémarrez les services qui utilisent WinHTTP.

Étapes suivantes

- Pour configurer l'entrée de Registre `DefaultSecureProtocols` de plusieurs machines, consultez Configurer un élément de service.

Recommandations relatives au réseau principal pour Windows Server

Article • 05/10/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server, Windows Server 2016

Cette rubrique fournit une vue d'ensemble de l'aide sur le réseau principal pour Windows Server® 2016 et contient les sections suivantes.

- Introduction au réseau de base Windows Server
- Guide du réseau de base pour Windows Server

Introduction au réseau de base Windows Server

Un réseau de base est un ensemble de matériels, périphériques et logiciels réseau qui fournissent les services centraux répondant aux besoins en technologies de l'information de votre organisation.

Un réseau de base Windows Server présente de nombreux avantages, notamment :

- Des protocoles centraux pour la connectivité réseau entre les ordinateurs et d'autres périphériques compatibles avec le protocole TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP est une suite de protocoles standard utilisée pour la connexion d'ordinateurs et la création de réseaux. TCP/IP est un logiciel de protocole réseau fourni avec les systèmes d'exploitation Microsoft® Windows® qui implémente et prend en charge la suite de protocoles TCP/IP.
- Adressage IP automatique par un serveur DHCP (Dynamic Host Configuration Protocol). La configuration manuelle d'adresses IP sur tous les ordinateurs de votre réseau prend du temps et est moins souple que l'attribution dynamique de baux d'adresses IP aux ordinateurs et autres périphériques par un serveur DHCP.
- Un service de résolution de noms (DNS, Domain Name System). Le service DNS permet aux utilisateurs, aux ordinateurs, aux applications et aux services de trouver les adresses IP des ordinateurs et périphériques du réseau d'après le nom de domaine complet (FQDN, Fully Qualified Domain Name) de l'ordinateur ou du périphérique.

- Une forêt, qui est constituée d'un ou de plusieurs domaines Active Directory partageant les mêmes définitions de classes et d'attributs (schéma), les mêmes informations de site et de réplication (configuration) et des fonctionnalités de recherche à l'échelle de la forêt (catalogue global).

- Un domaine racine de forêt, qui est le premier domaine de forêt créé dans une nouvelle forêt. Les groupes Administrateurs de l'entreprise et Administrateurs du schéma, qui sont des groupes d'administration s'appliquant à l'ensemble de la forêt, sont situés dans le domaine racine de la forêt. Par ailleurs, un domaine racine de forêt, comme les autres domaines, est une collection d'objets de type ordinateur, utilisateur et groupe qui sont définis par l'administrateur dans les services de domaine Active Directory (AD DS). Ces objets partagent une base de données d'annuaire commune et des stratégies de sécurité. Ils peuvent également partager des relations de sécurité avec d'autres domaines si vous ajoutez des domaines à mesure que votre organisation se développe. Le service d'annuaire stocke également des données d'annuaire et permet aux ordinateurs, applications et utilisateurs autorisés d'accéder aux données.

- Une base de données de comptes d'utilisateurs et d'ordinateurs. Le service d'annuaire offre une base de données de comptes d'utilisateurs centralisée qui vous permet de créer des comptes d'utilisateurs et d'ordinateurs pour les personnes et les ordinateurs qui sont autorisés à se connecter à votre réseau et à accéder aux ressources réseau, comme les applications, les bases de données, les fichiers et dossiers partagés, ainsi que les imprimantes.

Un réseau de base vous permet également de faire évoluer votre réseau à mesure que votre organisation se développe et que vos besoins en technologies de l'information évoluent. Par exemple, avec un réseau de base, vous pouvez ajouter des domaines, des sous-réseaux IP, des services d'accès à distance, des services sans fil et d'autres fonctionnalités, ainsi que les rôles serveur fournis par Windows Server 2016.

Guide du réseau de base pour Windows Server

Le Guide du réseau de base Windows Server 2016 fournit des instructions sur la façon de planifier et déployer les composants centraux requis pour créer un réseau pleinement fonctionnel et un nouveau domaine Active Directory® dans une nouvelle forêt. Ce guide vous explique comment déployer des ordinateurs configurés avec les composants Windows Server suivants :

- Rôle serveur des services de domaine Active Directory (AD DS)

- Rôle serveur DNS (Domain Name System)

- Rôle serveur DHCP (Dynamic Host Configuration Protocol)
- Service de rôle NPS (Network Policy Server) du rôle serveur Services de stratégie et d'accès réseau
- Rôle serveur Serveur Web (IIS)
- Connexions TCP/IP (Transmission Control Protocol/Internet Protocol) version 4 sur les ordinateurs individuels

Ce guide est disponible à l'emplacement suivant.

- Le Guide du réseau principal dans la bibliothèque technique Windows Server 2016.

Composants d’un réseau de base

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Ce guide fournit des instructions sur la planification et le déploiement des composants de base nécessaires pour créer un réseau pleinement fonctionnel ainsi qu’un domaine Active Directory dans une nouvelle forêt.

Ce guide contient les sections suivantes :

- À propos de ce guide
- Vue d’ensemble d’un réseau de base
- Planification d’un réseau de base
- Déploiement d’un réseau de base
- Ressources techniques supplémentaires
- Annexes A à E

À propos de ce guide

Ce guide s’adresse aux administrateurs système et réseau qui installent un nouveau réseau ou qui souhaitent créer un réseau basé sur des domaines pour remplacer un réseau constitué de groupes de travail. Le scénario de déploiement fourni dans ce guide est particulièrement utile si vous savez déjà que vous aurez besoin d’ajouter des services et des fonctionnalités supplémentaires à votre réseau dans le futur.

Il est recommandé de passer en revue les guides de conception et de développement de chacune des technologies utilisées dans ce scénario de déploiement pour vous aider à déterminer si ce guide propose les services et la configuration dont vous avez besoin.

Un réseau de base est un ensemble de matériels, périphériques et logiciels réseau qui fournissent les services centraux répondant aux besoins en technologies de l’information de votre organisation.

Un réseau de base Windows Server présente de nombreux avantages, notamment :

- Des protocoles centraux pour la connectivité réseau entre les ordinateurs et d’autres périphériques compatibles avec le protocole TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP est une suite de protocoles standard utilisée pour la

connexion d'ordinateurs et la création de réseaux. TCP/IP est un logiciel de protocole réseau fourni avec les systèmes d'exploitation Microsoft Windows. Il implémente et prend en charge la suite de protocoles TCP/IP.

- L'attribution automatique d'adresses IP avec le protocole DHCP (Dynamic Host Configuration Protocol) pour les ordinateurs et autres périphériques configurés en tant que clients DHCP. La configuration manuelle d'adresses IP sur tous les ordinateurs de votre réseau prend du temps et est moins souple que l'attribution dynamique de configurations d'adresses IP aux ordinateurs et autres périphériques avec un serveur DHCP.

- Un service de résolution de noms (DNS, Domain Name System). Le service DNS permet aux utilisateurs, aux ordinateurs, aux applications et aux services de trouver les adresses IP des ordinateurs et périphériques du réseau d'après le nom de domaine complet (FQDN, Fully Qualified Domain Name) de l'ordinateur ou du périphérique.

- Une forêt, qui est constituée d'un ou de plusieurs domaines Active Directory partageant les mêmes définitions de classes et d'attributs (schéma), les mêmes informations de site et de réplication (configuration) et des fonctionnalités de recherche à l'échelle de la forêt (catalogue global).

- Un domaine racine de forêt, qui est le premier domaine de forêt créé dans une nouvelle forêt. Les groupes Administrateurs de l'entreprise et Administrateurs du schéma, qui sont des groupes d'administration s'appliquant à l'ensemble de la forêt, sont situés dans le domaine racine de la forêt. Par ailleurs, un domaine racine de forêt, comme les autres domaines, est une collection d'objets de type ordinateur, utilisateur et groupe qui sont définis par l'administrateur dans les services de domaine Active Directory (AD DS). Ces objets partagent une base de données d'annuaire commune et des stratégies de sécurité. Ils peuvent également partager des relations de sécurité avec d'autres domaines si vous ajoutez des domaines à mesure que votre organisation se développe. Le service d'annuaire stocke également des données d'annuaire et permet aux ordinateurs, applications et utilisateurs autorisés d'accéder aux données.

- Une base de données de comptes d'utilisateurs et d'ordinateurs. Le service d'annuaire offre une base de données de comptes d'utilisateurs centralisée qui vous permet de créer des comptes d'utilisateurs et d'ordinateurs pour les personnes et les ordinateurs qui sont autorisés à se connecter à votre réseau et à accéder aux ressources réseau, comme les applications, les bases de données, les fichiers et dossiers partagés, ainsi que les imprimantes.

Un réseau de base vous permet également de faire évoluer votre réseau à mesure que votre organisation se développe et que vos besoins en technologies de l'information évoluent. Par exemple, avec un réseau de base, vous pouvez ajouter des domaines, des sous-réseaux IP, des

services d’accès à distance, des services sans fil et d’autres fonctionnalités, ainsi que les rôles serveur fournis par Windows Server 2016.

Configuration matérielle réseau

Pour réussir le déploiement d’un réseau de base, vous devez déployer du matériel réseau, notamment :

- un câblage Ethernet, Fast Ethernet ou Gigabyte Ethernet ;
- un concentrateur, un commutateur de couche 2 ou 3, un routeur, ou un autre périphérique assurant la fonction de relais du trafic réseau entre les ordinateurs et les périphériques ;
- des ordinateurs conformes à la configuration minimale requise pour leurs systèmes d’exploitation client et serveur respectifs.

Ce que ce guide ne contient pas

Ce guide ne fournit pas d’instructions sur le déploiement des éléments suivants :

- Matériel réseau, comme le câblage, les routeurs, les commutateurs et les concentrateurs
- Ressources réseau supplémentaires, comme les imprimantes et les serveurs de fichiers
- Internet connectivity
- Accès à distance
- Accès sans fil
- Déploiement d’ordinateurs clients

> **Notes**
>
> Les ordinateurs exécutant des systèmes d’exploitation clients Windows sont configurés par défaut pour recevoir des baux d’adresses IP de la part du serveur DHCP. Par conséquent, aucune configuration DHCP ou IPv4 (Internet Protocol version 4) supplémentaire n’est requise sur les ordinateurs clients.

Vue d’ensemble des technologies

Les sections suivantes fournissent de brèves vues d'ensemble des technologies à déployer pour créer un réseau de base.

Services de domaine Active Directory

Un annuaire est une structure hiérarchique où sont stockées les informations relatives aux objets du réseau, tels que les utilisateurs et les ordinateurs. Un service d'annuaire, comme les services de domaine Active Directory, propose des méthodes pour stocker des données d'annuaire et rendre ces données disponibles aux utilisateurs et administrateurs du réseau. Par exemple, les services de domaine Active Directory stockent des informations sur les comptes d'utilisateurs (notamment les noms, les adresses de messagerie, les mots de passe et les numéros de téléphone), auxquelles les utilisateurs autorisés du même réseau peuvent accéder.

DNS

DNS est un protocole de résolution de noms pour les réseaux TCP/IP, tels qu'Internet ou le réseau d'une organisation. Un serveur DNS héberge les informations qui permettent aux ordinateurs clients et aux services de résoudre des noms DNS alphanumériques explicites en adresses IP utilisées par les ordinateurs pour communiquer.

DHCP

DHCP est une norme IP permettant de simplifier la gestion de la configuration IP de l'hôte. Cette norme permet d'utiliser des serveurs DHCP comme moyen de gérer l'allocation dynamique d'adresses IP et d'autres informations de configuration pour les clients DHCP sur votre réseau.

DHCP vous permet d'utiliser un serveur DHCP pour attribuer dynamiquement une adresse IP à un ordinateur ou un autre périphérique, tel qu'une imprimante, sur votre réseau local. Chaque ordinateur d'un réseau TCP/IP doit avoir une adresse IP unique, car cette adresse et son masque de sous-réseau associé sont utilisés pour identifier l'ordinateur hôte et le sous-réseau auquel l'ordinateur est joint. Avec le protocole DHCP, vous avez l'assurance que tous les ordinateurs configurés en tant que clients DHCP reçoivent une adresse IP correspondant à leur emplacement réseau et leur sous-réseau. De plus, en utilisant les options DHCP, telles qu'une passerelle par défaut et des serveurs DNS, vous fournissez automatiquement aux clients DHCP les informations dont ils ont besoin pour fonctionner correctement sur votre réseau.

Pour les réseaux TCP/IP, le réseau DHCP réduit la complexité et le travail d'administration nécessaires pour reconfigurer les ordinateurs.

TCP/IP

TCP/IP dans Windows Server 2016 est le suivant :

- un logiciel réseau reposant sur des protocoles réseau standard ;
- un protocole réseau d'entreprise routable qui prend en charge la connexion de votre ordinateur Windows aux environnements de réseau local (LAN, Local Area Network) et de réseau étendu (WAN, Wide Area Network) ;
- un ensemble de technologies et d'utilitaires centraux permettant de connecter votre ordinateur Windows à des systèmes hétérogènes pour le partage d'informations ;
- une base pour pouvoir accéder aux services Internet globaux, comme les serveurs Web et FTP (File Transfer Protocol) ;
- une infrastructure client/serveur interplateforme, évolutive et robuste.

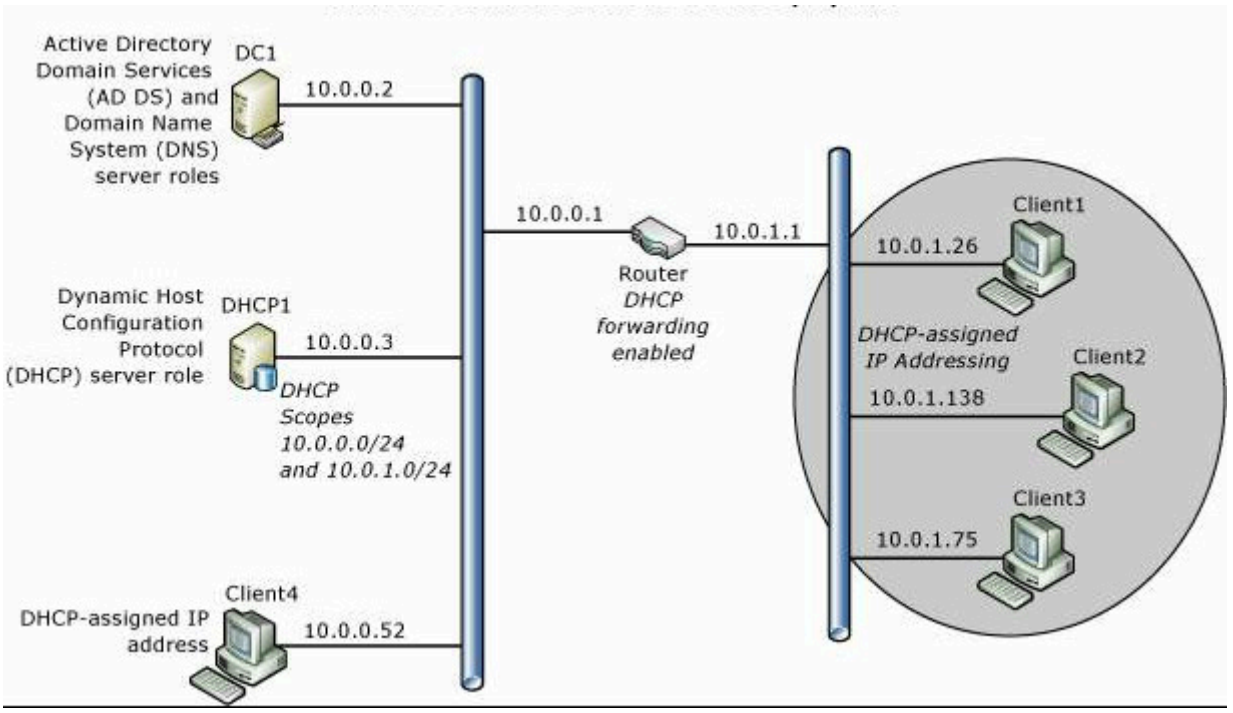
TCP/IP propose des utilitaires TCP/IP de base qui permettent aux ordinateurs Windows de se connecter à d'autres systèmes d'exploitation Microsoft et non-Microsoft pour partager des informations, notamment :

- Windows Server 2016
- Windows 10
- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2
- Windows 7
- Windows Server 2008
- Windows Vista
- Hôtes Internet
- Systèmes Apple Macintosh
- Ordinateurs mainframes IBM
- Systèmes UNIX et Linux

- Systèmes Open VMS
- Imprimantes prêtes pour le réseau
- Tablettes et téléphones cellulaires avec activation de la technologie filaire Ethernet ou sans fil 802.11

Vue d'ensemble d'un réseau de base

L'illustration suivante décrit la topologie d'un réseau de base Windows Server.



> ⓘ **Notes**
>
> Ce guide comprend également des instructions pour l'ajout facultatif de serveurs NPS (Network Policy Server) et Web (IIS) à la topologie de votre réseau. Ces serveurs peuvent servir de base de déploiement des solutions d'accès réseau sécurisées, telles que les connexions sans fil et câblées 802.1X déployées à l'aide des guides d'accompagnement du réseau de base. Pour plus d'informations, voir **Déploiement de fonctionnalités facultatives pour l'authentification d'accès réseau et les services Web**.

Composants d'un réseau de base

Les composants d'un réseau de base sont les suivants :

Router

Ce guide de déploiement fournit des instructions sur le déploiement d'un réseau de base avec deux sous-réseaux séparés par un routeur sur lequel l'acheminement DHCP est activé. Vous pouvez néanmoins déployer un commutateur de couche 2, un commutateur de couche 3 ou un concentrateur, en fonction de vos exigences et de vos ressources. Si vous déployez un commutateur, celui-ci doit prendre en charge l'acheminement DHCP. Sinon, vous devez placer un serveur DHCP sur chaque sous-réseau. Si vous déployez un concentrateur, vous déployez un seul sous-réseau et vous n'avez pas besoin de l'acheminement DHCP ni d'une seconde étendue sur votre serveur DHCP.

Configurations TCP/IP statiques

Les serveurs de ce déploiement sont configurés avec des adresses IPv4 statiques. Les ordinateurs clients sont configurés par défaut pour recevoir des baux d'adresses IP du serveur DHCP.

Catalogue global des services de domaine Active Directory et serveur DNS DC1

Les services de domaine Active Directory (AD DS) et DNS sont tous deux installés sur ce serveur, appelé DC1, qui fournit des services d'annuaire et de résolution de noms pour tous les ordinateurs et périphériques du réseau.

Serveur DHCP DHCP1

Le serveur DHCP, appelé DHCP1, est configuré avec une étendue qui fournit des baux d'adresses IP aux ordinateurs sur le sous-réseau local. Le serveur DHCP peut également être configuré avec des étendues supplémentaires pour fournir des baux d'adresses IP aux ordinateurs sur d'autres sous-réseaux si l'acheminement DHCP est configuré sur les routeurs.

Ordinateurs clients

Les ordinateurs exécutant des systèmes d'exploitation clients Windows sont configurés par défaut en tant que clients DHCP, qui obtiennent automatiquement les adresses IP et les options DHCP du serveur DHCP.

Planification d'un réseau de base

Avant de déployer un réseau de base, vous devez effectuer les tâches suivantes :

- Planification des sous-réseaux

- Planification de la configuration de base de tous les serveurs
- Planification du déploiement du serveur DC1
- Planification de l'accès au domaine
- Planification du déploiement du serveur DHCP1

Chacun de ces éléments est présenté en détail dans les sections qui suivent.

> ⓘ **Notes**
>
> Pour obtenir de l'aide sur la planification de votre déploiement, consultez également l'**Annexe E - Feuille de préparation de la planification d'un réseau de base**.

Planification des sous-réseaux

Dans les réseaux TCP/IP (Transmission Control Protocol/Internet Protocol), des routeurs sont utilisés pour interconnecter le matériel et les logiciels utilisés sur différents segments physiques du réseau, appelés sous-réseaux, et pour acheminer des paquets IP entre ces sous-réseaux. Vous devez déterminer la disposition physique de votre réseau, y compris le nombre de routeurs et de sous-réseaux dont vous avez besoin, avant de suivre les instructions de ce guide.

Par ailleurs, pour configurer les serveurs de votre réseau avec des adresses IP statiques, vous devez déterminer la plage d'adresses IP que vous souhaitez utiliser pour le sous-réseau sur lequel sont situés les serveurs de votre réseau de base. Dans ce guide, les plages d'adresses IP privées allant de 10.0.0.1 à 10.0.0.254 et de 10.0.1.1 à 10.0.1.254 sont utilisées à titre d'exemples, mais vous pouvez en utiliser d'autres.

> ⓘ **Important**
>
> Une fois que vous avez sélectionné la plage d'adresses IP à utiliser pour chaque sous-réseau, veillez à configurer votre routeur avec une adresse IP de la même plage d'adresses IP que celle utilisée pour le sous-réseau sur lequel le routeur est installé. Par exemple, si votre routeur est configuré par défaut avec l'adresse IP 192.168.1.1, et que vous l'installez sur un sous-réseau avec la plage d'adresses IP 10.0.0.0/24, vous devez reconfigurer le routeur pour utiliser à la place une adresse IP de la plage d'adresses IP 10.0.0.0/24.

Les plages d'adresses IP privées reconnues sont spécifiées par le document RFC (Request for Comments) Internet 1918 :

- 10.0.0.0 - 10.255.255.255

- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Lorsque vous utilisez les plages d'adresses IP privées spécifiées dans le document RFC 1918, vous ne pouvez pas vous connecter directement à Internet en utilisant une adresse IP privée, car les demandes dirigées vers ces adresses ou émanant de celles-ci sont automatiquement ignorées par les routeurs des fournisseurs de services Internet. Pour ajouter ultérieurement la connectivité Internet à votre réseau de base, vous devez prendre un abonnement auprès d'un fournisseur de services Internet de manière à obtenir une adresse IP publique.

> ⓘ **Important**
>
> Lorsque vous utilisez des adresses IP privées, vous devez utiliser un serveur proxy ou un serveur NAT (Network Address Translation) quel qu'il soit pour convertir les plages d'adresses IP privées sur votre réseau local en adresse IP publique qui peut être routée sur Internet. La plupart des routeurs fournissant des services NAT, le choix d'un routeur NAT ne devrait pas poser de problème particulier.

Pour plus d'informations, voir Planification du déploiement du serveur DHCP1.

Planification de la configuration de base de tous les serveurs

Pour chaque serveur du réseau de base, vous devez renommer l'ordinateur, lui attribuer une adresse IPv4 statique et configurer d'autres propriétés TCP/IP.

Planification des conventions de dénomination pour les ordinateurs et les périphériques

Pour garantir l'homogénéité de votre réseau, il est judicieux d'utiliser des noms cohérents pour les serveurs, les imprimantes et autres périphériques. Des noms d'ordinateurs peuvent être utilisés pour aider les utilisateurs et les administrateurs à identifier le rôle et l'emplacement du serveur, de l'imprimante ou des autres périphériques. Par exemple, si vous avez trois serveurs DNS, un à San Francisco, un à Los Angeles et un à Chicago, vous pouvez utiliser le*numérod'emplacement*- de *la fonction de serveur de convention*- d'affectation de noms :

- DNS-DEN-01. Ce nom représente le serveur DNS déployé à Denver (Colorado). Si d'autres serveurs DNS sont déployés à Denver, la valeur numérique du nom peut être incrémentée (DNS-DEN-02, DNS-DEN-03, etc.).
- DNS-SPAS-01. Ce nom représente le serveur DNS déployé à South Pasadena (Californie).

- DNS-ORL-01. Ce nom représente le serveur DNS déployé à Orlando (Floride).

Dans ce guide, la convention de dénomination des serveurs utilisée est très simple : le nom se compose de la fonction du serveur principal et d'un numéro. Par exemple, le contrôleur de domaine est appelé DC1 et le serveur DHCP, DHCP1.

Nous vous recommandons de choisir une convention de dénomination avant de procéder à l'installation de votre réseau de base à l'aide de ce guide.

Planification des adresses IP statiques

Avant de configurer chaque ordinateur avec une adresse IP statique, vous devez planifier vos sous-réseaux et les plages d'adresses IP. Par ailleurs, vous devez déterminer les adresses IP de vos serveurs DNS. Si vous prévoyez d'installer un routeur qui fournit l'accès à d'autres routeurs, comme des sous-réseaux supplémentaires ou Internet, vous devez connaître l'adresse IP du routeur, également appelé passerelle par défaut, pour pouvoir configurer les adresses IP statiques.

Le tableau ci-dessous propose des exemples de valeurs pour la configuration des adresses IP statiques.

Agrandir le tableau

Éléments de configuration	Exemples de valeurs
IP address	10.0.0.2
Masque de sous-réseau	255.255.255.0
Passerelle par défaut (adresse IP du routeur)	10.0.0.1
Serveur DNS préféré	10.0.0.2

Notes

Si vous planifiez de déployer plusieurs serveurs DNS, vous pouvez également planifier l'adresse IP du serveur DNS auxiliaire.

Planification du déploiement du serveur DC1

Cette section décrit les principales étapes de planification qui doivent être suivies avant d'installer les services de domaine Active Directory (AD DS) et DNS sur DC1.

Planification du nom du domaine racine de forêt

La première étape du processus de conception du déploiement des services de domaine Active directory consiste à déterminer le nombre de forêts nécessaires dans votre organisation. Une forêt est le conteneur de niveau supérieur des services de domaine Active Directory. Elle regroupe un ou plusieurs domaines qui partagent un modèle et un catalogue global communs. Une organisation peut avoir plusieurs forêts, même si la plupart préfèrent utiliser un modèle à une seule forêt qui est plus facile à administrer.

Lorsque vous créez le premier contrôleur de domaine dans votre organisation, vous créez en fait le premier domaine (également appelé le domaine racine de forêt) et la première forêt. Toutefois, vous devez avant cela déterminer le nom de domaine le plus approprié pour votre organisation. Le nom de l'organisation est généralement utilisé comme nom de domaine, lequel est bien souvent un nom déposé. Si vous planifiez de déployer des serveurs Web externes basés sur Internet pour fournir des informations et des services à vos clients ou partenaires, choisissez un nom de domaine encore inutilisé, puis déposez ce nom pour que votre organisation en ait la propriété.

Planification du niveau fonctionnel de la forêt

Lors de l'installation des services de domaine Active Directory, vous devez choisir le niveau fonctionnel que vous souhaitez utiliser pour la forêt. La fonctionnalité de domaine et de forêt, introduite pour la première fois dans Windows Server 2003 Active Directory, permet d'activer les fonctionnalités Active Directory à l'échelle du domaine ou de la forêt au sein de votre environnement réseau. Différents niveaux de fonctionnalités de domaine et de forêt sont disponibles, selon votre environnement.

La fonctionnalité de forêt active les fonctionnalités dans tous les domaines de votre forêt. Les niveaux fonctionnels de forêt suivants sont disponibles :

- Windows Server 2008. Ce niveau fonctionnel de forêt prend uniquement en charge les contrôleurs de domaine qui exécutent Windows Server 2008 et les versions ultérieures du système d'exploitation Windows Server.

- Windows Server 2008 R2. Ce niveau fonctionnel de forêt prend en charge les contrôleurs de domaine Windows Server 2008 R2 et les contrôleurs de domaine qui exécutent les versions ultérieures du système d'exploitation Windows Server.

- Windows Server 2012. Ce niveau fonctionnel de forêt prend en charge les contrôleurs de domaine Windows Server 2012 et les contrôleurs de domaine qui exécutent les versions ultérieures du système d'exploitation Windows Server.

- Windows Server 2012 R2. Ce niveau fonctionnel de forêt prend en charge les contrôleurs de domaine Windows Server 2012 R2 et les contrôleurs de domaine qui exécutent les versions ultérieures du système d'exploitation Windows Server.
- Windows Server 2016. Ce niveau fonctionnel de forêt prend en charge uniquement les contrôleurs de domaine Windows Server 2016 et les contrôleurs de domaine qui exécutent les versions ultérieures du système d'exploitation Windows Server.

Si vous déployez un nouveau domaine dans une nouvelle forêt, et si tous vos contrôleurs de domaine exécutent Windows Server 2016, il est recommandé de configurer AD DS avec le niveau fonctionnel de forêt Windows Server 2016 durant l'installation d'AD DS.

> **Important**
>
> Une fois que le niveau fonctionnel de la forêt a été augmenté, les contrôleurs de domaine exécutant des systèmes d'exploitation antérieurs ne peuvent plus être inclus dans la forêt. Par exemple, si vous élevez le niveau fonctionnel de forêt à celui de Windows Server 2016, les contrôleurs de domaine exécutant Windows Server 2012 R2 ou Windows Server 2008 ne peuvent pas être ajoutés à la forêt.

Le tableau suivant fournit des exemples d'éléments de configuration des services de domaine Active Directory :

Agrandir le tableau

Éléments de configuration :	**Exemples de valeurs :**
Nom DNS complet	Examples: - corp.contoso.com - example.com
Niveau fonctionnel d'une forêt	– Windows Server 2008 – Windows Server 2008 R2 – Windows Server 2012 – Windows Server 2012 R2 - Windows Server 2016
Emplacement du dossier de la base de données des services de domaine Active Directory	E:\Configuration\ Ou acceptez la valeur par défaut.
Emplacement du dossier des fichiers journaux des services de domaine Active Directory	E:\Configuration\ Ou acceptez la valeur par défaut.

Éléments de configuration :	Exemples de valeurs :
Emplacement du dossier SYSVOL des services de domaine Active Directory	E:\Configuration\ Ou acceptez la valeur par défaut.
Mot de passe administrateur de restauration des services d'annuaire	**J*p2leO4$F**
Nom du fichier de réponses (facultatif)	**AD DS_AnswerFile**

Planification des zones DNS

Sur les serveurs DNS principaux intégrés à Active Directory, une zone de recherche directe est créée par défaut lors de l'installation du rôle serveur DNS. Une zone de recherche directe permet aux ordinateurs et aux périphériques de rechercher l'adresse IP d'un autre ordinateur ou d'un autre périphérique en fonction de son nom DNS. Il est recommandé de créer en parallèle une zone de recherche inversée DNS. Avec une requête de recherche inversée DNS, un ordinateur ou un périphérique peut découvrir le nom d'un autre ordinateur ou périphérique en utilisant son adresse IP. Le déploiement d'une zone de recherche inversée permet généralement d'améliorer les performances DNS et d'assurer un plus grand succès des requêtes DNS.

Lorsque vous créez une zone de recherche inversée, le domaine in-addr.arpa est installé dans les services DNS ; défini dans les normes DNS, ce domaine est réservé dans l'espace de noms DNS Internet afin de fournir un moyen fiable et pratique d'effectuer des requêtes inversées. Pour créer l'espace de noms inversé, des sous-domaines sont formés dans le domaine in-addr.arpa en utilisant le classement inversé des nombres dans la notation décimale séparée par des points des adresses IP.

Le domaine in-addr.arpa s'applique à tous les réseaux TCP/IP basés sur l'adressage IPv4 (Internet Protocol version 4). L'Assistant Nouvelle zone suppose automatiquement que vous utilisez ce domaine lorsque vous créez une zone de recherche inversée.

Dans l'Assistant Nouvelle zone, nous vous recommandons de sélectionner les options suivantes :

Agrandir le tableau

Éléments de configuration	Exemples de valeurs
Type de zone	**La zone principale** et **stocker la zone dans Active Directory** est sélectionnée
Étendue de réplication de la zone Active	**Vers tous les serveurs DNS de ce domaine**

Éléments de configuration	Exemples de valeurs
Directory	
Première page Nom de la zone de recherche inversée de l'Assistant	**Zone de recherche inversée IPv4**
Seconde page Nom de la zone de recherche inversée de l'Assistant	ID réseau = 10.0.0.
Mises à jour dynamiques	**N'autoriser que les mises à jour dynamiques sécurisées**

Planification de l'accès au domaine

Pour ouvrir une session sur un domaine, l'ordinateur doit être membre du domaine et le compte d'utilisateur doit être créé dans les services de domaine Active Directory avant la tentative d'ouverture de session.

> **Notes**
>
> Chaque ordinateur exécutant Windows comporte une base de données de comptes d'utilisateurs et de groupes locaux ; il s'agit de la base de données des comptes d'utilisateurs du Gestionnaire de comptes de sécurité (SAM, Security Accounts Manager). Lorsque vous créez un compte d'utilisateur dans la base de données du Gestionnaire de comptes de sécurité sur un ordinateur local, vous pouvez ouvrir une session sur ce dernier, mais pas sur un domaine. Les comptes d'utilisateurs de domaine sont créés dans la console MMC (Microsoft Management Console) Utilisateurs et ordinateurs Active Directory sur un contrôleur de domaine, et pas avec des utilisateurs et groupes locaux sur l'ordinateur local.

Une fois la première ouverture de session réussie avec les informations d'ouverture de session de domaine, les paramètres d'ouverture de session sont conservés sauf si l'ordinateur est supprimé du domaine ou si les paramètres d'ouverture de session sont modifiés manuellement.

Avant d'ouvrir une session sur le domaine, effectuez les tâches suivantes :

- Créez des comptes d'utilisateurs dans Utilisateurs et ordinateurs Active Directory. Chaque utilisateur doit avoir un compte d'utilisateur des services de domaine Active Directory dans Utilisateurs et ordinateurs Active Directory. Pour plus d'informations, voir Créer un compte d'utilisateur dans Utilisateurs et ordinateurs Active Directory.

- Vérifiez que les adresses IP sont correctement configurées. Pour joindre un ordinateur au domaine, l'ordinateur doit avoir une adresse IP. Dans ce guide, les serveurs sont configurés avec des adresses IP statiques et les ordinateurs clients reçoivent des baux d'adresses IP du serveur DHCP. C'est pourquoi, le serveur DHCP doit être déployé avant que vous ne joigniez des clients au domaine. Pour plus d'informations, consultez Déploiement de DHCP1.

- Joignez l'ordinateur au domaine. Tout ordinateur fournissant des ressources réseau ou y accédant doit être joint au domaine. Pour plus d'informations, voir Joindre des ordinateurs au domaine et ouvrir une session et Joindre des ordinateurs clients au domaine et ouvrir une session.

Planification du déploiement du serveur DHCP1

Cette section décrit les principales étapes de planification qui doivent être suivies avant d'installer le rôle serveur DHCP sur DHCP1.

Planification des serveurs DHCP et de l'acheminement DHCP

Les messages DHCP étant des messages de diffusion, ils ne sont pas acheminés entre les sous-réseaux par les routeurs. Si vous avez plusieurs sous-réseaux et souhaitez proposer le service DHCP sur chacun d'eux, vous devez procéder comme suit :

- Installez un serveur DHCP sur chaque sous-réseau.

- Configurez les routeurs pour qu'ils acheminent les messages de diffusion DHCP dans les sous-réseaux et configurez plusieurs étendues sur le serveur DHCP, à raison d'une étendue par sous-réseau.

En règle générale, il est économiquement plus avantageux de configurer des routeurs pour qu'ils acheminent les messages de diffusion DHCP plutôt que de déployer un serveur DHCP sur chaque segment physique du réseau.

Planification de plages d'adresses IP

Chaque sous-réseau doit avoir sa propre plage d'adresses IP unique. Ces plages sont représentées sur un serveur DHCP avec des étendues.

Une étendue est un groupement administratif des adresses IP des ordinateurs d'un sous-réseau qui utilisent le service DHCP. L'administrateur crée d'abord une étendue pour chaque sous-réseau physique, puis utilise l'étendue pour définir les paramètres utilisés par les clients.

Une étendue possède les propriétés suivantes :

- une plage d'adresses IP où inclure ou exclure les adresses utilisées pour les offres de bail de service DHCP ;
- un masque de sous-réseau, qui détermine le préfixe de sous-réseau correspondant à une adresse IP donnée ;
- un nom affecté à l'étendue lors de sa création ;
- des valeurs de durée de bail, qui sont affectées aux clients DHCP recevant des adresses IP allouées de manière dynamique ;
- des options d'étendue DHCP configurées pour être affectées aux clients DHCP, telles que l'adresse IP d'un serveur DNS et l'adresse IP d'un routeur/d'une passerelle par défaut ;
- des réservations, utilisées de manière optionnelle pour s'assurer qu'un client DHCP reçoit toujours la même adresse IP.

Avant de déployer vos serveurs, dressez la liste de vos sous-réseaux et des plages d'adresses IP à utiliser pour chaque sous-réseau.

Planification des masques de sous-réseaux

Au sein d'une adresse IP, les ID de réseau et les ID d'hôte sont différenciés à l'aide d'un masque de sous-réseau. Chaque masque de sous-réseau est un nombre de 32 bits qui utilise des groupes de bits consécutifs composés uniquement de 1 pour identifier l'ID de réseau et composés uniquement de 0 pour identifier les parties de l'adresse IP relatives à l'ID d'hôte.

Par exemple, un masque de sous-réseau normalement utilisé avec l'adresse IP 131.107.16.200 correspond au nombre binaire de 32 bits suivant :

```
11111111 11111111 00000000 00000000
```

Ce numéro de masque de sous-réseau est formé de 16 bits de valeur 1, suivis de 16 bits de valeur zéro, indiquant que les sections ID de réseau et ID d'hôte de cette adresse IP ont toutes deux une longueur de 16 bits. Ce masque de sous-réseau est affiché en notation décimale séparée par des points sous la forme 255.255.0.0.

Le tableau ci-dessous indique les masques de sous-réseau des classes d'adresses Internet.

Agrandir le tableau

Classe Address	Bits du masque de sous-réseau	Masque de sous-réseau
Classe A	11111111 00000000 00000000 00000000	255.0.0.0
Classe B	11111111 11111111 00000000 00000000	255.255.0.0
Classe C	11111111 11111111 11111111 00000000	255.255.255.0

Lorsque vous créez une étendue dans DHCP et que vous entrez la plage d'adresses IP de cette étendue, DHCP fournit ces valeurs de masque de sous-réseau par défaut. Les valeurs de masque de sous-réseau par défaut conviennent généralement pour la plupart des réseaux qui ne nécessitent aucune configuration particulière et où chaque segment de réseau IP correspond au même réseau physique.

Dans d'autres cas, vous pourrez utiliser des masques de sous-réseau personnalisés pour implémenter la mise en sous-réseau IP. Dans le cadre de la mise en sous-réseau IP, vous pouvez subdiviser la partie ID d'hôte par défaut d'une adresse IP pour spécifier des sous-réseaux, qui sont des sous-divisions de l'ID de réseau basé sur la classe.

En personnalisant la longueur du masque de sous-réseau, vous pouvez réduire le nombre de bits utilisés pour l'ID d'hôte.

Pour éviter les problèmes d'adressage et de routage, vous devez veiller à ce que tous les ordinateurs TCP/IP d'un segment réseau utilisent le même masque de sous-réseau et que chaque ordinateur ou périphérique possède une adresse IP unique.

Planification des plages d'exclusion

Lorsque vous définissez une étendue sur un serveur DHCP, vous spécifiez une plage d'adresses IP qui inclut toutes les adresses IP que le serveur DHCP est autorisé à louer aux clients DHCP, tels que les ordinateurs et autres périphériques. Si, par la suite, vous configurez manuellement certains serveurs et autres périphériques avec des adresses IP statiques de la même plage d'adresses IP que le serveur DHCP utilise, vous risquez involontairement d'attribuer à un périphérique une adresse IP qui a déjà été attribuée à un autre périphérique par le serveur DHCP, et de générer ainsi un conflit d'adresse IP.

Vous pouvez éviter ce problème en créant une plage d'exclusion pour l'étendue DHCP. Une plage d'exclusion est une séquence d'adresses IP, au sein de la plage d'adresses IP de l'étendue, qui ne peuvent pas être utilisées par le serveur DHCP. Si vous créez une plage d'exclusion, le serveur DHCP ne peut attribuer aucune des adresses de cette plage. Vous pouvez alors attribuer manuellement ces adresses sans risque de générer un conflit d'adresse IP.

Vous pouvez exclure des adresses IP de la distribution par le serveur DHCP en créant une plage d'exclusion pour chaque étendue. Vous devez utiliser des exclusions pour tous les périphériques configurés avec une adresse IP statique. Dans les adresses exclues doivent figurer toutes les adresses IP que vous avez attribuées manuellement à d'autres serveurs DHCP, clients non DHCP, stations de travail sans disque ou clients de routage et d'accès à distance et clients PPP.

Il est recommandé de configurer votre plage d'exclusion avec des adresses supplémentaires afin de prendre en compte la croissance future du réseau. Le tableau suivant présente un exemple de plage d'exclusion pour une étendue définie avec une plage d'adresses IP de 10.0.0.1 à 10.0.0.254 et un masque de sous-réseau de 255.255.255.0.

Agrandir le tableau

Éléments de configuration	Exemples de valeurs
Adresse IP de début de la plage d'exclusion	10.0.0.1
Adresse IP de fin de la plage d'exclusion	10.0.0.25

Planification de la configuration TCP/IP statique

Certains périphériques, comme les routeurs, les serveurs DHCP et les serveurs DNS doivent être configurés avec une adresse IP statique. Par ailleurs, vous voudrez peut-être garantir que des périphériques supplémentaires, comme des imprimantes, disposent toujours de la même adresse IP. Dressez la liste des périphériques que vous souhaitez configurer de manière statique pour chaque sous-réseau, puis planifiez la plage d'exclusion que vous voulez utiliser sur le serveur DHCP pour faire en sorte que le serveur DHCP ne loue pas l'adresse IP d'un périphérique configuré de manière statique. Une plage d'exclusion est une séquence limitée d'adresses IP au sein d'une étendue, qui est exclue des offres du service DHCP. Les plages d'exclusion garantissent qu'aucune adresse figurant dans ces plages n'est offerte par le serveur aux clients DHCP sur votre réseau.

Par exemple, si la plage d'adresses IP d'un sous-réseau est 192.168.0.1 à 192.168.0.254 et que vous avez dix appareils que vous souhaitez configurer avec une adresse IP statique, vous pouvez créer une plage d'exclusion pour la version 192.168.0. étendue *x* incluant dix adresses IP ou plus : 192.168.0.1 à 192.168.0.15.

Dans cet exemple, vous utilisez dix des adresses IP exclues pour configurer des serveurs et autres périphériques avec des adresses IP statiques. Il reste cinq adresses IP pour configurer de manière statique de nouveaux périphériques que vous voudrez peut-être ajouter plus tard. Avec cette plage d'exclusion, le serveur DHCP dispose d'un pool d'adresses allant de 192.168.0.16 à 192.168.0.254.

Le tableau suivant fournit des exemples d'éléments de configuration supplémentaires pour les services de domaine Active Directory et DNS :

Agrandir le tableau

Éléments de configuration	Exemples de valeurs
Liaisons de connexion réseau	Ethernet
Paramètres du serveur DNS	DC1.corp.contoso.com
Adresse IP du serveur DNS préféré	10.0.0.2
Valeurs de la boîte de dialogue Ajouter un étendue 1. Nom de l'étendue 2. Adresse IP de début 3. Adresse IP de fin 4. Masque de sous-réseau 5. Passerelle par défaut (facultatif) 6. Durée du bail	1. Sous-réseau principal 2. 10.0.0.1 3. 10.0.0.254 4. 255.255.255.0 5. 10.0.0.1 6. 8 jours
Mode d'opération du serveur DHCP IPv6	Non activé

Déploiement d'un réseau de base

Le déploiement d'un réseau de base comprend les étapes suivantes :

1. Configuration de tous les serveurs
2. Déploiement de DC1
3. Jonction des serveurs au domaine et ouverture d'une session
4. Déploiement de DHCP1
5. Jonction des ordinateurs clients au domaine et ouverture d'une session
6. Déploiement des fonctionnalités facultatives pour l'authentification d'accès réseau et les services Web

Notes

- Les commandes Windows PowerShell équivalentes sont fournies pour la plupart des procédures décrites dans ce guide. Avant d'exécuter ces applets de commande dans Windows PowerShell, remplacez les exemples de valeurs par les valeurs qui sont appropriées pour votre déploiement de réseau. Par ailleurs, veillez à entrer chaque

applet de commande sur une ligne distincte dans Windows PowerShell. Dans ce guide, certaines applets de commande peuvent se présenter sur plusieurs lignes en raison des contraintes de mise en forme et des paramètres d'affichage définis dans votre navigateur ou toute autre application.

- Les procédures décrites dans ce guide ne donnent aucune instruction dans le cas où la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre pour demander votre autorisation de continuer. Si cette boîte de dialogue s'ouvre pendant que vous effectuez les procédures de ce guide et si la boîte de dialogue a été ouverte en réponse à vos actions, cliquez sur **Continuer**.

Configuration de tous les serveurs

Avant d'installer d'autres technologies, comme les services de domaine Active Directory ou DHCP, assurez-vous d'effectuer les tâches suivantes :

- Renommer l'ordinateur
- Configurer une adresse IP statique

Vous pouvez utiliser les sections suivantes pour effectuer ces tâches sur chaque serveur.

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer ces procédures.

Renommer l'ordinateur

Vous pouvez utiliser la procédure de cette section pour changer le nom d'un ordinateur. Cela peut être utile si vous souhaitez modifier un nom d'ordinateur qui a été créé automatiquement par le système d'exploitation.

Notes

Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez les applets de commande suivantes sur des lignes distinctes, puis appuyez sur ENTRÉE. Vous devez également remplacer *ComputerName* par le nom que vous souhaitez utiliser.

`Rename-Computer` *ComputerName*

`Restart-Computer`

Pour renommer les ordinateurs exécutant Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012

1. Dans le Gestionnaire de serveur, cliquez sur **Serveur local**. Les **propriétés** de l'ordinateur sont affichées dans le volet d'informations.

2. Dans **Propriétés**, dans le **nom de l'ordinateur**, cliquez sur le nom de l'ordinateur existant. La boîte de dialogue **Propriétés système** s'ouvre. Cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.

3. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, dans **Nom de l'ordinateur**, tapez le nouveau nom à attribuer à l'ordinateur. Par exemple, si vous souhaitez nommer l'ordinateur DC1, tapez **DC1**.

4. Cliquez deux fois sur **OK** , puis sur **Fermer**. Si vous souhaitez redémarrer l'ordinateur immédiatement pour terminer la modification du nom, cliquez sur **Redémarrer maintenant**. Sinon, cliquez sur **Redémarrer ultérieurement**.

> ⓘ **Notes**
>
> Pour plus d'informations sur la façon de renommer les ordinateurs exécutant d'autres systèmes d'exploitation Microsoft, consultez l'Annexe A - Changement de nom des ordinateurs.

Configurer une adresse IP statique

Vous pouvez utiliser les procédures de cette rubrique afin de configurer les propriétés du protocole IPv4 (Internet Protocol version 4) d'une connexion réseau avec une adresse IP statique pour les ordinateurs exécutant Windows Server 2016.

> ⓘ **Notes**
>
> Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez les applets de commande suivantes sur des lignes distinctes, puis appuyez sur ENTRÉE. Remplacez les noms d'interface et les adresses IP utilisés dans cet exemple par les valeurs de configuration souhaitées pour votre ordinateur.
>
> `New-NetIPAddress -IPAddress 10.0.0.2 -InterfaceAlias "Ethernet" -DefaultGateway 10.0.0.1 -AddressFamily IPv4 -PrefixLength 24`
>
> `Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 127.0.0.1`

Pour configurer une adresse IP statique sur les ordinateurs exécutant Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012

1. Dans la barre des tâches, cliquez avec le bouton droit sur l'icône Réseau, puis cliquez sur **Ouvrir le Centre Réseau et partage**.

2. Dans **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de la carte**. Le dossier **Connexions réseau** s'ouvre et affiche les connexions réseau disponibles.

3. Dans **Connexions réseau**, cliquez avec le bouton droit sur la connexion que vous souhaitez configurer, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés** de la connexion réseau s'ouvre.

4. Dans la boîte de dialogue **Propriétés** de la connexion réseau, dans **Cette connexion utilise les éléments suivants**, sélectionnez **Internet Protocol Version 4 (TCP/IPv4),** puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés de Protocole Internet version 4 (TCP/IPv4)** s'ouvre.

5. Dans **Propriétés de Protocole Internet version 4 (TCP/IPv4)**, sous l'onglet **Général**, cliquez sur **Utiliser l'adresse IP suivante**. Dans **l'adresse IP**, tapez l'adresse IP que vous souhaitez utiliser.

6. Appuyez sur Tab pour placer le curseur dans le **masque de sous-réseau**. Une valeur par défaut pour le masque de sous-réseau est entrée automatiquement. Acceptez le masque de sous-réseau par défaut, ou tapez le masque de sous-réseau que vous voulez utiliser.

7. Dans **la passerelle par défaut**, tapez l'adresse IP de votre passerelle par défaut.

> ⓘ **Notes**
>
> Vous devez configurer la **passerelle par défaut** avec la même adresse IP que celle que vous utilisez sur l'interface réseau local (LAN) de votre routeur. Par exemple, si vous disposez d'un routeur connecté à un réseau étendu (WAN), tel que l'Internet et votre réseau local, configurez l'interface LAN avec la même adresse IP que celle que vous spécifiez comme **passerelle par défaut**. Prenons comme autre exemple un routeur qui est connecté à un réseau local LAN A et à un réseau local LAN B utilisant respectivement les plages d'adresses 10.0.0.0/24 et 192.168.0.0/24. Vous devez configurer l'adresse IP du routeur du réseau LAN A avec une adresse de la plage d'adresses 10.0.0.0/24, telle que 10.0.0.1. En outre, dans l'étendue DHCP de cette plage d'adresses, configurez la **passerelle par défaut** avec l'adresse IP 10.0.0.1. Pour le réseau local B, configurez l'interface de routeur LAN B avec une adresse de cette

plage d'adresses, par exemple 192.168.0.1, puis configurez l'étendue B LAN B 192.168.0.0/24 avec une valeur de **passerelle par défaut** de 192.168.0.1.

8. Dans **Serveur DNS préféré**, tapez l'adresse IP de votre serveur DNS. Si vous envisagez d'utiliser l'ordinateur local comme serveur DNS préféré, tapez son adresse IP.
9. Dans **Serveur DNS auxiliaire**, tapez l'adresse IP de votre serveur DNS auxiliaire, le cas échéant. Si vous envisagez d'utiliser l'ordinateur local comme serveur DNS auxiliaire, tapez son adresse IP.
10. Cliquez sur **OK**, puis sur **Fermer**.

> ⓘ **Notes**
>
> Pour plus d'informations sur la configuration d'une adresse IP statique sur les ordinateurs exécutant d'autres systèmes d'exploitation Microsoft, consultez l'**Annexe B - Configuration d'adresses IP statiques**.

Déploiement de DC1

Pour déployer le serveur DC1, qui exécute les services de domaine Active Directory (AD DS) et DNS, vous devez effectuer les étapes suivantes dans l'ordre indiqué :

- Effectuer la procédure indiquée dans la section Configuration de tous les serveurs
- Installer les services de domaine Active Directory et DNS dans une nouvelle forêt
- Créer un compte d'utilisateur dans Utilisateurs et ordinateurs Active Directory
- Attribuer des membres aux groupes
- Configurer une zone de recherche inversée DNS

Privilèges d'administration

Si vous installez un petit réseau dont vous êtes le seul administrateur, nous vous recommandons de créer un compte d'utilisateur pour vous-même, puis d'ajouter votre compte d'utilisateur en tant que membre des groupes Administrateurs de l'entreprise et Administrateurs du domaine. Vous pourrez ainsi plus facilement jouer le rôle d'administrateur pour toutes les ressources réseau. Nous vous recommandons également d'ouvrir une session avec ce compte uniquement lorsque vous avez besoin d'effectuer des tâches d'administration et de créer un autre compte d'utilisateur pour réaliser les tâches non informatiques.

Dans une organisation de plus grande taille comptant plusieurs administrateurs, reportez-vous à la documentation des services de domaine Active Directory pour déterminer à quels groupes il est préférable que les utilisateurs appartiennent.

Différences entre les comptes d'utilisateurs de domaine et les comptes d'utilisateurs sur l'ordinateur local

L'un des avantages d'une infrastructure reposant sur des domaines est qu'il n'est pas nécessaire de créer des comptes d'utilisateurs sur chaque ordinateur du domaine. Ceci vaut que l'ordinateur soit un ordinateur client ou un serveur.

Par conséquent, vous ne devez pas créer des comptes d'utilisateurs sur chaque ordinateur du domaine. Créez tous les comptes d'utilisateurs dans Utilisateurs et ordinateurs Active Directory et utilisez les procédures précédentes pour attribuer des membres aux groupes. Par défaut, tous les comptes d'utilisateurs sont membres du groupe Utilisateurs du domaine.

Tous les membres du groupe Utilisateurs du domaine peuvent ouvrir une session sur un ordinateur client qui a été joint au domaine.

Vous pouvez configurer les comptes d'utilisateurs de sorte qu'ils indiquent les jours et les heures auxquels l'utilisateur est autorisé à ouvrir une session sur l'ordinateur. Vous pouvez également désigner les ordinateurs que chaque utilisateur est autorisé à utiliser. Pour configurer ces paramètres, ouvrez Utilisateurs et ordinateurs Active Directory, recherchez le compte d'utilisateur à configurer, puis double-cliquez sur ce compte. Dans les **propriétés** du compte d'utilisateur, cliquez sur l'onglet **Compte** , puis sur **Heures** de **connexion ou Connectez-vous**.

Installer les services de domaine Active Directory et DNS dans une nouvelle forêt

Vous pouvez utiliser l'une des procédures suivantes pour installer Active Directory Domain Services (AD DS) et DNS, et pour créer un domaine dans une forêt.

La première procédure fournit des instructions sur l'exécution de ces actions à l'aide de Windows PowerShell, tandis que la deuxième vous montre comment installer AD DS et DNS en utilisant le Gestionnaire de serveur.

> ⓘ **Important**
>
> Une fois que vous avez effectué les étapes de cette procédure, l'ordinateur redémarre automatiquement.

Installer AD DS et DNS à l'aide de Windows PowerShell

Vous pouvez utiliser les commandes suivantes pour installer et configurer AD DS et DNS. Vous devez remplacer le nom de domaine dans cet exemple par la valeur à utiliser pour votre domaine.

> **Notes**
>
> Pour plus d'informations sur ces commandes Windows PowerShell, consultez les rubriques de référence suivantes.
>
> - Install-WindowsFeature
> - Install-ADDSForest

L'appartenance aux **administrateurs** est la valeur minimale requise pour effectuer cette procédure.

- Exécutez Windows PowerShell en tant qu'administrateur, tapez la commande suivante, puis appuyez sur ENTRÉE :

PowerShell

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools`
```

Une fois l'installation correctement effectuée, le message suivant s'affiche dans Windows PowerShell.

Agrandir le tableau

Success	Redémarrer nécessaire	Code de sortie	Résultat de la fonctionnalité
True	No	Success	{Services de domaine Active Directory, groupe P...

- Dans Windows PowerShell, tapez la commande suivante, en remplaçant le texte **corp.contoso.com** par votre nom de domaine, puis appuyez sur Entrée :

PowerShell

```
Install-ADDSForest -DomainName "corp.contoso.com"
```

- Durant le processus d'installation et de configuration, qui est visible en haut de la fenêtre Windows PowerShell, l'invite suivante s'affiche. Une fois qu'elle s'est affichée, tapez un mot de passe, puis appuyez sur ENTRÉE.

SafeModeAdministratorPassword:

- Une fois que vous avez tapé un mot de passe et appuyé sur ENTRÉE, l'invite de confirmation suivante s'affiche. Tapez le même mot de passe, puis appuyez sur ENTRÉE.

Confirmez SafeModeAdministratorPassword :

- Lorsque l'invite suivante s'affiche, tapez la lettre **Y** , puis appuyez sur Entrée.

```
The target server will be configured as a domain controller and restarted
when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

- Si vous le souhaitez, vous pouvez lire les messages d'avertissement qui s'affichent durant une installation normale réussie d'AD DS et de DNS. Ces messages sont normaux et n'indiquent pas un échec de l'installation.

- Une fois l'installation réussie, un message s'affiche pour vous indiquer que vous êtes sur le point d'être déconnecté de l'ordinateur afin qu'il puisse redémarrer. Si vous cliquez sur **Fermer**, vous êtes immédiatement déconnecté de l'ordinateur et l'ordinateur redémarre. Si vous ne cliquez pas sur **Fermer**, l'ordinateur redémarre après une période de temps par défaut.

- Une fois le serveur redémarré, vous pouvez vérifier si l'installation d'Active Directory Domain Services (AD DS) et de DNS a réussi. Ouvrez Windows PowerShell, tapez la commande suivante, puis appuyez sur ENTRÉE.

PowerShell

```
Get-WindowsFeature
```

Les résultats de cette commande s'affichent dans Windows PowerShell, et doivent être similaires aux résultats de l'image ci-dessous. Pour les technologies installées, les crochets à gauche du nom de la technologie contiennent le caractère **X** et la valeur de **l'état d'installation** est **installée**.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS D:\Users\jm> Get-WindowsFeature

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[ ] Active Directory Certificate Services               AD-Certificate                 Available
    [ ] Certification Authority                         ADCS-Cert-Authority            Available
    [ ] Certificate Enrollment Policy Web Service       ADCS-Enroll-Web-Pol            Available
    [ ] Certificate Enrollment Web Service              ADCS-Enroll-Web-Svc            Available
    [ ] Certification Authority Web Enrollment          ADCS-Web-Enrollment            Available
    [ ] Network Device Enrollment Service               ADCS-Device-Enrollment         Available
    [ ] Online Responder                                ADCS-Online-Cert               Available
[X] Active Directory Domain Services                    AD-Domain-Services             Installed
[ ] Active Directory Federation Services                ADFS-Federation                Available
[ ] Active Directory Lightweight Directory Services     ADLDS                          Available
[ ] Active Directory Rights Management Services         ADRMS                          Available
    [ ] Active Directory Rights Management Server       ADRMS-Server                   Available
    [ ] Identity Federation Support                     ADRMS-Identity                 Available
[ ] Device Health Attestation                           DeviceHealthAttestat...        Available
[ ] DHCP Server                                         DHCP                           Available
[X] DNS Server                                          DNS                            Installed
```

Installer AD DS et DNS à l'aide du Gestionnaire de serveur

1. Sur DC1, dans **le Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.

2. Dans **Avant de commencer**, cliquez sur **Suivant**.

   > ⓘ Notes
   >
   > La page **Avant de commencer** de l'Assistant Ajout de rôles et de fonctionnalités ne s'affiche pas si vous avez préalablement sélectionné **Ignorer cette page par défaut** dans l'Assistant.

3. Dans **Sélectionner le type d'installation**, vérifiez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.

4. Dans **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné. Dans le **pool de serveurs**, vérifiez que l'ordinateur local est sélectionné. Cliquez sur **Suivant**.

5. Dans **Sélectionner des rôles de serveurs**, dans **Rôles**, cliquez sur **Services de domaine Active Directory**. Dans **Ajouter les fonctionnalités requises pour les services de domaine Active Directory**, cliquez sur **Ajouter des fonctionnalités**. Cliquez sur **Suivant**.

6. Dans **Sélectionner des fonctionnalités**, cliquez sur **Suivant**, puis, dans **Les services de domaine Active Directory**, passez en revue les informations fournies, puis cliquez sur **Suivant**.

7. Dans **Confirmer les sélections pour l'installation**, cliquez sur **Installer**. La page de progression de l'installation indique l'état du processus d'installation. À la fin du

processus, dans les détails du message, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**. L'Assistant Configuration des services de domaine Active Directory s'ouvre.

8. Dans **Configuration du déploiement**, sélectionnez **Ajouter une nouvelle forêt**. Dans **Nom de domaine racine**, tapez le nom de domaine complet (FQDN) du domaine. Par exemple, si votre nom de domaine complet est corp.contoso.com, tapez **corp.contoso.com**. Cliquez sur **Suivant**.

9. Dans **Options du contrôleur de domaine**, dans **Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine**, sélectionnez le niveau fonctionnel souhaité pour la forêt et le domaine. Dans **Spécifier les fonctionnalités de contrôleur de domaine**, vérifiez que **Serveur DNS (Domain Name System)** et **Catalogue global (GC)** sont sélectionnés. Dans **Mot de passe** et **Confirmer le mot de passe**, tapez le mot de passe du mode de restauration des services d'annuaire (DSRM) que vous souhaitez utiliser. Cliquez sur **Suivant**.

10. Dans **Options DNS**, cliquez sur **Suivant**.

11. Dans **Options supplémentaires**, vérifiez le nom NetBIOS affecté au domaine et modifiez-le uniquement si nécessaire. Cliquez sur **Suivant**.

12. Dans **Chemins d'accès**, dans **Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et SYSVOL, effectuez** l'une des opérations suivantes :

    - Acceptez la valeur par défaut.

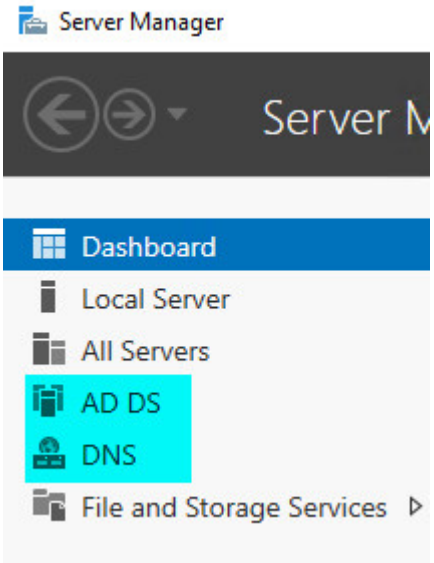
    - Tapez les emplacements des dossiers que vous souhaitez utiliser pour le **dossier De base de données**, le **dossier Fichiers journaux** et le **dossier SYSVOL**.

13. Cliquez sur **Suivant**.

14. Dans **Options de révision**, passez en revue vos sélections.

15. Si vous souhaitez exporter des paramètres vers un script Windows PowerShell, cliquez sur **Afficher le script**. Le script s'ouvre dans le Bloc-notes. Vous pouvez ensuite l'enregistrer à l'emplacement de dossier de votre choix. Cliquez sur **Suivant**. Dans **Vérification des conditions préalables**, vos sélections sont validées. Une fois la vérification terminée, cliquez sur **Installer**. Lorsque vous y êtes invité par Windows, cliquez sur **Fermer**. Le serveur redémarre pour effectuer l'installation d'AD DS et de DNS.

16. Pour vérifier la réussite de l'installation, visualisez la console du Gestionnaire de serveur après le redémarrage du serveur. AD DS et DNS doivent apparaître dans le volet gauche, comme le montre les éléments mis en surbrillance dans l'image ci-dessous.



Créer un compte d'utilisateur dans Utilisateurs et ordinateurs Active Directory

Vous pouvez utiliser cette procédure pour créer un compte d'utilisateur de domaine dans la console MMC (Microsoft Management Console) Utilisateurs et ordinateurs Active Directory.

L'appartenance aux **administrateurs de domaine** ou équivalent est la condition minimale requise pour effectuer cette procédure.

> ⓘ **Notes**
>
> Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez l'applet de commande suivante sur une seule ligne, puis appuyez sur ENTRÉE. Remplacez le nom de compte d'utilisateur utilisé dans cet exemple par le nom de votre choix.
>
> `New-ADUser -SamAccountName User1 -AccountPassword (read-host "Set user password" -assecurestring) -name "User1" -enabled $true -PasswordNeverExpires $true -ChangePasswordAtLogon $false`
>
> Après avoir appuyé sur ENTRÉE, tapez le mot de passe du compte d'utilisateur. Le compte ainsi créé appartient par défaut au groupe Utilisateurs du domaine.
>
> Si vous le souhaitez, vous pouvez ajouter ce nouveau compte d'utilisateur à d'autres groupes en utilisant l'applet de commande suivante. Dans cet exemple, User1 est ajouté aux deux groupes Administrateurs du domaine et Administrateurs de l'entreprise. Avant d'exécuter la commande ci-dessous, remplacez les exemples de nom de compte d'utilisateur, de nom de domaine et de groupes par les valeurs souhaitées.

```
Add-ADPrincipalGroupMembership -Identity
"CN=User1,CN=Users,DC=corp,DC=contoso,DC=com" -MemberOf "CN=Enterprise
Admins,CN=Users,DC=corp,DC=contoso,DC=com","CN=Domain
Admins,CN=Users,DC=corp,DC=contoso,DC=com"
```

Pour créer un compte d'utilisateur

1. Sur DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. La console MMC Utilisateurs et ordinateurs Active Directory s'ouvre. Si le nœud de votre domaine n'est pas encore sélectionné, cliquez dessus. Par exemple, si votre domaine est corp.contoso.com, cliquez **sur corp.contoso.com**.

2. Dans le volet d'informations, cliquez avec le bouton droit sur le dossier auquel ajouter un compte d'utilisateur.

   Where?

   - Dossier utilisateurs et ordinateurs/*nœud*/ de domaine Active Directory

3. Pointez sur **Nouveau**, puis cliquez sur **Utilisateur**. La boîte de dialogue **Nouvel objet - Utilisateur** s'ouvre.

4. Dans **Prénom**, tapez le prénom de l'utilisateur.

5. Dans **Initials**, tapez les initiales de l'utilisateur.

6. Dans **Nom**, tapez le nom de l'utilisateur.

7. Modifiez **le nom complet** pour ajouter des initiales ou inverser l'ordre des prénoms et des noms.

8. Dans **Nom d'ouverture de session de l'utilisateur**, tapez le nom d'ouverture de session de l'utilisateur. Cliquez sur **Suivant**.

9. Dans **Nouvel objet - Utilisateur**, dans **Mot de passe** et **Confirmer le mot de passe**, tapez le mot de passe de l'utilisateur, puis sélectionnez les options de mot de passe appropriées.

10. Cliquez **sur Suivant**, passez en revue les nouveaux paramètres du compte d'utilisateur, puis cliquez sur **Terminer**.

Attribuer des membres aux groupes

Vous pouvez utiliser cette procédure pour ajouter un utilisateur, un ordinateur ou un groupe à un groupe dans la console MMC (Microsoft Management Console) Utilisateurs et ordinateurs Active Directory.

L'appartenance aux **administrateurs de domaine** ou équivalente est la condition minimale requise pour effectuer cette procédure.

Pour attribuer des membres à un groupe

1. Sur DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. La console MMC Utilisateurs et ordinateurs Active Directory s'ouvre. Si le nœud de votre domaine n'est pas encore sélectionné, cliquez dessus. Par exemple, si votre domaine est corp.contoso.com, cliquez **sur corp.contoso.com**.

2. Dans le volet d'informations, double-cliquez sur le dossier qui contient le groupe auquel ajouter un membre.

   Where?

   - **Utilisateurs et ordinateurs Active Directory**/*nœud de domaine/dossier qui contient le groupe*

3. Dans le volet d'informations, cliquez avec le bouton droit sur l'objet que vous souhaitez ajouter à un groupe, tel qu'un utilisateur ou un ordinateur, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés** de l'objet s'ouvre. Cliquez sur le **membre de l'onglet** .

4. Sous **l'onglet Membre** , cliquez sur **Ajouter**.

5. Dans **Entrez les noms des objets à sélectionner**, tapez le nom du groupe auquel vous voulez ajouter l'objet, puis cliquez sur **OK**.

6. Pour attribuer d'autres utilisateurs, groupes ou ordinateurs au groupe, répétez les étapes 4 et 5 de cette procédure.

Configurer une zone de recherche inversée DNS

Vous pouvez utiliser cette procédure pour configurer une zone de recherche inversée dans DNS (Domain Name System).

L'appartenance aux **administrateurs de domaine** est la valeur minimale requise pour effectuer cette procédure.

> ⓘ **Notes**

- Pour les moyennes et les grandes organisations, il est recommandé de configurer et d'utiliser le groupe DNSAdmins dans Utilisateurs et ordinateurs Active Directory. Pour plus d'informations, voir **Ressources techniques supplémentaires**.
- Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez l'applet de commande suivante sur une seule ligne, puis appuyez sur ENTRÉE. Remplacez les noms de zone de recherche inversée DNS et de fichier de zone utilisés dans cet exemple par les noms de votre choix. Veillez à inverser l'ordre de l'ID réseau dans le nom de la zone de recherche inversée. Par exemple, si l'ID réseau est 192.168.0, créez le nom de zone de recherche inverse **0.168.192.in-addr.arpa**.

```
Add-DnsServerPrimaryZone 0.0.10.in-addr.arpa -ZoneFile 0.0.10.in-addr.arpa.dns
```

Pour configurer une zone de recherche inversée DNS

1. Sur DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**. La console MMC DNS s'ouvre.
2. Dans DNS, le cas échéant, double-cliquez sur le nom du serveur pour développer son arborescence. Par exemple, si le nom du serveur DNS est DC1, double-cliquez sur **DC1**.
3. Sélectionnez **Zones de recherche inversée**, cliquez dessus avec le bouton droit, puis cliquez sur **Nouvelle zone**. L'Assistant Nouvelle Zone s'ouvre.
4. Sur la page **Bienvenue !**, cliquez sur **Suivant**.
5. Dans **Type de zone**, sélectionnez **Zone principale**.
6. Si votre serveur DNS est un contrôleur de domaine accessible en écriture, vérifiez que **Enregistrer la zone dans Active Directory** est sélectionné. Cliquez sur **Suivant**.
7. Dans **Étendue de la zone de réplication de Active Directory**, sélectionnez **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine**, sauf si vous souhaitez spécifiquement choisir une autre option. Cliquez sur **Suivant**.
8. Dans la première page **Nom de la zone de recherche inversée**, sélectionnez **Zone de recherche inversée IPv4**. Cliquez sur **Suivant**.
9. Dans la seconde page **Nom de la zone de recherche inversée**, effectuez l'une des opérations suivantes :

- Dans **l'ID réseau**, tapez l'ID réseau de votre plage d'adresses IP. Par exemple, si votre plage d'adresses IP est 10.0.0.1 à 10.0.0.254, tapez **10.0.0.**
- Le nom de votre zone de recherche inversée IPv4 est automatiquement ajouté dans **Nom de la zone de recherche inversée**. Cliquez sur **Suivant**.

10. Dans **La mise à jour** dynamique, sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser. Cliquez sur **Suivant**.
11. Dans **Fin de l'Assistant Nouvelle zone**, passez en revue vos sélections, puis cliquez sur **Terminer**.

Jonction des serveurs au domaine et ouverture d'une session

Une fois que vous avez installé les services de domaine Active Directory (AD DS) et créé un ou plusieurs comptes d'utilisateur autorisés à joindre un ordinateur au domaine, vous pouvez joindre des serveurs du réseau de base au domaine, puis ouvrir une session sur ces serveurs pour y installer d'autres technologies, telles que le protocole DHCP (Dynamic Host Configuration Protocol).

Sur tous les serveurs en cours de déploiement, à l'exception du serveur exécutant les services de domaine Active Directory, procédez comme suit :

1. Effectuez les procédures indiquées dans Configuration de tous les serveurs.
2. Utilisez les instructions indiquées dans les deux procédures suivantes pour joindre vos serveurs au domaine et ouvrir une session sur ces serveurs afin de réaliser des tâches de déploiement supplémentaires :

> **Notes**
>
> Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez l'applet de commande suivante, puis appuyez sur ENTRÉE. Remplacez le nom de domaine utilisé dans cet exemple par le nom de votre choix.
>
> ```
> Add-Computer -DomainName corp.contoso.com
> ```
>
> Lorsque vous y êtes invité, tapez le nom d'utilisateur et le mot de passe d'un compte qui est autorisé à joindre un ordinateur au domaine. Pour redémarrer l'ordinateur, tapez la commande suivante, puis appuyez sur ENTRÉE.
>
> ```
> Restart-Computer
> ```

Pour joindre des ordinateurs exécutant Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012 au domaine

1. Dans le Gestionnaire de serveur, cliquez sur **Serveur local**. Dans le volet d'informations, cliquez sur **WORKGROUP**. La boîte de dialogue **Propriétés système** s'ouvre.

2. Dans la boîte de dialogue **Propriétés système** , cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.

3. Dans **Nom de l'ordinateur**, dans **Membre de**, cliquez sur **Domaine**, puis tapez le nom du domaine que vous souhaitez joindre. Par exemple, si le nom de domaine est corp.contoso.com, tapez **corp.contoso.com**.

4. Cliquez sur **OK**. La boîte de dialogue **Sécurité Windows** s'ouvre.

5. Dans **Modification du nom ou du domaine de l'ordinateur**, dans **Nom d'utilisateur**, tapez le nom d'utilisateur. Dans **Mot de passe**, tapez le mot de passe, puis cliquez sur **OK**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre et vous souhaite la bienvenue dans le domaine. Cliquez sur **OK**.

6. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** affiche un message indiquant que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **OK**.

7. Dans la boîte de dialogue **Propriétés système**, sous l'onglet Nom de **l'ordinateur**, cliquez sur Fermer. La boîte de dialogue **Microsoft Windows** s'ouvre et affiche un message, indiquant à nouveau que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **Redémarrer maintenant**.

> ⓘ **Notes**
>
> Pour plus d'informations sur la façon de joindre des ordinateurs exécutant d'autres systèmes d'exploitation Microsoft au domaine, consultez l'Annexe C - Jonction d'ordinateurs au domaine.

Pour se connecter au domaine à l'aide d'ordinateurs exécutant Windows Server 2016

1. Fermez la session sur l'ordinateur et redémarrez-le.

2. Appuyez sur Ctrl+Alt+Suppr. L'écran d'ouverture de session s'affiche.

3. Dans le coin inférieur gauche, cliquez sur **Autre utilisateur**.

4. Dans **Nom d'utilisateur**, tapez votre nom d'utilisateur.
5. Dans **Mot de passe**, tapez votre mot de passe de domaine, puis cliquez sur la flèche, ou appuyez sur Entrée.

> ⓘ **Notes**
>
> Pour plus d'informations sur la connexion au domaine à l'aide d'ordinateurs exécutant d'autres systèmes d'exploitation Microsoft, consultez l'Annexe D - Connexion au domaine.

Déploiement de DHCP1

Avant de déployer ce composant sur le réseau de base, vous devez effectuer les actions suivantes :

- Effectuer la procédure indiquée dans la section Configuration de tous les serveurs
- Effectuer la procédure indiquée dans la section Jonction des serveurs au domaine et ouverture d'une session

Pour déployer le serveur DHCP1, qui exécute le rôle serveur DHCP (Dynamic Host Configuration Protocol), vous devez effectuer les étapes suivantes dans l'ordre indiqué :

- Installer DHCP (Dynamic Host Configuration Protocol)
- Créer et activer une nouvelle étendue DHCP

> ⓘ **Notes**
>
> Pour effectuer ces procédures en utilisant Windows PowerShell, ouvrez PowerShell et tapez les applets de commande suivantes sur des lignes distinctes, puis appuyez sur ENTRÉE. Remplacez le nom de l'étendue, les adresses IP de début et de fin de plage, le masque de sous-réseau et autres valeurs utilisés dans cet exemple par les valeurs de votre choix.
>
> `Install-WindowsFeature DHCP -IncludeManagementTools`
>
> `Add-DhcpServerv4Scope -name "Corpnet" -StartRange 10.0.0.1 -EndRange 10.0.0.254 -SubnetMask 255.255.255.0 -State Active`
>
> `Add-DhcpServerv4ExclusionRange -ScopeID 10.0.0.0 -StartRange 10.0.0.1 -EndRange 10.0.0.15`

```
Set-DhcpServerv4OptionValue -OptionID 3 -Value 10.0.0.1 -ScopeID 10.0.0.0 -ComputerName DHCP1.corp.contoso.com

Add-DhcpServerv4Scope -name "Corpnet2" -StartRange 10.0.1.1 -EndRange 10.0.1.254 -SubnetMask 255.255.255.0 -State Active

Add-DhcpServerv4ExclusionRange -ScopeID 10.0.1.0 -StartRange 10.0.1.1 -EndRange 10.0.1.15

Set-DhcpServerv4OptionValue -OptionID 3 -Value 10.0.1.1 -ScopeID 10.0.1.0 -ComputerName DHCP1.corp.contoso.com

Set-DhcpServerv4OptionValue -DnsDomain corp.contoso.com -DnsServer 10.0.0.2

Add-DhcpServerInDC -DnsName DHCP1.corp.contoso.com
```

Installer DHCP (Dynamic Host Configuration Protocol)

Vous pouvez utiliser cette procédure pour installer et configurer le rôle Serveur DHCP à l'aide de l'Assistant Ajout de rôles et de fonctionnalités.

L'appartenance aux **administrateurs de domaine** ou équivalent est la condition minimale requise pour effectuer cette procédure.

Pour installer DHCP

1. Sur DHCP1, dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.

2. Dans **Avant de commencer**, cliquez sur **Suivant**.

   > ⓘ **Notes**
   >
   > La page **Avant de commencer** de l'Assistant Ajout de rôles et de fonctionnalités ne s'affiche pas si vous avez préalablement sélectionné **Ignorer cette page par défaut** dans l'Assistant.

3. Dans **Sélectionner le type d'installation**, vérifiez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.

4. Dans **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné. Dans le **pool de serveurs**, vérifiez que l'ordinateur local

est sélectionné. Cliquez sur **Suivant**.

5. Dans **Sélectionner les rôles serveur**, dans **Rôles**, sélectionnez **Serveur DHCP**. Dans **Ajouter les fonctionnalités requises pour le serveur DHCP**, cliquez sur **Ajouter des fonctionnalités**. Cliquez sur **Suivant**.

6. Dans **Sélectionner des fonctionnalités**, cliquez sur **Suivant**, puis sur **Serveur DHCP**, passez en revue les informations fournies, puis cliquez sur **Suivant**.

7. Dans **Confirmer les sélections d'installation**, cliquez sur **Redémarrer automatiquement le serveur de destination, si nécessaire**. Lorsque vous êtes invité à confirmer cette sélection, cliquez sur **Oui**, puis sur **Installer**. La page **Progression de l'installation** affiche l'état pendant le processus d'installation. À la fin du processus, le message « Configuration nécessaire. L'installation a réussi sur *ComputerName* » s'affiche, où *ComputerName* est le nom de l'ordinateur sur lequel vous avez installé le serveur DHCP. Dans la fenêtre de message, cliquez sur **Terminer la configuration DHCP**. L'Assistant Configuration post-installation DHCP s'ouvre. Cliquez sur **Suivant**.

8. Dans **Autorisation**, spécifiez les informations d'identification que vous souhaitez utiliser pour autoriser le serveur DHCP dans Les services de domaine Active Directory, puis cliquez sur **Valider**. Une fois l'autorisation terminée, cliquez sur **Fermer**.

Créer et activer une nouvelle étendue DHCP

Vous pouvez utiliser cette procédure pour créer une étendue DHCP à l'aide de la console MMC (Microsoft Management Console) DHCP. Cette procédure permet d'activer une étendue et de définir une plage d'exclusion pour empêcher le serveur DHCP de louer les adresses IP statiques avec lesquelles vous avez configuré vos serveurs et autres périphériques nécessitant ce type d'adresse.

L'appartenance aux **administrateurs DHCP**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour créer et activer une nouvelle étendue DHCP

1. Sur DHCP1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP**. La console MMC DHCP s'ouvre.

2. Dans **DHCP**, développez le nom du serveur. Par exemple, si le nom du serveur DHCP est DHCP1.corp.contoso.com, cliquez sur la flèche vers le bas en regard de **DHCP1.corp.contoso.com**.

3. Sous le nom du serveur, cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**. L'Assistant Nouvelle étendue s'ouvre.

4. Sur la page **Bienvenue !**, cliquez sur **Suivant**.

5. Dans **Nom de l'étendue**, dans **Nom**, tapez un nom pour l'étendue. Par exemple, tapez **Sous-réseau 1**.

6. Dans **Description**, tapez une description pour la nouvelle étendue, puis cliquez sur **Suivant**.

7. Dans **Plage d'adresses IP**, procédez comme suit :

   a. Dans **Adresse IP de début**, tapez la première adresse IP de la plage. Par exemple, tapez **10.0.0.1**.

   b. Dans **Adresse IP de fin**, tapez la dernière adresse IP de la plage. Par exemple, tapez **10.0.0.254**. Les valeurs du masque **de longueur** et de **sous-réseau** sont entrées automatiquement, en fonction de l'adresse IP que vous avez entrée pour **l'adresse IP de démarrage**.

   c. Si nécessaire, modifiez les valeurs du masque **de longueur** ou **de sous-réseau**, le cas échéant pour votre schéma d'adressage.

   d. Cliquez sur **Suivant**.

8. Dans **Ajouter des exclusions**, procédez comme suit :

   a. Dans **Adresse IP de début**, tapez la première adresse IP de la plage d'exclusion. Par exemple, tapez **10.0.0.1**.

   b. Dans **Adresse IP de fin**, tapez la dernière adresse IP de la plage d'exclusion. Par exemple, tapez **10.0.0.15**.

9. Cliquez sur **Ajouter**, puis sur **Suivant**.

10. Dans **Durée du bail**, modifiez les valeurs par défaut pour **Jours**, **Heures** et **Minutes**, selon les besoins de votre réseau, puis cliquez sur **Suivant**.

11. Dans **Configuration des paramètres DHCP**, sélectionnez **Oui, je veux configurer ces options maintenant**, puis cliquez sur **Suivant**.

12. Dans **Routeur (passerelle par défaut)**, effectuez l'une des actions suivantes :

    - Si vous n'avez pas de routeurs sur votre réseau, cliquez sur **Suivant**.

- Dans **l'adresse IP**, tapez l'adresse IP de votre routeur ou de votre passerelle par défaut. Par exemple, tapez **10.0.0.1**. Cliquez sur **Ajouter**, puis sur **Suivant**.

13. Dans **Nom de domaine et serveurs DNS**, procédez comme suit :

    a. Dans **le domaine parent**, tapez le nom du domaine DNS que les clients utilisent pour la résolution de noms. Par exemple, tapez **corp.contoso.com**.

    b. Dans le **nom du serveur**, tapez le nom de l'ordinateur DNS que les clients utilisent pour la résolution de noms. Par exemple, tapez **DC1**.

    c. Cliquez sur **Résoudre**. L'adresse IP du serveur DNS est ajoutée à **l'adresse IP**. Cliquez sur **Ajouter**, attendez que la validation de l'adresse IP du serveur DNS soit terminée, puis cliquez sur **Suivant**.

14. Dans **les serveurs WINS**, car vous n'avez pas de serveurs WINS sur votre réseau, cliquez sur **Suivant**.

15. Dans **Activer l'étendue**, sélectionnez **Oui, je souhaite activer cette étendue maintenant**.

16. Cliquez sur **Suivant**, puis sur **Terminer**.

> **Important**
>
> Si vous souhaitez créer d'autres étendues pour des sous-réseaux supplémentaires, répétez cette procédure. Utilisez une plage d'adresses IP distincte pour chaque sous-réseau que vous prévoyez de déployer et assurez-vous que l'acheminement des messages DHCP est activé sur tous les routeurs d'accès aux autres sous-réseaux.

Jonction des ordinateurs clients au domaine et ouverture d'une session

> **Notes**
>
> Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez l'applet de commande suivante, puis appuyez sur ENTRÉE. Remplacez le nom de domaine utilisé dans cet exemple par le nom de votre choix.
>
> ```
> Add-Computer -DomainName corp.contoso.com
> ```
>
> Lorsque vous y êtes invité, tapez le nom d'utilisateur et le mot de passe d'un compte qui est autorisé à joindre un ordinateur au domaine. Pour redémarrer l'ordinateur, tapez la commande suivante, puis appuyez sur ENTRÉE.

```
Restart-Computer
```

Pour joindre des ordinateurs exécutant Windows 10 au domaine

1. Ouvrez une session sur l'ordinateur avec le compte Administrateur local.
2. Dans **Rechercher sur le web et dans Windows**, tapez **Système**. Dans les résultats de la recherche, cliquez sur **Système (Panneau de configuration)**. La boîte de dialogue **Système** s'ouvre.
3. Dans **Système**, cliquez sur **Paramètres système avancés**. La boîte de dialogue **Propriétés système** s'ouvre. Cliquez sur l'onglet **Nom de l'ordinateur** .
4. Dans **Nom de l'ordinateur**, cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.
5. Dans **Modification du nom ou du domaine de l'ordinateur**, dans **Membre de**, cliquez sur **Domaine**, puis tapez le nom du domaine auquel l'ordinateur doit être joint. Par exemple, si le nom de domaine est corp.contoso.com, tapez **corp.contoso.com**.
6. Cliquez sur **OK**. La boîte de dialogue **Sécurité Windows** s'ouvre.
7. Dans **Modification du nom ou du domaine de l'ordinateur**, dans **Nom d'utilisateur**, tapez le nom d'utilisateur. Dans **Mot de passe**, tapez le mot de passe, puis cliquez sur **OK**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre et vous souhaite la bienvenue dans le domaine. Cliquez sur **OK**.
8. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** affiche un message indiquant que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **OK**.
9. Dans la boîte de dialogue **Propriétés système**, sous l'onglet Nom de **l'ordinateur**, cliquez sur Fermer. La boîte de dialogue **Microsoft Windows** s'ouvre et affiche un message, indiquant à nouveau que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **Redémarrer maintenant**.

Pour joindre des ordinateurs exécutant Windows 8.1 au domaine

1. Ouvrez une session sur l'ordinateur avec le compte Administrateur local.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Système**. La boîte de dialogue **Système** s'ouvre.

3. Dans **Système**, cliquez sur **Paramètres système avancés**. La boîte de dialogue **Propriétés système** s'ouvre. Cliquez sur l'onglet **Nom de l'ordinateur** .

4. Dans **Nom de l'ordinateur**, cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.

5. Dans **Modification du nom ou du domaine de l'ordinateur**, dans **Membre de**, cliquez sur **Domaine**, puis tapez le nom du domaine auquel l'ordinateur doit être joint. Par exemple, si le nom de domaine est corp.contoso.com, tapez **corp.contoso.com**.

6. Cliquez sur **OK**. La boîte de dialogue **Sécurité Windows** s'ouvre.

7. Dans **Modification du nom ou du domaine de l'ordinateur**, dans **Nom d'utilisateur**, tapez le nom d'utilisateur. Dans **Mot de passe**, tapez le mot de passe, puis cliquez sur **OK**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre et vous souhaite la bienvenue dans le domaine. Cliquez sur **OK**.

8. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** affiche un message indiquant que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **OK**.

9. Dans la boîte de dialogue **Propriétés système**, sous l'onglet Nom de **l'ordinateur**, cliquez sur Fermer. La boîte de dialogue **Microsoft Windows** s'ouvre et affiche un message, indiquant à nouveau que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **Redémarrer maintenant**.

Pour se connecter au domaine à l'aide d'ordinateurs exécutant Windows 10

1. Fermez la session sur l'ordinateur et redémarrez-le.

2. Appuyez sur Ctrl+Alt+Suppr. L'écran d'ouverture de session s'affiche.

3. En bas à gauche, cliquez sur **Autre utilisateur**.

4. Dans **Nom d'utilisateur**, tapez votre domaine et votre nom d'utilisateur au format *domaine\utilisateur*. Par exemple, pour vous connecter au domaine corp.contoso.com avec un compte nommé **User-01**, tapez **CORP\User-01**.

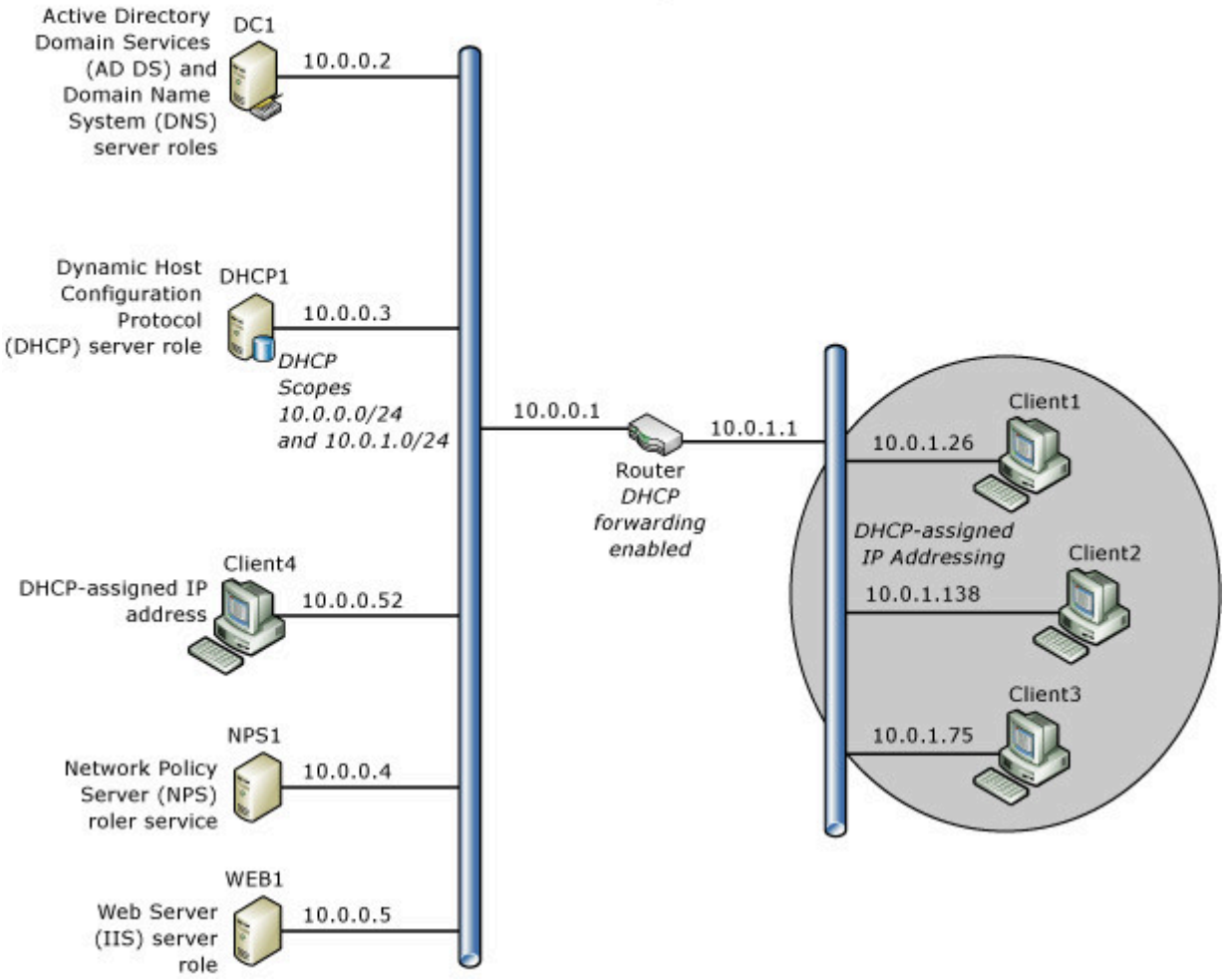
5. Dans **Mot de passe**, tapez votre mot de passe de domaine, puis cliquez sur la flèche, ou appuyez sur Entrée.

Déploiement des fonctionnalités facultatives pour l'authentification d'accès réseau et les services Web

Si vous comptez déployer des serveurs d'accès réseau, par exemple des points d'accès sans fil ou des serveurs VPN, après l'installation de votre réseau de base, il est recommandé de déployer un serveur NPS et un serveur web. Pour les déploiements de l'accès réseau, nous vous recommandons d'utiliser des méthodes d'authentification sécurisée basée sur les certificats. Vous pouvez utiliser le serveur NPS pour gérer les stratégies d'accès réseau et déployer des méthodes d'authentification sécurisée. Utilisez un serveur Web pour publier la liste de révocation de certificats émise par l'autorité de certification qui fournit les certificats d'authentification sécurisée.

> ⓘ **Notes**
>
> Vous pouvez déployer des certificats de serveur et des fonctionnalités supplémentaires à l'aide des guides d'accompagnement du réseau de base. Pour plus d'informations, voir Ressources techniques supplémentaires.

L'illustration suivante montre la topologie de réseau Windows Server Core avec l'ajout de serveurs NPS et web.



Les sections suivantes fournissent des informations sur l'ajout de serveurs NPS et Web à votre réseau.

- Déploiement de NPS1
- Déploiement de WEB1

Déploiement de NPS1

Le serveur NPS (Network Policy Server) est installé lors d'une étape préparatoire au déploiement d'autres technologies d'accès au réseau, comme les serveurs VPN (Virtual Private Network), les points d'accès sans fil et les commutateurs d'authentification 802.1X.

Le serveur NPS (Network Policy Server) vous permet de configurer et de gérer de manière centralisée les stratégies réseau avec les fonctionnalités suivantes : Serveur RADIUS (Remote Authentication Dial-In User Service) et proxy RADIUS.

Le serveur NPS est un composant facultatif d'un réseau de base, mais vous devez l'installer si l'une des conditions suivantes est vraie :

- Vous comptez développer votre réseau pour inclure des serveurs d'accès à distance compatibles avec le protocole RADIUS, par exemple un ordinateur qui exécute Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 ou Windows Server 2008 ainsi que les services Routage et accès à distance, Passerelle des services Terminal Server ou Passerelle des services Bureau à distance.
- Vous comptez déployer l'authentification 802.1X pour un accès filaire ou sans fil.

Avant de déployer ce service de rôle, vous devez effectuer les étapes suivantes sur l'ordinateur que vous configurez en tant que serveur NPS.

- Effectuer la procédure indiquée dans la section Configuration de tous les serveurs
- Effectuer la procédure indiquée dans la section Jonction des serveurs au domaine et ouverture d'une session

Pour déployer le serveur NPS1, qui exécute le service de rôle NPS (Network Policy Server) du rôle serveur Services de stratégie et d'accès réseau, vous devez effectuer les tâches suivantes :

- Planification du déploiement du serveur NPS1
- Installer un serveur NPS (Network Policy Server)
- Inscrire le serveur NPS dans le domaine par défaut

Notes

Ce guide fournit des instructions sur le déploiement du serveur NPS sur un serveur autonome ou une machine virtuelle portant le nom NPS1. L'installation du serveur NPS sur un contrôleur de domaine est un autre modèle de déploiement recommandé. Si vous préférez installer le serveur NPS sur un contrôleur de domaine plutôt que sur un serveur autonome, installez NPS sur DC1.

Planifier le déploiement du serveur NPS1

Si vous envisagez de déployer des serveurs d'accès réseau, comme des points d'accès sans fil ou des serveurs VPN, après avoir déployé le réseau de base, il est recommandé de déployer un serveur NPS.

Si vous utilisez un serveur NPS comme serveur RADIUS (Remote Authentication Dial-in User Service), le serveur NPS effectue l'authentification et l'autorisation pour les demandes de connexion par le biais de vos serveurs d'accès réseau. Le serveur NPS vous permet également de configurer et gérer de manière centralisée les stratégies réseau qui déterminent qui est autorisé à accéder au réseau, comment et quand.

Cette section décrit les principales étapes de planification qui doivent être suivies avant d'installer le serveur NPS.

- Planifiez la base de données des comptes d'utilisateurs. Par défaut, si vous joignez le serveur exécutant le serveur NPS à un domaine Active Directory, NPS effectue l'authentification et l'autorisation à l'aide de la base de données des comptes d'utilisateurs des services de domaine Active Directory. Dans certains cas, par exemple avec les réseaux de grand taille qui utilisent un serveur NPS en tant que proxy RADIUS pour acheminer les demandes de connexion vers d'autres serveurs RADIUS, vous voudrez peut-être installer le serveur NPS sur un ordinateur qui n'est pas membre du domaine.
- Planifiez la gestion de comptes RADIUS. Un serveur NPS vous permet d'enregistrer les données de gestion de comptes dans une base de données SQL Server ou dans un fichier texte sur l'ordinateur local. Si vous souhaitez utiliser la journalisation SQL Server, planifiez l'installation et la configuration de votre serveur exécutant SQL Server.

Installer un serveur NPS (Network Policy Server)

Vous pouvez utiliser cette procédure pour installer le serveur NPS (Network Policy Server) à l'aide de l'Assistant Ajout de rôles et de fonctionnalités. NPS est un service de rôle du rôle serveur Services de stratégie et d'accès réseau.

Notes

Par défaut, le serveur NPS écoute le trafic RADIUS sur les ports 1812, 1813, 1645 et 1646 sur toutes les cartes réseau installées. Si Windows Pare-feu avec fonctionnalités de sécurité avancées est activé lorsque vous installez le serveur NPS (Network Policy Server), des exceptions de pare-feu pour ces ports sont automatiquement créées au cours du processus d'installation pour le trafic IPv6 et IPv4. Si vos serveurs d'accès réseau sont configurés pour envoyer le trafic RADIUS sur d'autres ports que ces ports par défaut, supprimez les exceptions qui ont créées dans le pare-feu Windows avec fonctions de sécurité avancées pendant l'installation du serveur NPS, et créez des exceptions pour les ports que vous utilisez pour le trafic RADIUS.

Informations d'identification administratives

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs de domaine** .

ⓘ **Notes**

Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez l'applet de commande suivante, puis appuyez sur ENTRÉE.

```
Install-WindowsFeature NPAS -IncludeManagementTools
```

Pour installer le serveur NPS

1. Sur NPS1, dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.

2. Dans **Avant de commencer**, cliquez sur **Suivant**.

   ⓘ **Notes**

   La page **Avant de commencer** de l'Assistant Ajout de rôles et de fonctionnalités ne s'affiche pas si vous avez préalablement sélectionné **Ignorer cette page par défaut** dans l'Assistant.

3. Dans **Sélectionner le type d'installation**, vérifiez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.

4. Dans **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné. Dans le **pool de serveurs**, vérifiez que l'ordinateur local est sélectionné. Cliquez sur **Suivant**.

5. Dans **Sélectionner des rôles de serveurs**, dans **Rôles**, sélectionnez **Services de stratégie et d'accès réseau**. Une boîte de dialogue s'ouvre pour demander s'il faut ajouter les fonctionnalités requises pour les services de stratégie et d'accès réseau. Cliquez sur **Ajouter les fonctionnalités**, puis sur **Suivant**.

6. Dans **Sélectionner des fonctionnalités**, cliquez sur **Suivant**, puis, dans **Stratégie réseau et Services d'accès**, passez en revue les informations fournies, puis cliquez sur **Suivant**.

7. Dans **Sélectionner des services de rôle**, cliquez sur **Serveur NPS (Network Policy Server)**. Dans **Ajouter les fonctionnalités requises pour le serveur NPS (Network Policy Server)**, cliquez sur **Ajouter des fonctionnalités**. Cliquez sur **Suivant**.

8. Dans **Confirmer les sélections d'installation**, cliquez sur **Redémarrer automatiquement le serveur de destination, si nécessaire**. Lorsque vous êtes invité à confirmer cette sélection, cliquez sur **Oui**, puis sur **Installer**. La page de progression de l'installation indique l'état du processus d'installation. Une fois le processus terminé, le message « Installation réussie sur *ComputerName* » s'affiche, où *ComputerName* est le nom de l'ordinateur sur lequel vous avez installé le serveur de stratégie réseau. Cliquez sur **Fermer**.

Inscrire le serveur NPS dans le domaine par défaut

Vous pouvez utiliser cette procédure pour inscrire un serveur NPS (Network Policy Server) dans le domaine auquel appartient le serveur.

Les serveurs NPS (Network Policy Server) doivent être inscrits dans Active Directory pour avoir le droit de lire les propriétés de numérotation des comptes d'utilisateurs pendant le processus d'autorisation. L'inscription d'un serveur NPS permet d'ajouter le serveur au groupe **Serveurs RAS et IAS** dans Active Directory.

Informations d'identification d'administration

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs de domaine** .

> ⓘ **Notes**
>
> Pour effectuer cette procédure à l'aide des commandes d'interpréteur de commandes réseau (Netsh) dans Windows PowerShell, ouvrez PowerShell, tapez ce qui suit, puis appuyez sur ENTRÉE.
>
> ```
> netsh nps add registeredserver domain=corp.contoso.com server=NPS1.corp.contoso.com
> ```

Pour inscrire un serveur NPS dans son domaine par défaut

1. Sur le serveur NPS1, dans le Gestionnaire de serveur, cliquez sur Outils, puis sur **Serveur NPS (Network Policy Server)**. La console MMC Serveur NPS (Network Policy Server) s'ouvre.

2. Cliquez avec le bouton droit sur **NPS (local),** puis cliquez sur **Inscrire le serveur dans Active Directory**. La boîte de dialogue **Serveur NPS (Network Policy Server)** s'ouvre.

3. Dans **Serveur NPS (Network Policy Server)**, cliquez sur **OK**, puis à nouveau sur **OK**.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Déploiement de WEB1

Le rôle Serveur web (IIS) dans Windows Server 2016 fournit une plateforme sécurisée, facile à gérer, modulaire et extensible pour l'hébergement fiable des sites web, des services et des applications. À l'aide d'IIS (Internet Information Services), vous pouvez partager des informations avec d'autres utilisateurs sur Internet, un intranet ou un extranet. IIS est une plateforme web unifiée qui intègre IIS, ASP.NET, les services FTP, PHP et WCF (Windows Communication Foundation).

En plus de vous permettre de publier une liste de révocation de certificats pour l'accès des ordinateurs membres du domaine, le rôle serveur Serveur web (IIS) vous permet de configurer et de gérer plusieurs sites web, applications web et sites FTP. IIS offre également les avantages suivants :

- Maximiser la sécurité Web grâce à un encombrement serveur réduit et l'isolation d'applications automatique.

- Déployer et exécuter facilement des applications Web ASP.NET, Classic ASP et PHP sur le même serveur.

- Mettre en place l'isolation d'applications en donnant aux processus de travail une identité unique et une configuration en mode bac à sable (sandbox) par défaut, réduisant ainsi les risques de sécurité.

- Ajouter, supprimer et même remplacer facilement les composants IIS intégrés par des modules personnalisés, adaptés aux besoins des clients.

- Accroître les performances de votre site Web grâce à la mise en cache dynamique intégrée et à une compression améliorée.

Pour déployer le serveur WEB1, qui exécute le rôle serveur Serveur Web (IIS), vous devez effectuer les tâches suivantes :

- Effectuer la procédure indiquée dans la section Configuration de tous les serveurs
- Effectuer la procédure indiquée dans la section Jonction des serveurs au domaine et ouverture d'une session
- Installer le rôle du serveur web (IIS)

Installer le rôle du serveur web (IIS)

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs** .

> ⓘ **Notes**
>
> Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et tapez l'applet de commande suivante, puis appuyez sur ENTRÉE.
>
> `Install-WindowsFeature Web-Server -IncludeManagementTools`

1. Dans **le Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.
2. Dans **Avant de commencer**, cliquez sur **Suivant**.

   > ⓘ **Notes**
   >
   > La page **Avant de commencer** de l'Assistant Ajout de rôles et de fonctionnalités ne s'affiche pas si vous avez préalablement sélectionné **Ignorer cette page par défaut** dans l'Assistant.

3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, vérifiez que l'ordinateur local est sélectionné, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner les rôles serveur**, faites défiler l'affichage, puis sélectionnez **Serveur web (IIS)**. La boîte de dialogue **Ajouter des fonctionnalités nécessaires au serveur web (IIS)** s'ouvre. Cliquez sur **Ajouter les fonctionnalités**, puis sur **Suivant**.
6. Cliquez sur **Suivant** jusqu'à ce que vous ayez accepté tous les paramètres de serveur web par défaut, puis cliquez sur **Installer**.

7. Vérifiez que toutes les installations ont réussi, puis cliquez sur **Fermer**.

Ressources techniques supplémentaires

Pour plus d'informations sur les technologies présentées dans ce guide, consultez les ressources suivantes :

Ressources de bibliothèque technique Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012

- Nouveautés d'Active Directory Domain Services (AD DS) dans Windows Server 2016
- Vue d'ensemble d'Active Directory Domain Services (AD DS) sur https://technet.microsoft.com/library/hh831484.aspx .
- Vue d'ensemble de DNS (Domain Name System) sur https://technet.microsoft.com/library/hh831667.aspx .
- Implémentation du rôle Administrateurs DNS
- Vue d'ensemble du protocole DHCP (Dynamic Host Configuration Protocol) sur https://technet.microsoft.com/library/hh831825.aspx .
- Vue d'ensemble des services de stratégie et d'accès réseau sur https://technet.microsoft.com/library/hh831683.aspx .
- Vue d'ensemble du serveur web (IIS) sur https://technet.microsoft.com/library/hh831725.aspx .

Annexes A à E

Les sections suivantes contiennent des informations de configuration supplémentaires pour les ordinateurs qui exécutent d'autres systèmes d'exploitation que Windows Server 2016, Windows 10, Windows Server 2012 et Windows 8. De plus, une feuille de calcul de préparation du réseau est fournie pour vous aider dans votre déploiement.

1. Annexe A - Changement de nom des ordinateurs
2. Annexe B - Configuration d'adresses IP statiques
3. Annexe C - Jonction d'ordinateurs au domaine
4. Annexe D - Connexion au domaine
5. Annexe E - Feuille de préparation de la planification d'un réseau de base

Annexe A - Changement de nom des ordinateurs

Vous pouvez utiliser les procédures de cette section pour fournir aux ordinateurs exécutant Windows Server 2008 R2, Windows 7, Windows Server 2008 et Windows Vista un autre nom d'ordinateur.

- Windows Server 2008 R2 et Windows 7
- Windows Server 2008 et Windows Vista

Windows Server 2008 R2 et Windows 7

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer ces procédures.

Pour renommer des ordinateurs exécutant Windows Server 2008 R2 et Windows 7

1. Cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Ordinateur**, puis cliquez sur **Propriétés**. La boîte de dialogue **Système** s'ouvre.
2. Dans **Paramètres de nom d'ordinateur, de domaine et de groupe de travail**, cliquez sur **Modifier les paramètres**. La boîte de dialogue **Propriétés système** s'ouvre.

   > ⓘ Notes
   >
   > Sur les ordinateurs exécutant Windows 7, avant l'ouverture de la boîte de dialogue **Propriétés système** , la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre, demandant l'autorisation de continuer. Cliquez sur **Continuer** pour continuer.

3. Cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.
4. Dans **Nom de l'ordinateur**, tapez le nom de votre ordinateur. Par exemple, si vous souhaitez nommer l'ordinateur DC1, tapez **DC1**.
5. Cliquez deux fois sur **OK** , cliquez sur **Fermer**, puis sur **Redémarrer maintenant** pour redémarrer l'ordinateur.

Windows Server 2008 et Windows Vista

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer ces procédures.

Pour renommer des ordinateurs exécutant Windows Server 2008 et Windows Vista

1. Cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Ordinateur**, puis cliquez sur **Propriétés**. La boîte de dialogue **Système** s'ouvre.

2. Dans **Paramètres de nom d'ordinateur, de domaine et de groupe de travail**, cliquez sur **Modifier les paramètres**. La boîte de dialogue **Propriétés système** s'ouvre.

   > ⓘ **Notes**
   >
   > Sur les ordinateurs exécutant Windows Vista, avant l'ouverture de la boîte de dialogue **Propriétés système** , la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre, demandant l'autorisation de continuer. Cliquez sur **Continuer** pour continuer.

3. Cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.

4. Dans **Nom de l'ordinateur**, tapez le nom de votre ordinateur. Par exemple, si vous souhaitez nommer l'ordinateur DC1, tapez **DC1**.

5. Cliquez deux fois sur **OK** , cliquez sur **Fermer**, puis sur **Redémarrer maintenant** pour redémarrer l'ordinateur.

Annexe B - Configuration d'adresses IP statiques

Cette rubrique présente les procédures à suivre pour configurer des adresses IP statiques sur des ordinateurs exécutant les systèmes d'exploitation suivants :

- Windows Server 2008 R2
- Windows Server 2008

Windows Server 2008 R2

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour configurer une adresse IP statique sur un ordinateur exécutant Windows Server 2008 R2

1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.

2. Dans **le Panneau de configuration**, cliquez sur **Réseau et Internet**. La boîte de dialogue **Réseau et Internet** s'ouvre.

   Dans **Réseau et Internet**, cliquez sur **Centre Réseau et partage**. La boîte de dialogue **Centre Réseau et partage** s'ouvre.

3. Dans **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de la carte**. **Les connexions réseau** s'ouvrent.

4. Dans **Connexions réseau**, cliquez avec le bouton droit sur la connexion réseau que vous souhaitez configurer, puis cliquez sur **Propriétés**.

5. Dans **Propriétés de la connexion au réseau local**, dans **Cette connexion utilise les éléments suivants**, sélectionnez **Protocole Internet version 4 (TCP/IPv4)**, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés de Protocole Internet version 4 (TCP/IPv4)** s'ouvre.

6. Dans **Propriétés de Protocole Internet version 4 (TCP/IPv4)**, sous l'onglet **Général**, cliquez sur **Utiliser l'adresse IP suivante**. Dans **l'adresse IP**, tapez l'adresse IP que vous souhaitez utiliser.

7. Appuyez sur Tab pour placer le curseur dans le **masque de sous-réseau**. Une valeur par défaut pour le masque de sous-réseau est entrée automatiquement. Acceptez le masque de sous-réseau par défaut, ou tapez le masque de sous-réseau que vous voulez utiliser.

8. Dans **la passerelle par défaut**, tapez l'adresse IP de votre passerelle par défaut.

9. Dans **Serveur DNS préféré**, tapez l'adresse IP de votre serveur DNS. Si vous envisagez d'utiliser l'ordinateur local comme serveur DNS préféré, tapez son adresse IP.

10. Dans **Serveur DNS auxiliaire**, tapez l'adresse IP de votre serveur DNS auxiliaire, le cas échéant. Si vous envisagez d'utiliser l'ordinateur local comme serveur DNS auxiliaire, tapez son adresse IP.

11. Cliquez sur **OK**, puis sur **Fermer**.

Windows Server 2008

L’appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer ces procédures.

Pour configurer une adresse IP statique sur un ordinateur exécutant Windows Server 2008

1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
2. Dans **le Panneau de configuration**, vérifiez que **l’affichage classique** est sélectionné, puis double-cliquez sur **Réseau et Centre de partage**.
3. Dans le **Centre Réseau et partage**, dans **Tâches**, cliquez sur **Gérer les connexions réseau**.
4. Dans **Connexions réseau**, cliquez avec le bouton droit sur la connexion réseau que vous souhaitez configurer, puis cliquez sur **Propriétés**.
5. Dans **Propriétés de la connexion au réseau local**, dans **Cette connexion utilise les éléments suivants**, sélectionnez **Protocole Internet version 4 (TCP/IPv4)**, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés de Protocole Internet version 4 (TCP/IPv4)** s’ouvre.
6. Dans **Propriétés de Protocole Internet version 4 (TCP/IPv4)**, sous l’onglet **Général**, cliquez sur **Utiliser l’adresse IP suivante**. Dans **l’adresse IP**, tapez l’adresse IP que vous souhaitez utiliser.
7. Appuyez sur Tab pour placer le curseur dans le **masque de sous-réseau**. Une valeur par défaut pour le masque de sous-réseau est entrée automatiquement. Acceptez le masque de sous-réseau par défaut, ou tapez le masque de sous-réseau que vous voulez utiliser.
8. Dans **la passerelle par défaut**, tapez l’adresse IP de votre passerelle par défaut.
9. Dans **Serveur DNS préféré**, tapez l’adresse IP de votre serveur DNS. Si vous envisagez d’utiliser l’ordinateur local comme serveur DNS préféré, tapez son adresse IP.
10. Dans **Serveur DNS auxiliaire**, tapez l’adresse IP de votre serveur DNS auxiliaire, le cas échéant. Si vous envisagez d’utiliser l’ordinateur local comme serveur DNS auxiliaire, tapez son adresse IP.
11. Cliquez sur **OK**, puis sur **Fermer**.

Annexe C - Jonction d’ordinateurs au domaine

Vous pouvez utiliser ces procédures pour joindre des ordinateurs exécutant Windows Server 2008 R2, Windows 7, Windows Server 2008 et Windows Vista au domaine.

- Windows Server 2008 R2 et Windows 7
- Windows Server 2008 et Windows Vista

> **Important**
>
> Pour joindre un ordinateur à un domaine, vous devez avoir ouvert une session sur l'ordinateur avec le compte Administrateur local ou, si vous avez ouvert une session avec un compte d'utilisateur qui ne possède pas les informations d'identification d'administration de l'ordinateur local, vous devez fournir les informations d'identification du compte Administrateur local au cours du processus visant à joindre l'ordinateur au domaine. Par ailleurs, vous devez posséder un compte d'utilisateur dans le domaine auquel vous voulez joindre l'ordinateur. Au cours du processus visant à joindre l'ordinateur au domaine, vous serez invité à fournir vos informations d'identification de compte de domaine (nom d'utilisateur et mot de passe).

Windows Server 2008 R2 et Windows 7

L'appartenance aux **utilisateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour joindre des ordinateurs exécutant Windows Server 2008 R2 et Windows 7 au domaine

1. Ouvrez une session sur l'ordinateur avec le compte Administrateur local.
2. Cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Ordinateur**, puis cliquez sur **Propriétés**. La boîte de dialogue **Système** s'ouvre.
3. Dans **Paramètres de nom d'ordinateur, de domaine et de groupe de travail**, cliquez sur **Modifier les paramètres**. La boîte de dialogue **Propriétés système** s'ouvre.

   > **Notes**
   >
   > Sur les ordinateurs exécutant Windows 7, avant l'ouverture de la boîte de dialogue **Propriétés système** , la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre, demandant l'autorisation de continuer. Cliquez sur **Continuer** pour continuer.

4. Cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.

5. Dans **Nom de l'ordinateur**, dans **Membre de**, sélectionnez **Domaine**, puis tapez le nom du domaine que vous souhaitez joindre. Par exemple, si le nom de domaine est corp.contoso.com, tapez **corp.contoso.com**.

6. Cliquez sur **OK**. La boîte de dialogue **Sécurité Windows** s'ouvre.

7. Dans **Modification du nom ou du domaine de l'ordinateur**, dans **Nom d'utilisateur**, tapez le nom d'utilisateur. Dans **Mot de passe**, tapez le mot de passe, puis cliquez sur **OK**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre et vous souhaite la bienvenue dans le domaine. Cliquez sur **OK**.

8. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** affiche un message indiquant que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **OK**.

9. Dans la boîte de dialogue **Propriétés système**, sous l'onglet Nom de **l'ordinateur**, cliquez sur Fermer. La boîte de dialogue **Microsoft Windows** s'ouvre et affiche un message, indiquant à nouveau que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **Redémarrer maintenant**.

Windows Server 2008 et Windows Vista

L'appartenance aux **utilisateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour joindre des ordinateurs exécutant Windows Server 2008 et Windows Vista au domaine

1. Ouvrez une session sur l'ordinateur avec le compte Administrateur local.

2. Cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Ordinateur**, puis cliquez sur **Propriétés**. La boîte de dialogue **Système** s'ouvre.

3. Dans **Paramètres de nom d'ordinateur, de domaine et de groupe de travail**, cliquez sur **Modifier les paramètres**. La boîte de dialogue **Propriétés système** s'ouvre.

4. Cliquez sur **Modifier**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre.

5. Dans **Nom de l'ordinateur**, dans **Membre de**, sélectionnez **Domaine**, puis tapez le nom du domaine que vous souhaitez joindre. Par exemple, si le nom de domaine est

corp.contoso.com, tapez **corp.contoso.com**.

6. Cliquez sur **OK**. La boîte de dialogue **Sécurité Windows** s'ouvre.

7. Dans **Modification du nom ou du domaine de l'ordinateur**, dans **Nom d'utilisateur**, tapez le nom d'utilisateur. Dans **Mot de passe**, tapez le mot de passe, puis cliquez sur **OK**. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** s'ouvre et vous souhaite la bienvenue dans le domaine. Cliquez sur **OK**.

8. La boîte de dialogue **Modification du nom ou du domaine de l'ordinateur** affiche un message indiquant que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **OK**.

9. Dans la boîte de dialogue **Propriétés système**, sous l'onglet Nom de **l'ordinateur**, cliquez sur Fermer. La boîte de dialogue **Microsoft Windows** s'ouvre et affiche un message, indiquant à nouveau que vous devez redémarrer l'ordinateur pour appliquer les modifications. Cliquez sur **Redémarrer maintenant**.

Annexe D - Connexion au domaine

Vous pouvez utiliser ces procédures pour vous connecter au domaine à l'aide d'ordinateurs exécutant Windows Server 2008 R2, Windows 7, Windows Server 2008 et Windows Vista.

- Windows Server 2008 R2 et Windows 7
- Windows Server 2008 et Windows Vista

Windows Server 2008 R2 et Windows 7

L'appartenance aux **utilisateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour ouvrir une session sur le domaine à l'aide d'ordinateurs exécutant Windows Server 2008 R2 et Windows 7

1. Fermez la session sur l'ordinateur et redémarrez-le.

2. Appuyez sur Ctrl+Alt+Suppr. L'écran d'ouverture de session s'affiche.

3. Cliquez sur **Changer d'utilisateur**, puis sur **Autre utilisateur**.

4. Dans **Nom d'utilisateur**, tapez votre domaine et votre nom d'utilisateur au format *domaine\utilisateur*. Par exemple, pour vous connecter au domaine corp.contoso.com avec un compte nommé **User-01**, tapez **CORP\User-01**.

5. Dans **Mot de passe**, tapez votre mot de passe de domaine, puis cliquez sur la flèche, ou appuyez sur Entrée.

Windows Server 2008 et Windows Vista

L'appartenance aux **utilisateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour ouvrir une session sur le domaine à l'aide d'ordinateurs exécutant Windows Server 2008 et Windows Vista

1. Fermez la session sur l'ordinateur et redémarrez-le.
2. Appuyez sur Ctrl+Alt+Suppr. L'écran d'ouverture de session s'affiche.
3. Cliquez sur **Changer d'utilisateur**, puis sur **Autre utilisateur**.
4. Dans **Nom d'utilisateur**, tapez votre domaine et votre nom d'utilisateur au format *domaine\utilisateur*. Par exemple, pour vous connecter au domaine corp.contoso.com avec un compte nommé **User-01**, tapez **CORP\User-01**.
5. Dans **Mot de passe**, tapez votre mot de passe de domaine, puis cliquez sur la flèche, ou appuyez sur Entrée.

Annexe E - Feuille de préparation de la planification d'un réseau de base

Vous pouvez utiliser la feuille de préparation de la planification de réseau proposée dans cette annexe pour collecter les informations nécessaires à l'installation d'un réseau de base. Cette annexe comporte des tableaux répertoriant les éléments de configuration propres à chaque ordinateur serveur pour lesquels vous devez fournir des informations ou des valeurs spécifiques au cours du processus d'installation ou de configuration. Des exemples de valeurs sont fournis pour chaque élément de configuration.

Des espaces sont prévus dans chaque tableau pour que vous puissiez entrer les valeurs utilisées pour votre déploiement. Si vous enregistrez des valeurs relatives à la sécurité dans ces tableaux, assurez-vous de stocker ces informations en lieu sûr.

Les liens suivants permettent d'accéder aux différentes sections de cette annexe qui présentent les éléments de configuration et les exemples de valeurs qui sont associés aux procédures de déploiement décrites dans ce guide.

1. Installation des services de domaine Active Directory et DNS
    - Configuration d'une zone de recherche inversée DNS
2. Installation du protocole DHCP
    - Création d'une plage d'exclusion dans DHCP
    - Création d'une étendue DHCP
3. Installation d'un serveur NPS (Network Policy Server) (facultatif)

Installation des services de domaine Active Directory et DNS

Les tableaux de cette section répertorient les éléments de configuration pour la préinstallation et l'installation des services de domaine Active Directory (AD DS) et DNS.

Éléments de configuration pour la préinstallation des services de domaine Active Directory et DNS

Les tableaux suivants répertorient les éléments de configuration pour la préinstallation comme décrit dans la procédure Configuration de tous les serveurs :

- Configurer une adresse IP statique

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
IP address	10.0.0.2	
Masque de sous-réseau	255.255.255.0	
Passerelle par défaut	10.0.0.1	
Serveur DNS préféré	127.0.0.1	
Serveur DNS auxiliaire	10.0.0.15	

- Renommer l'ordinateur

Agrandir le tableau

Élément de configuration	Valeur d'exemple	Value
Nom de l'ordinateur	DC1	

Éléments de configuration pour l'installation des services de domaine Active Directory et DNS

Éléments de configuration pour le déploiement d'un réseau de base Windows Server comme décrit dans la procédure Installer les services de domaine Active Directory et DNS dans une nouvelle forêt :

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
Nom DNS complet	corp.contoso.com	
Niveau fonctionnel d'une forêt	Windows Server 2003	
Emplacement du dossier de la base de données des services de domaine Active Directory	E:\Configuration\ Ou acceptez la valeur par défaut.	
Emplacement du dossier des fichiers journaux des services de domaine Active Directory	E:\Configuration\ Ou acceptez la valeur par défaut.	
Emplacement du dossier SYSVOL des services de domaine Active Directory	E:\Configuration\ Ou acceptez la valeur par défaut.	
Mot de passe administrateur de restauration des services d'annuaire	J*p2leO4$F	
Nom du fichier de réponses (facultatif)	AD DS_AnswerFile	

Configuration d'une zone de recherche inversée DNS

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
Type de zone :	- Zone principale - Zone secondaire - Zone de stub	
Type de zone **Enregistrer la zone dans Active Directory**	-Sélectionné - Non sélectionné	
Étendue de réplication de la zone Active Directory	- Vers tous les serveurs DNS de cette forêt - Vers tous les serveurs DNS de ce domaine	

Éléments de configuration	Exemples de valeurs	Values
	- Vers tous les contrôleurs de ce domaine - Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire	
Nom de la zone de recherche inversée (Type IP)	- Zone de recherche inversée IPv4 - Zone de recherche inversée IPv6	
Nom de la zone de recherche inversée (ID réseau)	10.0.0	

Installation du protocole DHCP

Les tableaux de cette section répertorient les éléments de configuration pour la préinstallation et l'installation de DHCP.

Éléments de configuration pour la préinstallation de DHCP

Les tableaux suivants répertorient les éléments de configuration pour la préinstallation comme décrit dans la procédure Configuration de tous les serveurs :

- Configurer une adresse IP statique

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
IP address	10.0.0.3	
Masque de sous-réseau	255.255.255.0	
Passerelle par défaut	10.0.0.1	
Serveur DNS préféré	10.0.0.2	
Serveur DNS auxiliaire	10.0.0.15	

- Renommer l'ordinateur

Agrandir le tableau

Élément de configuration	Valeur d'exemple	Value
Nom de l'ordinateur	DHCP1	

Éléments de configuration pour l'installation de DHCP

Éléments de configuration pour le déploiement d'un réseau de base Windows Server comme décrit dans la procédure Installer DHCP (Dynamic Host Configuration Protocol) :

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
Liaisons de connexion réseau	Ethernet	
Paramètres du serveur DNS	DC1	
Adresse IP du serveur DNS préféré	10.0.0.2	
Adresse IP du serveur DNS auxiliaire	10.0.0.15	
Nom de l'étendue	Corp1	
Adresse IP de début	10.0.0.1	
Adresse IP de fin	10.0.0.254	
Masque de sous-réseau	255.255.255.0	
Passerelle par défaut (facultatif)	10.0.0.1	
Durée du bail	8 jours	
Mode d'opération du serveur DHCP IPv6	Non activé	

Création d'une plage d'exclusion dans DHCP

Éléments de configuration pour créer une plage d'exclusion lors de la création d'une étendue dans DHCP.

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
Nom de l'étendue	Corp1	
Description de l'étendue	Sous-réseau 1 du siège social	
Adresse IP de début de la plage d'exclusion	10.0.0.1	
Adresse IP de fin de la plage d'exclusion	10.0.0.15	

Création d'une étendue DHCP

Éléments de configuration pour le déploiement d'un réseau de base Windows Server comme décrit dans la procédure Créer et activer une nouvelle étendue DHCP :

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
Nom de la nouvelle étendue	Corp2	
Description de l'étendue	Sous-réseau 2 du siège de l'entreprise	
(Plage d'adresses IP) Adresse IP de début	10.0.1.1	
(Plage d'adresses IP) Adresse IP de fin	10.0.1.254	
Length	8	
Masque de sous-réseau	255.255.255.0	
Adresse IP de début de la plage d'exclusion	10.0.1.1	
Adresse IP de fin de la plage d'exclusion	10.0.1.15	
Durée du bail Days Hours Minutes	- 8 - 0 - 0	
Routeur (passerelle par défaut) IP address	10.0.1.1	
Domaine parent DNS	corp.contoso.com	
DNS server IP address	10.0.0.2	

Installation d'un serveur NPS (Network Policy Server) (facultatif)

Les tableaux de cette section répertorient les éléments de configuration pour la préinstallation et l'installation d'un serveur NPS.

Éléments de configuration pour la préinstallation

Les trois tableaux suivants répertorient les éléments de configuration pour la préinstallation comme décrit dans la procédure Configuration de tous les serveurs :

- Configurer une adresse IP statique

Agrandir le tableau

Éléments de configuration	Exemples de valeurs	Values
IP address	10.0.0.4	
Masque de sous-réseau	255.255.255.0	
Passerelle par défaut	10.0.0.1	
Serveur DNS préféré	10.0.0.2	
Serveur DNS auxiliaire	10.0.0.15	

- Renommer l'ordinateur

Agrandir le tableau

Élément de configuration	Valeur d'exemple	Value
Nom de l'ordinateur	NPS1	

Éléments de configuration pour l'installation d'un serveur NPS

Éléments de configuration pour les procédures de déploiement d'un serveur NPS sur un réseau Windows Server Core Installer un serveur NPS (Network Policy Server) et Inscrire le serveur NPS dans le domaine par défaut.

- Aucun élément de configuration supplémentaire n'est requis pour installer et inscrire un serveur NPS.

Guide complémentaire du réseau principal

Article • 05/10/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Le Guide du réseau de base de Windows Server 2016 fournit des instructions sur la façon de déployer un nouveau domaine racine dans une nouvelle forêt Active Directory®, avec l’infrastructure de mise en réseau requise. De leur côté, les différents guides d’accompagnement vous aident à ajouter des fonctionnalités à votre réseau.

Chaque guide d’accompagnement est consacré à la mise en œuvre d’un objectif particulier après le déploiement de votre réseau de base. Dans certains cas, il existe plusieurs guides d’accompagnement qui, lorsqu’ils sont déployés ensemble et dans l’ordre approprié, vous permettent de mener à bien des objectifs très complexes selon des méthodes mesurables, rentables et fiables.

Si vous avez déployé votre domaine Active Directory et votre réseau de base sans vous aider du Guide du réseau de base, vous pouvez quand même utiliser les guides d’accompagnement pour ajouter des fonctionnalités à votre réseau. Dans ce cas, servez-vous du Guide du réseau de base pour dresser la liste des conditions préalables que votre réseau doit remplir si vous prévoyez de déployer des fonctionnalités supplémentaires avec les guides d’accompagnement.

Guide d’accompagnement du réseau de base : Déployer des certificats de serveur pour des déploiements câblés et sans fil 802.1X

Ce guide d’accompagnement explique comment déployer, sur le serveur de base, des certificats de serveur pour les ordinateurs qui exécutent NPS (Network Policy Server) ou RAS (Remote Access Service), ou les deux à la fois.

Des certificats de serveur sont requis lorsque vous déployez des méthodes d’authentification basées sur des certificats avec le protocole EAP (Extensible Authentication Protocol) et le protocole PEAP (Protected EAP) pour l’authentification d’accès au réseau. Le déploiement de certificats de serveur avec les services de certificats Active Directory (AD CS) pour les méthodes d’authentification basées sur des certificats EAP et PEAP offre les avantages suivants :

- Liaison de l'identité du serveur NPS ou RAS à une clé privée
- Méthode rentable et sûre pour inscrire automatiquement des certificats sur des serveurs NPS et RAS membres du domaine
- Méthode efficace pour gérer les certificats et les autorités de certification
- Sécurité fournie par l'authentification basée sur des certificats
- Possibilité d'étendre l'utilisation de certificats à d'autres usages

Pour obtenir des instructions sur le déploiement des certificats de serveur, consultez Déployer des certificats de serveur pour les déploiements filaires et sans fil 802.1X.

Guide d'accompagnement du réseau de base : Déploiement d'un accès sans fil authentifié 802.1X basé sur des mots de passe

Ce guide d'accompagnement explique comment effectuer un déploiement sur le réseau de base. Pour cela, il fournit des instructions sur la façon de déployer un accès sans fil IEEE (Institute of Electrical and Electronics Engineers) 802.11, authentifié par IEEE 802.1X à l'aide du protocole PEAP (Protected Extensible Authentication Protocol)\– Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2).

La méthode d'authentification PEAP-MS-CHAP v2 exige que l'authentification des serveurs exécutant un serveur NPS (Network Policy Server) présente aux clients sans fil un certificat de serveur pour prouver l'identité NPS au client. Toutefois, l'authentification utilisateur n'est pas effectuée à l'aide d'un certificat. À la place, les utilisateurs fournissent leur nom d'utilisateur de domaine et leur mot de passe.

Étant donné que PEAP-MS-CHAP v2 exige que les utilisateurs fournissent des informations d'identification basées sur un mot de passe plutôt qu'un certificat pendant le processus d'authentification, il est généralement plus facile et moins coûteux de déployer que EAP-TLS ou PEAP-TLS.

Avant d'utiliser ce guide pour déployer l'accès sans fil avec la méthode d'authentification PEAP-MS-CHAP v2, vous devez effectuer les opérations suivantes :

1. Suivez les instructions du Guide du réseau de base pour déployer votre infrastructure réseau principale, à moins de déjà disposer des technologies présentées dans ce guide sur votre réseau.
2. Suivez les instructions du Guide d'accompagnement du réseau de base Déployer des certificats de serveur pour les déploiements filaires et sans fil 802.1X, à moins de déjà disposer des technologies présentées dans ce guide déployées sur votre réseau.

Pour obtenir des instructions sur le déploiement de l'accès sans fil avec PEAP-MS-CHAP v2, consultez Déployer un accès sans fil authentifié 802.1X basé sur des mots de passe.

Guide d'accompagnement du réseau de base : déploiement du mode de cache hébergé de BranchCache

Ce guide d'accompagnement explique comment déployer BranchCache en mode cache hébergé dans une ou plusieurs filiales.

BranchCache est une technologie d'optimisation de la bande passante des réseaux étendus (WAN), disponible dans certaines éditions de Windows Server 2016 et Windows 10, ainsi que certaines anciennes versions de Windows et Windows Server.

Lorsque vous déployez BranchCache en mode de cache hébergé, le cache de contenu dans la filiale est hébergé sur un ou plusieurs ordinateurs serveurs, lesquels sont appelés « serveurs de cache hébergé ». Les serveurs de cache hébergé peuvent exécuter des charges de travail en plus de l'hébergement du cache, ce qui vous permet d'utiliser le serveur à plusieurs fins dans la filiale.

Le mode de cache hébergé BranchCache augmente l'efficacité du cache, car le contenu est disponible même si le client qui avait demandé et mis en cache les données à l'origine n'est pas connecté. Étant donné que le serveur de cache hébergé est toujours disponible, davantage de contenu est mis en cache, ce qui économise davantage la bande passante du réseau étendu et améliore l'efficacité de BranchCache.

Lorsque vous effectuez le déploiement en mode de cache hébergé, tous les clients d'une filiale comportant plusieurs sous-réseaux peuvent accéder à un seul et même cache, qui est stocké sur le serveur de cache hébergé, même si les clients se trouvent sur des sous-réseaux différents.

Pour obtenir des instructions sur le déploiement de BranchCache en mode cache hébergé, consultez Déployer le mode de cache hébergé BranchCache.

Déployer des certificats de serveur pour des déploiements câblés et sans fil 802.1X

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser ce guide pour déployer des certificats de serveur sur vos serveurs d'infrastructure NPS (Network Policy Server) et d'accès à distance.

Ce guide contient les sections suivantes.

- Conditions préalables à l'utilisation de ce guide
- Ce que ce guide ne fournit pas
- Vue d'ensemble des technologies
- Vue d'ensemble du déploiement de certificats de serveur
- Planification du déploiement des certificats de serveur
- Déploiement de certificats de serveur

Certificats de serveur numérique

Ce guide fournit des instructions sur l'utilisation des services de certificats Active Directory (AD CS) pour inscrire automatiquement les certificats auprès des serveurs d'infrastructure NPS et d'accès à distance. AD CS vous permet de générer une infrastructure à clé publique (PKI) et de fournir un chiffrement à clé publique, des certificats numériques et des fonctions de signature numérique pour votre organisation.

Quand vous utilisez des certificats de serveur numériques pour l'authentification entre ordinateurs de votre réseau, les certificats fournissent :

1. la confidentialité grâce au chiffrement ;
2. l'intégrité grâce aux signatures numériques ;
3. L'authentification par association de clés de certificat à des comptes d'ordinateur, d'utilisateur ou d'appareil sur un réseau informatique.

Types de serveurs

À l'aide de ce guide, vous pouvez déployer des certificats de serveur sur les types de serveur suivants.

- Serveurs qui exécutent le service d'accès à distance, qui sont des serveurs de réseau privé virtuel (VPN) DirectAccess ou standard, et qui sont membres du groupe **serveurs RAS et IAS** .
- Serveurs qui exécutent le service NPS (Network Policy Server) qui sont membres du groupe **serveurs RAS et IAS** .

Avantages de l'inscription automatique des certificats

L'inscription automatique des certificats de serveur, également appelée inscription automatique, offre les avantages suivants.

- L'autorité de certification AD CS inscrit automatiquement un certificat de serveur auprès de tous vos serveurs NPS et d'accès à distance.
- Tous les ordinateurs du domaine reçoivent automatiquement votre certificat d'autorité de certification, qui est installé dans le magasin Autorités de certification racines de confiance sur chaque ordinateur membre du domaine. Ainsi, tous les ordinateurs du domaine font confiance aux certificats émis par votre autorité de certification. Cette approbation permet à vos serveurs d'authentification de se prouver leur identité entre eux, et d'établir des communications sécurisées.
- À l'exception de l'actualisation de la stratégie de groupe, la reconfiguration manuelle de chaque serveur n'est pas nécessaire.
- Chaque certificat de serveur inclut à la fois l'objectif d'authentification serveur et l'objectif d'authentification client dans les extensions d'utilisation améliorée de la clé.
- Scalability. Une fois que vous avez déployé votre AC racine d'entreprise à l'aide de ce guide, vous pouvez étendre votre infrastructure PKI (infrastructure à clé publique) en ajoutant des autorités de certification secondaires d'entreprise.
- Manageability. Vous pouvez gérer AD CS à l'aide de la console AD CS ou de commandes et de scripts Windows PowerShell.
- Simplicity. Vous spécifiez les serveurs qui inscrivent les certificats de serveur à l'aide des comptes de groupe Active Directory et de l'appartenance aux groupes.
- Quand vous déployez des certificats de serveur, ils sont basés sur un modèle que vous configurez en suivant les instructions de ce guide. Cela signifie que vous pouvez personnaliser différents modèles de certificat pour des types de serveur spécifiques, ou que vous pouvez utiliser le même modèle pour tous les certificats de serveur à émettre.

Conditions préalables à l'utilisation de ce guide

Ce guide fournit des instructions sur le déploiement de certificats de serveur à l'aide d'AD CS et du rôle serveur Serveur web (IIS) dans Windows Server 2016. Vous trouverez ci-dessous les prérequis pour l'exécution des procédures décrites dans ce guide.

- Vous devez déployer un réseau de base à l'aide du Guide du réseau de base pour Windows Server 2016, ou vous devez avoir installé et fait fonctionner correctement les technologies décrites dans le Guide du réseau de base sur votre réseau. Ces technologies incluent TCP/IP v4, DHCP, Active Directory Domain Services (AD DS), DNS et NPS.

  > ⓘ **Notes**
  >
  > Le Guide du réseau principal Windows Server 2016 est disponible dans la bibliothèque technique Windows Server 2016. Pour plus d'informations, consultez **le Guide du réseau principal**.

- Vous devez lire la section de ce guide relative à la planification pour vérifier si vous êtes prêt à effectuer le déploiement.
- Vous devez effectuer les étapes de ce guide dans l'ordre dans lequel elles sont présentées. Ne vous précipitez pas et ne déployez pas votre autorité de certification sans avoir effectué les étapes qui mènent au déploiement du serveur, sinon votre déploiement sera un échec.
- Vous devez être prêt à déployer deux nouveaux serveurs sur votre réseau : un serveur sur lequel vous allez installer AD CS en tant qu'AC racine d'entreprise, et un autre serveur sur lequel vous allez installer le serveur web (IIS) pour que votre autorité de certification puisse publier la liste de révocation de certificats sur le serveur web.

> ⓘ **Notes**
>
> Vous êtes prêt à affecter une adresse IP statique aux serveurs web et AD CS que vous déployez avec ce guide ainsi qu'à nommer les ordinateurs en fonction des conventions de nommage de votre organisation. De plus, vous devez joindre les ordinateurs à votre domaine.

Ce que ce guide ne contient pas

Ce guide ne fournit pas d'instructions complètes sur la conception et le déploiement d'une infrastructure PKI (infrastructure à clé publique) à l'aide d'AD CS. Il est recommandé de passer en revue la documentation d'AD CS ainsi que la documentation relative à la conception d'une infrastructure PKI avant de déployer les technologies décrites dans ce guide.

Vue d’ensemble des technologies

Vous trouverez ci-dessous des vues d’ensemble des technologies pour AD CS et le serveur web (IIS).

Services de certificats Active Directory

AD CS dans Windows Server 2016 fournit des services personnalisables pour la création et la gestion des certificats X.509 utilisés dans les systèmes de sécurité logicielle qui emploient des technologies reposant sur une clé publique. Les organisations peuvent utiliser AD CS pour améliorer la sécurité en liant l’identité d’une personne, d’un appareil ou d’un service à une clé publique correspondante. AD CS comprend également des fonctionnalités qui vous permettent de gérer l’inscription et la révocation de certificats dans divers environnements scalables.

Pour plus d’informations, consultez la vue d’ensemble des services de certificats Active Directory et les conseils de conception de l’infrastructure à clé publique.

Serveur Web (IIS)

Le rôle Serveur web (IIS) dans Windows Server 2016 fournit une plateforme sécurisée, facile à gérer, modulaire et extensible pour l’hébergement fiable des sites web, des services et des applications. À l’aide d’IIS, vous pouvez partager des informations avec d’autres utilisateurs sur Internet, un intranet ou un extranet. IIS est une plateforme web unifiée qui intègre IIS, ASP.NET, les services FTP, PHP et WCF (Windows Communication Foundation).

Pour plus d’informations, consultez Vue d’ensemble du serveur web (IIS).

Présentation du déploiement de certificats de serveur

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Cette rubrique contient les sections suivantes.

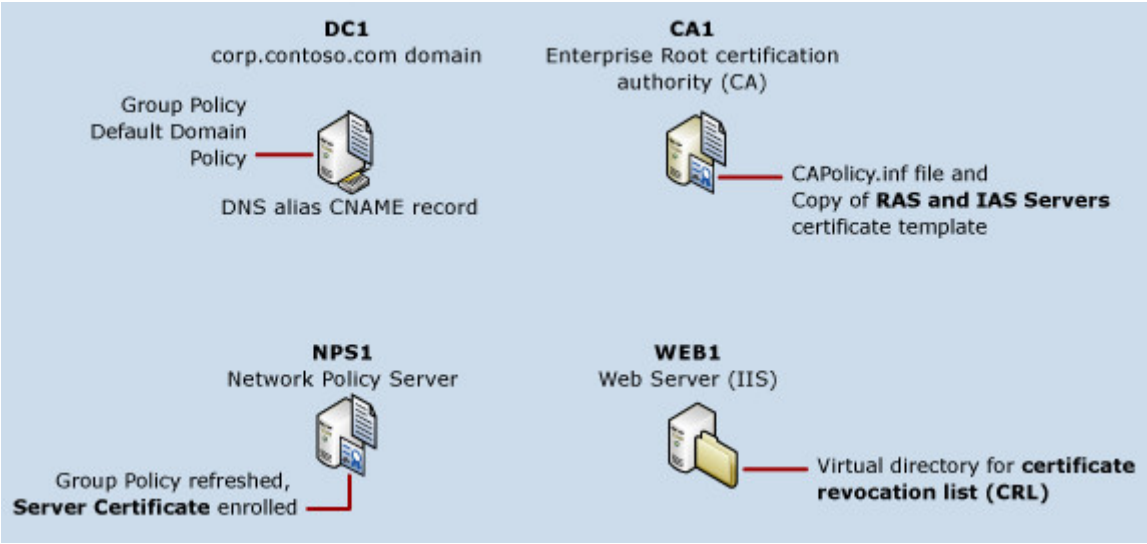
- Composants du déploiement de certificats de serveur
- Présentation du processus de déploiement de certificats de serveur

Composants du déploiement de certificats de serveur

Vous pouvez utiliser ce guide pour installer Active Directory Certificate Services (AD CS) en tant qu'autorité de certification racine d'entreprise et pour inscrire des certificats de serveur sur des serveurs qui exécutent le serveur NPS (Network Policy Server), le service de routage et d'accès à distance (RRAS), ou les deux.

Si vous déployez SDN avec l'authentification basée sur les certificats, les serveurs doivent utiliser un certificat de serveur pour prouver leurs identités à d'autres serveurs afin d'obtenir des communications sécurisées.

L'illustration suivante montre les composants requis pour déployer des certificats de serveur sur des serveurs de votre infrastructure SDN.



> **Notes**
>
> Dans l'illustration ci-dessus, plusieurs serveurs sont représentés : DC1, CA1, WEB1 et de nombreux serveurs SDN. Ce guide fournit des instructions pour le déploiement et la configuration de CA1 et WEB1, ainsi que pour la configuration de DC1, que ce guide suppose que vous avez déjà installé sur votre réseau. Si vous n'avez pas encore installé votre domaine Active Directory, vous pouvez le faire à l'aide du **Guide réseau principal** pour Windows Server 2016.

Pour plus d'informations sur chaque élément représenté dans l'illustration ci-dessus, consultez les éléments suivants :

- CA1
- WEB1
- DC1
- NPS1

CA1 exécutant le rôle serveur AD CS

Dans ce scénario, l'autorité de certification racine d'entreprise est également une autorité de certification émettrice. L'autorité de certification émet des certificats pour les ordinateurs serveurs qui disposent des autorisations de sécurité appropriées pour inscrire un certificat. Les services de certificats Active Directory (AD CS) sont installés sur CA1.

Pour les réseaux plus volumineux ou lorsque les problèmes de sécurité fournissent une justification, vous pouvez séparer les rôles de l'autorité de certification racine et de l'autorité de certification émettrice, et déployer des autorités de certification subordonnées qui émettent des autorités de certification.

Dans les déploiements les plus sécurisés, l'autorité de certification racine d'entreprise est mise hors connexion et physiquement sécurisée.

CAPolicy.inf

Avant d'installer AD CS, vous configurez le fichier CAPolicy.inf avec des paramètres spécifiques pour votre déploiement.

Copie du modèle de certificat des serveurs RAS et IAS

Lorsque vous déployez des certificats de serveur, vous effectuez une copie du modèle de certificat des **serveurs RAS et IAS**, puis vous configurez le modèle en fonction de vos besoins et des instructions de ce guide.

Vous utilisez une copie du modèle plutôt que le modèle d'origine afin que la configuration du modèle d'origine soit conservée pour une utilisation future possible. Vous configurez la copie du modèle de **serveurs RAS et IAS** afin que l'autorité de certification puisse créer des certificats de serveur qu'elle émet pour les groupes dans Utilisateurs et ordinateurs Active Directory que vous spécifiez.

Configuration CA1 supplémentaire

L'autorité de certification publie une liste de révocation de certificats (CRL) que les ordinateurs doivent vérifier pour s'assurer que les certificats qui leur sont présentés comme preuve d'identité sont des certificats valides et n'ont pas été révoqués. Vous devez configurer votre autorité de certification avec l'emplacement correct de la liste de révocation de certificats afin que les ordinateurs sachent où rechercher la liste de révocation de certificats pendant le processus d'authentification.

WEB1 exécutant le rôle serveur services web (IIS)

Sur l'ordinateur qui exécute le rôle serveur web (IIS), WEB1, vous devez créer un dossier dans Windows Explorer pour l'utiliser comme emplacement pour la liste de révocation de certificats et l'AIA.

Répertoire virtuel pour la liste de révocation de certificats et l'AIA

Après avoir créé un dossier dans Windows Explorer, vous devez configurer le dossier en tant que répertoire virtuel dans le Gestionnaire des services Internet (IIS), ainsi que configurer la liste de contrôle d'accès pour le répertoire virtuel afin de permettre aux ordinateurs d'accéder à l'AIA et à la liste de révocation de certificats après leur publication.

DC1 exécutant les rôles serveur AD DS et DNS

DC1 est le contrôleur de domaine et le serveur DNS sur votre réseau.

Stratégie de domaine par défaut de la stratégie de groupe

Après avoir configuré le modèle de certificat sur l'autorité de certification, vous pouvez configurer la stratégie de domaine par défaut dans la stratégie de groupe afin que les

certificats soient automatiquement inscrits sur les serveurs NPS et RAS. La stratégie de groupe est configurée dans AD DS sur le serveur DC1.

Enregistrement de ressource d'alias DNS (CNAME)

Vous devez créer un enregistrement de ressource d'alias (CNAME) pour le serveur Web afin de vous assurer que d'autres ordinateurs peuvent trouver le serveur, ainsi que l'AIA et la liste de révocation de certificats qui sont stockés sur le serveur. En outre, l'utilisation d'un enregistrement de ressource d'alias CNAME offre une flexibilité qui vous permet d'utiliser le serveur Web à d'autres fins, telles que l'hébergement de sites Web et FTP.

NPS1 exécutant le rôle serveur NPS (Network Policy Server) de la stratégie réseau et du rôle serveur Access Services

Le serveur NPS est installé lorsque vous effectuez les tâches décrites dans le Guide du réseau principal Windows Server 2016. Avant d'effectuer les tâches de ce guide, vous devez déjà avoir installé un ou plusieurs serveurs NPS sur votre réseau.

Stratégie de groupe appliquée et certificat inscrit aux serveurs

Une fois que vous avez configuré le modèle de certificat et l'inscription automatique, vous pouvez actualiser la stratégie de groupe sur tous les serveurs cibles. À ce stade, les serveurs inscrivent le certificat de serveur auprès de CA1.

Présentation du processus de déploiement de certificats de serveur

> ⓘ **Notes**
>
> Les détails de l'exécution de ces étapes sont fournis dans la section **Déploiement de certificats de serveur**.

Le processus de configuration de l'inscription de certificat de serveur se produit dans les étapes suivantes :

1. Sur WEB1, installez le rôle serveur web (IIS).
2. Sur DC1, créez un enregistrement d'alias (CNAME) pour votre serveur web, WEB1.

3. Configurez votre serveur web pour héberger la liste de révocation de certificats à partir de l'autorité de certification, puis publiez la liste de révocation de certificats et copiez le certificat d'autorité de certification racine d'entreprise dans le nouveau répertoire virtuel.

4. Sur l'ordinateur sur lequel vous envisagez d'installer AD CS, attribuez à l'ordinateur une adresse IP statique, renommez l'ordinateur, joignez l'ordinateur au domaine, puis connectez-vous à l'ordinateur avec un compte d'utilisateur membre des groupes Administrateurs de domaine et Administrateurs d'entreprise.

5. Sur l'ordinateur sur lequel vous envisagez d'installer AD CS, configurez le fichier CAPolicy.inf avec des paramètres spécifiques à votre déploiement.

6. Installez le rôle serveur AD CS et effectuez une configuration supplémentaire de l'autorité de certification.

7. Copiez la liste de révocation de certificats et le certificat d'autorité de certification de CA1 vers le partage sur le serveur web WEB1.

8. Sur l'autorité de certification, configurez une copie du modèle de certificats de serveurs RAS et IAS. L'autorité de certification émet des certificats basés sur un modèle de certificat. Vous devez donc configurer le modèle pour le certificat de serveur avant que l'autorité de certification puisse émettre un certificat.

9. Configurez l'inscription automatique du certificat de serveur dans la stratégie de groupe. Lorsque vous configurez l'inscription automatique, tous les serveurs que vous avez spécifiés avec les appartenances aux groupes Active Directory reçoivent automatiquement un certificat de serveur lorsque la stratégie de groupe sur chaque serveur est actualisée. Si vous ajoutez d'autres serveurs ultérieurement, ils recevront également automatiquement un certificat de serveur.

10. Actualisez la stratégie de groupe sur les serveurs. Lorsque la stratégie de groupe est actualisée, les serveurs reçoivent le certificat de serveur, qui est basé sur le modèle que vous avez configuré à l'étape précédente. Ce certificat est utilisé par le serveur pour prouver son identité aux ordinateurs clients et à d'autres serveurs pendant le processus d'authentification.

> ⓘ **Notes**
>
> Tous les ordinateurs membres du domaine reçoivent automatiquement le certificat de l'autorité de certification racine d'entreprise sans la configuration de l'inscription automatique. Ce certificat est différent du certificat de serveur que vous configurez et distribuez à l'aide de l'inscription automatique. Le

certificat de l’autorité de certification est automatiquement installé dans le magasin de certificats d’autorité de certification racines de confiance pour tous les ordinateurs membres du domaine afin qu’ils approuvent les certificats émis par cette autorité de certification.

11. Vérifiez que tous les serveurs ont inscrit un certificat de serveur valide.

Planification du déploiement de certificats de serveur

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Avant de déployer des certificats de serveur, vous devez planifier les éléments suivants :

- Planifier la configuration de base du serveur
- Planifier l'accès au domaine
- Planifier l'emplacement et le nom du répertoire virtuel sur votre serveur Web
- Planifier un enregistrement d'alias DNS (CNAME) pour votre serveur Web
- Planifier la configuration de CAPolicy.inf
- Planifier la configuration des extensions CDP et AIA sur CA1
- Planifier l'opération de copie entre l'autorité de certification et le serveur Web
- Planifier la configuration du modèle de certificat de serveur sur l'autorité de certification

Planifier la configuration du serveur de base

Après avoir installé Windows Server 2016 sur les ordinateurs que vous envisagez d'utiliser comme autorité de certification et serveur Web, vous devez renommer l'ordinateur et attribuer et configurer une adresse IP statique pour l'ordinateur local.

Pour plus d'informations, consultez le Guide du réseau de base Windows Server 2016.

Planifier l'accès au domaine

Pour ouvrir une session sur un domaine, l'ordinateur doit être membre du domaine et le compte d'utilisateur doit être créé dans les services de domaine Active Directory avant la tentative d'ouverture de session. En outre, la plupart des procédures décrites dans ce guide exigent que le compte d'utilisateur soit membre des groupes Administrateurs d'entreprise ou Administrateurs de domaine dans Utilisateurs et ordinateurs Active

Directory. Vous devez donc vous connecter à l'autorité de certification avec un compte disposant de l'appartenance au groupe appropriée.

Pour plus d'informations, consultez le Guide du réseau de base Windows Server 2016.

Planifier l'emplacement et le nom du répertoire virtuel sur votre serveur Web

Pour fournir l'accès à la liste de révocation de certificats et au certificat d'autorité de certification à d'autres ordinateurs, vous devez stocker ces éléments dans un répertoire virtuel sur votre serveur Web. Dans ce guide, le répertoire virtuel se trouve sur le serveur Web WEB1. Ce dossier se trouve sur le lecteur « C: » et est nommé « pki ». Vous pouvez localiser votre répertoire virtuel sur votre serveur Web à n'importe quel emplacement de dossier approprié pour votre déploiement.

Planifier un enregistrement d'alias DNS (CNAME) pour votre serveur Web

Les enregistrements de ressources d'alias (CNAME) sont également parfois appelés enregistrements de ressources de noms canoniques. Avec ces enregistrements, vous pouvez utiliser plusieurs noms pour pointer vers un seul hôte, ce qui facilite l'hébergement d'un serveur FTP (File Transfer Protocol) et d'un serveur Web sur le même ordinateur. Par exemple, les noms de serveur connus (ftp, www) sont enregistrés à l'aide d'enregistrements de ressources d'alias (CNAME) mappés au nom d'hôte DNS (Domain Name System), tel que WEB1, pour l'ordinateur serveur qui héberge ces services.

Ce guide fournit des instructions pour la configuration de votre serveur Web afin d'héberger la liste de révocation de certificats (CRL) pour votre autorité de certification. Étant donné que vous souhaiterez peut-être également utiliser votre serveur Web à d'autres fins, par exemple pour héberger un FTP ou un site Web, il est judicieux de créer un enregistrement de ressource d'alias dans DNS pour votre serveur Web. Dans ce guide, l'enregistrement CNAME est nommé « pki », mais vous pouvez choisir un nom approprié pour votre déploiement.

Planifier la configuration de CAPolicy.inf

Avant d'installer AD CS, vous devez configurer CAPolicy.inf sur l'autorité de certification avec des informations appropriées pour votre déploiement. Un fichier CAPolicy.inf contient les informations suivantes :

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID=1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=https://pki.corp.contoso.com/pki/cps.txt
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=weeks
CRLPeriodUnits=1
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=1
```

Vous devez planifier les éléments suivants pour ce fichier :

- **URL**. L'exemple de fichier CAPolicy.inf a une valeur d'URL de https://pki.corp.contoso.com/pki/cps.txt. Cela est dû au fait que le serveur Web de ce guide est nommé WEB1 et a un enregistrement de ressource CNAME DNS de pki. Le serveur Web est également joint au domaine corp.contoso.com. En outre, il existe un répertoire virtuel sur le serveur Web nommé « pki » où la liste de révocation des certificats est stockée. Assurez-vous que la valeur que vous fournissez pour l'URL dans votre fichier CAPolicy.inf pointe vers un répertoire virtuel sur votre serveur Web dans votre domaine.

- **RenewalKeyLength**. La longueur de la clé de renouvellement par défaut pour AD CS dans Windows Server 2012 est 2048. La longueur de clé que vous sélectionnez doit être aussi longue que possible tout en assurant la compatibilité avec les applications que vous envisagez d'utiliser.

- **RenewalValidityPeriodUnits**. L'exemple de fichier CAPolicy.inf a une valeur RenewalValidityPeriodUnits de 5 ans. Cela est dû au fait que la durée de vie attendue de l'autorité de certification est d'environ dix ans. La valeur de RenewalValidityPeriodUnits doit refléter la période de validité globale de l'autorité de certification ou le nombre le plus élevé d'années pour lesquelles vous souhaitez effectuer l'inscription.

- **CRLPeriodUnits**. L'exemple de fichier CAPolicy.inf a une valeur CRLPeriodUnits de 1. Cela est dû au fait que l'exemple d'intervalle d'actualisation pour la liste de révocation de certificats dans ce guide est de 1 semaine. À la valeur d'intervalle que vous spécifiez avec ce paramètre, vous devez publier la liste de révocation de

certificats sur l'autorité de certification dans le répertoire virtuel du serveur Web où vous stockez la liste de révocation de certificats et fournir l'accès à celle-ci pour les ordinateurs qui sont dans le processus d'authentification.

- **AlternateSignatureAlgorithm**. Ce fichier CaPolicy.inf implémente un mécanisme de sécurité amélioré en implémentant d'autres formats de signature. Vous ne devez pas implémenter ce paramètre si vous avez toujours des clients Windows XP qui nécessitent des certificats de cette autorité de certification.

Si vous ne prévoyez pas d'ajouter ultérieurement d'autorités de certification secondaires à votre infrastructure à clé publique et si vous souhaitez empêcher l'ajout d'autorités de certification secondaires, vous pouvez ajouter la clé PathLength à votre fichier CAPolicy.inf avec la valeur 0. Pour ajouter cette clé, copiez et collez le code suivant dans votre fichier :

```
[BasicConstraintsExtension]
PathLength=0
Critical=Yes
```

> **Important**
>
> Il n'est pas recommandé de modifier d'autres paramètres dans le fichier CAPolicy.inf, sauf si vous avez une raison spécifique de le faire.

Planifier la configuration des extensions CDP et AIA sur CA1

Lorsque vous configurez le point de distribution de liste de révocation de certificats (CDP) et les paramètres d'accès aux informations de l'autorité (AIA) sur CA1, vous avez besoin du nom de votre serveur Web et de votre nom de domaine. Vous avez également besoin du nom du répertoire virtuel que vous créez sur votre serveur Web où sont stockés la liste de révocation de certificats (CRL) et le certificat d'autorité de certification.

L'emplacement CDP que vous devez entrer pendant cette étape de déploiement a le format suivant :

```
http:\/\/*DNSAlias\
(CNAME\)RecordName*.*Domain*.com\/*VirtualDirectoryName*\/<CaName><CRLNameSuffix>
```

`<DeltaCRLAllowed>.crl.`

Par exemple, si votre serveur Web est nommé WEB1 et que votre enregistrement CNAME d'alias DNS pour le serveur Web est « pki », votre domaine est corp.contoso.com et votre répertoire virtuel est nommé pki, l'emplacement CDP est :

`http:\/\/pki.corp.contoso.com\/pki\/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`

L'emplacement AIA que vous devez entrer a le format suivant :

`http:\/\/*DNSAlias\(CNAME\)RecordName*.*Domain*.com\/*VirtualDirectoryName*\/<ServerDNSName>\_<CaName><CertificateName>.crt.`

Par exemple, si votre serveur Web est nommé WEB1 et que l'enregistrement CNAME de votre alias DNS pour le serveur Web est « pki », votre domaine est corp.contoso.com et votre répertoire virtuel est nommé pki, l'emplacement AIA est :

`http:\/\/pki.corp.contoso.com\/pki\/<ServerDNSName>\_<CaName><CertificateName>.crt`

Planifier l'opération de copie entre l'autorité de certification et le serveur Web

Pour publier la liste de révocation de certificats et le certificat d'autorité de certification de l'autorité de certification dans le répertoire virtuel du serveur Web, vous pouvez exécuter la commande certutil -crl après avoir configuré les emplacements CDP et AIA sur l'autorité de certification. Veillez à configurer les chemins d'accès corrects sous l'onglet **Extensions** des propriétés de l'autorité de certification avant d'exécuter cette commande en suivant les instructions de ce guide. En outre, pour copier le certificat d'autorité de certification d'entreprise sur le serveur Web, vous devez avoir déjà créé le répertoire virtuel sur le serveur Web et configuré le dossier en tant que dossier partagé.

Planifier la configuration du modèle de certificat de serveur sur l'autorité de certification

Pour déployer des certificats de serveur inscrits automatiquement, vous devez copier le modèle de certificat nommé **Serveurs RAS et IAS**. Par défaut, cette copie est nommée **Copie des serveurs RAS et IAS**. Si vous souhaitez renommer cette copie de modèle, planifiez le nom que vous souhaitez utiliser pendant cette étape de déploiement.

Notes

Les trois dernières sections de déploiement de ce guide, qui vous permettent de configurer l'inscription automatique du certificat de serveur, d'actualiser la stratégie de groupe sur les serveurs et de vérifier que les serveurs ont reçu un certificat de serveur valide de l'autorité de certification, ne nécessitent pas d'étapes de planification supplémentaires.

Déploiement de certificats de serveur

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Suivez ces étapes pour installer une autorité de certification racine d'entreprise et déployer des certificats de serveur à utiliser avec PEAP et EAP.

> ⓘ **Important**
>
> Avant d'installer les services de certificats Active Directory, vous devez nommer l'ordinateur, configurer l'ordinateur avec une adresse IP statique et joindre l'ordinateur au domaine. Après avoir installé AD CS, vous ne pouvez pas modifier le nom de l'ordinateur ou l'appartenance au domaine de l'ordinateur, mais vous pouvez modifier l'adresse IP si nécessaire. Pour plus d'informations sur la manière de réaliser ces tâches, consultez le Guide du réseau principal Windows Server® 2016.

- Installer le serveur Web WEB1
- Créer un enregistrement d'alias (CNAME) dans DNS pour WEB1
- Configurer WEB1 pour distribuer des listes de révocation de certificats (CRL)
- Préparer le fichier CAPolicy inf
- Installer l'autorité de certification
- Configurer les extensions CDP et AIA sur CA1
- Copier le certificat d'autorité de certification et la liste de révocation de certificats dans le répertoire virtuel
- Configurer le modèle de certificat de serveur
- Configurer l'inscription automatique du certificat de serveur
- Actualiser la stratégie de groupe
- Vérifier l'inscription de serveur d'un certificat de serveur

> ⓘ **Notes**

Les procédures décrites dans ce guide n'incluent aucune instruction dans le cas où la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre pour demander votre autorisation de continuer. Si cette boîte de dialogue s’ouvre pendant que vous effectuez les procédures de ce guide et si la boîte de dialogue a été ouverte en réponse à vos actions, cliquez sur **Continuer**.

Installer le serveur Web WEB1

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Le rôle Serveur web (IIS) dans Windows Server 2016 fournit une plateforme sécurisée, facile à gérer, modulaire et extensible pour l'hébergement fiable des sites web, des services et des applications. À l'aide d'IIS, vous pouvez partager des informations avec d'autres utilisateurs sur Internet, un intranet ou un extranet. IIS est une plateforme web unifiée qui intègre IIS, ASP.NET, les services FTP, PHP et WCF (Windows Communication Foundation).

Lorsque vous déployez des certificats de serveur, votre serveur Web vous fournit un emplacement où vous pouvez publier la liste de révocation de certificats (CRL) pour votre autorité de certification. Après publication, la liste de révocation de certificats est accessible à tous les ordinateurs de votre réseau afin qu'ils puissent utiliser cette liste pendant le processus d'authentification pour vérifier que les certificats présentés par d'autres ordinateurs ne sont pas révoqués.

Si un certificat est révoqué sur la liste de révocation de certificats, l'effort d'authentification échoue et votre ordinateur est protégé contre l'approbation d'une entité qui a un certificat qui n'est plus valide.

Avant d'installer le rôle Serveur web (IIS), vérifiez que vous avez configuré le nom et l'adresse IP du serveur et que vous avez joint l'ordinateur au domaine.

Pour installer le rôle serveur Serveur Web (IIS)

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs** .

> ⓘ **Notes**
>
> Pour effectuer cette procédure en utilisant Windows PowerShell, ouvrez PowerShell et entrez la commande suivante, puis appuyez sur ENTRÉE. `Install-WindowsFeature Web-Server -IncludeManagementTools`

1. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.
2. Dans **Avant de commencer**, cliquez sur **Suivant**.

Note La page **Avant de commencer** de l'Assistant Ajout de rôles et de fonctionnalités n'est pas affichée si vous avez déjà exécuté l'Assistant Ajout de rôles et de fonctionnalités et que vous

avez sélectionné **Ignorer cette page par défaut** à ce moment-là.

3. Dans la page **Type d'installation** , cliquez sur **Suivant**.
4. Dans la page **de sélection du serveur** , cliquez sur **Suivant**.
5. Dans la page **Rôles serveur** , sélectionnez **Serveur web (IIS),** puis cliquez sur **Suivant**.
6. Cliquez sur **Suivant** jusqu'à ce que vous ayez accepté tous les paramètres de serveur web par défaut, puis cliquez sur **Installer**.
7. Vérifiez que toutes les installations ont réussi, puis cliquez sur **Fermer**.

Créer un enregistrement d'alias (CNAME) dans DNS pour WEB1

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure afin d'ajouter un enregistrement de ressource de nom canonique (CNAME) d'alias pour votre serveur web à une zone DNS de votre contrôleur de domaine. Avec les enregistrements CNAME, vous pouvez utiliser plusieurs noms pour pointer vers un seul hôte, ce qui facilite l'hébergement d'un serveur FTP (File Transfer Protocol) et d'un serveur web sur le même ordinateur.

Ainsi, vous êtes libre d'utiliser votre serveur web pour héberger la liste de révocation de certificats de votre autorité de certification ainsi que pour proposer des services supplémentaires, par exemple un serveur FTP ou un serveur web.

Lorsque vous effectuez cette procédure, remplacez **le nom de l'alias** et d'autres variables par des valeurs appropriées pour votre déploiement.

Pour effectuer cette procédure, vous devez être membre des **administrateurs de domaine**.

Pour ajouter un enregistrement de ressource (CNAME) d'alias à une zone

> ⓘ **Notes**
>
> Pour effectuer cette procédure à l'aide de Windows PowerShell, consultez Add-DnsServerResourceRecordCName.

1. Sur DC1, dans le Gestionnaire de serveur, cliquez sur **Outils** , puis sur **DNS**. La console MMC (Microsoft Management Console) du Gestionnaire DNS s'ouvre.

2. Dans l'arborescence de la console, double-cliquez sur **Zones de recherche directe**, cliquez avec le bouton droit sur la zone de recherche directe où vous souhaitez ajouter l'enregistrement de ressource d'alias, puis cliquez sur **Nouvel alias (CNAME)**. La boîte de dialogue **Nouvel enregistrement de ressource** s'ouvre.

3. Dans le **nom de l'alias**, tapez le nom de l'alias **pki**.

4. Lorsque vous tapez une valeur pour le **nom d'alias**, le **nom de domaine complet (FQDN)** remplit automatiquement la boîte de dialogue. Par exemple, si votre nom d'alias est « pki » et que votre domaine est corp.contoso.com, la valeur **pki.corp.contoso.com** est renseignée automatiquement pour vous.

5. Dans **Nom de domaine complet (FQDN) pour l'hôte cible**, tapez le FQDN de votre serveur web. Par exemple, si votre serveur web est nommé WEB1 et que votre domaine est corp.contoso.com, tapez **WEB1.corp.contoso.com**.

6. Cliquez sur **OK** pour ajouter le nouvel enregistrement à la zone.

Configurer WEB1 pour distribuer des listes de révocation de certificats (CRL)

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour configurer le serveur web WEB1 afin de distribuer des listes de contrôle d'accès.

Dans les extensions de l'autorité de certification racine, il a été indiqué que la liste CRL de l'autorité de certification racine serait disponible via `https://pki.corp.contoso.com/pki`. Actuellement, comme il n'existe aucun répertoire virtuel PKI sur WEB1, il convient d'en créer un.

Pour effectuer cette procédure, vous devez être membre des **administrateurs de domaine**.

> ⓘ **Notes**
>
> Dans la procédure ci-dessous, remplacez le nom du compte d'utilisateur, le nom du serveur web, les noms et emplacements des dossiers et d'autres valeurs par celles qui sont appropriées pour votre déploiement.

Pour configurer WEB1 pour distribuer des certificats et des listes de révocation de certificats

1. Sur WEB1, exécutez Windows PowerShell en tant qu'administrateur, tapez `explorer c:\`, puis appuyez sur ENTRÉE. L'Explorateur Windows s'ouvre pour le lecteur C.

2. Créez un dossier nommé PKI sur le lecteur C:. Pour ce faire, cliquez sur **Accueil**, puis sur **Nouveau dossier**. Un nouveau dossier est créé avec le nom temporaire mis en évidence. Tapez **pki** , puis appuyez sur Entrée.

3. Dans l'Explorateur Windows, cliquez avec le bouton droit sur le dossier que vous venez de créer, pointez le curseur de la souris sur **Partager** avec, puis cliquez sur **Personnes spécifiques**. La boîte de dialogue **Partage de fichiers** s'ouvre.

4. Dans **Partage de fichiers**, tapez **Serveurs de publication de certificats**, puis cliquez sur **Ajouter**. Le groupe Éditeurs de certificats est ajouté à la liste. Dans la liste, dans **le niveau d'autorisation**, cliquez sur la flèche en regard des **serveurs de publication de certificats**, puis cliquez sur **Lecture/écriture**. Cliquez sur **Partager**, puis sur **Terminé**.

5. Fermez l'Explorateur Windows.

6. Ouvrez la console IIS. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire des services Internet (IIS).**

7. Dans l'arborescence de la console du Gestionnaire IIS (Internet Information Services), développez **WEB1**. Si vous êtes invité à commencer à utiliser Microsoft Web Platform, cliquez sur **Annuler**.

8. Développez **Sites** , puis cliquez avec le bouton droit sur le **site web par défaut** , puis cliquez sur **Ajouter un répertoire virtuel**.

9. Dans **Alias**, tapez **pki**. Dans le type **de chemin d'accès physiqueC :\pki**, cliquez sur **OK**.

10. Activez l'accès anonyme au répertoire virtuel pki, afin que n'importe quel client puisse vérifier la validité des certificats d'autorité de certification et des listes de révocation de certificats. Pour cela :

    a. Dans le volet **Connexions** , vérifiez que **pki** est sélectionné.

    b. Sur **pki Home** , cliquez sur **Authentification**.

    c. Dans le volet **Actions** , cliquez sur **Modifier les autorisations**.

    d. Sous l'onglet **Sécurité** , cliquez sur **Modifier**

    e. Dans la boîte de dialogue **Autorisations pour pki**, cliquez sur **Ajouter**.

    f. Dans **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, tapez **ANONYMOUS LOGON; Everyone**, puis cliquez sur **Vérifier les noms**. Cliquez sur **OK**.

    g. Cliquez sur **OK** dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes** .

    h. Cliquez sur **OK** dans la boîte de dialogue **Autorisations pour pki** .

11. Cliquez sur **OK** dans la boîte de dialogue **Propriétés pki** .

12. Dans le volet **Accueil pki** , double-cliquez sur **Filtrage des demandes**.

13. L'onglet **Extensions de noms de fichiers** est sélectionné par défaut dans le volet **Filtrage des demandes**. Dans le volet **Actions** , cliquez sur **Modifier les paramètres de fonctionnalité**.

14. Dans **Modifier les paramètres de filtrage des demandes**, sélectionnez **Autoriser le double-échappement**, pus cliquez sur **OK**.

15. Dans la console MMC du Gestionnaire des services Internet (IIS), cliquez sur le nom de votre serveur web. Par exemple, si votre serveur web est nommé WEB1, cliquez sur **WEB1**.

16. Dans **Actions**, cliquez sur **Redémarrer**. Les services Internet sont arrêtés, puis redémarrés.

Syntaxe CAPolicy.inf

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

CAPolicy.inf est un fichier de configuration qui définit les extensions, les contraintes et les autres paramètres de configuration appliqués à un certificat d'autorité de certification racine et à tous les certificats émis par l'autorité de certification racine. Le fichier CAPolicy.inf doit être installé sur un serveur hôte avant le début de la routine d'installation de l'autorité de certification racine. Lorsque les restrictions de sécurité sur une autorité de certification racine doivent être modifiées, le certificat racine doit être renouvelé et un fichier CAPolicy.inf mis à jour doit être installé sur le serveur avant le début du processus de renouvellement.

CaPolicy.inf est :

- Créé et défini manuellement par un administrateur
- Utilisé lors de la création de certificats d'autorité de certification racine et subordonnés
- Défini sur l'autorité de certification de signature où vous signez et émettez le certificat (et non l'autorité de certification où la demande est accordée)

Une fois que vous avez créé votre fichier CAPolicy.inf, vous devez le copier dans le dossier **%systemroot%** de votre serveur avant d'installer ADCS ou de renouveler le certificat d'autorité de certification.

CAPolicy.inf permet de spécifier et de configurer un large éventail d'attributs et d'options d'autorité de certification. La section suivante décrit toutes les options permettant de créer un fichier .inf adapté à vos besoins spécifiques.

Structure de fichiers CAPolicy.inf

Les termes suivants sont utilisés pour décrire la structure de fichiers .inf :

- *Section* : est une zone du fichier qui couvre un groupe logique de clés. Les noms de section dans les fichiers .inf sont identifiés en apparaissant entre crochets. De nombreuses sections, mais pas toutes, sont utilisées pour configurer des extensions de certificat.
- *Clé* : est le nom d'une entrée et apparaît à gauche du signe égal.
- *Valeur* : est le paramètre et apparaît à droite du signe égal.

Dans l'exemple suivant, **[Version]** est la section, **Signature** est la clé et « **$Windows NT$** » est la valeur.

Example:

```text
[Version]
Signature="$Windows NT$"
```

Version

Identifie le fichier en tant que fichier .inf. La version est la seule section requise et doit se trouver au début de votre fichier CAPolicy.inf.

PolicyStatementExtension

Répertorie les stratégies qui ont été définies par l'organisation, et indique si elles sont facultatives ou obligatoires. Plusieurs stratégies sont séparées par des virgules. Les noms ont une signification dans le contexte d'un déploiement spécifique, ou par rapport aux applications personnalisées qui vérifient la présence de ces stratégies.

Pour chaque stratégie définie, il doit y avoir une section qui définit les paramètres de cette stratégie particulière. Pour chaque stratégie, vous devez fournir un identificateur d'objet défini par l'utilisateur (OID) et le texte que vous souhaitez afficher en tant qu'instruction de stratégie ou pointeur d'URL vers l'instruction de stratégie. L'URL peut être sous la forme d'une URL HTTP, FTP ou LDAP.

Si vous voulez avoir un texte descriptif dans l'instruction de stratégie, les trois lignes suivantes de CAPolicy.inf ressemblent à ceci :

```text
[InternalPolicy]
OID=1.1.1.1.1.1.1
Notice="Legal policy statement text"
```

Si vous envisagez d'utiliser une URL pour héberger l'instruction de stratégie d'autorité de certification, les trois lignes suivantes ressemblent plutôt à ceci :

```text
[InternalPolicy]
OID=1.1.1.1.1.1.2
```

```
URL=https://pki.wingtiptoys.com/policies/legalpolicy.asp
```

De plus :

- Plusieurs clés d'URL et d'avis sont prises en charge.
- Les clés d'URL et d'avis de la même section de stratégie sont prises en charge.
- Les URL avec des espaces ou du texte avec des espaces doivent être entourées de guillemets. Cela est vrai pour la clé **d'URL** , quelle que soit la section dans laquelle elle apparaît.

Voici un exemple de plusieurs avis et URL dans une section de stratégie :

Text

```
[InternalPolicy]
OID=1.1.1.1.1.1.1
URL=https://pki.wingtiptoys.com/policies/legalpolicy.asp
URL=ftp://ftp.wingtiptoys.com/pki/policies/legalpolicy.asp
Notice="Legal policy statement text"
```

CRLDistributionPoint

Vous pouvez spécifier des points de distribution de liste de révocation de certificats (CDP) pour un certificat d'autorité de certification racine dans CAPolicy.inf. Après avoir installé l'autorité de certification, vous pouvez configurer les URL CDP que l'autorité de certification inclut dans chaque certificat émis. Le certificat d'autorité de certification racine affiche les URL spécifiées dans cette section du fichier CAPolicy.inf.

Text

```
[CRLDistributionPoint]
URL=http://pki.wingtiptoys.com/cdp/WingtipToysRootCA.crl
```

Les points de distribution de la liste de révocation de certificats (CDP) prennent en charge :

- HTTP
- URL de fichier
- URL LDAP
- URL multiples

> ⓘ **Important**

Les points de distribution de la liste de révocation de certificats (CDP) ne prennent pas en charge les URL HTTPS.

- Les guillemets doivent entourer les URL d'espaces.
- Si aucune URL n'est spécifiée, autrement dit, si la section **[CRLDistributionPoint]** existe dans le fichier mais est vide, l'extension Point de distribution de CRL est omise du certificat de l'autorité de certification racine. Cela est préférable lors de la configuration d'une autorité de certification racine. Windows n'effectue pas de vérification de révocation sur un certificat d'autorité de certification racine, de sorte que l'extension CDP est superflue dans un certificat d'autorité de certification racine.
- L'autorité de certification peut publier dans FILE UNC, par exemple, sur un partage qui représente le dossier d'un site web où un client récupère via HTTP.
- Utilisez cette section uniquement si vous configurez une autorité de certification racine ou renouvelez le certificat d'autorité de certification racine. L'autorité de certification détermine les extensions CDP d'autorité de certification subordonnées.

AuthorityInformationAccess

Vous pouvez spécifier les points d'accès aux informations d'autorité dans CAPolicy.inf pour le certificat d'autorité de certification racine.

Text

```
[AuthorityInformationAccess]
URL=http://pki.wingtiptoys.com/Public/myCA.crt
```

Quelques remarques supplémentaires sur la section d'accès aux informations de l'autorité :

- Plusieurs URL sont prises en charge.
- Les URL HTTP, FTP, LDAP et FILE sont prises en charge. Les URL HTTPS ne sont pas prises en charge.
- Cette section est utilisée uniquement si vous configurez une autorité de certification racine ou renouvelez le certificat d'autorité de certification racine. Les extensions AIA de l'autorité de certification subordonnée sont déterminées par l'autorité de certification qui a émis le certificat de l'autorité de certification subordonnée.
- Les URL avec des espaces doivent être entourées de guillemets.

- Si aucune URL n'est spécifiée , autrement dit, si la section **[AuthorityInformationAccess]** existe dans le fichier, mais est vide, l'extension d'accès aux informations de l'autorité est omise du certificat d'autorité de certification racine. Là encore, il s'agit du paramètre préféré lorsqu'il n'existe aucune autorité supérieure à une autorité de certification racine qui doit être référencée par un lien vers son certificat.

certsrv_Server

La section `[certsrv_server]` de CAPolicy.inf est facultative. La section `[certsrv_server]` est utilisée pour spécifier la longueur de la clé de renouvellement, la période de validité du renouvellement et la période de validité de la liste de révocation de certificats (CRL) pour une autorité de certification en cours de renouvellement ou d'installation. Aucune des clés de cette section n'est requise. La plupart de ces paramètres ont des valeurs par défaut suffisantes pour la plupart des besoins et peuvent être omis du fichier CAPolicy.inf. Vous pouvez également modifier la plupart de ces paramètres après l'installation de l'autorité de certification.

Voici un exemple :

Text

```
[certsrv_server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=Days
CRLPeriodUnits=2
CRLDeltaPeriod=Hours
CRLDeltaPeriodUnits=4
ClockSkewMinutes=20
LoadDefaultTemplates=True
AlternateSignatureAlgorithm=0
ForceUTF8=0
EnableKeyCounting=0
```

RenewalKeyLength définit la taille de clé pour le renouvellement uniquement. Elle est utilisée uniquement lorsqu'une nouvelle paire de clés est générée lors du renouvellement du certificat d'autorité de certification. La taille de clé du certificat d'autorité de certification initiale est définie lors de l'installation de l'autorité de certification.

Lors du renouvellement d'un certificat d'autorité de certification avec une nouvelle paire de clés, la longueur de la clé peut être augmentée ou réduite. Par exemple, si vous avez défini une taille de clé d'autorité de certification racine de 4096 octets ou plus, puis que vous découvrez que vous avez des applications Java ou des périphériques réseau qui ne peuvent prendre en charge que des tailles de clé de 2048 octets. Que vous augmentiez ou diminuiez la taille, vous devez réémettre tous les certificats émis par cette autorité de certification.

RenewalValidityPeriod et **RenewalValidityPeriodUnits** établissent la durée de vie du nouveau certificat d'autorité de certification racine lors du renouvellement de l'ancien certificat d'autorité de certification racine. Elle s'applique uniquement à une autorité de certification racine. La durée de vie du certificat d'une autorité de certification subordonnée est déterminée par son supérieur. RenewalValidityPeriod peut avoir les valeurs suivantes : heures, jours, semaines, mois et années.

CRLPeriod et **CRLPeriodUnits** déterminent la durée de validité de la CRL de base. **CRLPeriod** peut avoir les valeurs suivantes : Heures, Jours, Semaines, Mois et Années.

CRLDeltaPeriod et **CRLDeltaPeriodUnits** établissent la période de validité de la liste de révocation de certificats delta. **CRLDeltaPeriod** peut avoir les valeurs suivantes : Heures, Jours, Semaines, Mois et Années.

Chacun de ces paramètres peut être configuré après l'installation de l'autorité de certification :

CLI

```
Certutil -setreg CACRLPeriod Weeks
Certutil -setreg CACRLPeriodUnits 1
Certutil -setreg CACRLDeltaPeriod Days
Certutil -setreg CACRLDeltaPeriodUnits 1
```

N'oubliez pas de redémarrer les services de certificats Active Directory pour que les modifications prennent effet.

LoadDefaultTemplates s'applique uniquement lors de l'installation d'une autorité de certification d'entreprise. Ce paramètre, True ou False (ou 1 ou 0), détermine si l'autorité de certification est configurée avec l'un des modèles par défaut.

Dans une installation par défaut de l'autorité de certification, un sous-ensemble des modèles de certificat par défaut est ajouté au dossier Modèles de certificats dans le composant logiciel enfichable Autorité de certification. Cela signifie que dès que le service AD CS démarre après l'installation du rôle, un utilisateur ou un ordinateur disposant d'autorisations suffisantes peut immédiatement s'inscrire pour obtenir un certificat.

Vous ne souhaiterez peut-être pas émettre de certificats immédiatement après l'installation d'une autorité de certification. Vous pouvez donc utiliser le paramètre LoadDefaultTemplates pour empêcher l'ajout des modèles par défaut à l'autorité de certification Enterprise. Si aucun modèle n'est configuré sur l'autorité de certification, elle ne peut émettre aucun certificat.

AlternateSignatureAlgorithm configure l'autorité de certification pour prendre en charge le format de signature PKCS#1 V2.1 pour le certificat d'autorité de certification et les demandes de certificat. Lorsque la valeur est 1 sur une autorité de certification racine, le certificat

d'autorité de certification inclut le format de signature PKCS#1 V2.1. Lorsque la valeur est définie sur une autorité de certification subordonnée, l'autorité de certification subordonnée crée une demande de certificat qui inclut le format de signature PKCS#1 V2.1.

ForceUTF8 modifie l'encodage par défaut des noms uniques relatifs (RDN) dans les noms uniques objet et émetteur en UTF-8. Seuls les RDN qui prennent en charge UTF-8, tels que ceux qui sont définis en tant que types de chaîne de répertoires par une RFC, sont affectés. Par exemple, le RDN pour le contrôleur de domaine (DC) prend en charge l'encodage en tant que IA5 ou UTF-8, tandis que le RDN de pays (C) prend uniquement en charge l'encodage sous forme de chaîne imprimable. La directive ForceUTF8 affecte donc un RDN DC, mais n'affecte pas un RDN C.

EnableKeyCounting configure l'autorité de certification pour incrémenter un compteur chaque fois que la clé de signature de l'autorité de certification est utilisée. N'activez pas ce paramètre, sauf si vous disposez d'un module de sécurité matériel (HSM) et d'un fournisseur de services de chiffrement (CSP) associé qui prend en charge le comptage des clés. Le comptage des clés n'est pas pris en charge par le fournisseur de solutions cloud Microsoft Strong ou par le fournisseur de stockage de clés logicielles (KSP) Microsoft.

Créer le fichier CAPolicy.inf

Avant d'installer AD CS, vous configurez le fichier CAPolicy.inf avec des paramètres spécifiques pour votre déploiement.

Prérequis: Vous devez être membre du groupe Administrateurs.

1. Sur l'ordinateur sur lequel vous envisagez d'installer AD CS, ouvrez Windows PowerShell, tapez **notepad.exe** et `appuyez sur Entrée`.

2. Tapez le texte suivant :

Text

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID=1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=https://pki.corp.contoso.com/pki/cps.txt
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=weeks
```

```
CRLPeriodUnits=1
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=1
[CRLDistributionPoint]
[AuthorityInformationAccess]
```

3. Sélectionnez **Fichier**, puis **sélectionnez Enregistrer sous**.

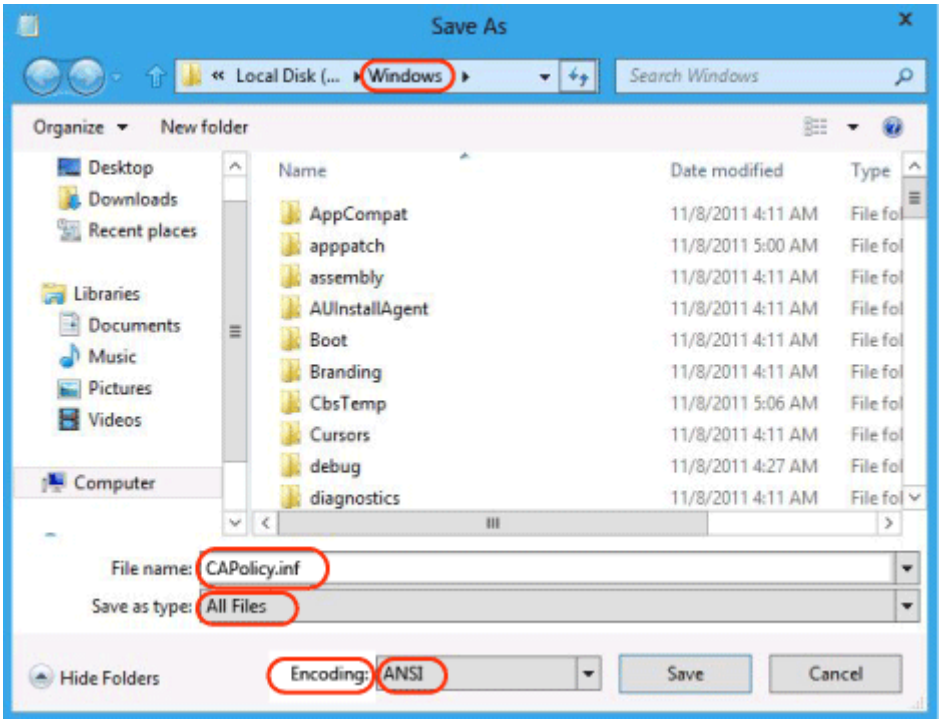
4. Accédez au dossier *%systemroot%* .

5. Vérifiez que les options suivantes sont activées :

   - **Le nom de fichier** est défini sur **CAPolicy.inf**
   - **Type** a la valeur **Tous les fichiers**
   - **L'encodage** est **ANSI**

6. Cliquez sur **Enregistrer**.

7. Lorsque vous êtes invité à remplacer le fichier, sélectionnez **Oui**.



> ⊗ **Attention**
>
> Veillez à enregistrer le fichier CAPolicy.inf avec l'extension inf. Si vous ne tapez pas spécifiquement **.inf** à la fin du nom de fichier et ne sélectionnez pas les options décrites ci-dessus, le fichier sera enregistré en tant que fichier texte et ne sera pas utilisé pendant l'installation de l'autorité de certification.

8. Fermez le Bloc-notes.

> **Important**
>
> Dans le fichier CAPolicy.inf, vous pouvez voir une ligne qui spécifie l'URL `https://pki.corp.contoso.com/pki/cps.txt`. La section de stratégie interne du fichier CAPolicy.inf est juste affichée en tant qu'exemple de spécification de l'emplacement d'une déclaration de mise en œuvre des certificats. Dans ce guide, vous n'êtes pas invité à créer l'instruction de pratique de certificat (CPS).

Installer l'autorité de certification sur Windows Server

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Suivez ces étapes pour configurer les services de certificats Active Directory (AD CS). Cela vous permet d'émettre des certificats de serveur pour les serveurs exécutant le serveur de stratégie réseau (NPS), le routage et le service d'accès à distance (RRAS) ou les deux.

Prerequisites

- L'appartenance aux **administrateurs d'entreprise** et au groupe **Administrateurs** de domaine racine du domaine est la condition minimale requise pour effectuer cette procédure.
- Avant d'installer les services de certificats Active Directory, **vous devez nommer l'ordinateur, configurer l'ordinateur avec une adresse IP statique et joindre l'ordinateur au domaine**.
  - Pour plus d'informations sur l'accomplissement de ces tâches, consultez les composants réseau Windows Server Core.
  - Pour effectuer cette procédure, l'ordinateur sur lequel vous installez AD CS doit être joint à un domaine dans lequel les services de domaine Active Directory (AD DS) sont installés.

Installer les services de certificats Active Directory à l'aide de PowerShell

Pour utiliser Windows PowerShell pour installer les services de certificats Active Directory, procédez comme suit.

1. Ouvrez Windows PowerShell et tapez la commande suivante, puis appuyez sur Entrée.

   PowerShell

   ```
   Install-WindowsFeature -Name ADCS-Cert-Authority -IncludeManagementTools
   ```

2. Une fois AD CS installé, tapez la commande suivante et appuyez sur Entrée.

```
PowerShell

Install-AdcsCertificationAuthority -CAType EnterpriseRootCA
```

Pour plus d'informations sur cette applet de commande et ses paramètres disponibles, consultez Install-AdcsCertificationAuthority.

Installer les services de certificats Active Directory à l'aide du Gestionnaire de serveur

Pour utiliser le Gestionnaire de serveur pour installer les services de certificats Active Directory, procédez comme suit.

1. Ouvrez une session en tant que membre du groupe Administrateurs de l'entreprise et du groupe Admins du domaine du domaine racine.
2. Dans le Gestionnaire de serveur, sélectionnez **Gérer**, puis **ajoutez des rôles et des fonctionnalités** pour ouvrir l'Assistant Ajout de rôles et de fonctionnalités.
3. Dans **Avant de commencer**, sélectionnez **Suivant**.

   > ⓘ **Notes**
   >
   > La page **Avant de commencer** de l'Assistant Ajout de rôles et de fonctionnalités ne s'affiche pas si vous avez précédemment sélectionné **Ignorer cette page par défaut**.

4. Dans **Sélectionner le type d'installation**, vérifiez que **Role-Based ou l'installation basée sur les fonctionnalités** est sélectionnée, puis sélectionnez **Suivant**.
5. Dans **Sélectionner un serveur de destination**, vérifiez que **sélectionnez un serveur à partir du pool de serveurs** . Dans le **pool de serveurs**, vérifiez que l'ordinateur local est sélectionné. Cliquez sur **Suivant**.
6. Dans **Sélectionner des rôles de serveur**, dans **Rôles**, sélectionnez **Services de certificats Active Directory**. Lorsque vous êtes invité à ajouter des fonctionnalités requises, sélectionnez **Ajouter des fonctionnalités**, puis sélectionnez **Suivant**.
7. Dans **Sélectionner des fonctionnalités**, sélectionnez **Suivant**.
8. Dans **Les services de certificats Active Directory**, lisez les informations fournies, puis sélectionnez **Suivant**.

9. Dans **Confirmer les sélections d'installation**, sélectionnez **Installer**. Ne fermez pas l'Assistant pendant le processus d'installation. Une fois l'installation terminée, sélectionnez **Configurer les services de certificats Active Directory sur le serveur de destination**. L'assistant de configuration des services AD CS s'ouvre. Lisez les informations d'identification et, si nécessaire, fournissez les informations d'identification d'un compte membre du groupe Administrateurs d'entreprise. Cliquez sur **Suivant**.

10. Dans **Services de rôle**, sélectionnez **Autorité de certification**, puis **Sélectionnez Suivant**.

11. Dans la **Type de configuration**, vérifiez que **CA Enterprise** est sélectionnée, puis sélectionnez **Suivant**.

12. Dans la page « Spécifier le type de l'autorité de certification », vérifiez que « Autorité de certification racine » est bien sélectionnée, puis sélectionnez « Suivant ».

13. Dans **la page Spécifier le type de la clé privée, vérifiez** que **créer une clé privée** est sélectionnée, puis sélectionnez **Suivant**.

14. Dans la page **Cryptographie pour l'AC**, conservez les paramètres par défaut du **RSA#Microsoft Software Key Storage Provider** pour le fournisseur de stockage de clés logicielles et de l'algorithme de hachage **SHA2**, puis déterminez la meilleure longueur de clé pour votre déploiement. Les grandes longueurs de caractères de clé offrent une sécurité optimale. Toutefois, cela peut avoir un impact sur les performances du serveur et peuvent ne pas être compatibles avec les applications héritées. Il est recommandé de conserver le paramètre par défaut 2048. Cliquez sur **Suivant**.

15. Dans la page **Nom** de l'autorité de certification, conservez le nom commun suggéré pour l'autorité de certification ou modifiez le nom en fonction de vos besoins. Vérifiez que vous êtes certain que le nom de l'autorité de certification est compatible avec vos conventions et objectifs d'affectation de noms, car vous ne pouvez pas modifier le nom de l'autorité de certification une fois que vous avez installé AD CS. Cliquez sur **Suivant**.

16. Dans la page **Période** de validité, dans **Spécifier la période de validité**, tapez le nombre et sélectionnez une valeur de temps (Années, Mois, Semaines ou Jours). Le paramètre par défaut de cinq ans est recommandé. Cliquez sur **Suivant**.

17. Dans la page **Base de données de l'autorité de certification**, dans **Spécifier les emplacements de la base de données**, spécifiez l'emplacement du dossier de la base de données de certificat et du journal de la base de données de certificat. Si vous spécifiez des emplacements autres que les emplacements par défaut, assurez-vous que les dossiers sont sécurisés avec des listes de contrôle d'accès qui empêchent les utilisateurs ou ordinateurs non autorisés d'accéder à la base de données et aux fichiers journaux de l'autorité de certification. Cliquez sur **Suivant**.

18. Dans **Confirmation**, sélectionnez **Configurer** pour appliquer vos sélections, puis **sélectionnez Fermer**.

Configurer les extensions CDP et AIA sur CA1

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour configurer le point de distribution de la liste de révocation de certificats (CDP) et les paramètres d'accès aux informations d'autorité (AIA) sur CA1.

Pour effectuer cette procédure, vous devez être membre des Administrateurs de domaine.

Pour configurer les extensions CDP et AIA sur CA1

1. Dans Gestionnaire de serveur, cliquez sur **Tools** puis cliquez sur **Certification Authority**.

2. Dans l'arborescence de la console Autorité de certification, cliquez avec le bouton droit sur **corp-CA1-CA**, puis cliquez sur **Propriétés**.

   > ⓘ **Remarque**
   >
   > Le nom de votre autorité de certification est différent si vous n'avez pas nommé l'ordinateur CA1 et si votre nom de domaine est différent de celui de cet exemple. Le nom de l'autorité de certification est au format *domain-CAComputerName*-CA.

3. Cliquez sur l'onglet **Extensions** . Vérifiez que **l'extension Select** est définie sur **CRL Distribution Point (CDP)** et, dans les **emplacements de spécification des emplacements à partir desquels les utilisateurs peuvent obtenir une liste de révocation de certificats (CRL),** procédez comme suit :

   a. Sélectionnez l'entrée `file://\\<ServerDNSName>\CertEnroll\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`, puis cliquez sur **Supprimer**. Dans **Confirmer la suppression**, cliquez sur **Oui**.

   b. Sélectionnez l'entrée `http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`, puis cliquez sur **Supprimer**. Dans **Confirmer la suppression**, cliquez sur **Oui**.

c. Sélectionnez l'entrée qui commence par le chemin d'accès `ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>`, puis cliquez sur **Supprimer**. Dans **Confirmer la suppression**, cliquez sur **Oui**.

4. Dans **Spécifier les emplacements à partir desquels les utilisateurs peuvent obtenir une liste de révocation de certificats (CRL)**, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un emplacement** s'ouvre.

5. Dans **Ajouter un emplacement**, dans **Emplacement**, tapez `http://pki.corp.contoso.com/pki/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`, puis cliquez sur **OK**. Cela vous renvoie à la boîte de dialogue Propriétés de l'autorité de certification.

6. Sous l'onglet **Extensions** , cochez les cases suivantes :

   - **Inclure dans les listes de révocation de certificats. Les clients l'utilisent pour retrouver les emplacements des listes de révocation de certificats delta**

   - **Inclure dans l'extension CDP des certificats émis**

7. Dans **Spécifier les emplacements à partir desquels les utilisateurs peuvent obtenir une liste de révocation de certificats (CRL)**, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un emplacement** s'ouvre.

8. Dans **Ajouter un emplacement**, dans **Emplacement**, tapez `file://\\pki.corp.contoso.com\pki\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`, puis cliquez sur **OK**. Cela vous renvoie à la boîte de dialogue Propriétés de l'autorité de certification.

9. Sous l'onglet **Extensions** , cochez les cases suivantes :

   - **Publier les listes de révocation de certificats sur cet emplacement**

   - **Publier les listes de révocation de certificats delta sur cet emplacement**

10. Changez **l'extension à Sélectionner** à **Accès aux Informations d'Autorité (AIA)**, et dans **les emplacements à partir desquels les utilisateurs peuvent obtenir un certificat pour cette autorité de certification**, procédez comme suit :

    a. Sélectionnez l'entrée qui commence par le chemin d'accès `ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services`, puis cliquez sur **Supprimer**. Dans **Confirmer la suppression**, cliquez sur **Oui**.

b. Sélectionnez l'entrée `http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt`, puis cliquez sur **Supprimer**. Dans **Confirmer la suppression**, cliquez sur **Oui**.

c. Sélectionnez l'entrée `file://\\<ServerDNSName>\CertEnroll\<ServerDNSName><CaName><CertificateName>.crt`, puis cliquez sur **Supprimer**. Dans **Confirmer la suppression**, cliquez sur **Oui**.

11. Dans **Spécifier les emplacements à partir desquels les utilisateurs peuvent obtenir le certificat pour cette autorité de certification**, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un emplacement** s'ouvre.

12. Dans **Ajouter un emplacement**, dans **Emplacement**, tapez `http://pki.corp.contoso.com/pki/<ServerDNSName>_<CaName><CertificateName>.crt`, puis cliquez sur **OK**. Cela vous renvoie à la boîte de dialogue Propriétés de l'autorité de certification.

13. Sous l'onglet **Extensions** , sélectionnez **Inclure dans l'AIA des certificats émis**.

14. Lorsque vous êtes invité à redémarrer Active Directory Services de certificats, cliquez sur **No**. Vous redémarrerez le service ultérieurement.

Last updated on 21/04/2026

Copiez le certificat d'autorité de certification et la liste CRL dans le répertoire virtuel

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour copier la liste de révocation de certificats et le certificat d'autorité de certification racine d'entreprise de votre autorité de certification vers un répertoire virtuel sur votre serveur Web, et vérifier que AD CS est correctement configuré. Avant d'exécuter les commandes ci-dessous, veillez à remplacer les noms de répertoire et de serveur par ceux qui sont appropriés pour votre déploiement.

Pour effectuer cette procédure, vous devez être membre des **administrateurs de domaine**.

Pour copier la liste de révocation de certificats de CA1 vers WEB1

1. Sur CA1, exécutez Windows PowerShell en tant qu'administrateur, puis publiez la liste de révocation de certificats avec la commande suivante :

   - Tapez `certutil -crl`, puis appuyez sur ENTRÉE.

   - Pour copier le certificat CA1 dans le partage de fichiers sur votre serveur Web, tapez `copy C:\Windows\system32\certsrv\certenroll\*.crt \\WEB1\pki`, puis appuyez sur Entrée.

   - Pour copier les listes de révocation de certificats dans le partage de fichiers sur votre serveur Web, tapez `copy C:\Windows\system32\certsrv\certenroll\*.crl \\WEB1\pki`, puis appuyez sur ENTRÉE.

2. Pour vérifier que les emplacements des extensions CDP et AIA sont correctement configurés, tapez `pkiview.msc`, puis appuyez sur la touche ENTRÉE. La console MMC pkiview Enterprise PKI s'ouvre.

3. Dans le volet gauche, cliquez sur le nom d'AC.

   Par exemple, si votre nom d'autorité de certification est corp-CA1-CA, cliquez sur **corp-CA1-CA**.

4. Dans la colonne État du volet de résultats, vérifiez que les valeurs des éléments suivants indiquent **OK** :

- **Certificat d'autorité de certification**
- **Emplacement AIA 1**
- **Emplacement CDP 1**

Conseil

Si **l'état** d'un élément n'est pas **OK**, procédez comme suit :

- Ouvrez le partage sur votre serveur Web pour vérifier que les fichiers de liste de certificats et de révocation de certificats ont été correctement copiés dans le partage. Si elles n'ont pas été correctement copiées dans le partage, modifiez vos commandes de copie avec la source de fichier et la destination de partage appropriées, puis réexécutez les commandes.
- Vérifiez que vous avez entré les emplacements appropriés pour CDP et AIA dans l'onglet Extensions d'AC. Assurez-vous qu'il n'y a pas d'espaces ou d'autres caractères supplémentaires dans les emplacements que vous avez fournis.
- Vérifiez que vous avez copié la liste de révocation de certificats et le certificat d'autorité de certification vers l'emplacement approprié sur votre serveur Web, et que l'emplacement correspond à l'emplacement que vous avez fourni pour les emplacements CDP et AIA sur l'autorité de certification.
- Vérifiez que vous avez correctement configuré les autorisations pour le dossier virtuel dans lequel le certificat d'autorité de certification et la liste de révocation de certificats sont stockés.

Configurer le modèle de certificat de serveur pour l'accès à distance et le serveur de stratégie réseau

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Cet article explique comment configurer un modèle de certificat de serveur dans Les services de certificats Active Directory (AD CS) à utiliser avec l'accès à distance, notamment les serveurs de passerelle RAS et le serveur de stratégie réseau (NPS). En suivant ces étapes, vous pouvez configurer l'inscription automatique des certificats pour les serveurs exécutant des services d'accès à distance ou NPS, ce qui simplifie la gestion des certificats et améliore la sécurité réseau.

Lorsque vous configurez ce modèle, vous pouvez spécifier les serveurs par le groupe de sécurité Active Directory qui doivent recevoir automatiquement un certificat de serveur à partir d'AD CS.

Prerequisites

Avant de commencer, vérifiez que les conditions préalables suivantes sont remplies :

- Active Directory Certificate Services (AD CS) est installé et configuré avec au moins une autorité de certification d'entreprise.
- Un compte d'utilisateur membre des **administrateurs d'entreprise** et du groupe **Administrateurs de domaine** racine.
- Serveurs exécutant le service d'accès à distance ou NPS qui sont membres du groupe de sécurité **ras et serveurs IAS** dans Active Directory.

Configurer le modèle de certificat de serveur

Pour configurer le modèle de certificat de serveur pour l'accès à distance et NPS, procédez comme suit :

1. Sur votre serveur AD CS, dans le Gestionnaire de serveur, sélectionnez **Outils**, puis **autorité de certification**. La Console de gestion de l'autorité de certification Microsoft (Microsoft Management Console - MMC) s'ouvre.

2. Dans la console MMC, double-cliquez sur le nom de l'autorité de certification, cliquez avec le bouton droit sur **Modèles de certificat**, puis sélectionnez **Gérer**.

3. La console Modèles de certificats s'ouvre. Tous les modèles de certificat sont affichés dans le volet d'informations.

4. Dans le volet d'informations, sélectionnez le modèle **RAS et le serveur IAS**.

5. Sélectionnez le menu **Action** , puis sélectionnez **Dupliquer le modèle**. La boîte de dialogue **Propriétés** du modèle s'ouvre.

6. Sélectionnez l'onglet **Sécurité** .

7. Sous l'onglet **Sécurité** , pour les **noms de groupe ou d'utilisateur**, sélectionnez **les serveurs RAS et IAS**.

8. Dans **Autorisations pour les serveurs RAS et IAS**, pour **Autoriser**, **vérifiez que l'inscription** est cochée, puis cochez la case pour **l'inscription automatique**. Sélectionnez **OK**, puis fermez la console MMC des modèles de certificat.

9. Dans la console MMC de l'autorité de certification, sélectionnez **Modèles de certificat**. Dans le menu **Action** , sélectionnez **Nouveau**, puis sélectionnez **Modèle de certificat à émettre**. La boîte de dialogue **Activer les modèles de certificat** s'ouvre.

10. Dans **Activer les modèles de certificat**, sélectionnez le nom du modèle de certificat que vous avez configuré, puis sélectionnez **OK**. Par exemple, si vous n'avez pas modifié le nom du modèle de certificat par défaut, sélectionnez **Copier du serveur RAS et IAS**, puis **sélectionnez OK**.

11. Fermez la MMC de l'autorité de certification.

Vous avez configuré le modèle de certificat de serveur pour l'accès à distance et NPS. Ce modèle permet aux serveurs du groupe de sécurité **RAS et IAS Servers** de s'inscrire automatiquement pour un certificat de serveur à partir du service AD CS.

Étape suivante

Configurez l'inscription automatique des certificats pour le serveur de stratégie réseau.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Configurer l’inscription automatique des certificats pour le serveur de stratégie réseau

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

L’inscription automatique de certificat simplifie le processus de déploiement et de gestion des certificats sur les serveurs exécutant le serveur de stratégie réseau (NPS) dans un environnement Active Directory. Cet article explique comment configurer l’inscription automatique pour les certificats serveur et utilisateur à l’aide de la stratégie de groupe. En suivant ces étapes, vous pouvez vous assurer que les certificats sont émis, renouvelés et gérés automatiquement pour les serveurs et les utilisateurs de votre organisation.

Prerequisites

Avant de commencer, vérifiez que les conditions préalables suivantes sont remplies :

- Active Directory Certificate Services (AD CS) est installé et configuré avec au moins une autorité de certification d’entreprise.
- Vous avez configuré le modèle de certificat de serveur pour l’inscription automatique. Pour plus d’informations, consultez Configurer un modèle de certificat de serveur pour l’inscription automatique.
- Vous disposez d’un compte d’utilisation membre des administrateurs **d’entreprise** et des groupes de sécurité **Administrateurs de domaine** du domaine racine.
- Accès aux consoles de gestion suivantes :
  - Gestion des stratégies de groupe
  - Serveur de stratégie réseau.

Configurer l'autorégistration du serveur et du certificat utilisateur

Pour configurer l’inscription automatique pour les certificats de serveur, procédez comme suit :

1. Ouvrez la console gestion des stratégies de groupe.
2. Développez les nœuds de votre forêt et de votre domaine Active Directory et recherchez la **stratégie de domaine par défaut**. Cliquez avec le bouton droit sur la stratégie **de**

domaine par défaut , puis sélectionnez **Modifier**, ce qui ouvre l'éditeur de gestion des stratégies de groupe.

3. Accédez au chemin d'accès suivant dans l'éditeur de gestion des stratégies de groupe : **Configuration de l'ordinateur**>**Stratégies**>**Paramètres Windows**>**Paramètres de sécurité**>**Stratégies de clé publique**.

4. Dans le volet d'informations, double-cliquez sur **Client des services de certificats - Inscription automatique**. La boîte de dialogue **Propriétés** s'ouvre. Configurez les éléments suivants :
   a. Pour **le modèle de configuration**, sélectionnez **Activé**.
   b. Cochez la case **Renouveler les certificats expirés, mettez à jour les certificats en attente et supprimez les certificats révoqués**.
   c. Cochez la case pour **mettre à jour les certificats qui utilisent des modèles de certificat**.

5. Cliquez sur **OK**. Laissez la console de l'Éditeur de gestion des stratégies de groupe ouverte pour configurer l'inscription automatique des certificats utilisateur.

6. Accédez au chemin d'accès suivant : **Configuration de l'utilisateur**>**Stratégies**>**Paramètres Windows**>**Paramètres de sécurité**>**Stratégies de clé publique**.

7. Dans le volet d'informations, double-cliquez sur **Client des services de certificats - Inscription automatique**. La boîte de dialogue **Propriétés** s'ouvre. Configurez les éléments suivants :
   a. Pour **le modèle de configuration**, sélectionnez **Activé**.
   b. Cochez la case **Renouveler les certificats expirés, mettez à jour les certificats en attente et supprimez les certificats révoqués**.
   c. Cochez la case pour **mettre à jour les certificats qui utilisent des modèles de certificat**.

8. Sélectionnez **OK**, puis fermez la console Éditeur de gestion des stratégies de groupe.

9. Actualisez les paramètres de stratégie de groupe sur vos serveurs NPS pour appliquer les paramètres d'inscription automatique. Vous pouvez forcer une actualisation immédiate en exécutant la commande suivante dans une invite de commandes avec élévation de privilèges :

Invite de commandes Windows
`gpupdate /force`

Vérifier l’inscription des certificats de serveur pour NPS

Une fois que vous avez configuré l’inscription automatique et la stratégie de groupe actualisée, vous pouvez vérifier que le certificat de serveur est correctement inscrit. Pour vérifier qu’un certificat de serveur est correctement configuré et inscrit au serveur NPS, vous créez une stratégie de réseau de test et autorisez NPS à vérifier que NPS peut utiliser le certificat pour l’authentification. Vous n’avez pas terminé l'assistant. Par conséquent, la stratégie de réseau de test n'est pas créée dans NPS. Cependant, vous pouvez vérifier que le certificat de serveur est inscrit.

Pour vérifier l'inscription d'un certificat de serveur dans NPS :

1. Ouvrez la console **du serveur de stratégie réseau** .
2. Développez **Stratégies** et sélectionnez **Stratégies réseau**.
3. Cliquez avec le bouton droit sur **Stratégies réseau**, puis sélectionnez **Nouveau**. L’**Assistant Nouvelle stratégie réseau** s’ouvre.
4. Pour **spécifier le nom de la stratégie réseau et le type de connexion**, dans **le nom** de la stratégie, entrez un nom, tel que *tester la stratégie d’inscription automatique*. Vérifiez que **le type de serveur d’accès réseau** a la valeur **Non spécifiée**, puis sélectionnez **Suivant**.
5. Pour **spécifier des conditions**, sélectionnez **Ajouter**. Sélectionnez **Groupes Windows**, puis **sélectionnez Ajouter**.
6. Pour **les groupes Windows**, sélectionnez **Ajouter des groupes**. Entrez un groupe valide, tel que **Les utilisateurs de domaine**, puis sélectionnez **OK**. Sélectionnez **à nouveau OK** pour **les groupes Windows**. Vérifiez que votre groupe est répertorié en tant que condition, puis sélectionnez **Suivant**.
7. Pour **spécifier l’autorisation d’accès**, vérifiez que **l’accès accordé** est sélectionné, puis sélectionnez **Suivant**.
8. Pour **configurer les méthodes d’authentification**, sélectionnez **Ajouter**. Pour **Ajouter EAP**, sélectionnez **Microsoft : Protected EAP (PEAP),** puis **ok**.
9. Dans **Types EAP**, sélectionnez **Microsoft : Protected EAP (PEAP),** puis sélectionnez **Modifier**.
10. Dans la boîte de dialogue **Modifier les propriétés EAP protégées** , dans **Certificat émis,** NPS affiche le nom de votre certificat de serveur en tant que nom de domaine complet (FQDN). Par exemple, si votre serveur NPS est nommé NPS-01 et que votre domaine est

example.com, NPS affiche le certificat **NPS-01.example.com**. De plus, dans **l'émetteur**, le nom de votre autorité de certification s'affiche et, dans la **date d'expiration**, la date d'expiration du certificat de serveur s'affiche.

> ⓘ **Important**
>
> Si NPS n'affiche pas de certificat de serveur valide et s'il fournit le message indiquant qu'un tel certificat est introuvable sur l'ordinateur local, il existe deux raisons possibles :
>
> a. La stratégie de groupe n'a pas été actualisée correctement et le serveur NPS n'a pas obtenu un certificat de la part de l'autorité de certification. Dans ce cas, redémarrez le serveur NPS. Lorsque le serveur redémarre, la stratégie de groupe est actualisée et vous pouvez réessayer pour vérifier que le certificat de serveur est inscrit.
>
> b. Le modèle de certificat, l'inscription automatique de certificat ou les deux ne sont pas configurés correctement. Pour résoudre ces problèmes, vérifiez que vous avez suivi correctement toutes les étapes décrites dans cet article pour vous assurer que les paramètres que vous avez fournis sont exacts.

11. Une fois que vous avez vérifié la présence d'un certificat de serveur valide, vous pouvez sélectionner **OK** et **Annuler** pour quitter l'Assistant. Étant donné que vous n'avez pas mené à bien l'assistant de configuration, la stratégie de réseau de test n'est pas créée dans NPS.

Ce processus montre que votre serveur NPS inscrit un certificat de serveur valide qu'il peut utiliser pour prouver son identité aux ordinateurs clients qui tentent d'accéder au réseau via vos serveurs d'accès réseau, tels que les serveurs de réseau privé virtuel (VPN), les points d'accès sans fil compatibles 802.1X, les serveurs de passerelle Bureau à distance et les commutateurs Ethernet compatibles 802.1X.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Last updated on 16/08/2025

Déployer un accès sans fil authentifié 802.1X basé sur des mots de passe

Article • 14/04/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Il s'agit d'un guide d'accompagnement au Guide du réseau principal de Windows Server® 2016. Le Guide du réseau principal fournit des instructions sur la planification et le déploiement des composants requis pour un réseau pleinement fonctionnel et un nouveau domaine Active Directory® dans une nouvelle forêt.

Ce guide explique comment effectuer un déploiement sur un réseau de base. Pour cela, il fournit des instructions sur la façon de déployer un accès sans fil IEEE (Institute of Electrical and Electronics Engineers) 802.11, authentifié par IEEE 802.1X à l'aide du protocole PEAP (Protected Extensible Authentication Protocol) - Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2).

Étant donné que PEAP-MS-CHAP v2 exige que les utilisateurs fournissent des informations d'identification basées sur un mot de passe plutôt qu'un certificat pendant le processus d'authentification, il est généralement plus facile et moins coûteux de déployer que EAP-TLS ou PEAP-TLS.

> **Notes**
>
> Dans ce guide, l'accès sans fil authentifié IEEE 802.1X avec PEAP-MS-CHAP v2 est abrégé en « accès sans fil » et « accès Wi-Fi ».

À propos de ce guide

Ce guide, en combinaison avec les guides de prérequis décrits ci-dessous, fournit des instructions sur le déploiement de l'infrastructure d'accès Wi-Fi suivante.

- Un ou plusieurs points d'accès sans fil 802.11 compatibles avec 802.1X.
- Utilisateurs et ordinateurs Active Directory Domain Services (AD DS).
- Gestion des stratégies de groupe
- Un ou plusieurs serveurs NPS (Network Policy Server).

- Certificats de serveur pour les ordinateurs exécutant NPS (Network Policy Server)
- Ordinateurs clients sans fil exécutant Windows® 10, Windows 8.1 ou Windows 8.

Dépendances pour ce guide

Pour déployer correctement une connexion sans fil authentifiée avec ce guide, vous devez disposer d'un environnement réseau et de domaine avec toutes les technologies requises déployées. Vous devez également avoir des certificats de serveur déployés sur vos serveurs NPS (Network Policy Server) d'authentification.

Les sections suivantes fournissent des liens vers la documentation qui vous montre comment déployer ces technologies.

Dépendances de l'environnement de réseau et de domaine

Ce guide s'adresse aux administrateurs système et réseau ayant suivi les instructions fournies dans le **Guide du réseau principal** Windows Server 2016 pour déployer un réseau principal, ou pour ceux qui ont déjà déployé les technologies de base incluses dans le réseau principal, y compris AD DS, DNS (Domain Name Service), le protocole DHCP (Dynamic Host Configuration Protocol), TCP/IP, NPS et le service WINS (Windows Internet Name Service).

Le Guide du réseau principal Windows Server 2016 est disponible dans la bibliothèque technique Windows Server 2016.

Dépendances de certificats de serveur

Il existe deux options disponibles pour inscrire des serveurs d'authentification avec des certificats de serveur à utiliser avec l'authentification 802.1X : déployer votre propre infrastructure de clé publique à l'aide des services de certificats Active Directory (AD CS) ou utiliser des certificats de serveur inscrits par une autorité de certification publique.

AD CS

Les administrateurs réseau et système qui déploient une connexion sans fil authentifiée doivent suivre les instructions du guide d'accompagnement du réseau principal Windows Server 2016, **Déployer des certificats de serveur pour les déploiements câblés et sans fil 802.1X**. Ce guide explique comment déployer et utiliser AD CS pour inscrire automatiquement des certificats de serveur sur des ordinateurs exécutant NPS.

Ce guide est disponible à l'emplacement suivant.

- Le Guide d'accompagnement du réseau principal Windows Server 2016 Déployer des certificats de serveur pour les déploiements câblés et sans fil 802.1X au format HTML dans la bibliothèque technique.

Autorité de certification publique

Vous pouvez acheter des certificats serveur auprès d'une autorité de certification publique, telle que VeriSign, que les ordinateurs clients approuvent déjà.

Un ordinateur client approuve une autorité de certification lorsque le certificat d'autorité de certification est installé dans le magasin de certificats d'autorité de certification racines de confiance. Par défaut, les ordinateurs exécutant Windows ont plusieurs certificats d'autorité de certification publique installés dans leur magasin de certificats d'autorité de certification racines de confiance.

Il est recommandé de consulter les guides de conception et de déploiement pour chacune des technologies utilisées dans ce scénario de déploiement. Ces guides peuvent vous aider à déterminer si ce scénario de déploiement fournit les services et la configuration dont vous avez besoin pour le réseau de votre organisation.

Configuration requise

Voici les conditions requises pour le déploiement d'une infrastructure d'accès sans fil à l'aide du scénario décrit dans ce guide :

- Avant de déployer ce scénario, vous devez d'abord acheter des points d'accès sans fil compatibles 802.1X pour fournir une couverture sans fil aux emplacements souhaités sur votre site. La section de planification de ce guide vous aide à déterminer les fonctionnalités que vos points d'accès doivent prendre en charge.

- Active Directory Domain Services (AD DS) est installé, de même que les autres technologies réseau requises, conformément aux instructions du Guide du réseau principal Windows Server 2016.

- AD CS est déployé et les certificats de serveur sont inscrits auprès des serveurs NPS (Network Policy Server). Ces certificats sont requis lorsque vous déployez la méthode d'authentification basée sur les certificats PEAP-MS-CHAP v2 utilisée dans ce guide.

- Un membre de votre organisation connaît les normes IEEE 802.11 prises en charge par vos points d'accès sans fil et les cartes réseau sans fil installés sur les ordinateurs clients et les appareils de votre réseau. Par exemple, un membre de

votre organisation connaît les types de fréquences radio, l'authentification sans fil 802.11 (WPA2 ou WPA) et les chiffrements (AES ou TKIP).

Ce que ce guide ne contient pas

Voici quelques éléments que ce guide ne fournit pas :

Conseils complets pour la sélection des points d'accès sans fil compatibles avec 802.1X

Étant donné qu'il existe de nombreuses différences entre les marques et les modèles des points d'accès sans fil compatibles avec 802.1X, ce guide ne fournit pas d'informations détaillées sur :

- Déterminer la marque ou le modèle de point d'accès sans fil le mieux adapté à vos besoins.
- Déploiement physique des points d'accès sans fil sur votre réseau.
- Configuration avancée des points d'accès sans fil, par exemple pour les réseaux locaux virtuels (VLAN) sans fil.
- Instructions sur la configuration des attributs spécifiques aux fournisseurs des points d'accès sans fil dans le serveur NPS (Network Policy Server).

En outre, la terminologie et les noms des paramètres varient entre les marques et les modèles de points d'accès sans fil, et peuvent ne pas correspondre aux noms de paramètres génériques utilisés dans ce guide. Pour plus d'informations sur la configuration des points d'accès sans fil, vous devez consulter la documentation du produit fournie par le fabricant de vos points d'accès sans fil.

Instructions pour le déploiement de certificats du serveur NPS (Network Policy Server)

Il existe deux alternatives pour déployer des certificats NPS. Ce guide ne fournit pas d'aide complète pour vous aider à déterminer l'alternative qui répondra le mieux à vos besoins. En général, cependant, les choix auxquels vous êtes confronté sont les suivants :

- Achat de certificats auprès d'une autorité de certification publique, telle que VeriSign, qui sont déjà approuvés par les clients Windows. Cette option est généralement recommandée pour les réseaux plus petits.

- Déploiement d’une infrastructure à clé publique (PKI) sur votre réseau à l’aide d’AD CS. Cela est recommandé pour la plupart des réseaux, et les instructions pour déployer des certificats de serveur avec AD CS sont disponibles dans le guide de déploiement mentionné précédemment.

Stratégies réseau du serveur NPS (Network Policy Server) et autres paramètres NPS

À l’exception des paramètres de configuration créés lorsque vous exécutez l’Assistant **Configuration 802.1X**, comme indiqué dans ce guide, ce guide ne fournit pas d’informations détaillées pour la configuration manuelle des conditions NPS, des contraintes ou d’autres paramètres NPS.

DHCP

Ce guide de déploiement ne fournit pas d’informations sur la conception ou le déploiement de sous-réseaux DHCP pour les réseaux locaux sans fil.

Vues d’ensemble des technologies

Voici des vues d’ensemble de la technologie pour le déploiement de l’accès sans fil :

IEEE 802.1X

La norme IEEE 802.1X définit le contrôle d’accès réseau basé sur le port qui sert à fournir un accès réseau authentifié à des réseaux Ethernet. Ce contrôle d’accès réseau basé sur le port utilise les caractéristiques physiques de l’infrastructure de réseau local commutée pour authentifier des périphériques attachés à un port LAN. L'accès au port peut être refusé en cas d'échec du processus d'authentification. Bien que cette norme ait été conçue pour les réseaux Ethernet câblés, elle a été adaptée en vue d’une utilisation sur les réseaux locaux sans fils 802.11.

Points d’accès sans fil compatibles avec 802.1X

Ce scénario nécessite le déploiement d’un ou plusieurs points d’accès sans fil prenant en charge 802.1X avec le protocole RADIUS (Remote Authentication Dial-In User Service).

Quand des points d’accès compatibles avec 802.1X et RADIUS sont déployés dans une infrastructure RADIUS, avec un serveur RADIUS, tel qu’un serveur NPS (Network Policy Server), ils portent le nom de *clients RADIUS*.

Clients sans fil

Ce guide fournit des détails de configuration complets pour fournir un accès authentifié 802.1X aux utilisateurs membres du domaine qui se connectent au réseau avec des ordinateurs clients sans fil exécutant Windows 10, Windows 8.1 et Windows 8. Les ordinateurs doivent être joints au domaine pour établir correctement l'accès authentifié.

> ⓘ **Notes**
>
> Vous pouvez également utiliser des ordinateurs exécutant Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012 en tant que clients sans fil.

Prise en charge des normes IEEE 802.11

Les systèmes d'exploitation Windows et Windows Server pris en charge fournissent une prise en charge intégrée de la mise en réseau sans fil 802.11. Dans ces systèmes d'exploitation, une carte réseau sans fil 802.11 installée apparaît en tant que connexion réseau sans fil dans le Centre réseau et partage.

Bien qu'il existe une prise en charge intégrée de la mise en réseau sans fil 802.11, les composants sans fil de Windows dépendent des éléments suivants :

- Fonctionnalités de la carte réseau sans fil. La carte réseau sans fil installée doit prendre en charge les normes de sécurité sans fil LAN ou sans fil dont vous avez besoin. Par exemple, si la carte réseau sans fil ne prend pas en charge l'accès protégé Wi-Fi (WPA), vous ne pouvez pas activer ou configurer les options de sécurité WPA.

- Fonctionnalités du pilote de carte réseau sans fil. Pour vous permettre de configurer les options de réseau sans fil, le pilote de la carte réseau sans fil doit prendre en charge la création de rapports de toutes ses fonctionnalités à Windows. Vérifiez que le pilote de votre carte réseau sans fil est écrit pour les fonctionnalités de votre système d'exploitation. Vérifiez également que le pilote est la version la plus récente en consultant Microsoft Update ou le site Web du fournisseur de la carte réseau sans fil.

Le tableau suivant présente les taux de transmission et les fréquences pour les normes sans fil IEEE 802.11 courantes.

Standards	Fréquences	Débits de transmission de bits	Usage

Standards	Fréquences	Débits de transmission de bits	Usage
802.11	Plage de fréquences industrielle, scientifique et médicale (ISM) en bande S (2,4 à 2,5 GHz)	2 mégabits par seconde (Mbits/s)	Obsolète. Ce n'est pas couramment utilisé.
802.11b	ISM à bande S	11 Mbits/s	Couramment utilisé.
802.11a	ISM en bande C (5,725 à 5,875 GHz)	54 Mbits/s	Ce n'est pas couramment utilisé en raison d'une dépense et d'une plage limitées.
802.11g	ISM à bande S	54 Mbits/s	Largement utilisé. Les appareils 802.11g sont compatibles avec les appareils 802.11b.
802.11n \2,4 et 5,0 GHz	ISM en bande C et en bande S	250 Mbit/s	Les appareils basés sur la norme IEEE 802.11n pré-ratification sont devenus disponibles en août 2007. De nombreux appareils 802.11n sont compatibles avec les appareils 802.11a, b et g.
802.11ac	5 GHz	6,93 Gbit/s	802.11ac, approuvé par l'IEEE en 2014, est plus évolutif et plus rapide que 802.11n, et est déployé là où les points d'accès et les clients sans fil le prennent en charge.

Méthodes de sécurité réseau sans fil

Les **méthodes de sécurité réseau sans fil** sont un regroupement informel d'authentification sans fil (parfois appelée sécurité sans fil) et de chiffrement de sécurité sans fil. L'authentification et le chiffrement sans fil sont utilisés par paires pour empêcher les utilisateurs non autorisés d'accéder au réseau sans fil et pour protéger les transmissions sans fil.

Lors de la configuration des paramètres de sécurité sans fil dans les stratégies de réseau sans fil de stratégie de groupe, vous avez le choix entre plusieurs combinaisons. Toutefois, seules les normes d'authentification WPA2-Enterprise, WPA-Enterprise et Open avec 802.1X sont prises en charge pour les déploiements sans fil authentifiés 802.1X.

ⓘ **Notes**

Lors de la configuration des stratégies de réseau sans fil, vous devez sélectionner **WPA2-Enterprise**, **WPA-Enterprise** ou **Ouvrir avec 802.1X** afin d'accéder aux paramètres EAP requis pour les déploiements sans fil authentifiés 802.1X.

Authentification sans fil

Ce guide recommande l'utilisation des normes d'authentification sans fil suivantes pour les déploiements sans fil authentifiés 802.1X.

Accès protégé Wi-Fi – Entreprise (WPA-Enterprise) WPA est une norme provisoire développée par Wi-Fi Alliance pour se conformer au protocole de sécurité sans fil 802.11. Le protocole WPA a été développé en réponse à un certain nombre de graves défauts qui ont été découverts dans le protocole WEP (Wired Equivalent Privacy) précédent.

WPA-Enterprise offre une sécurité améliorée par rapport à WEP en :

1. Exigeant une authentification qui utilise l'infrastructure EAP 802.1X dans le cadre de l'infrastructure qui garantit l'authentification mutuelle centralisée et la gestion dynamique des clés

2. Améliorant la valeur de vérification de l'intégrité (ICV) avec un contrôle d'intégrité des messages (MIC) pour protéger l'en-tête et la charge utile

3. Implémentant un compteur d'images pour décourager les attaques par relecture

Accès protégé Wi-Fi 2 – Entreprise (WPA2-Enterprise) Comme la norme WPA-Enterprise, WPA2-Enterprise utilise l'infrastructure 802.1X et EAP. WPA2-Enterprise offre une protection des données plus forte pour plusieurs utilisateurs et de grands réseaux managés. WPA2-Enterprise est un protocole robuste conçu pour empêcher l'accès réseau non autorisé en vérifiant les utilisateurs du réseau via un serveur d'authentification.

Chiffrement de sécurité sans fil

Le chiffrement de sécurité sans fil est utilisé pour protéger les transmissions sans fil envoyées entre le client sans fil et le point d'accès sans fil. Le chiffrement de sécurité sans fil est utilisé conjointement avec la méthode d'authentification de sécurité réseau sélectionnée. Par défaut, les ordinateurs exécutant Windows 10, Windows 8.1 et Windows 8 prennent en charge deux normes de chiffrement :

1. Le protocole TKIP (**Temporal Key Integrity Protocol**) est un protocole de chiffrement plus ancien qui a été initialement conçu pour fournir un chiffrement sans fil plus sécurisé que celui fourni par le protocole WEP (Wired Equivalent Privacy) par nature faible. TKIP a été conçu par le groupe de tâches IEEE 802.11i et Wi-Fi Alliance pour remplacer WEP sans nécessiter le remplacement du matériel hérité. TKIP est une suite d'algorithmes qui encapsule la charge utile WEP et permet aux utilisateurs d'équipements Wi-Fi hérités de se mettre à niveau vers TKIP sans remplacer le matériel. Comme WEP, TKIP utilise l'algorithme de chiffrement de flux RC4 comme base. Toutefois, le nouveau protocole chiffre chaque paquet de données avec une clé de chiffrement unique, et les clés sont beaucoup plus fortes que celles de WEP. Bien que TKIP soit utile pour mettre à niveau la sécurité sur des appareils plus anciens qui ont été conçus pour utiliser uniquement WEP, il ne résout pas tous les problèmes de sécurité auxquels sont confrontés les réseaux locaux sans fil et, dans la plupart des cas, n'est pas suffisamment robuste pour protéger les transmissions de données gouvernementales ou d'entreprise sensibles.

2. **Advanced Encryption Standard** (AES) est le protocole de chiffrement préféré pour le chiffrement des données commerciales et gouvernementales. AES offre un niveau de sécurité de transmission sans fil plus élevé que TKIP ou WEP. Contrairement à TKIP et WEP, AES nécessite du matériel sans fil qui prend en charge la norme AES. AES est une norme de chiffrement à clé symétrique qui utilise trois chiffrements par blocs, AES-128, AES-192 et AES-256.

Dans Windows Server 2016, les méthodes de chiffrement sans fil AES suivantes sont disponibles pour la configuration dans les propriétés de profil sans fil lorsque vous sélectionnez une méthode d'authentification WPA2-Enterprise, ce qui est recommandé.

1. **AES-CCMP**. Le protocole CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) implémente la norme 802.11i. Il est conçu pour un chiffrement de sécurité plus élevé que celui fourni par WEP. Il utilise des clés de chiffrement AES 128 bits.
2. **AES-GCMP**. Galois Counter Mode Protocol (GCMP) est pris en charge par 802.11ac, est plus efficace qu'AES-CCMP et fournit de meilleures performances pour les clients sans fil. GCMP utilise des clés de chiffrement AES 256 bits.

> ⓘ **Important**
>
> WEP (Wired Equivalency Privacy) était la norme de sécurité sans fil d'origine utilisée pour chiffrer le trafic réseau. Vous ne devez pas déployer WEP sur votre réseau, car il existe des vulnérabilités connues dans cette forme de sécurité obsolète.

Active Directory Domain Services (AD DS)

Les services AD DS fournissent une base de données distribuée qui stocke et gère des informations sur les ressources réseau et les données spécifiques à des applications provenant d'applications utilisant un annuaire. Les administrateurs peuvent utiliser AD DS pour organiser les éléments d'un réseau, tels que les utilisateurs, les ordinateurs et les autres périphériques, en une structure hiérarchique de type contenant-contenu. La structure hiérarchique de type contenant-contenu inclut la forêt Active Directory, les domaines inclus dans la forêt et les unités d'organisation de chaque domaine. Un serveur qui exécute les services AD DS est appelé *contrôleur de domaine*.

AD DS contient les comptes d'utilisateur, les comptes d'ordinateur et les propriétés de compte requis par IEEE 802.1X et PEAP-MS-CHAP v2 pour authentifier les informations d'identification utilisateur et évaluer l'autorisation des connexions sans fil.

Utilisateurs et ordinateurs Active Directory

Utilisateurs et ordinateurs Active Directory est un composant d'AD DS qui contient des comptes représentant des entités physiques comme un ordinateur, une personne ou un groupe de sécurité. Un *groupe de sécurité* est un ensemble de comptes d'utilisateurs ou d'ordinateurs que les administrateurs peuvent gérer comme une seule unité. Les comptes d'utilisateurs et d'ordinateurs appartenant à un groupe particulier représentent les *membres du groupe*.

Gestion des stratégies de groupe

La gestion des stratégies de groupe permet de gérer la configuration et les modifications basées sur l'annuaire des paramètres utilisateur et ordinateur, notamment la sécurité et les informations utilisateur. Vous utilisez une stratégie de groupe pour définir des configurations pour des groupes d'utilisateurs et d'ordinateurs. Une stratégie de groupe vous permet de spécifier des paramètres pour les entrées de Registre, la sécurité, l'installation de logiciels, les scripts, la redirection de dossiers, les services d'installation à distance et la maintenance d'Internet Explorer. Les paramètres de stratégie de groupe que vous créez sont contenus dans un objet de stratégie de groupe (GPO). Vous pouvez associer un objet de stratégie de groupe à certains conteneurs système Active Directory sélectionnés (sites, domaines et unités d'organisation) pour appliquer les paramètres de l'objet de stratégie de groupe aux utilisateurs et ordinateurs de ces conteneurs Active Directory. Pour gérer les objets de stratégie de groupe dans une entreprise, vous pouvez utiliser la console MMC (Microsoft Management Console) Éditeur de gestion des stratégies de groupe.

Ce guide fournit des instructions détaillées sur la spécification des paramètres dans l'extension de stratégies de réseau sans fil (IEEE 802.11) de stratégie de groupe Gestion. Les stratégies de réseau sans fil (IEEE 802.11) configurent les ordinateurs clients sans fil membres du domaine avec la connectivité et les paramètres sans fil nécessaires pour l'accès sans fil authentifié 802.1X.

Certificats de serveur

Ce scénario de déploiement nécessite des certificats de serveur pour chaque serveur NPS (Network Policy Server) qui effectue l'authentification 802.1X.

Un certificat de serveur est un document numérique couramment utilisé pour l'authentification et pour sécuriser des informations sur les réseaux ouverts. Un certificat associe de manière sécurisée une clé publique à l'entité qui détient la clé privée correspondante. Les certificats sont signés numériquement par l'autorité de certification émettrice et ils peuvent être émis pour un utilisateur, un ordinateur ou un service.

Une autorité de certification est une entité responsable de l'établissement et de la garantie de l'authenticité des clés publiques qui appartiennent à des sujets (généralement des utilisateurs ou des ordinateurs) ou à d'autres autorités de certification. Parmi les activités d'une autorité de certification figurent la liaison de clés publiques à des noms uniques par le biais de certificats signés, la gestion de numéros de série de certificats et la révocation de certificats.

Les services de certificats Active Directory (AD CS) sont un rôle de serveur qui émet des certificats en qualité d'autorité de certification réseau. Une infrastructure de certificat AD CS, également appelée *infrastructure à clé publique (PKI)*, fournit des services personnalisables pour l'émission et la gestion des certificats pour l'entreprise.

EAP, PEAP et PEAP-MS-CHAP v2

Le protocole EAP (Extensible Authentication Protocol) étend le protocole PPP (Point-to-Point Protocol) en autorisant des méthodes d'authentification supplémentaires qui utilisent des informations d'identification et des échanges d'informations de longueurs arbitraires. Avec l'authentification EAP, le client d'accès réseau et l'authentificateur (par exemple un serveur NPS) doivent prendre en charge le même type EAP pour que l'authentification réussisse. Windows Server 2016 inclut une infrastructure EAP, prend en charge deux types EAP et la possibilité de transmettre des messages EAP aux serveurs NPS (Network Policy Server). En utilisant EAP, vous pouvez prendre en charge des schémas d'authentification supplémentaires, appelés *types EAP*. Les types EAP pris en charge par Windows Server 2016 sont les suivants :

- TLS (Transport Layer Security)
- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)

> ⓘ **Important**
>
> Les types EAP forts (tels que ceux basés sur des certificats) offrent une meilleure sécurité contre les attaques par force brute, les attaques par dictionnaire et les attaques par prédiction de mot de passe que les protocoles d'authentification par mot de passe (tels que CHAP ou MS-CHAP version 1).

Le protocole EAP protégé (PEAP) utilise TLS pour créer un canal chiffré entre un client PEAP d'authentification, tel qu'un ordinateur sans fil, et un authentificateur PEAP, tel qu'un serveur NPS (Network Policy Server) ou d'autres serveurs RADIUS. PEAP ne spécifie pas de méthode d'authentification, mais il fournit une sécurité supplémentaire pour d'autres protocoles d'authentification EAP (tels que EAP-MS-CHAP v2) qui peuvent fonctionner via le canal chiffré TLS fourni par PEAP. PEAP est utilisé comme méthode d'authentification pour les clients d'accès qui se connectent au réseau de votre organisation via les types suivants de serveurs d'accès réseau (NAS) :

- Points d'accès sans fil compatibles avec 802.1X
- Commutateurs d'authentification 802.1X
- Ordinateurs exécutant Windows Server 2016 et le service d'accès à distance (RAS) configurés en tant que serveurs de réseau privé virtuel (VPN), serveurs DirectAccess, ou les deux
- Ordinateurs exécutant Windows Server 2016 et services Bureau à distance

PEAP-MS-CHAP v2 est plus facile à déployer que EAP-TLS, car l'authentification utilisateur est effectuée à l'aide d'informations d'identification basées sur un mot de passe (nom d'utilisateur et mot de passe), au lieu de certificats ou de cartes à puce. Seuls les serveurs NPS (Network Policy Server) ou d'autres serveurs RADIUS doivent disposer d'un certificat. Le certificat NPS est utilisé par le serveur NPS (Network Policy Server) pendant le processus d'authentification pour prouver son identité aux clients PEAP.

Ce guide fournit des instructions pour configurer vos clients sans fil et vos serveurs NPS (Network Policy Server) afin d'utiliser PEAP-MS-CHAP v2 pour l'accès authentifié 802.1X.

Serveur de stratégie réseau

Le serveur NPS (Network Policy Server) vous permet de configurer et de gérer de manière centralisée les stratégies réseau à l'aide du serveur RADIUS (Remote Authentication Dial-In User Service) et du proxy RADIUS. Le serveur NPS (Network Policy Server) est nécessaire pour déployer un accès sans fil 802.1X.

Lorsque vous configurez vos points d'accès sans fil 802.1X en tant que clients RADIUS dans le serveur NPS (Network Policy Server), NPS traite les demandes de connexion envoyées par les points d'accès. Pendant le traitement des demandes de connexion, le serveur NPS (Network Policy Server) effectue l'authentification et l'autorisation. L'authentification détermine si le client a présenté des informations d'identification valides. Si le serveur NPS (Network Policy Server) authentifie correctement le client demandeur, NPS détermine si le client est autorisé à établir la connexion demandée et autorise ou refuse la connexion. Ceci est expliqué plus en détail comme suit :

Authentification

L'authentification mutuelle PEAP-MS-CHAP v2 réussie comprend deux parties principales :

1. Le client authentifie le serveur NPS (Network Policy Server). Au cours de cette phase d'authentification mutuelle, le serveur NPS (Network Policy Server) envoie son certificat serveur à l'ordinateur client afin que le client puisse vérifier l'identité du serveur NPS avec le certificat. Pour authentifier correctement le serveur NPS (Network Policy Server), l'ordinateur client doit approuver l'autorité de certification qui a émis le certificat NPS. Le client approuve cette autorité de certification lorsque le certificat de l'autorité de certification est présent dans le magasin de certificats d'autorité de certification racines de confiance sur l'ordinateur client.

   Si vous déployez votre propre autorité de certification privée, le certificat d'autorité de certification est automatiquement installé dans le magasin de certificats d'autorité de certification racines de confiance pour l'utilisateur actuel et pour l'ordinateur local lorsque la stratégie de groupe est actualisée sur l'ordinateur client membre du domaine. Si vous décidez de déployer des certificats de serveur à partir d'une autorité de certification publique, assurez-vous que le certificat d'autorité de certification publique se trouve déjà dans le magasin de certificats d'autorité de certification racines de confiance.

2. Le serveur NPS (Network Policy Server) authentifie l'utilisateur. Une fois que le client a correctement authentifié le serveur NPS (Network Policy Server), il envoie les informations d'identification basées sur un mot de passe de l'utilisateur au serveur NPS, qui vérifie les informations d'identification de l'utilisateur par rapport

à la base de données des comptes d'utilisateur dans Active Directory Domain Services (AD DS).

Si les informations d'identification sont valides et que l'authentification réussit, le serveur NPS (Network Policy Server) commence la phase d'autorisation du traitement de la demande de connexion. Si les informations d'identification ne sont pas valides et que l'authentification échoue, le serveur NPS (Network Policy Server) envoie un message de refus d'accès et la demande de connexion est refusée.

Autorisation

Le serveur exécutant le serveur NPS (Network Policy Server) effectue l'autorisation comme suit :

1. NPS recherche les restrictions dans les propriétés de connexion du compte d'utilisateur ou d'ordinateur dans AD DS. Chaque compte d'utilisateur et d'ordinateur dans Utilisateurs et ordinateurs Active Directory inclut plusieurs propriétés, y compris celles qui se trouvent sous l'onglet **Rendez-vous**. Sous cet onglet, dans **Autorisation d'accès réseau**, si la valeur est **Autoriser l'accès**, l'utilisateur ou l'ordinateur est autorisé à se connecter au réseau. Si la valeur est **Refuser l'accès**, l'utilisateur ou l'ordinateur n'est pas autorisé à se connecter au réseau. Si la valeur est **Contrôler l'accès via une stratégie réseau NPS**, le serveur NPS (Network Policy Server) évalue les stratégies réseau configurées pour déterminer si l'utilisateur ou l'ordinateur est autorisé à se connecter au réseau.

2. Le serveur NPS (Network Policy Server) traite ensuite ses stratégies réseau pour trouver une stratégie qui correspond à la demande de connexion. Si une stratégie de correspondance est trouvée, le serveur NPS (Network Policy Server) accorde ou refuse la connexion en fonction de la configuration de cette stratégie.

Si l'authentification et l'autorisation réussissent, et si la stratégie réseau correspondante accorde l'accès, le serveur NPS (Network Policy Server) accorde l'accès au réseau, et l'utilisateur et l'ordinateur peuvent se connecter aux ressources réseau pour lesquelles ils disposent d'autorisations.

Notes

Pour déployer l'accès sans fil, vous devez configurer des stratégies NPS. Ce guide fournit des instructions pour utiliser l'**Assistant Configurer 802.1X** dans le serveur NPS (Network Policy Server) afin de créer des stratégies NPS pour l'accès sans fil authentifié 802.1X.

Profils d’amorçage

Dans les réseaux sans fil authentifiés par 802.1X, les clients sans fil doivent fournir des informations d’identification de sécurité authentifiées par un serveur RADIUS pour se connecter au réseau. Pour Protected EAP [PEAP]-Microsoft Challenge Handshake Authentication Protocol version 2 [MS-CHAP v2], les informations d’identification de sécurité sont un nom d’utilisateur et un mot de passe. Pour EAP-Transport Layer Security [TLS] ou PEAP-TLS, les informations d’identification de sécurité sont des certificats, tels que des certificats d’utilisateur et d’ordinateur client ou des cartes à puce.

Lors de la connexion à un réseau configuré pour effectuer l’authentification PEAP-MS-CHAP v2, PEAP-TLS ou EAP-TLS, par défaut, les clients sans fil Windows doivent également valider un certificat d’ordinateur envoyé par le serveur RADIUS. Le certificat d’ordinateur envoyé par le serveur RADIUS pour chaque session d’authentification est communément appelé certificat de serveur.

Comme mentionné précédemment, vous pouvez émettre à vos serveurs RADIUS leur certificat de serveur de deux manières : à partir d’une autorité de certification commerciale (telle que VeriSign, Inc.), ou à partir d’une autorité de certification privée que vous déployez sur votre réseau. Si le serveur RADIUS envoie un certificat d’ordinateur émis par une autorité de certification commerciale qui a déjà installé un certificat racine dans le magasin de certificats d’autorité de certification racines de confiance du client, le client sans fil peut valider le certificat d’ordinateur du serveur RADIUS, que le client sans fil ait ou non rejoint le domaine Active Directory. Dans ce cas, le client sans fil peut se connecter au réseau sans fil, puis vous pouvez joindre l’ordinateur au domaine.

> ⓘ **Notes**
>
> Le comportement exigeant que le client valide le certificat de serveur peut être désactivé, mais la désactivation de la validation du certificat de serveur n’est pas recommandée dans les environnements de production.

Les profils d’amorçage sans fil sont des profils temporaires configurés de manière à permettre aux utilisateurs clients sans fil de se connecter au réseau sans fil authentifié 802.1X avant que l’ordinateur soit joint au domaine et/ou avant que l’utilisateur ne se soit connecté au domaine à l’aide d’un ordinateur sans fil donné pour la première fois. Cette section récapitule le problème rencontré lors de la tentative de jointure d’un ordinateur sans fil au domaine, ou lorsqu’un utilisateur utilise un ordinateur sans fil joint à un domaine pour la première fois pour se connecter au domaine.

Pour les déploiements dans lesquels l'utilisateur ou l'administrateur informatique ne peut pas connecter physiquement un ordinateur au réseau Ethernet câblé pour joindre l'ordinateur au domaine, et où l'ordinateur n'a pas le certificat d'autorité de certification racine nécessaire installé dans son magasin de certificats d'**autorité de certification racines de confiance**, vous pouvez configurer des clients sans fil avec un profil de connexion sans fil temporaire, appelé *profil d'amorçage*, pour se connecter au réseau sans fil.

Un *profil d'amorçage* supprime l'obligation de valider le certificat d'ordinateur du serveur RADIUS. Cette configuration temporaire permet à l'utilisateur sans fil de joindre l'ordinateur au domaine, auquel cas les stratégies de réseau sans fil (IEEE 802.11) sont appliquées et le certificat d'autorité de certification racine approprié est automatiquement installé sur l'ordinateur.

Lorsque la stratégie de groupe est appliquée, un ou plusieurs profils de connexion sans fil qui appliquent l'exigence d'authentification mutuelle sont appliqués sur l'ordinateur. Le profil d'amorçage n'est plus requis et est supprimé. Après avoir joint l'ordinateur au domaine et redémarré l'ordinateur, l'utilisateur peut utiliser une connexion sans fil pour se connecter au domaine.

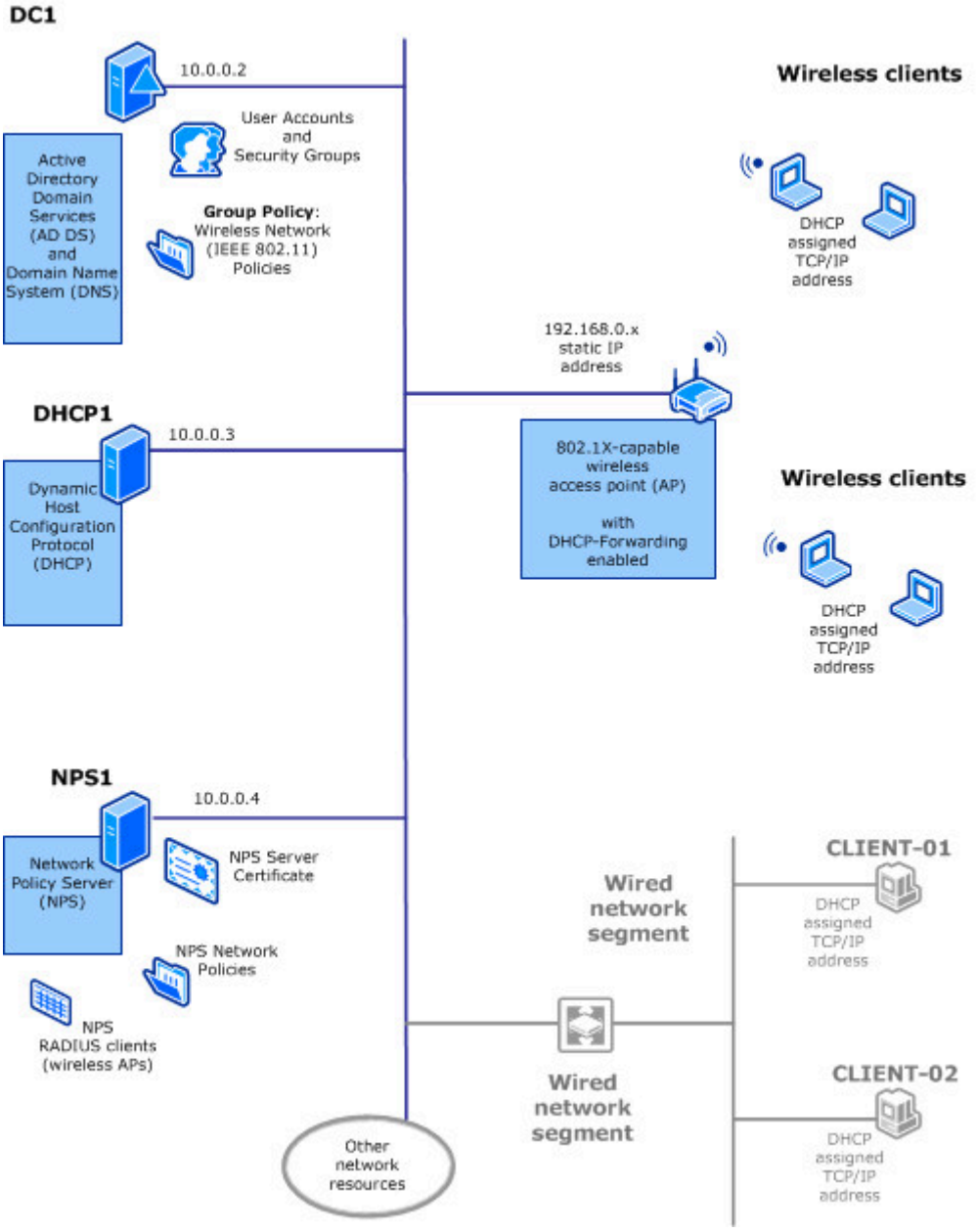
Pour obtenir une vue d'ensemble du processus de déploiement d'accès sans fil à l'aide de ces technologies, consultez Vue d'ensemble du déploiement de l'accès sans fil.

Vue d'ensemble du déploiement de l'accès sans fil

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

L'illustration suivante montre les composants requis pour déployer l'accès sans fil authentifié 802.1X avec PEAP-MS-CHAP v2.



Composants de déploiement d'accès sans fil

L'infrastructure suivante est requise pour ce déploiement d'accès sans fil :

Points d’accès sans fil compatibles 802.1X

Une fois que les services d’infrastructure réseau requis prenant en charge votre réseau local sans fil sont en place, vous pouvez commencer le processus de conception pour l’emplacement des points d’accès sans fil. Le processus de conception de déploiement des points d’accès sans fil implique les étapes suivantes :

- Identifier les zones de couverture pour les utilisateurs sans fil. Tout en identifiant les zones de couverture, veillez à déterminer si vous souhaitez fournir un service sans fil à l’extérieur du bâtiment et, le cas échéant, à déterminer précisément où se trouvent ces zones externes.
- Déterminer le nombre d’adresses IP sans fil à déployer pour garantir une couverture adéquate.
- Déterminer où placer des adresses IP sans fil.
- Sélectionner les fréquences de canal pour les points d’accès sans fil.

Services de domaine Active Directory

Les éléments suivants d’AD DS sont requis pour le déploiement d’accès sans fil.

Utilisateurs et ordinateurs

Utilisez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory pour créer et gérer des comptes d’utilisateur, et pour créer un groupe de sécurité sans fil qui inclut chaque membre de domaine auquel vous souhaitez accorder l’accès sans fil.

Stratégie de réseau sans fil (IEEE 802.11)

Vous pouvez utiliser l’extension de stratégies de réseau sans fil (IEEE 802.11) de stratégie de groupe Gestion pour configurer les stratégies appliquées aux ordinateurs sans fil lorsqu’ils tentent d’accéder au réseau.

Dans stratégie de groupe Éditeur de gestion, lorsque vous cliquez avec le bouton droit sur **Stratégies de réseau sans fil (IEEE 802.11),** vous disposez des deux options suivantes pour le type de stratégie sans fil que vous créez.

- **Créer une stratégie de réseau sans fil pour Windows Vista et versions ultérieures**
- **Créer une stratégie Windows XP**

> **Conseil**
>
> Lors de la configuration d'une nouvelle stratégie de réseau sans fil, vous avez la possibilité de modifier le nom et la description de la stratégie. Si vous modifiez le nom de la stratégie, la modification est reflétée dans le volet **Détails** de l'Éditeur de gestion des stratégies de groupe et dans la barre de titre de la boîte de dialogue stratégie réseau sans fil. Quelle que soit la façon dont vous renommez vos stratégies, la nouvelle stratégie sans fil XP est toujours répertoriée dans l'Éditeur de gestion des stratégies de groupe avec le **type** affichant **XP**. D'autres stratégies sont répertoriées avec le **type** montrant **Vista et versions ultérieures**.

La stratégie de réseau sans fil pour Windows Vista et versions ultérieures vous permet de configurer, hiérarchiser et gérer plusieurs profils sans fil. Un profil sans fil est un ensemble de paramètres de connectivité et de sécurité utilisés pour se connecter à un réseau sans fil spécifique. Lorsque la stratégie de groupe est mise à jour sur vos ordinateurs clients sans fil, les profils que vous créez dans la stratégie de réseau sans fil sont automatiquement ajoutés à la configuration sur vos ordinateurs clients sans fil auxquels la stratégie de réseau sans fil s'applique.

Autorisation des connexions à plusieurs réseaux sans fil

Si vous avez des clients sans fil qui sont déplacés entre des emplacements physiques de votre organisation, par exemple entre un bureau principal et une filiale, vous souhaiterez peut-être que les ordinateurs se connectent à plusieurs réseaux sans fil. Dans ce cas, vous pouvez configurer un profil sans fil qui contient les paramètres de connectivité et de sécurité spécifiques pour chaque réseau.

Par exemple, supposons que votre entreprise dispose d'un réseau sans fil pour le siège social principal, avec un identificateur de jeu de services (SSID) WlanCorp.

Votre filiale dispose également d'un réseau sans fil auquel vous souhaitez également vous connecter. La filiale a le SSID configuré en tant que WlanBranch.

Dans ce scénario, vous pouvez configurer un profil pour chaque réseau, et les ordinateurs ou autres appareils utilisés au bureau d'entreprise et à la filiale peuvent se connecter à l'un des réseaux sans fil lorsqu'ils sont physiquement à portée de la zone de couverture d'un réseau.

Réseaux sans fil en mode mixte

Vous pouvez également supposer que votre réseau dispose d'un mélange d'ordinateurs et d'appareils sans fil qui prennent en charge différentes normes de sécurité. Certains ordinateurs

plus anciens ont peut-être des adaptateurs sans fil qui ne peuvent utiliser que WPA-Enterprise, tandis que les appareils plus récents peuvent utiliser la norme WPA2-Enterprise plus forte.

Vous pouvez créer deux profils différents qui utilisent le même SSID et des paramètres de connectivité et de sécurité presque identiques.

Dans un profil, vous pouvez définir l'authentification sans fil sur WPA2-Enterprise avec AES, et dans l'autre profil, vous pouvez spécifier WPA-Enterprise avec TKIP.

Il s'agit d'un déploiement en mode mixte qui permet aux ordinateurs de différents types et fonctionnalités sans fil de partager le même réseau sans fil.

Serveur NPS (Network Policy Server)

NPS vous permet de créer et d'appliquer des stratégies d'accès réseau pour l'authentification et l'autorisation des demandes de connexion.

Lorsque vous utilisez NPS en tant que serveur RADIUS, vous devez configurer les serveurs d'accès réseau, tels que les point d'accès sans fil, en tant que clients RADIUS dans NPS. Vous configurez également les stratégies réseau que NPS utilise pour authentifier les clients d'accès et autoriser leurs demandes de connexion.

Ordinateurs clients sans fil

Pour les besoins de ce guide, les ordinateurs clients sans fil sont des ordinateurs et d'autres appareils équipés de cartes réseau sans fil IEEE 802.11 et qui exécutent Windows client ou les systèmes d'exploitation Windows Server.

Ordinateurs serveurs en tant que clients sans fil

Par défaut, la fonctionnalité sans fil 802.11 est désactivée sur les ordinateurs qui exécutent Windows Server.

Pour activer la connectivité sans fil sur les ordinateurs exécutant des systèmes d'exploitation serveur, vous devez installer et activer la fonctionnalité de service LAN sans fil (WLAN) à l'aide de Windows PowerShell ou de l'Assistant Ajout de rôles et de fonctionnalités dans Gestionnaire de serveur.

Lorsque vous installez la fonctionnalité **service LAN sans fil**, le nouveau service **WLAN AutoConfig** est installé dans **Services**. Une fois l'installation terminée, vous devez redémarrer le serveur.

Une fois le serveur redémarré, vous pouvez accéder à la configuration automatique DU RÉSEAU LOCAL lorsque vous cliquez sur **Démarrer**, **Outils d'administration Windows** et **Services**.

Une fois l'installation et le redémarrage du serveur redémarrés, le service de configuration automatique DU RÉSEAU LOCAL est dans un état arrêté avec un type de démarrage **automatique**. Pour démarrer le service, double-cliquez sur **CONFIGURATION automatique DU RÉSEAU LOCAL.** Sous l'onglet **Général** , cliquez sur **Démarrer**, puis sur **OK**.

Le service WLAN AutoConfig énumère les cartes sans fil et gère à la fois les connexions sans fil et les profils sans fil qui contiennent les paramètres requis pour configurer le serveur pour qu'il se connecte à un réseau sans fil.

Pour obtenir une vue d'ensemble du déploiement de l'accès sans fil, consultez Processus de déploiement de l'accès sans fil.

Processus de déploiement de l'accès sans fil

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Le processus que vous utilisez pour déployer l'accès sans fil intervient au cours des phases suivantes :

Phase 1 - Déploiement des points d'accès

Planifiez, déployez et configurez vos points d'accès pour la connectivité des clients sans fil ainsi que pour NPS. Selon vos préférences et les dépendances réseau, vous pouvez préconfigurer les paramètres de vos points d'accès sans fil avant de les installer sur le réseau, ou vous pouvez les configurer à distance une fois l'installation effectuée.

Phase 2 - Configuration du groupe AD DS

Dans AD DS, vous devez créer un ou plusieurs groupes de sécurité d'utilisateurs sans fil.

Identifiez ensuite les utilisateurs autorisés à accéder sans fil au réseau.

Enfin, ajoutez les utilisateurs aux groupes de sécurité d'utilisateurs sans fil appropriés que vous avez créés.

> ⓘ **Notes**
>
> Par défaut, le paramètre **Autorisation d'accès réseau** dans les propriétés d'appel entrant du compte d'utilisateur est configuré avec le paramètre **Contrôler l'accès via une stratégie réseau NPS**. À moins que vous n'ayez des raisons spécifiques de changer ce paramètre, il est recommandé de conserver la valeur par défaut. Cela vous permet de contrôler l'accès au réseau via les stratégies réseau que vous configurez dans NPS.

Phase 3 - Configuration de la stratégie de groupe

Configurez l'extension Stratégies de réseau sans fil (IEEE 802.11) de la stratégie de groupe en utilisant le composant MMC (Microsoft Management Console) Éditeur de gestion des stratégies de groupe.

Pour configurer les ordinateurs membres d'un domaine à l'aide des paramètres des stratégies de réseau sans fil, vous devez appliquer une stratégie de groupe. Quand un ordinateur est joint au domaine pour la première fois, la stratégie de groupe est automatiquement appliquée. Si des changements sont apportés à la stratégie de groupe, les nouveaux paramètres sont automatiquement appliqués :

- Par la stratégie de groupe à des intervalles prédéfinis
- Si un utilisateur de domaine se déconnecte, puis se reconnecte au réseau
- Via le redémarrage de l'ordinateur client et la connexion au domaine

Vous pouvez également forcer l'actualisation de la stratégie de groupe lors de la connexion à un ordinateur en exécutant la commande **gpupdate** à l'invite de commandes.

Phase 4 - Configuration de NPS

Utilisez un Assistant Configuration dans NPS pour ajouter des points d'accès sans fil en tant que clients RADIUS, et créer les stratégies réseau utilisées par NPS durant le traitement des demandes de connexion.

Quand vous utilisez l'Assistant pour créer les stratégies réseau, spécifiez PEAP en tant que type EAP ainsi que le groupe de sécurité d'utilisateurs sans fil créé au cours de la deuxième phase.

Phase 5 - Déployer les clients sans fil

Utilisez des ordinateurs clients pour vous connecter au réseau.

Pour les ordinateurs membres du domaine qui peuvent se connecter au réseau local filaire, les paramètres de configuration sans fil nécessaires sont automatiquement appliqués au moment de l'actualisation de la stratégie de groupe.

Si vous avez activé le paramètre dans Stratégies de réseau sans fil (IEEE 802.11) pour déclencher une connexion automatique quand l'ordinateur se trouve dans la plage de diffusion du réseau sans fil, vos ordinateurs sans fil joints à un domaine tentent automatiquement de se connecter au réseau local sans fil.

Pour se connecter au réseau sans fil, les utilisateurs doivent simplement fournir leur nom d'utilisateur de domaine et leurs informations d'identification par mot de passe quand Windows les y invite.

Pour planifier votre déploiement de l'accès sans fil, consultez Planification du déploiement de l'accès sans fil.

Planification du déploiement de l’accès sans fil

Article • 09/03/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Avant de déployer l’accès sans fil, vous devez planifier les éléments suivants :

- Installation de points d’accès sans fil (AP) sur votre réseau
- Configuration de client d'accès sans fil

Les sections suivantes fournissent des détails sur ces étapes de planification.

Planification des installations d’AP sans fil

Lorsque vous concevez votre solution d’accès réseau sans fil, vous devez effectuer les opérations suivantes :

1. Déterminez les normes que vos points d’accès sans fil doivent prendre en charge
2. Déterminer les zones de couverture où vous souhaitez fournir un service sans fil
3. Déterminer où vous souhaitez localiser les points d’accès sans fil

En outre, vous devez planifier un schéma d’adresses IP pour les clients sans fil et d’AP sans fil. Pour plus d’informations, consultez **la section Planifier la configuration des AP sans fil dans NPS** ci-dessous.

Vérifier la prise en charge des points d’accès sans fil pour les normes

Pour des raisons de cohérence et de facilité de déploiement et de gestion des AP, il est recommandé de déployer des points d’accès sans fil de la même marque et du même modèle.

Les points d’accès sans fil que vous déployez doivent prendre en charge les éléments suivants :

- **IEEE 802.1X**
- **Authentification RADIUS**

- **Authentification et chiffrement sans fil.** Répertorié dans l'ordre de la plupart des à moins préférés :

    1. WPA2-Enterprise avec AES
    2. WPA2-Enterprise avec TKIP
    3. WPA2-Enterprise avec AES
    4. WPA2-Enterprise avec TKIP

> ⓘ **Notes**
>
> Pour déployer WPA2, vous devez utiliser des cartes réseau sans fil et des points d'accès sans fil qui prennent également en charge WPA2. Sinon, utilisez WPA-Enterprise.

En outre, pour renforcer la sécurité du réseau, les points d'accès sans fil doivent prendre en charge les options de sécurité suivantes :

- **Filtrage DHCP.** Le point d'accès sans fil doit filtrer sur les ports IP pour empêcher la transmission de messages de diffusion DHCP dans les cas où le client sans fil est configuré en tant que serveur DHCP. Le point d'accès sans fil doit empêcher le client d'envoyer des paquets IP du port UDP 68 au réseau.
- **Filtrage DNS.** Le point d'accès sans fil doit filtrer sur les ports IP pour empêcher un client de fonctionner en tant que serveur DNS. L'AP sans fil doit empêcher le client d'envoyer des paquets IP à partir du port TCP ou UDP 53 au réseau.
- **Isolation du client** Si votre point d'accès sans fil fournit des fonctionnalités d'isolation du client, vous devez activer la fonctionnalité pour empêcher d'éventuelles attaques d'usurpation d'identité du protocole de résolution d'adresses (ARP).

Identifier les zones de couverture pour les utilisateurs sans fil

Utilisez des dessins architecturaux de chaque étage pour chaque bâtiment pour identifier les zones où vous souhaitez fournir une couverture sans fil. Par exemple, identifiez les bureaux, les salles de conférence, les halls d'entrée, les cafétérias ou les cours appropriés.

Sur les dessins, indiquez tous les appareils qui interfèrent avec les signaux sans fil, tels que l'équipement médical, les caméras vidéo sans fil, les téléphones sans fil qui fonctionnent dans la gamme 2,4 à 2,5 GHz Industrial, Scientific and Medical (ISM) et les appareils compatibles Bluetooth.

Sur le dessin, marquer les aspects du bâtiment susceptibles d'interférer avec les signaux sans fil; les objets métalliques utilisés dans la construction d'un bâtiment peuvent affecter le signal sans fil. Par exemple, les objets courants suivants peuvent interférer avec la propagation du signal : ascenseurs, conduits de chauffage et de climatisation, et poutres de support en béton.

Pour plus d'informations sur les sources susceptibles d'entraîner une atténuation de la fréquence radio AP sans fil, consultez le fabricant de votre AP. La plupart des points d'accès fournissent des logiciels de test que vous pouvez utiliser pour vérifier la force du signal, le taux d'erreur et le débit de données.

Déterminer où installer les points d'accès sans fil

Sur les dessins architecturaux, localisez vos points d'accès sans fil suffisamment proches les uns des autres pour fournir une couverture sans fil suffisante, mais suffisamment éloignés pour qu'ils n'interfèrent pas entre eux.

La distance nécessaire entre les points d'accès dépend du type d'antenne AP et AP, des aspects du bâtiment qui bloquent les signaux sans fil et d'autres sources d'interférence. Vous pouvez marquer les emplacements d'AP sans fil afin que chaque point d'accès sans fil ne soit pas situé à plus de 300 pieds d'un point d'accès sans fil adjacent. Consultez la documentation du fabricant de l'AP sans fil pour connaître les spécifications d'AP et les instructions relatives à l'emplacement.

Installez temporairement des points d'accès sans fil aux emplacements spécifiés sur vos dessins architecturaux. Ensuite, à l'aide d'un ordinateur portable équipé d'un adaptateur sans fil 802.11 et du logiciel d'enquête de site qui est généralement fourni avec des adaptateurs sans fil, déterminez la puissance du signal dans chaque zone de couverture.

Dans les zones de couverture où la puissance du signal est faible, positionnez le point d'accès pour améliorer la puissance du signal pour la zone de couverture, installez des points d'accès sans fil supplémentaires pour fournir la couverture nécessaire, déplacez ou supprimez les sources d'interférence de signal.

Mettez à jour vos dessins architecturaux pour indiquer l'emplacement final de toutes les points d'accès sans fil. Disposer d'une carte de placement d'AP précise vous aidera ultérieurement lors des opérations de résolution des problèmes ou lorsque vous souhaitez mettre à niveau ou remplacer des points d'accès.

Planifier la configuration de l'AP sans fil et du client RADIUS NPS

Vous pouvez utiliser NPS pour configurer des points d'accès sans fil individuellement ou en groupes.

Si vous déployez un réseau sans fil volumineux qui comprend de nombreuses points d'accès, il est beaucoup plus facile de configurer des points d'accès dans des groupes. Pour ajouter les points d'accès en tant que groupes de clients RADIUS dans NPS, vous devez configurer les points d'accès avec ces propriétés.

- Les points d'accès sans fil sont configurés avec des adresses IP de la même plage d'adresses IP.
- Les points d'accès sans fil sont tous configurés avec le même secret partagé.

Planifier l'utilisation de la reconnexion rapide PEAP

Dans une infrastructure 802.1X, les points d'accès sans fil sont configurés en tant que clients RADIUS pour les serveurs RADIUS. Lorsque la connexion rapide PEAP est déployée, un client sans fil qui se déplace entre deux points d'accès ou plus n'est pas obligatoirement authentifié à chaque nouvelle association.

La reconnexion rapide PEAP réduit le temps de réponse pour l'authentification entre le client et l'authentificateur, car la demande d'authentification est transférée à partir du nouveau point d'accès au NPS qui a initialement effectué l'authentification et l'autorisation pour la demande de connexion client.

Étant donné que le client PEAP et NPS utilisent tous deux des propriétés de connexion TLS (Transport Layer Security) précédemment mises en cache (dont la collection est nommée handle TLS), le NPS peut rapidement déterminer que le client est autorisé à se reconnecter.

> **ⓘ Important**
>
> Pour que la connexion rapide fonctionne correctement, les points d'accès doivent être configurés en tant que clients RADIUS du même NPS.

Si le serveur NPS d'origine devient indisponible ou si le client se déplace vers un point d'accès configuré en tant que client RADIUS vers un autre serveur RADIUS, l'authentification complète doit se produire entre le client et le nouvel authentificateur.

Configuration de l'AP sans fil

La liste suivante récapitule les éléments couramment configurés sur les points d'accès sans fil compatibles 802.1X :

> **Notes**
>
> Les noms d'éléments peuvent varier selon la marque et le modèle et peuvent être différents de ceux de la liste suivante. Pour plus d'informations sur la configuration, consultez la documentation de votre AP sans fil.

- **Identificateur du jeu de services (SSID).** Il s'agit du nom du réseau sans fil (par exemple, ExampleWlan) et du nom qui est publié pour les clients sans fil. Pour réduire la confusion, le SSID que vous choisissez de publier ne doit pas correspondre au SSID diffusé par les réseaux sans fil qui se trouvent dans la plage de réception de votre réseau sans fil.

  Dans les cas où plusieurs adresses APS sans fil sont déployées dans le cadre du même réseau sans fil, configurez chaque AP sans fil avec le même SSID. Dans les cas où plusieurs adresses APS sans fil sont déployées dans le cadre du même réseau sans fil, configurez chaque AP sans fil avec le même SSID.

  Dans les cas où vous avez besoin de déployer différents réseaux sans fil pour répondre à des besoins métier spécifiques, les API sans fil sur un réseau doivent diffuser un SSID différent de celui de vos autres réseaux. Par exemple, si vous avez besoin d'un réseau sans fil distinct pour vos employés et invités, vous pouvez configurer vos points d'accès sans fil pour le réseau d'entreprise avec le SSID défini pour diffuser **ExampleWLAN**. Pour votre réseau invité, vous pouvez ensuite définir le SSID de chaque point d'accès sans fil pour diffuser **GuestWLAN**. De cette façon, vos employés et invités peuvent se connecter au réseau prévu sans confusion inutile.

  > **Conseil**
  >
  > Certains points d'accès sans fil ont la possibilité de diffuser plusieurs SSID pour prendre en charge les déploiements multi-réseau. Les POINTS d'accès sans fil qui peuvent diffuser plusieurs SSID peuvent réduire les coûts de déploiement et de maintenance opérationnelle.

- **Authentification et chiffrement sans fil**.

L'authentification sans fil est l'authentification de sécurité utilisée lorsque le client sans fil est associé à un point d'accès sans fil.

Le chiffrement sans fil est le chiffrement de sécurité utilisé avec l'authentification sans fil pour protéger les communications envoyées entre le point d'accès sans fil et le client sans fil.

- **Adresse IP de l'AP sans fil (statique).** Sur chaque point d'accès sans fil, configurez une adresse IP statique unique. Si le sous-réseau est pris en charge par un serveur DHCP, assurez-vous que toutes les adresses IP AP se trouvent dans une plage d'exclusion DHCP afin que le serveur DHCP n'essaie pas d'émettre la même adresse IP sur un autre ordinateur ou appareil. Les plages d'exclusion sont documentées dans la procédure « Pour créer et activer une nouvelle étendue DHCP » dans le Guide du réseau principal. Si vous envisagez de configurer des points d'accès en tant que clients RADIUS par groupe dans NPS, chaque point d'accès du groupe doit avoir une adresse IP de la même plage d'adresses IP.

- **Nom DNS**. Certaines adresses IP sans fil peuvent être configurées avec un nom DNS. Configurez chaque point d'accès sans fil avec un nom unique. Par exemple, si vous avez déployé des points d'accès sans fil dans un bâtiment à plusieurs étages, vous pouvez nommer les trois premières points d'accès sans fil déployés au troisième étage AP3-01, AP3-02 et AP3-03.

- **Masque de sous-réseau AP sans fil**. Configurez le masque pour désigner la partie de l'adresse IP qui correspond à l'ID réseau et la partie de l'adresse IP qui correspond à l'hôte.

- **Service DHCP AP**. Si votre point d'accès sans fil dispose d'un service DHCP intégré, désactivez-le.

- **Secret partagé RADIUS**. Utilisez un secret partagé RADIUS unique pour chaque AP sans fil, sauf si vous envisagez de configurer des clients RADIUS NPS dans des groupes. Dans ce cas, vous devez configurer tous les points d'accès du groupe avec le même secret partagé. Les secrets partagés doivent être une séquence aléatoire d'au moins 22 caractères, avec des lettres majuscules et minuscules, des chiffres et des signes de ponctuation. Pour garantir l'aléatoire, vous pouvez utiliser un programme de génération de caractères aléatoires pour créer vos secrets partagés. Il est recommandé d'enregistrer le secret partagé pour chaque point d'accès sans fil et de le stocker dans un emplacement sécurisé, tel qu'un coffre-fort du bureau. Quand vous configurez des clients RADIUS dans la console NPS, vous créez une version virtuelle de chaque AP. Le secret partagé que vous configurez sur chaque AP virtuel dans NPS doit correspondre au secret partagé sur l'AP physique réelle.

- **Adresse IP du serveur RADIUS**. Tapez l'adresse IP du serveur NPS que vous souhaitez utiliser pour authentifier et autoriser les demandes de connexion à ce point d'accès.

- **Port(s) UDP**. Par défaut, NPS utilise les ports UDP 1812 et 1645 pour les messages d'authentification RADIUS et les ports UDP 1813 et 1646 pour les messages de comptabilité RADIUS. Il est recommandé de ne pas modifier les paramètres de ports UDP RADIUS par défaut.

- **VSAs**. Certaines adresses IP sans fil nécessitent des attributs spécifiques au fournisseur (VSA) pour fournir des fonctionnalités d'AP sans fil complètes.

- **Filtrage DHCP**. Configurez des points d'accès sans fil pour empêcher les clients sans fil d'envoyer des paquets IP du port UDP 68 au réseau. Consultez la documentation de votre POINT d'accès sans fil pour configurer le filtrage DHCP.

- **Filtrage DNS**. Configurez les points d'accès sans fil pour empêcher les clients sans fil d'envoyer des paquets IP à partir du port TCP ou UDP 53 au réseau. Consultez la documentation de votre point d'accès sans fil pour configurer le filtrage DNS.

Planification de la configuration et de l'accès des clients sans fil

Lorsque vous planifiez le déploiement de l'accès sans fil authentifié 802.1X, vous devez prendre en compte plusieurs facteurs spécifiques au client :

- **Planification de la prise en charge de plusieurs normes**.

  Déterminez si vos ordinateurs sans fil utilisent tous la même version de Windows ou s'ils sont un mélange d'ordinateurs exécutant des systèmes d'exploitation différents. Si elles sont différentes, veillez à comprendre les différences de normes prises en charge par les systèmes d'exploitation.

  Déterminez si toutes les cartes réseau sans fil de tous les ordinateurs clients sans fil prennent en charge les mêmes normes sans fil, ou si vous devez prendre en charge différentes normes. Par exemple, déterminez si certains pilotes matériels de carte réseau prennent en charge WPA2-Enterprise et AES, tandis que d'autres prennent uniquement en charge WPA-Enterprise et TKIP.

- **Planification du mode d'authentification du client**. Les modes d'authentification définissent la façon dont les clients Windows traitent les informations d'identification de domaine. Vous pouvez choisir parmi les trois modes d'authentification réseau suivants dans les stratégies de réseau sans fil.

1. **Nouvelle authentification de l'utilisateur** Ce mode spécifie que l’authentification est toujours effectuée à l’aide d’informations d’identification de sécurité basées sur l’état actuel de l’ordinateur. Lorsqu’aucun utilisateur n’est connecté à l’ordinateur, l’authentification est effectuée en utilisant les informations d’identification de l’ordinateur. Si un utilisateur est connecté sur l'ordinateur, l'authentification est toujours effectuée avec les informations d'identification de l'utilisateur.

2. **Ordinateur uniquement** Le mode Ordinateur uniquement spécifie que l’authentification est toujours effectuée en utilisant uniquement les informations d’identification de l’ordinateur.

3. **Authentification utilisateur**. Le mode d’authentification utilisateur spécifie que l’authentification est effectuée uniquement lorsque l’utilisateur est connecté à l’ordinateur. Lorsqu’aucun utilisateur n’est connecté à l’ordinateur, les tentatives d’authentification ne sont pas effectuées.

- **Planification des restrictions sans fil**. Déterminez si vous souhaitez fournir à tous vos utilisateurs sans fil le même niveau d’accès à votre réseau sans fil, ou si vous souhaitez restreindre l’accès à certains de vos utilisateurs sans fil. Vous pouvez appliquer des restrictions dans NPS à des groupes spécifiques d’utilisateurs sans fil. Par exemple, vous pouvez définir des jours et des heures spécifiques pendant lesquels certains groupes sont autorisés à accéder au réseau sans fil.

- **Méthodes de planification pour l’ajout de nouveaux ordinateurs sans fil**. Pour les ordinateurs sans fil qui sont joints à votre domaine avant de déployer votre réseau sans fil, si l’ordinateur est connecté à un segment du réseau câblé qui n’est pas protégé par la norme 802.1X, les paramètres de configuration sans fil sont automatiquement appliqués après avoir configuré les stratégies de réseau sans fil (IEEE 802.11) sur le contrôleur de domaine et après que stratégie de groupe a été actualisé sur le client sans fil.

  Toutefois, pour les ordinateurs qui ne sont pas déjà joints à votre domaine, vous devez planifier une méthode pour appliquer les paramètres requis pour l’accès authentifié 802.1X. Par exemple, déterminez si vous souhaitez joindre l’ordinateur au domaine à l’aide de l’une des méthodes suivantes.

  1. Connectez l’ordinateur à un segment du réseau câblé qui n’est pas protégé par 802.1X, puis joignez l’ordinateur au domaine.

  2. Fournissez à vos utilisateurs sans fil les étapes et les paramètres dont ils ont besoin pour ajouter leur propre profil de démarrage sans fil, ce qui leur permet de joindre l’ordinateur au domaine.

3. Affecter le personnel informatique pour joindre des clients sans fil au domaine.

Planification de la prise en charge de plusieurs normes

L'extension de stratégies de réseau sans fil (IEEE 802.11) dans stratégie de groupe fournit un large éventail d'options de configuration pour prendre en charge diverses options de déploiement.

Vous pouvez déployer des points d'accès sans fil configurés avec les normes que vous souhaitez prendre en charge, puis configurer plusieurs profils sans fil dans les stratégies de réseau sans fil (IEEE 802.11), chaque profil spécifiant un ensemble de normes dont vous avez besoin.

Par exemple, si votre réseau dispose d'ordinateurs sans fil qui prennent en charge WPA2-Enterprise et AES, d'autres ordinateurs qui prennent en charge WPA-Enterprise et AES, et d'autres ordinateurs qui prennent en charge uniquement WPA-Enterprise et TKIP, vous devez déterminer si vous souhaitez :

- Configurez un profil unique pour prendre en charge tous les ordinateurs sans fil à l'aide de la méthode de chiffrement la plus faible prise en charge par tous vos ordinateurs , dans ce cas, WPA-Enterprise et TKIP.
- Configurez deux profils pour fournir la meilleure sécurité possible prise en charge par chaque ordinateur sans fil. Dans ce cas, vous devez configurer un profil qui spécifie le chiffrement le plus fort (WPA2-Enterprise et AES) et un profil qui utilise le chiffrement WPA-Enterprise et TKIP le plus faible. Dans cet exemple, il est essentiel de placer le profil qui utilise WPA2-Enterprise et AES le plus élevé dans l'ordre de préférence. Les ordinateurs qui ne sont pas en mesure d'utiliser WPA2-Enterprise et AES passent automatiquement au profil suivant dans l'ordre de préférence et traitent le profil qui spécifie WPA-Enterprise et TKIP.

> **ⓘ Important**
>
> Vous devez placer le profil avec les normes les plus sécurisées plus haut dans la liste triée des profils, car les ordinateurs connectés utilisent le premier profil qu'ils sont capables d'utiliser.

Planification de l'accès restreint au réseau sans fil

Dans de nombreux cas, vous souhaiterez peut-être fournir aux utilisateurs sans fil différents niveaux d'accès au réseau sans fil. Par exemple, vous pouvez autoriser certains

utilisateurs à accéder sans restriction, à n'importe quelle heure de la journée, tous les jours de la semaine. Pour les autres utilisateurs, vous souhaiterez peut-être autoriser l'accès uniquement pendant les heures de base, du lundi au vendredi, et refuser l'accès le samedi et le dimanche.

Ce guide fournit des instructions pour créer un environnement d'accès qui place tous vos utilisateurs sans fil dans un groupe avec un accès commun aux ressources sans fil. Vous créez un groupe de sécurité d'utilisateurs sans fil dans le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, puis vous faites de chaque utilisateur auquel vous souhaitez accorder l'accès sans fil un membre de ce groupe.

Lorsque vous configurez des stratégies réseau NPS, vous spécifiez le groupe de sécurité des utilisateurs sans fil comme objet que NPS traite lors de la détermination de l'autorisation.

Toutefois, si votre déploiement nécessite la prise en charge de différents niveaux d'accès, vous devez uniquement effectuer les opérations suivantes :

1. Créez plusieurs groupes de sécurité Utilisateurs sans fil pour créer des groupes de sécurité sans fil supplémentaires dans Utilisateurs et ordinateurs Active Directory. Par exemple, vous pouvez créer un groupe qui contient des utilisateurs disposant d'un accès complet, un groupe pour ceux qui n'ont accès qu'aux heures normales de travail et d'autres groupes qui répondent à d'autres critères qui correspondent à vos besoins.

2. Ajoutez des utilisateurs aux groupes de sécurité appropriés que vous avez créés.

3. Configurez des stratégies réseau NPS supplémentaires pour chaque groupe de sécurité sans fil supplémentaire et configurez les stratégies pour appliquer les conditions et les contraintes dont vous avez besoin pour chaque groupe.

Méthodes de planification pour l'ajout de nouveaux ordinateurs sans fil

La méthode recommandée pour joindre de nouveaux ordinateurs sans fil au domaine, puis se connecter au domaine consiste à utiliser une connexion câblée à un segment du réseau local qui a accès aux contrôleurs de domaine et qui n'est pas protégé par un commutateur Ethernet d'authentification 802.1X.

Dans certains cas, toutefois, il peut ne pas être pratique d'utiliser une connexion câblée pour joindre des ordinateurs au domaine ou, pour un utilisateur, d'utiliser une connexion câblée pour sa première tentative d'ouverture de session à l'aide d'ordinateurs déjà joints au domaine.

Pour joindre un ordinateur au domaine à l'aide d'une connexion sans fil ou pour que les utilisateurs se connectent au domaine la première fois à l'aide d'un ordinateur joint à un domaine et d'une connexion sans fil, les clients sans fil doivent d'abord établir une connexion au réseau sans fil sur un segment qui a accès aux contrôleurs de domaine réseau à l'aide de l'une des méthodes suivantes.

1. **Un membre du personnel informatique joint un ordinateur sans fil au domaine, puis configure un profil sans fil d'amorçage de l'authentification unique.** Avec cette méthode, un administrateur informatique connecte l'ordinateur sans fil au réseau Ethernet câblé, puis joint l'ordinateur au domaine. Ensuite, l'administrateur distribue l'ordinateur à l'utilisateur. Lorsque l'utilisateur démarre l'ordinateur, les informations d'identification de domaine qu'il spécifie manuellement pour le processus d'ouverture de session de l'utilisateur sont utilisées pour établir une connexion au réseau sans fil et se connecter au domaine.

2. **L'utilisateur configure manuellement l'ordinateur sans fil avec le profil sans fil bootstrap, puis rejoint le domaine.** Avec cette méthode, les utilisateurs configurent manuellement leurs ordinateurs sans fil avec un profil sans fil de démarrage en fonction des instructions d'un administrateur informatique. Le profil sans fil de démarrage permet aux utilisateurs d'établir une connexion sans fil, puis de joindre l'ordinateur au domaine. Après avoir joint l'ordinateur au domaine et redémarré l'ordinateur, l'utilisateur peut se connecter au domaine à l'aide d'une connexion sans fil et des informations d'identification de son compte de domaine.

Pour déployer l'accès sans fil, consultez Déploiement de l'accès sans fil.

Déploiement de l’accès sans fil

15/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Pour déployer l’accès sans fil, procédez comme suit :

- Déployer et configurer des points d’accès sans fil
- Créer un groupe de sécurité Utilisateurs sans fil
- Configurer les règles du réseau sans fil (IEEE 802.11)
- Configurer des serveurs NPS
- Joindre de nouveaux ordinateurs sans fil au domaine

Déployer et configurer des points d’accès sans fil

Procédez comme suit pour déployer et configurer vos points d’accès sans fil :

- Spécifier les fréquences des canaux des points d’accès sans fil
- Configurer des points d’accès sans fil

> ⓘ **Notes**
>
> Les procédures décrites dans ce guide n'incluent aucune instruction dans le cas où la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre pour demander votre autorisation de continuer. Si cette boîte de dialogue s’ouvre pendant que vous effectuez les procédures de ce guide et si la boîte de dialogue a été ouverte en réponse à vos actions, cliquez sur **Continuer**.

Spécifier les fréquences des canaux des points d’accès sans fil

Lorsque vous déployez plusieurs points d’accès sans fil sur un même site géographique, vous devez configurer des points d’accès sans fil qui ont des signaux qui se chevauchent pour utiliser des fréquences de canal uniques afin de réduire les interférences entre les points d’accès sans fil.

Vous pouvez utiliser les directives suivantes pour vous aider à choisir des fréquences de canal qui n’entrent pas en conflit avec d’autres réseaux sans fil à l’emplacement géographique de

votre réseau sans fil.

- Si d'autres organisations ont des bureaux à proximité ou dans le même bâtiment que votre organisation, déterminez s'il existe des réseaux sans fil appartenant à ces organisations. Découvrez à la fois l'emplacement et les fréquences de canal attribuées à leurs points d'accès sans fil, car vous devez attribuer différentes fréquences de canal à vos points d'accès et vous devez déterminer le meilleur emplacement pour installer vos points d'accès.

- Identifiez les signaux sans fil qui se chevauchent sur les étages adjacents au sein de votre propre organisation. Après avoir identifié les zones de couverture qui se chevauchent à l'extérieur et à l'intérieur de votre organisation, attribuez des fréquences de canal pour vos points d'accès sans fil, en veillant à ce que les deux points d'accès sans fil dont la couverture se chevauche se voient attribuer des fréquences de canal différentes.

Configurer des points d'accès sans fil

Utilisez les informations suivantes, ainsi que la documentation produit fournie par le fabricant du point d'accès sans fil pour configurer vos points d'accès sans fil.

Cette procédure énumère les éléments couramment configurés sur un point d'accès sans fil. Les noms d'éléments peuvent varier selon la marque et le modèle et peuvent être différents de ceux de la liste suivante. Pour plus d'informations, consultez la documentation de votre point d'accès sans fil.

Pour configurer vos points d'accès sans fil

- **SSID**. Spécifiez le nom du ou des réseaux sans fil (par exemple, ExampleWLAN). Il s'agit du nom qui est annoncé aux clients sans fil.

- **Encryption**. Spécifiez WPA2-Enterprise (préféré) ou WPA-Enterprise, et le chiffrement AES (préféré) ou TKIP, selon les versions prises en charge par les adaptateurs réseau de votre ordinateur client sans fil.

- **Adresse IP de l'AP sans fil (statique)**. Sur chaque point d'accès, configurez une adresse IP statique unique qui se trouve dans la plage d'exclusion de l'étendue DHCP pour le sous-réseau. L'utilisation d'une adresse exclue de l'attribution par DHCP empêche le serveur DHCP d'attribuer la même adresse IP à un ordinateur ou à un autre appareil.

- **Masque de sous-réseau**. Configurez cette option pour qu'elle corresponde aux paramètres du masque de sous-réseau du réseau local auquel vous avez connecté le point d'accès sans fil.

- **Nom DNS**. Certaines adresses IP sans fil peuvent être configurées avec un nom DNS. Le service DNS sur le réseau peut résoudre les noms DNS en une adresse IP. Sur chaque point d'accès sans fil qui prend en charge cette fonctionnalité, entrez un nom unique pour la résolution DNS.

- **Service DHCP**. Si votre point d'accès sans fil dispose d'un service DHCP intégré, désactivez-le.

- **Secret partagé RADIUS**. Utilisez un secret partagé RADIUS unique pour chaque point d'accès sans fil, sauf si vous envisagez de configurer des points d'accès en tant que clients RADIUS dans le serveur NPS par groupe. Si vous envisagez de configurer des points d'accès par groupe dans le serveur NPS, le secret partagé doit être le même pour chaque membre du groupe. En outre, chaque secret partagé que vous utilisez doit être une séquence aléatoire d'au moins 22 caractères mélangeant des lettres majuscules et minuscules, des chiffres et des signes de ponctuation. Pour garantir la randomité, vous pouvez utiliser un générateur de caractères aléatoires, tel que le générateur de caractères aléatoires trouvé dans l'Assistant NPS **Configure 802.1X** , pour créer les secrets partagés.

> **Conseil**
>
> Enregistrez le secret partagé pour chaque point d'accès sans fil et stockez-le dans un emplacement sécurisé, tel qu'un coffre-fort de bureau. Vous devez connaître le secret partagé pour chaque point d'accès sans fil lorsque vous configurez des clients RADIUS dans le serveur NPS.

- **Adresse IP du serveur RADIUS**. Tapez l'adresse IP du serveur exécutant le serveur NPS.

- **Ports UDP**. Par défaut, le serveur NPS utilise les ports UDP 1812 et 1645 pour les messages d'authentification, et les ports UDP 1813 et 1646 pour les messages de comptabilité. Il est recommandé d'utiliser ces mêmes ports UDP sur vos points d'accès, mais si vous avez une raison valable d'utiliser des ports différents, veillez non seulement à configurer les points d'accès avec les nouveaux numéros de port, mais également à reconfigurer tous vos serveurs NPS pour utiliser les mêmes numéros de port que les points d'accès. Si les points d'accès et les serveurs NPS ne sont pas configurés avec les mêmes ports UDP, le serveur NPS ne peut pas recevoir ou traiter les requêtes de connexion des points d'accès, et toutes les tentatives de connexion sans fil sur le réseau échoueront.

- **VSAs**. Certaines adresses IP sans fil nécessitent des attributs spécifiques au fournisseur (VSA) pour fournir des fonctionnalités d'AP sans fil complètes. Les VSA sont ajoutés dans la stratégie réseau du serveur NPS.

- **Filtrage DHCP**. Configurez les points d'accès sans fil pour empêcher les clients sans fil d'envoyer des paquets IP à partir du port UDP 68 vers le réseau, comme indiqué par le fabricant du point d'accès sans fil.
- **Filtrage DNS**. Configurez les points d'accès sans fil pour empêcher les clients sans fil d'envoyer au réseau des paquets IP à partir du port TCP ou UDP 53, comme indiqué par le fabricant du point d'accès sans fil.

Créez des groupes de sécurité pour les utilisateurs sans fil

Procédez comme suit pour créer un ou plusieurs groupes de sécurité d'utilisateurs sans fil, puis pour ajouter des utilisateurs au groupe de sécurité d'utilisateurs sans fil approprié :

- Créer un groupe de sécurité Utilisateurs sans fil
- Ajouter des utilisateurs au groupe de sécurité sans fil

Créer un groupe de sécurité Utilisateurs sans fil

Vous pouvez utiliser cette procédure pour créer un groupe de sécurité sans fil dans le composant logiciel enfichable MMC (Microsoft Management Console) des utilisateurs et ordinateurs d'Active Directory.

L'appartenance aux **administrateurs de domaine** ou équivalent est la condition minimale requise pour effectuer cette procédure.

Pour créer un groupe de sécurité utilisateurs sans fil

1. Cliquez sur **Démarrer**, cliquez sur **Outils d'administration**, puis sur **Utilisateurs et ordinateurs Active Directory**. Le composant logiciel enfichable Utilisateurs et ordinateurs d'Active Directory s'ouvre. Si le nœud de votre domaine n'est pas encore sélectionné, cliquez dessus. Par exemple, si votre domaine est example.com, cliquez sur **example.com**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur le dossier dans lequel vous souhaitez ajouter un nouveau groupe (par exemple, cliquez avec le bouton droit sur **Utilisateurs**), pointez sur **Nouveau**, puis cliquez sur **Groupe**.
3. Dans **Nouvel objet - Groupe**, tapez le nom du nouveau groupe dans la zone **Nom du groupe**. Par exemple, tapez **Groupe sans fil**.
4. Dans **l'étendue du groupe**, sélectionnez l'une des options suivantes :

- **Domaine local**
- **Global**
- **Universal**

5. Dans **le type de groupe**, sélectionnez **Sécurité**.
6. Cliquez sur **OK**.

Si vous avez besoin de plusieurs groupes de sécurité pour les utilisateurs sans fil, répétez ces étapes pour créer des groupes d'utilisateurs sans fil supplémentaires. Par la suite, vous pouvez créer des stratégies réseau individuelles dans le serveur NPS pour appliquer différentes conditions et contraintes à chaque groupe, en leur fournissant des autorisations d'accès et des règles de connectivité différentes.

Ajoutez des utilisateurs au groupe de sécurité Utilisateurs sans fil

Vous pouvez utiliser cette procédure pour ajouter un utilisateur, un ordinateur ou un groupe à votre groupe de sécurité sans fil dans le composant logiciel enfichable MMC (Microsoft Management Console) des Utilisateurs et Ordinateurs d'Active Directory.

L'appartenance aux **administrateurs de domaine** ou équivalente est la condition minimale requise pour effectuer cette procédure.

Pour ajouter des utilisateurs au groupe de sécurité sans fil

1. Cliquez sur **Démarrer**, cliquez sur **Outils d'administration**, puis sur **Utilisateurs et ordinateurs Active Directory**. La console MMC Utilisateurs et ordinateurs Active Directory s'ouvre. Si le nœud de votre domaine n'est pas encore sélectionné, cliquez dessus. Par exemple, si votre domaine est example.com, cliquez sur **example.com**.
2. Dans le volet d'informations, double-cliquez sur le dossier qui contient votre groupe de sécurité sans fil.
3. Dans le volet d'informations, cliquez avec le bouton droit sur le groupe de sécurité sans fil, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés** du groupe de sécurité s'ouvre.
4. Sous l'onglet **Membres** , cliquez sur **Ajouter**, puis effectuez l'une des procédures suivantes pour ajouter un ordinateur ou ajouter un utilisateur ou un groupe.

Pour ajouter un utilisateur ou un groupe

1. Dans l'onglet **Entrer les noms d'objets à sélectionner**, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter, puis cliquez sur **OK**.
2. Pour attribuer l'appartenance à un groupe à d'autres utilisateurs ou groupes, répétez l'étape 1 de cette procédure.

Pour ajouter un ordinateur

1. Cliquez sur **Types d'objets**. La boîte de dialogue **Types d'objets** s'ouvre.
2. Dans **les types d'objets**, sélectionnez **Ordinateurs**, puis cliquez sur **OK**.
3. Dans l'onglet **Entrer les noms d'objets à sélectionner**, saisissez le nom de l'ordinateur que vous souhaitez ajouter, puis cliquez sur **OK**.
4. Pour attribuer l'appartenance à un groupe à d'autres ordinateurs, répétez les étapes 1 à 3 de cette procédure.

Configurer les règles du réseau sans fil (IEEE 802.11)

Procédez comme suit pour configurer l'extension de stratégie de groupe pour les stratégies de réseau sans fil (IEEE 802.11) :

- Ouvrir ou ajouter et ouvrir un objet de stratégie de groupe
- Activer les stratégies par défaut du réseau sans fil (IEEE 802.11)
- Configurer la nouvelle stratégie de réseau sans fil

Ouvrir ou ajouter et ouvrir un objet de stratégie de groupe

Par défaut, la fonctionnalité de gestion des stratégies de groupe est installée sur les ordinateurs exécutant Windows Server 2016 lorsque le rôle de serveur Active Directory Domain Services (AD DS) est installé et que le serveur est configuré en tant que contrôleur de domaine. La procédure suivante décrit comment ouvrir la console de gestion des stratégies de groupe (GPMC) sur votre contrôleur de domaine. La procédure décrit ensuite comment ouvrir un objet de stratégie de groupe (GPO) existant au niveau du domaine pour le modifier, ou créer un nouveau GPO de domaine et l'ouvrir pour le modifier.

L'appartenance aux **administrateurs de domaine** ou équivalent est la condition minimale requise pour effectuer cette procédure.

Pour ouvrir ou ajouter et ouvrir un objet de stratégie de groupe

1. Sur votre contrôleur de domaine, cliquez sur **Démarrer**, sur **Outils d'administration Windows**, puis sur **Gestion des stratégies de groupe**. La Console de gestion des stratégies de groupe s'ouvre.

2. Dans le volet de gauche, double-cliquez sur votre forêt. Par exemple, double-cliquez sur **Forêt : example.com**.

3. Dans le volet gauche, double-cliquez sur **Domaines**, puis double-cliquez sur le domaine pour lequel vous souhaitez gérer un objet de stratégie de groupe. Par exemple, double-cliquez sur **example.com**.

4. Effectuez l'une des opérations suivantes :

   - **Pour ouvrir un objet de stratégie de groupe existant au niveau du domaine afin de le modifier**, double-cliquez sur le domaine contenant l'objet de stratégie de groupe à gérer, faites un clic droit sur la stratégie de domaine à gérer, telle que la stratégie de domaine par défaut, puis cliquez sur **Modifier**. **L'éditeur de gestion des stratégies de groupe (GPME)** s'ouvre.

   - **Pour créer un nouvel objet de stratégie de groupe et l'ouvrir pour modification**, faites un clic droit sur le domaine pour lequel vous souhaitez créer un nouvel objet de stratégie de groupe, puis cliquez sur **Créer un objet de stratégie de groupe dans ce domaine, puis liez-le ici**.

     Dans **Nouvel objet de stratégie de groupe**, dans **Name**, tapez un nom pour le nouvel objet de stratégie de groupe, puis cliquez sur **OK**.

     Cliquez avec le bouton droit sur votre nouvel objet de stratégie de groupe, puis cliquez sur **Modifier**. **L'éditeur de gestion des stratégies de groupe (GPME)** s'ouvre.

Dans la section suivante, vous allez utiliser l'Éditeur de gestion des stratégies de groupe pour créer une stratégie sans fil.

Activer les stratégies par défaut du réseau sans fil (IEEE 802.11)

Cette procédure explique comment activer les stratégies de réseau sans fil (IEEE 802.11) par défaut à l'aide de l'Éditeur de gestion des stratégies de groupe (GPME).

> ⓘ **Notes**
>
> Après avoir activé la version **Windows Vista et versions ultérieures** des stratégies de réseau sans fil (IEEE 802.11) ou la version **Windows XP**, l'option de version est

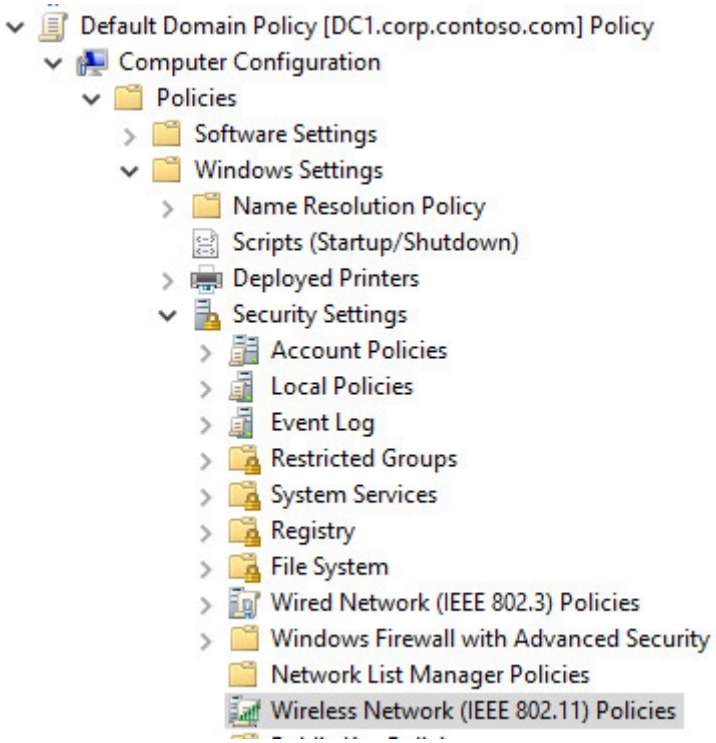
automatiquement supprimée de la liste des options lorsque vous faites un clic droit sur **Stratégies de réseau sans fil (IEEE 802.11).** Cela se produit car après avoir sélectionné une version de stratégie, la stratégie est ajoutée dans le volet d'informations du GPME lorsque vous sélectionnez le nœud **Stratégies de réseau sans fil (IEEE 802.11)**. Cet état reste inchangé jusqu'à ce que vous supprimiez la stratégie sans fil, auquel cas la version de la stratégie sans fil réapparaît dans le menu contextuel pour les **Stratégies de réseau sans fil (IEEE 802.11)** dans le GPME. En outre, les stratégies sans fil sont répertoriées uniquement dans le volet d'informations GPME lorsque le nœud **Stratégies de réseau sans fil (IEEE 802.11)** est sélectionné.

L'appartenance aux **administrateurs de domaine** ou équivalent est la condition minimale requise pour effectuer cette procédure.

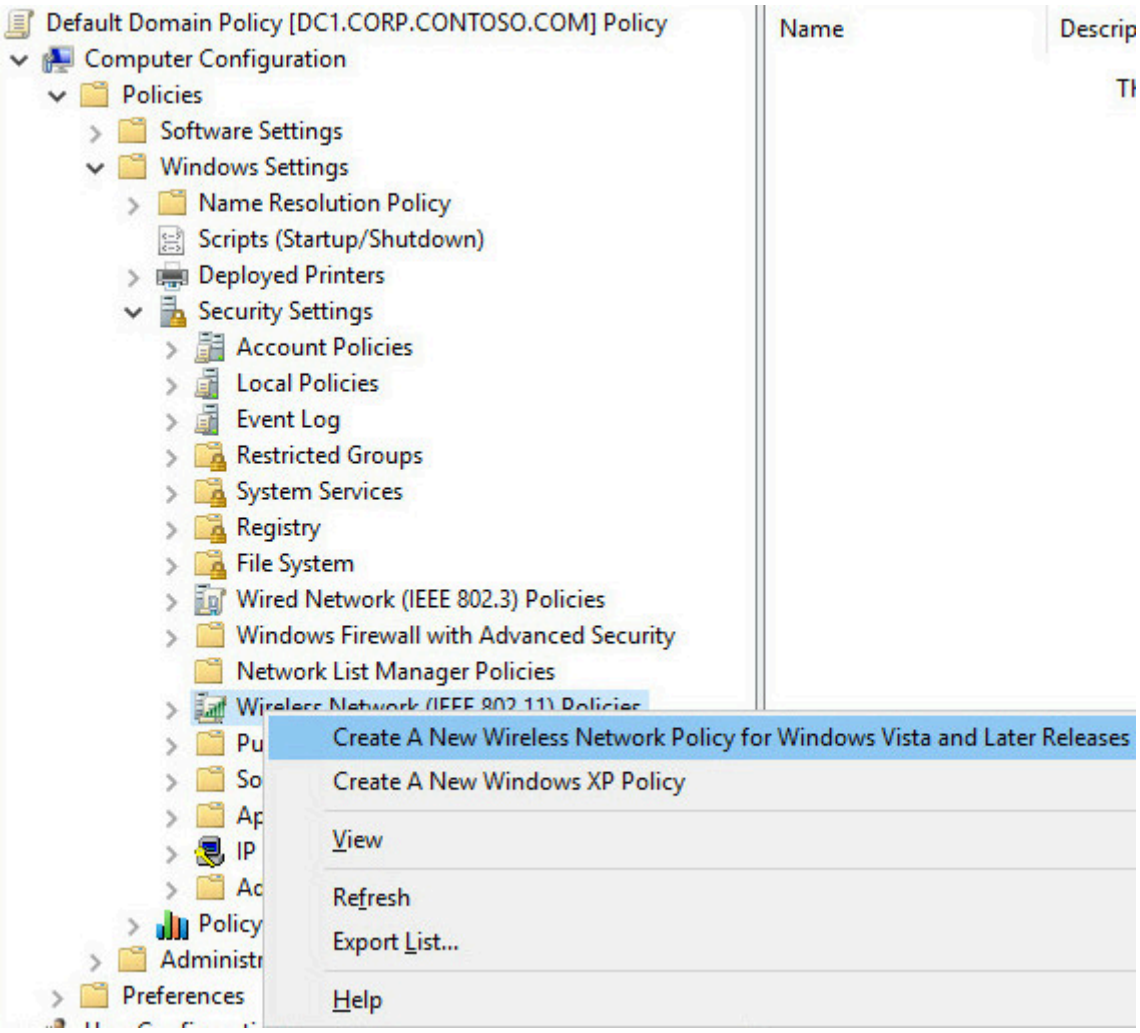
Pour activer les stratégies de réseau sans fil par défaut (IEEE 802.11)

1. Suivez la procédure précédente, **Pour ouvrir ou ajouter et ouvrir un objet de stratégie de groupe** pour ouvrir le GPME.

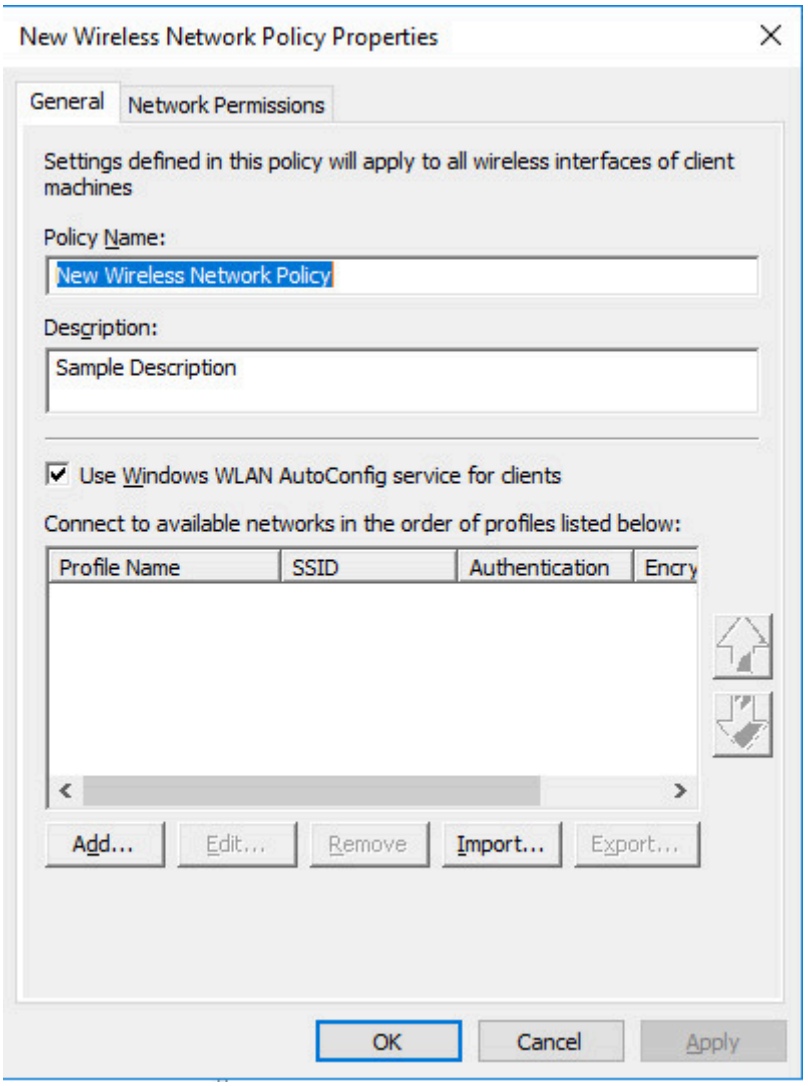
2. Dans le GPME, dans le volet gauche, double-cliquez sur **Configuration de l'ordinateur**, double-cliquez sur **Stratégies**, double-cliquez sur **Paramètres Windows**, puis double-cliquez sur **Paramètres de sécurité**.



3. Dans **Paramètres de sécurité**, cliquez avec le bouton droit sur **Les stratégies de réseau sans fil (IEEE 802.11),** puis cliquez sur **Créer une stratégie sans fil pour Windows Vista et versions ultérieures**.



4. La boîte de dialogue **Propriétés de la nouvelle stratégie de réseau sans fil** s'ouvre. Dans **Nom de** la stratégie, tapez un nouveau nom pour la stratégie ou conservez le nom par défaut. Cliquez sur **OK** pour enregistrer la stratégie. La stratégie par défaut est activée et répertoriée dans le volet d'informations du GPME avec le nouveau nom que vous avez fourni ou avec le nom par défaut **Nouvelle stratégie de réseau sans fil**.



5. Dans le volet d'informations, double-cliquez sur **Nouvelle stratégie de réseau sans fil** pour l'ouvrir.

Dans la section suivante, vous pouvez procéder à la configuration de la stratégie, à l'ordre de préférence de traitement de la stratégie et aux autorisations réseau.

Configurer la nouvelle stratégie de réseau sans fil

Vous pouvez utiliser les procédures de cette section pour configurer la stratégie de réseau sans fil (IEEE 802.11). Cette stratégie vous permet de configurer les paramètres de sécurité et d'authentification, de gérer les profils sans fil et de spécifier des autorisations pour les réseaux sans fil qui ne sont pas configurés en tant que réseaux préférés.

- Configurer un profil de connexion sans fil pour PEAP-MS-CHAP v2
- Définir l'ordre de préférence pour les profils de connexion sans fil
- Définir les autorisations réseau

Configurer un profil de connexion sans fil pour PEAP-MS-CHAP v2

Cette procédure fournit les étapes requises pour configurer un profil sans fil PEAP-MS-CHAP v2.

L’appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour configurer un profil de connexion sans fil pour PEAP-MS-CHAP v2

1. Dans GPME, dans la boîte de dialogue propriétés du réseau sans fil pour la stratégie que vous venez de créer, sous l’onglet **Général** et dans **Description**, tapez une brève description de la stratégie.

2. Pour spécifier que WLAN AutoConfig est utilisé pour configurer les paramètres de l’adaptateur réseau sans fil, vérifiez que l’option **Utiliser le service Windows WLAN AutoConfig pour les clients** est sélectionnée.

3. Dans la section **Se connecter aux réseaux disponibles dans l’ordre des profils répertoriés ci-dessous**, cliquez sur **Ajouter**, puis sélectionnez **Infrastructure**. La boîte de dialogue **Propriétés du nouveau profil** s’ouvre.

4. Dans la boîte de dialogue**Propriétés du nouveau profil**, dans l’onglet **Connexion**, dans le champ **Nom du profil**, saisissez un nouveau nom pour le profil. Par exemple, saisissez **Example.com Profil WLAN pour Windows 10**.

5. Dans **Nom(s) de réseau (SSID)**, saisissez l'identificateur SSID (Service Set Identifier) correspondant à l'identificateur SSID sur vos points d'accès sans fil, puis cliquez sur **Ajouter**.

   Si votre déploiement utilise plusieurs identificateurs SSID et que chaque point d'accès sans fil utilise les mêmes paramètres de sécurité sans fil, répétez cette étape pour ajouter l'identificateur SSID pour chaque point d'accès sans fil auquel vous voulez appliquer ce profil.

   Si votre déploiement utilise plusieurs identificateurs SSID et que les paramètres de sécurité pour chaque identificateur SSID ne sont pas identiques, configurez un profil distinct pour chaque groupe d'identificateurs SSID utilisant les mêmes paramètres de sécurité. Par exemple, si vous avez un groupe de points d'accès sans fil configurés pour utiliser WPA2-Enterprise et AES et un autre groupe de points d'accès sans fil configurés pour utiliser WPA-Enterprise et TKIP, configurez un profil pour chaque groupe de points d'accès sans fil.

6. Si le texte **par défaut NEWSSID** est présent, sélectionnez-le, puis cliquez sur **Supprimer**.

7. Si vous avez déployé des points d'accès sans fil configurés pour supprimer la balise de diffusion, sélectionnez **Se connecter même s'il ne s'agit pas d'un réseau de diffusion**.

> ⓘ **Notes**
>
> L'activation de cette option peut créer un risque de sécurité, car les clients sans fil chercheront à se connecter à n'importe quel réseau sans fil. Par défaut, ce paramètre n'est pas activé.

8. Cliquez sur l'onglet **Sécurité** , cliquez sur **Avancé**, puis configurez les éléments suivants :

   a. Pour configurer les paramètres 802.1X avancés, dans **IEEE 802.1X**, sélectionnez **Appliquer les paramètres avancés 802.1X**.

      Quand les paramètres 802.1X avancés sont appliqués, les valeurs par défaut pour **Nbre max. de messages Eapol-Start**, **Période de maintien**, **Période de démarrage** et **Période d'authentification** sont suffisantes pour les déploiements sans fil typiques. Pour cette raison, vous n'avez pas besoin de modifier les valeurs par défaut, sauf si vous avez une raison spécifique de le faire.

   b. Pour activer l'authentification unique, sélectionnez **Activer l'authentification unique pour ce réseau**.

   c. Les autres valeurs par défaut dans **Authentification unique** sont suffisantes pour les déploiements sans fil standard.

   d. Dans **Fast Roaming**, si votre API sans fil est configurée pour la pré-authentification, sélectionnez **Ce réseau utilise la pré-authentification**.

9. Pour spécifier que les communications sans fil respectent les normes FIPS 140-2, sélectionnez **Effectuer le chiffrement en mode certifié FIPS 140-2**.

10. Cliquez sur **OK** pour revenir à l'onglet **Sécurité** . Dans **Sélectionner les méthodes de sécurité pour ce réseau**, dans **Authentification**, sélectionnez **WPA2-Enterprise** s'il est pris en charge par vos cartes réseau sans fil et vos cartes réseau clientes sans fil. Sinon, sélectionnez **WPA-Enterprise**.

11. Dans **Chiffrement**, si votre API sans fil et vos cartes réseau clientes sans fil sont prises en charge, sélectionnez **AES-CCMP**. Si vous utilisez des points d'accès et des cartes réseau sans fil qui prennent en charge 802.11ac, sélectionnez **AES-GCMP**. Sinon, sélectionnez **TKIP**.

> ⓘ **Notes**

Les paramètres de **l'authentification** et du **chiffrement** doivent correspondre aux paramètres configurés sur vos adresses IP sans fil. Les paramètres par défaut pour le **mode d'authentification**, **les échecs d'authentification maximal** et les **informations utilisateur du cache pour les connexions ultérieures à ce réseau** sont suffisants pour les déploiements sans fil classiques.

12. Dans **Sélectionner une méthode d'authentification réseau**, sélectionnez **PEAP (Protected EAP)**, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés EAP protégées** s'ouvre.

13. Dans **Propriétés EAP protégées**, confirmez que l'option **Vérifier l'identité du serveur en validant le certificat** est sélectionnée.

14. Dans **Autorités de certification racine de confiance**, sélectionnez l'autorité de certification (AC) racine de confiance qui a émis le certificat de serveur pour votre serveur NPS.

    ⓘ **Notes**

    Ce paramètre limite aux seules autorités de certification sélectionnées les autorités de certification racines auxquelles les clients font confiance. Si aucune autorité de certification racine de confiance n'est sélectionnée, les clients feront confiance à toutes les autorités de certification racine figurant dans leur magasin de certificats d'autorités de certification racine de confiance.

15. Dans la liste **Sélectionner la méthode d'authentification**, sélectionnez **Mot de passe sécurisé (EAP-MS-CHAP v2)**.

16. Cliquez sur **Configurer**. Dans la boîte de dialogue **Propriétés EAP MSCHAPv2**, vérifiez que l'option **Utiliser automatiquement mon nom et mon mot de passe de connexion Windows (et mon domaine le cas échéant)** est sélectionnée, puis cliquez sur **OK**.

17. Pour activer la Reconnexion rapide PEAP, vérifiez que l'option **Activer la reconnexion rapide** est sélectionnée.

18. Pour exiger le TLV de liaison de chiffrement du serveur lors des tentatives de connexion, sélectionnez **Déconnecter si le serveur ne présente pas de TLV de liaison de chiffrement**.

19. Pour spécifier que l'identité de l'utilisateur est masquée lors de la première phase d'authentification, sélectionnez **Activer la confidentialité des identités** et, dans la zone de texte, tapez un nom d'identité anonyme ou laissez la zone de texte vide.

    > [!NOTES]

- La stratégie NPS pour 802.1X Wireless doit être créée à l'aide de la **Stratégie de requête de connexion** du serveur NPS. Si la stratégie NPS est créée à l'aide de la stratégie **réseau** NPS, la confidentialité des identités ne fonctionnera pas.
- La confidentialité des identités EAP est fournie par certaines méthodes EAP où une identité vide ou anonyme (différente de l'identité réelle) est envoyée en réponse à la requête d'identité EAP. PEAP envoie l'identité deux fois pendant l'authentification. Dans la première phase, l'identité est envoyée en texte brut et cette identité est utilisée à des fins de routage, et non pour l'authentification du client. L'identité réelle, utilisée pour l'authentification, est envoyée au cours de la deuxième phase de l'authentification, dans le tunnel sécurisé établi dans la première phase. Si la case **Activer la confidentialité des identités** est cochée, le nom d'utilisateur est remplacé par l'entrée spécifiée dans la zone de texte. Par exemple, supposons que l'option **Activer la confidentialité des identités** soit sélectionnée et que l'alias de confidentialité d'identité **anonyme** soit spécifié dans la zone de texte. Pour un utilisateur avec un alias d'identité réel **jdoe@example.com**, l'identité envoyée dans la première phase d'authentification sera remplacée par **anonymous@example.com**. La partie du domaine de l'identité de la première phase n'est pas modifiée, car elle est utilisée à des fins de routage.

20. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés EAP protégées** .

21. Cliquez sur **OK** pour fermer l'onglet **Sécurité** .

22. Si vous souhaitez créer des profils supplémentaires, cliquez sur **Ajouter**, puis répétez les étapes précédentes, en faisant des choix différents pour personnaliser chaque profil pour les clients sans fil et le réseau auxquels vous souhaitez appliquer le profil. Lorsque vous avez terminé d'ajouter des profils, cliquez sur **OK** pour fermer la boîte de dialogue Propriétés de la stratégie réseau sans fil.

Dans la section suivante, vous pouvez commander les profils de stratégie pour une sécurité optimale.

Définir l'ordre de préférence pour les profils de connexion sans fil

Vous pouvez utiliser cette procédure si vous avez créé plusieurs profils sans fil dans votre stratégie de réseau sans fil et que vous souhaitez les classer pour une efficacité et une sécurité optimales.

Pour garantir que les clients sans fil se connectent avec le niveau de sécurité le plus élevé qu'ils peuvent prendre en charge, placez vos stratégies les plus restrictives en haut de la liste.

Par exemple, si vous avez deux profils, l'un pour les clients qui prennent en charge WPA2 et l'autre pour les clients qui prennent en charge WPA, placez le profil WPA2 plus haut dans la liste. Cela garantit que les clients qui prennent en charge WPA2 utiliseront cette méthode pour la connexion plutôt que la méthode WPA moins sécurisée.

Cette procédure fournit les étapes permettant de spécifier l'ordre dans lequel les profils de connexion sans fil sont utilisés pour connecter les clients sans fil des membres du domaine aux réseaux sans fil.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour définir l'ordre de préférence pour les profils de connexion sans fil

1. Dans GPME, dans la boîte de dialogue propriétés du réseau sans fil pour la stratégie que vous venez de configurer, cliquez sur l'onglet **Général** .
2. Sous l'onglet **Général** , dans **Se connecter aux réseaux disponibles dans l'ordre des profils répertoriés ci-dessous**, sélectionnez le profil à déplacer dans la liste, puis cliquez sur le bouton « Flèche haut » ou « flèche bas » pour déplacer le profil vers l'emplacement souhaité dans la liste.
3. Répétez l'étape 2 pour chaque profil que vous souhaitez déplacer dans la liste.
4. Cliquez sur **OK** pour enregistrer toutes les modifications.

Dans la section suivante, vous pouvez définir des autorisations réseau pour la stratégie sans fil.

Définir les autorisations réseau

Vous pouvez configurer les paramètres sous l'onglet **Autorisations réseau** pour les membres du domaine auxquels les stratégies de réseau sans fil (IEEE 802.11) s'appliquent.

Vous pouvez uniquement appliquer les paramètres suivants pour les réseaux sans fil qui ne sont pas configurés sous l'onglet **Général** dans la page Propriétés de la stratégie **réseau sans fil** :

- Autorisez ou refusez des connexions à des réseaux sans fil spécifiques que vous spécifiez par type de réseau et identificateur de l'ensemble de services (SSID)
- Autorisez ou refusez des connexions à des réseaux ad hoc
- Autorisez ou refusez des connexions à des réseaux d'infrastructure

- Autorisez ou refusez aux utilisateurs d'afficher les types de réseaux (ad hoc ou infrastructure) auxquels ils n'ont pas accès
- Autorisez ou refusez aux utilisateurs de créer un profil qui s'applique à tous les utilisateurs
- Les utilisateurs peuvent uniquement se connecter aux réseaux autorisés à l'aide de profils de stratégie de groupe

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer ces procédures.

Pour autoriser ou refuser des connexions à des réseaux sans fil spécifiques

1. Dans GPME, dans la boîte de dialogue propriétés réseau sans fil, cliquez sur l'onglet **Autorisations réseau** .
2. Sous l'onglet **Autorisations réseau** , cliquez sur **Ajouter**. La boîte de dialogue **Nouvelle entrée d'autorisation** s'ouvre.
3. Dans la boîte de dialogue **Nouvelle entrée d'autorisation**, dans le champ **Nom du réseau (SSID),** tapez le SSID réseau du réseau pour lequel vous souhaitez définir des autorisations.
4. Dans **Type de réseau**, sélectionnez **Infrastructure** ou **Ad hoc**.

   > ⓘ **Notes**
   >
   > Si vous ne savez pas si le réseau de diffusion est une infrastructure ou un réseau ad hoc, vous pouvez configurer deux entrées d'autorisation réseau, une pour chaque type de réseau.

5. Dans **Autorisation**, sélectionnez **Autoriser** ou **Refuser**.
6. Cliquez sur **OK** pour revenir à l'onglet **Autorisations réseau** .

Pour spécifier des autorisations réseau supplémentaires (facultatif)

1. Sous l'onglet **Autorisations réseau** , configurez l'une ou l'autre des options suivantes :
   - Pour refuser aux membres de votre domaine l'accès aux réseaux ad hoc, sélectionnez **Empêcher les connexions aux réseaux ad hoc**.

- Pour refuser aux membres de votre domaine l'accès aux réseaux d'infrastructure, sélectionnez **Empêcher les connexions aux réseaux d'infrastructure**.
- Pour permettre aux membres de votre domaine d'afficher les types de réseau (ad hoc ou infrastructure) dont l'accès leur est refusé, sélectionnez **Autoriser l'utilisateur à afficher les réseaux refusés**.
- Pour permettre aux utilisateurs de créer des profils qui s'appliquent à tous les utilisateurs, sélectionnez **Autoriser tout le monde à créer tous les profils utilisateur**.
- Pour spécifier que vos utilisateurs peuvent uniquement se connecter aux réseaux autorisés à l'aide de profils de stratégie de groupe, sélectionnez **Utiliser uniquement les profils de stratégie de groupe pour les réseaux autorisés**.

Configurez vos serveurs NPS

Procédez comme suit pour configurer les serveur NPS afin d'effectuer l'authentification 802.1X pour l'accès sans fil :

- Enregistrer les serveurs NPS dans Active Directory Domain Services
- Configurer un point d'accès sans fil en tant que client RADIUS du serveur NPS
- Créer des stratégies de serveur NPS pour l'accès sans fil 802.1X à l'aide d'un Assistant

Enregistrer les serveurs NPS dans Active Directory Domain Services

Vous pouvez utiliser cette procédure pour inscrire un serveur exécutant le serveur NPS (Network Policy Server) dans Active Directory Domain Services (AD DS) dans le domaine où le serveur NPS est membre. Pour que les serveurs NPS soient autorisés à lire les propriétés de numérotation des comptes d'utilisateurs pendant le processus d'autorisation, chaque serveur NPS doit être enregistré dans AD DS. L'enregistrement d'un serveur NPS permet d'ajouter le serveur au groupe de sécurité des **Serveurs RAS et IAS** dans AD DS.

> **Notes**
>
> Vous pouvez installer le serveur NPS sur un contrôleur de domaine ou sur un serveur dédié. Exécutez la commande Windows PowerShell suivante pour installer le serveur NPS si vous ne l'avez pas encore fait :

PowerShell

```
Install-WindowsFeature NPAS -IncludeManagementTools
```

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour inscrire un serveur NPS dans son domaine par défaut

1. Sur votre serveur NPS, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Serveur de stratégie réseau**. Le composant logiciel enfichable du serveur NPS s'ouvre.
2. Cliquez avec le bouton droit sur **NPS (local),** puis cliquez sur **Inscrire le serveur dans Active Directory**. La boîte de dialogue **Serveur NPS (Network Policy Server)** s'ouvre.
3. Dans **Serveur NPS (Network Policy Server)**, cliquez sur **OK**, puis à nouveau sur **OK**.

Configurer un point d'accès sans fil en tant que client RADIUS du serveur NPS

Vous pouvez utiliser cette procédure pour configurer un point d'accès, également appelé *serveur d'accès réseau (NAS),* en tant que client RADIUS (Remote Authentication Dial-In User Service) à l'aide du composant logiciel enfichable du serveur NPS.

> **ⓘ Important**
>
> Les ordinateurs clients, tels que les ordinateurs portables sans fil et autres ordinateurs exécutant des systèmes d'exploitation clients, ne sont pas des clients RADIUS. Les clients RADIUS sont des serveurs d'accès au réseau, tels que les points d'accès sans fil, les commutateurs compatibles 802.1X, les serveurs de réseaux privés virtuels (VPN) et les serveurs d'accès à distance, car ils utilisent le protocole RADIUS pour communiquer avec les serveurs RADIUS tels que les serveurs NPS.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour ajouter un serveur d'accès réseau en tant que client RADIUS dans le serveur NPS

1. Sur votre serveur NPS, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Serveur de stratégie réseau**. Le composant logiciel enfichable du serveur NPS s'ouvre.

2. Dans le composant logiciel enfichable du serveur NPS, double-cliquez sur **Clients et serveurs RADIUS**. Cliquez avec le bouton droit sur **Clients RADIUS**, puis cliquez sur **Nouveau**.

3. Dans **Nouveau client RADIUS**, vérifiez que la case **Activer ce client RADIUS** est cochée.

4. Dans **Nouveau client RADIUS**, dans **Nom convivial**, tapez un nom d'affichage pour le point d'accès sans fil.

   Par exemple, si vous souhaitez ajouter un point d'accès sans fil nommé AP-01, tapez **AP-01**.

5. Dans **Adresse (IP ou serveur DNS),** tapez l'adresse IP ou le nom de domaine complet (FQDN) du NAS.

   Si vous entrez le nom de domaine complet, pour vérifier que le nom est correct et mappé à une adresse IP valide, cliquez sur **Vérifier**, puis, dans **Vérifier l'adresse**, dans le champ **Adresse** , cliquez sur **Résoudre**. Si le nom de nom de domaine complet est mappé à une adresse IP valide, l'adresse IP de ce NAS apparaît automatiquement dans **l'adresse IP**. Si le nom de domaine complet n'est pas résolu en une adresse IP, vous recevrez un message indiquant qu'aucun hôte de ce type n'est connu. Si cela se produit, vérifiez que le nom du point d'accès est correct, que le point d'accès est sous tension et qu'il est connecté au réseau.

   Cliquez sur **OK** pour fermer **l'adresse de vérification**.

6. Dans **Nouveau client RADIUS**, dans **Secret partagé**, effectuez l'une des opérations suivantes :

   - Pour configurer manuellement un secret partagé RADIUS, sélectionnez **Manuel**, puis dans **Secret partagé**, tapez le mot de passe fort qui est également entré sur le NAS. Retapez le secret partagé dans **Confirmer le secret partagé**.

   - Pour générer automatiquement un secret partagé, **cochez** la case Générer, puis cliquez sur le bouton **Générer** . Enregistrez le secret partagé généré, puis utilisez cette valeur pour configurer le NAS afin qu'il puisse communiquer avec le serveur NPS.

     > ⓘ **Important**
     >
     > Le secret partagé RADIUS que vous entrez pour vos points d'accès virtuels dans le serveur NPS doit correspondre exactement au secret partagé RADIUS configuré sur vos points d'accès sans fil réels. Si vous utilisez l'option du serveur NPS pour générer un secret partagé RADIUS, vous devez configurer le point

d'accès sans fil réel correspondant avec le secret partagé RADIUS qui a été généré par le serveur NPS.

7. Dans **Nouveau client RADIUS**, dans l'onglet **Avancé**, dans **Nom du fournisseur**, spécifiez le nom du fabricant du NAS. Si vous n'êtes pas sûr du nom du fabricant NAS, sélectionnez **RADIUS standard**.

8. Dans **Options supplémentaires**, si vous utilisez des méthodes d'authentification autres que EAP et PEAP, et si votre NAS prend en charge l'utilisation de l'attribut d'authentificateur de message, sélectionnez **Les messages de demande d'accès doivent contenir l'attribut Message-Authenticator**.

9. Cliquez sur **OK**. Votre NAS apparaît dans la liste des clients RADIUS configurés sur le serveur NPS.

Créer des stratégies de serveur NPS pour l'accès sans fil 802.1X à l'aide d'un Assistant

Vous pouvez utiliser cette procédure pour créer les stratégies de requête de connexion et les stratégies réseau requises pour déployer des points d'accès sans fil compatibles 802.1X en tant que clients RADIUS (Remote Authentication Dial-In User Service) sur le serveur RADIUS exécutant le serveur NPS (Network Policy Server). Après avoir exécuté l'Assistant, les stratégies suivantes sont créées :

- Une stratégie de demande de connexion
- Une stratégie réseau

> **Notes**
>
> Vous pouvez exécuter l'Assistant Nouvelles connexions câblées et sans fil sécurisées IEEE 802.1X chaque fois que vous devez créer de nouvelles stratégies pour l'accès authentifié 802.1X.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Créez des stratégies pour l'authentification sans fil 802.1X à l'aide d'un Assistant

1. Ouvrez le composant logiciel enfichable du serveur NPS. S'il n'est pas déjà sélectionné, cliquez sur **NPS (local)**. Si vous exécutez le composant logiciel enfichable MMC du serveur NPS et que vous souhaitez créer des stratégies sur un serveur NPS distant, sélectionnez le serveur.

2. Dans **Prise en main**, dans **Configuration standard**, sélectionnez **le serveur RADIUS pour les connexions sans fil ou câblées 802.1X**. Le texte et les liens sous le texte changent pour refléter votre sélection.

3. Cliquez sur **Configurer 802.1X**. L'Assistant Configurer 802.1X s'ouvre.

4. Dans la page De l'Assistant **Sélectionner un type de connexions 802.1X**, dans **Type de connexions 802.1X**, sélectionnez **Connexions sans fil sécurisées**, puis, dans **Nom**, tapez un nom pour votre stratégie, ou laissez le nom par défaut **Connexions sans fil sécurisées**. Cliquez sur **Suivant**.

5. Sur la page de l'assistant **Spécifier les commutateurs 802.1X**, dans **Clients RADIUS**, tous les commutateurs 802.1X et points d'accès sans fil que vous avez ajoutés en tant que clients RADIUS dans le composant logiciel enfichable du serveur NPS sont affichés. Faites ce qui suit :

   - Pour ajouter des serveurs d'accès réseau supplémentaires (NAS), tels que des adresses IP sans fil, dans **les clients RADIUS**, cliquez sur **Ajouter**, puis dans **le nouveau client RADIUS**, entrez les informations pour : **nom convivial**, **adresse IP ou DNS etsecret partagé**.

   - Pour modifier les paramètres de n'importe quel NAS, dans **les clients RADIUS**, sélectionnez l'API pour laquelle vous souhaitez modifier les paramètres, puis cliquez sur **Modifier**. Modifiez les paramètres en fonction des besoins.

   - Pour supprimer un NAS de la liste, dans **les clients RADIUS**, sélectionnez le NAS, puis cliquez sur **Supprimer**.

     > ⚠ **Avertissement**
     >
     > La suppression d'un client RADIUS à partir de l'Assistant **Configurer 802.1X** supprime le client de la configuration NPS. Tous les ajouts, modifications et suppressions que vous effectuez dans l'Assistant **Configurer 802.1X** sur les clients RADIUS sont reflétés dans le composant logiciel enfichable NPS, dans le nœud **Clients RADIUS** sous**clients ET serveurs RADIUS** / . Par exemple, si vous utilisez l'assistant pour supprimer un commutateur 802.1X, le commutateur est également supprimé du composant logiciel enfichable du serveur NPS.

6. Cliquez sur **Suivant**. Dans la page de l'Assistant **Configurer une méthode d'authentification**, dans **Type (en fonction de la méthode d'accès et de la configuration du réseau),** sélectionnez **Microsoft : EAP protégé (PEAP),** puis cliquez sur **Configurer**.

> **Conseil**
>
> Si vous recevez un message d'erreur indiquant qu'un certificat est introuvable pour être utilisé avec la méthode d'authentification et que vous avez configuré les services de certificats Active Directory pour émettre automatiquement des certificats sur des serveurs RAS et IAS sur votre réseau, vérifiez d'abord que vous avez suivi les étapes d'inscription du serveur NPS dans Active Directory Domain Services, puis utilisez les étapes suivantes pour mettre à jour la stratégie de groupe : Cliquez sur **Démarrer**, cliquez sur **Système Windows**, **sur Exécuter**, puis, dans **Ouvrir**, tapez **gpupdate**, puis appuyez sur Entrée. Lorsque la commande renvoie des résultats indiquant que la stratégie de groupe de l'utilisateur et de l'ordinateur a été mise à jour avec succès, sélectionnez à nouveau **Microsoft : EAP protégé (PEAP)**, puis cliquez sur **Configurer**.
>
> Si, après l'actualisation de la stratégie de groupe vous continuez à recevoir le message d'erreur indiquant qu'un certificat ne peut pas être trouvé pour une utilisation avec la méthode d'authentification, le certificat ne s'affiche pas, car il ne répond pas aux exigences minimales en matière de certificat de serveur, comme indiqué dans Core Network Companion Guide : Déployer des certificats de serveur pour les déploiements 802.1X avec et sans fil. Si cela se produit, vous devez interrompre la configuration du serveur NPS, révoquer le certificat émis pour votre (vos) serveur(s) NPS, puis suivre les instructions pour configurer un nouveau certificat à l'aide du guide de déploiement des certificats de serveur.

7. Dans la page de l'Assistant **Modifier les propriétés EAP protégées**, dans **Certificat émis**, vérifiez que le certificat NPS correct est sélectionné, puis procédez comme suit :

> **Notes**
>
> Vérifiez que la valeur de **l'émetteur** est correcte pour le certificat sélectionné dans **certificat émis**. Par exemple, l'émetteur attendu pour un certificat émis par une autorité de certification exécutant active Directory Certificate Services (AD CS) nommée corp\DC1, dans le domaine contoso.com, est **corp-DC1-CA**.

- Pour permettre aux utilisateurs d'utiliser un profil itinérant avec leurs ordinateurs sans fil entre les points d'accès sans avoir à s'authentifier à nouveau chaque fois

qu'ils s'associent à un nouveau point d'accès, sélectionnez **Activer la reconnexion rapide**.

- Pour spécifier que la connexion des clients sans fil mettra fin au processus d'authentification du réseau si le serveur RADIUS ne présente pas de type-longueur-valeur (TLV) de liaison de chiffrement, sélectionnez **Déconnecter les clients sans liaison de chiffrement**.

- Pour modifier les paramètres de stratégie pour le type EAP, dans **types EAP**, cliquez sur **Modifier**, dans **les propriétés EAP MSCHAPv2**, modifiez les paramètres en fonction des besoins, puis cliquez sur **OK**.

8. Cliquez sur **OK**. La boîte de dialogue Modifier les propriétés EAP protégées se ferme, vous renvoyant à l'Assistant **Configurer 802.1X** . Cliquez sur **Suivant**.

9. Dans **Spécifier des groupes d'utilisateurs**, cliquez sur **Ajouter**, puis tapez le nom du groupe de sécurité que vous avez configuré pour vos clients sans fil dans le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Par exemple, si vous avez nommé votre groupe de sécurité sans fil Sans fil, tapez **Groupe sans fil**. Cliquez sur **Suivant**.

10. Cliquez sur **Configurer** pour configurer des attributs standard RADIUS et des attributs spécifiques au fournisseur pour le réseau local virtuel (VLAN) en fonction des besoins, et comme spécifié par la documentation fournie par votre fournisseur de matériel AP sans fil. Cliquez sur **Suivant**.

11. Passez en revue les détails du résumé de la configuration, puis cliquez sur **Terminer**.

Vos stratégies de serveur NPS sont maintenant créées et vous pouvez passer à la jonction des ordinateurs sans fil au domaine.

Joindre de nouveaux ordinateurs sans fil au domaine

La méthode la plus simple pour joindre de nouveaux ordinateurs sans fil au domaine consiste à attacher physiquement l'ordinateur à un segment du réseau local câblé (segment non contrôlé par un commutateur 802.1X) avant de joindre l'ordinateur au domaine. C'est la solution la plus simple car les paramètres de stratégie de groupe sans fil sont automatiquement et immédiatement appliqués et, si vous avez déployé votre propre infrastructure à clé publique, l'ordinateur reçoit le certificat de l'autorité de certification et le place dans le magasin de certificats de l'autorité de certification racine de confiance, ce qui permet au client sans fil de

faire confiance aux serveurs NPS dont les certificats de serveur ont été émis par votre autorité de certification.

De même, une fois qu'un nouvel ordinateur sans fil est joint au domaine, la méthode préférée pour les utilisateurs pour se connecter au domaine consiste à effectuer une connexion câblée au réseau.

Autres méthodes de jonction de domaines

Dans les cas où il n'est pas pratique de joindre des ordinateurs au domaine à l'aide d'une connexion Ethernet câblée, ou dans les cas où l'utilisateur ne peut pas se connecter au domaine pour la première fois à l'aide d'une connexion câblée, vous devez utiliser une autre méthode.

- **Configuration de l'ordinateur du personnel informatique**. Un membre du personnel informatique joint un ordinateur sans fil au domaine et configure un profil d'authentification unique sans fil au démarrage. Avec cette méthode, l'administrateur informatique connecte l'ordinateur sans fil au réseau Ethernet câblé joint l'ordinateur au domaine. Ensuite, l'administrateur distribue l'ordinateur à l'utilisateur. Lorsque l'utilisateur démarre l'ordinateur sans utiliser de connexion câblée, les informations d'identification de domaine qu'il spécifie manuellement pour la connexion de l'utilisateur sont utilisées à la fois pour établir une connexion au réseau sans fil et pour se connecter au domaine.

Pour plus d'informations, consultez la section Joindre le domaine et ouvrir une session à l'aide de la méthode de configuration de l'ordinateur du personnel informatique

- **Configuration du profil sans fil au démarrage par les utilisateurs**. L'utilisateur configure manuellement l'ordinateur sans fil avec un profil sans fil de démarrage et rejoint le domaine, en fonction des instructions fournies par un administrateur informatique. Le profil sans fil de démarrage permet à l'utilisateur d'établir une connexion sans fil, puis de joindre le domaine. Après avoir joint l'ordinateur au domaine et redémarré l'ordinateur, l'utilisateur peut se connecter au domaine à l'aide d'une connexion sans fil et des informations d'identification de son compte de domaine.

Pour plus d'informations, voir la section Joindre le domaine et se connecter à l'aide de la configuration du profil sans fil de démarrage par les utilisateurs.

Joignez le domaine et connectez-vous à l'aide de la méthode de configuration de l'ordinateur du personnel informatique

Les utilisateurs membres du domaine disposant d'ordinateurs clients sans fil joints à un domaine peuvent utiliser un profil sans fil temporaire pour se connecter à un réseau sans fil

authentifié 802.1X sans se connecter au préalable au réseau local câblé. Ce profil sans fil temporaire est appelé *profil sans fil de démarrage*.

Un profil sans fil de démarrage nécessite que l'utilisateur spécifie manuellement ses informations d'identification de compte d'utilisateur de domaine et ne valide pas le certificat du serveur RADIUS (Remote Authentication Dial-In User Service) exécutant le serveur NPS (Network Policy Server).

Une fois la connectivité sans fil établie, la stratégie de groupe est appliquée à l'ordinateur client sans fil et un nouveau profil sans fil est créé automatiquement. La nouvelle stratégie utilise les informations d'identification de l'ordinateur et du compte d'utilisateur pour l'authentification du client.

En outre, dans le cadre de l'authentification mutuelle PEAP-MS-CHAP v2 à l'aide du nouveau profil au lieu du profil de démarrage, le client valide les informations d'identification du serveur RADIUS.

Après avoir joint l'ordinateur au domaine, utilisez cette procédure pour configurer un profil sans fil de démarrage de l'authentification unique, avant de distribuer l'ordinateur sans fil à l'utilisateur membre du domaine.

Pour configurer un profil sans fil de démarrage de l'authentification unique

1. Créez un profil de démarrage à l'aide de la procédure décrite dans ce guide, intitulée Configurer un profil de connexion sans fil pour PEAP-MS-CHAP v2 et utilisez les paramètres suivants :
    - Authentification PEAP-MS-CHAP v2
    - Validez le certificat de serveur RADIUS désactivé
    - Authentification unique activée
2. Dans les propriétés de la stratégie de réseau sans fil dans laquelle vous avez créé le nouveau profil de démarrage, sous l'onglet **Général** , sélectionnez le profil de démarrage, puis cliquez sur **Exporter** pour exporter le profil vers un partage réseau, un lecteur flash USB ou un autre emplacement facilement accessible. Le profil est enregistré en tant que fichier *.xml à l'emplacement que vous spécifiez.
3. Joignez le nouvel ordinateur sans fil au domaine (par exemple, via une connexion Ethernet qui ne nécessite pas d'authentification IEEE 802.1X) et ajoutez le profil sans fil de démarrage à l'ordinateur à l'aide de la commande **netsh wlan add profile**.

> ⓘ **Notes**
>
> Pour plus d'informations, consultez Commandes Netsh pour le Réseau local sans fil (WLAN) à http://technet.microsoft.com/library/dd744890.aspx.

4. Distribuez le nouvel ordinateur sans fil à l'utilisateur en suivant la procédure « Se connecter au domaine à l'aide d'ordinateurs exécutant Windows 10 »

Lorsque l'utilisateur démarre l'ordinateur, Windows l'invite à saisir le nom et le mot de passe de son compte d'utilisateur de domaine. Étant donné que l'authentification unique est activée, l'ordinateur utilise les informations d'identification du compte d'utilisateur de domaine pour établir d'abord une connexion avec le réseau sans fil, puis pour se connecter au domaine.

Connectez-vous au domaine à partir d'ordinateurs fonctionnant sous Windows 10

1. Fermez la session sur l'ordinateur et redémarrez-le.

2. Appuyez sur n'importe quelle touche de votre clavier ou cliquez sur le bureau. L'écran de connexion s'affiche avec un nom de compte d'utilisateur local et un champ d'entrée de mot de passe sous le nom. Ne vous connectez pas avec le compte d'utilisateur local.

3. Dans le coin inférieur gauche de l'écran, cliquez sur **Autre utilisateur**. L'écran de connexion de l'autre utilisateur s'affiche avec deux champs, l'un pour le nom d'utilisateur et l'autre pour le mot de passe. Sous le champ de mot de passe se trouve le texte **Se connecter à :** puis le nom du domaine où l'ordinateur est joint. Par exemple, si votre domaine s'appelle example.com, le texte indique **Se connecter à : EXEMPLE**.

4. Dans **Nom d'utilisateur**, tapez votre nom d'utilisateur de domaine.

5. Dans **Mot de passe**, tapez votre mot de passe de domaine, puis cliquez sur la flèche, ou appuyez sur Entrée.

> ⓘ **Notes**
>
> Si l'écran **Autre utilisateur** n'inclut pas le texte **de connexion à :** et votre nom de domaine, vous devez entrer votre nom d'utilisateur au format *domaine\utilisateur*. Par exemple, pour vous connecter au domaine example.com avec un compte nommé **User-01**, tapez **example\User-01**.

Joignez le domaine et ouvrez une session à l'aide de la configuration du profil sans fil de démarrage par les utilisateurs

Avec cette méthode, vous effectuez les étapes de la section Étapes générales, puis vous fournissez à vos utilisateurs membres du domaine les instructions concernant la configuration manuelle d'un ordinateur sans fil avec un profil sans fil de démarrage. Le profil sans fil de démarrage permet à l'utilisateur d'établir une connexion sans fil, puis de joindre le domaine. Une fois l'ordinateur joint au domaine et redémarré, l'utilisateur peut se connecter au domaine via une connexion sans fil.

Étapes générales

1. Configurez un compte d'administrateur d'ordinateur local, dans le **Panneau de configuration**, pour l'utilisateur.

   > **Important**
   >
   > Pour joindre un ordinateur à un domaine, l'utilisateur doit être connecté à l'ordinateur avec le compte Administrateur local. L'utilisateur doit également fournir les informations d'identification du compte administrateur local pendant le processus de jointure de l'ordinateur au domaine. Par ailleurs, l'utilisateur doit posséder un compte utilisateur dans le domaine auquel il souhaite rattacher l'ordinateur. Au cours du processus de connexion de l'ordinateur au domaine, l'utilisateur sera invité à fournir les informations d'identification du compte de domaine (nom d'utilisateur et mot de passe).

2. Fournissez aux utilisateurs de votre domaine les instructions de configuration d'un profil sans fil de démarrage, comme indiqué dans la procédure suivante **Pour configurer un profil sans fil de démarrage**.

3. En outre, fournissez aux utilisateurs les informations d'identification de l'ordinateur local (nom d'utilisateur et mot de passe) et les informations d'identification de domaine (nom et mot de passe du compte d'utilisateur de domaine) sous la forme *DomainName\UserName*, ainsi que les procédures permettant de « joindre l'ordinateur au domaine » et de « Se connecter au domaine », comme indiqué dans le Guide réseau principal de Windows Server 2016.

Pour configurer un profil sans fil de démarrage

1. Utilisez les informations d'identification fournies par votre administrateur réseau ou un professionnel de l'assistance informatique pour vous connecter à l'ordinateur avec le compte administrateur de l'ordinateur local.

2. Faites un clic droit sur l'icône du réseau sur le bureau, puis cliquez sur **Ouvrir le centre de réseau et de partage**. La boîte de dialogue **Centre Réseau et partage** s'ouvre. Dans **Modifier vos paramètres de mise en réseau**, cliquez sur **Configurer une nouvelle connexion ou un nouveau réseau**. La boîte de dialogue **Configurer une connexion ou un réseau** s'ouvre.

3. Cliquez sur **Se connecter manuellement à un réseau sans fil**, puis sur **Suivant**.

4. Dans **Se connecter manuellement à un réseau sans fil**, dans **Nom du réseau**, tapez le nom SSID du point d'accès.

5. Dans **Le type de sécurité**, sélectionnez le paramètre fourni par votre administrateur.

6. Dans **Le type de chiffrement** et **la clé de sécurité**, sélectionnez ou tapez les paramètres fournis par votre administrateur.

7. Sélectionnez **Démarrer cette connexion automatiquement**, puis cliquez sur **Suivant**.

8. Dans **l'ajout réussi** de *votre SSID réseau*, cliquez sur **Modifier les paramètres de connexion**.

9. Cliquez sur **Modifier les paramètres de connexion**. La boîte de dialogue de propriété du réseau sans fil *Votre réseau SSID* s'ouvre.

10. Cliquez sur l'onglet **Sécurité**, puis, dans **Choisir une méthode d'authentification réseau**, sélectionnez **Protected EAP (PEAP).**

11. Cliquez sur **Paramètres**. La page **Propriétés EAP protégées (PEAP)** s'ouvre.

12. Dans la page **Propriétés EAP protégées (PEAP),** vérifiez que l'option **Valider le certificat de serveur** n'est pas sélectionnée, cliquez deux fois sur **OK**, puis sur **Fermer**.

13. Windows tente ensuite de se connecter au réseau sans fil. Les paramètres du profil sans fil de démarrage spécifient que vous devez fournir vos informations d'identification de domaine. Lorsque Windows vous invite à entrer un nom de compte et un mot de passe, tapez les informations d'identification de votre compte de domaine comme suit : *Nom de domaine\Nom d'utilisateur*, *Mot de passe de domaine*.

Pour joindre un ordinateur au domaine

1. Ouvrez une session sur l'ordinateur avec le compte Administrateur local.

2. Dans la zone de texte de recherche, tapez **PowerShell**. Dans les résultats de la recherche, cliquez avec le bouton droit sur **Windows PowerShell**, puis cliquez sur **Exécuter en tant qu'administrateur**. Windows PowerShell s'ouvre avec une invite élevée.

3. Dans Windows PowerShell, tapez la commande suivante, puis appuyez sur ENTRÉE. Veillez à remplacer la variable DomainName par le nom du domaine que vous souhaitez joindre.

   Add-Computer DomainName

4. Lorsque vous y êtes invité, tapez le nom d'utilisateur et le mot de passe de votre domaine, puis cliquez sur **OK**.

5. Redémarrez l'ordinateur.

6. Suivez les instructions de la section précédente Connectez-vous au domaine à l'aide d'ordinateurs exécutant Windows 10.

Déployer le mode de cache hébergé de BranchCache

Article • 14/04/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Le Guide du réseau de base Windows Server 2016 fournit des instructions sur la planification et le déploiement des composants principaux nécessaires pour un réseau pleinement fonctionnel et un nouveau domaine Active Directory® dans une nouvelle forêt.

Ce guide explique comment tirer parti du réseau de base en fournissant des instructions relatives au déploiement de BranchCache en mode de cache hébergé dans une ou plusieurs filiales avec un contrôleur de domaine en lecture seule, où les ordinateurs clients exécutent Windows 10, Windows 8.1 ou Windows 8, et sont joints au domaine.

> **ⓘ Important**
>
> N'utilisez pas ce guide si vous comptez déployer, ou si vous avez déjà déployé, un serveur BranchCache en mode de cache hébergé, qui exécute Windows Server 2008 R2. Ce guide fournit des instructions pour le déploiement du mode de cache hébergé avec un serveur de cache hébergé qui exécute Windows Server® 2016, Windows Server 2012 R2 ou Windows Server 2012.

Ce guide contient les sections suivantes.

- Conditions préalables à l'utilisation de ce guide
- À propos de ce guide
- Ce que ce guide ne contient pas
- Vues d'ensemble des technologies
- Présentation du déploiement du mode de cache hébergé BranchCache
- Planification du déploiement du mode de cache hébergé BranchCache
- Déploiement de BranchCache en mode de cache hébergé
- Ressources supplémentaires

Conditions préalables à l'utilisation de ce guide

Il s'agit d'un guide qui sert de complément au Guide du réseau de base de Windows Server 2016. Pour déployer BranchCache en mode cache hébergé à l'aide de ce guide, vous devez tout d'abord procéder comme suit.

- Déployez un réseau de base dans votre siège social à l'aide du Guide du réseau de base ou installez les technologies indiquées dans le Guide du réseau de base et faites en sorte qu'elles fonctionnent correctement sur votre réseau. Ces technologies incluent TCP/IP v4, DHCP, Active Directory Domain Services (AD DS) et DNS.

  > ⓘ **Notes**
  >
  > Le **Guide du réseau principal** Windows Server 2016 est disponible dans la bibliothèque technique Windows Server 2016.

- Déployez des serveurs de contenu BranchCache qui exécutent Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012 au siège de votre entreprise ou dans un centre de données cloud. Pour plus d'informations sur le déploiement de serveurs de contenu BranchCache, consultez Ressources supplémentaires.

- Établissez des connexions de réseau étendu (WAN) entre votre filiale, votre siège social et, le cas échéant, vos ressources cloud, en utilisant un réseau privé virtuel (VPN), DirectAccess ou une autre méthode de connexion.

- Déployez dans votre filiale des ordinateurs clients qui exécutent l'un des systèmes d'exploitation suivants, ce qui permet à BranchCache de prendre en charge le service de transfert intelligent en arrière-plan (BITS), le protocole HTTP (Hyper Text Transfer Protocol) et le protocole SMB (Server Message Block).
  - Windows 10 Entreprise
  - Windows 10 Éducation
  - Windows 8.1 Enterprise
  - Windows 8 Entreprise

> ⓘ **Notes**
>
> Dans les systèmes d'exploitation suivants, BranchCache ne prend pas en charge les fonctionnalités HTTP et SMB, mais prend en charge la fonctionnalité BranchCache BITS. - Windows 10 Professionnel, prise en charge du service BITS uniquement -

Windows 8.1 Professionnel, prise en charge du service BITS uniquement - Windows 8 Professionnel, prise en charge du service BITS uniquement

À propos de ce guide

Ce guide s'adresse aux administrateurs réseau et système qui ont suivi les instructions du Guide du réseau de base Windows Server 2016 ou du Guide du réseau de base Windows Server 2012 pour déployer un réseau de base, ou à ceux qui ont déjà déployé les technologies incluses dans le Guide du réseau de base, notamment Active Directory Domain Services (AD DS), DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol) et TCP/IP v4.

Il est recommandé de consulter les guides de conception et de déploiement pour chacune des technologies utilisées dans ce scénario de déploiement. Ces guides peuvent vous aider à déterminer si ce scénario de déploiement fournit les services et la configuration dont vous avez besoin pour le réseau de votre organisation.

Ce que ce guide ne contient pas

Ce guide ne fournit pas d'informations conceptuelles sur BranchCache, notamment des informations sur ses fonctionnalités et ses modes.

Il ne fournit pas d'informations sur la façon de déployer des connexions WAN ou d'autres technologies dans votre filiale, telles que DHCP, un contrôleur de domaine en lecture seule ou un serveur VPN.

Ce guide ne donne pas non plus de conseils sur le matériel à utiliser lorsque vous déployez un serveur de cache hébergé. Il est possible d'exécuter d'autres services et applications sur votre serveur de cache hébergé, toutefois, vous devez déterminer, en fonction de la charge de travail, des capacités matérielles et de la taille de la filiale s'il convient d'installer le serveur de cache hébergé BranchCache sur un ordinateur en particulier et la quantité d'espace disque à allouer au cache. Ce guide ne fournit pas d'instructions sur la configuration des ordinateurs qui exécutent Windows 7. Si vous disposez d'ordinateurs clients qui exécutent Windows 7 dans vos filiales, vous devez les configurer en utilisant d'autres procédures que celles fournies dans ce guide pour les ordinateurs clients qui exécutent Windows 10, Windows 8.1 et Windows 8.

De plus, si vos ordinateurs exécutent Windows 7, vous devez configurer votre serveur de cache hébergé avec un certificat de serveur émis par une autorité de certification approuvée par les ordinateurs clients. (Si tous vos ordinateurs clients exécutent

Windows 10, Windows 8.1 ou Windows 8, vous n'avez pas besoin de configurer le serveur de cache hébergé avec un certificat de serveur.)

> ⓘ **Important**
>
> Si vos serveurs de cache hébergé exécutent Windows Server 2008 R2, utilisez le **Guide de déploiement de BranchCache** pour Windows Server 2008 R2 à la place de ce guide pour déployer BranchCache en mode de cache hébergé. Appliquez les paramètres de stratégie de groupe décrits dans ce guide à tous les clients BranchCache qui exécutent des versions de Windows, de Windows 7 à Windows 10. Vous ne pouvez pas configurer les ordinateurs qui exécutent Windows Server 2008 R2 en suivant les étapes de ce guide.

Vues d'ensemble des technologies

Pour ce guide d'accompagnement, BranchCache est la seule technologie que vous avez besoin d'installer et de configurer. Vous devez exécuter les commandes BranchCache Windows PowerShell sur vos serveurs de contenu, tels que les serveurs web et de fichiers. Toutefois, il est inutile de modifier ou de reconfigurer les serveurs de contenu de toute autre manière. De plus, vous devez configurer les ordinateurs clients à l'aide de la stratégie de groupe sur les contrôleurs de domaine qui exécutent AD DS sur Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012.

BranchCache

BranchCache est une technologie d'optimisation de la bande passante du réseau étendu (WAN), qui est incluse dans certaines éditions des systèmes d'exploitation Windows Server 2016 et Windows 10 ainsi que dans certaines éditions de Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2 et Windows 7.

Pour optimiser la bande passante WAN quand les utilisateurs accèdent à du contenu sur des serveurs distants, BranchCache télécharge le contenu demandé par les clients à partir du siège de votre entreprise ou des serveurs de contenu cloud hébergés, puis met en cache le contenu chez les filiales, ce qui permet aux autres ordinateurs clients des filiales d'accéder au même contenu localement au lieu de passer par le WAN.

Lorsque vous déployez BranchCache en mode cache hébergé, vous devez configurer les ordinateurs clients de la filiale en tant que clients en mode cache hébergé, puis déployer un serveur de cache hébergé dans la filiale. Ce guide montre comment déployer votre

serveur de cache hébergé avec du contenu préhaché et préchargé à partir de vos serveurs de contenu reposant sur des serveurs web et de fichiers.

Stratégie de groupe

La stratégie de groupe dans Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012 est une infrastructure utilisée pour remettre et appliquer une ou plusieurs configurations, voire un ou plusieurs paramètres de stratégie souhaités à un ensemble d'utilisateurs et d'ordinateurs ciblés au sein d'un environnement Active Directory.

Cette infrastructure se compose d'un moteur de stratégie de groupe et de plusieurs extensions côté client (CSE) responsables de la lecture des paramètres de stratégie sur les ordinateurs clients cibles.

Dans ce scénario, la stratégie de groupe permet de configurer les ordinateurs clients membres d'un domaine avec le mode cache hébergé de BranchCache.

Pour continuer avec ce guide, consultez Présentation du déploiement du mode de cache hébergé BranchCache.

Présentation du déploiement du mode de cache hébergé BranchCache

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

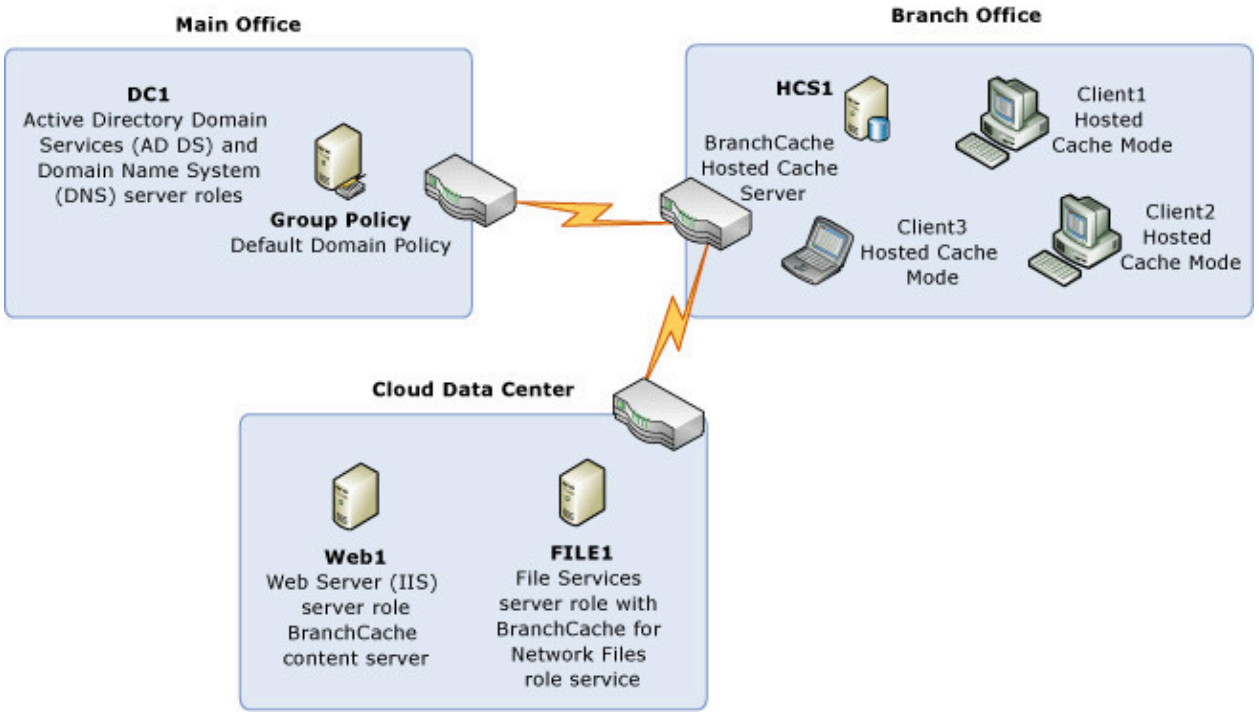
Vous pouvez utiliser ce guide pour déployer un serveur de cache hébergé BranchCache dans une filiale où les ordinateurs sont joints à un domaine. Vous pouvez utiliser cette rubrique pour obtenir une vue d'ensemble du processus de déploiement du mode cache hébergé BranchCache.

Cette vue d'ensemble inclut l'infrastructure BranchCache dont vous avez besoin, ainsi qu'une simple vue d'ensemble pas à pas du déploiement.

Déploiement d'un serveur de cache hébergé Infrastructure

Dans ce déploiement, le serveur de cache hébergé est déployé à l'aide de points de connexion de service dans services de domaine Active Directory (AD DS), et vous avez la possibilité d'utiliser BranchCache dans Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012, pour préchargé le contenu partagé sur le web et les serveurs de contenu basés sur des fichiers, préchargez le contenu sur les serveurs de cache hébergés.

L'illustration suivante montre l'infrastructure requise pour déployer un serveur de cache hébergé BranchCache.



> **ⓘ Important**
>
> Bien que ce déploiement représente des serveurs de contenu dans un centre de données cloud, vous pouvez utiliser ce guide pour déployer un serveur de cache hébergé BranchCache, quel que soit l'endroit où vous déployez vos serveurs de contenu, dans votre bureau principal ou dans un emplacement cloud.

HCS1 dans la succursale

Vous devez configurer cet ordinateur en tant que serveur de cache hébergé. Si vous choisissez de pré-hacher les données du serveur de contenu afin de pouvoir précharger le contenu sur vos serveurs de cache hébergés, vous pouvez importer des packages de données qui contiennent le contenu de vos serveurs web et de fichiers.

WEB1 dans le centre de données cloud

WEB1 est un serveur de contenu prenant en charge BranchCache. Si vous choisissez de pré-hacher les données du serveur de contenu afin de pouvoir précharger le contenu sur vos serveurs de cache hébergés, vous pouvez pré-hacher le contenu partagé sur WEB1, puis créer un package de données que vous copiez dans HCS1.

FILE1 dans le centre de données cloud

FILE1 est un serveur de contenu prenant en charge BranchCache. Si vous choisissez de pré-hacher les données du serveur de contenu afin de pouvoir précharger le contenu

sur vos serveurs de cache hébergé, vous pouvez pré-hacher le contenu partagé sur FILE1, puis créer un package de données que vous copiez dans HCS1.

DC1 dans le bureau principal

DC1 est un contrôleur de domaine et vous devez configurer la stratégie de domaine par défaut, ou une autre stratégie plus appropriée pour votre déploiement, avec branchCache stratégie de groupe paramètres pour activer la découverte automatique du cache hébergé par point de connexion de service.

Lorsque les ordinateurs clients de la branche ont stratégie de groupe actualisés et que ce paramètre de stratégie est appliqué, ils recherchent et commencent automatiquement à utiliser le serveur de cache hébergé dans la filiale.

Ordinateurs clients dans la filiale

Vous devez actualiser stratégie de groupe sur les ordinateurs clients pour appliquer de nouveaux paramètres de stratégie de groupe BranchCache et permettre aux clients de localiser et d'utiliser le serveur de cache hébergé.

Vue d'ensemble du processus de déploiement du serveur de cache hébergé

> ⓘ **Notes**
>
> Les détails de l'exécution de ces étapes sont fournis dans la section **Déploiement du mode de cache hébergé BranchCache**.

Le processus de déploiement d'un serveur de cache hébergé BranchCache se produit au cours des étapes suivantes :

> ⓘ **Notes**
>
> Certaines des étapes ci-dessous sont facultatives, comme celles qui montrent comment pré-hacher et précharger du contenu sur des serveurs de cache hébergé. Lorsque vous déployez BranchCache en mode cache hébergé, vous n'êtes pas obligé de préchargé du contenu sur vos serveurs de contenu Web et de fichiers, de créer un package de données et d'importer le package de données afin de précharger vos serveurs de cache hébergés avec du contenu. Les étapes sont

indiquées comme facultatives dans cette section et dans la section **Déploiement du mode de cache hébergé BranchCache** afin que vous puissiez les ignorer si vous préférez.

1. Sur HCS1, utilisez Windows PowerShell commandes pour configurer l'ordinateur en tant que serveur de cache hébergé et inscrire un point de connexion de service dans Active Directory.

2. (Facultatif) Sur HCS1, si les valeurs par défaut de BranchCache ne correspondent pas à vos objectifs de déploiement pour le serveur et le cache hébergé, configurez la quantité d'espace disque que vous souhaitez allouer au cache hébergé. Configurez également l'emplacement de disque que vous préférez pour le cache hébergé.

3. (Facultatif) Pré-hacher du contenu sur des serveurs de contenu, créer des packages de données et précharger du contenu sur le serveur de cache hébergé.

   Notes

   Le pré-hachage et le préchargement du contenu sur votre serveur de cache hébergé sont facultatifs. Toutefois, si vous choisissez de pré-hacher et de précharger, vous devez effectuer toutes les étapes ci-dessous qui s'appliquent à votre déploiement. (Par exemple, si vous n'avez pas de serveurs Web, vous n'avez pas besoin d'effectuer les étapes liées au pré-hachage et au préchargement du contenu du serveur Web.)

   a. Sur WEB1, pré-hachez le contenu du serveur Web et créez un package de données.

   b. Sur FILE1, pré-hachez le contenu du serveur fichier et créez un package de données.

   c. À partir de WEB1 et FILE1, copiez les packages de données sur le serveur de cache hébergé HCS1.

   d. Sur HCS1, importez les packages de données pour précharger le cache de données.

4. Sur DC1, configurez les ordinateurs clients de succursale joints à un domaine pour le mode de cache hébergé en configurant stratégie de groupe avec les paramètres de stratégie BranchCache.

5. Sur les ordinateurs clients, actualisez stratégie de groupe.

Pour continuer à suivre ce guide, consultez La planification du déploiement du mode de cache hébergé BranchCache.

Commentaires

Cette page a-t-elle été utile ? Yes No

Planification du déploiement du mode de cache hébergé BranchCache

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour planifier votre déploiement de BranchCache en mode Cache hébergé.

> ⓘ **Important**
>
> Votre serveur de cache hébergé doit exécuter Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012.

Avant de déployer votre serveur de cache hébergé, vous devez planifier les éléments suivants :

- Planifier la configuration de base du serveur
- Planifier l'accès au domaine
- Planifier l'emplacement et la taille du cache hébergé
- Planifier le partage vers lequel les packages de serveur de contenu doivent être copiés
- Planifier le pré-hachage et la création de packages de données sur les serveurs de contenu

Planifier la configuration du serveur de base

Si vous envisagez d'utiliser un serveur existant dans votre filiale comme serveur de cache hébergé, vous n'avez pas besoin d'effectuer cette étape de planification, car l'ordinateur est déjà nommé et dispose d'une configuration d'adresse IP.

Après avoir installé Windows Server 2016 sur votre serveur de cache hébergé, vous devez renommer l'ordinateur et attribuer et configurer une adresse IP statique pour l'ordinateur local.

> ⓘ **Notes**

Dans ce guide, le serveur de cache hébergé est nommé HCS1, mais vous devez utiliser un nom de serveur approprié pour votre déploiement.

Planifier l'accès au domaine

Si vous envisagez d'utiliser un serveur existant dans votre filiale comme serveur de cache hébergé, vous n'avez pas besoin d'effectuer cette étape de planification, car l'ordinateur est déjà nommé et dispose d'une configuration d'adresse IP.

Pour ouvrir une session sur un domaine, l'ordinateur doit être membre du domaine et le compte d'utilisateur doit être créé dans les services de domaine Active Directory avant la tentative d'ouverture de session. En outre, vous devez joindre l'ordinateur au domaine avec un compte qui a l'appartenance au groupe appropriée.

Planifier l'emplacement et la taille du cache hébergé

Sur HCS1, déterminez où, sur votre serveur de cache hébergé, vous souhaitez localiser le cache hébergé. Par exemple, choisissez le disque dur, le volume et l'emplacement du dossier où vous envisagez de stocker le cache.

En outre, déterminez le pourcentage d'espace disque que vous souhaitez allouer au cache hébergé.

Planifier le partage vers lequel les packages de serveur de contenu doivent être copiés

Après avoir créé des packages de données sur vos serveurs de contenu, vous devez les copier sur le réseau dans un partage sur votre serveur de cache hébergé.

Planifiez l'emplacement du dossier et les autorisations de partage pour le dossier partagé. En outre, si vos serveurs de contenu hébergent une grande quantité de données et que les packages que vous créez sont des fichiers volumineux, prévoyez d'effectuer l'opération de copie pendant les heures creuses afin que la bande passante WAN ne soit pas consommée par l'opération de copie pendant une période où d'autres utilisateurs doivent utiliser la bande passante pour les opérations métier normales.

Planifier le pré-hachage et la création de packages de données sur les serveurs de contenu

Avant de pré-enregistrer du contenu sur vos serveurs de contenu, vous devez identifier les dossiers et fichiers qui contiennent du contenu que vous souhaitez ajouter au package de données.

En outre, vous devez planifier l'emplacement du dossier local où vous pouvez stocker les packages de données avant de les copier sur le serveur de cache hébergé.

Pour continuer avec ce guide, consultez Déploiement du mode de cache hébergé BranchCache.

Commentaires

Cette page a-t-elle été utile ? Yes No

Déploiement du mode de cache hébergé BranchCache

14/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour obtenir des liens vers les rubriques de procédure détaillées qui vous guideront tout au long du processus de déploiement de BranchCache en mode de cache hébergé.

Suivez ces étapes pour déployer BranchCache en mode de cache hébergé.

- Installer la fonctionnalité BranchCache et configurer le serveur de cache hébergé par le point de connexion de service
- Déplacer et redimensionner le cache hébergé (facultatif)
- Préhacher et précharger du contenu sur le serveur de cache hébergé (facultatif)
- Configurer la découverte automatique du cache hébergé du client par le point de connexion de service

> ⓘ **Notes**
>
> Les procédures décrites dans ce guide n'incluent aucune instruction dans le cas où la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre pour demander votre autorisation de continuer. Si cette boîte de dialogue s’ouvre pendant que vous effectuez les procédures de ce guide et si la boîte de dialogue a été ouverte en réponse à vos actions, cliquez sur **Continuer**.

Pour continuer avec ce guide, consultez Installer la fonctionnalité BranchCache et configurer le serveur de cache hébergé par le point de connexion de service.

Installer la fonctionnalité BranchCache et configurer le serveur de cache hébergé par le point de connexion de service

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour installer la fonctionnalité BranchCache sur votre serveur de cache hébergé, HCS1, et configurer le serveur afin d'inscrire un point de connexion de service (SCP) auprès d'Active Directory Domain Services (AD DS).

Quand vous inscrivez des serveurs de cache hébergé auprès d'un point de connexion de service (SCP) dans AD DS, le point de connexion de service permet aux ordinateurs clients correctement configurés de découvrir automatiquement les serveurs de cache hébergé en interrogeant AD DS au sujet du point de connexion de service. Des instructions sur la façon de configurer les ordinateurs clients pour effectuer cette action sont fournies plus loin dans ce guide.

> **ⓘ Important**
>
> Avant d'effectuer cette procédure, vous devez joindre l'ordinateur au domaine et configurer l'ordinateur avec une adresse IP statique.

Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs.

Pour installer la fonctionnalité BranchCache et configurer le serveur de cache hébergé

1. Sur l'ordinateur serveur, exécutez Windows PowerShell en tant qu'administrateur. Tapez la commande suivante, puis appuyez sur ENTRÉE.

```
Install-WindowsFeature BranchCache
```

2. Pour configurer l'ordinateur en tant que serveur de cache hébergé une fois la fonctionnalité BranchCache installée, et inscrire un point de connexion de service dans AD DS, tapez la commande suivante dans Windows PowerShell, puis appuyez sur ENTRÉE.

```
Enable-BCHostedServer -RegisterSCP
```

3. Pour vérifier la configuration du serveur de cache hébergé, tapez la commande suivante et appuyez sur ENTRÉE.

```
Get-BCStatus
```

   Les résultats de la commande affichent l'état pour tous les aspects de votre installation BranchCache. Voici quelques-uns des paramètres BranchCache et la valeur correcte pour chaque élément :

   - BranchCacheIsEnabled: True
   - HostedCacheServerIsEnabled: True
   - HostedCacheScpRegistrationEnabled: True

4. Pour préparer l'étape de copie des packages de données de vos serveurs de contenu vers vos serveurs de cache hébergé, identifiez un partage existant sur le serveur de cache hébergé, ou créez un dossier et partagez-le afin qu'il soit accessible à partir de vos serveurs de contenu. Une fois que vous avez créé vos packages de données sur vos serveurs de contenu, vous devez copier les packages de données dans ce dossier partagé sur le serveur de cache hébergé.

5. Si vous déployez plusieurs serveurs de cache hébergé, répétez cette procédure sur chaque serveur.

Pour continuer avec ce guide, consultez Déplacer et redimensionner le cache hébergé (facultatif).

Commentaires

Cette page a-t-elle été utile ?

Yes No

Déplacer et redimensionner le cache hébergé (facultatif)

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour déplacer le cache hébergé vers le lecteur et le dossier que vous préférez, et pour spécifier la quantité d'espace disque que le serveur de cache hébergé peut utiliser pour le cache hébergé.

Cette procédure est facultative. Si l'emplacement du cache par défaut (%windir%\ServiceProfiles\NetworkService\AppData\Local\PeerDistPub) et la taille (soit 5 % de l'espace disque total) sont appropriés pour votre déploiement, vous n'avez pas besoin de les modifier.

Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs.

Pour déplacer et redimensionner le cache hébergé

1. Ouvrez Windows PowerShell avec des privilèges d'administrateur.
2. Tapez la commande suivante pour déplacer le cache hébergé vers un autre emplacement sur l'ordinateur local, puis appuyez sur Entrée.

   > **ⓘ Important**
   >
   > Avant d'exécuter la commande suivante, remplacez les valeurs de paramètre, telles que –Path et –MoveTo, par les valeurs appropriées pour votre déploiement.

   ```
   Set-BCCache -Path C:\datacache –MoveTo D:\datacache
   ```

3. Tapez la commande suivante pour redimensionner le cache hébergé, en particulier le cache de données, sur l'ordinateur local. Appuyez sur Entrée.

   > **ⓘ Important**

Avant d'exécuter la commande suivante, remplacez les valeurs de paramètre, telles que -Pourcentage, par des valeurs appropriées pour votre déploiement.

```
Set-BCCache -Percentage 20
```

4. Pour vérifier la configuration du serveur de cache hébergé, tapez la commande suivante et appuyez sur ENTRÉE.

```
Get-BCStatus
```

Les résultats de la commande affichent l'état pour tous les aspects de votre installation BranchCache. Voici quelques-uns des paramètres BranchCache et la valeur correcte pour chaque élément :

- DataCache | CacheFileDirectoryPath : affiche l'emplacement du disque dur qui correspond à la valeur que vous avez fournie avec le paramètre –MoveTo de la commande SetBCCache. Par exemple, si vous avez fourni la valeur D:\datacache, cette valeur s'affiche dans la sortie de la commande.

- DataCache | MaxCacheSizeAsPercentageOfDiskVolume : affiche le nombre qui correspond à la valeur que vous avez fournie avec le paramètre –Pourcentage de la commande SetBCCache. Par exemple, si vous avez fourni la valeur 20, cette valeur s'affiche dans la sortie de la commande.

Pour continuer avec ce guide, consultez Pré-hacher et précharger du contenu sur le serveur de cache hébergé (facultatif).

Préhacher et précharger le contenu sur le serveur de cache hébergé (facultatif)

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser les procédures de cette section pour préhacher du contenu sur vos serveurs de contenu, ajouter le contenu aux packages de données, puis précharger le contenu sur vos serveurs de cache hébergé.

Ces procédures sont facultatives, car vous n'êtes pas obligé de préhacher et de précharger du contenu sur vos serveurs de cache hébergé.

Si vous ne préchargez pas de contenu, les données sont automatiquement ajoutées au cache hébergé au fur et à mesure que les clients les téléchargent via la connexion WAN.

> **Important**
>
> Bien que ces procédures soient facultatives collectivement, si vous décidez de préhacher et de précharger du contenu sur vos serveurs de cache hébergé, l'exécution des deux procédures est nécessaire.

- Créer des packages de données de serveur de contenu Web et de fichier (facultatif)
- Importer des packages de données sur le serveur de cache hébergé (facultatif)

Pour continuer avec ce guide, consultez Créer des packages de données de serveur de contenu pour le contenu web et de fichier (facultatif).

Commentaires

Cette page a-t-elle été utile ? Yes No

Créer des packages de données de serveur de contenu Web et de fichier (facultatif)

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour préhacher du contenu sur les serveurs web et les serveurs de fichiers, puis créer des packages de données à importer sur votre serveur de cache hébergé.

Cette procédure est facultative, car vous n'êtes pas obligé de préhacher et de précharger du contenu sur vos serveurs de cache hébergé. Si vous ne préchargez pas de contenu, les données sont automatiquement ajoutées au cache hébergé au fur et à mesure que les clients les téléchargent via la connexion WAN.

Cette procédure fournit des instructions sur le préhachage de contenu sur les serveurs de fichiers et les serveurs web. Si vous ne disposez pas de l'un de ces types de serveur de contenu, vous n'avez pas à suivre les instructions correspondant à ce type de serveur de contenu.

> **ⓘ Important**
>
> Avant d'effectuer cette procédure, vous devez installer et configurer BranchCache sur vos serveurs de contenu. De plus, si vous comptez changer le secret du serveur sur un serveur de contenu, faites-le avant le préhachage du contenu. La modification du secret du serveur rend les codes de hachage générés non valides.

Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs.

Pour créer des packages de données de serveur de contenu

1. Sur chaque serveur de contenu, recherchez les dossiers et fichiers à préhacher, et à ajouter à un package de données. Identifiez ou créez un dossier dans lequel enregistrer votre package de données plus loin dans cette procédure.

2. Sur l'ordinateur serveur, ouvrez Windows PowerShell avec des privilèges d'administrateur.

3. Effectuez l'une des opérations suivantes, ou les deux, selon les types de serveur de contenu dont vous disposez :

> ⓘ **Notes**
>
> La valeur du paramètre -Path correspond au dossier où se trouve votre contenu. Vous devez remplacer les exemples de valeurs dans les commandes ci-dessous par un emplacement de dossier valide sur votre serveur de contenu, qui contient les données à préhacher et à ajouter à un package.

   - Si le contenu à préhacher se trouve sur un serveur de fichiers, tapez la commande suivante, puis appuyez sur ENTRÉE.

     ```
     Publish-BCFileContent -Path D:\share -StageData
     ```

   - Si le contenu à préhacher se trouve sur un serveur web, tapez la commande suivante, puis appuyez sur ENTRÉE.

     ```
     Publish-BCWebContent –Path D:\inetpub\wwwroot -StageData
     ```

4. Créez le package de données en exécutant la commande suivante sur chacun de vos serveurs de contenu. Remplacez l'exemple de valeur (D:\temp) du paramètre -Destination par l'emplacement que vous avez identifié ou créé au début de cette procédure.

   ```
   Export-BCDataPackage –Destination D:\temp
   ```

5. À partir du serveur de contenu, accédez au partage de vos serveurs de cache hébergé où vous souhaitez précharger le contenu, puis copiez les packages de données sur les partages des serveurs de cache hébergé.

Pour continuer avec ce guide, consultez Importer des packages de données sur le serveur de cache hébergé (facultatif).

Commentaires

Cette page a-t-elle été utile ? Yes No

Importer des packages de données sur le serveur de cache hébergé (facultatif)

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour importer des packages de données et précharger du contenu sur vos serveurs de cache hébergé.

Cette procédure est facultative, car vous n'êtes pas obligé de préhacher et de précharger du contenu sur vos serveurs de cache hébergé.

Si vous ne préchargez pas de contenu, les données sont automatiquement ajoutées au cache hébergé au fur et à mesure que les clients les téléchargent via la connexion WAN.

Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs.

Pour importer des packages de données sur le serveur de cache hébergé

1. Sur l'ordinateur serveur, ouvrez Windows PowerShell avec des privilèges d'administrateur.
2. Tapez la commande suivante, en remplaçant la valeur du paramètre –Path par l'emplacement du dossier où vous avez stocké vos packages de données, puis appuyez sur ENTRÉE.

   ```
   Import-BCCachePackage –Path D:\temp\PeerDistPackage.zip
   ```

3. Si vous avez plusieurs serveurs de cache hébergé sur lesquels vous souhaitez précharger le contenu, effectuez cette procédure sur chaque serveur de cache hébergé.

Pour continuer avec ce guide, consultez Configurer la découverte automatique du cache hébergé client par point de connexion de service.

Commentaires

Cette page a-t-elle été utile ? Yes No

Configurer la découverte automatique du cache hébergé par le point de connexion de service

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Avec cette procédure, vous pouvez utiliser Stratégie de groupe pour activer et configurer le mode de cache hébergé BranchCache sur les ordinateurs joints à un domaine qui exécutent les systèmes d'exploitation Windows compatibles avec BranchCache suivants.

- Windows 10 Entreprise
- Windows 10 Éducation
- Windows 8.1 Entreprise
- Windows 8 Entreprise

> ⓘ **Notes**
>
> Pour configurer des ordinateurs joints à un domaine exécutant Windows Server 2008 R2 ou Windows 7, consultez le Guide de déploiement BranchCache de Windows Server 2008 R2.

L'appartenance aux **administrateurs de domaine** ou équivalente est la condition minimale requise pour effectuer cette procédure.

Utiliser la stratégie de groupe afin de configurer le mode de cache hébergé

1. Sur un ordinateur sur lequel le rôle serveur Des services de domaine Active Directory est installé, ouvrez le Gestionnaire de serveur, sélectionnez le serveur local, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**. La Console de gestion des stratégies de groupe s'ouvre.

2. Dans la console Gestion des stratégies de groupe, développez le chemin suivant : **Forêt :***corp.contoso.com*, **Domaines**, *corp.contoso.com*, **Objets de** stratégie de groupe, où *corp.contoso.com* est le nom du domaine où se trouvent les comptes d'ordinateurs clients BranchCache que vous souhaitez configurer.

3. Cliquez avec le bouton droit sur Objets de stratégie de **groupe**, puis cliquez sur **Nouveau**. La boîte de dialogue **Nouvel objet de stratégie de groupe** s'ouvre. Dans **Name**, tapez un nom pour le nouvel objet de stratégie de groupe (GPO). Par exemple, si vous souhaitez nommer l'objet Ordinateurs clients BranchCache, tapez **Ordinateurs clients BranchCache**. Cliquez sur **OK**.

4. Dans la console Gestion des stratégies de groupe, vérifiez que les **objets de** stratégie de groupe sont sélectionnés, puis dans le volet d'informations, cliquez avec le bouton droit sur l'objet de stratégie de groupe que vous venez de créer. Par exemple, si vous avez nommé votre GPO Ordinateurs clients BranchCache, cliquez avec le bouton droit sur **Ordinateurs clients BranchCache**. Cliquez sur **Modifier**. La console de l'Éditeur de gestion des stratégies de groupe s'ouvre.

5. Dans la console éditeur de gestion des stratégies de groupe, développez le chemin suivant : **Configuration de** l'ordinateur, **Stratégies**, **Modèles d'administration : définitions de stratégie (fichiers ADMX) récupérées à partir de l'ordinateur local**, **réseau**, **BranchCache**.

6. Cliquez sur **BranchCache**, puis dans le volet d'informations, double-cliquez **sur Activer BranchCache**. La boîte de dialogue **Activer BranchCache** s'ouvre.

7. Dans la boîte de dialogue **Activer BranchCache** , cliquez sur **Activé**, puis sur **OK**.

8. Dans la console Éditeur de gestion des stratégies de groupe, vérifiez que **BranchCache** est toujours sélectionné, puis dans le volet d'informations, double-cliquez sur **Activer la découverte automatique du cache hébergé par point de connexion de service**. La boîte de dialogue des paramètres de stratégie s'ouvre.

9. Dans la boîte de dialogue **Activer la découverte automatique du cache hébergé par point de connexion de service** , cliquez sur **Activé**, puis sur **OK**.

10. Pour permettre aux ordinateurs clients de télécharger et de mettre en cache du contenu à partir de serveurs de contenu basés sur le serveur de fichiers BranchCache : dans la console éditeur de gestion des stratégies de groupe, vérifiez que **BranchCache** est toujours sélectionné, puis dans le volet d'informations, double-cliquez sur **BranchCache pour les fichiers réseau**. La boîte de dialogue **Configurer BranchCache pour les fichiers réseau** s'ouvre.

11. Dans la boîte de dialogue **Configurer BranchCache pour les fichiers réseau** , cliquez sur **Activé**. Dans **Options**, tapez une valeur numérique, en millisecondes, pour le temps maximal de latence réseau aller-retour, puis cliquez sur **OK**.

> ⓘ **Notes**

Par défaut, les ordinateurs clients mettent en cache le contenu des serveurs de fichiers si le temps de réponse du réseau aller-retour est supérieure à 80 millisecondes.

12. Pour configurer la quantité d'espace disque alloué sur chaque ordinateur client pour le cache BranchCache : dans la console éditeur de gestion des stratégies de groupe, vérifiez que **BranchCache** est toujours sélectionné, puis dans le volet d'informations, double-cliquez sur **Définir le pourcentage d'espace disque utilisé pour le cache de l'ordinateur client**. La boîte de dialogue **Définir le pourcentage d'espace disque utilisé pour le cache de l'ordinateur client** s'ouvre. Cliquez sur **Activé**, puis, dans **Options** , tapez une valeur numérique qui représente le pourcentage d'espace disque dur utilisé sur chaque ordinateur client pour le cache BranchCache. Cliquez sur **OK**.

13. Pour spécifier l'âge par défaut, en jours, pour lequel les segments sont valides dans le cache de données BranchCache sur les ordinateurs clients : dans la console Éditeur de gestion des stratégies de groupe, vérifiez que **BranchCache** est toujours sélectionné, puis dans le volet d'informations, double-cliquez sur **Définir l'âge des segments dans le cache de données**. La boîte de dialogue **Définir l'âge des segments dans la boîte de dialogue Cache de données** s'ouvre. Cliquez sur **Activé**, puis, dans le volet d'informations, tapez le nombre de jours que vous préférez. Cliquez sur **OK**.

14. Configurez des paramètres de stratégie BranchCache supplémentaires pour les ordinateurs clients en fonction de votre déploiement.

15. Actualisez la stratégie de groupe sur les ordinateurs clients de succursale en exécutant la commande **gpupdate /force** ou en redémarrant les ordinateurs clients.

Votre déploiement en mode cache hébergé BranchCache est maintenant terminé.

Pour plus d'informations sur les technologies de ce guide, consultez Ressources supplémentaires.

Ressources supplémentaires sur BranchCache

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Pour plus d'informations sur les technologies présentées dans ce guide, consultez les ressources suivantes :

- BranchCache dans Windows Server 2016
- Installer et configurer des serveurs de contenu
- Commandes d'environnement réseau et Windows PowerShell pour BranchCache
- Vue d'ensemble de la stratégie de groupe pour Windows Server 2012 R2
- Guide de déploiement de BranchCache pour Windows Server 2008 R2

BranchCache

Article • 09/03/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Cette rubrique, qui s'adresse aux professionnels de l'informatique, présente des informations générales sur BranchCache, notamment les modes BranchCache, les caractéristiques et les capacités, ainsi que les fonctionnalités BranchCache disponibles dans différents systèmes d'exploitation.

Notes

Outre cette rubrique, la documentation BranchCache suivante est disponible.

- **Commandes d’environnement réseau et Windows PowerShell pour BranchCache**
- **Guide de déploiement BranchCache**

À qui BranchCache s’adresse-t-il ?

Si vous êtes administrateur système, architecte de solutions réseau ou de stockage, ou tout autre professionnel de l’informatique, BranchCache peut vous intéresser dans les cas suivants :

- Vous assurez la conception ou la maintenance de l’infrastructure informatique d’une organisation disposant de deux emplacements physiques, ou plus, et d’une connexion de réseau étendu (WAN, Wide Area Network) des filiales vers le siège social.
- Vous assurez la conception ou la maintenance de l’infrastructure informatique d’une organisation qui a déployé des technologies de nuage, et une connexion WAN est utilisée par les travailleurs pour accéder aux données et aux applications se trouvant dans des emplacements distants.
- Vous voulez optimiser l’utilisation de la bande passante du réseau étendu (WAN) en réduisant la quantité de trafic réseau entre les filiales et le siège social.
- Vous avez déployé ou prévoyez de déployer, à votre siège social, des serveurs de contenu qui correspondent aux configurations décrites dans cette rubrique.

- Les ordinateurs clients de vos filiales exécutent Windows 10, Windows 8.1, Windows 8 ou Windows 7 .

Cette rubrique contient les sections suivantes :

- Qu'est-ce que BranchCache ?
- Modes BranchCache
- Serveurs de contenu prenant en charge BranchCache
- BranchCache et le nuage
- Versions des informations de contenu
- Gestion des mises à jour de contenu dans les fichiers par BranchCache
- Guide d'installation de BranchCache
- Versions des systèmes d'exploitation pour BranchCache
- Sécurité BranchCache
- Flux de contenu et processus
- Sécurité du cache

Qu'est-ce que BranchCache ?

BranchCache est une technologie d'optimisation de la bande passante de réseau étendu (WAN) qui est incluse dans certaines éditions des systèmes d'exploitation Windows Server 2016 et Windows 10, ainsi que dans certaines éditions de Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2 et Windows 7. Pour optimiser la bande passante d'un réseau étendu lorsque des utilisateurs accèdent à du contenu sur des serveurs distants, BranchCache extrait le contenu des serveurs de contenu de votre siège social ou du cloud hébergé et le met en cache sur les systèmes des filiales, permettant ainsi aux ordinateurs clients des filiales d'accéder localement au contenu au lieu de passer par le réseau étendu.

Dans les filiales, le contenu est mis en cache sur les serveurs configurés pour héberger le cache ou, si aucun serveur n'est disponible, sur les ordinateurs exécutant Windows 10, Windows 8.1, Windows 8 ou Windows 7. Lorsqu'un ordinateur client demande et reçoit du contenu à partir du siège social et que le contenu est mis en cache dans la filiale, les autres ordinateurs de la même filiale peuvent obtenir le contenu localement au lieu de

télécharger le contenu à partir du serveur de contenu via une liaison de réseau étendu (WAN).

Lorsque des demandes ultérieures pour le même contenu sont effectuées par des ordinateurs clients, ceux-ci téléchargent les *informations de contenu* à partir du serveur au lieu du contenu proprement dit. Les informations de contenu se composent de hachages qui sont calculés à l'aide de segments du contenu d'origine et qui sont extrêmement petits par rapport au contenu des données d'origine. Les ordinateurs clients utilisent alors les informations de contenu pour localiser le contenu dans un cache de la filiale, que le cache se trouve sur un ordinateur client ou sur un serveur. Les ordinateurs clients et les serveurs utilisent également les informations de contenu pour sécuriser le contenu mis en cache afin qu'il ne soit pas accessible par des utilisateurs non autorisés.

BranchCache augmente la productivité de l'utilisateur final en améliorant les délais de réponse aux requêtes des clients et serveurs des filiales ; il peut également participer à l'amélioration des performances du réseau en réduisant le trafic sur les liaisons de réseau étendu (WAN).

Modes BranchCache

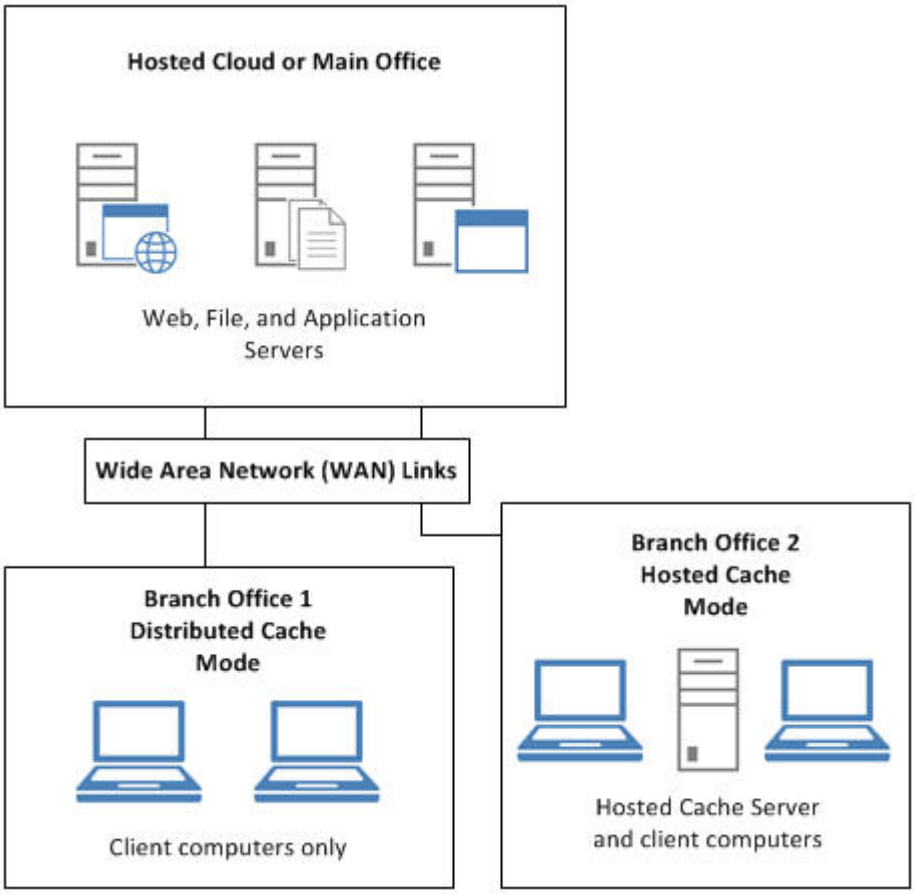
BranchCache a deux modes de fonctionnement : le mode de cache distribué et le mode de cache hébergé.

Lorsque vous déployez BranchCache en mode de cache distribué, le cache de contenu dans la filiale est distribué entre les ordinateurs clients.

Lorsque vous déployez BranchCache en mode de cache hébergé, le cache de contenu dans la filiale est hébergé sur un ou plusieurs ordinateurs serveurs, lesquels sont appelés « serveurs de cache hébergé ».

> ⓘ **Notes**
>
> Vous pouvez déployer BranchCache à l'aide des deux modes. Cependant, un seul mode peut être utilisé par filiale. Par exemple, si vous avez deux filiales, une disposant d'un serveur et l'autre pas, vous pouvez déployer BranchCache en mode de cache hébergé dans le bureau ayant le serveur, tout en déployant BranchCache en mode de cache distribué dans le bureau disposant uniquement d'ordinateurs clients.

Dans l'illustration suivante, BranchCache est déployé dans les deux modes.



Le mode de cache distribué convient mieux aux petites filiales ne disposant pas d'un serveur local à utiliser en tant que serveur de cache hébergé. Le mode de cache distribué vous permet de déployer BranchCache sans matériel supplémentaire dans les filiales.

Si la filiale où vous voulez déployer BranchCache comprend une infrastructure supplémentaire, telle qu'un ou plusieurs serveurs exécutant d'autres charges de travail, le déploiement de BranchCache en mode de cache hébergé est avantageux pour les raisons suivantes :

Disponibilité améliorée du cache

Le mode de cache hébergé augmente l'efficacité du cache, car le contenu est disponible même si le client qui avait demandé et mis en cache les données à l'origine n'est pas connecté. Étant donné que le serveur de cache hébergé est toujours disponible, davantage de contenu est mis en cache, ce qui économise davantage la bande passante du réseau étendu et améliore l'efficacité de BranchCache.

Mise en cache centralisée pour les filiales à plusieurs sous-réseaux

Le mode de cache distribué ne fonctionne que sur un seul sous-réseau. Dans une filiale comportant plusieurs sous-réseaux et qui est configurée pour le mode de cache distribué, un fichier téléchargé sur un sous-réseau ne peut pas être partagé avec des ordinateurs clients se trouvant sur d'autres sous-réseaux.

Par conséquent, les clients sur d'autres sous-réseaux, qui sont dans l'impossibilité de détecter que le fichier a déjà été téléchargé, obtiennent le fichier auprès du serveur de contenu du siège social, en utilisant la bande passante du réseau étendu dans le processus.

Ce n'est cependant pas le cas lorsque vous effectuez le déploiement en mode de cache hébergé : tous les clients d'une filiale comportant plusieurs sous-réseaux peuvent accéder à un seul et même cache, qui est stocké sur le serveur de cache hébergé, même si les clients se trouvent sur des sous-réseaux différents. En outre, BranchCache dans Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012 offre la possibilité de déployer plusieurs serveurs de cache hébergés par filiale.

⊗ Attention

Si vous utilisez BranchCache pour la mise en cache SMB des fichiers et dossiers, ne désactivez pas la fonctionnalité Fichiers hors connexion. Si vous la désactivez, la mise en cache SMB de BranchCache ne fonctionne pas correctement.

Serveurs de contenu prenant en charge BranchCache

Lorsque vous déployez BranchCache, le contenu source est stocké sur des serveurs de contenu prenant en charge BranchCache dans votre siège social ou dans un centre de données cloud. Les types de serveurs de contenu suivants sont pris en charge par BranchCache :

ⓘ Notes

Seul le contenu source, c'est-à-dire le contenu que les ordinateurs clients obtiennent initialement d'un serveur de contenu prenant en charge BranchCache, est accéléré par BranchCache. Le contenu que les ordinateurs clients obtiennent directement auprès d'autres sources, telles que des serveurs Web sur Internet ou Windows Update, n'est pas mis en cache par les ordinateurs clients ou les serveurs de cache hébergé puis partagé avec d'autres ordinateurs de la filiale. Toutefois, si vous voulez accélérer du contenu Windows Update, vous pouvez installer un

serveur d'applications WSUS (Windows Server Update Services) au siège social ou centre de données cloud et le configurer en tant que serveur de contenu BranchCache.

Serveurs Web

Les serveurs web pris en charge incluent les ordinateurs exécutant Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2 sur utilisant le rôle serveur Web Server (IIS) installé et qui utilisent le protocole HTTP (Hypertext Transfer Protocol) ou HTTP Secure (HTTPS).

De plus, la fonctionnalité BranchCache doit être installée sur le serveur Web.

Serveurs de fichiers

Les serveurs de fichiers pris en charge incluent les ordinateurs qui exécutent Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2 qui ont le rôle serveur Services de fichiers et le service de rôle BranchCache pour les fichiers réseau installés.

Ces serveurs de fichiers utilisent le protocole SMB (Server Message Block) pour échanger des informations entre les ordinateurs. Une fois l'installation de votre serveur de fichiers terminée, vous devez également partager des dossiers et permettre la génération de hachage pour les dossiers partagés en utilisant une stratégie de groupe ou une stratégie de l'ordinateur local pour activer BranchCache.

Serveurs d'applications

Les serveurs d'applications pris en charge incluent les ordinateurs qui exécutent Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2 sur lesquels le service BITS (Background Intelligent Transfer Service) est installé et activé.

De plus, la fonctionnalité BranchCache doit être installée sur le serveur d'applications. Comme exemples de serveurs d'application, vous pouvez déployer des serveurs de services Microsoft WSUS (Windows Server Update Services) et de points de distribution de branche Microsoft Endpoint Configuration Manager en tant que serveurs de contenu BranchCache.

BranchCache et le nuage

Avec le nuage, le potentiel de réduire les frais de fonctionnement et de prendre une nouvelle ampleur est énorme. Toutefois, séparer les charges de travail des personnes qui en dépendent peut augmenter les coûts de mise en réseau et affecter la productivité. Les utilisateurs souhaitent des performances élevées et ne se soucient pas de l'endroit où leurs applications et leurs données sont hébergées.

BranchCache peut améliorer les performances d'applications en réseau et réduire la consommation de bande passante à l'aide d'un cache de données partagé. Cette fonctionnalité améliore la productivité dans les filiales et dans les sièges sociaux, où les travailleurs utilisent des serveurs qui sont déployés dans le nuage.

Étant donné que BranchCache ne requiert pas de nouveau matériel ou de modifications de topologie de réseau, c'est une excellente solution pour améliorer la communication entre des bureaux et des nuages aussi bien publics que privés.

> ⓘ **Notes**
>
> Étant donné que certains proxys Web ne peuvent pas traiter les en-têtes d'encodage de contenu non standard, il est recommandé d'utiliser BranchCache avec le protocole HTTPS (Hyper Text Transfer Protocol Secure) et non HTTP.

======= Pour plus d'informations sur les technologies cloud dans Windows Server 2016, consultez SDN (Software Defined Networking).

Versions des informations de contenu

Il existe deux versions des informations de contenu :

- Les informations de contenu qui sont compatibles avec les ordinateurs exécutant Windows Server 2008 R2 et Windows 7 sont appelées version 1, ou V1. Avec la segmentation de fichiers BranchCache V1, les segments de fichiers sont plus grands que dans V2 et ont une taille fixe. En raison des importantes tailles de segments fixes, lorsqu'un utilisateur apporte une modification qui change la longueur du fichier, non seulement le segment avec la modification est invalidé, mais tous les segments jusqu'à la fin du fichier le sont aussi. L'appel suivant pour le fichier modifié par un autre utilisateur de la filiale aboutit donc à des économies de bande passante du réseau étendu réduites, car le contenu modifié et l'intégralité du contenu après la modification sont envoyés par la liaison de réseau étendu.

- Les informations de contenu compatibles avec les ordinateurs exécutant Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server

2012 et Windows 8 sont appelées version 2 ou V2. Les informations de contenu V2 utilisent des segments plus petits de taille variable qui sont plus tolérants aux modifications dans un fichier. Cela augmente la probabilité que des segments d'une version plus ancienne du fichier puissent être réutilisés lorsque les utilisateurs accèdent à une version mise à jour ; ils récupèrent ainsi uniquement la partie modifiée du fichier à partir du serveur de contenu et utilisent moins de bande passante du réseau étendu.

Le tableau suivant fournit des informations sur la version des informations de contenu qui est utilisée selon les systèmes d'exploitation du client, du serveur de contenu et du serveur de cache hébergé que vous utilisez dans votre déploiement BranchCache.

> ⓘ **Notes**
>
> Dans le tableau ci-dessous, l'acronyme « SE » signifie système d'exploitation.

Système d'exploitation client	SE du serveur de contenu	SE du serveur de cache hébergé	Version des informations de contenu
Windows Server 2008 R2 et Windows 7	Windows Server 2012 ou version ultérieure	Windows Server 2012 ou version ultérieure ; aucun pour le mode de cache distribué	V1
Windows Server 2012 ou version ultérieure ; Windows 8 ou version ultérieure	Windows Server 2008 R2	Windows Server 2012 ou version ultérieure ; aucun pour le mode de cache distribué	V1
Windows Server 2012 ou version ultérieure ; Windows 8 ou version ultérieure	Windows Server 2012 ou version ultérieure	Windows Server 2008 R2	V1
Windows Server 2012 ou version ultérieure ; Windows 8 ou version ultérieure	Windows Server 2012 ou version ultérieure	Windows Server 2012 ou version ultérieure ; aucun pour le mode de cache distribué	V2

Lorsque vous avez des serveurs de contenu et des serveurs de cache hébergé qui exécutent Windows Server 2016, Windows Server 2012 R2, et Windows Server 2012, ils utilisent la version des informations de contenu appropriée en fonction du système d'exploitation du client BranchCache qui demande les informations.

Lorsque des ordinateurs exécutant Windows Server 2012 et Windows 8 demandent du contenu, les serveurs de contenu et de cache hébergé utilisent les informations de contenu V2 ; lorsque des ordinateurs exécutant Windows Server 2008 R2 et Windows 7 demandent du contenu, les serveurs de contenu et de cache hébergé utilisent les informations de contenu V1.

> **Important**
>
> Lorsque vous déployez BranchCache en mode de cache distribué, les clients qui utilisent différentes versions des informations de contenu ne partagent pas le contenu entre eux. Par exemple, un ordinateur client exécutant Windows 7 et un ordinateur client exécutant des Windows 10 installés dans la même succursale ne partagent pas de contenu entre eux.

Gestion des mises à jour de contenu dans les fichiers par BranchCache

Quand les utilisateurs des filiales modifient ou mettent à jour le contenu des documents, leurs modifications sont écrites directement sur le serveur de contenu dans le siège social sans implication de BranchCache. Cela est vrai que l'utilisateur ait téléchargé le document à partir du serveur de contenu ou qu'il l'ait obtenu à partir d'un cache hébergé ou distribué dans la filiale.

Quand le fichier modifié est demandé par un autre client dans une filiale, les nouveaux segments du fichier sont téléchargés depuis le serveur du siège social et ajoutés au cache distribué ou hébergé dans cette filiale. Pour cette raison, les utilisateurs des filiales reçoivent toujours les dernières versions du contenu mis en cache.

Guide d’installation de BranchCache

Vous pouvez utiliser le Gestionnaire de serveur dans Windows Server 2016 pour installer la fonctionnalité BranchCache ou le service de rôle BranchCache pour fichiers réseau du rôle de serveur Services de fichiers. Le tableau suivant vous permet de déterminer si vous devez installer le service de rôle ou la fonctionnalité.

Fonctionnalités	Emplacement de l’ordinateur	Installer cet élément BranchCache

Fonctionnalités	Emplacement de l'ordinateur	Installer cet élément BranchCache
Serveur de contenu (serveur d'applications BITS)	Siège social ou centre de données en nuage	Fonctionnalité BranchCache
Serveur de contenu (serveur Web)	Siège social ou centre de données en nuage	Fonctionnalité BranchCache
Serveur de contenu (serveur de fichiers utilisant le protocole SMB)	Siège social ou centre de données en nuage	Service de rôle BranchCache pour fichiers réseau du rôle serveur Services de fichiers
Serveur de cache hébergé	Filiale	Fonctionnalité BranchCache avec le mode de serveur de cache hébergé activé
Ordinateur client prenant en charge BranchCache	Filiale	Aucune installation nécessaire ; activer simplement BranchCache et un mode BranchCache (distribué ou hébergé) sur le client

Pour installer le service de rôle ou la fonctionnalité, ouvrez le Gestionnaire de serveur et sélectionnez les ordinateurs sur lesquels vous voulez activer la fonctionnalité BranchCache. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant **Ajout de rôles et de fonctionnalités** s'ouvre. Lorsque vous exécutez l'Assistant, effectuez les sélections suivantes :

- Dans la page **Sélectionner le type d'installation** de l'Assistant, sélectionnez **Installation basée sur un rôle ou une fonctionnalité**.
- Dans la page de l'Assistant **Sélectionner des rôles de serveur**, si vous installez un serveur de fichiers avec BranchCache, développez **Services de fichiers et de stockage et Services** de **Fichiers et iSCSI**, puis sélectionnez **BranchCache pour fichiers réseau**. Pour économiser de l'espace disque, vous pouvez également sélectionner le service de rôle **Déduplication des données**, puis continuer via l'Assistant jusqu'à l'installation et à l'achèvement. Si vous ne voulez pas installer un serveur de fichiers prenant en charge BranchCache, n'installez pas le rôle Services de fichiers et de stockage avec le service de rôle BranchCache pour fichiers réseau.
- Dans la page **Sélectionner des fonctionnalités** de l'Assistant, si vous installez un serveur de contenu qui n'est pas un serveur de fichiers ou si vous installez un serveur de cache hébergé, sélectionnez **BranchCache**, puis continuez avec

l'Assistant pour installer et terminer. Si vous ne voulez pas installer un serveur de contenu autre qu'un serveur de fichiers ou un serveur de cache hébergé, n'installez pas la fonctionnalité BranchCache.

Versions des systèmes d'exploitation pour BranchCache

Voici la liste des systèmes d'exploitation qui prennent en charge les différents types de fonctionnalités BranchCache.

Systèmes d'exploitation pour les fonctionnalités des ordinateurs clients BranchCache

Les systèmes d'exploitation suivants fournissent à BranchCache la prise en charge du service de transfert intelligent en arrière-plan (BITS), du protocole HTTP (Hyper Text Transfer Protocol) et du bloc de messages serveur (SMB).

- Windows 10 Entreprise
- Windows 10 Éducation
- Windows 8.1 Enterprise
- Windows 8 Entreprise
- Windows 7 Entreprise
- Windows 7 Édition Intégrale

Dans les systèmes d'exploitation suivants, BranchCache ne prend pas en charge les fonctionnalités HTTP et SMB, mais prend en charge la fonctionnalité BranchCache BITS.

- Windows 10 Professionnel, BITS prend uniquement en charge
- Windows 8.1 Professionnel, BITS prend uniquement en charge
- Windows 8 Professionnel, BITS prend uniquement en charge
- Windows 7 Professionnel, BITS prend uniquement en charge

Notes

BranchCache n'est pas disponible par défaut dans les systèmes d'exploitation Windows Server 2008 ou Windows Vista. Toutefois, sur ces systèmes d'exploitation,

si vous téléchargez et installez la mise à jour Windows Management Framework, la fonctionnalité BranchCache est disponible uniquement pour le protocole BITS (Background Intelligent Transfer Service). Pour plus d'informations et pour télécharger Windows Management Framework, consultez **Windows Management Framework (Windows PowerShell 2.0, WinRM 2.0 et BITS 4.0)** à l'adresse /powershell/scripting/windows-powershell/install/installing-the-windows-powershell-2.0-engine.

Systèmes d'exploitation pour les fonctionnalités du serveur de contenu BranchCache

Vous pouvez utiliser les familles de systèmes d'exploitation Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012 en tant que serveurs de contenu BranchCache.

De plus, les membres de la famille de systèmes d'exploitation Windows Server 2008 R2 peuvent aussi être utilisés comme serveurs de contenu BranchCache, avec les exceptions suivantes :

- BranchCache n'est pas pris en charge dans les installations Server Core de Windows Server 2008 R2 Enterprise avec Hyper-V.
- BranchCache n'est pas pris en charge dans les installations Server Core de Windows Server 2008 R2 Datacenter avec Hyper-V.

Systèmes d'exploitation pour les fonctionnalités de serveur de cache hébergé de BranchCache

Vous pouvez utiliser les familles de systèmes d'exploitation Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012 en tant que serveurs de cache hébergés BranchCache.

De plus, les systèmes d'exploitation Windows Server 2008 R2 suivants peuvent aussi être utilisés comme serveurs de cache hébergé BranchCache :

- Windows Server 2008 R2 Entreprise
- Windows Server 2008 R2 Enterprise avec Hyper-V
- Windows Server 2008 R2 Entreprise Installation minimale de serveur
- Windows Server 2008 R2 Entreprise Installation minimale de serveur avec Hyper-V

- Windows Server 2008 R2 pour les systèmes Itanium
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 R2 Datacenter avec Hyper-V
- Windows Server 2008 R2 Datacenter Installation minimale de serveur avec Hyper-V

Sécurité BranchCache

BranchCache implémente une approche de sécurisation de par sa conception, qui fonctionne de façon transparente avec vos architectures de sécurité réseau existantes, sans qu'un équipement supplémentaire ou une configuration supplémentaire complexe de la sécurité ne soit nécessaire.

BranchCache est non invasif et ne modifie aucun processus d'authentification ou d'autorisation Windows. Une fois que vous avez déployé BranchCache, l'authentification continue à être effectuée à l'aide d'informations d'identification de domaine, et le fonctionnement de l'autorisation avec des listes de contrôles d'accès reste inchangé. De plus, les autres configurations continuent à fonctionner exactement de la même façon qu'avant le déploiement de BranchCache.

Le modèle de sécurité BranchCache est basé sur la création de métadonnées, qui prennent la forme d'une série de hachages. Ces hachages sont également appelés « informations de contenu ».

Une fois les informations de contenu créées, elles sont utilisées dans des échanges de messages BranchCache à la place des données réelles, et elles sont échangées à l'aide des protocoles pris en charge (HTTP, HTTPS et SMB).

Les données mises en cache sont maintenues chiffrées et ne sont pas accessibles par des clients qui ne disposent pas d'une autorisation pour accéder au contenu de la source d'origine. Les clients doivent être authentifiés et autorisés par la source de contenu d'origine pour pouvoir récupérer les métadonnées du contenu. De plus, ils doivent posséder les métadonnées du contenu pour accéder au cache dans le bureau local.

Comment BranchCache génère-t-il les informations de contenu ?

Étant donné que les informations de contenu sont créées à partir de plusieurs éléments, la valeur des informations de contenu est toujours unique. Ces éléments sont les

suivants :

- Le contenu réel (tel que des pages Web ou des fichiers partagés) duquel les hachages sont dérivés.
- Des paramètres de configuration, tels que l'algorithme de hachage et la taille de bloc. Pour générer les informations de contenu, le serveur de contenu divise le contenu en segments, puis subdivise ces segments en blocs. BranchCache utilise des hachages de chiffrement sécurisés pour identifier et vérifier chaque bloc et chaque segment, en prenant en charge l'algorithme de hachage SHA256.
- Un secret de serveur. Tous les serveurs de contenu doivent être configurés avec un secret de serveur, qui est une valeur binaire de longueur arbitraire.

> ⓘ **Notes**
>
> L'utilisation d'un secret de serveur garantit que les ordinateurs clients ne peuvent pas générer eux-mêmes les informations de contenu. Cela empêche les utilisateurs malveillants d'utiliser des attaques en force brute avec les ordinateurs clients prenant en charge BranchCache pour deviner des modifications mineures entre les versions dans les cas où le client avait accès à la version précédente mais n'a pas accès à la version actuelle.

Détails sur les informations de contenu

BranchCache utilise le secret de serveur comme clé afin de dériver un hachage spécifique au contenu qui est envoyé aux clients autorisés. L'application d'un algorithme de hachage au secret de serveur et au hachage de données combinés génère ce hachage.

Ce hachage est appelé « secret de segment ». BranchCache utilise des secrets de segment pour sécuriser les communications. De plus, BranchCache crée une liste des hachages de blocs, qui est la liste des blocs de données hachés, et le hachage de données, qui est généré en hachant la liste des hachages de blocs.

Les informations de contenu incluent les éléments suivants :

- La liste des hachages de blocs :

  `BlockHashi = Hash(dataBlocki) 1<=i<=n`

- Le hachage de données (HoD) :

`HoD = Hash(BlockHashList)`

- Le secret de segment (Kp) :

  `Kp = HMAC(Ks, HoD)`

BranchCache utilise le protocole de mise en cache de contenu des homologues (Peer Content Caching) et le protocole de récupération (Retrieval) Framework pour implémenter les processus requis pour garantir la mise en cache et la récupération sécurisées de données entre des caches de contenu.

De plus, BranchCache gère les informations de contenu avec le même niveau de sécurité que lors de la gestion et de la transmission du contenu réel lui-même.

Flux de contenu et processus

Le flux d'informations de contenu et de contenu réel est divisé en quatre phases :

1. Processus BranchCache : demander du contenu
2. Processus BranchCache : localiser du contenu
3. Processus BranchCache : récupérer du contenu
4. Processus BranchCache : mettre en cache du contenu

Les sections suivantes décrivent ces différentes phases.

Processus BranchCache : demander du contenu

Au cours de la première phase, l'ordinateur client de la filiale demande du contenu, tel qu'un fichier ou une page Web, d'un serveur de contenu situé dans un emplacement distant, tel qu'un siège social. Le serveur de contenu vérifie que l'ordinateur client est autorisé à recevoir le contenu demandé. Si l'ordinateur client est autorisé, et que le serveur de contenu et le client prennent tous les deux en charge BranchCache, le serveur de contenu génère des informations de contenu.

Le serveur de contenu envoie alors les informations de contenu à l'ordinateur client en utilisant le même protocole que celui qui aurait été utilisé pour le contenu réel.

Par exemple, si l'ordinateur client a demandé une page Web via HTTP, le serveur de contenu envoie les informations de contenu en utilisant HTTP. C'est pourquoi les garanties de sécurité du contenu au niveau du réseau et les informations de contenu sont identiques.

Une fois la partie initiale des informations de contenu (hachage de données + secret de segment) reçue, l'ordinateur client effectue les actions suivantes :

- Il utilise le secret de segment (Kp) comme clé de chiffrement (Ke).
- Il génère l'ID de segment (HoHoDk) à partir des valeurs HoD et Kp :

  `HoHoDk = HMAC(Kp, HoD + C), where C is the ASCII string "MS_P2P_CACHING" with NUL terminator.`

À ce stade, la principale menace est le risque encouru par le secret de serveur. Toutefois, BranchCache chiffre les blocs de données de contenu pour protéger le secret de segment. Pour cela, cette fonctionnalité utilise la clé de chiffrement qui est dérivée du secret de segment du segment de contenu dans lequel se trouvent les blocs de contenu.

Cette approche garantit qu'une entité qui n'est pas en possession du secret de serveur ne peut pas découvrir le contenu réel d'un bloc de données. Le secret de segment est traité avec le même niveau de sécurité que le segment en texte brut lui-même, car le fait de connaître le secret de segment d'un segment donné permet à une entité d'obtenir le segment auprès d'homologues, puis de le déchiffrer. La connaissance du secret de serveur ne produit pas immédiatement un texte brut particulier, mais permet de dériver certains types de données du texte chiffré, puis d'exposer éventuellement certaines données partiellement connues à une attaque de déchiffrement en force brute. Par conséquent, le secret de serveur doit être maintenu confidentiel.

Processus BranchCache : localiser du contenu

Une fois les informations de contenu reçues par l'ordinateur client, le client utilise l'ID de segment pour localiser le contenu demandé dans le cache de la filiale locale, que le cache soit distribué entre les ordinateurs clients ou situé sur un serveur de cache hébergé.

Si l'ordinateur client est configuré pour le mode de cache hébergé, il est configuré avec le nom d'ordinateur du serveur de cache hébergé et contacte ce serveur pour récupérer le contenu.

Toutefois, si l'ordinateur client est configuré pour le mode de cache distribué, il est possible que le contenu soit stocké dans plusieurs caches de plusieurs ordinateurs de la filiale. Avant que le contenu soit récupéré, l'ordinateur client doit découvrir où il se trouve.

Lorsque les ordinateurs clients sont configurés pour le mode de cache distribué, ils localisent le contenu en utilisant un protocole de découverte basé sur le protocole WS-

Discovery (Web Services Dynamic Discovery). Les clients envoient des messages d'exploration (Probe) de multidiffusion WS-Discovery pour découvrir le contenu mis en cache sur le réseau. Les messages d'exploration incluent l'ID de segment, ce qui permet aux clients de vérifier si le contenu demandé correspond au contenu stocké dans leur cache. Les clients qui reçoivent le message d'exploration initial répondent au client effectuant la demande avec des messages de type Probe-Match de monodiffusion si l'ID de segment correspond au contenu mis en cache localement.

La réussite du processus WS-Discovery dépend du fait que le client qui effectue la découverte dispose des informations de contenu correctes, lesquelles ont été fournies par le serveur de contenu, pour le contenu qu'il demande.

La principale menace pour les données pendant la phase de demande de contenu est la divulgation d'informations, car l'accès aux informations de contenu implique un accès autorisé au contenu. Pour réduire ce risque, le processus de découverte ne divulgue pas les informations de contenu, hormis l'ID de segment, ce qui ne révèle rien sur le segment en texte brut dans lequel se trouve le contenu

En outre, un autre ordinateur client exécuté par un utilisateur malveillant sur le même sous-réseau de réseau peut voir le trafic de découverte BranchCache vers la source de contenu d'origine passant par le routeur.

Si le contenu demandé est introuvable dans la filiale, le client demande le contenu directement à partir du serveur de contenu via la liaison de réseau étendu (WAN).

Une fois le contenu reçu, il est ajouté au cache local, soit sur l'ordinateur client, soit sur un serveur de cache hébergé. Dans ce cas, les informations de contenu empêchent un client ou un serveur de cache hébergé d'ajouter au cache local du contenu qui ne correspond pas aux hachages. Le processus de vérification du contenu en faisant correspondre les hachages garantit que seul le contenu valide est ajouté au cache, protégeant ainsi l'intégrité du cache local.

Processus BranchCache : récupérer du contenu

Une fois qu'un ordinateur client a localisé le contenu souhaité sur l'hôte de contenu, lequel est soit un serveur de cache hébergé soit un ordinateur client en mode de cache distribué, il commence le processus de récupération du contenu.

L'ordinateur client commence par envoyer une demande à l'hôte de contenu pour le premier bloc dont il a besoin. La demande contient l'ID de segment et la plage de blocs qui identifient le contenu souhaité. Étant donné qu'un seul bloc est retourné, la plage de blocs contient un seul bloc. (Les demandes pour plusieurs blocs ne sont actuellement

pas prises en charge.) Le client stocke également la demande dans sa liste des demandes en attente locale.

Lorsqu'il reçoit un message de demande valide d'un client, l'hôte de contenu vérifie si le bloc spécifié dans la demande existe dans le cache de contenu de l'hôte de contenu.

Si l'hôte de contenu est en possession du bloc de contenu, il envoie une réponse contenant l'ID de segment, l'ID de bloc, le bloc de données chiffré et le vecteur d'initialisation utilisé pour le chiffrement du bloc.

Si l'hôte de contenu n'est pas en possession du bloc de contenu, il envoie un message de réponse vide. Cela informe l'ordinateur client que l'hôte de contenu ne dispose pas du bloc demandé. Un message de réponse vide contient l'ID de segment et l'ID de bloc du bloc demandé, ainsi qu'un bloc de données de taille zéro.

Lorsque l'ordinateur client reçoit la réponse de l'hôte de contenu, le client vérifie que le message correspond à un message de demande figurant dans sa liste des demandes non traitées. (L'ID de segment et l'index de bloc doivent correspondre à ceux d'une demande non traitée.)

Si ce processus de vérification échoue et que l'ordinateur client n'a pas de message de demande correspondant dans sa liste de demandes non traitées, l'ordinateur client ignore le message.

Si ce processus de vérification réussit et que l'ordinateur client a un message de demande correspondant dans sa liste de demandes non traitées, l'ordinateur client déchiffre le bloc. Le client valide alors le bloc déchiffré par rapport au hachage de bloc approprié présent dans les informations de contenu initialement obtenues par le client auprès du serveur de contenu d'origine.

Si la validation du bloc réussit, le bloc déchiffré est stocké dans le cache.

Ce processus est répété jusqu'à ce que le client ait tous les blocs requis.

Notes

Si les segments de contenu complets n'existent pas sur un ordinateur, le protocole de récupération récupère et assemble le contenu à partir d'une combinaison de sources : un ensemble d'ordinateurs clients en mode de cache distribué, un serveur de cache hébergé et, si les caches des filiales ne contiennent pas le contenu complet, le serveur de contenu d'origine installé au siège social.

Avant que BranchCache envoie les informations de contenu ou le contenu, les données sont chiffrées. BranchCache chiffre le bloc dans le message de réponse. Dans Windows 7, l'algorithme de chiffrement par défaut utilisé par BranchCache est AES-128, la clé de chiffrement est Ke et la taille de clé est 128 bits, comme stipulé par l'algorithme de chiffrement.

BranchCache génère un vecteur d'initialisation qui convient à l'algorithme de chiffrement et utilise la clé de chiffrement pour chiffrer le bloc. BranchCache enregistre alors l'algorithme de chiffrement et le vecteur d'initialisation dans le message.

Les serveurs et les clients ne s'échangent, ne partagent et ne s'envoient jamais la clé de chiffrement. Le client reçoit la clé de chiffrement du serveur de contenu qui héberge le contenu source. À l'aide de l'algorithme de chiffrement et du vecteur d'initialisation qu'il a reçu du serveur, il déchiffre alors le bloc. Aucune autre authentification ou autorisation explicite n'est intégrée au protocole de téléchargement.

Menaces pour la sécurité

À ce stade, les principales menaces de sécurité sont les suivantes :

- Falsification des données :

  Un client fournissant des données à un demandeur falsifie les données. Le modèle de sécurité BranchCache utilise des hachages pour vérifier que ni le client ni le serveur n'a altéré les données.

- Divulgation d'informations :

  BranchCache envoie du contenu chiffré à tout client qui spécifie l'ID de segment approprié. Étant donné que les ID de segment sont publics, tous les clients peuvent recevoir du contenu chiffré. Toutefois, si un utilisateur malveillant obtient du contenu chiffré, il doit connaître la clé de chiffrement pour le déchiffrer. Le protocole de couche supérieure effectue l'authentification, puis donne les informations de contenu au client authentifié et autorisé. La sécurité des informations de contenu est équivalente à la sécurité fournie au contenu lui-même, et BranchCache n'expose jamais les informations de contenu.

  Un agresseur « écoute » le réseau afin d'obtenir du contenu. BranchCache chiffre tous les transferts entre les clients à l'aide du chiffrement AES128, où la clé secrète est Ke, ce qui empêche la détection de données sur le réseau. Les informations de contenu qui sont téléchargées à partir du serveur de contenu sont protégées exactement de la même manière que les données elles-mêmes l'auraient été. Elles

ne sont donc protégées ni plus ni moins contre la divulgation d'informations que si BranchCache n'avait pas du tout été utilisé.

- Refus de service :

  Un client est submergé de demandes de données. Les protocoles BranchCache incorporent des compteurs de gestion des files d'attente et des minuteurs pour éviter que les clients soient surchargés.

Processus BranchCache : mettre en cache du contenu

Sur les ordinateurs clients en mode de cache distribué et sur les serveurs de cache hébergé situés dans les filiales, des caches de contenu sont progressivement intégrés à mesure que du contenu est récupéré via des liaisons de réseau étendu (WAN).

Lorsque des ordinateurs clients sont configurés avec le mode de cache hébergé, ils ajoutent le contenu à leur propre cache local et proposent également des données au serveur de cache hébergé. Le protocole de cache hébergé offre un mécanisme permettant aux clients d'informer le serveur de cache hébergé sur la disponibilité du contenu et des segments.

Pour télécharger du contenu vers le serveur de cache hébergé, le client informe le serveur qu'il a un segment disponible. Le serveur de cache hébergé récupère alors toutes les informations de contenu associées au segment proposé, et télécharge les blocs présents dans le segment dont il a réellement besoin. Ce processus est répété jusqu'à ce que le client n'ait plus de segments à proposer au serveur de cache hébergé.

Pour mettre à jour le serveur de cache hébergé en utilisant le protocole de cache hébergé, les exigences suivantes doivent être satisfaites :

- L'ordinateur client doit disposer d'un ensemble de blocs contenus dans un segment qu'il peut proposer au serveur de cache hébergé. Le client doit fournir les informations de contenu correspondant au segment proposé ; elles sont constituées de l'ID de segment, du hachage de données du segment, du secret de segment et de la liste de tous les hachages de blocs contenus dans le segment.

- Pour les serveurs de cache hébergé qui exécutent Windows Server 2008 R2, un certificat de serveur de cache hébergé et une clé privée associée sont requis, et l'autorité de certification ayant délivré le certificat doit être approuvée par les ordinateurs clients dans la filiale. Cela permet au client et au serveur de participer correctement à l'authentification de serveur HTTPS.

> **Important**
>
> Les serveurs de cache hébergé qui exécutent Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012 ne nécessitent pas de certificat de serveur de cache hébergé et de clé privée associée.

- L'ordinateur client est configuré avec le nom d'ordinateur du serveur de cache hébergé et le numéro de port TCP (Transmission Control Protocol) sur lequel le serveur de cache hébergé écoute le trafic BranchCache. Le certificat du serveur de cache hébergé est lié à ce port. Le nom d'ordinateur du serveur de cache hébergé peut être un nom de domaine complet (FQDN) si le serveur de cache hébergé est un ordinateur membre d'un domaine ; ou ce peut être le nom NetBIOS de l'ordinateur si le serveur de cache hébergé n'est pas membre d'un domaine.
- L'ordinateur client écoute activement les demandes de blocs entrantes. Le port sur lequel il effectue l'écoute est passé en tant que partie des messages d'offre envoyés par le client au serveur de cache hébergé. Cela permet au serveur de cache hébergé d'utiliser les protocoles BranchCache pour se connecter à l'ordinateur client afin de récupérer des blocs de données se trouvant dans le segment.
- Le serveur de cache hébergé commence à écouter les requêtes HTTP entrantes quand il est initialisé.
- Si le serveur de cache hébergé est configuré pour exiger l'authentification de l'ordinateur client, le client et le serveur de cache hébergé doivent tous les deux prendre en charge l'authentification HTTPS.

Remplissage du cache en mode cache hébergé

Le processus d'ajout de contenu au cache du serveur de cache hébergé de la filiale commence quand le client envoie un message INITIAL_OFFER_MESSAGE, lequel inclut l'ID de segment. L'ID de segment dans la demande INITIAL_OFFER_MESSAGE est utilisé pour récupérer le hachage de données du segment, la liste des hachages de blocs et le secret de segment correspondants à partir du cache de blocs du serveur de cache hébergé. Si le serveur de cache hébergé dispose déjà de toutes les informations de contenu pour un segment particulier, la réponse au message INITIAL_OFFER_MESSAGE est OK, et aucune demande de téléchargement de blocs ne se produit.

Si le serveur de cache hébergé ne dispose pas de tous les blocs de données proposés qui sont associés aux hachages du segment, la réponse au message INITIAL_OFFER_MESSAGE est INTERESTED. Le client envoie alors un message

SEGMENT_INFO_MESSAGE décrivant l'unique segment qui est proposé. Le serveur de cache hébergé répond par un message OK et commence le téléchargement des blocs manquants à partir de l'ordinateur client émetteur de l'offre.

Le hachage de données du segment, la liste des hachages de blocs et le secret de segment sont utilisés pour garantir que le contenu qui est téléchargé n'a pas été falsifié ou altéré. Les blocs téléchargés sont alors ajoutés au cache de blocs du serveur de cache hébergé.

Sécurité du cache

Cette section fournit des informations sur la façon dont BranchCache sécurise les données mises en cache sur les ordinateurs clients et les serveurs de cache hébergé.

Sécurité du cache sur l'ordinateur client

La falsification constitue la plus grande menace pour les données stockées dans le cache BranchCache. Si une personne malveillante peut falsifier le contenu et les informations de contenu stockées dans le cache, il est possible d'utiliser cette faille pour essayer de lancer une attaque contre les ordinateurs qui utilisent BranchCache. Des personnes malveillantes peuvent initier une attaque en insérant un logiciel malveillant à la place d'autres données. BranchCache réduit ce risque en validant tout le contenu à l'aide des hachages de blocs se trouvant dans les informations de contenu. Si une personne malveillante tente d'altérer ces données, elles sont ignorées et sont remplacées par les données valides provenant de la source d'origine.

La divulgation d'informations représente une menace secondaire pour les données stockées dans le cache BranchCache. En mode de cache distribué, le client met en cache uniquement le contenu qu'il a lui-même demandé ; toutefois, les données, qui sont stockées en texte clair, courent un risque. Pour limiter l'accès au cache uniquement au service BranchCache, le cache local est protégé par les autorisations du système de fichiers qui sont spécifiées dans une liste de contrôle d'accès.

Même si la liste de contrôle d'accès est efficace pour empêcher des utilisateurs non autorisés d'accéder au cache, il est possible qu'un utilisateur disposant de privilèges d'administrateur accède au cache en modifiant manuellement les autorisations spécifiées dans la liste de contrôle d'accès. BranchCache ne protège pas contre une utilisation malveillante d'un compte administratif.

Les données stockées dans le cache de contenu ne sont pas chiffrées ; par conséquent, si la perte de données représente un problème, vous pouvez utiliser des technologies de chiffrement telles que BitLocker ou le système de fichiers EFS (Encrypting File System).

Le cache local utilisé par BranchCache n’augmente pas la menace de divulgation d’informations que représente un ordinateur de la filiale ; il contient uniquement des copies de fichiers qui résident non chiffrés ailleurs sur le disque.

Il est particulièrement important de chiffrer la totalité du disque dans les environnements dans lesquels la sécurité physique des clients est difficile à garantir. Par exemple, le chiffrement de la totalité du disque permet de sécuriser des données sensibles sur des ordinateurs portables qui peuvent être sortis de l’environnement de la filiale.

Sécurité du cache sur le serveur de cache hébergé

En mode de cache hébergé, la plus grande menace pour la sécurité du serveur de cache hébergé est la divulgation d’informations. Dans un environnement de cache hébergé, BranchCache se comporte de la même manière qu’en mode de cache distribué, avec l’autorisation du système de fichiers qui protège les données mises en cache. La différence est que le serveur de cache hébergé stocke tout le contenu que n’importe quel ordinateur prenant en charge BranchCache dans la filiale demande, et non pas uniquement les données demandées par un seul client. Les conséquences d’une intrusion non autorisée dans ce cache pourraient être beaucoup plus graves, car davantage de données sont menacées.

Dans un environnement de cache hébergé où le serveur de cache hébergé exécute Windows Server 2008 R2, l’utilisation de technologies de chiffrement telles que BitLocker ou EFS est conseillée si l’un des clients de la filiale peut accéder à des données sensibles sur la liaison WAN. Il est également nécessaire d’empêcher un accès physique au cache hébergé, car le chiffrement de disque fonctionne uniquement lorsque l’ordinateur est éteint au moment où la personne malveillante y accède physiquement. Si l’ordinateur est allumé ou en mode veille, la protection offerte par le chiffrement de disque est faible.

> **Notes**
>
> Les serveurs de cache hébergé qui exécutent Windows Server 2016, Windows Server 2012 R2, ou Windows Server 2012 chiffrent toutes les données du cache par défaut ; le recours à des technologies de chiffrement supplémentaire n'est donc pas nécessaire.

Même si un client est configuré en mode de cache hébergé, il met toujours en cache les données localement, et vous pouvez prendre des mesures pour protéger le cache local en plus du cache situé sur le serveur de cache hébergé.

Commandes BranchCache Network Shell et Windows PowerShell

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Dans Windows Server, vous pouvez configurer et gérer BranchCache en utilisant les commandes Windows PowerShell ou les commandes d'environnement réseau (Netsh) pour BranchCache.

Dans les prochaines versions de Windows, il se peut que Microsoft supprime la fonctionnalité Netsh pour BranchCache. Microsoft vous recommande de passer à Windows PowerShell si vous utilisez actuellement la fonctionnalité Netsh pour configurer et gérer BranchCache, et d'autres technologies de mise en réseau.

Les informations de référence sur les commandes Windows PowerShell et les commandes Netsh sont disponibles aux emplacements suivants. Bien que les deux références de commande aient été publiées pour les systèmes d'exploitation antérieurs à Windows Server 2016, elles sont exactes pour ce système d'exploitation.

- Commandes netsh pour BranchCache
- Applets de commande BranchCache dans Windows PowerShell

> **Conseil**
>
> Pour afficher la liste des commandes Windows PowerShell pour BranchCache, à l'invite Windows PowerShell tapez `Get-Command -Module BranchCache`, puis appuyez sur ENTRÉE.

Last updated on 31/10/2025

Guide de déploiement BranchCache

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Vous pouvez utiliser ce guide pour découvrir comment déployer BranchCache dans Windows Server 2016.

En plus de cette rubrique, ce guide contient les sections suivantes.

- Choix d'une conception BranchCache
- Déployer BranchCache

Présentation du déploiement de BranchCache

BranchCache est une technologie d'optimisation de la bande passante des réseaux étendus (WAN), disponible dans certaines éditions de Windows Server 2016, Windows Server® 2012 R2, Windows Server® 2012, Windows Server® 2008 R2 et les systèmes d'exploitation clients Windows associés.

Pour optimiser la bande passante du réseau étendu, BranchCache copie le contenu des serveurs de contenu de votre site principal et le met en cache dans les filiales, permettant ainsi aux ordinateurs clients des filiales d'accéder localement au contenu au lieu de passer par le réseau étendu.

Dans les filiales, le contenu est mis en cache sur les serveurs qui exécutent la fonctionnalité BranchCache de Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2. Ou, s'il n'y a pas de serveurs disponibles dans la filiale, le contenu est mis en cache sur les ordinateurs clients qui exécutent Windows 10®, Windows® 8.1, Windows 8 ou Windows 7®.

Lorsqu'un ordinateur client demande et reçoit du contenu à partir du siège social ou du centre de données cloud et que le contenu est mis en cache dans la filiale, les autres ordinateurs de la même filiale peuvent obtenir le contenu localement au lieu de contacter le contenu à partir du serveur de contenu via une liaison de réseau étendu (WAN).

Avantages du déploiement de BranchCache

BranchCache met en cache le contenu du fichier, du web et de l'application dans les filiales, ce qui permet aux ordinateurs clients d'accéder aux données à l'aide du réseau

local (LAN) plutôt que d’accéder au contenu via des connexions WAN lentes.

BranchCache réduit à la fois le trafic WAN et le temps nécessaire pour que les utilisateurs de la filiale ouvrent des fichiers sur le réseau. BranchCache fournit toujours aux utilisateurs les données les plus récentes et protège la sécurité de votre contenu en chiffrant les caches sur le serveur de cache hébergé et sur les ordinateurs clients.

Ce que ce guide contient

Ce guide de déploiement vous permet de déployer BranchCache dans les modes suivants :

- Mode de cache distribué. Dans ce mode, les ordinateurs clients des filiales téléchargent le contenu à partir des serveurs de contenu dans le siège social ou le cloud, puis mettent en cache le contenu pour d’autres ordinateurs de la même filiale. Le mode de cache distribué ne requiert pas de serveur dans la filiale.

- Mode de cache hébergé. Dans ce mode, les ordinateurs clients des filiales téléchargent le contenu à partir des serveurs de contenu du siège social ou du cloud, puis un serveur de cache hébergé extrait le contenu des clients. Le serveur de cache hébergé met ensuite en cache le contenu pour d’autres ordinateurs clients.

Ce guide fournit également des instructions sur le déploiement de trois types de serveurs de contenu. Les serveurs de contenu contiennent le contenu source téléchargé par les ordinateurs clients de la filiale, et un ou plusieurs serveurs de contenu sont nécessaires pour déployer BranchCache dans l’un ou l’autre mode. Les types de serveurs de contenu sont :

- **Serveurs de contenu basés sur un serveur Web**. Ces serveurs de contenu envoient le contenu aux ordinateurs clients BranchCache à l'aide des protocoles HTTP et HTTPS. Ces serveurs de contenu doivent exécuter des versions Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2 qui prennent en charge BranchCache et sur lesquelles la fonctionnalité BranchCache est installée.

- **Serveurs d’applications basés sur BITS**. Ces serveurs de contenu envoient du contenu aux ordinateurs clients BranchCache à l’aide du service de transfert intelligent en arrière-plan (BITS). Ces serveurs de contenu doivent exécuter des versions Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2 qui prennent en charge BranchCache et sur lesquelles la fonctionnalité BranchCache est installée.

- **Serveurs de contenu basés sur des serveurs de contenu**. Ces serveurs de contenu doivent exécuter des versions Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2 qui prennent en charge BranchCache et sur lesquelles le rôle serveur Services de fichiers est installé. De plus, le service de rôle **BranchCache pour fichiers réseau** du rôle serveur Services de fichiers doit être installé et configuré. Ces serveurs de contenu envoient le contenu aux ordinateurs clients BranchCache à l'aide du protocole SMB.

Pour plus d'informations, consultez Versions du système d'exploitation pour BranchCache.

Conditions requises pour le déploiement de BranchCache

Voici les conditions requises pour le déploiement de BranchCache à l'aide de ce guide.

- Les **serveurs de contenu web et de contenu** doivent exécuter l'un des systèmes d'exploitation suivants pour fournir les fonctionnalités BranchCache : Windows Server 2016, Windows Server 2012 R2 , Windows Server 2012 ou Windows Server 2008 R2. Les clients Windows 8 et versions ultérieures continuent de voir les avantages de BranchCache lors de l'accès aux serveurs de contenu qui exécutent Windows Server 2008 R2, mais ils ne peuvent pas utiliser les nouvelles technologies de segmentation et de hachage dans Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012.

- Les **ordinateurs clients** doivent exécuter Windows 10, Windows 8.1 ou Windows 8 pour utiliser le modèle de déploiement le plus récent et les améliorations de segmentation et de hachage introduites avec Windows Server 2012.

- Les **serveurs de cache hébergé** doivent exécuter Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012 pour tirer profit des améliorations de déploiement et des fonctionnalités de mise à l'échelle décrites dans ce document. Un ordinateur qui exécute l'un de ces systèmes d'exploitation configuré en tant que serveur de cache hébergé peut continuer à servir les ordinateurs clients exécutant Windows 7, mais pour ce faire, il doit être équipé d'un certificat adapté au protocole TLS (Transport Layer Security), comme décrit dans le Guide de déploiement de Windows Server 2008 R2 et Windows 7 BranchCache.

- Un **domaine Active Directory** est requis pour tirer parti de la stratégie de groupe et de la détection automatique du cache hébergé, mais un domaine n'est pas obligatoire pour utiliser BranchCache. Vous pouvez configurer des ordinateurs individuels à l'aide de Windows PowerShell. En outre, il n'est pas nécessaire que vos contrôleurs de domaine exécutent Windows Server 2012 ou une version

ultérieure pour utiliser les nouveaux paramètres de stratégie de groupe BranchCache. Vous pouvez importer les modèles d'administration BranchCache sur des contrôleurs de domaine qui exécutent des systèmes d'exploitation antérieurs, ou vous pouvez créer les objets de stratégie de groupe à distance sur d'autres ordinateurs qui exécutent Windows 10, Windows Server 2016, Windows 8.1, Windows Server 2012 R2, Windows 8 ou Windows Server 2012.

- Les **sites Active Directory** sont utilisés pour limiter l'étendue des serveurs de cache hébergé qui sont détectés automatiquement. Pour détecter automatiquement un serveur de cache hébergé, les ordinateurs client et serveur doivent appartenir au même site. BranchCache est conçu pour avoir un impact minimal sur les clients et les serveurs et n'impose pas d'exigences matérielles supplémentaires au-delà de celles nécessaires pour exécuter leurs systèmes d'exploitation respectifs.

Historique et documentation BranchCache

BranchCache a été introduit pour la première fois dans Windows 7® et Windows Server® 2008 R2, et a été amélioré dans les systèmes d'exploitation Windows Server 2012, Windows 8 et ultérieurs.

> ⓘ **Notes**
>
> Si vous déployez BranchCache dans des systèmes d'exploitation autres que Windows Server 2016, les ressources de documentation suivantes sont disponibles.
>
> - Pour plus d'informations sur BranchCache dans Windows 8, Windows 8.1, Windows Server 2012 et Windows Server 2012 R2, consultez **Vue d'ensemble de BranchCache**.
> - Pour plus d'informations sur BranchCache dans Windows 7 et Windows Server 2008 R2, consultez **BranchCache pour Windows Server 2008 R2**.

Choix d’une conception BranchCache

Article • 02/11/2024 •

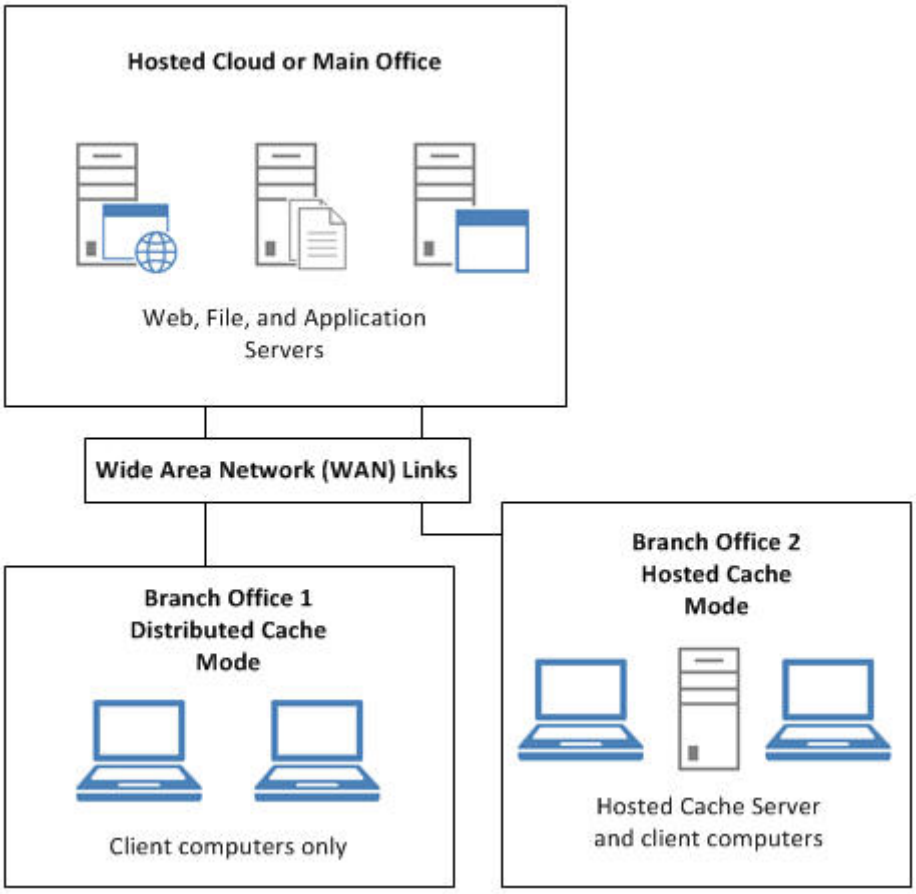
S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour en savoir plus sur les modes BranchCache et sélectionner les meilleurs modes pour votre déploiement.

Vous pouvez utiliser ce guide pour déployer BranchCache dans les modes et combinaisons de modes suivants.

- Toutes les filiales sont configurées pour le mode de cache distribué.
- Toutes les filiales sont configurées pour le mode de cache hébergé et disposent d’un serveur de cache hébergé sur le site.
- Certaines filiales sont configurées pour le mode de cache distribué et certaines filiales disposent d’un serveur de cache hébergé sur le site et sont configurées pour le mode de cache hébergé.

L’illustration suivante illustre une installation en mode double, avec une filiale configurée pour le mode de cache distribué et une filiale configurée pour le mode de cache hébergé.



Avant de déployer BranchCache, sélectionnez le mode que vous préférez pour chaque filiale de votre organisation.

Commentaires

Cette page a-t-elle été utile ? Yes No

Déployer BranchCache

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Les sections suivantes fournissent des informations sur le déploiement de BranchCache en mode de cache distribué et hébergé.

- Installer et configurer des serveurs de contenu
- Déployer des serveurs de cache hébergé (facultatif)
- Hachage préalable et préchargement du contenu sur les serveurs de cache hébergé (facultatifs)
- Configurer les ordinateurs clients BranchCache

> ⓘ **Notes**
>
> Les procédures décrites dans ce guide ne donnent aucune instruction dans le cas où la boîte de dialogue **Contrôle de compte d'utilisateur** s'ouvre pour demander votre autorisation de continuer. Si cette boîte de dialogue s'ouvre pendant que vous effectuez les procédures de ce guide et si la boîte de dialogue a été ouverte en réponse à vos actions, cliquez sur **Continuer**.

Installer et configurer des serveurs de contenu

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Lorsque vous déployez BranchCache en mode de cache distribué ou en mode de cache hébergé, vous devez déployer un ou plusieurs serveurs de contenu au siège social ou sur le cloud. Les serveurs de contenu qui sont des serveurs web ou des serveurs d'applications utilisent la fonctionnalité BranchCache. Les serveurs de contenu qui sont des serveurs de fichiers utilisent le service de rôle BranchCache pour fichiers réseau du rôle serveur Services de fichiers dans Windows Server 2016.

Consultez les rubriques suivantes pour déployer des serveurs de contenu.

- Installer des serveurs de contenu qui utilisent la fonctionnalité BranchCache
- Installer des serveurs de contenu Services de fichiers

Commentaires

Cette page a-t-elle été utile ? Yes No

Installer des serveurs de contenu qui utilisent la fonctionnalité BranchCache

Article • 02/04/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Pour déployer des serveurs de contenu qui sont des serveurs web HTTPS (Secure Hypertext Transfer Protocol), des serveurs web HTTP (Hypertext Transfer Protocol) et des serveurs d'applications BITS (Background Intelligent Transfer Service), tels que les serveurs système de site de distribution de branche de Windows Server Update Services (WSUS) et de Microsoft Endpoint Configuration Manager, vous devez installer la fonctionnalité BranchCache, démarrer le service BranchCache et (pour les serveurs WSUS uniquement) effectuer des étapes de configuration supplémentaires.

Consultez les rubriques suivantes pour déployer des serveurs de contenu.

- Installer la fonctionnalité BranchCache
- Configurer des serveurs de contenu Windows Server Update Services (WSUS)

Commentaires

Cette page a-t-elle été utile ? Yes No

Installer la fonctionnalité BranchCache

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour installer la fonctionnalité BranchCache et démarrer le service BranchCache sur un ordinateur exécutant Windows Server® 2016, Windows Server 2012 R2 ou Windows Server 2012.

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer cette procédure.

Avant d'effectuer cette procédure, il est recommandé d'installer et de configurer votre application BITS ou votre serveur web.

> ⓘ **Notes**
>
> Pour effectuer cette procédure à l'aide de Windows PowerShell, exécutez Windows PowerShell en tant qu'administrateur, tapez les commandes suivantes à l'invite de Windows PowerShell, puis appuyez sur Entrée.
>
> `Install-WindowsFeature BranchCache`
>
> `Restart-Computer`

Pour installer et activer la fonctionnalité BranchCache

1. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre. Cliquez sur **Suivant**.
2. Dans **Sélectionner le type d'installation**, vérifiez que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
3. Dans **Sélectionner le serveur de destination**, vérifiez que le serveur approprié soit sélectionné, puis cliquez sur **Suivant**.
4. Dans **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
5. Dans **Sélectionner des fonctionnalités**, cliquez sur **BranchCache**, puis sur **Suivant**.

6. Dans **Confirmer les sélections pour l'installation**, cliquez sur **Installer**. Dans la **progression de l'installation**, l'installation de la fonctionnalité BranchCache se poursuit. Une fois l'installation terminée, cliquez sur **Fermer**.

Après avoir installé la fonctionnalité BranchCache, le service BranchCache, également appelé PeerDistSvc, est activé et le type de démarrage est Automatique.

Configurer des serveurs de contenu Windows Server Update Services (WSUS)

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Après avoir installé la fonctionnalité BranchCache et démarré le service BranchCache, vous devez configurer les serveurs WSUS pour stocker les fichiers de mise à jour sur l'ordinateur local.

Lorsque vous configurez des serveurs WSUS pour stocker des fichiers de mise à jour sur l'ordinateur local, les métadonnées de mise à jour et les fichiers de mise à jour sont téléchargés et stockés directement sur le serveur WSUS. Cela permet de s'assurer que les ordinateurs clients BranchCache reçoivent les fichiers de mise à jour des produits Microsoft du serveur WSUS plutôt que directement du site Web Microsoft Update.

Pour plus d'informations sur la synchronisation WSUS, consultez Configuration des synchronisations de mise à jour

---

Commentaires

Cette page a-t-elle été utile ? Yes No

Installer des serveurs de contenu Services de fichiers

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Pour déployer des serveurs de contenu qui exécutent le rôle serveur Services de fichiers, vous devez installer le service de rôle BranchCache pour fichiers réseau du rôle serveur Services de fichiers. De plus, vous devez activer BranchCache sur les partages de fichiers en fonction de vos besoins.

Pendant la configuration du serveur de contenu, vous pouvez autoriser la publication BranchCache de contenu pour tous les partages de fichiers ou vous pouvez sélectionner un sous-ensemble de partages de fichiers à publier.

> ⓘ **Notes**
>
> Quand vous déployez un serveur de fichiers ou un serveur web prenant en charge BranchCache en tant que serveur de contenu, les informations de contenu sont désormais calculées hors connexion, bien avant qu'un client BranchCache demande un fichier. En raison de cette amélioration, vous n'avez pas besoin de configurer la publication des codes de hachage pour les serveurs de contenu, comme vous le faisiez dans la version précédente de BranchCache.
>
> Cette génération automatique des codes de hachage permet d'accroître les performances et d'économiser davantage de bande passante, car les informations de contenu sont prêtes pour le premier client qui demande le contenu, et les calculs ont déjà été effectués.

Consultez les rubriques suivantes pour déployer des serveurs de contenu.

- Configurer le rôle serveur Services de fichiers
- Activer la publication des codes de hachage pour les serveurs de fichiers
- Activer BranchCache sur un partage de fichiers (facultatif)

Commentaires

Cette page a-t-elle été utile ? Yes No

Configurer le rôle serveur Services de fichiers

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez déployer des serveurs de contenu basés sur des serveurs de fichiers BranchCache sur des ordinateurs exécutant Windows Server 2016 ainsi que le rôle serveur Services de fichiers, et sur lesquels le service de rôle **BranchCache pour fichiers réseau** est installé.

- Pour installer un serveur de contenu BranchCache sur un ordinateur où les services de fichiers n'ont pas encore été installés, consultez Installer un nouveau serveur de fichiers comme serveur de contenu.
- Pour installer un serveur de contenu BranchCache sur un ordinateur déjà configuré avec le rôle serveur Services de fichiers, consultez Configurer un serveur de fichiers existant comme serveur de contenu.

Commentaires

Cette page a-t-elle été utile ? Yes No

Installer un nouveau serveur de fichiers comme serveur de contenu

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour installer le rôle de serveur Services de fichiers et le service de rôle **BranchCache pour fichiers réseau** sur un ordinateur qui exécute Windows Server 2016.

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer cette procédure.

> ⓘ **Notes**
>
> Pour effectuer cette procédure à l'aide de Windows PowerShell, exécutez Windows PowerShell en tant qu'administrateur, tapez les commandes suivantes à l'invite de Windows PowerShell, puis appuyez sur Entrée.
>
> `Install-WindowsFeature FS-BranchCache -IncludeManagementTools`
>
> `Restart-Computer`
>
> Pour installer le service de rôle Déduplication des données, tapez la commande suivante, puis appuyez sur Entrée.
>
> `Install-WindowsFeature FS-Data-Deduplication -IncludeManagementTools`

Pour installer les services de fichiers et le service de rôle BranchCache pour fichiers réseau

1. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre. Dans **Avant de commencer**, cliquez sur **Suivant**.

2. Dans **Sélectionner le type d'installation**, vérifiez que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.

3. Dans **Sélectionner le serveur de destination**, vérifiez que le serveur approprié soit sélectionné, puis cliquez sur **Suivant**.

4. Dans **Sélectionner des rôles de serveur**, dans **Rôles**, notez que le rôle **Services de fichiers et de stockage** est déjà installé. Cliquez sur la flèche à gauche du nom du rôle pour développer la sélection des services de rôle, puis cliquez sur la flèche à gauche des **services de fichiers et iSCSI**.

5. Cochez les cases pour **le serveur** de **fichiers et BranchCache pour les fichiers réseau**.

   > **Conseil**
   >
   > Il est recommandé de cocher également la case à cocher pour la **déduplication des données**.

   Cliquez sur **Suivant**.

6. Dans **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

7. Dans **Confirmer les sélections pour l'installation**, passez en revue vos sélections, puis cliquez sur **Installer**. Le volet **Progression de l'installation** s'affiche pendant l'installation. Une fois l'installation terminée, cliquez sur **Fermer**.

Configurer un serveur de fichiers existant comme serveur de contenu

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour installer le service de rôle **BranchCache pour fichiers réseau** du rôle serveur Services de fichiers sur un ordinateur qui exécute Windows Server 2016.

> ⓘ **Important**
>
> Si le rôle serveur Services de fichiers n'est pas déjà installé, ne suivez pas cette procédure. À la place, consultez [Installer un nouveau serveur de fichiers comme serveur de contenu](#).

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer cette procédure.

> ⓘ **Notes**
>
> Pour effectuer cette procédure à l'aide de Windows PowerShell, exécutez Windows PowerShell en tant qu'administrateur, tapez les commandes suivantes à l'invite de Windows PowerShell, puis appuyez sur Entrée.
>
> ```
> Install-WindowsFeature FS-BranchCache -IncludeManagementTools
> ```
>
> Pour installer le service de rôle Déduplication des données, tapez la commande suivante, puis appuyez sur Entrée.
>
> ```
> Install-WindowsFeature FS-Data-Deduplication -IncludeManagementTools
> ```

Pour installer le service de rôle BranchCache pour fichiers réseau

1. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre. Cliquez sur **Suivant**.

2. Dans **Sélectionner le type d'installation**, vérifiez que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.

3. Dans **Sélectionner le serveur de destination**, vérifiez que le serveur approprié soit sélectionné, puis cliquez sur **Suivant**.

4. Dans **Sélectionner des rôles de serveur**, dans **Rôles**, notez que le rôle **Services de fichiers et de stockage** est déjà installé. Cliquez sur la flèche à gauche du nom du rôle pour développer la sélection des services de rôle, puis cliquez sur la flèche à gauche des **services de fichiers et iSCSI**.

5. Cochez la case **BranchCache pour les fichiers réseau**.

   > **Conseil**
   >
   > Si vous ne l'avez pas encore fait, il est recommandé de cocher également la case à cocher pour la **déduplication des données**.

   Cliquez sur **Suivant**.

6. Dans **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

7. Dans **Confirmer les sélections pour l'installation**, passez en revue vos sélections, puis cliquez sur **Installer**. Le volet **Progression de l'installation** s'affiche pendant l'installation. Une fois l'installation terminée, cliquez sur **Fermer**.

Activer la publication de hachages pour des serveurs de fichiers

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez activer la publication de hachages BranchCache sur un serveur de fichiers ou sur plusieurs serveurs de fichiers.

- Pour activer la publication de codes de hachage sur un seul serveur de fichiers à l'aide de la stratégie de groupe de l'ordinateur local, consultez Activer la publication de codes de hachage pour les serveurs de fichiers membres n'appartenant pas au domaine.
- Pour activer la publication de codes de hachage sur plusieurs serveur de fichiers à l'aide de la stratégie de groupe du domaine, consultez Activer la publication de codes de hachage pour les serveurs de fichiers membres du domaine.

> **Notes**
>
> Si vous disposez de plusieurs serveurs de fichiers et si vous souhaitez activer la publication de codes de hachage par partage, au lieu d'activer la publication de codes de hachage pour tous les partages, vous pouvez utiliser les instructions de la rubrique Activer la publication de codes de hachage pour les serveurs de fichiers membres n'appartenant pas au domaine.

Commentaires

Cette page a-t-elle été utile ? Yes No

Activer la publication de hachages pour les serveurs de fichiers n’appartenant pas au domaine

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour configurer la publication de hachages pour BranchCache à l’aide de la stratégie de groupe de l’ordinateur local sur un serveur de fichiers qui exécute Windows Server 2016 avec **BranchCache pour le service de rôle Fichiers réseau** du rôle serveur Services de fichiers installé.

Cette procédure est destinée à être utilisée sur un serveur de fichiers non membre du domaine. Si vous exécutez cette procédure sur un serveur de fichiers membre appartenant au domaine et que vous configurez également BranchCache à l'aide de la stratégie de groupe du domaine, les paramètres de stratégie de groupe du domaine remplacent les paramètres de la stratégie de groupe locale.

L’appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer cette procédure.

> ⓘ **Notes**
>
> Si vous avez un ou plusieurs serveurs de fichiers membres du domaine, vous pouvez les ajouter à une unité d'organisation dans les services ADDS (Active Directory Domain Services), puis utiliser la stratégie de groupe pour configurer la publication de hachages pour tous les serveurs de fichiers en même temps, plutôt que de configurer chaque serveur de fichiers individuellement. Pour plus d’informations, consultez Activer la publication de hachages pour les serveurs de fichiers membres du domaine.

Pour activer la publication de hachages pour un serveur de fichiers

1. Ouvrez Windows PowerShell, tapez **mmc**, puis appuyez sur Entrée. La console MMC s'affiche.

2. Dans la console MMC, dans le menu **Fichier** , cliquez sur **Ajouter/Supprimer le composant logiciel enfichable**. La boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** s'ouvre.

3. Dans **Ajouter ou supprimer des composants logiciels enfichables**, dans **Composants logiciels enfichables disponibles**, double-cliquez sur **Éditeur d'objets de stratégie de groupe**. L'Assistant Stratégie de groupe s'ouvre avec l'objet Ordinateur local sélectionné. Cliquez sur **Terminer**, puis sur **OK**.

4. Dans la console MMC Éditeur de stratégie de groupe local, développez le chemin d'accès suivant : **Stratégie d'ordinateur local**, **Configuration de l'ordinateur**, **Modèles d'administration**, **Réseau**, **Serveur Lanman**. Cliquez sur **Le serveur Lanman**.

5. Dans le volet d'informations, double-cliquez sur **Publication de hachages pour BranchCache**. La boîte de dialogue **Publication de hachages pour BranchCache** s'ouvre.

6. Dans la boîte de dialogue **Publication de hachages pour BranchCache**, cliquez sur **Activé**.

7. Dans **Options**, cliquez sur **Autoriser la publication de hachage pour tous les dossiers partagés**, puis cliquez sur l'une des options suivantes :

   a. Pour activer la publication de hachages pour tous les dossiers partagés sur cet ordinateur, cliquez sur **Autoriser la publication de hachages pour tous les dossiers partagés**.

   b. Pour activer la publication de hachages uniquement pour les dossiers partagés pour lesquels BranchCache est activé, cliquez sur **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**.

   c. Pour désactiver la publication de hachages pour tous les dossiers partagés sur l'ordinateur même si BranchCache est activé sur les partages de fichiers, cliquez sur **N'autoriser la publication de hachages pour aucun dossier partagé**.

8. Cliquez sur **OK**.

Activer la publication de hachages pour les serveurs de fichiers membres du domaine

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Lorsque vous utilisez les services AD DS, vous pouvez utiliser la stratégie de groupe de domaine pour activer la publication de hachages BranchCache pour plusieurs serveurs de fichiers. Pour ce faire, vous devez créer une unité d'organisation, ajouter des serveurs de fichiers à l'unité d'organisation, créer un objet de stratégie de groupe Publication de hachages BranchCache, puis configurer l'objet de stratégie de groupe.

Consultez les rubriques suivantes pour activer la publication de hachage pour plusieurs serveurs de fichiers.

- Créer l'unité d'organisation Serveurs de fichiers BranchCache
- Déplacer des serveurs de fichiers vers l'unité d'organisation Serveurs de fichiers BranchCache
- Créer l'objet de stratégie de groupe de la publication de hachages BranchCache
- Configurer l'objet de stratégie de groupe de la publication de hachages BranchCache

---

Commentaires

Cette page a-t-elle été utile ? Yes No

Créer l’unité d’organisation Serveurs de fichiers BranchCache

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour créer une unité d’organisation dans Active Directory Domain Services (AD DS) pour les serveurs de fichiers BranchCache.

L’appartenance aux **administrateurs de domaine** ou équivalente est la condition minimale requise pour effectuer cette procédure.

Pour créer l’unité d’organisation Serveurs de fichiers BranchCache

1. Sur un ordinateur sur lequel AD DS est installé, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. La console Utilisateurs et ordinateurs Active Directory s'ouvre.

2. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur le domaine auquel vous souhaitez ajouter une unité d’organisation. Par exemple, si votre domaine est nommé example.com, cliquez avec le bouton droit sur **example.com**. Pointez sur **Nouveau**, puis cliquez sur **Unité organisationnelle**. La boîte de dialogue **Nouvel objet : Unité d’organisation** s’affiche.

3. Dans la boîte de dialogue **Nouvel objet : Unité d’organisation**, dans **Nom**, tapez un nom pour la nouvelle unité d’organisation. Par exemple, si vous souhaitez nommer l'unité d'organisation Serveurs de fichiers BranchCache, tapez **Serveurs de fichiers BranchCache**, puis cliquez sur **OK**.

Déplacer des serveurs de fichiers vers l’unité d’organisation Serveurs de fichiers BranchCache

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour ajouter des serveurs de fichiers BranchCache à une unité d’organisation dans services de domaine Active Directory (AD DS).

L’appartenance aux **administrateurs de domaine** ou équivalente est la condition minimale requise pour effectuer cette procédure.

> ⓘ **Notes**
>
> Vous devez créer une unité d'organisation Serveurs de fichiers BranchCache dans la console Utilisateurs et ordinateurs Active Directory avant d'ajouter des comptes d'ordinateur à l'unité d'organisation avec cette procédure. Pour plus d'informations, consultez Créer l'unité d'organisation Serveurs de fichiers BranchCache.

Pour déplacer des serveurs de fichiers vers l'unité d'organisation Serveurs de fichiers BranchCache

1. Sur un ordinateur sur lequel AD DS est installé, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. La console Utilisateurs et ordinateurs Active Directory s'ouvre.

2. Dans la console Utilisateurs et ordinateurs Active Directory, recherchez le compte d'ordinateur pour un serveur de fichiers BranchCache, cliquez pour sélectionner le compte, puis glissez-déplacez le compte d'ordinateur sur l'unité d'organisation Serveurs de fichiers BranchCache que vous avez créée précédemment. Par exemple, si vous avez créé précédemment une unité d’organisation nommée **Serveurs de fichiers BranchCache**, glissez-déplacez le compte d’ordinateur sur l’unité d’organisation **Serveurs de fichiers BranchCache**.

3. Répétez l’étape précédente pour chaque serveur de fichiers BranchCache dans le domaine que vous souhaitez déplacer vers l’unité d’organisation.

Créer l’objet de stratégie de groupe de la publication de hachages BranchCache

14/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour créer l’objet de stratégie de groupe (GPO) de publication de hachage BranchCache.

L’appartenance aux **administrateurs de domaine** ou équivalente est la condition minimale requise pour effectuer cette procédure.

> ⓘ **Notes**
>
> Avant d'exécuter cette procédure, vous devez créer l'unité d'organisation Serveurs de fichiers BranchCache et déplacer les serveurs de fichiers dans l'unité d'organisation. Pour plus d’informations, consultez Activer la publication de hachages pour les serveurs de fichiers membres du domaine.

Pour créer l’objet de stratégie de groupe de publication de hachage BranchCache

1. Ouvrez Windows PowerShell, tapez **mmc**, puis appuyez sur Entrée. La console MMC s'affiche.

2. Dans la console MMC, dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant enfichable**. La boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** s'ouvre.

3. Dans **Ajouter ou supprimer des composants logiciels enfichables**, dans **Composants logiciels enfichables disponibles**, double-cliquez sur **Gestion des stratégies de groupe**, puis cliquez sur **OK**.

4. Dans la console MMC de gestion de la stratégie groupe, développez le chemin d'accès à l'unité d'organisation Serveurs de fichiers BranchCache que vous avez créée précédemment. Par exemple, si votre forêt s’appelle example.com, si votre domaine s’appelle example1.com et si votre UO s’appelle serveurs de fichiers BranchCache, développez le chemin suivant : **Gestion des stratégies de groupe**, **Forêt : example.com**, **Domaines**, **example1.com**, **Serveurs de fichiers BranchCache**.

5. Cliquez avec le bouton droit sur **Serveurs de fichiers BranchCache**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**. La boîte de dialogue **Nouvelle GPO** s'ouvre. Dans **Nom**, tapez un nom pour le nouvel objet de stratégie de groupe. Par exemple, si vous souhaitez nommer l'objet Publication de hachages BranchCache, tapez **Publication de hachages BranchCache**. Cliquez sur **OK**.

Configurer l’objet de stratégie de groupe de la publication de hachages BranchCache

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour configurer l’objet de stratégie de groupe de publication de hachage BranchCache afin que tous les serveurs de fichiers que vous avez ajoutés à votre unité d’organisation disposent du même paramètre de stratégie de publication de hachage.

L’appartenance aux **administrateurs de domaine** ou équivalente est la condition minimale requise pour effectuer cette procédure.

> ⓘ **Notes**
>
> Avant d'exécuter cette procédure, vous devez créer l’unité d’organisation Serveurs de fichiers BranchCache, déplacer les serveurs de fichiers dans l’unité d’organisation et créer l’objet de stratégie de groupe de publication de hachage BranchCache. Pour plus d’informations, consultez Activer la publication de hachages pour les serveurs de fichiers membres du domaine.

Pour configurer l’objet de stratégie de groupe de publication de hachage BranchCache

1. Exécutez Windows PowerShell en tant qu’administrateur, tapez **mmc**, puis appuyez sur Entrée. La console MMC s'affiche.

2. Dans la console MMC, dans le menu **Fichier** , cliquez sur **Ajouter/Supprimer le composant logiciel enfichable**. La boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** s'ouvre.

3. Dans **Ajouter ou supprimer des composants logiciels enfichables**, dans **Composants logiciels enfichables disponibles**, double-cliquez sur **Gestion des stratégies de groupe**, puis cliquez sur **OK**.

4. Dans la console MMC de gestion de la stratégie groupe, développez le chemin d'accès à l'objet de stratégie de groupe Publication de hachages BranchCache que vous avez créé précédemment. Par exemple, si votre forêt est nommée example.com, que votre domaine est nommé example1.com et que votre objet de stratégie de groupe est nommé

Publication de hachage BranchCache, développez le chemin d'accès suivant : **Gestion de la stratégie de groupe**, **Forêt : example.com**, **Domaines**, **example1.com**, **Objets de stratégie de groupe**, **Publication de hachage BranchCache**.

5. Cliquez avec le bouton droit sur l'objet de stratégie de groupe **Publication de hachages BranchCache**, puis cliquez sur **Modifier**. La console de l'Éditeur de gestion des stratégies de groupe s'ouvre.

6. Dans la console éditeur de gestion des stratégies de groupe, développez le chemin d'accès suivant : **Configuration de l'ordinateur**, **Stratégies**, **Modèles d'administration**, **Réseau**, **Serveur Lanman**.

7. Dans la console Éditeur de gestion des stratégies de groupe, cliquez sur **Serveur Lanman**. Dans le volet d'informations, double-cliquez sur **Publication de hachages pour BranchCache**. La boîte de dialogue **Publication de hachages pour BranchCache** s'ouvre.

8. Dans la boîte de dialogue **Publication de hachages pour BranchCache**, cliquez sur **Activé**.

9. Dans **Options**, cliquez sur **Autoriser la publication de hachage pour tous les dossiers partagés**, puis cliquez sur l'une des options suivantes :

   a. Pour activer la publication de hachage pour tous les dossiers partagés pour tous les serveurs de fichiers que vous avez ajoutés à l'unité d'organisation, cliquez sur **Autoriser la publication de hachage pour tous les dossiers partagés**.

   b. Pour activer la publication de hachages uniquement pour les dossiers partagés pour lesquels BranchCache est activé, cliquez sur **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**.

   c. Pour désactiver la publication de hachages pour tous les dossiers partagés sur l'ordinateur même si BranchCache est activé sur les partages de fichiers, cliquez sur **N'autoriser la publication de hachages pour aucun dossier partagé**.

10. Cliquez sur **OK**.

> ⓘ **Notes**
>
> Dans la plupart des cas, vous devez enregistrer la console MMC et actualiser l'affichage afin de visualiser les modifications de configuration apportées.

Activer BranchCache sur un partage de fichiers (facultatif)

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour activer BranchCache sur un partage de fichiers.

> ⓘ **Important**
>
> Vous n'avez pas besoin d'effectuer cette procédure si vous configurez le paramètre de publication des codes de hachage avec la valeur **Autoriser la publication des codes de hachage pour tous les dossiers partagés**.

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer cette procédure.

Pour activer BranchCache sur un partage de fichiers

1. Ouvrez Windows PowerShell, tapez **mmc**, puis appuyez sur Entrée. La console MMC s'affiche.
2. Dans la console MMC, dans le menu **Fichier** , cliquez sur **Ajouter/Supprimer le composant logiciel enfichable**. La boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** s'ouvre.
3. Dans **Ajouter ou supprimer des composants logiciels enfichables**, dans **Composants logiciels enfichables disponibles**, double-cliquez sur **Dossiers partagés**. L'Assistant Dossiers partagés s'ouvre avec l'objet Ordinateur local sélectionné. Configurez l'affichage que vous préférez, cliquez sur **Terminer**, puis sur **OK**.
4. Double-cliquez sur **Dossiers partagés (local)**, puis cliquez sur **Partages**.
5. Dans le volet d'informations, cliquez avec le bouton droit sur un partage, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés** du partage s'ouvre.
6. Dans la boîte de dialogue **Propriétés** , sous l'onglet **Général** , cliquez sur **Paramètres hors connexion**. La boîte de dialogue **Paramètres hors connexion** s'ouvre.
7. Vérifiez que l'option **Seuls les fichiers et les programmes spécifiés par les utilisateurs sont disponibles hors connexion** est sélectionnée, puis cliquez sur **Activer BranchCache**.

8. Cliquez deux fois sur **OK** .

Déployer des serveurs de Cache hébergé (facultatif)

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour installer et configurer les serveurs de cache hébergé BranchCache situés dans les filiales où vous souhaitez déployer le mode de cache hébergé BranchCache. Avec BranchCache dans Windows Server 2016, vous pouvez déployer plusieurs serveurs de cache hébergé dans une filiale.

> ⓘ **Important**
>
> Cette étape est facultative, car le mode de cache distribué ne nécessite pas un ordinateur de serveur de cache hébergé dans les filiales. Si vous ne prévoyez pas de déployer le mode de cache hébergé dans une filiale, vous n'avez pas besoin de déployer un serveur de cache hébergé et vous n'avez pas besoin d'effectuer les étapes de cette procédure.

Vous devez être membre des **administrateurs** ou équivaut à effectuer cette procédure.

Pour installer et configurer un serveur de cache hébergé

1. Sur l'ordinateur que vous souhaitez configurer en tant que serveur de cache hébergé, exécutez la commande suivante à une invite de Windows PowerShell pour installer la fonctionnalité BranchCache.

   ```
   Install-WindowsFeature BranchCache -IncludeManagementTools
   ```

2. Configurez l'ordinateur en tant que serveur de cache hébergé à l'aide de l'une des commandes suivantes :

   - Pour configurer un ordinateur qui n'est pas joint à un domaine en tant que serveur de cache hébergé, tapez la commande suivante à l'invite de Windows PowerShell, puis appuyez sur Entrée.

     ```
     Enable-BCHostedServer
     ```

   - Pour configurer un ordinateur joint à un domaine en tant que serveur de cache hébergé et inscrire un point de connexion de service dans Active Directory pour la détection automatique du serveur de cache hébergé par les ordinateurs clients,

tapez la commande suivante à l'invite de Windows PowerShell, puis appuyez sur Entrée.

```
Enable-BCHostedServer -RegisterSCP
```

3. Pour vérifier la configuration correcte du serveur de cache hébergé, tapez la commande suivante à l'invite de Windows PowerShell, puis appuyez sur Entrée.

```
Get-BCStatus
```

> ⓘ **Notes**
>
> Après avoir exécuté cette commande, dans la section **HostedCacheServerConfiguration**, la valeur de **HostedCacheServerIsEnabled** est **True**. Si vous avez configuré un serveur de cache hébergé joint à un domaine pour inscrire un point de connexion de service (SCP) dans Active Directory, la valeur de **HostedCacheScpRegistrationEnabled** est **True**.

Hachage préalable et préchargement du contenu sur les serveurs de Cache hébergé (facultatifs)

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour forcer la création d'informations de contenu (également appelées hachages) sur des serveurs Web et de fichiers prenant en charge BranchCache. Vous pouvez également collecter les données sur les serveurs de fichiers et Web dans des packages qui peuvent être transférés vers des serveurs de cache hébergés à distance. Cela vous permet de précharger du contenu sur des serveurs de cache hébergé à distance afin que les données soient disponibles pour le premier accès client.

Vous devez être membre des **Administrateurs**, ou équivalent pour effectuer cette procédure.

Pour préhacher le contenu et précharger le contenu sur des serveurs de cache hébergé

1. Connectez-vous au fichier ou au serveur Web qui contient les données que vous souhaitez précharger, puis identifiez les dossiers et fichiers que vous souhaitez charger sur un ou plusieurs serveurs de cache hébergé à distance.

2. Exécutez Windows PowerShell en tant qu'administrateur. Pour chaque dossier et fichier, exécutez la commande `Publish-BCFileContent` ou la commande `Publish-BCWebContent`, selon le type de serveur de contenu, pour déclencher la génération de hachage et ajouter des données à un package de données.

3. Une fois que toutes les données ont été ajoutées au package de données, exportez-les à l'aide de la commande `Export-BCCachePackage` pour créer un fichier de package de données.

4. Déplacez le fichier du package de données vers les serveurs de cache hébergé à distance à l'aide de la technologie de transfert de fichiers de votre choix. Les disques durs FTP, SMB, HTTP, DVD et portables sont tous des transports viables.

5. Importez le fichier de package de données sur les serveurs de cache hébergé à distance à l'aide de la commande `Import-BCCachePackage`.

Commentaires

Cette page a-t-elle été utile ? Yes No

Configurer les ordinateurs clients BranchCache

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser les rubriques suivantes pour configurer des ordinateurs clients membres et non membres de domaine en tant que clients de cache distribué BranchCache ou en mode de cache hébergé.

- Utiliser la stratégie de groupe pour configurer les ordinateurs clients membres du domaine
- Utiliser Windows PowerShell pour configurer les ordinateurs clients n'appartenant pas au domaine
- Configurer les règles de pare-feu pour les membres n'appartenant pas au domaine afin d'autoriser le trafic BranchCache
- Vérifier les paramètres de l'ordinateur client

Commentaires

Cette page a-t-elle été utile ? Yes No

Utiliser la stratégie de groupe pour configurer les ordinateurs clients membres du domaine

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Dans cette section, vous allez créer un objet stratégie de groupe pour tous les ordinateurs de votre organisation, configurer les ordinateurs clients membres du domaine avec le mode de cache distribué ou le mode de cache hébergé, et configurer le Pare-feu Windows avec Advanced Security pour autoriser le trafic BranchCache.

Cette section contient les procédures suivantes.

1. Pour créer un objet stratégie de groupe et configurer les modes BranchCache
2. Pour configurer le Pare-feu Windows avec des règles de trafic entrant de sécurité avancées
3. Pour configurer le Pare-feu Windows avec des règles de trafic sortant de sécurité avancées

> **Conseil**
>
> Dans la procédure suivante, vous êtes invité à créer un objet stratégie de groupe dans la stratégie de domaine par défaut. Toutefois, vous pouvez créer l'objet dans une unité d'organisation (UO) ou un autre conteneur approprié pour votre déploiement.

Vous devez être membre des **administrateurs de domaine**, ou équivalent à effectuer ces procédures.

Pour créer un objet stratégie de groupe et configurer les modes BranchCache

1. Sur un ordinateur sur lequel le rôle serveur Des services de domaine Active Directory est installé, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**. La Console de gestion des stratégies de groupe s'ouvre.

2. Dans la console Gestion des stratégies de groupe, développez le chemin suivant : **Forêt :***example.com*, **Domaines**, *example.com*, Objets de stratégie de **groupe**, où *example.com* est le nom du domaine où se trouvent les comptes d'ordinateurs clients BranchCache que vous souhaitez configurer.

3. Cliquez avec le bouton droit de la souris sur **Objets de stratégie de groupe** et puis cliquez sur **Nouveau**. La boîte de dialogue **Nouvel objet de stratégie de groupe** s'ouvre. Dans **Name**, tapez un nom pour le nouvel objet de stratégie de groupe (GPO). Par exemple, si vous voulez nommer l'objet Ordinateurs clients BranchCache, tapez **Ordinateurs clients BranchCache**. Cliquez sur **OK**.

4. Dans la console de gestion des stratégies de groupe, vérifiez que **Objets de stratégie de groupe** est sélectionné, et dans le volet d'informations, cliquez avec le bouton droit sur l'objet de stratégie de groupe que vous venez de créer. Par exemple, si vous avez nommé votre objet de stratégie de groupe Ordinateurs clients BranchCache, cliquez avec le bouton droit sur **Ordinateurs clients BranchCache**. Cliquez sur **Modifier**. La console de l'Éditeur de gestion des stratégies de groupe s'ouvre.

5. Dans la console éditeur de gestion des stratégies de groupe, développez le chemin suivant : **Configuration de** l'ordinateur, **Stratégies**, **Modèles d'administration : définitions de stratégie (fichiers ADMX) récupérées à partir de l'ordinateur local**, **réseau**, **BranchCache**.

6. Cliquez sur **BranchCache**, puis dans le volet d'informations, double-cliquez **sur Activer BranchCache**. La boîte de dialogue des paramètres de stratégie s'ouvre.

7. Dans la boîte de dialogue **Activer BranchCache**, cliquez sur **Activé**, puis sur **OK**.

8. Pour activer le mode de cache distribué BranchCache, dans le volet d'informations, double-cliquez sur **Définir le mode de cache distribué BranchCache**. La boîte de dialogue des paramètres de stratégie s'ouvre.

9. Dans la boîte de dialogue **Définir le mode de cache distribué de BranchCache**, cliquez sur **Activé**, puis sur **OK**.

10. Si vous avez une ou plusieurs succursales dans lesquelles vous déployez BranchCache en mode de cache hébergé et que vous avez déployé des serveurs de cache hébergé dans ces bureaux, double-cliquez sur **Activer la découverte automatique du cache hébergé par point de connexion de service**. La boîte de dialogue des paramètres de stratégie s'ouvre.

11. Dans la boîte de dialogue **Activer la découverte automatique du cache hébergé par point de connexion de service** , cliquez sur **Activé**, puis sur **OK**.

> ⓘ **Notes**
>
> Lorsque vous activez les paramètres de stratégie **Définir le mode de cache distribué BranchCache** et **Activer la découverte automatique du cache hébergé par point de connexion de service**, les ordinateurs clients fonctionnent en mode de cache distribué BranchCache, sauf s'ils trouvent un serveur de cache hébergé dans la filiale, à ce stade ils fonctionnent en mode cache hébergé.

12. Utilisez les procédures ci-dessous pour configurer les paramètres de pare-feu sur les ordinateurs clients à l'aide de stratégie de groupe.

Pour configurer le Pare-feu Windows avec des règles de trafic entrant de sécurité avancées

1. Dans la console Gestion des stratégies de groupe, développez le chemin suivant : **Forêt :***example.com*, **Domaines**, *example.com*, Objets de stratégie de **groupe**, où *example.com* est le nom du domaine où se trouvent les comptes d'ordinateurs clients BranchCache que vous souhaitez configurer.

2. Dans la console de gestion des stratégies de groupe, vérifiez que **Objets de stratégie de groupe** est sélectionné, et dans le volet d'informations, cliquez avec le bouton droit sur l'objet de stratégie de groupe Ordinateurs clients BranchCache précédemment créé. Par exemple, si vous avez nommé votre objet de stratégie de groupe Ordinateurs clients BranchCache, cliquez avec le bouton droit sur **Ordinateurs clients BranchCache**. Cliquez sur **Modifier**. La console de l'Éditeur de gestion des stratégies de groupe s'ouvre.

3. Dans la console Éditeur de gestion des stratégies de groupe, développez le chemin d'accès suivant : **Configuration ordinateur**, **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Pare-feu Windows avec sécurité avancée**, **Pare-feu Windows avec sécurité avancée - LDAP**, **Règles de trafic entrant**.

4. Cliquez avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**. L'Assistant Nouvelle règle de trafic entrant s'ouvre.

5. Dans **Type de règle**, cliquez sur **Prédéfini**, développez la liste des choix, puis cliquez sur **BranchCache - Récupération de contenu (utilise HTTP).** Cliquez sur **Suivant**.

6. Dans **Règles prédéfinies**, cliquez sur **Suivant**.

7. Dans **Action**, vérifiez que **l'option Autoriser la connexion** est sélectionnée, puis cliquez sur **Terminer**.

> **Important**
>
> Vous devez sélectionner **Autoriser la connexion** pour le client BranchCache afin d'être en mesure de recevoir le trafic sur ce port.

8. Pour créer l'exception de pare-feu WS-Discovery, cliquez de nouveau avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**. L'Assistant Nouvelle règle de trafic entrant s'ouvre.

9. Dans **Type de règle**, cliquez sur **Prédéfini**, développez la liste des choix, puis cliquez sur **BranchCache - Découverte d'homologues (utilise WSD).** Cliquez sur **Suivant**.

10. Dans **Règles prédéfinies**, cliquez sur **Suivant**.

11. Dans **Action**, vérifiez que **l'option Autoriser la connexion** est sélectionnée, puis cliquez sur **Terminer**.

> **Important**
>
> Vous devez sélectionner **Autoriser la connexion** pour le client BranchCache afin d'être en mesure de recevoir le trafic sur ce port.

Pour configurer le Pare-feu Windows avec des règles de trafic sortant de sécurité avancées

1. Dans la console Éditeur de gestion des stratégies de groupe, cliquez avec le bouton droit sur **Règles de trafic sortant**, puis cliquez sur **Nouvelle règle**. L'Assistant Nouvelle règle de trafic sortant s'ouvre.

2. Dans **Type de règle**, cliquez sur **Prédéfini**, développez la liste des choix, puis cliquez sur **BranchCache - Récupération de contenu (utilise HTTP).** Cliquez sur **Suivant**.

3. Dans **Règles prédéfinies**, cliquez sur **Suivant**.

4. Dans **Action**, vérifiez que **l'option Autoriser la connexion** est sélectionnée, puis cliquez sur **Terminer**.

> **Important**

Vous devez sélectionner **Autoriser la connexion** pour le client BranchCache afin d'être en mesure d'envoyer le trafic sur ce port.

5. Pour créer l'exception de pare-feu WS-Discovery, cliquez de nouveau avec le bouton droit sur **Règles de trafic sortant**, puis cliquez sur **Nouvelle règle**. L'Assistant Nouvelle règle de trafic sortant s'ouvre.

6. Dans **Type de règle**, cliquez sur **Prédéfini**, développez la liste des choix, puis cliquez sur **BranchCache - Découverte d'homologues (utilise WSD).** Cliquez sur **Suivant**.

7. Dans **Règles prédéfinies**, cliquez sur **Suivant**.

8. Dans **Action**, vérifiez que **l'option Autoriser la connexion** est sélectionnée, puis cliquez sur **Terminer**.

> ⓘ **Important**
>
> Vous devez sélectionner **Autoriser la connexion** pour le client BranchCache afin d'être en mesure d'envoyer le trafic sur ce port.

Utiliser Windows PowerShell pour configurer les ordinateurs clients n'appartenant pas au domaine

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour configurer manuellement un ordinateur client BranchCache en mode cache distribué ou en mode cache hébergé.

> **Notes**
>
> Si vous avez configuré des ordinateurs clients BranchCache à l'aide de la stratégie de groupe, les paramètres de stratégie de groupe remplacent toute configuration manuelle des ordinateurs clients auxquels les stratégies sont appliquées.

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer cette procédure.

Pour activer le mode de cache distribué ou hébergé de BranchCache

1. Sur l'ordinateur client BranchCache que vous souhaitez configurer, exécutez Windows PowerShell en tant qu'administrateur, puis effectuez l'une des opérations suivantes.

   - Pour configurer l'ordinateur client pour le mode de cache distribué BranchCache, entrez la commande suivante, puis appuyez sur Entrée.

     `Enable-BCDistributed`

   - Pour configurer l'ordinateur client pour le mode de cache hébergé BranchCache, entrez la commande suivante, puis appuyez sur Entrée.

     `Enable-BCHostedClient`

     > **Conseil**
     >
     > Si vous souhaitez spécifier les serveurs de cache hébergé disponibles, utilisez le paramètre `-ServerNames` avec une liste séparée par des virgules de vos serveurs

de cache hébergé comme valeur de paramètre. Par exemple, si vous avez deux serveurs de cache hébergé nommés HCS1 et HCS2, configurez l'ordinateur client pour le mode de cache hébergé avec la commande suivante.

```
Enable-BCHostedClient -ServerNames HCS1,HCS2
```

Configurer les règles de pare-feu pour les membres n'appartenant pas au domaine afin d'autoriser le trafic BranchCache

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser les informations dans cette rubrique pour configurer des produits pare-feu tiers et à configurer manuellement un ordinateur client avec des règles de pare-feu qui permettent à BranchCache de fonctionner en mode cache distribué.

> ⓘ **Notes**
>
> - Si vous avez configuré des ordinateurs clients BranchCache à l'aide de la stratégie de groupe, les paramètres de stratégie de groupe remplacent toute configuration manuelle des ordinateurs clients auxquels les stratégies sont appliquées.
> - Si vous avez déployé BranchCache avec DirectAccess, vous pouvez utiliser les paramètres dans cette rubrique pour configurer des règles IPsec pour autoriser le trafic BranchCache.

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour apporter ces modifications de configuration.

[MS-PCCRD] : Mise en cache du contenu des homologues et protocole de découverte pour la récupération

Les clients de cache distribué doivent autoriser le trafic MS-PCCRD entrant et sortant, via le protocole WS-Discovery (Web Services Dynamic Discovery).

Les paramètres de pare-feu doivent autoriser le trafic multidiffusion en plus du trafic entrant et sortant. Vous pouvez utiliser les paramètres suivants pour configurer des exceptions de pare-feu pour le mode de cache distribué.

Multidiffusion IPv4 : 239.255.255.250

Multidiffusion IPv6 : FF02::C

Trafic entrant : Port local : 3702, Port distant : éphémère

Trafic entrant : Port local : 3702, Port distant : éphémère

Programme : %systemroot%\system32\svchost.exe (BranchCache Service [PeerDistSvc])

[MS-PCCRD] : Mise en cache du contenu des homologues et Récupération : protocole de récupération

Les clients de cache distribué doivent autoriser le trafic MS-PCCRR entrant et sortant, qui est porté via le protocole HTTP 1.1 comme indiqué dans la requête pour commentaires (RFC) 2616.

Les paramètres de pare-feu doivent autoriser le trafic entrant et sortant. Vous pouvez utiliser les paramètres suivants pour configurer des exceptions de pare-feu pour le mode de cache distribué.

Trafic entrant : Port local : 80, Port distant : éphémère

Trafic sortant : Port local : éphémère, Port distant : 80

Vérifier les paramètres de l'ordinateur client

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette procédure pour vérifier que l'ordinateur client est correctement configuré pour BranchCache.

> ⓘ **Notes**
>
> Cette procédure comprend les étapes de mise à jour manuelle de stratégie de groupe et de redémarrage du service BranchCache. Vous n'avez pas besoin d'effectuer ces actions si vous redémarrez l'ordinateur, car elles se produisent automatiquement dans ce cas.

Vous devez être membre des **administrateurs** ou équivaut à effectuer cette procédure.

Pour vérifier les paramètres de l'ordinateur client BranchCache

1. Pour actualiser la stratégie de groupe sur l'ordinateur client dont vous souhaitez vérifier la configuration BranchCache, exécutez Windows PowerShell en tant qu'administrateur, tapez la commande suivante, puis appuyez sur Entrée.

   ```
   gpupdate /force
   ```

2. Pour les ordinateurs clients configurés en mode cache hébergé et configurés pour détecter automatiquement les serveurs de cache hébergé par point de connexion de service, exécutez les commandes suivantes pour arrêter et redémarrer le service BranchCache.

   ```
   net stop peerdistsvc
   ```

   ```
   net start peerdistsvc
   ```

3. Inspectez le mode opérationnel BranchCache actuel en exécutant la commande suivante.

   ```
   Get-BCStatus
   ```

4. Dans Windows PowerShell, passez en revue la sortie de la commande **Get-BCStatus** .

   La valeur de **BranchCacheIsEnabled** doit être **True**.

   Dans **ClientSettings**, la valeur de **CurrentClientMode** doit être **DistributedClient** ou **HostedCacheClient**, en fonction du mode que vous avez configuré à l'aide de ce guide.

Dans **ClientSettings**, si vous avez configuré le mode de cache hébergé et fourni les noms de vos serveurs de cache hébergés pendant la configuration, ou si le client a automatiquement localisé des serveurs de cache hébergés à l'aide de points de connexion de service, **HostedCacheServerList** doit avoir une valeur identique au nom ou aux noms de vos serveurs de cache hébergés. Par exemple, si votre serveur de cache hébergé est nommé HCS1 et que votre domaine est corp.contoso.com, la valeur de **HostedCacheServerList** est **HCS1.corp.contoso.com**.

5. Si l'un des paramètres BranchCache répertoriés ci-dessus n'a pas les valeurs correctes, suivez les étapes décrites dans ce guide pour vérifier les paramètres de stratégie de groupe ou de l'ordinateur local, ainsi que les exceptions de pare-feu que vous avez configurées, et vérifiez qu'ils sont corrects. En outre, redémarrez l'ordinateur ou suivez les étapes de cette procédure pour actualiser la stratégie de groupe et redémarrer le service BranchCache.

DirectAccess

08/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10

> ⓘ **Important**
>
> Microsoft recommande vivement d'utiliser Always On VPN au lieu de DirectAccess pour les nouveaux déploiements. Pour plus d'informations, consultez Always On VPN

Vous pouvez utiliser cette rubrique pour obtenir une brève vue d'ensemble de DirectAccess, y compris les systèmes d'exploitation serveur et clients qui prennent en charge DirectAccess, et pour obtenir des liens vers une documentation DirectAccess supplémentaire pour Windows Server.

> ⓘ **Notes**
>
> Outre cette rubrique, la documentation DirectAccess suivante est également disponible.
>
> - Chemins de déploiement de DirectAccess dans Windows Server
> - Conditions préalables pour le déploiement de DirectAccess
> - Configurations non prises en charge DirectAccess
> - Guides de laboratoire de Test de DirectAccess
> - Problèmes connus de DirectAccess
> - Planification de la capacité DirectAccess
> - Jonction de domaine hors connexion DirectAccess
> - Dépannage de DirectAccess
> - Déployer un serveur DirectAccess individuel avec l'Assistant de démarrage
> - Déployer un serveur DirectAccess unique avec des paramètres avancés
> - Ajouter DirectAccess à un déploiement (VPN) de l'accès à distance existant

DirectAccess permet aux utilisateurs distants de se connecter aux ressources réseau de l'organisation sans avoir besoin des connexions de réseau privé virtuel (VPN) traditionnelles. Avec les connexions DirectAccess, les ordinateurs clients distants sont toujours connectés à votre organisation. Les utilisateurs distants n'ont pas besoin de démarrer et d'arrêter les connexions, comme cela est nécessaire avec les connexions VPN. Par ailleurs, vos administrateurs informatiques peuvent gérer les ordinateurs clients DirectAccess chaque fois qu'ils sont en cours d'exécution et connectés à Internet.

> **Important**
>
> N'essayez pas de déployer l'accès à distance sur une machine virtuelle dans Microsoft Azure. L'utilisation de l'accès à distance dans Microsoft Azure n'est pas prise en charge. Vous ne pouvez pas utiliser l'accès à distance dans un ordinateur virtuel Azure pour déployer un VPN, DirectAccess ni toute autre fonctionnalité d'accès à distance dans Windows Server. Pour plus d'informations, consultez Prise en charge des logiciels serveur Microsoft pour les machines virtuelles Microsoft Azure .

DirectAccess prend en charge uniquement les clients joints à un domaine qui incluent la prise en charge du système d'exploitation pour DirectAccess.

Les systèmes d'exploitation clients suivants prennent en charge DirectAccess.

- Windows 11 Entreprise
- Windows 10 Entreprise
- Windows 10 Entreprise 2015 Branche de Service à Long Terme (LTSB)
- Windows 8.1 Enterprise

Qu’est-ce que le système DNS (Domain Name System) ?

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

DNS est un protocole standard qui mappe les noms d’ordinateurs aux adresses IP, ce qui active la résolution de noms pour les ordinateurs et les utilisateurs. Dans les réseaux Windows, DNS est le service de résolution de noms par défaut. Dans le cadre de la suite de protocoles TCP/IP, toutes les connexions réseau sont configurées avec l’adresse IP d’au moins un serveur DNS pour garantir une résolution de noms transparente.

Utilisation du DNS dans Windows et Windows Server

Dans Windows Server, DNS est un rôle serveur qui peut être installé à l’aide du Gestionnaire de serveur ou des commandes PowerShell. Lors de la configuration d’une nouvelle forêt et d’un domaine Active Directory, DNS est automatiquement installé avec Active Directory.

DNS est essentiel pour les services de domaine Active Directory (AD DS), servant de mécanisme d’emplacement du contrôleur de domaine pour les opérations telles que l’authentification, les mises à jour et les recherches. Les contrôleurs de domaine utilisent également DNS pour se localiser les uns les autres. Les contrôleurs de domaine utilisent également DNS pour se localiser les uns les autres. Le serveur DNS est chargé de stocker et de répliquer les zones DNS qui contiennent les noms et adresses IP de tous les ordinateurs du domaine. Cela permet aux clients de résoudre les noms en adresses IP et de rechercher des contrôleurs de domaine.

Windows Server DNS peut fonctionner comme une solution DNS autonome sans Active Directory, comme l’hébergement de zones de recherche publiques pour une organisation.

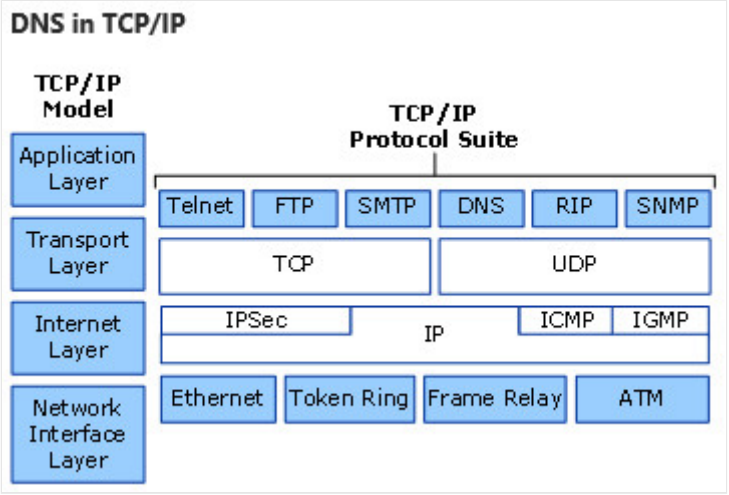
Le service client DNS est inclus dans toutes les versions client et serveur du système d’exploitation Windows. Le service s’exécute par défaut après l’installation du système d’exploitation. Lorsque vous configurez une connexion réseau TCP/IP avec l’adresse IP d’un serveur DNS, le client DNS interroge le serveur DNS pour effectuer deux tâches clés :

- Il découvre les contrôleurs de domaine.
- Il résout les noms d’ordinateurs en adresses IP.

Par exemple, lorsqu’un utilisateur réseau disposant d’un compte d’utilisateur Active Directory se connecte à un domaine Active Directory, le service client DNS interroge le serveur DNS pour

localiser un contrôleur de domaine pour le domaine. Une fois que le serveur DNS répond avec l'adresse IP du contrôleur de domaine, le client contacte le contrôleur de domaine pour commencer le processus d'authentification.

Le serveur DNS Windows Server et les services client DNS utilisent le protocole DNS inclus dans la suite de protocole TCP/IP. DNS fait partie de la couche d'application du modèle de référence TCP/IP, comme illustré dans l'illustration suivante.



Fonctionnalités du serveur DNS

Windows Server DNS offre des fonctionnalités qui améliorent les fonctionnalités et les performances dans les environnements Windows. Certaines des fonctionnalités clés incluent :

- **Intégration d'Active Directory** : Sécuriser les mises à jour et la réplication des données DNS.
- **Mises à jour dynamiques** : inscription automatique et mises à jour des enregistrements DNS clients.
- **DNSSEC** : garantit l'intégrité et l'authenticité des données, ce qui empêche les attaques telles que l'empoisonnement du cache.
- **Transfert et transfert conditionnel** : résout efficacement les noms en dehors du réseau local en transférant des requêtes.
- **Mise en cache** : améliore les performances et réduit le trafic réseau en stockant les résultats de la requête.
- **Surveillance et journalisation** : effectue le suivi de l'activité DNS et aide à la résolution des problèmes.
- **Stratégies DNS** : configure le comportement DNS en fonction de critères tels que l'adresse IP du client ou l'heure de la journée.
- **Anycast** : fournit une redondance et un équilibrage de charge en partageant la même adresse IP sur plusieurs serveurs DNS.

Scénarios de déploiement

Le DNS Windows Server peut être déployé dans divers scénarios pour répondre à divers besoins organisationnels. Pour les environnements utilisant Active Directory Domain Services (AD DS), DNS est intégré pour faciliter l'emplacement et l'authentification du contrôleur de domaine. Les organisations peuvent également utiliser DNS pour héberger des zones de recherche publiques, ce qui permet aux clients externes de résoudre les noms en adresses IP ou dans des zones de recherche privées, ce qui garantit la résolution de noms sécurisée au sein des réseaux internes.

Dans les environnements hybrides, le DNS Windows Server peut intégrer le DNS local à des services DNS basés sur le cloud, fournissant une résolution de noms transparente sur différentes plateformes. Pour garantir des performances et une fiabilité optimales, l'équilibrage de charge DNS peut distribuer les requêtes sur plusieurs serveurs, tandis que le basculement DNS assure une haute disponibilité en redirigeant les requêtes vers des serveurs de secours en cas de défaillance. En outre, les mesures de sécurité DNS, telles que DNSSEC, peuvent être implémentées pour protéger contre les attaques et maintenir l'intégrité des données.

Get started

Prêt à plonger ? Suivez le guide de démarrage rapide : Installez et configurez DNS Server sur Windows Server pour configurer DNS dans votre environnement.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Vue d’ensemble de Anycast DNS

Article • 14/04/2023

> S’applique à : Windows Server 2022, Windows Server 2016, Windows Server 2019

Cette rubrique fournit des informations sur le fonctionnement de Anycast DNS.

Qu’est-ce que Anycast ?

Anycast est une technologie qui fournit plusieurs chemins d’accès de routage à un groupe de points de terminaison auxquels la même adresse IP est affectée. Chaque appareil du groupe publie la même adresse sur un réseau et les protocoles de routage sont utilisés pour choisir la meilleure destination.

Anycast vous permet de mettre à l’échelle un service sans état, tel que DNS ou HTTP, en plaçant plusieurs nœuds derrière la même adresse IP et en utilisant le routage ECMP (Equal-Cost Multi-Path) pour diriger le trafic entre ces nœuds. Anycast est différent de la monodiffusion, dans laquelle chaque point de terminaison a sa propre adresse IP distincte.

Pourquoi utiliser Anycast avec DNS ?

Avec Anycast DNS, vous pouvez activer un serveur DNS ou un groupe de serveurs pour répondre aux requêtes DNS en fonction de l’emplacement géographique d’un client DNS. Cela peut améliorer le temps de réponse DNS et simplifier les paramètres du client DNS. Anycast DNS fournit également une couche supplémentaire de redondance et peut vous aider à vous protéger contre les attaques par déni de service DNS.

Fonctionnement de Anycast DNS

Anycast DNS fonctionne à l’aide de protocoles de routage tels que le protocole BGP (Border Gateway Protocol) pour envoyer des requêtes DNS à un serveur DNS préféré ou à un groupe de serveurs DNS (par exemple, un groupe de serveurs DNS gérés par un équilibreur de charge). Cette conception peut optimiser les communications DNS en obtenant des réponses DNS à partir d’un serveur DNS le plus proche d’un client.

Avec Anycast, les serveurs qui existent dans plusieurs emplacements géographiques publient chacun une adresse IP unique identique à leur passerelle locale (routeur). Lorsqu’un client DNS lance une requête à l’adresse Anycast, les itinéraires disponibles

sont évalués et la requête DNS est envoyée à l'emplacement préféré. En général, cet emplacement est le plus proche en fonction de la topologie de réseau. Consultez l'exemple qui suit.

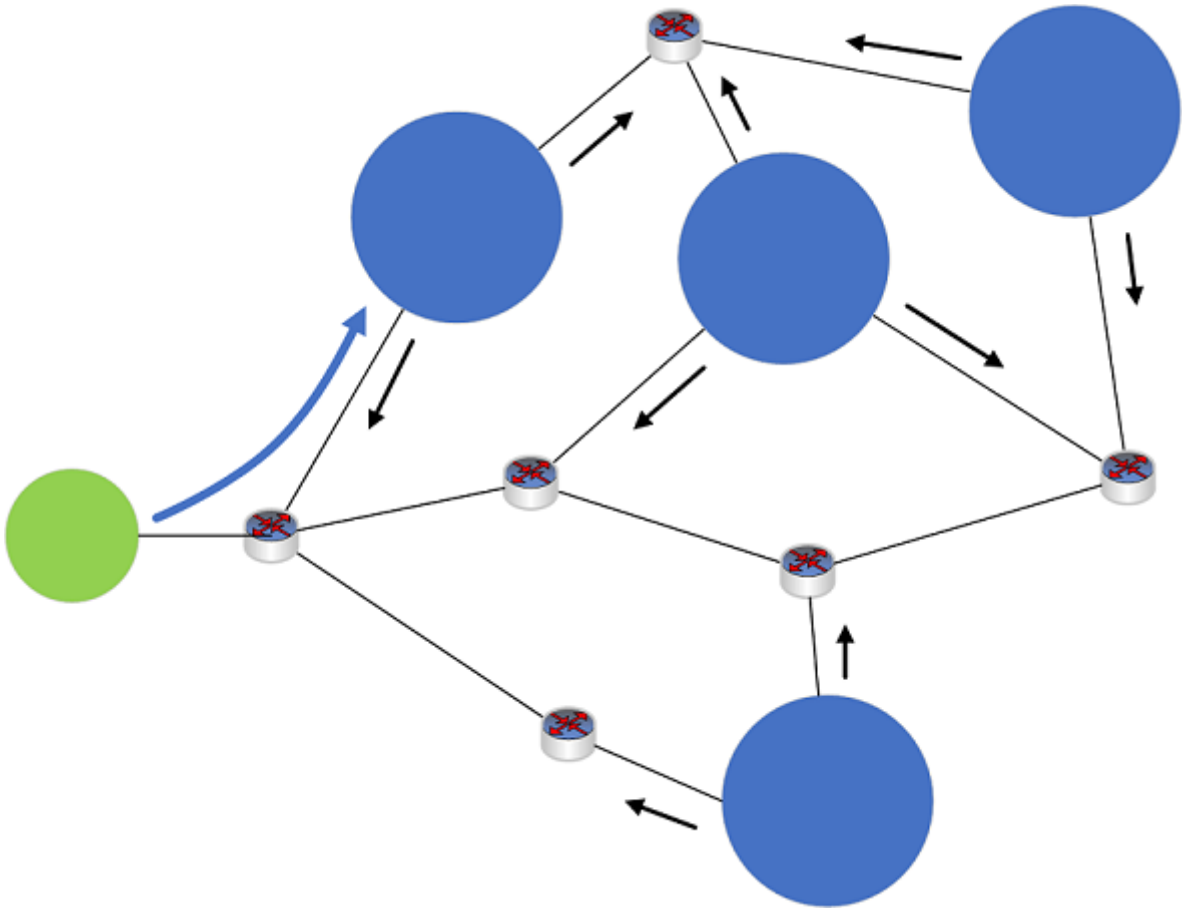


Figure 1 : Exemple de réseau Anycast

- Quatre serveurs DNS (cercles bleus), situés sur différents sites d'un réseau, annoncent chacun la même adresse IP Anycast à leur périphérique de routage local (non affiché).
- Les itinéraires sont partagés entre les appareils du réseau (flèches noires).
- Un appareil client DNS (cercle vert) envoie une requête DNS à l'adresse IP Anycast.
- La requête DNS du client est reçue par un appareil de routage sur le réseau (non affiché).
- Le périphérique de routage analyse les itinéraires disponibles vers l'adresse IP Anycast et achemine la requête DNS à l'aide de l'itinéraire disponible le plus court.
- La requête DNS est envoyée au serveur DNS le plus proche (flèche bleue).

Anycast DNS est couramment utilisé aujourd'hui pour acheminer le trafic DNS pour de nombreux services DNS globaux. Par exemple, le système de serveur DNS racine dépend fortement de Anycast DNS. Anycast fonctionne également avec de nombreux protocoles de routage différents et peut être utilisé exclusivement sur des intranets.

Démonstration de BGP natif sur Windows Server avec Anycast

La procédure suivante montre comment le protocole BGP natif sur Windows Server peut être utilisé avec Anycast DNS.

Configuration requise

- Un appareil physique avec le rôle Hyper-V installé.
  - Windows Server 2012 R2, Windows 10 ou version ultérieure.
- 2 machines virtuelles clientes (n'importe quel système d'exploitation).
  - L'installation d'outils BIND pour DNS, tels que dig, est recommandée.
- 3 machines virtuelles serveur (Windows Server 2016 ou Windows Server 2019).
  - Si le module Windows PowerShell LoopbackAdapter n'est pas encore installé sur les machines virtuelles serveur (DC001, DC002), l'accès à Internet est temporairement requis pour installer ce module.

Configuration de Hyper-V

Configurez votre serveur Hyper-V comme suit :

- 2 réseaux de commutateur virtuel privé sont configurés
  - Un réseau Internet fictif 131.253.1.0/24
  - Un réseau intranet fictif 10.10.10.0/24
- 2 machines virtuelles clientes sont attachées au réseau 131.253.1.0/24
- 2 machines virtuelles serveur sont attachées au réseau 10.10.10.0/24
- 1 serveur est doublement hébergé et attaché aux réseaux 131.253.1.0/24 et 10.10.10.0/24.

Configuration du réseau de machines virtuelles

Configurez les paramètres réseau sur les machines virtuelles avec les paramètres suivants :

1. Client1, client2

- Client1 : 131.253.1.1
- Client2 : 131.253.1.2
- Masque de sous-réseau : 255.255.255.0
- DNS : 51.51.51.51
- Passerelle : 131.253.1.254

2. Passerelle (Windows Server)

- NIC1 : 131.253.1.254, sous-réseau 255.255.255.0
- NIC2 : 10.10.10.254, sous-réseau 255.255.255.0
- DNS : 51.51.51.51
- Passerelle : 131.253.1.100 (peut être ignoré pour la démonstration)

3. DC001 (Windows Server)

- NIC1 : 10.10.10.1
- Sous-réseau : 255.255.255.0
- DNS : 10.10.10.1
- Passerelle : 10.10.10.254

4. DC002 (Windows Server)

- NIC1 : 10.10.10.2
- Sous-réseau 255.255.255.0
- DNS : 10.10.10.2*
- Passerelle : 10.10.10.254

*Utilisez la version 10.10.10.1 pour DNS initialement lors de l'exécution de la jonction de domaine pour DC002 afin de pouvoir localiser le domaine Active Directory sur DC001.

Configurer DNS

Utilisez Gestionnaire de serveur et la console de gestion DNS ou Windows PowerShell pour installer les rôles serveur suivants et créer une zone DNS statique sur chacun des deux serveurs.

1. DC001, DC002

- Installer Active Directory Domain Services et promouvoir le contrôleur de domaine (facultatif)
- Installer le rôle DNS (obligatoire)
- Créer une zone statique (non intégrée à AD) nommée **zone.tst** sur DC001 et DC002
  - Ajouter le **serveur** de noms d'enregistrement statique unique dans la zone de type « TXT »
  - Données (texte) pour l'enregistrement TXT sur DC001 = **DC001**
  - Données (texte) pour l'enregistrement TXT sur DC002 = **DC002**

Configurer des adaptateurs de bouclage

Entrez les commandes suivantes à une invite de Windows PowerShell avec élévation de privilèges sur DC001 et DC002 pour configurer des adaptateurs de bouclage.

> ⓘ **Notes**
>
> La commande **Install-Module** nécessite un accès Internet. Pour ce faire, affectez temporairement la machine virtuelle à un réseau externe dans Hyper-V.

PowerShell

```
$primary_interface = (Get-NetAdapter |?{$_.Status -eq "Up" -and
!$_.Virtual}).Name
$loopback_ipv4 = '51.51.51.51'
$loopback_ipv4_length = '32'
$loopback_name = 'Loopback'
Install-Module -Name LoopbackAdapter -MinimumVersion 1.2.0.0 -Force
Import-Module -Name LoopbackAdapter
New-LoopbackAdapter -Name $loopback_name -Force
$interface_loopback = Get-NetAdapter -Name $loopback_name
$interface_main = Get-NetAdapter -Name $primary_interface
Set-NetIPInterface -InterfaceIndex $interface_loopback.ifIndex -
InterfaceMetric "254" -WeakHostReceive Enabled -WeakHostSend Enabled -DHCP
Disabled
Set-NetIPInterface -InterfaceIndex $interface_main.ifIndex -WeakHostReceive
Enabled -WeakHostSend Enabled
Set-NetIPAddress -InterfaceIndex $interface_loopback.ifIndex -SkipAsSource
$True
Get-NetAdapter $loopback_name | Set-DNSClient –
RegisterThisConnectionsAddress $False
New-NetIPAddress -InterfaceAlias $loopback_name -IPAddress $loopback_ipv4 -
PrefixLength $loopback_ipv4_length -AddressFamily ipv4
Disable-NetAdapterBinding -Name $loopback_name -ComponentID ms_msclient
Disable-NetAdapterBinding -Name $loopback_name -ComponentID ms_pacer
Disable-NetAdapterBinding -Name $loopback_name -ComponentID ms_server
Disable-NetAdapterBinding -Name $loopback_name -ComponentID ms_lltdio
Disable-NetAdapterBinding -Name $loopback_name -ComponentID ms_rspndr
```

Configuration du routage des machines virtuelles

Utilisez les commandes Windows PowerShell suivantes sur les machines virtuelles pour configurer le routage.

1. Passerelle

PowerShell

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
Install-RemoteAccess -VpnType RoutingOnly
```

```
Add-BgpRouter -BgpIdentifier “10.10.10.254” -LocalASN 8075
Add-BgpPeer -Name "DC001" -LocalIPAddress 10.10.10.254 -PeerIPAddress
10.10.10.1 -PeerASN 65511 –LocalASN 8075
Add-BgpPeer -Name "DC002" -LocalIPAddress 10.10.10.254 -PeerIPAddress
10.10.10.2 -PeerASN 65511 –LocalASN 8075
```

2. DC001

PowerShell

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
Install-RemoteAccess -VpnType RoutingOnly
Add-BgpRouter -BgpIdentifier “10.10.10.1” -LocalASN 65511
Add-BgpPeer -Name "Labgw" -LocalIPAddress 10.10.10.1 -PeerIPAddress
10.10.10.254 -PeerASN 8075 –LocalASN 65511
Add-BgpCustomRoute -Network 51.51.51.0/24
```

3. DC002

PowerShell

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
Install-RemoteAccess -VpnType RoutingOnly
Add-BgpRouter -BgpIdentifier "10.10.10.2" -LocalASN 65511
Add-BgpPeer -Name "Labgw" -LocalIPAddress 10.10.10.2 -PeerIPAddress
10.10.10.254 -PeerASN 8075 –LocalASN 65511
Add-BgpCustomRoute -Network 51.51.51.0/24
```

Diagramme de résumé

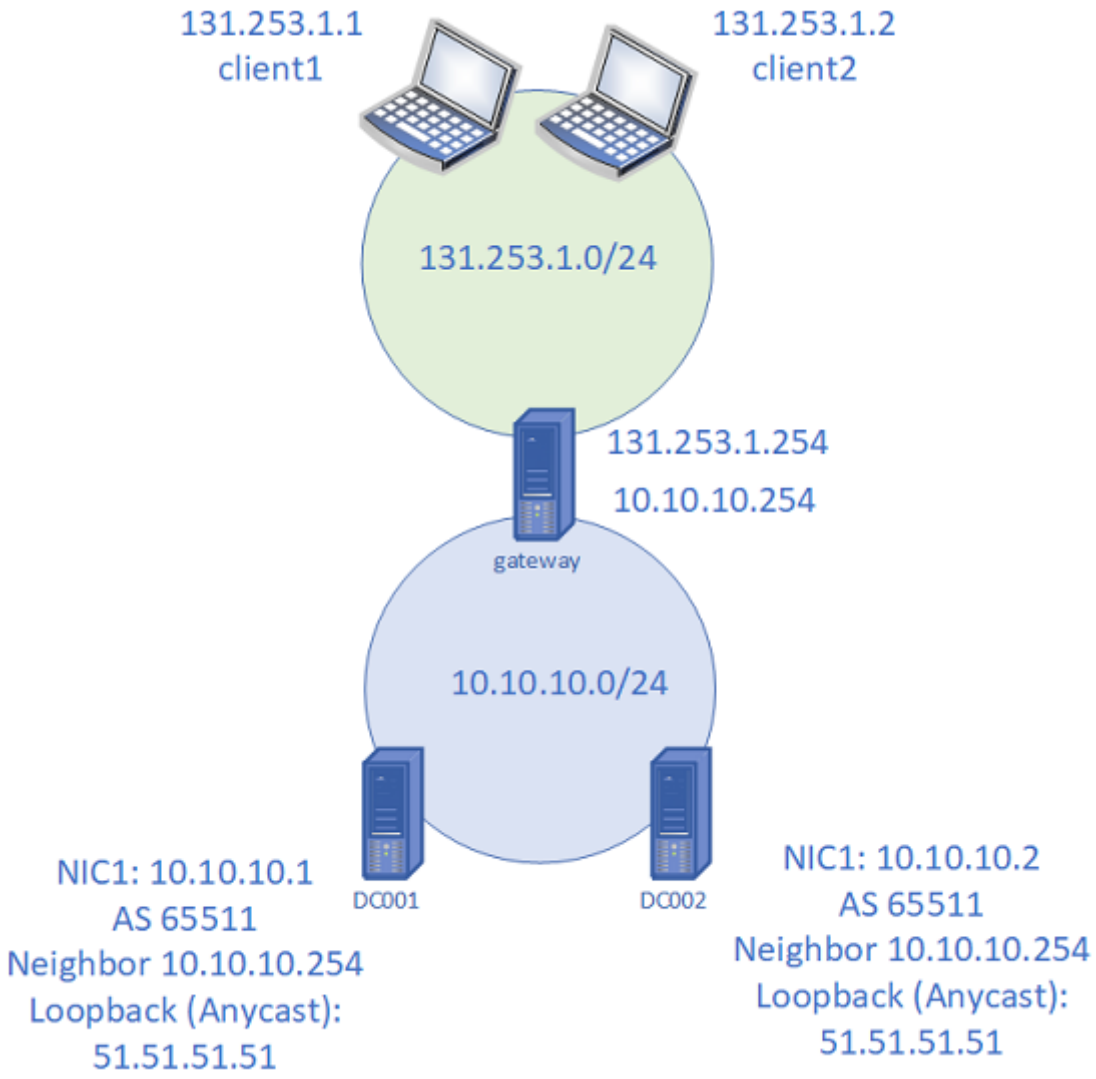


Figure 2 : Configuration du laboratoire pour la démonstration du BGP natif avec Anycast DNS

Démonstration avec Anycast DNS

1. Vérifier le routage BGP sur le serveur de passerelle

   `PS C:\> Get-BgpRouteInformation`

   DestinationNetwork NextHop LearnedFromPeer State LocalPref MED
   ---------- ------- ---------- ----- --------- ---
   51.51.51.0/24 10.10.10.1 DC001 Best
   51.51.51.0/24 10.10.10.2 DC002 Best

2. Sur client1 et client2, vérifiez que vous pouvez atteindre 51.51.51.51

   `PS C:\> ping 51.51.51.51`

Ping 51.51.51.51 avec 32 octets de données :
Réponse de 51.51.51.51 : octets=32 temps<1 ms TTL=126
Réponse de 51.51.51.51 : octets=32 temps<1 ms TTL=126
Réponse de 51.51.51.51 : octets=32 temps<1 ms TTL=126
Réponse de 51.51.51.51 : octets=32 temps<1 ms TTL=126

Statistiques ping pour 51.51.51.51 :
Paquets : Envoyé = 4, Reçu = 4, Perdu = 0 (perte de 0 %),
Durées approximatives d'aller-retour en millisecondes :
Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms

> ⓘ **Notes**
>
> En cas d'échec du test ping, vérifiez également qu'il n'existe aucune règle de pare-feu bloquant ICMP.

3. Sur client1 et client2, utilisez nslookup ou dig pour interroger l'enregistrement TXT. Les deux exemples sont présentés.

   `PS C:\> dig server.zone.tst TXT +short`

   `PS C:\> nslookup -type=txt server.zone.tst 51.51.51.51`

   Un client affiche « DC001 » et l'autre client affiche « DC002 » pour vérifier que Anycast fonctionne correctement. Vous pouvez également interroger à partir du serveur de passerelle.

4. Ensuite, désactivez l'adaptateur Ethernet sur DC001.

   `PS C:\> (Get-NetAdapter).Name`
   Bouclage
   Ethernet 2
   `PS C:\> Disable-NetAdapter "Ethernet 2"`
   Confirmer
   Êtes-vous sûr de vouloir effectuer cette action ?
   Disable-NetAdapter « Ethernet 2 »
   [Y] Oui [A] Oui à tous [N] Non [L] Non à tous [S] Suspendre [?] Aide (la valeur par défaut est « Y ») :
   `PS C:\> (Get-NetAdapter).Status`
   Haut
   Désactivé

5. Vérifiez que les clients DNS qui recevaient auparavant des réponses de DC001 ont basculé vers DC002.

   `PS C:\> nslookup -type=txt server.zone.tst 51.51.51.51`

   Serveur : Non reconnu
   Adresse : 51.51.51.51

   server.zone.tst text =

   « DC001 »

   `PS C:\> nslookup -type=txt server.zone.tst 51.51.51.51`

   Serveur : Non reconnu
   Adresse : 51.51.51.51

   server.zone.tst text =

   « DC002 »

6. Vérifiez que la session BGP est en panne sur DC001 à l'aide de Get-BgpStatistics sur le serveur de passerelle.

7. Réactivez l'adaptateur Ethernet sur DC001 et vérifiez que la session BGP est restaurée et que les clients reçoivent à nouveau des réponses DNS de DC001.

> ⓘ **Notes**
>
> Si aucun équilibreur de charge n'est utilisé, un client individuel utilise le même serveur DNS principal s'il est disponible. Cela crée un chemin BGP cohérent pour le client. Pour plus d'informations, consultez la section 4.4.3 de RFC4786 : **Chemins d'accès à coût égal**.

Forum aux questions

Q : Anycast DNS est-il une bonne solution à utiliser dans un environnement DNS local ?
R : Anycast DNS fonctionne en toute transparence avec un service DNS local. Toutefois, Anycast n'est pas *nécessaire* pour que le service DNS soit mis à l'échelle.

Q : Quel est l'impact de l'implémentation de Anycast DNS dans un environnement avec un grand nombre (par exemple, >50) de contrôleurs de domaine ?
R : Il n'y a aucun impact direct sur les fonctionnalités. Si un équilibreur de charge est utilisé, aucune autre configuration sur les contrôleurs de domaine n'est requise.

Q : Une configuration Anycast DNS est-elle prise en charge par le service client Microsoft ?
R : Si vous utilisez un équilibreur de charge non-Microsoft pour transférer des requêtes DNS, Microsoft prend en charge les problèmes liés au service serveur DNS. Consultez le fournisseur de l'équilibreur de charge pour les problèmes liés au transfert DNS.

Q : Quelle est la meilleure pratique pour Anycast DNS avec un grand nombre (par exemple, >50) de contrôleurs de domaine ?
R : La meilleure pratique consiste à utiliser un équilibreur de charge à chaque emplacement géographique. Les équilibreurs de charge sont généralement fournis par un fournisseur externe.

Q : Anycast DNS et Azure DNS ont-ils des fonctionnalités similaires ?
R : Azure DNS utilise Anycast. Pour utiliser Anycast avec Azure DNS, configurez votre équilibreur de charge pour transférer les requêtes au serveur Azure DNS.

Vue d’ensemble des stratégies DNS

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour en savoir plus sur la stratégie DNS, qui est une nouveauté dans Windows Server 2016. Vous pouvez utiliser la stratégie DNS pour la gestion du trafic basée sur la géolocalisation, les réponses DNS intelligentes en fonction de l’heure de la journée, afin de gérer un serveur DNS unique configuré pour le déploiement du cerveau, l’application de filtres sur les requêtes DNS, etc. Les éléments suivants fournissent plus de détails sur ces fonctionnalités.

- **Équilibrage de charge d’application.** Lorsque vous avez déployé plusieurs instances d’une application à différents emplacements, vous pouvez utiliser la stratégie DNS pour équilibrer la charge du trafic entre les différentes instances d’application, en allouant dynamiquement la charge de trafic pour l’application.

- **Gestion du trafic basée sur la géolocalisation.** Vous pouvez utiliser la stratégie DNS pour autoriser les serveurs DNS principaux et secondaires à répondre aux requêtes du client DNS en fonction de l’emplacement géographique du client et de la ressource à laquelle le client tente de se connecter, en fournissant au client l’adresse IP de la ressource la plus proche.

- **DNS « split brain ».** Avec le DNS « split brain », les enregistrements DNS sont divisés en différentes étendues de zone sur le même serveur DNS, et les clients DNS reçoivent une réponse selon qu’ils sont des clients internes ou externes. Vous pouvez configurer le DNS « split brain » pour les zones intégrées Active Directory ou pour les zones sur des serveurs DNS autonomes.

- **Filtering.** Vous pouvez configurer la stratégie DNS pour créer des filtres de requête basés sur des critères que vous fournissez. Les filtres de requête dans la stratégie DNS vous permettent de configurer le serveur DNS pour répondre de manière personnalisée en fonction de la requête DNS et du client DNS qui envoie la requête DNS.

- **Forensics.** Vous pouvez utiliser la stratégie DNS pour rediriger des clients DNS malveillants vers une adresse IP inexistante au lieu de les diriger vers l’ordinateur qu’ils essaient d’atteindre.

- **Redirection basée sur l’heure de la journée.** Vous pouvez utiliser la stratégie DNS pour distribuer le trafic d’application entre différentes instances distribuées géographiquement d’une application à l’aide de stratégies DNS basées sur l’heure de la journée.

Nouveaux concepts

Pour créer des stratégies pour prendre en charge les scénarios répertoriés ci-dessus, il est nécessaire de pouvoir identifier des groupes d'enregistrements dans une zone, des groupes de clients sur un réseau, entre autres éléments. Ces éléments sont représentés par les nouveaux objets DNS suivants :

- **Sous-réseau client :** un objet de sous-réseau client représente un sous-réseau IPv4 ou IPv6 à partir duquel les requêtes sont soumises à un serveur DNS. Vous pouvez créer des sous-réseaux pour définir ultérieurement des stratégies à appliquer en fonction du sous-réseau duquel les requêtes proviennent. Par exemple, dans un scénario DNS fractionné de cerveau, la demande de résolution d'un nom tel *quewww.microsoft.com* peut être traitée avec une adresse IP interne aux clients à partir de sous-réseaux internes et une autre adresse IP aux clients dans des sous-réseaux externes.

- **Étendue de récursivité :** les étendues de récursivité sont des instances uniques d'un groupe de paramètres qui contrôlent la récursivité sur un serveur DNS. Une étendue de récursivité contient une liste de redirecteurs et indique si la récursivité est activée. Un serveur DNS peut comporter de nombreuses étendues de récursivité. Les stratégies de récursivité du serveur DNS vous permettent de choisir une étendue de récursivité pour un ensemble de requêtes. Si le serveur DNS ne fait pas autorité pour certaines requêtes, les stratégies de récursivité du serveur DNS vous permettent de contrôler la façon de résoudre ces requêtes. Vous pouvez spécifier les redirecteurs à utiliser et s'il faut utiliser la récursivité.

- **Étendues** de zone : une zone DNS peut avoir plusieurs étendues de zone, chaque étendue de zone contenant leur propre jeu d'enregistrements DNS. Le même enregistrement peut être présent dans plusieurs étendues, avec différentes adresses IP. En outre, les transferts de zone sont effectués au niveau de l'étendue de la zone. Cela signifie que les enregistrements d'une étendue de zone dans une zone principale seront transférés vers la même étendue de zone dans une zone secondaire.

Types de stratégies

Les stratégies DNS sont divisées par niveau et par type. Vous pouvez utiliser des stratégies de résolution de requêtes pour définir le mode de traitement des requêtes, et des stratégies de transfert de zone pour définir la façon dont les transferts de zone se produisent. Vous pouvez appliquer chaque type de stratégie au niveau du serveur ou au niveau de la zone.

Stratégies de résolution de requêtes

Vous pouvez utiliser des stratégies de résolution de requêtes DNS pour spécifier la façon dont les requêtes de résolution entrantes sont gérées par un serveur DNS. Chaque stratégie de résolution de requête DNS contient les éléments suivants :

Agrandir le tableau

Field	Description	Valeurs possibles
Name	Nom de la stratégie	– Jusqu'à 256 caractères – Peut contenir n'importe quel caractère valide pour un nom de fichier
State	État de la stratégie	– Activer (par défaut) -Handicapé
Level	Niveau de stratégie	-Serveur -Zone
Ordre de traitement	Une fois qu'une requête est classée par niveau et s'applique, le serveur trouve la première stratégie pour laquelle la requête correspond aux critères et l'applique à la requête	– Valeur numérique – Valeur unique par stratégie contenant le même niveau et s'applique à la valeur
Action	Action à effectuer par le serveur DNS	– Autoriser (par défaut pour le niveau de la zone) – Refuser (par défaut au niveau du serveur) -Ignorer
Criteria	Condition de stratégie (AND/OR) et liste des critères à respecter pour l'application de la stratégie	– Opérateur de condition (AND/OR) – Liste des critères (voir le tableau de critères ci-dessous)
Scope	Liste des étendues de zone et des valeurs pondérées par étendue. Les valeurs pondérées sont utilisées pour la distribution de l'équilibrage de charge. Par exemple, si cette liste inclut datacenter1 avec un poids de 3 et datacenter2 avec un poids de 5, le serveur répond avec un enregistrement du datacentre1 trois fois sur huit requêtes	– Liste des étendues de zone (par nom) et poids

Notes

Les stratégies au niveau du serveur peuvent uniquement avoir les valeurs **Refuser** ou **Ignorer** en tant qu'action.

Le champ critères de stratégie DNS est composé de deux éléments :

Agrandir le tableau

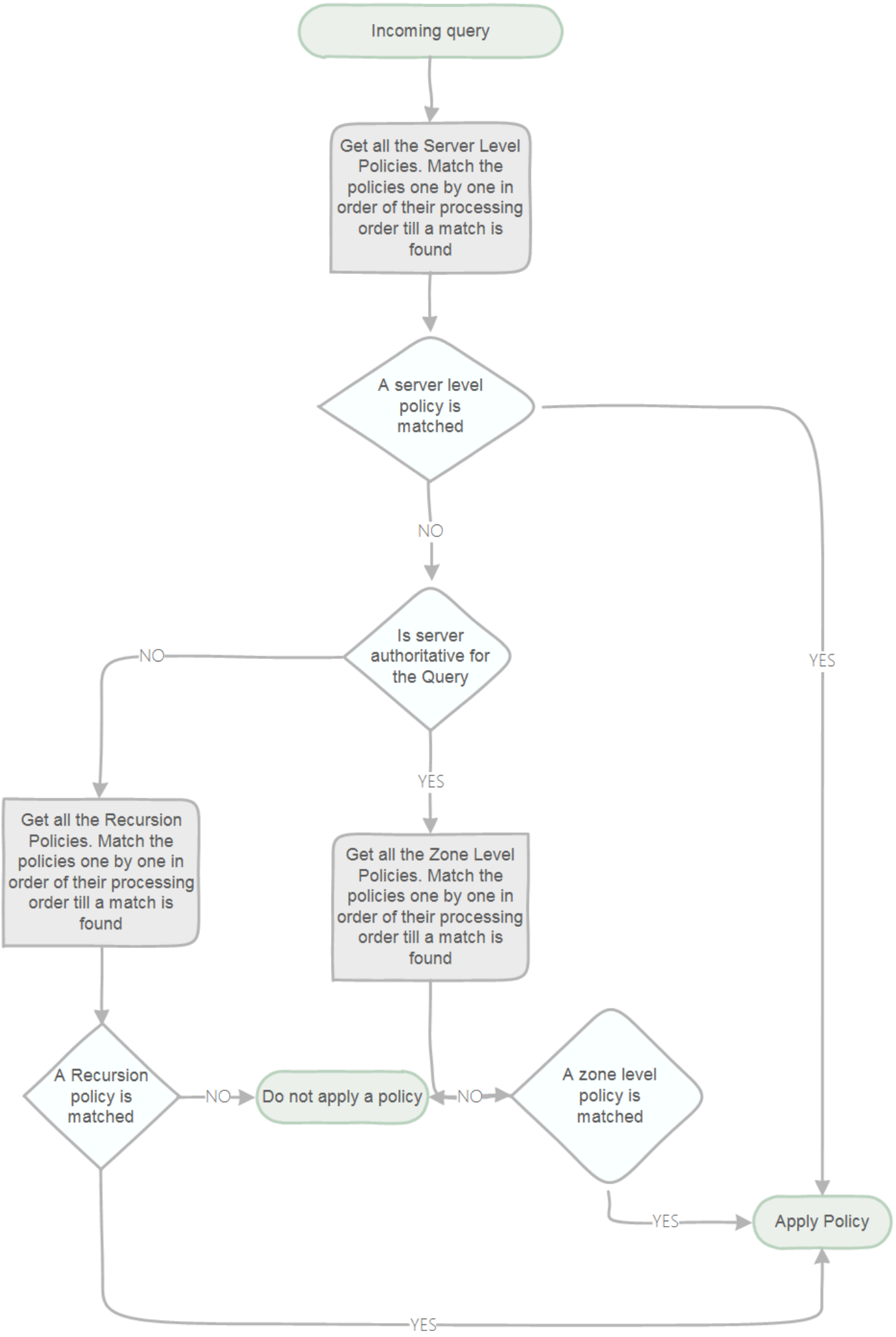
Name	Description	Exemples de valeurs
Sous-réseau client	Nom d'un sous-réseau client prédéfini. Permet de vérifier le sous-réseau à partir duquel la requête a été envoyée.	- **EQ,Espagne,France** - résout la valeur true si le sous-réseau est identifié comme l'Espagne ou la France - **NE,Canada,Mexique** - se résout à true si le sous-réseau client est un sous-réseau autre que le Canada et le Mexique
Protocole de transport	Protocole de transport utilisé dans la requête. Les entrées possibles sont **UDP** et **TCP**	- **EQ,TCP** - **EQ,UDP**
Protocole Internet	Protocole réseau utilisé dans la requête. Les entrées possibles sont **IPv4** et **IPv6**	- **EQ,IPv4** - **EQ,IPv6**
Adresse IP de l'interface serveur	Adresse IP de l'interface réseau du serveur DNS entrant	- **EQ,10.0.0.1** - **EQ,192.168.1.1**
FQDN	Nom de domaine complet d'enregistrement dans la requête, avec la possibilité d'utiliser une carte générique	- **EQ,www.contoso.com** : résout la valeur true uniquement si la requête tente de résoudre le nom de domaine complet *www.contoso.com* - **EQ,*.contoso.com,*.woodgrove.com** : résout la valeur true si la requête concerne un enregistrement se terminant par *contoso.com***OR***woodgrove.com*
Type de requête	Type d'enregistrement interrogé (A, SRV, TXT)	- **EQ,TXT,SRV** : résout la valeur true si la requête demande un enregistrement TXT **OR** SRV - **EQ,MX** : résout la valeur true si la requête demande un enregistrement MX
Heure de la journée	Heure de la réception de la requête	- **EQ,10:00-12:00,22:00-23:00** - résout la valeur true si la requête est reçue entre 10 h et midi, **OU** entre 10 h et 11 h

En utilisant le tableau ci-dessus comme point de départ, le tableau ci-dessous peut être utilisé pour définir un critère permettant de faire correspondre des requêtes pour n'importe quel type d'enregistrements, sauf les enregistrements SRV dans le domaine contoso.com provenant d'un client dans le sous-réseau 10.0.0.0/24 via TCP entre 20h et 22h jusqu'à l'interface 10.0.0.3 :

Agrandir le tableau

Name	Value
Sous-réseau client	EQ,10.0.0.0/24
Protocole de transport	EQ,TCP
Adresse IP de l’interface serveur	EQ,10.0.0.3
FQDN	EQ,*.contoso.com
Type de requête	NE,SRV
Heure de la journée	EQ,20:00-22:00

Vous pouvez créer plusieurs stratégies de résolution de requêtes du même niveau, tant qu’elles ont une valeur différente pour l’ordre de traitement. Lorsque plusieurs stratégies sont disponibles, le serveur DNS traite les requêtes entrantes de la manière suivante :


Incoming query
Get all the Server Level Policies. Match the policies one by one in order of their processing order till a match is found
A server level policy is matched
YES
NO
Is server authoritative for the Query
NO
YES
Get all the Recursion Policies. Match the policies one by one in order of their processing order till a match is found
Get all the Zone Level Policies. Match the policies one by one in order of their processing order till a match is found
A Recursion policy is matched
NO
Do not apply a policy
NO
A zone level policy is matched
YES
Apply Policy
YES

Stratégies de récursivité

Les stratégies de récursivité sont un **type** spécial de stratégies de niveau serveur. Les stratégies de récursivité contrôlent la façon dont le serveur DNS effectue la récursivité pour une requête. Les stratégies de récurrence s'appliquent uniquement lorsque le traitement de la requête atteint le chemin de récursivité. Vous pouvez choisir la valeur REFUSER ou IGNORER pour la récursivité pour un ensemble de requêtes. En alternative, vous pouvez choisir un ensemble de redirecteurs pour un ensemble de requêtes.

Vous pouvez utiliser des stratégies de récursivité pour implémenter une configuration DNS fractionnée. Dans cette configuration, le serveur DNS effectue une récursivité pour un ensemble de clients pour une requête, tandis que le serveur DNS n'effectue pas de récursivité pour d'autres clients pour cette requête.

Les stratégies de récursivité contiennent les mêmes éléments que la stratégie de résolution de requêtes DNS standard, ainsi que les éléments du tableau ci-dessous :

Agrandir le tableau

Name	Description
Appliquer sur la récursivité	Spécifie que cette stratégie doit uniquement être utilisée pour la récursivité.
Étendue de récursivité	Nom de l'étendue de récursivité.

> **Notes**
>
> Les stratégies de récursivité ne peuvent être créées qu'au niveau du serveur.

Stratégies de transfert de zone

Les stratégies de transfert de zone contrôlent si un transfert de zone est autorisé ou non par votre serveur DNS. Vous pouvez créer des stratégies pour le transfert de zone au niveau de serveur ou de la zone. Les stratégies au niveau du serveur s'appliquent à chaque requête de transfert de zone qui se produit sur le serveur DNS. Les stratégies au niveau de la zone s'appliquent uniquement aux requêtes sur une zone hébergée sur le serveur DNS. Les stratégies au niveau de la zone sont le plus souvent utilisées pour implémenter des listes bloquées ou sécurisées.

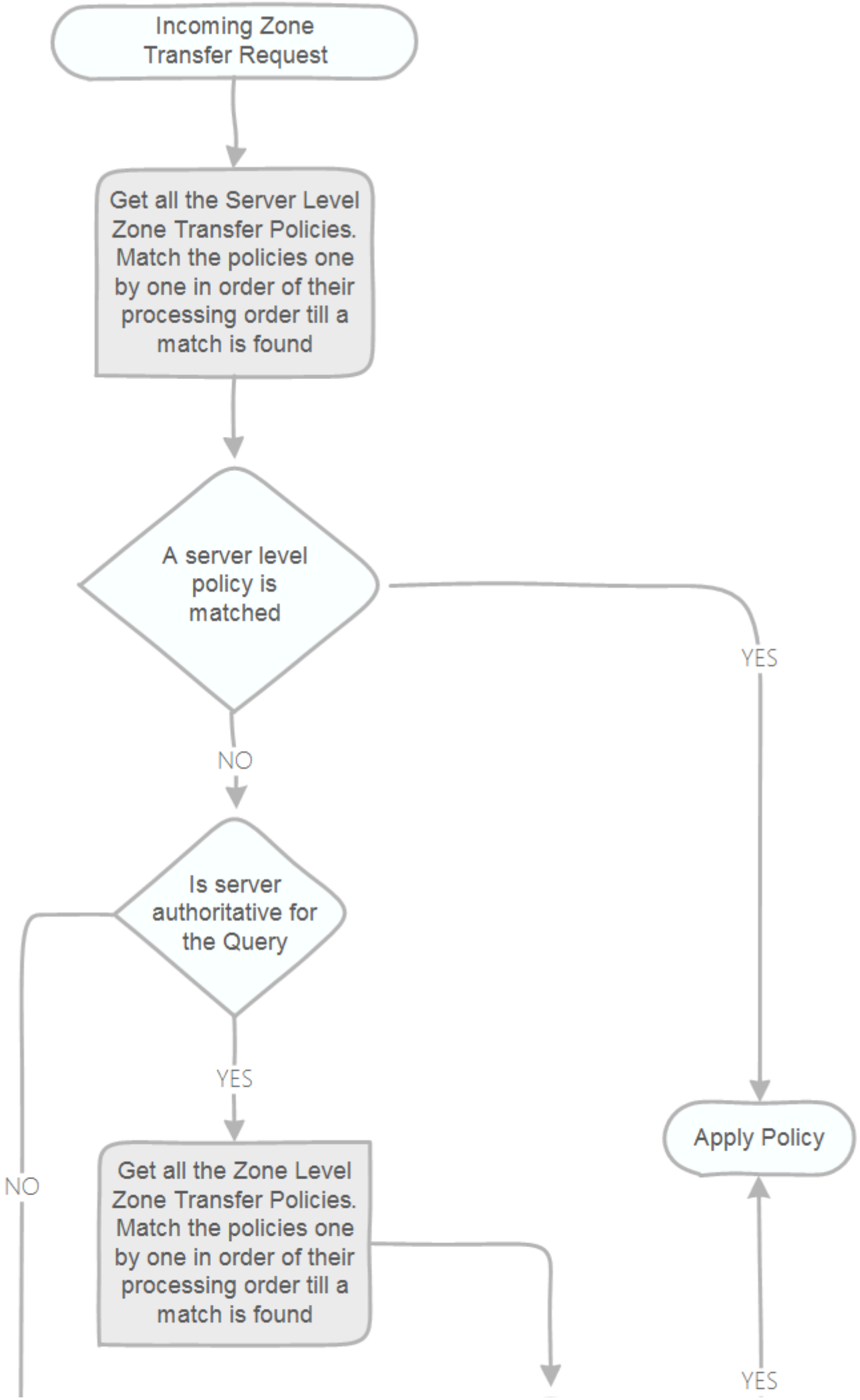
> **Notes**

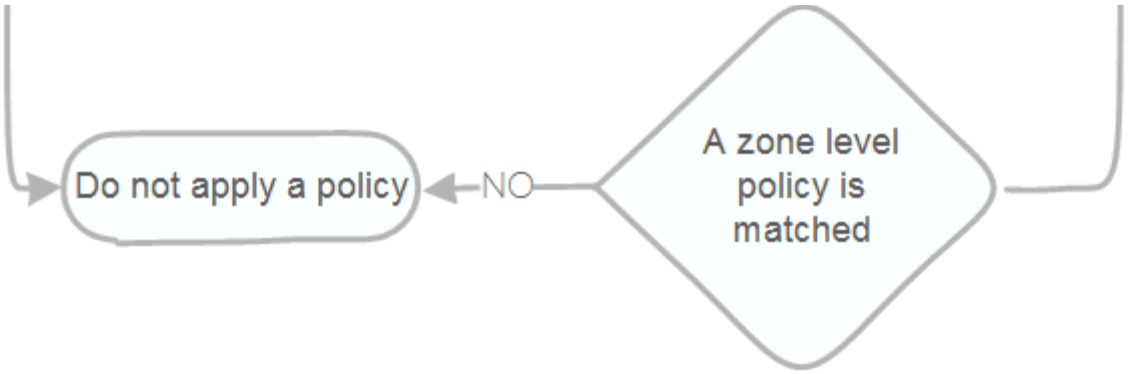
Les stratégies de transfert de zone peuvent uniquement utiliser REFUSER ou IGNORER en tant qu'actions.

Vous pouvez utiliser la stratégie de transfert de zone au niveau du serveur ci-dessous pour refuser un transfert de zone pour le domaine contoso.com à partir d'un sous-réseau donné :

```
Add-DnsServerZoneTransferPolicy -Name DenyTransferOfContosoToFabrikam -Zone
contoso.com -Action DENY -ClientSubnet "EQ,192.168.1.0/24"
```

Vous pouvez créer plusieurs stratégies de transfert de zone du même niveau, tant qu'elles ont une valeur différente pour l'ordre de traitement. Lorsque plusieurs stratégies sont disponibles, le serveur DNS traite les requêtes entrantes de la manière suivante :


Incoming Zone Transfer Request
Get all the Server Level Zone Transfer Policies. Match the policies one by one in order of their processing order till a match is found
A server level policy is matched
YES
NO
Is server authoritative for the Query
YES
NO
Get all the Zone Level Zone Transfer Policies. Match the policies one by one in order of their processing order till a match is found
Apply Policy
YES



Gestion des stratégies DNS

Vous pouvez créer et gérer des stratégies DNS à l'aide de PowerShell. Les exemples ci-dessous parcourent différents exemples de scénarios que vous pouvez configurer via des stratégies DNS :

Gestion du trafic

Vous pouvez diriger le trafic en fonction d'un nom de domaine complet vers différents serveurs en fonction de l'emplacement du client DNS. L'exemple ci-dessous montre comment créer des stratégies de gestion du trafic pour diriger les clients d'un certain sous-réseau vers un centre de données nord-américain et d'un autre sous-réseau vers un centre de données européen.

```
Add-DnsServerClientSubnet -Name "NorthAmericaSubnet" -IPv4Subnet "172.21.33.0/24"
Add-DnsServerClientSubnet -Name "EuropeSubnet" -IPv4Subnet "172.17.44.0/24"
Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "NorthAmericaZoneScope"
Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "EuropeZoneScope"
Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address
"172.17.97.97" -ZoneScope "EuropeZoneScope"
Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address
"172.21.21.21" -ZoneScope "NorthAmericaZoneScope"
Add-DnsServerQueryResolutionPolicy -Name "NorthAmericaPolicy" -Action ALLOW -
ClientSubnet "eq,NorthAmericaSubnet" -ZoneScope "NorthAmericaZoneScope,1" -
ZoneName "Contoso.com"
Add-DnsServerQueryResolutionPolicy -Name "EuropePolicy" -Action ALLOW -
ClientSubnet "eq,EuropeSubnet" -ZoneScope "EuropeZoneScope,1" -ZoneName
contoso.com
```

Les deux premières lignes du script créent des objets de sous-réseau client pour l'Amérique du Nord et l'Europe. Les deux lignes qui suivent créent une étendue de zone dans le domaine contoso.com, une pour chaque région. Les deux lignes après cela créent un enregistrement dans chaque zone qui associe `www.contoso.com` à une adresse IP différente, une pour l'Europe, une autre pour l'Amérique du Nord. Enfin, les dernières lignes du script créent deux stratégies

de résolution de requêtes DNS, l'une à appliquer au sous-réseau Amérique du Nord, l'autre au sous-réseau Europe.

Bloquer les requêtes pour un domaine

Vous pouvez utiliser une stratégie de résolution de requêtes DNS pour bloquer les requêtes dans un domaine. L'exemple ci-dessous bloque toutes les requêtes à treyresearch.net :

```
Add-DnsServerQueryResolutionPolicy -Name "BlackholePolicy" -Action IGNORE -FQDN
"EQ,*.treyresearch.com"
```

Bloquer les requêtes à partir d'un sous-réseau

Vous pouvez également bloquer les requêtes provenant d'un sous-réseau spécifique. Le script ci-dessous crée un sous-réseau pour 172.0.33.0/24, puis crée une stratégie pour ignorer toutes les requêtes provenant de ce sous-réseau :

```
Add-DnsServerClientSubnet -Name "MaliciousSubnet06" -IPv4Subnet 172.0.33.0/24
Add-DnsServerQueryResolutionPolicy -Name "BlackholePolicyMalicious06" -Action
IGNORE -ClientSubnet  "EQ,MaliciousSubnet06"
```

Autoriser la récursivité pour les clients internes

Vous pouvez contrôler la récursivité à l'aide d'une stratégie de résolution de requêtes DNS. L'exemple ci-dessous peut être utilisé pour activer la récursivité pour les clients internes, tout en la désactivant pour les clients externes dans un scénario de fractionnement du cerveau.

```
Set-DnsServerRecursionScope -Name . -EnableRecursion $False
Add-DnsServerRecursionScope -Name "InternalClients" -EnableRecursion $True
Add-DnsServerQueryResolutionPolicy -Name "SplitBrainPolicy" -Action ALLOW -
ApplyOnRecursion -RecursionScope "InternalClients" -ServerInterfaceIP
"EQ,10.0.0.34"
```

La première ligne du script modifie l'étendue de récursivité par défaut, simplement nommée « » (point) pour désactiver la récursivité. La deuxième ligne crée une étendue de *récursivité nommée InternalClients avec récursion* activée. Et la troisième ligne crée une stratégie pour

appliquer l'étendue de récursivité nouvellement créée à toutes les requêtes entrantes via une interface de serveur dont l'adresse IP est 10.0.0.34.

Créer une stratégie de transfert de zone au niveau du serveur

Vous pouvez contrôler le transfert de zone sous une forme plus granulaire à l'aide de stratégies de transfert de zone DNS. L'exemple de script ci-dessous peut être utilisé pour autoriser les transferts de zone pour n'importe quel serveur sur un sous-réseau donné :

```
Add-DnsServerClientSubnet -Name "AllowedSubnet" -IPv4Subnet 172.21.33.0/24
Add-DnsServerZoneTransferPolicy -Name "NorthAmericaPolicy" -Action IGNORE -
ClientSubnet "ne,AllowedSubnet"
```

La première ligne du script crée un objet de sous-réseau nommé *AllowedSubnet* avec le bloc IP 172.21.33.0/24. La deuxième ligne crée une stratégie de transfert de zone pour autoriser les transferts de zone vers n'importe quel serveur DNS sur le sous-réseau créé précédemment.

Créer une stratégie de transfert de zone au niveau de la zone

Vous pouvez également créer des stratégies de transfert de zone au niveau de la zone. L'exemple ci-dessous ignore toute demande de transfert de zone pour contoso.com provenant d'une interface serveur dont l'adresse IP est 10.0.0.33 :

```
Add-DnsServerZoneTransferPolicy -Name "InternalTransfers" -Action IGNORE -
ServerInterfaceIP "eq,10.0.0.33" -PassThru -ZoneName "contoso.com"
```

Scénarios de stratégie DNS

Pour plus d'informations sur l'utilisation de la stratégie DNS pour des scénarios spécifiques, consultez les rubriques suivantes dans ce guide.

- Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des serveurs principaux
- Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des déploiements principaux/secondaires
- Utiliser une stratégie DNS pour les réponses DNS intelligentes basées sur l'heure du jour
- Réponses DNS basées sur l'heure du jour avec un serveur d'applications cloud Azure
- Utiliser une stratégie DNS pour un déploiement DNS Split-Brain

- Utiliser une stratégie DNS pour un déploiement DNS Split-Brain dans Active Directory
- Utiliser une stratégie DNS pour l'application de filtres sur les requêtes DNS
- Utiliser une stratégie DNS pour l'équilibrage de charge des applications
- Utiliser une stratégie DNS pour l'équilibrage de charge des applications avec connaissance de la géolocalisation

Utiliser la stratégie DNS sur les contrôleurs de domaine en lecture seule

La stratégie DNS est compatible avec les contrôleurs de domaine en lecture seule. Notez qu'un redémarrage du service serveur DNS est nécessaire pour que les nouvelles stratégies DNS soient chargées sur les contrôleurs de domaine en lecture seule. Cela n'est pas nécessaire sur les contrôleurs de domaine accessibles en écriture.

Démarrage rapide : Installer et configurer DNS Server sur Windows Server

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Dns (Domain Name System) est essentiel pour traduire les noms de domaine en adresses IP, ce qui permet la connectivité réseau et l'accès aux ressources. Ce guide de démarrage rapide vous guide tout au long de l'installation et de la configuration du rôle serveur DNS sur Windows Server. Découvrez comment configurer des zones DNS, gérer des requêtes et configurer des options de serveur à l'aide de PowerShell ou du Gestionnaire de serveur. Vous trouverez également des informations sur la façon de transférer des requêtes DNS vers les serveurs de noms racine par défaut DNS, ou optionnellement vers un serveur de noms supérieur.

Prerequisites

Avant de pouvoir installer et configurer votre serveur DNS, votre ordinateur doit remplir les prérequis suivants :

- Un ordinateur exécutant une version de Windows Server prise en charge.
- Une adresse IP statique.
- Un compte membre du groupe Administrateurs ou équivalent.

Installer le serveur DNS

L'installation d'un serveur DNS (Domain Name System) implique l'ajout du rôle serveur DNS à un serveur Windows Server existant.

> **Conseil**
>
> Quand vous installez Active Directory Domain Services (AD DS) avec l'Assistant Installation Active Directory Domain Services, l'Assistant offre une option permettant d'installer et de configurer automatiquement un serveur DNS. La zone DNS obtenue est intégrée à l'espace de noms du domaine AD DS. Pour plus d'informations, consultez Présentation de l'intégration d'Active Directory Domain Services.

Pour installer le rôle serveur DNS en tant que serveur autonome, procédez comme suit :

PowerShell

Voici comment installer le rôle serveur DNS à l'aide de la commande Install-WindowsFeature .

1. Exécutez PowerShell sur votre ordinateur dans une session avec élévation de privilèges.

2. Pour installer le rôle DNS, exécutez la commande suivante. L'installation ne nécessite pas de redémarrage.

   PowerShell

   ```
   Install-WindowsFeature -Name DNS
   ```

Configurer le serveur DNS

Vous pouvez maintenant continuer à configurer le serveur.

Configurer des interfaces

Par défaut, un serveur DNS écoute les requêtes sur toutes les interfaces d'adresse IP. Vous pouvez configurer le serveur DNS pour écouter sur une interface spécifiée à l'aide de l'interface graphique ou à l'aide de PowerShell.

PowerShell

Voici comment configurer l'interface utilisée pour écouter les requêtes DNS à l'aide de la commande Set-DNSServerSetting .

1. Exécutez PowerShell sur votre ordinateur dans une session avec élévation de privilèges.

2. Recherchez vos ordinateurs à l'adresse IP existante en exécutant l'applet de commande Get-NetIPAddress . Notez l'adresse IP que vous souhaitez utiliser pour votre serveur DNS.

   PowerShell

   ```
   Get-NetIPAddress | fl IPAddress,InterfaceAlias
   ```

3. Stockez le paramètre de serveur DNS actuel dans une variable temporaire, définissez la propriété **ListeningIpAddress** et appliquez les nouveaux paramètres en exécutant les commandes suivantes. Remplacez l'espace réservé `<ip_address>` par l'adresse IP que vous avez notée précédemment.

   PowerShell

   ```
   $DnsServerSettings = Get-DnsServerSetting -ALL
   $DnsServerSettings.ListeningIpAddress = @("<ip_address>")
   Set-DNSServerSetting $DnsServerSettings
   ```

Configurer les indications de racine

Les serveurs d'indications de racine sont utilisés pour résoudre les informations d'adresse DNS quand le serveur DNS n'est pas en mesure de résoudre la requête localement à partir d'une zone hébergée ou du cache du serveur DNS. Les serveurs de noms d'indications de racine sont renseignés par défaut dans les nouvelles installations.

Vous pouvez modifier la liste des serveurs de noms racines si nécessaire en accédant à l'onglet **Indicateurs racines** de la boîte de dialogue Propriétés du serveur DNS ou à l'aide de PowerShell.

La suppression de tous les serveurs d'indications de racine n'est pas prise en charge. Au lieu de cela, configurez votre serveur DNS pour ne pas utiliser le serveur de noms d'indicateur racine en sélectionnant l'option Désactiver le serveur **de récursivité** dans l'onglet **Avancé** de la console du Gestionnaire DNS. La désactivation de la récursivité désactive également tous les redirecteurs configurés. Vous pouvez également désactiver l'option **Utiliser les indications de racine si aucun redirecteur n'est disponible** dans l'onglet **Redirecteurs**.

PowerShell

Voici comment mettre à jour un serveur de noms d'indicateur racine DNS à l'aide de la commande Set-DnsServerRootHint .

1. Exécutez PowerShell sur votre ordinateur dans une session avec élévation de privilèges.

2. Recherchez l'adresse IP existante de votre ordinateur en exécutant l'applet de commande Get-DnsServerRootHint . Notez le serveur de noms que vous souhaitez mettre à jour.

   PowerShell

```
Get-DnsServerRootHint
```

3. Stockez le paramètre de serveur DNS actuel dans une variable en exécutant les commandes suivantes. Remplacez l'espace réservé `<root_hint_name_server>` par le serveur de noms d'indications de racine que vous avez noté précédemment.

   PowerShell

   ```
   $RootHintServer = (Get-DnsServerRootHint | Where-Object
   {$_.NameServer.RecordData.NameServer -match "<root_hint_name_server>"} )
   ```

4. Définissez la propriété **Ipv4address** dans la variable temporaire en exécutant les commandes suivantes. Remplacez l'espace réservé `<ip_address>` par l'adresse IP mise à jour.

   PowerShell

   ```
   $RootHintServer.IPAddress[0].RecordData.Ipv4address = "<ip_address>"
   ```

5. Appliquez l'enregistrement mis à jour en exécutant les commandes suivantes.

   PowerShell

   ```
   Set-DnsServerRootHint $RootHintServer
   ```

6. Pour vérifier les indications de racine mises à jour, exécutez la commande suivante. Notez que le serveur de noms a un point de fin (.).

   PowerShell

   ```
   Get-DnsServerRootHint
   ```

Configurer des redirecteurs

Vous pouvez éventuellement configurer un redirecteur pour résoudre les informations d'adresse DNS au lieu de transférer le trafic vers les serveurs racine DNS. Vous pouvez ajouter des redirecteurs à l'aide de l'interface graphique ou à l'aide de la cmdlet PowerShell `Set-DNSServerForwarder`.

> **Notes**
>
> Les indicateurs racines DNS ne sont pas utilisés, sauf si vos redirecteurs ne répondent pas.

PowerShell

Voici comment installer le rôle serveur DNS à l'aide de la commande Install-WindowsFeature .

1. Exécutez PowerShell sur votre ordinateur dans une session avec élévation de privilèges.
2. Pour configurer les redirecteurs DNS, remplacez les espaces réservés `<ip_forwarder_1>` et `<ip_forwarder_2>` par l'adresse IP du serveur DNS que vous souhaitez utiliser comme redirecteurs. Exécutez ensuite les commande suivantes.

   PowerShell

   ```
   $Forwarders = "<ip_forwarder_1>","<ip_forwarder_2>"
   Set-DnsServerForwarder -IPAddress $Forwarders
   ```

Supprimer le rôle serveur DNS

Pour supprimer le rôle serveur DNS, procédez comme suit.

PowerShell

Voici comment désinstaller le rôle serveur DNS à l'aide de la commande Uninstall-WindowsFeature .

1. Dans une invite PowerShell avec élévation de privilèges, exécutez la commande suivante :

   PowerShell

   ```
   Uninstall-WindowsFeature -Name DNS
   ```

> **Important**

Lorsque vous supprimez le service de rôle serveur DNS d'un ordinateur Windows Server, tenez compte des points suivants :

- Pour un serveur DNS qui héberge des zones intégrées à AD DS, ces zones sont enregistrées ou supprimées selon le type de stockage. Les données de zone ne sont pas supprimées, sauf si le serveur DNS que vous désinstallez est le dernier serveur DNS hébergeant cette zone.
- Pour un serveur DNS qui héberge des zones DNS standard, les fichiers de zone restent dans le *répertoire%systemroot%\System32\Dns* , mais ils ne sont pas rechargés si le serveur DNS est réinstallé. Si vous créez une zone portant le même nom qu'une zone ancienne, l'ancien fichier de zone est remplacé par le nouveau.

Contenu connexe

- Vue d'ensemble des stratégies DNS
- Vue d'ensemble de Anycast DNS

DNS zones

30/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Une zone DNS est la partie spécifique d'un espace de noms DNS hébergée sur un serveur DNS. Une zone DNS contient des enregistrements de ressources, et le serveur DNS répond aux requêtes d'enregistrements dans cet espace de noms. Par exemple, le serveur DNS faisant autorité pour la résolution de `www.contoso.com` en adresse IP héberge la zone `contoso.com`.

Le contenu de la zone DNS peut être stocké dans un fichier ou dans Active Directory Domain Services (AD DS). Si le serveur DNS stocke la zone dans un fichier :

- Ce fichier se trouve dans un dossier local sur le serveur.
- Une seule copie de la zone est accessible en écriture.
- Les autres copies, qui sont en lecture seule, sont appelées zones secondaires.

Les zones DNS stockées dans AD DS sont appelées « zones intégrées à Active Directory ». Les zones intégrées à Active Directory sont disponibles uniquement sur les contrôleurs de domaine sur lesquels le rôle serveur DNS est installé.

Types de zones DNS

Le service Serveur DNS prend en charge les types de zones suivants :

- Primary zone.
- Secondary zone.
- Stub zone.
- Zone de recherche inversée.

Primary zones

Un serveur DNS hébergeant une zone principale constitue la principale source d'informations sur cette zone. Il stocke les données de la zone dans un fichier local ou dans AD DS. Pour créer, modifier ou supprimer des enregistrements de ressources, vous devez utiliser la zone principale. Les zones secondaires sont des copies en lecture seule des zones principales.

Vous pouvez stocker une zone principale standard dans un fichier local, ou vous pouvez stocker les données de zone dans AD DS. Quand vous stockez les données de la zone dans AD DS, d'autres fonctionnalités sont disponibles. Citons notamment les mises à jour dynamiques sécurisées et la possibilité pour chaque contrôleur de domaine qui héberge la

zone d'être utilisée comme zone primaire et de traiter les mises à jour de la zone. Lorsque la zone est stockée dans un fichier, le fichier de zone principale est nommé `zone_name.dns` par défaut et se trouve dans le dossier `%windir%\System32\Dns` sur le serveur.

Quand vous déployez Active Directory, une zone DNS associée au nom de domaine AD DS de votre organisation est automatiquement créée. Par défaut, la zone DNS AD DS est répliquée sur tout autre contrôleur de domaine configuré en tant que serveur DNS dans le domaine. Vous pouvez également configurer des zones DNS intégrées à Active Directory pour qu'elles soient répliquées sur tous les contrôleurs de domaine d'une forêt AD DS ou sur des contrôleurs de domaine spécifiques inscrits dans une partition de domaine AD DS particulière.

Secondary zone

Une zone secondaire est une copie en lecture seule d'une zone principale. Quand une zone hébergée par ce serveur DNS est une zone secondaire, le serveur DNS est une source secondaire d'informations sur cette zone. La zone de ce serveur doit être obtenue à partir d'un autre ordinateur serveur DNS distant qui héberge également la zone. Ce serveur DNS doit avoir un accès réseau au serveur DNS distant qui fournit à ce serveur des informations mises à jour sur la zone. Une zone secondaire étant simplement une copie d'une zone principale hébergée sur un autre serveur, elle ne peut pas être stockée dans AD DS en tant que zone intégrée à Active Directory.

Dans la plupart des cas, une zone secondaire copie périodiquement les enregistrements de ressources directement à partir de la zone principale. Toutefois, dans certaines configurations complexes, une zone secondaire peut copier des enregistrements de ressources à partir d'une autre zone secondaire.

Stub zone

Une zone de stub contient uniquement des informations sur les serveurs de noms faisant autorité pour la zone. La zone hébergée par le serveur DNS doit obtenir ses informations auprès d'un autre serveur DNS qui héberge la zone. Ce serveur DNS doit avoir un accès réseau au serveur DNS distant pour copier les informations du serveur de noms faisant autorité sur la zone.

Vous pouvez utiliser les zones de stub pour :

- Tenir à jour les informations sur les zones déléguées. Le serveur DNS met régulièrement à jour les enregistrements de stub pour ses zones enfants. Le serveur DNS qui héberge la zone parente et la zone de stub conserve une liste à jour de serveurs DNS faisant autorité pour la zone enfant.

- Améliorer la résolution de noms. Les zones de stub permettent à un serveur DNS d'effectuer une recherche récursive en utilisant la liste des serveurs de noms de la zone de stub, sans avoir à interroger Internet ou un serveur racine interne pour l'espace de noms DNS.
- Simplifier l'administration DNS. En utilisant des zones de stub dans votre infrastructure DNS, vous pouvez distribuer une liste des serveurs DNS faisant autorité pour une zone sans utiliser de zones secondaires. Toutefois, les zones de stub n'ont pas le même objectif que les zones secondaires et ne constituent pas une alternative pour améliorer la redondance et le partage de charge.

Il existe deux listes de serveurs DNS impliqués dans le chargement et la maintenance d'une zone de stub :

- La liste des serveurs de noms à partir desquels le serveur DNS charge et met à jour une zone de stub. Un serveur de noms peut être un serveur DNS principal ou secondaire pour la zone. Dans les deux cas, il dispose d'une liste complète des serveurs DNS pour la zone.
- La liste des serveurs DNS faisant autorité pour une zone. Cette liste est contenue dans la zone de stub à l'aide des enregistrements de ressources du serveur de noms (NS).

Quand un serveur DNS charge une zone de stub, par exemple `widgets.tailspintoys.com`, il interroge les serveurs de noms, qui peuvent se trouver à des emplacements différents, pour obtenir les enregistrements de ressources nécessaires des serveurs faisant autorité pour la zone `widgets.tailspintoys.com`. La liste des serveurs de noms peut comporter un ou plusieurs serveurs et être modifiée à tout moment.

Une zone de stub est une copie d'une zone qui contient uniquement les enregistrements de ressources nécessaires pour identifier les serveurs DNS (Domain Name System) faisant autorité pour cette zone. En règle générale, vous utilisez une zone de stub pour résoudre les noms entre des espaces de noms DNS distincts.

Si vous utilisez des sous-zones, tenez compte des points suivants :

- La zone de stub ne peut pas être hébergée sur un serveur DNS faisant autorité pour la même zone.
- Si vous intégrez la zone de stub à AD DS, vous pouvez spécifier si le serveur DNS hébergeant la zone de stub utilise une liste locale de serveurs de noms ou la liste stockée dans AD DS. Si vous souhaitez utiliser une liste de serveurs de noms locaux, vous devez disposer des adresses IP de chaque serveur de noms.

Zones de recherche inversée

Dans la plupart des recherches DNS (Domain Name System), les clients effectuent généralement une recherche directe, c'est-à-dire une recherche basée sur le nom DNS d'un

autre ordinateur stocké dans un enregistrement de ressource d'hôte (A). Ce type de requête attend une adresse IP en tant que données de ressource pour la réponse répondue.

DNS fournit également un processus de recherche inversée qui permet aux clients d'utiliser une adresse IP connue et de rechercher un nom d'ordinateur en fonction de son adresse. Une recherche inversée prend la forme d'une question, par exemple : « Pouvez-vous me dire le nom DNS de l'ordinateur qui utilise l'adresse IP 192.168.1.20 ? »

Le domaine `in-addr.arpa` a été défini dans les normes DNS et réservé dans l'espace de noms DNS Internet afin de fournir un moyen pratique et fiable d'effectuer des requêtes inversées. Pour créer l'espace de noms inversé, des sous-domaines sont formés dans le domaine `in-addr.arpa` en utilisant le classement inversé des nombres dans la notation décimale à points des adresses IP.

Le domaine `in-addr.arpa` s'applique à tous les réseaux TCP/IP basés sur l'adressage IPv4 (Internet Protocol version 4). L'Assistant Nouvelle zone part automatiquement du principe que vous utilisez ce domaine quand vous créez une zone de recherche inversée.

L'ordre des octets d'adresse IP doit être inversé lors de la création de l'arborescence du domaine `in-addr.arpa`. Les adresses IP de l'arborescence DNS `in-addr.arpa` peuvent être déléguées à des organisations, car elles se voient attribuer un ensemble spécifique ou limité d'adresses IP au sein des classes d'adresses définies par Internet.

Répliquer la base de données DNS

Plusieurs zones peuvent représenter la même partie de l'espace de noms. Ces zones peuvent être de trois types :

- Primary
- Secondary
- Stub

Une zone principale est une zone dans laquelle toutes les mises à jour des enregistrements qui appartiennent à cette zone sont effectuées. Une zone secondaire est une copie en lecture seule de la zone principale. Une zone de stub est une copie en lecture seule de la zone principale comportant uniquement les enregistrements de ressources qui identifient les serveurs DNS faisant autorité pour un nom de domaine DNS. Toutes les modifications apportées au fichier de zone principale sont répliquées dans le fichier de zone secondaire. Les serveurs DNS hébergeant une zone principale, secondaire ou de stub sont considérés comme faisant autorité pour les noms DNS de la zone.

Comme un serveur DNS peut héberger plusieurs zones, il peut donc héberger à la fois une zone principale (comportant la copie accessible en écriture d'un fichier de zone) et une zone secondaire distincte (obtenant une copie en lecture seule d'un fichier de zone). Un serveur DNS hébergeant une zone principale est considéré comme le serveur DNS principal de cette zone, et un serveur DNS hébergeant une zone secondaire est considéré comme le serveur DNS secondaire de cette zone.

> ⓘ **Notes**
>
> Une zone secondaire ou de stub ne peut pas être hébergée sur un serveur DNS qui héberge une zone principale pour le même nom de domaine.

Zone transfer

Le « transfert de zone » implique de répliquer un fichier de zone sur plusieurs serveurs DNS. Il résulte de la copie du fichier de zone d'un serveur DNS sur un autre serveur DNS. Les transferts de zone peuvent être effectués à partir de serveurs DNS principaux et secondaires.

Un serveur DNS principal est un serveur faisant autorité, configuré pour être la source du transfert de zone. Si le serveur DNS est un serveur DNS principal, le transfert de zone s'effectue directement à partir du serveur DNS hébergeant la zone principale. Si le serveur principal héberge une zone DNS secondaire, le fichier de zone reçu du serveur DNS principal avec un transfert de zone est une copie du fichier de zone secondaire en lecture seule.

Le transfert de zone est initié de l'une des manières suivantes :

- Le serveur DNS principal envoie une notification (RFC 1996) de modification du fichier de zone à un ou plusieurs serveurs DNS secondaires.
- Lorsque le service de Serveur DNS sur le serveur DNS secondaire démarre ou que l'intervalle d'actualisation de la zone expire, le serveur DNS secondaire interroge le serveur DNS principal pour obtenir les modifications. Par défaut, l'intervalle d'actualisation est défini sur 15 minutes dans le RR SOA de la zone.

Paramètres de transfert de zone

Les transferts de zone vous permettent de contrôler les circonstances dans lesquelles une zone secondaire doit être répliquée à partir d'une zone principale. Pour améliorer la sécurité de votre infrastructure DNS, autorisez les transferts de zone uniquement pour les serveurs DNS dans les enregistrements de ressources du serveur de noms (NS) pour une zone ou des serveurs DNS spécifiés. Si vous autorisez un serveur DNS à effectuer un transfert de zone, vous

autorisez le transfert des informations réseau internes vers n'importe quel hôte pouvant contacter votre serveur DNS.

Types de réplication de fichiers de zone

Il existe deux types de réplication de fichiers de zone. Le premier, le transfert de zone complet (AXFR), réplique l'intégralité du fichier de zone. Le second, le transfert de zone incrémentiel (IXFR), réplique uniquement les enregistrements modifiés.

Les logiciels de serveur DNS BIND 4.9.3 et les versions antérieures, ainsi que Windows NT 4.0 DNS, prennent en charge le transfert de zone complet (AXFR) uniquement. Il existe deux types d'AXFR : l'un nécessite un seul enregistrement par paquet, l'autre autorise plusieurs enregistrements par paquet. Le service de Serveur DNS dans les serveurs Windows prend en charge les deux types de transfert de zone, mais utilise par défaut plusieurs enregistrements par paquet. Il peut être configuré différemment pour être compatible avec les serveurs qui n'autorisent pas plusieurs enregistrements par paquet, comme les serveurs BIND versions 4.9.4 et antérieures.

Zone delegation

Vous pouvez diviser votre espace de noms DNS (Domain Name System) en une ou plusieurs zones. Vous pouvez déléguer la gestion d'une partie de votre espace de noms à un autre emplacement ou service de votre organisation en déléguant la gestion de la zone correspondante. Par exemple, vous pouvez déléguer la zone `australia.contoso.com` de la zone `contoso.com`.

Quand vous déléguez une zone, n'oubliez pas que pour chaque zone que vous créez, vous avez besoin d'enregistrements de délégation dans d'autres zones qui pointent vers les serveurs DNS faisant autorité pour la nouvelle zone. Des enregistrements de délégation sont nécessaires pour transférer l'autorité et fournir une référence correcte aux autres serveurs DNS et clients des nouveaux serveurs qui font autorité pour la nouvelle zone.

Accès aux zones et aux noms

L'accès aux zones DNS et aux enregistrements de ressources stockés dans Active Directory est contrôlé par des listes de contrôle d'accès (ACL). Les ACL peuvent être spécifiées pour le service de Serveur DNS, une zone entière ou pour des noms DNS spécifiques. Par défaut, tout utilisateur Active Directory authentifié peut créer les RR A ou PTR dans n'importe quelle zone. Lorsqu'un propriétaire crée un enregistrement A ou PTR (quel que soit le type d'enregistrement de ressource), seuls les utilisateurs ou les groupes spécifiés dans l'ACL pour ce nom qui

disposent d'une autorisation d'écriture sont autorisés à modifier les enregistrements correspondant à ce nom. Bien que cette approche soit souhaitable dans la plupart des scénarios, certaines situations doivent être examinées séparément.

DNSAdmins group

By default, the *DNSAdmins* group has full control of all zones and records in the Active Directory domain. Pour qu'un utilisateur puisse énumérer des zones dans un domaine spécifique, cet utilisateur (ou un groupe dont il fait partie) doit être inscrit dans le groupe DNSAdmin.

Il se peut qu'un administrateur de domaine ne souhaite pas accorder le contrôle total à tous les utilisateurs répertoriés dans le groupe DNSAdmins. Au lieu de cela, un administrateur de domaine peut souhaiter accorder à un ensemble spécifique d'utilisateurs un contrôle total pour une zone et des autorisations en lecture seule pour les autres zones. Pour configurer ces autorisations, l'administrateur de domaine peut créer un groupe distinct pour chacune des zones et ajouter des utilisateurs spécifiques à chaque groupe. Ensuite, la liste de contrôle d'accès (ACL) pour chaque zone contient un groupe avec un contrôle complet pour cette zone uniquement. Tous les groupes sont ajoutés au groupe DNSAdmins, qui peut être configuré avec des autorisations de lecture uniquement. L'ACL d'une zone contient toujours le groupe DNSAdmins, ce qui signifie que tous les utilisateurs inscrits dans les groupes spécifiques à une zone peuvent lire toutes les zones du domaine.

Reserving names

Les environnements qui nécessitent un haut niveau de sécurité peuvent avoir besoin de réserver des noms dans une zone et d'empêcher les utilisateurs authentifiés de créer de nouveaux noms dans cette zone, ce qui est le comportement par défaut. Pour sécuriser les enregistrements DNS, l'ACL par défaut peut être modifiée pour permettre la création d'objets par certains groupes ou utilisateurs uniquement. L'administration des ACL par nom offre une autre solution à ce problème. Un administrateur peut réserver un nom dans une zone, laissant le reste de la zone ouvert à la création de nouveaux objets par tous les utilisateurs authentifiés. Un administrateur crée un enregistrement pour le nom réservé et définit la liste appropriée de groupes ou d'utilisateurs dans l'ACL. En d'autres termes, seuls les utilisateurs répertoriés dans l'ACL peuvent enregistrer un autre enregistrement sous le nom réservé.

Next steps

- Gérer des zones DNS à l'aide d'un serveur DNS
- Présentation des stratégies DNS

- Présentation d’Anycast DNS

Architecture DNS dans Windows Server

Article • 30/04/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

DNS est une base de données distribuée hiérarchique et un ensemble de protocoles associé qui définissent :

- Mécanisme d'interrogation et de mise à jour de la base de données
- Mécanisme de réplication des informations dans la base de données entre les serveurs
- Schéma de la base de données

Les noms d'hôtes DNS résident dans une base de données qui peut être distribuée entre plusieurs serveurs, réduisant la charge sur n'importe quel serveur et permettant d'administrer ce système d'affectation de noms par partition. Le DNS prend en charge les noms hiérarchiques et permet l'enregistrement de divers types de données en plus de la correspondance nom d'hôte/adresse IP utilisée dans les fichiers HOSTS. La base de données DNS est distribuée, ce qui lui permet d'effectuer un scale-up et d'effectuer un scale-out, ce qui signifie que les performances ne sont pas dégradées lorsque d'autres serveurs sont ajoutés.

Le DNS d'origine était basé sur la requête de commentaire (RFC) 1035 (Implémentation et spécification des noms de domaine). D'autres RFC décrivent les problèmes de sécurité, d'implémentation et d'administration DNS qui ont ultérieurement enrichi les spécifications de conception d'origine.

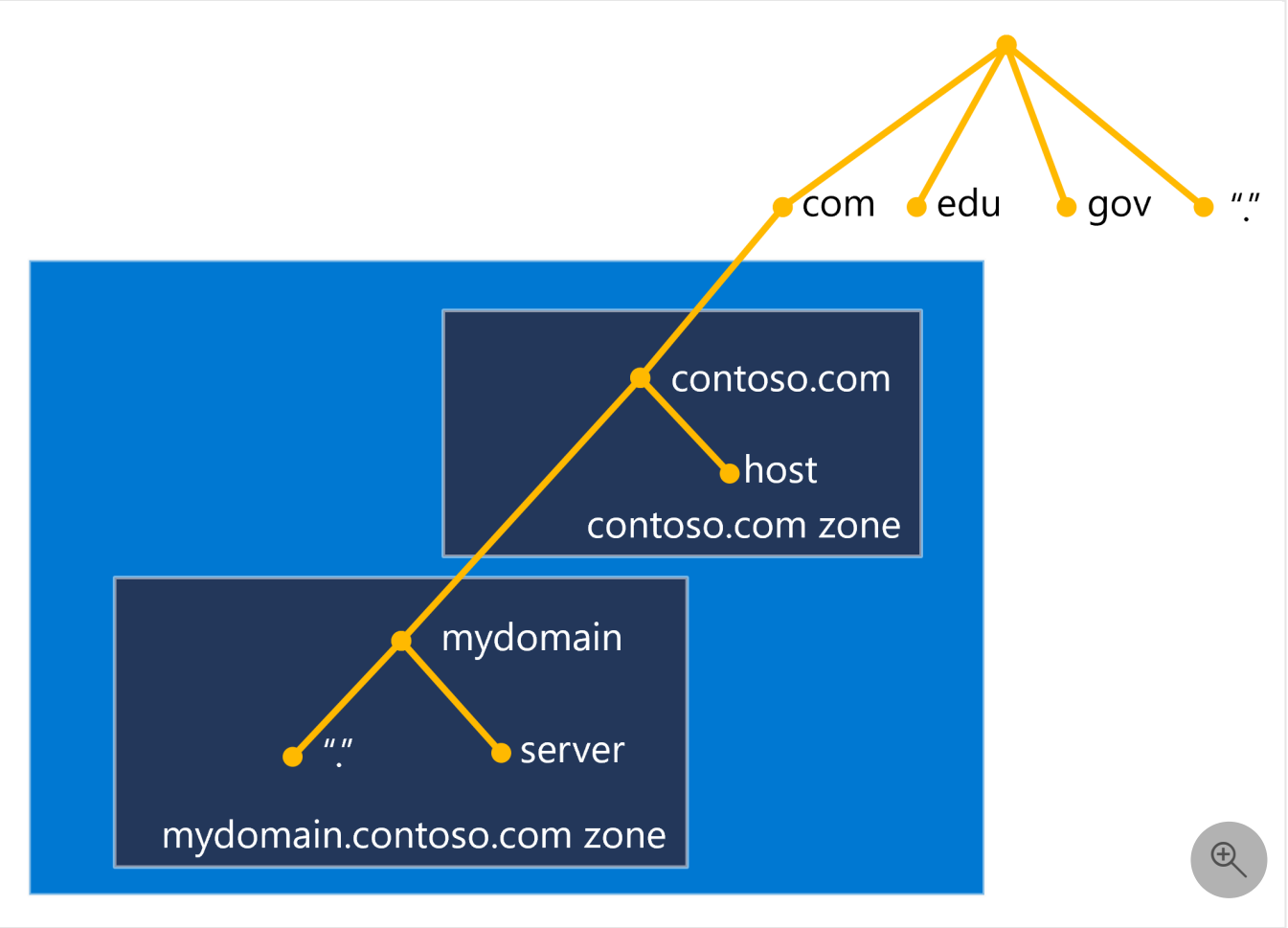
Les RFC utilisés dans les systèmes d'exploitation Windows Server sont les suivants :

- Noms de domaine - concepts et installations RFC 1034
- Noms de domaine - implémentation et spécification RFC 1035
- Extensions DNS pour prendre en charge IP version 6 RFC 1886
- Mécanisme de notification rapide des modifications de zone (NOTIFICATION DNS) RFC 1996
- Transfert de zone incrémentielle dans DNS RFC 1995
- Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)RFC 2136
- Mise en cache négative des requêtes DNS (DNS NCACHE) RFC 2308
- Enregistrements de ressources pour les extensions de sécurité DNS RFC 4034
- Modifications du protocole pour les extensions de sécurité DNS RFC 4035
- Un RR DNS pour spécifier le lieu des services (DNS SRV) RFC 2052

Noms de domaine DNS

DNS est implémenté en tant que base de données hiérarchique et distribuée contenant différents types de données, y compris les noms d'hôte et les noms de domaine. Les noms d'une base de données DNS forment une arborescence hiérarchique appelée espace de noms de domaine. Les noms de domaine se composent d'étiquettes individuelles séparées par des points, par exemple : `mydomain.contoso.com`.

Un nom de domaine complet (FQDN) identifie de façon unique la position de l'hôte dans l'arborescence hiérarchique DNS. Le nom de domaine complet (FQDN) spécifie une liste de noms séparés par des points dans le chemin d'accès de l'hôte référencé à la racine. La figure suivante montre un exemple d'arborescence DNS avec un hôte appelé `mydomain` dans le domaine `contoso.com`. Le nom de domaine complet de l'hôte serait `mydomain.contoso.com`.



Présentation de l'espace de noms de domaine DNS

L'espace de noms de domaine DNS, comme illustré dans la figure précédente, est basé sur le concept d'une arborescence de domaines nommés. Chaque niveau de l'arborescence peut représenter une branche ou une feuille. Une branche est un niveau où plusieurs noms sont utilisés pour identifier une collection de ressources nommées. Une feuille représente un nom unique utilisé une fois à ce niveau pour indiquer une ressource spécifique.

Hiérarchie des noms de domaine DNS

Les clients et serveurs DNS utilisent des requêtes comme méthode de résolution des noms dans l'arborescence pour des types spécifiques d'informations sur les ressources. Ces informations sont fournies par les serveurs DNS dans les réponses de requête aux clients DNS qui extraient ensuite les informations et les transmettent à un programme demandeur pour résoudre le nom interrogé. Dans le processus de résolution d'un nom, les serveurs DNS fonctionnent souvent en tant que clients DNS, interrogeant d'autres serveurs afin de résoudre entièrement un nom interrogé.

Contoso se voit par exemple attribuer l'autorité par les serveurs racines Internet pour la partie de l'arborescence des espaces de noms de domaine DNS sur Internet, c'est-à-dire, `contoso.com`. La résolution d'un nom en dehors de l'espace de noms `contoso.com` nécessite que les serveurs DNS Contoso interrogent d'autres serveurs DNS, tels que les serveurs racine.

Organisation de l'espace de noms de domaine DNS

Tout nom de domaine DNS utilisé dans l'arborescence est techniquement un domaine. Toutefois, la plupart des discussions DNS identifient les noms de l'une des cinq façons, en fonction du niveau et de la façon dont un nom est couramment utilisé. Par exemple, le nom de domaine DNS inscrit auprès de Contoso (`contoso.com`) est appelé domaine de second niveau. Le nom comporte deux parties (appelées étiquettes) qui indiquent qu'il se trouve à deux niveaux en dessous de la racine ou du haut de l'arborescence. La plupart des noms de domaine DNS ont deux étiquettes ou plus, chacune indiquant un nouveau niveau dans l'arborescence. Les points sont utilisés dans les noms pour séparer les étiquettes.

Le tableau suivant décrit les cinq catégories de noms de domaine DNS par leur fonction dans l'espace de noms, ainsi qu'un exemple de chaque type de nom.

Agrandir le tableau

Type de nom	Descriptif	Exemple
Domaine racine	En haut de l'arborescence, représentant un niveau sans nom ; il est parfois affiché sous la forme de deux guillemets vides (« »), indiquant une valeur Null. Lorsqu'il est utilisé dans un nom de domaine DNS, il est indiqué par une période de fin (.) pour désigner que le nom se trouve à la racine ou au niveau le plus élevé de la hiérarchie de domaine. Dans cette instance, le nom de domaine DNS est considéré comme complet et pointe vers un emplacement exact dans l'arborescence des noms.	Un point (.) seul ou un point utilisé à la fin d'un nom, tel que `example.contoso.com.`

Type de nom	Descriptif	Exemple
	Les noms indiqués de cette façon sont des FQDN (noms de domaine complets). Un point (.) seul ou un point utilisé à la fin d'un nom, tel que `example.contoso.com.`	
Domaine de niveau supérieur (TLD)	Nom utilisé pour indiquer un pays ou une région ou le type d'organisation à l'aide d'un nom.	`.com`, qui indique un nom inscrit à une entreprise pour une utilisation commerciale sur Internet.
Domaine de deuxième niveau	Noms de longueur variable inscrits auprès d'une personne ou d'une organisation à utiliser sur Internet. Ces noms sont toujours basés sur un domaine de niveau supérieur approprié, selon le type d'organisation ou l'emplacement géographique où un nom est utilisé.	`contoso.com.` est le nom de domaine de deuxième niveau inscrit auprès de Contoso par le bureau d'enregistrement de noms de domaine DNS Internet.
Sous-domaine	Autres noms qu'une organisation peut créer qui sont dérivés du nom de domaine de deuxième niveau inscrit. Les sous-domaines incluent des noms ajoutés pour développer l'arborescence DNS des noms d'une organisation et la diviser en départements ou emplacements géographiques.	`example.contoso.com.` est un sous-domaine attribué par Contoso pour une utilisation dans des exemples de noms de documentation.
Nom de l'hôte ou de la ressource	Noms qui représentent une feuille dans l'arborescence DNS des noms et identifient une ressource spécifique. En règle générale, l'étiquette la plus à gauche d'un nom de domaine DNS identifie un ordinateur spécifique sur le réseau. Par exemple, si un nom à ce niveau est utilisé dans un enregistrement de ressource hôte (A), il est utilisé pour rechercher l'adresse IP de l'ordinateur en fonction de son nom d'hôte.	`host-a.example.contoso.com.` La première étiquette (host-a) est le nom d'hôte DNS d'un ordinateur spécifique sur le réseau.

Domaines DNS et Internet

Les autorités d'inscription Internet gèrent le système de noms de domaine. Les autorités d'inscription sont responsables de la gestion des domaines de niveau supérieur attribués par l'organisation et par pays/région. Ces noms de domaine suivent la Norme internationale pour les codes de pays (ISO 3166). Il existe des centaines de noms de domaine de niveau supérieur disponibles pour une utilisation par le public. Le tableau suivant présente quelques TLD courants, ainsi que des exemples d'abréviations à deux lettres utilisées pour les pays et les régions.

Agrandir le tableau

Nom de domaine DNS	Type d'organisation
.Com	Organisations commerciales
.edu	Établissements d'enseignement
.Org	Organisations à but non lucratif
.net	Réseaux (principal de l'Internet)
.Gov	Organisations gouvernementales non militaires
.mil	Organisations gouvernementales militaires
.arpa	DNS inversé
.xx	Codes pays à deux lettres (par exemple, `.us`, `.au`, `.ca`., `.fr`)

Enregistrements de ressources DNS

Les enregistrements de ressources DNS contiennent les informations qu'une zone gère sur les ressources (telles que les hôtes) que la zone contient. Un enregistrement de ressource classique se compose des éléments suivants :

- Nom (hôte) de l'enregistrement de ressource.
- Informations sur la durée pendant laquelle l'enregistrement de ressource peut rester dans le cache.
- Type d'enregistrement de ressource, tel qu'un enregistrement de ressource hôte (A).
- Données spécifiques au type d'enregistrement, telles que l'adresse IPv4 des hôtes.

Vous pouvez ajouter directement des enregistrements de ressources, ou ils peuvent être ajoutés automatiquement lorsque des clients compatibles avec DHCP sous Windows rejoignent un réseau grâce à la mise à jour dynamique.

Types d'enregistrements de ressources

Les enregistrements de ressources courants sont les suivants :

Agrandir le tableau

Type d'enregistrement de ressource	Descriptif
Enregistrements	Associe un nom d'hôte à une adresse IP.

Type d'enregistrement de ressource	Descriptif
hôtes (A, AAAA)	
Enregistrements alias (CNAME)	Transférez un nom de domaine ou un sous-domaine d'alias à un autre nom principal ou canonique. Les enregistrements de ressources Alias (CNAME) sont également appelés enregistrements de noms canoniques. Avec ces enregistrements, vous pouvez utiliser plusieurs noms DNS pour pointer vers un seul hôte.
Enregistrements de serveur de messagerie (MX)	Spécifie le nom d'un ordinateur qui échange ou transfère le courrier. Les applications de messagerie utilisent l'enregistrement de ressource MX (Mail Exchanger) pour localiser un serveur de messagerie en fonction d'un nom de domaine DNS dans l'adresse de destination du destinataire de messagerie d'un message. Si plusieurs enregistrements de ressources MX (Mail Exchanger) existent, le service client DNS tente de contacter les serveurs de messagerie dans l'ordre de préférence entre la valeur la plus basse (priorité la plus élevée) et la valeur la plus élevée (priorité la plus basse).
Enregistrements de pointeur (PTR)	Utilisé par les recherches DNS inversées pour mapper une adresse IP au domaine. Les enregistrements de ressources de pointeur (PTR) prennent en charge le processus de recherche inverse, en fonction des zones créées et enracinées dans le domaine `in-addr.arpa`. Vous devez disposer de la zone de recherche inversée appropriée sur votre serveur DNS pour créer un enregistrement PTR qui mappe une adresse IP à un nom d'hôte spécifique.
Enregistrements de l'emplacement du service (SRV)	Spécifie l'hôte, le port et le protocole d'un service. Les enregistrements de ressources d'emplacement de service (SRV) sont requis lorsque les clients utilisent DNS pour localiser les services d'emplacement tels que les contrôleurs de domaine Active Directory.
Enregistrements de serveur de noms (NS)	Spécifie les serveurs de noms faisant autorité pour un domaine.
Enregistrement de texte (TXT)	Active la publication de texte dans un enregistrement DNS. Les enregistrements de texte vous permettent d'ajouter des informations de texte retournées en interrogeant DNS. Les enregistrements TXT sont souvent utilisés pour authentifier la propriété des zones DNS.
Enregistrement de nom de délégation (DNAME)	Fournit un alias pour un domaine, comme un enregistrement CNAME, mais inclut tous les sous-domaines.
Enregistrement de début d'autorité (SOA)	Fournit des informations faisant autorité sur une zone DNS. L'enregistrement SOA inclut le serveur de noms principal, le contact de l'administrateur de zone DNS, les informations d'actualisation et d'autres informations.

Durée de vie des enregistrements de ressources

La valeur de durée de vie (TTL) dans un enregistrement de ressource indique une durée de temps utilisée par d’autres serveurs DNS pour déterminer la durée de mise en cache des informations d’un enregistrement avant d’expirer et de l’ignorer. Par exemple, la plupart des enregistrements de ressources créés par le service serveur DNS héritent de la durée de vie minimale (par défaut) d’une heure à partir du début de l’enregistrement de ressource d’autorité (SOA), ce qui empêche la mise en cache étendue par d’autres serveurs DNS.

Un programme de résolution de client DNS met en cache les réponses qu’il reçoit lorsqu’il résout les requêtes DNS. Ces réponses mises en cache peuvent ensuite être utilisées pour répondre à des requêtes ultérieures pour obtenir les mêmes informations. Toutefois, les données mises en cache ont une durée de vie limitée spécifiée dans le paramètre TTL retourné avec les données de réponse. TTL garantit que le serveur DNS ne conserve pas les informations si longtemps qu'elles ne deviennent obsolètes. La durée de vie du cache peut être définie sur la base de données DNS (pour chaque enregistrement de ressource individuel, en spécifiant le champ TTL de l’enregistrement et par zone via le champ de durée de vie minimale de l’enregistrement SOA) et côté programme de résolution du client DNS en spécifiant la durée de vie maximale que le programme de résolution permet de mettre en cache les enregistrements de ressources.

Il existe deux facteurs concurrents à prendre en compte lors de la définition de la durée de vie. La première est la précision des informations mises en cache, et la seconde est l’utilisation des serveurs DNS et la quantité de trafic réseau. Si la durée de vie est courte, la probabilité d’avoir d’anciennes informations est réduite considérablement, mais elle augmente l’utilisation des serveurs DNS et du trafic réseau, car le client DNS doit interroger les serveurs DNS pour les données expirées la prochaine fois qu’il est demandé. Si la durée de vie est longue, les réponses mises en cache peuvent devenir obsolètes, ce qui signifie que le programme de résolution peut donner de fausses réponses aux requêtes. En même temps, une durée de vie longue diminue l’utilisation des serveurs DNS et réduit le trafic réseau, car le client DNS répond aux requêtes à l’aide de ses données mises en cache.

Si une requête reçoit une réponse depuis le cache, la durée de vie de l’entrée est également transmise avec la réponse. Ainsi, les résolveurs qui reçoivent la réponse savent combien de temps l’entrée est valide. Les résolveurs respectent le TTL du serveur de réponse ; ils ne le réinitialisent pas en fonction de leur propre TTL. Ainsi, les entrées n'existent pas indéfiniment mais expirent lorsqu'elles passent d'un serveur DNS à un autre DNS avec une durée de vie (TTL) mise à jour.

Notes

En général, ne configurez jamais le TTL à zéro. La différence entre un réglage de 0 ou 60 est minime pour la précision de l'enregistrement, mais lorsque le TTL est réglé sur 0, cela a

un impact significatif sur les performances du serveur DNS, car le serveur DNS effectue constamment des requêtes pour les données expirées.

Zones et délégation

Une base de données DNS peut être partitionnée en plusieurs zones. Une zone est une partie de la base de données DNS qui contient les enregistrements de ressources avec les noms de propriétaire appartenant à la partie contiguë de l'espace de noms DNS. Les fichiers de zone sont conservés sur les serveurs DNS. Un seul serveur DNS peut être configuré pour héberger zéro, un ou plusieurs zones.

Chaque zone est ancrée à un nom de domaine spécifique appelé domaine racine de la zone. Une zone contient des informations sur tous les noms qui se terminent par le nom de domaine racine de la zone. Un serveur DNS est considéré comme faisant autorité pour un nom s'il charge la zone contenant ce nom. Le premier enregistrement dans n'importe quel fichier de zone est un enregistrement de ressource Start of Authority (SOA). L'enregistrement de ressource SOA identifie un serveur de noms DNS principal pour la zone comme la meilleure source d'informations pour les données de cette zone. SOA fonctionne également en tant qu'entité chargée de traiter les mises à jour de la zone.

Un nom dans une zone peut également être délégué à une autre zone hébergée sur un autre serveur DNS. La délégation est un processus d'attribution de responsabilité pour une partie d'un espace de noms DNS à un serveur DNS appartenant à une entité distincte. Cette entité distincte peut être une autre organisation, un service ou un groupe de travail au sein de votre entreprise. Cette délégation est représentée par l'enregistrement de ressource NS qui spécifie la zone déléguée et le nom DNS du serveur faisant autorité pour cette zone. La délégation entre plusieurs zones faisait partie de l'objectif de conception d'origine du DNS.

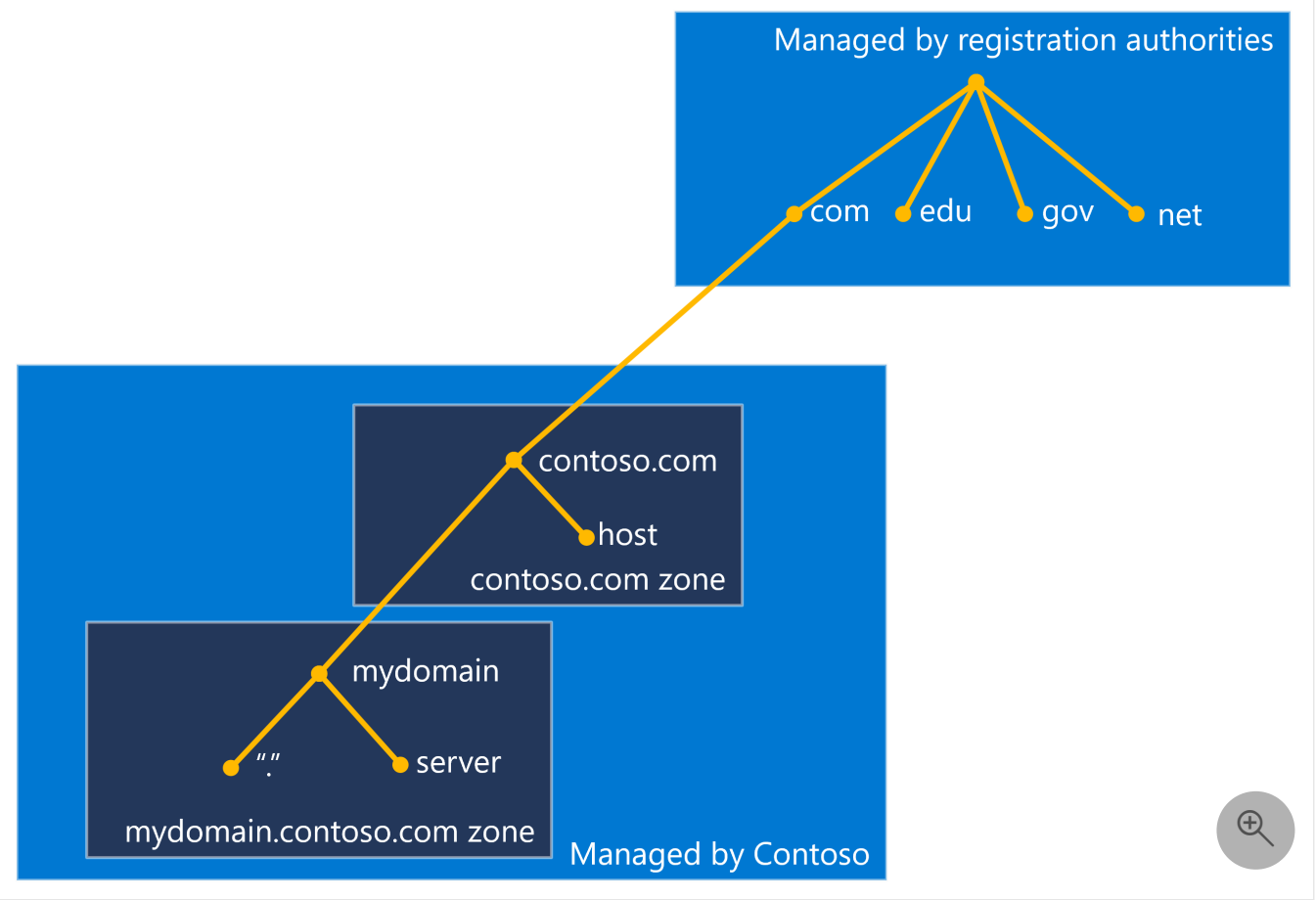
Pour en savoir plus sur les types et la réplication des zones DNS, consultez zones DNS.

Les raisons de déléguer un espace de noms DNS sont les suivantes :

- Vous devez déléguer la gestion d'un domaine DNS à de nombreuses organisations ou services au sein d'une organisation.
- Il est nécessaire de distribuer la charge de la maintenance d'une base de données DNS volumineuse entre plusieurs serveurs DNS pour améliorer les performances de résolution de noms et créer un environnement à tolérance de panne DNS.
- Vous devez autoriser l'affiliation organisationnelle d'un hôte en incluant l'hôte dans les domaines appropriés. Les enregistrements de ressources du serveur de noms (NS) facilitent la délégation en identifiant les serveurs DNS pour chaque zone et les

enregistrements de ressources NS apparaissent dans toutes les zones. Chaque fois qu'un serveur DNS doit traverser une délégation pour résoudre un nom, il fait référence aux enregistrements de ressources NS pour les serveurs DNS dans la zone cible.

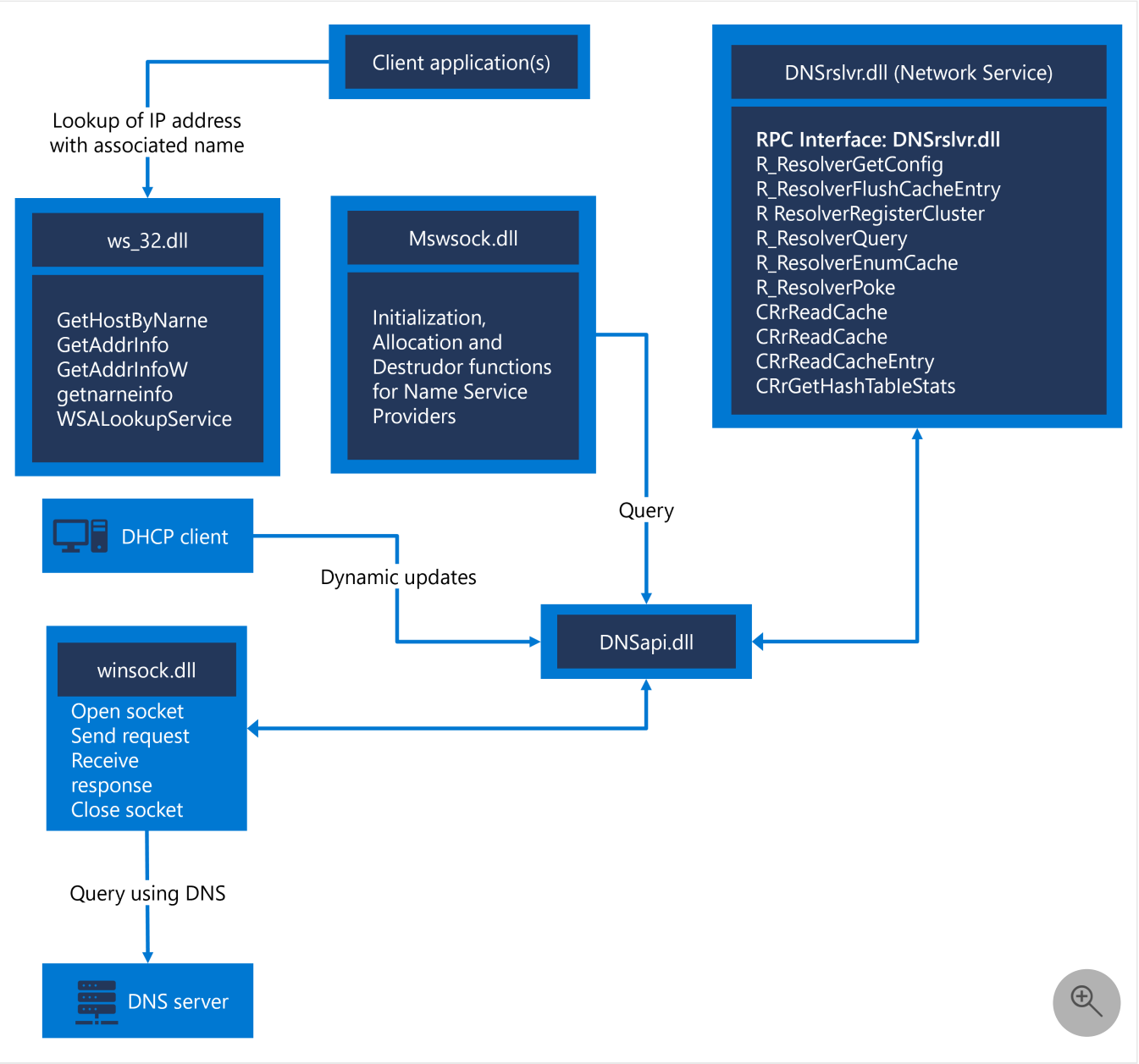
L'image suivante montre comment la gestion du domaine `contoso.com` est déléguée entre deux zones, `contoso.com` et `mydomain.contoso.com`.



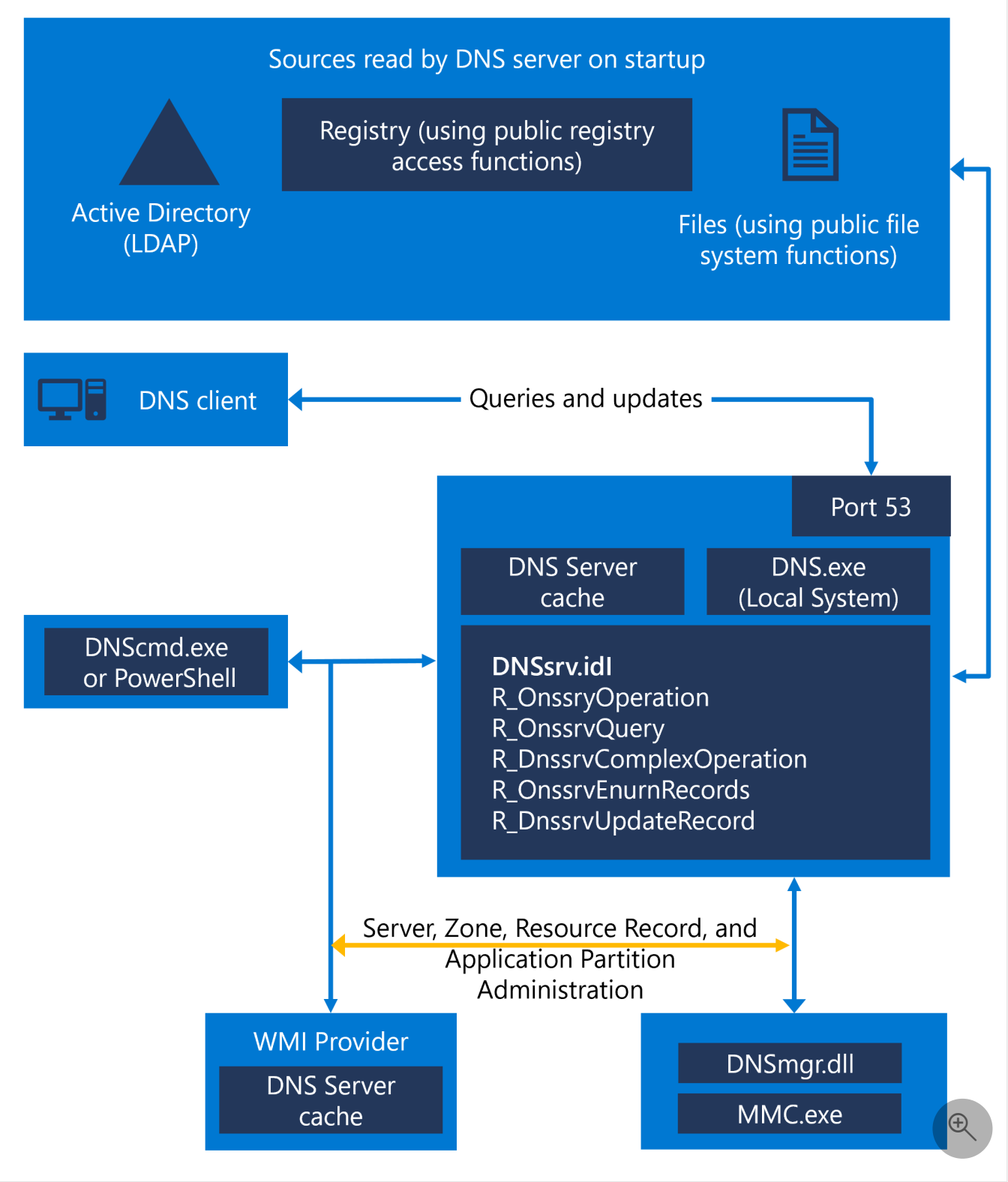
> **Notes**
>
> Si plusieurs enregistrements NS existent pour une zone déléguée identifiant plusieurs serveurs DNS disponibles pour l'interrogation, le service serveur DNS Windows Server sera en mesure de sélectionner le serveur DNS le plus proche en fonction des intervalles d'aller-retour mesurés au fil du temps pour chaque serveur DNS.

Architecture du service DNS

Le diagramme suivant illustre l'architecture du service client DNS dans ses opérations de résolution de noms et de mise à jour dans le client Windows et Windows Server. L'architecture de résolution de noms est illustrée à l'aide d'une application cliente et des mises à jour sont représentées par le client DHCP.



Le diagramme suivant illustre l'architecture du service DNS Server avec ses outils d'administration et l'interface WMI (Windows Management Instrumentation) dans Windows Server.



Les sections suivantes décrivent le processus de requête DNS et la façon dont les mises à jour DNS sont gérées.

Requêtes DNS

Les requêtes DNS peuvent être envoyées à partir d'un client DNS (programme de résolution) vers un serveur DNS ou entre deux serveurs DNS.

Une requête DNS est simplement une requête pour les enregistrements de ressources DNS d'un type d'enregistrement de ressource spécifié avec un nom DNS spécifié. Par exemple, une requête DNS peut demander tous les enregistrements de ressources de type A (hôte) avec un nom DNS spécifié.

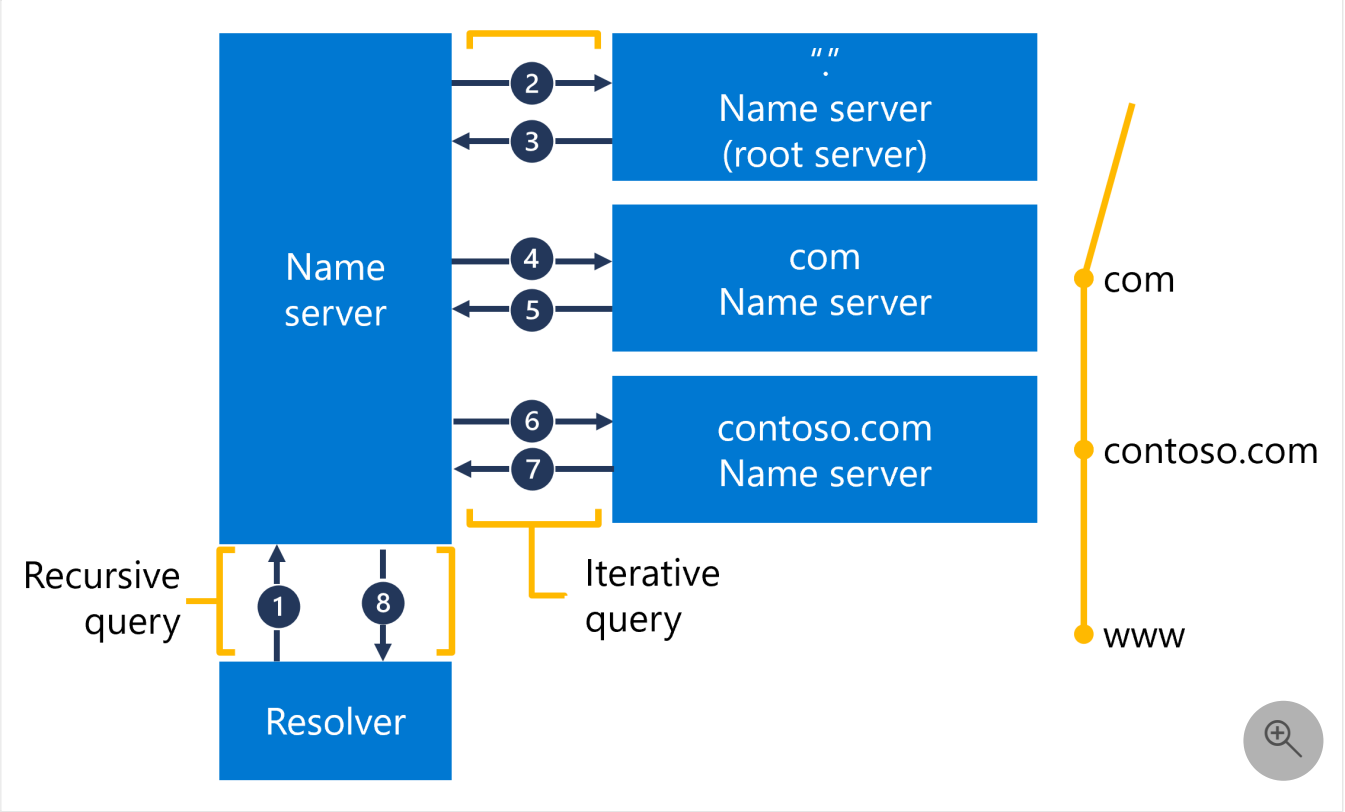
Il existe deux types de requêtes DNS qui peuvent être envoyées à un serveur DNS :

- récursive : une requête récursive force un serveur DNS à répondre à une demande avec un échec ou une réponse réussie. Les clients DNS (résolveurs) effectuent généralement des requêtes récursives. Avec une requête récursive, le serveur DNS doit contacter les autres serveurs DNS dont il a besoin pour résoudre la requête. Lorsqu'il reçoit une réponse réussie de l'autre serveur DNS (ou serveurs), il envoie ensuite une réponse au client DNS. La requête récursive est le type de requête classique utilisé par un programme de résolution interrogeant un serveur DNS et par un serveur DNS interrogeant son redirecteur, qui est un autre serveur DNS configuré pour gérer les requêtes transférées vers celui-ci.

  Lorsqu'un serveur DNS traite une requête récursive et que la requête ne peut pas être résolue à partir de données locales (fichiers de zone locaux ou cache des requêtes précédentes), la requête récursive doit être transférée à un serveur DNS racine. Chaque implémentation basée sur des normes du DNS inclut un fichier de cache (ou des indicateurs de serveur racine) qui contient des entrées pour les serveurs DNS racines des domaines Internet. (Si le serveur DNS est configuré avec un redirecteur, le redirecteur est utilisé avant l'utilisation d'un serveur racine.)

- itératif : une requête itérative est une requête dans laquelle le serveur DNS est censé répondre avec les meilleures informations locales qu'il possède, en fonction de ce que le serveur DNS connaît des fichiers de zone locale ou de la mise en cache. Cette réponse est également appelée référence si le serveur DNS ne fait pas autorité pour le nom. Si un serveur DNS n'a pas d'informations locales pouvant répondre à la requête, il envoie simplement une réponse négative. Un serveur DNS effectue ce type de requête car il tente de trouver des noms en dehors de son domaine local (ou domaines) (lorsqu'il n'est pas configuré avec un redirecteur). Il peut être amené à interroger en dehors des serveurs DNS dans une tentative de résolution du nom.

La figure suivante montre un exemple des deux types de requêtes.



Le diagramme montre comment plusieurs requêtes ont été utilisées pour déterminer l'adresse IP de `www.contoso.com`. La séquence de requêtes est décrite comme suit :

1. Requête récursive pour `www.contoso.com` (enregistrement de ressource A).
2. Requête itérative pour `www.contoso.com` (enregistrement de ressource A).
3. Référence au serveur de noms `.com` (enregistrements de ressources NS, pour `.com`) ; par souci de simplicité, les requêtes A itératives par le serveur DNS pour résoudre les adresses IP des noms d'hôte du serveur de noms renvoyés par d'autres serveurs DNS ont été omises.
4. Requête itérative pour `www.contoso.com` (enregistrement de ressource A).
5. Référence au serveur de noms `contoso.com` (enregistrement de ressource NS, pour `contoso.com`).
6. Requête itérative pour `www.contoso.com` (enregistrement de ressource A).
7. Réponse à la requête itérative du serveur contoso.com (adresse IP `www.contoso.com`).
8. Réponse à la requête récursive d'origine du serveur DNS local au résolveur (adresse IP `www.contoso.com`).

Mettre à jour DNS

Les enregistrements de ressources changent souvent en tant qu'ordinateurs, serveurs et appareils sont ajoutés ou supprimés du réseau. L'implémentation de DNS dans Windows Server prend en charge les mises à jour statiques et dynamiques de la base de données DNS.

Les enregistrements de ressources peuvent être ajoutés à une zone existante à l'aide de la commande PowerShell Add-DNSServerResourceRecord . Certains types d'enregistrements de ressources courants ont d'autres commandes PowerShell dans lesquelles vous n'avez pas besoin de spécifier le type d'enregistrement de ressource. Vous pouvez également ajouter des enregistrements de ressources à l'aide de la console du Gestionnaire DNS. Consultez La rubrique Gestion des enregistrements de ressources DNS pour obtenir des conseils sur l'utilisation des enregistrements de ressources, notamment la création et la modification d'enregistrements de ressources existants de tous les types.

Prise en charge des caractères Unicode

Lorsque DNS a été introduit dans le cadre du RFC 1035, les noms étaient limités à l'utilisation de lettres majuscules et minuscules (A-Z, a-z), nombres (0-9) et traits d'union (-). En outre, le premier caractère du nom DNS peut être un nombre et des noms doivent être encodés et représentés à l'aide de caractères US-ASCII. Pour l'utilisation de DNS dans les paramètres internationaux, cette exigence crée des limitations significatives lorsque des jeux de caractères étendus sont utilisés pour les normes d'affectation de noms locales. Le service DNS Windows Server offre une prise en charge améliorée, au-delà de la spécification RFC 1035, pour les caractères UTF-8.

Qu'est-ce que UTF-8 ?

UTF-8 est le jeu de caractères recommandé pour les protocoles qui évoluent au-delà de l'utilisation d'ASCII. Le protocole UTF-8 fournit la prise en charge des caractères ASCII étendus et de la traduction d'UCS-2, un jeu de caractères Unicode 16 bits qui englobe la plupart des systèmes d'écriture du monde. UTF-8 permet une plage de noms beaucoup plus grande que possible à l'aide d'un encodage ASCII ou étendu ASCII pour les données de caractères.

Les ordinateurs exécutant Windows Server 2008 prennent en compte UTF-8. Cela signifie que lorsque des caractères codés en UTF-8 sont reçus ou utilisés comme données par le serveur, le serveur peut charger et stocker ces données dans ses zones. Bien que les serveurs DNS Windows soient compatibles avec UTF-8, ils restent compatibles avec d'autres serveurs DNS qui utilisent l'encodage de données traditionnel US-ASCII et les normes DNS actuelles.

Comment le service DNS implémente UTF-8

Pour assurer la compatibilité et l'interopérabilité des normes avec d'autres implémentations DNS, le service DNS utilise une réduction uniforme des données de caractères reçues. Dans ce processus, le service DNS convertit tous les caractères majuscules utilisés dans les données standard US-ASCII en données équivalentes en minuscules pour les raisons suivantes :

- Pour maintenir la compatibilité avec les normes DNS actuelles et existantes.
- Pour fournir une interopérabilité avec les implémentations de serveur DNS qui ne reconnaissent pas ou ne prennent pas en charge l'encodage UTF-8.

Pour comprendre pourquoi la mise en minuscule uniforme a été choisie, plusieurs points connexes doivent d'abord être pris en compte à partir des normes Internet révisées actuelles pour le DNS. Plusieurs points clés dans les normes concernent directement la façon dont les données de caractères doivent être gérées entre les serveurs DNS et d'autres serveurs et clients. Les points clés sont les suivants :

- Toute chaîne binaire peut être utilisée dans un nom DNS. (RFC 2181)
- Les serveurs DNS doivent être en mesure de comparer les noms de manière non sensible à la casse. (RFC 1035)
- Le cas d'origine des données de caractères doit être conservé chaque fois que les données sont saisies dans le système. (RFC 1035)

La non-sensibilité à la casse étant une partie requise de la norme DNS principale, et la conservation de la casse étant une recommandation facultative, la mise en minuscule uniforme a été choisie pour fournir une solution conforme aux normes efficace. En décasant les noms codés en UTF-8 avant la transmission, d'autres serveurs DNS (qui ne sont pas conscients de UTF-8) peuvent recevoir et effectuer des comparaisons binaires réussies des données et obtenir les résultats souhaités.

Considérations relatives à l'interopérabilité avec UTF-8

Le service serveur DNS peut être défini pour autoriser ou bloquer l'utilisation de caractères UTF-8 pour chaque serveur. Certains serveurs DNS qui ne prennent pas en charge UTF-8 peuvent accepter des zones avec des noms UTF-8, mais peuvent avoir des difficultés à enregistrer ou recharger ces noms. Veillez à transférer des zones avec des noms UTF-8 vers des serveurs qui ne prennent pas en charge UTF-8.

Certains protocoles placent des restrictions sur les caractères autorisés dans un nom. En outre, les noms destinés à être globalement visibles (RFC 1958) doivent contenir des caractères ASCII uniquement, comme recommandé dans RFC 1123.

L'utilisation de UTF-8 pour transformer des caractères Unicode est invisible pour les utilisateurs. Toutefois, vous pouvez voir des caractères codés en UTF-8 si vous utilisez le moniteur réseau ou un outil similaire pour analyser le trafic DNS.

En plus de la prise en charge du serveur DNS pour le format d'encodage UTF-8, le programme de résolution du client utilise par défaut le format d'encodage de caractères UTF-8.

Les noms encodés au format UTF-8 ne doivent pas dépasser les limites de taille spécifiées dans RFC 2181, qui spécifie un maximum de 63 octets par étiquette et 255 octets par nom. Le nombre de caractères est insuffisant pour déterminer la taille, car certains caractères UTF-8 dépassent un octet de longueur.

Le protocole d'encodage UTF-8 s'adapte à l'utilisation avec les implémentations de protocole DNS existantes qui s'attendent à US-ASCII caractères, car la représentation de US-ASCII caractères dans UTF-8 est identique, octet pour octet, à la représentation US-ASCII. Les implémentations de client ou de serveur DNS qui ne reconnaissent pas les caractères UTF-8 encodent toujours les noms au format US-ASCII. Le service serveur DNS est en mesure d'interpréter correctement ces noms.

Le service DNS peut configurer la vérification des noms pour autoriser ou restreindre l'utilisation de caractères UTF-8 dans les données DNS.

Par défaut, la vérification du nom UTF-8 multioctet est utilisée, ce qui permet la plus grande tolérance lorsque le service DNS traite les caractères. La vérification de nom UTF-8 multioctet est la méthode de vérification de noms préférée pour la plupart des serveurs DNS gérés en privé qui ne fournissent pas de service de nom pour les hôtes Internet.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Ports réseau utilisés par DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Pendant la résolution DNS, les messages DNS sont envoyés des clients DNS vers des serveurs DNS ou entre des serveurs DNS. Les messages sont envoyés via des serveurs UDP et DNS liés au port UDP 53. Lorsque la longueur du message dépasse la taille de message par défaut d'un datagramme UDP (User Datagram Protocol) (512 octets), la première réponse au message est envoyée avec autant de données que le datagramme UDP autorise. Lorsque la taille du message est dépassée, le serveur DNS définit un indicateur indiquant une réponse tronquée. Le client DNS (expéditeur de message) peut ensuite choisir de réémettre la requête sur le serveur DNS à l'aide du protocole TCP (via le port TCP 53). Cette approche tire parti des performances de l'UDP mais dispose également d'une solution de basculement de secours pour les requêtes plus longues.

Les requêtes DNS sont généralement envoyées à partir d'un port source numéroté élevé (à partir de 49152 et d'augmentation) au port de destination 53. Les réponses sont envoyées à partir du port source 53 vers un port de destination à numéro élevé. Le tableau suivant répertorie les ports UDP et TCP utilisés pour différents types de messages DNS. Pour se conformer aux recommandations IANA (Internet Assigned Numbers Authority), le port de démarrage par défaut est 49152 et le port de fin par défaut est 65535. L'utilisation de ports dynamiques numérotés élevés est une modification de la configuration des versions antérieures à Windows Server 2008 qui a utilisé une plage de ports par défaut comprise entre 1025 et 5 000.

Agrandir le tableau

Type de trafic	Source de transmission	Source Port	Destination de la transmission	Port de destination
Requêtes à partir d'un serveur DNS local	Serveur DNS local	Un port aléatoire numéroté 49152 ou supérieur	Tout serveur DNS distant	53
Réponses au serveur DNS local	Tout serveur DNS distant	53	Serveur DNS local	Un port aléatoire numéroté 49152 ou supérieur
Requêtes à partir d'un serveur DNS distant	Tout serveur DNS distant	Un port aléatoire numéroté 49152 ou supérieur	Serveur DNS local	53

Type de trafic	Source de transmission	Source Port	Destination de la transmission	Port de destination
Réponses au serveur DNS distant	Serveur DNS local	53	Tout serveur DNS distant	Un port aléatoire numéroté 49152 ou supérieur

Le service serveur DNS prend en charge les mécanismes d'extension pour DNS (EDNS0), comme défini dans RFC 2671. EDNS0 permet aux demandeurs DNS de publier la taille de leurs paquets UDP et de faciliter le transfert de paquets de plus de 512 octets. Lorsqu'un serveur DNS reçoit une requête sur UDP, il identifie la taille de paquet UDP du demandeur à partir de l'enregistrement de ressource d'option (OPT) et met à l'échelle sa réponse pour contenir autant d'enregistrements de ressources que ceux autorisés dans la taille maximale de paquet UDP spécifiée par le demandeur.

Le serveur DNS Windows Server prend en charge EDNS0 et est activé par défaut. Elle peut être désactivée à l'aide du Registre. Recherchez la sous-clé de Registre suivante :

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS\Parameters`

Pour désactiver EDNS0, ajoutez une valeur DWORD avec le nom `EnableEDNSProbes` et une valeur définie sur `0x0`.

Attention

Utilisez une prudence extrême lors de la modification du Registre. Les modifications apportées au Registre ne sont pas validées par l'éditeur de Registre ou par Windows avant qu'elles ne soient appliquées. Par conséquent, des valeurs incorrectes peuvent être stockées. Des valeurs incorrectes peuvent entraîner des erreurs irrécupérables dans le système.

Formats des messages DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Cet article explique la structure et le format des messages DNS (Domain Name System) dans les environnements Windows et Windows Server. Comprendre les formats de message DNS est essentiel pour les administrateurs de serveurs DNS qui doivent analyser le trafic DNS, résoudre les problèmes de résolution de noms et optimiser les performances DNS.

DNS utilise des formats de message standardisés pour la communication entre clients et serveurs. Tous les messages DNS – qu'il s'agisse de requêtes, de réponses ou de mises à jour – se conforment à une structure commune avec des champs spécifiques déterminant comment l'information est traitée. Cet article couvre les trois principaux types de messages DNS et détaille leurs composants pour vous aider à comprendre comment fonctionne la communication DNS au niveau du protocole.

Protocoles et normes DNS

Le DNS dans Windows et Windows Server respecte les standards et protocoles définis par l'IETF (Internet Engineering Task Force). Le protocole DNS principal est spécifié dans RFC 1035, qui décrit le format des messages DNS, y compris les requêtes et les réponses. Des normes supplémentaires, telles que RFC 2136 pour les mises à jour dynamiques et RFC 4033 pour les extensions de sécurité DNS (DNSSEC), améliorent les fonctionnalités et la sécurité du DNS.

Le protocole DNS comprend différents types de messages traités en fonction des informations contenues dans leurs champs. Cette section traite des types de messages DNS et des champs présents dans chaque type de message.

Il existe trois types de messages DNS :

- Queries
- Responses
- Updates

Les requêtes et les réponses sont définies dans la norme DNS d'origine, et les mises à jour sont définies dans la RFC 2136. Les trois types suivent un format de message commun.

Pour en savoir plus sur les formats de message, consultez les sections suivantes.

Format d'un message de requête DNS

Le format de message DNS commun comprend un en-tête de 12 octets de longueur fixe et une partie variable réservée aux enregistrements de ressources DNS de type question, réponse, autorité et supplémentaires. Il peut être illustré comme suit :

Format de message de requête DNS standard

- **En-tête DNS** (longueur fixe)
- **Entrées de questions** (longueur variable)
- **Enregistrements de ressources de réponse** (longueur variable)
- **Enregistrements de ressources d'autorité** (longueur variable)
- **Enregistrements de ressources supplémentaires** (longueur variable)

En-tête d'un message de requête DNS

L'en-tête du message DNS contient les champs suivants, dans cet ordre :

Champs d'en-tête de message de requête DNS

- **ID de transaction** :
  Champ de 16 bits identifiant une transaction DNS spécifique. Il est créé par l'émetteur du message et recopié par le répondeur dans sa réponse. Cela permet au client DNS d'associer les réponses à ses requêtes.

- **Indicateurs** :
  Champ de 16 bits contenant divers indicateurs de service échangés entre le client et le serveur DNS, notamment :
  - **Requête/réponse** : champ 1 bits défini sur 0 pour une demande ou 1 pour une réponse.
  - **Code d'opération** : champ 4 bits représentant l'opération de service de nom du paquet ; `0x0` est une requête.
  - **Réponse faisant** autorité : champ 1 bits indiquant que le répondeur fait autorité pour le nom de domaine interrogé.
  - **Troncation** : champ 1 bits défini sur 1 si le nombre total de réponses a dépassé la taille du datagramme UDP. Sauf si les datagrammes UDP supérieurs à 512 octets ou EDNS0 sont activés, seuls les 512 premiers octets de la réponse UDP sont renvoyés.
  - **Récursivité souhaitée** : champ 1 bits défini sur 1 pour une requête récursive et 0 pour les requêtes itératives. Si la valeur est 0, le serveur DNS renvoie une liste d'autres serveurs DNS à partir de son cache local.
  - **Récursivité disponible** : champ 1 bits défini par un serveur DNS sur 1 s'il peut gérer les requêtes récursives. Si la récursivité est désactivée, le champ est configuré en

conséquence.
  - **Réservé** : champ 3 bits réservé et défini sur 0.
  - **Code de retour** : champ 4 bits contenant le code de retour :
    - `0` : réponse réussie (la réponse contient la réponse à la requête).
    - `0x3` : erreur de nom, indiquant qu'un serveur DNS autoritaire a répondu que le nom de domaine n'existe pas. Pour en savoir plus sur les codes de retour, consultez RCODEs DNS de l'IANA.

- **Nombre d'enregistrements de type Question** :
  Champ de 16 bits représentant le nombre d'entrées dans la section Question du message DNS.

- **Nombre d'enregistrements de type Réponse** :
  Champ de 16 bits représentant le nombre d'entrées dans la section Réponse du message DNS.

- **Nombre d'enregistrements de ressources d'autorité** :
  Champ de 16 bits représentant le nombre d'enregistrements d'autorité dans le message DNS.

- **Nombre d'enregistrements de ressources supplémentaires** :
  Champ de 16 bits représentant le nombre d'enregistrements supplémentaires dans le message DNS.

Entrées de la section Question des requêtes DNS

La section Question d'un message DNS contient le nom de domaine recherché, avec les trois champs suivants :

- **Nom de la question** :
  Nom de domaine interrogé. Les noms de domaine DNS sont exprimés sous forme de séries d'étiquettes (labels). Exemple : `microsoft.com`. Dans le champ Nom de la question, le nom de domaine est encodé en paires longueur-valeur : un octet indique la longueur de l'étiquette, suivi de l'étiquette elle-même. Par exemple, un nom comme `microsoft.com` est encodé sous la forme `0x09microsoft0x03com0x00`, où les chiffres hexadécimaux représentent des longueurs d'étiquettes, les caractères ASCII sont les étiquettes et le final `0` indique la fin du nom.

- **Type de question** :
  Entier de 16 bits représentant le type d'enregistrement demandé. Exemples de valeurs courantes :
  - `0x01` : enregistrement d'hôte (A)

- `0x02` : enregistrement du serveur de noms (NS)
- `0x05` : enregistrement d'alias (CNAME)
- `0x0C` (12) : enregistrement de recherche inversée (PTR)
- `0x0F` (15) : enregistrement d'échange de courrier (MX)
- `0x21` (33) : enregistrement de service (SRV)
- `0xFB` (251) : enregistrement de transfert de zone incrémentiel (IXFR)
- `0xFC` (252) : enregistrement de transfert de zone standard (AXFR)
- `0xFF` (255) : tous les enregistrements

- **Classe question** :
  Représente la classe de question IN (Internet), généralement définie sur `0x0001`.

Message de réponse à une requête DNS

Les sections réponse, autorité et supplémentaires d'un message de réponse DNS peuvent contenir des enregistrements qui répondent à la requête. Ces enregistrements sont formatés comme suit :

- **Nom de l'enregistrement de ressource** : nom de domaine DNS enregistré sous la forme d'un champ de longueur variable suivant la même mise en forme que le champ de nom de la question.
- **Type d'enregistrement de ressource** : valeur du type d'enregistrement de ressource.
- **Classe d'enregistrement de ressource** : code de classe d'enregistrement de ressource, classe Internet, 0x0001.
- **Durée de vie** : durée de vie exprimée en secondes sous la forme d'un champ non signé 32 bits.
- **Longueur des données de ressource** : champ de 2 octets indiquant la longueur des données de la ressource.
- **Données de** ressource : données de longueur variable correspondant au type d'enregistrement de ressource.

Le champ Nom de l'enregistrement est encodé de la même manière que le champ Nom de la question, sauf si le nom est déjà présent ailleurs dans le message DNS, auquel cas un champ de 2 octets est utilisé comme pointeur vers ce nom.

Format de message de requête de nom

Un format de message de requête de nom suit le même format que celui décrit ci-dessus pour les messages DNS. Dans un message de requête de nom typique, les champs du message DNS sont définis comme suit :

- **Identifiant de requête (ID de transaction)** :
  Défini sur une valeur unique permettant au résolveur DNS du client d'associer la réponse à la requête. L'ID de transaction de la réponse correspond toujours à celui de la requête.

- **Indicateurs** :
  Défini pour indiquer une requête standard avec récursivité activée.

- **Nombre de questions** :
  Définissez la valeur sur 1.

- **Entrée de question** :
  Défini au nom de domaine recherché et au type d'enregistrement à retourner.

Format du message de réponse à une requête de nom

Un format de message de réponse à une requête de nom suit le même format que celui décrit ci-dessus pour les messages DNS. Dans un message de requête de nom typique, les champs du message DNS seraient définis comme suit :

- **Identifiant de requête (ID de transaction)** :
  Défini sur une valeur unique permettant au résolveur DNS du client d'associer la réponse à la requête.

- **Indicateurs** :
  Défini pour indiquer une requête standard avec récursivité activée.

- **Nombre de questions** :
  Définissez la valeur sur 1.

- **Entrée de question** :
  Défini au nom de domaine recherché et au type d'enregistrement à retourner.

Format de message de requête de nom inverse

Les messages de requête inverse utilisent le format de message commun, avec les différences suivantes :

- Le client DNS construit le nom de domaine dans le domaine in-addr.arpa à partir de l'adresse IP recherchée.

- Un enregistrement de type PTR (pointeur) est interrogé au lieu d'un enregistrement A (hôte).

Format de message de mise à jour

Le format de message de mise à jour DNS utilise un en-tête définissant l'opération de mise à jour à effectuer et un ensemble d'enregistrements de ressources contenant la mise à jour. Le format de message de mise à jour DNS comprend les champs suivants :

- **Identification**. Identifiant de 16 bits attribué par le client DNS. Il est recopié dans la réponse correspondante et peut être utilisé par le demandeur pour associer les réponses à des requêtes en attente, ou par le serveur pour détecter les doublons.
- **Indicateurs**. Champ d'indicateurs de message de mise à jour DNS 16 bits. Pour obtenir une description des indicateurs, consultez la section « Champ d'indicateurs de message de mise à jour DNS » ci-dessous.
- **Nombre d'entrées de zone**. Nombre d'enregistrements de ressources dans la section Entrée de zone.
- **Nombre d'enregistrements de ressources requis**. Nombre d'enregistrements dans la section des enregistrements de ressources prérequis.
- **Nombre d'enregistrements de ressources de mise à jour**. Nombre d'enregistrements dans la section des enregistrements de ressources mis à jour.
- **Nombre d'enregistrements de ressources supplémentaires**. Nombre d'enregistrements dans la section des enregistrements de ressources supplémentaires.
- **Entrée de zone**. Désigne la zone des enregistrements à mettre à jour. Tous les enregistrements mis à jour doivent appartenir à la même zone. La section Zone ne peut donc contenir exactement qu'un enregistrement : Trois valeurs sont disponibles : ZNAME est le nom de la zone, ZTYPE doit être SOA et ZCLASS correspond à la classe de la zone.
- **Enregistrements de ressources prérequis**. Contient un ensemble de conditions qui doivent être satisfaites lorsque le message de mise à jour est reçu par le serveur maître DNS. Cinq types d'ensembles de valeurs de conditions peuvent être spécifiés :
    - Le jeu d'enregistrements de ressources existe (indépendant de la valeur). Au moins un enregistrement de ressource avec un nom et un type spécifiés (dans la zone et la classe spécifiées par la section Zone) doit exister.
    - Le jeu d'enregistrements de ressources existe (dépendant de la valeur). Un ensemble d'enregistrements de ressources avec un nom et un type spécifiés existe et comporte les mêmes membres avec les mêmes données que l'ensemble d'enregistrements de ressources spécifié dans cette section.

- Le jeu d'enregistrements de ressources n'existe pas. Il n'existe aucun enregistrement de ressource avec le nom et le type spécifiés (dans la zone et la classe indiquées dans la section Zone).
- Le nom est en cours d'utilisation. Il existe au moins un enregistrement de ressource avec un nom spécifié (dans la zone et la classe spécifiées par la section Zone). Cette condition préalable n'est pas remplie par les éléments non terminaux.
- Le nom n'est pas utilisé. Aucun enregistrement de ressource, quel qu'en soit le type, n'est associé à un nom spécifique. Cette condition préalable est remplie par les éléments non terminaux.

- **Enregistrements de mise à jour**. Contiennent les enregistrements de ressources à ajouter ou à supprimer de la zone. L'une des quatre opérations suivantes est effectuée pendant la mise à jour :
  - Ajout d'enregistrements de ressources à un ensemble existant d'enregistrements de ressources.
  - Suppression d'un ensemble d'enregistrements de ressources.
  - Suppression de tous les ensembles d'enregistrements de ressources d'un nom.
  - Suppression d'un enregistrement de ressource d'un ensemble d'enregistrements.
- **Enregistrements de ressources supplémentaires**. Contiennent les enregistrements liés à la mise à jour ou aux nouveaux enregistrements ajoutés par la mise à jour.

Champ des indicateurs de mise à jour DNS

Champ des indicateurs de mise à jour DNS utilise les indicateurs suivants :

- **Demande/réponse**. Champ d'1 bit : 0 = requête de mise à jour ; 1 = réponse de mise à jour.
- **Code d'opération**. Champ de 4 bits : défini sur 0x5 pour les mises à jour DNS.
- **Reserved**. Champ réservé de 7 bits : défini sur 0.
- **Retourne le code**. Champ de 4 bits : contient le code de résultat de la requête de mise à jour. Les codes sont les suivants :
  - **0 (NOERROR)** : Aucune erreur ; mise à jour réussie.
  - **1 (FORMERR)** : Erreur de format ; Le serveur DNS n'a pas compris la demande de mise à jour.

- **0x2 (SERVFAIL)** : un serveur DNS a rencontré une erreur interne, telle qu'un délai d'attente de transfert.
- **0x3 (NXDOMAIN)** : un nom qui doit exister n'existe pas.
- **0x4 (NOTIMP)** : le serveur DNS ne prend pas en charge le code d'opération spécifié.
- **0x5 (REFUSED)** : le serveur DNS refuse d'effectuer la mise à jour.
- **0x6 (YXDOMAIN)** : un nom qui n'existe pas n'existe pas.
- **0x7 (YXRRSET)** : un jeu d'enregistrements de ressources qui n'existe pas existe.
- **0x8 (NXRRSET)** : un jeu d'enregistrements de ressources qui doit exister n'existe pas.
- **0x9 (NOTAUTH)** : le serveur DNS ne fait pas autorité pour la zone nommée dans la section Zone.
- **0xA (NOTZONE)** : un nom utilisé dans les sections Prérequis ou Mise à jour n'est pas dans la zone spécifiée par la section Zone.

Format de message de réponse à une mise à jour dynamique

Suit le même format que le message de mise à jour DNS, à l'exception des indicateurs DNS. Les indicateurs d'en-tête du message de réponse de mise à jour dynamique indiquent si la mise à jour a réussi en incluant le code de réponse réussi ou l'un des codes d'erreur décrits dans les indicateurs de message de mise à jour DNS.

Requêtes et recherches DNS

29/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Cet article fournit une vue d'ensemble du processus de requête DNS (Domain Name System) et de la façon dont les serveurs DNS résolvent les requêtes. Il explique également comment les serveurs DNS utilisent la récursivité et l'itération pour résoudre les requêtes.

Fonctionnement des requêtes DNS

Lorsqu'un client DNS a besoin de rechercher un nom, il interroge les serveurs DNS pour résoudre ce nom. Chaque message de requête envoyé par le client contient trois informations, spécifiant une question à laquelle le serveur doit répondre :

- Un nom de domaine DNS spécifié, indiqué comme un nom de domaine complet (FQDN).
- Un type de requête spécifié, qui peut spécifier un enregistrement de ressource (RR) par type ou un type d'opération de requête spécialisé.
- Classe spécifiée pour le nom de domaine DNS. Pour les serveurs DNS exécutant le système d'exploitation Windows, cette classe doit toujours être spécifiée en tant que classe Internet (IN).

Par exemple, le nom spécifié peut être le nom de domaine complet d'un ordinateur, tel que `host-a.example.contoso.com.`, et le type de requête spécifié pour rechercher une adresse de RR (A) portant ce nom. Considérez une requête DNS comme un client posant à un serveur une question en deux parties, telle que « Y a-t-il des enregistrements de ressource A pour un ordinateur nommé `hostname.example.contoso.com.` ? » Lorsque le client reçoit une réponse du serveur, il lit et interprète la réponse de RR A et apprend ainsi l'adresse IP de l'ordinateur qu'il a demandé à partir de son nom.

Le tableau suivant décrit les types de requêtes DNS courants et les ID correspondants.

Agrandir le tableau

Type	ID
A	1
AAAA	28
SOA	6
SRV	33

Les requêtes DNS se résolvent de différentes manières. Un client peut parfois répondre à une requête localement à l'aide d'informations mises en cache obtenues à partir d'une requête précédente. Le serveur DNS peut utiliser son propre cache d'informations d'enregistrement de ressource pour répondre à une requête. Un serveur DNS peut également interroger d'autres serveurs DNS pour le compte du client. Ce processus est appelé récursivité. Le serveur résout le nom, puis renvoie une réponse au client.

De plus, le client lui-même peut tenter de contacter d'autres serveurs DNS pour résoudre un nom. Pour ce faire, il utilise des requêtes distinctes basées sur les réponses de référence des serveurs. On parle alors d'itération.

En général, le processus de requête DNS se déroule en deux parties :

- Une requête de nom commence sur un ordinateur client et est transmise à un résolveur, le service client DNS, pour résolution.
- Lorsque la requête ne peut pas être résolue localement, les serveurs DNS peuvent être interrogés si nécessaire pour résoudre le nom.

Chaque processus est expliqué plus en détail dans cet article.

Fonctionnement de l'itération

L'itération est le type de résolution de noms utilisé entre les clients DNS et les serveurs lorsque les conditions suivantes sont remplies :

- Le client demande l'utilisation de la récursivité, mais celle-ci est désactivée sur le serveur DNS.
- Le client ne demande pas l'utilisation de la récursivité lors de l'interrogation du serveur DNS.

Une requête itérative d'un client indique au serveur DNS que le client attend la meilleure réponse que le serveur DNS peut fournir immédiatement, sans contacter d'autres serveurs DNS.

Lorsque l'itération est utilisée, un serveur DNS répond à un client en fonction de sa propre connaissance spécifique de l'espace de noms concernant les données de noms interrogées. Par exemple, si un serveur DNS de votre intranet reçoit une requête d'un client local pour `www.contoso.com`, il peut renvoyer une réponse à partir de son cache de noms. Si le nom interrogé n'est pas actuellement stocké dans le cache de noms du serveur, celui-ci peut répondre en fournissant une référence. Une référence est une liste de RR NS et A vers d'autres serveurs DNS qui sont plus proches du nom demandé par le client.

Lorsqu'une itération est utilisée, un serveur DNS peut contribuer à la résolution d'une requête de nom au-delà du renvoi de sa propre meilleure réponse au client. Pour la plupart des requêtes itératives, un client utilise sa liste de serveurs DNS configurée localement pour contacter d'autres serveurs de noms dans l'espace de noms DNS si son serveur DNS principal ne peut pas résoudre la requête.

Le service client DNS Windows n'effectue pas de récursivité.

Comment la mise en cache fonctionne

Lorsque les serveurs DNS traitent les requêtes des clients à l'aide de la récursivité ou de l'itération, ils découvrent et acquièrent un stock important d'informations sur l'espace de noms DNS. Le serveur met ensuite ces informations en cache.

La mise en cache permet d'accélérer les performances de la résolution DNS pour les prochaines requêtes de noms populaires, tout en réduisant considérablement le trafic de requêtes DNS sur le réseau.

Lorsque les serveurs DNS effectuent des requêtes récursives pour le compte des clients, ils mettent temporairement en cache les enregistrements de ressources. Les enregistrements de ressources mis en cache contiennent des informations obtenues à partir de serveurs DNS. Ces serveurs font autorité pour les noms de domaine DNS. Les informations sont apprises lors de requêtes itératives. Ces requêtes permettent de répondre entièrement à une requête récursive effectuée pour le compte d'un client. Par la suite, lorsque d'autres clients placent de nouvelles requêtes qui demandent des informations d'enregistrement de ressource correspondant aux enregistrements mis en cache, le serveur DNS peut utiliser les informations mises en cache pour y répondre.

Lorsque des informations sont mises en cache, une valeur de durée de vie (TTL) s'applique à tous les enregistrements de ressources mis en cache. Tant que la durée de vie d'un enregistrement de ressource mis en cache n'expire pas, un serveur DNS peut continuer à mettre en cache. Il peut réutiliser l'enregistrement de ressource mis en cache lorsqu'il répond à des requêtes de ses clients qui correspondent à ces enregistrements. Les valeurs de durée de vie de mise en cache utilisées par les enregistrements de ressources dans la plupart des configurations de zone se voient attribuer la TTL minimale (par défaut) qui est définie dans l'enregistrement de ressource SOA (Start of Authority) de la zone. Par défaut, la durée de vie minimale est de 3 600 secondes (une heure), mais elle peut être ajustée ou, si nécessaire, des durées de vie individuelles de mise en cache peuvent être définies pour chaque enregistrement de ressource.

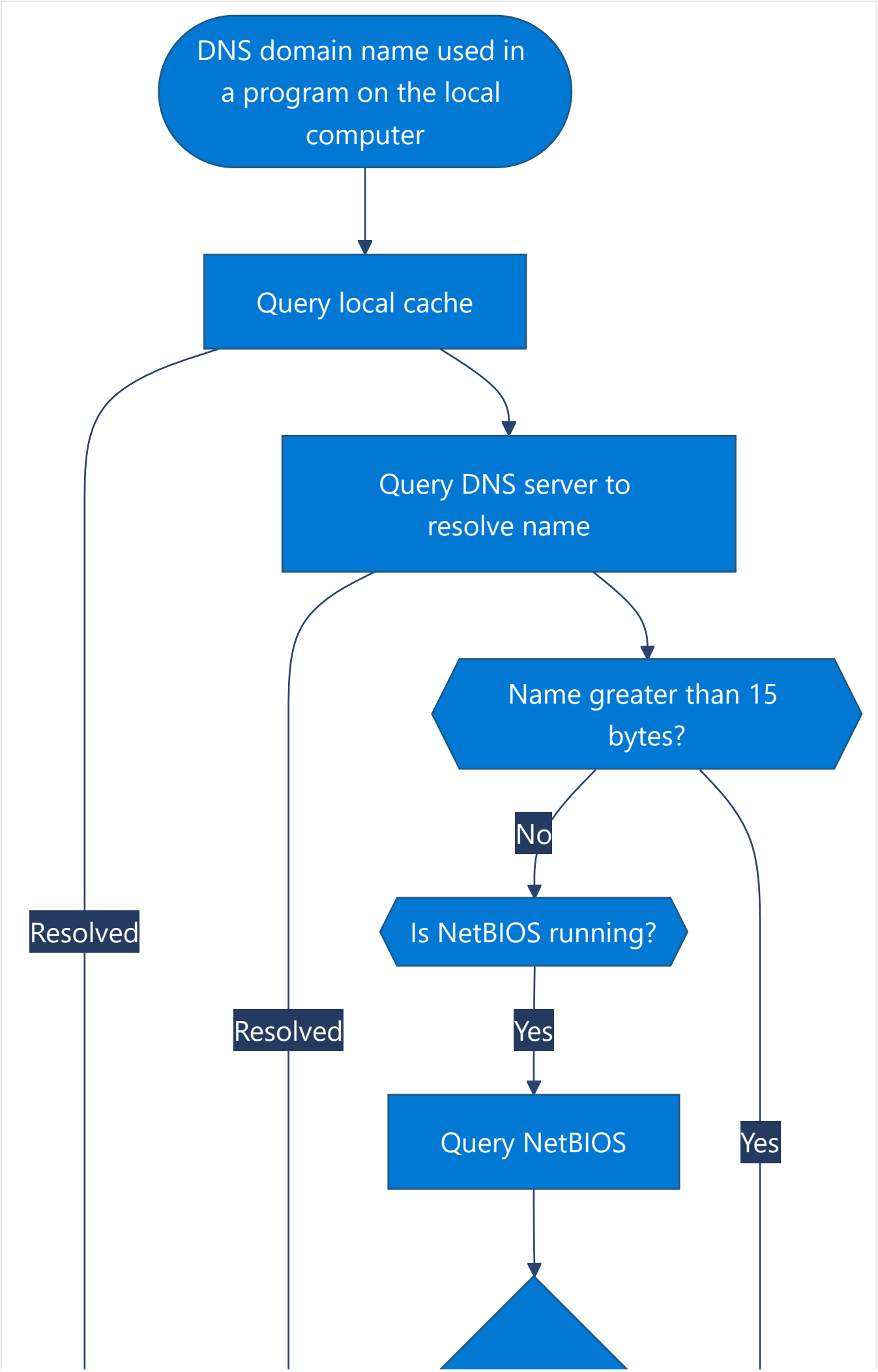
Notes

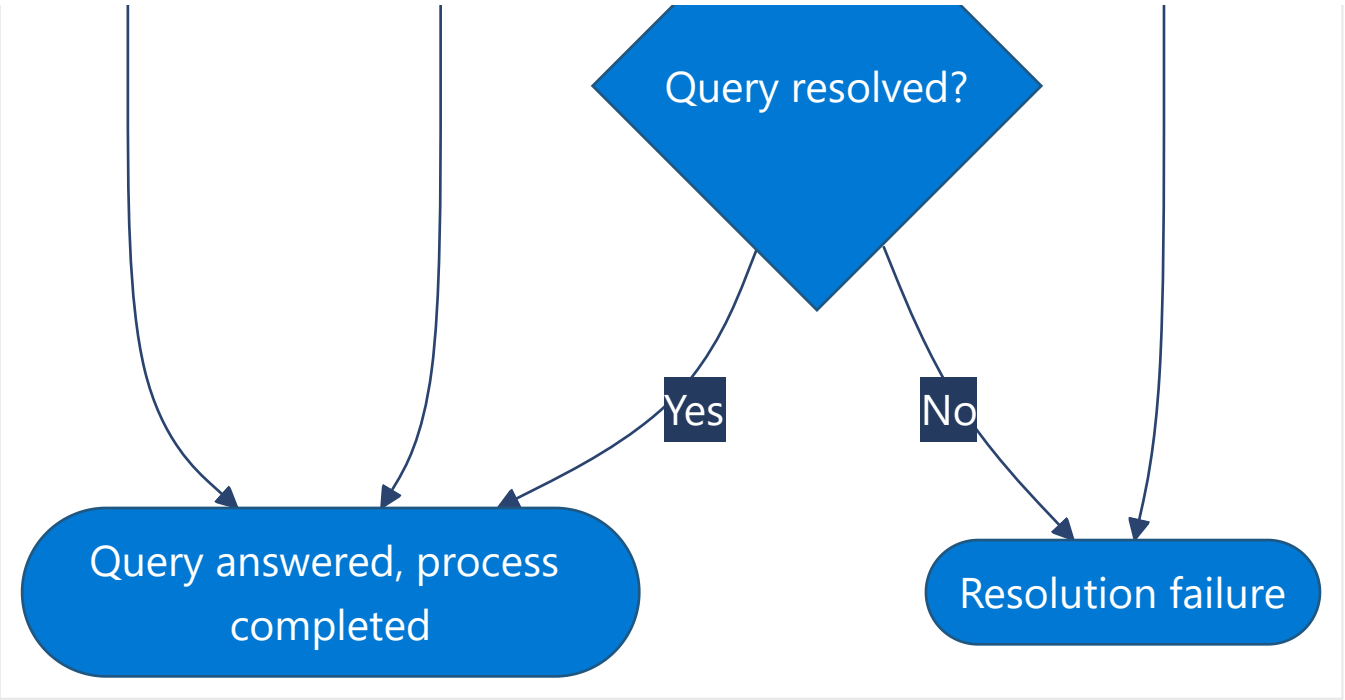
Par défaut, le service Serveur DNS utilise un fichier d'indications de racine, `cache.dns`, qui est stocké dans le dossier `<systemroot>\System32\Dns` de l'ordinateur serveur. Ce fichier contient les enregistrements de ressources NS et A pour les serveurs racine de l'espace de noms DNS (les serveurs racine Internet ou les serveurs racines intranet). Lorsque le service de serveur DNS est démarré, la liste des serveurs racine est interrogée pour obtenir une liste actuelle de tous les serveurs racines. Les résultats de la requête sont utilisés pour mettre à jour le fichier d'indications de racine. Cette opération est également effectuée périodiquement pendant l'exécution du service. Lorsqu'un administrateur apporte des modifications aux indications de racine, ces modifications sont écrites dans le fichier d'indications de racine.

Résolution du service client DNS

Lorsqu'un nom de domaine DNS est utilisé dans un programme sur l'ordinateur local, la demande est ensuite transmise pour résolution au service client DNS, qui vérifie d'abord les informations mises en cache localement. Si le nom interrogé peut être résolu, la réponse à la requête est donnée et le processus est terminé.

Le diagramme suivant montre un exemple simple d'un client DNS interrogeant le service client DNS pour une résolution de nom.


DNS domain name used in a program on the local computer
Query local cache
Resolved
Query DNS server to resolve name
Resolved
Name greater than 15 bytes?
No
Is NetBIOS running?
Yes
Query NetBIOS
Yes

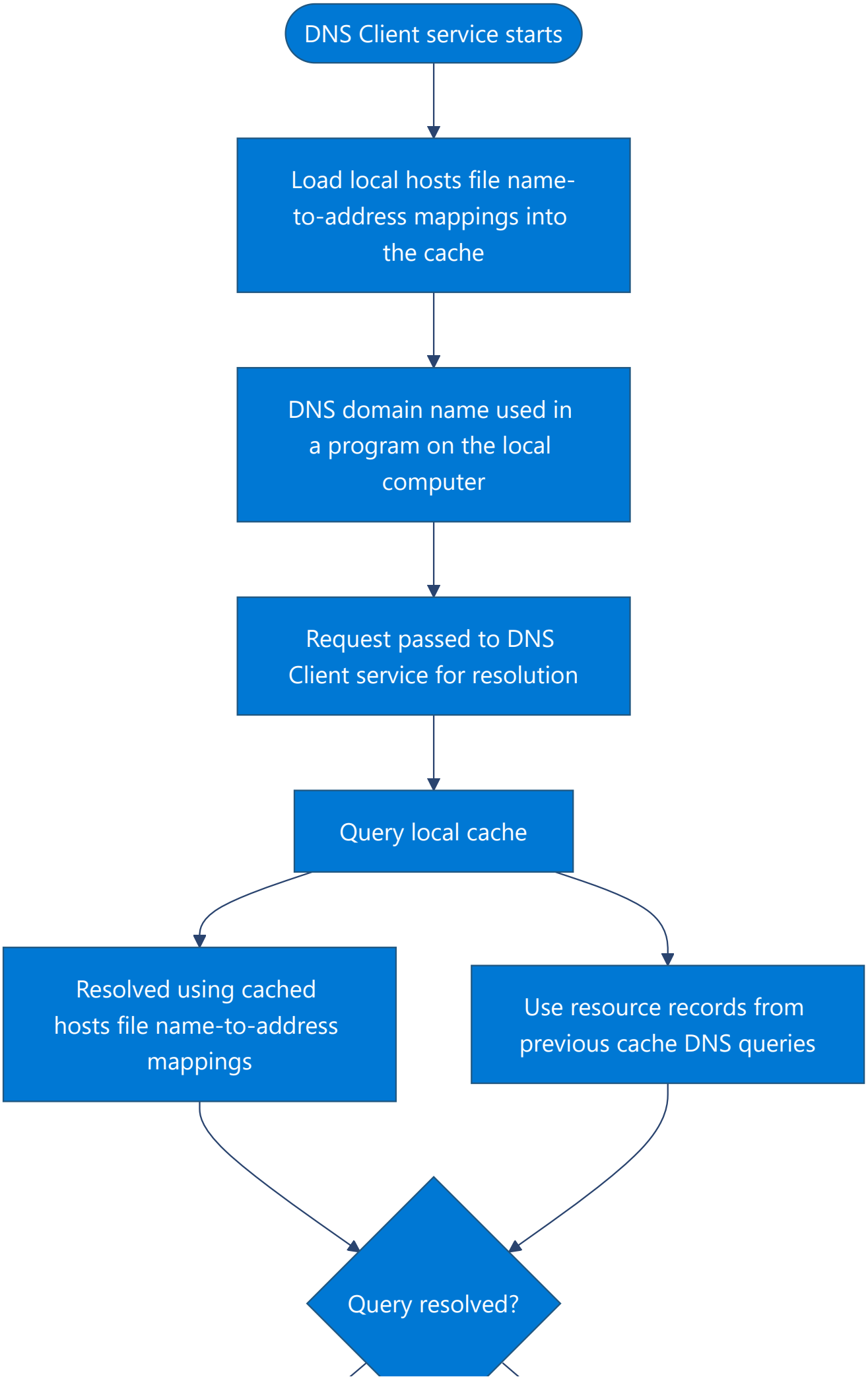


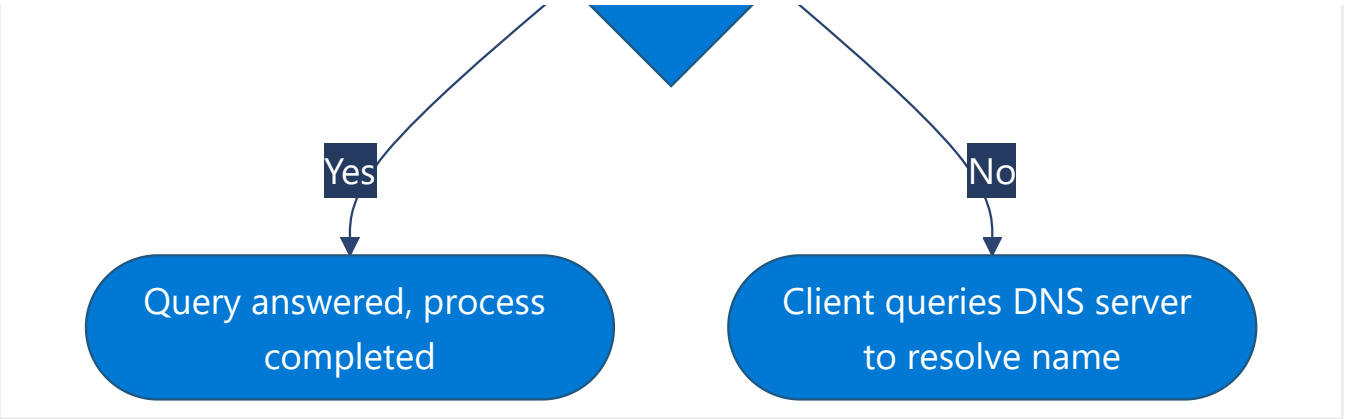
Le cache du résolveur local peut inclure des informations de nom obtenues à partir de deux sources possibles :

- Si un fichier Hosts est configuré localement, tous les mappages nom d'hôte-adresse de ce fichier sont chargés dans le cache au démarrage du service Client DNS.
- Les enregistrements de ressources obtenus dans les réponses aux requêtes DNS précédentes sont ajoutés au cache et conservés pendant une durée déterminée par la durée de vie (TTL).

Si la requête ne correspond pas à une entrée dans le cache, le processus de résolution se poursuit : le client interroge un serveur DNS pour résoudre le nom.

Le diagramme suivant montre le service Client DNS vérifiant le cache pour une requête DNS.


DNS Client service starts
Load local hosts file name-to-address mappings into the cache
DNS domain name used in a program on the local computer
Request passed to DNS Client service for resolution
Query local cache
Resolved using cached hosts file name-to-address mappings
Use resource records from previous cache DNS queries
Query resolved?



La configuration de clients DNS avec plusieurs adresses IP de serveur DNS ajoute une tolérance aux pannes à votre infrastructure DNS. L'ajout de plusieurs adresses IP de serveur DNS garantit que les noms DNS peuvent toujours être résolus en cas de défaillance du serveur DNS principal, de la liaison réseau ou de l'infrastructure de prise en charge.

Les défaillances de noms peuvent entraîner le blocage d'applications ou de composants, des pannes de ressources en attendant l'expiration des délais dépendants, ce qui provoque directement ou indirectement des défaillances opérationnelles. Consultez Délais d'expiration de la résolution du client DNS pour plus d'informations sur tous les scénarios possibles.

Pour ces raisons, nous vous recommandons de configurer tout client Windows avec plus d'un serveur DNS. Toutefois, le processus de résolution du client Windows varie en fonction du nombre de serveurs DNS configurés.

Processus de requête du serveur DNS

Lorsque le serveur DNS reçoit une requête, il vérifie d'abord s'il peut y répondre avec une source d'autorité. Le serveur DNS effectue des vérifications à l'aide des informations d'enregistrement de ressource contenues dans une zone configurée localement sur le serveur.

Si le nom interrogé renvoie une correspondance de RR dans les informations de zone locale, le serveur répond avec une source d'autorité, en utilisant ces informations pour résoudre le nom interrogé.

S'il n'existe aucune information de zone pour le nom interrogé, le serveur vérifie ensuite s'il peut résoudre le nom à l'aide des informations mises en cache localement des requêtes précédentes. Si une correspondance est trouvée ici, le serveur répond avec cette information. Là encore, si le serveur préféré peut répondre par une réponse positive à partir de son cache au client demandeur, la requête est terminée.

Si le nom interrogé ne trouve pas de correspondance sur le serveur préféré, que ce soit à partir du cache ou des informations de zone, le processus de requête peut se poursuivre, en utilisant la récursivité pour résoudre complètement le nom. Ce processus implique l'aide d'autres

serveurs DNS pour la résolution du nom. Par défaut, le service Client DNS demande au serveur d'utiliser un processus de récursivité pour résoudre entièrement les noms pour le compte du client avant de renvoyer une réponse.

Pour que le serveur DNS puisse effectuer correctement la récursivité, il a d'abord besoin d'informations de contact utiles sur d'autres serveurs DNS dans l'espace de noms de domaine DNS. Ces informations sont fournies en tant qu'indications de racine. Les indications de racine sont une liste d'enregistrements de ressources préliminaires. Le service DNS utilise ces enregistrements pour localiser d'autres serveurs DNS qui font autorité pour la racine de l'arborescence de l'espace de noms de domaine DNS. Les serveurs racines font autorité pour la racine du domaine et les domaines de niveau supérieur dans l'arborescence de l'espace de noms de domaine DNS.

En utilisant des indications de racine pour trouver des serveurs racines, un serveur DNS est capable d'utiliser la récursivité. En théorie, ce processus permet à n'importe quel serveur DNS de localiser les serveurs qui font autorité pour tout autre nom de domaine DNS utilisé à n'importe quel niveau de l'arborescence de l'espace de noms.

Les étapes suivantes décrivent le processus d'interrogation d'un serveur DNS :

1. S'il s'agit d'un nom de domaine complet (FQDN), c'est-à-dire qu'il se termine par un point de fin (`.`), la requête est soumise au serveur DNS. Par exemple, `www.contoso.com.`

2. S'il s'agit d'une requête multi-étiquettes non qualifiée, c'est-à-dire qu'elle ne se termine pas par un point de fin (`.`), le client DNS la soumet au serveur DNS avec un point de fin (`.`). Par exemple, `www.contoso.com.`

3. Si la non qualifiée est une requête à une seule étiquette telle que `www`. Ensuite, le comportement est différent en fonction des paramètres DNS de la carte réseau.

4. S'il existe une liste de recherche de suffixes DNS, le service Client DNS les ajoute du premier au dernier à la requête pour former une seule étiquette et soumet la requête avec le point de fin (`.`) au serveur DNS. Ce processus est répété jusqu'à ce que toute la liste de recherche de suffixes DNS soit utilisée.

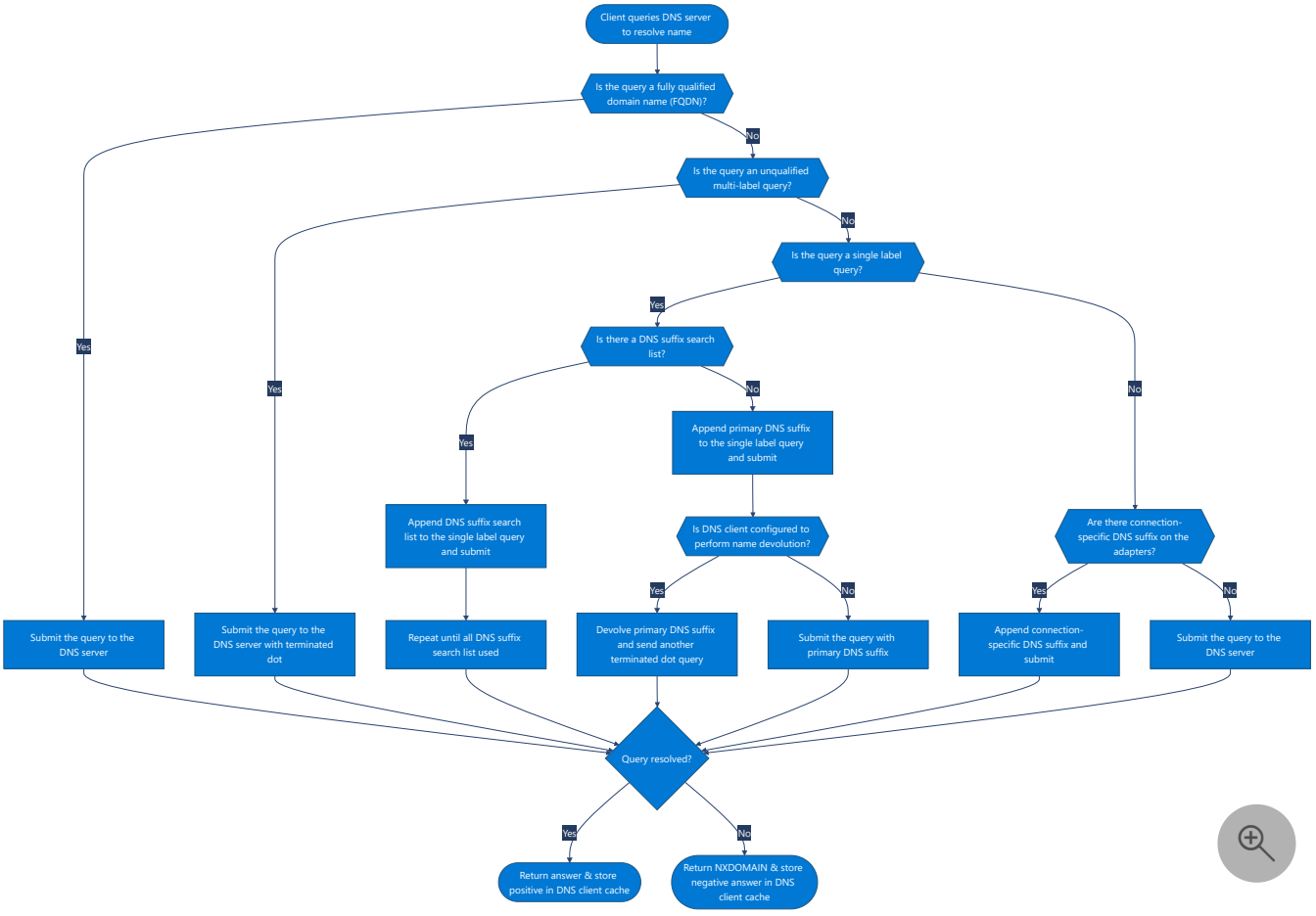
5. Si aucune liste de recherche de suffixe DNS n'est configurée, le service client DNS ajoute le suffixe DNS principal à la requête à étiquette unique avec le point de fin (`.`) et l'envoie au serveur DNS.

   Lorsque le client DNS est configuré pour effectuer la dévolution de nom, il dévolue le suffixe DNS principal et envoie une autre requête avec un point de fin (`.`) si le suffixe DNS principal échoue. Par exemple, si la résolution en `www.test.contoso.com` échoue, le client est dévolu à `www.contoso.com`

6. S'il existe un suffixe DNS spécifique aux connexions configuré sur les adaptateurs, il ajoute la requête avec un point (`.`) et la soumet au serveur DNS.

Dans tous les cas, la réponse est stockée dans le cache du client DNS, qu'elle soit positive ou négative.

L'organigramme suivant illustre le processus décrit d'interrogation d'un serveur DNS.



DNS recursion

Envisagez l'utilisation du processus de récursivité pour localiser le nom `host-b.example.contoso.com.` lorsque le client interroge un seul serveur DNS. Le processus se produit lorsqu'un serveur et un client DNS sont démarrés pour la première fois et qu'aucune information mise en cache localement n'est disponible pour aider à résoudre une requête de nom. Il suppose que le nom demandé par le client est celui d'un nom de domaine dont le serveur n'a pas de connaissance locale, en fonction de ses zones configurées.

Tout d'abord, le serveur préféré analyse le nom complet et détermine qu'il a besoin de l'emplacement du serveur qui fait autorité pour le domaine de premier niveau, `com`. Il utilise ensuite une requête itérative adressée au serveur DNS `com` pour obtenir une référence au serveur `contoso.com`. Ensuite, une réponse de référence est transmise du serveur `contoso.com` au serveur DNS pour `example.contoso.com`.

Enfin, le serveur `example.contoso.com.` est contacté. Étant donné que ce serveur contient le nom interrogé dans ses zones configurées, il envoie une réponse d'autorité au serveur d'origine qui a lancé la récursivité. Lorsque le serveur d'origine reçoit la réponse, il vérifie si la réponse fait autorité. Si c'est le cas, le serveur renvoie cette réponse au client demandeur, ce qui termine le processus de requête récursive.

Bien que le processus de requête récursive puisse être gourmand en ressources lorsqu'il est exécuté comme décrit, il présente certains avantages en termes de performances pour le serveur DNS. Par exemple, pendant le processus de récursivité, le serveur DNS qui effectue la recherche récursive obtient des informations sur l'espace de noms de domaine DNS. Le serveur met en cache les informations, qui peuvent être réutilisées pour accélérer la réponse aux requêtes ultérieures qui les utilisent ou qui leur correspondent. Au fil du temps, ces informations mises en cache peuvent augmenter jusqu'à occuper une partie importante des ressources de mémoire du serveur. Le cache est effacé chaque fois que le service DNS est redémarré.

Expiration adaptative de requête DNS

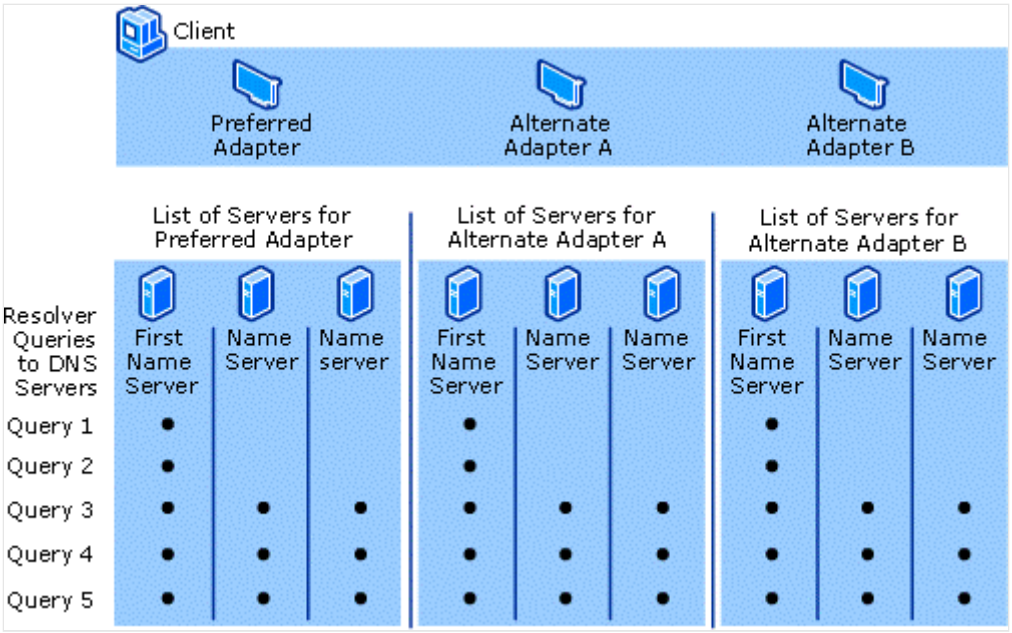
La fonctionnalité d'expiration adaptative des requêtes DNS permet d'adapter le délai d'expiration des requêtes DNS en fonction du temps requis pour les requêtes précédentes, réduisant ainsi l'expiration de la plupart des requêtes. Les délais d'expiration peuvent être augmentés pour les liaisons à latence élevée, telles que les liaisons satellite. Les applications du Windows Store peuvent optimiser la configuration des délais d'expiration DNS pour chaque interface réseau.

Au lieu d'attendre 1 000 ms avant de faire expirer une requête DNS, le premier délai d'expiration est ajusté pour être compris entre 25 ms et 1 000 ms, en fonction des performances passées du réseau.

Cache non réactif du serveur DNS

Les serveurs DNS non réactifs sont mis en cache et font régulièrement l'objet de nouvelles tentatives. Cela permet au client DNS d'utiliser de manière cohérente le meilleur serveur disponible et de passer moins de temps à attendre les serveurs DNS non réactifs.

La figure suivante montre un exemple de client DNS qui interroge chaque serveur sur chaque carte à l'aide du processus décrit dans cette section.



Le service Client DNS interroge les serveurs DNS dans l'ordre suivant :

1. Le service Client DNS envoie la requête de nom au premier serveur DNS de la liste des serveurs DNS préférés de la carte et attend une réponse pendant une seconde.

2. Si le service Client DNS ne reçoit pas de réponse du premier serveur DNS dans la seconde, il envoie la requête de nom aux premiers serveurs DNS sur toutes les cartes encore envisageables et attend une réponse pendant deux secondes.

3. Si le service Client DNS ne reçoit pas de réponse d'un serveur DNS dans les deux secondes, il envoie la requête à tous les serveurs DNS sur toutes les cartes encore envisageables. Le service Client DNS attend ensuite une réponse pendant deux secondes supplémentaires.

4. Si le service Client DNS ne reçoit toujours pas de réponse d'un serveur DNS, il envoie la requête de nom à tous les serveurs DNS sur toutes les cartes encore envisageables et attend une réponse pendant quatre secondes.

5. Si le service Client DNS ne reçoit pas de réponse d'un serveur DNS, le client DNS envoie la requête de nom à tous les serveurs DNS sur toutes les cartes encore envisageables et attend une réponse pendant huit secondes.

6. Si le service Client DNS ne reçoit pas de réponse d'un serveur dans les huit secondes, le service Client DNS répond avec un message d'expiration. Si le service Client DNS ne reçoit pas de réponse d'un serveur DNS sur une carte spécifique, toutes les requêtes adressées à ces serveurs pendant les 30 secondes suivantes sur cette carte expirent.

7. Si, à un moment donné, le service Client DNS reçoit une réponse négative d'un serveur, il supprime tous les serveurs de cette carte lors de cette recherche. Par exemple, si le

premier serveur de la carte secondaire A donne une réponse négative à l'étape 2, le service Client DNS n'interroge aucun autre serveur de la liste pour la carte secondaire A.

8. Si le service Client DNS reçoit une réponse positive, il arrête de demander le nom, ajoute la réponse au cache et renvoie la réponse au client.

Le service Client DNS assure le suivi des serveurs qui répondent le plus rapidement aux requêtes de nom et déplace les serveurs vers le haut ou vers le bas de la liste en fonction de la rapidité avec laquelle ils répondent aux requêtes de nom.

Autres réponses aux requêtes

La description précédente des requêtes DNS suppose que le processus se termine par une réponse positive renvoyée au client. Cependant, les requêtes peuvent également renvoyer d'autres réponses. Voici les réponses les plus courantes aux requêtes :

- Réponse faisant autorité
- Réponse positive
- Réponse de référence
- Réponse négative

Une réponse faisant autorité est une réponse positive d'un serveur DNS qui a une autorité directe sur le nom interrogé. Cette réponse inclut le bit d'autorité défini dans le message DNS pour indiquer son authenticité.

Une réponse positive peut contenir le RR demandé ou une liste de RR (également appelée ensemble de RR) qui correspond au nom de domaine DNS demandé et au type d'enregistrement spécifié dans le message de requête.

Une réponse de référence contient d'autres RR non spécifiés par nom ou type dans la requête. Ce type de réponse est renvoyé au client si le processus de récursivité n'est pas pris en charge. Les enregistrements sont destinés à servir de réponses de référence utiles que le client peut utiliser pour poursuivre la requête avec l'itération. Une réponse de référence contient plus de données comme les RR autres que le type interrogé. Par exemple, si le serveur DNS ne trouve pas de RR A pour le nom d'hôte `www` demandé dans cette zone, mais qu'il trouve un RR CNAME pour `www` à la place, il peut inclure ces informations dans sa réponse au client. Si le client est en mesure d'utiliser l'itération, il peut effectuer d'autres requêtes à l'aide des informations de référence pour tenter de résoudre entièrement le nom par lui-même.

Une réponse négative du serveur peut indiquer l'un des deux résultats suivants :

- Le serveur faisant autorité n'a pas pu trouver le nom demandé dans l'espace de noms DNS.

- Le serveur faisant autorité a trouvé le nom demandé, mais il n’existe aucun enregistrement du type spécifié pour ce nom.

Le résolveur traite la requête et renvoie les résultats au programme demandeur. La réponse peut être positive ou négative. De plus, le résolveur met en cache la réponse pour une utilisation ultérieure.

Si la réponse résultante à une requête est trop longue pour être envoyée et résolue dans un seul paquet de message UDP, le serveur DNS peut lancer une réponse de basculement sur le port TCP 53 pour répondre entièrement au client dans une session connectée via TCP.

La désactivation de l’utilisation de la récursivité sur un serveur DNS est effectuée lorsque les clients DNS sont limités à la résolution des noms sur un serveur DNS spécifique, tel qu’un serveur situé sur votre intranet. La récursivité peut également être désactivée lorsque le serveur DNS ne peut pas résoudre les noms DNS externes. Dans ce cas, les clients sont censés basculer vers un autre serveur DNS pour la résolution de noms. Si vous désactivez la récursivité sur le serveur DNS, vous ne pouvez pas utiliser de redirecteurs sur le même serveur.

Par défaut, les serveurs DNS utilisent plusieurs minutages par défaut lorsqu’ils exécutent une requête récursive et contactent d’autres serveurs DNS. Ces valeurs par défaut comprennent :

- Une récurrence essaie à nouveau toutes les 3 secondes. Cet intervalle correspond à la durée pendant laquelle le service DNS attend avant de réessayer une requête effectuée lors d’une recherche récursive.
- Un délai d’expiration de récursivité de 8 secondes. Cet intervalle correspond à la durée pendant laquelle le service DNS attend avant de déclarer l'échec d'un nouvel essai d'une recherche récursive.

Dans la plupart des cas, ces paramètres n’ont pas besoin d’être ajustés. Toutefois, si vous utilisez des recherches récursives sur une liaison de réseau étendu (WAN) à faible vitesse, vous pouvez améliorer les performances du serveur et la complétion des requêtes en apportant de légers ajustements aux paramètres.

Related content

To learn more about the reverse lookup process, see Reverse lookup.

Transfert DNS dans Windows Server

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Le transfert DNS est un processus de résolution de noms dans lequel un serveur DNS envoie une requête récursive à un autre serveur DNS qui agit comme un transiteur. Le serveur DNS peut utiliser des transiteurs au niveau serveur pour la résolution générale des noms et des transiteurs conditionnels pour certains espaces DNS sélectionnés. Comprendre comment la redirection interagit avec les délégations, les indices racine et les délais d'attente vous aide à prévoir quel serveur reçoit une requête et quand la résolution peut se poursuivre par une autre voie.

Cet article explique comment le serveur DNS sélectionne parmi les données disponibles localement, les transiteurs conditionnels, les délégations, les forwarders au niveau serveur et les hints racines lorsqu'il traite des requêtes client récursives. Cela explique aussi comment les paramètres de délai d'expiration et de repli déterminent si la résolution se poursuit ou échoue.

Comment le serveur DNS sélectionne un chemin de résolution

Lorsque le serveur DNS reçoit une requête récursive d'un client, il évalue les données disponibles localement puis sélectionne un chemin de résolution applicable. Le chemin dépend des zones hébergées par le serveur DNS ainsi que de sa configuration de transiteur conditionnel, de délégation, de redirection au niveau serveur et de ses indices racines.

La distinction entre une réponse terminale et une absence de réponse est centrale dans ce processus de sélection. Une réponse DNS comme `NXDOMAIN` ou `NODATA` est une réponse terminale valide et ne déclenche normalement pas de repli de secours. Le plan de secours s'applique généralement lorsqu'un serveur configuré ne répond pas ou lorsque le serveur DNS classe un résultat comme réessayable.

Cet ordre de résolution s'applique lorsque vous désactivez `ForwardDelegations`. Les politiques DNS et autres fonctionnalités DNS peuvent affecter le chemin pour une requête spécifique.

1. **Vérifiez les données DNS disponibles localement.** Le serveur évalue les zones d'autorité qu'il héberge ainsi que son cache. Si une zone d'autorité hébergée couvre la requête, cette zone détermine le résultat. Si des données autoritaires ou le cache fournissent un résultat terminal, le serveur le renvoie.

2. **Utilisez un transiteur conditionnel correspondant.** Si le nom de requête correspond à une zone de transitoire conditionnel, le serveur envoie la requête aux serveurs DNS cibles configurés de cette zone. Si ces serveurs ne répondent pas ou ne renvoient pas un résultat que le serveur DNS considère comme réessayable, le paramètre **Utiliser la récursion** du transiteur conditionnel détermine si le serveur peut essayer d'autres chemins de résolution récursive.

3. **Utilisez une délégation appropriée.** Si une délégation correspondante identifie les prochains serveurs faisant autorité, le serveur envoie des requêtes itératives aux serveurs de noms de cette délégation. Avec `ForwardDelegations` désactivé, les forwarders au niveau serveur ne contrôlent pas une requête tandis qu'une délégation applicable en contrôle la résolution.

4. **Utilisez des forwarders au niveau du serveur.** Si aucun retraiteur conditionnel ni délégation applicable ne contrôle la requête, le serveur utilise ses forwarders configurés au niveau serveur dans l'ordre actif et sous réserve des délais configurés.

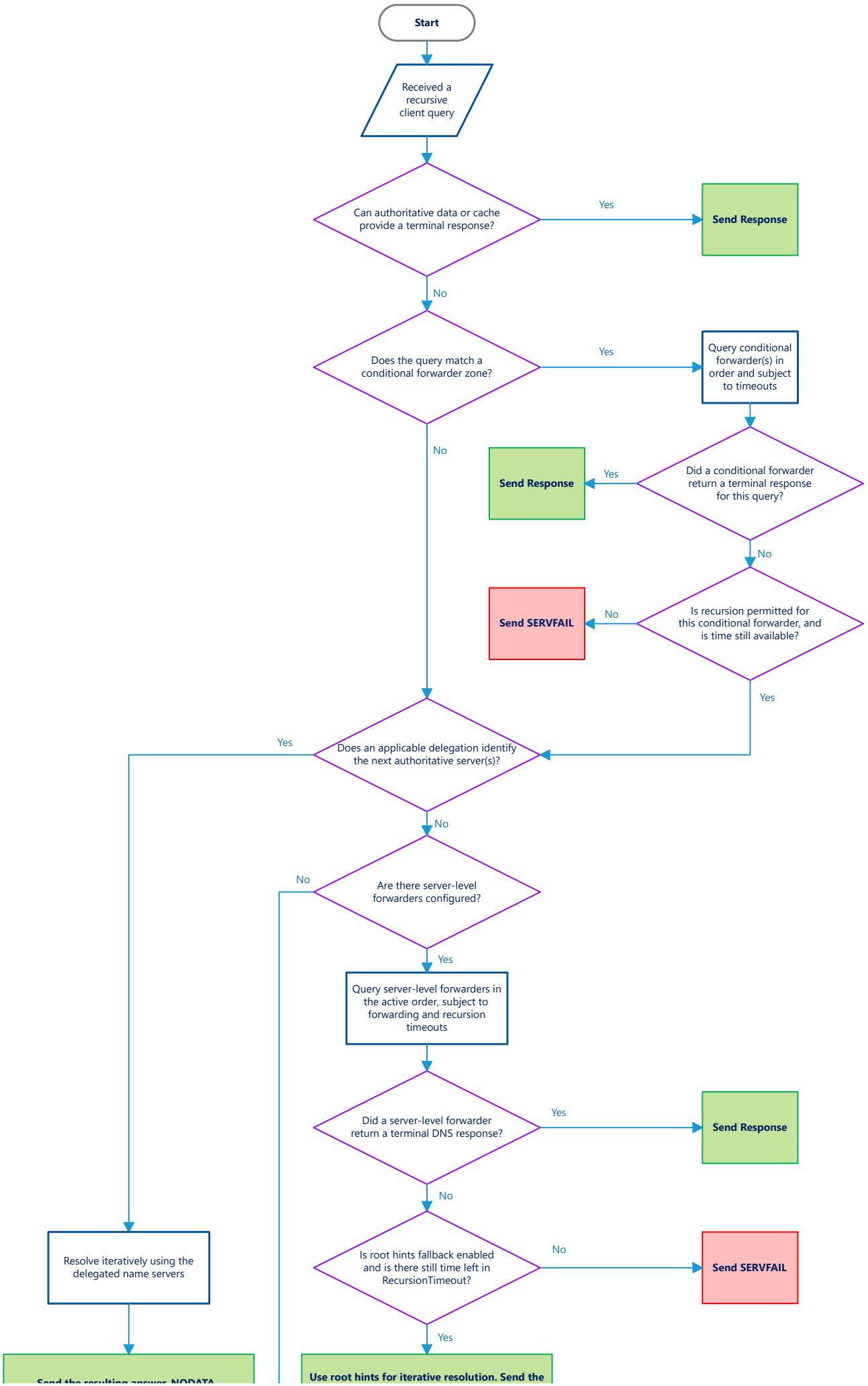
5. **Utilisez des indices racines lorsque la configuration le permet.** Si le serveur a épuisé tous ses redirecteurs configurés au niveau du serveur, il peut se rabattre sur les indications de racine lorsque sa configuration active la récursion et le recours aux indications de racine, et que le délai global de récursion n'a pas expiré. Si le serveur ne dispose pas de forwarders au niveau serveur configurés, les hints racines peuvent constituer le point de départ pour une résolution itérative.

6. **Retournez le résultat ou un échec.** Le serveur retourne le résultat du chemin sélectionné. Si la configuration du serveur désactive la récursion, le serveur retourne `REFUSED` normalement une requête nécessitant une récursion. Si le traitement récursif ne peut pas se terminer, le serveur retourne `SERVFAIL`.

> ⓘ **Remarque**
>
> Un redirecteur non réactif ne garantit pas que le serveur atteigne le repli d'indications de racine. Le serveur doit épuiser les redirecteurs applicables avant que `RecursionTimeout` n'expire. Si le délai global de récursion expire en premier, la requête échoue sans atteindre les indices racines.

Flux et repli de résolution du redirecteur de serveur DNS

Le diagramme de flux suivant montre le parcours décisionnel commun à partir des données locales disponibles à travers des méthodes de résolution progressivement plus larges. Une réponse terminale cesse le traitement à n'importe quelle étape. Un serveur non réactif ou un résultat réessayable ne peut mener à un autre chemin que lorsque la configuration permet un plan de secours et que le temps reste dans `RecursionTimeout`. La description du texte identifie chaque branche et chaque résultat.


Start
Received a recursive client query
Can authoritative data or cache provide a terminal response?
Yes
Send Response
No
Does the query match a conditional forwarder zone?
Yes
Query conditional forwarder(s) in order and subject to timeouts
Did a conditional forwarder return a terminal response for this query?
Yes
Send Response
No
Is recursion permitted for this conditional forwarder, and is time still available?
No
Send SERVFAIL
Yes
No
Does an applicable delegation identify the next authoritative server(s)?
Yes
Resolve iteratively using the delegated name servers
Send the resulting answer, NODATA
No
Are there server-level forwarders configured?
No
Yes
Query server-level forwarders in the active order, subject to forwarding and recursion timeouts
Did a server-level forwarder return a terminal DNS response?
Yes
Send Response
No
Is root hints fallback enabled and is there still time left in RecursionTimeout?
No
Send SERVFAIL
Yes
Use root hints for iterative resolution. Send the

Transiteurs au niveau serveur dans le serveur DNS

Les forwarders au niveau serveur gèrent les requêtes non résolues lorsque ni une zone d'autorité hébergée, ni une zone de transitoire conditionnelle correspondante, ni une délégation applicable ne contrôle la requête. Le serveur DNS envoie une requête récursive à un redirectionneur, qui devient responsable de la résolution de noms.

Centraliser les recherches externes via les transiteurs peut réduire l'exposition directe à Internet, consolider les réponses en cache, simplifier la surveillance et le contrôle d'accès, et réduire les requêtes externes répétées. Si vous ne configurez pas les forwarders au niveau du serveur, le serveur DNS utilise des hints root pour les noms non résolus lorsque vous activez la récursion et que des données d'hints root utilisables sont disponibles.

N'autorisez les requêtes récursives que depuis des clients et réseaux de confiance, et n'exposez pas de services DNS récursifs à des réseaux non fiables. Utilisez des transiteurs de confiance et des règles de pare-feu pour faire respecter les limites du trafic DNS.

Sélection et ordre des transiteurs au niveau serveur

Vous configurez les adresses IP du transiteur dans un ordre préféré. Par défaut, Dynamic Forwarder Reordering maintient un ordre actif en fonction des temps de réponse et rétablit la liste dans l'ordre configuré toutes les 15 minutes environ.

- Pour chaque requête, le serveur DNS sélectionne les redirectionnaires dans la liste active.
- Si un redirecteur met plus d'une seconde à répondre, le serveur considère la réponse comme lente à des fins de réordonnancement.
- Après trois réponses lentes consécutives ou expirations de délai, le serveur peut déplacer ce redirecteur à la fin de la liste active.
- Le serveur DNS ne détermine pas si un transiteur non réactif est hors ligne ou lent. Surveillez l'état de l'expéditeur séparément.

> **Remarque**
>
> Dans Windows Server 2022 et ultérieurs, si aucun des transiteurs ne répond, le serveur DNS utilise uniquement le premier serveur de la liste dynamique pour les requêtes suivantes jusqu'au redémarrage du service serveur DNS. Pour faire défiler le serveur à travers tous les

forwarders configurés comme dans les versions précédentes, désactivez le réordonnancement dynamique avec `Set-DnsServerForwarder -EnableReordering $false`.

Repli du redirecteur au niveau du serveur vers les indications de racine

Après que le serveur DNS a épuisé les forwarders au niveau du serveur concernés, il tente par défaut la récursion standard si les forwarders ne répondent pas ou ne renvoient que des résultats que le serveur DNS considère comme réessayables. La récursion standard utilise des requêtes itératives qui commencent par les serveurs dans les indices racines. Ce plan de repli nécessite toutes les conditions suivantes :

- Le serveur épuise les redirecteurs applicables avant que `RecursionTimeout` n'expire.
- Le serveur permet la récursion.
- Le `UseRootHint` réglage est `$true`, que vous configurez avec `Set-DnsServerForwarder -UseRootHint $true`.
- Le serveur dispose de données d'indices racines utilisables et d'un accès réseau aux serveurs DNS requis.

Définissez `UseRootHint` sur `$false` lorsque le serveur doit restreindre les requêtes non résolues aux redirecteurs de sa configuration. Avec cette configuration, le serveur n'essaie pas la résolution itérative lorsque les transiteurs échouent.

Transiteurs conditionnels dans le serveur DNS

Un transiteur conditionnel redirige les requêtes pour un espace de noms DNS spécifique vers des serveurs DNS désignés. Par exemple, un transiteur conditionnel peut envoyer toutes les requêtes de `south.contoso.com` vers les serveurs DNS qui hébergent cet espace de noms tandis que le serveur gère d'autres noms via des forwarders au niveau serveur ou des hints racines.

Le serveur DNS stocke les redirecteurs conditionnels sous forme de zones de redirecteur. Lorsqu'une requête correspond à un retraiteur conditionnel, le serveur DNS l'envoie à la liste des serveurs DNS de cette zone cible au lieu d'utiliser immédiatement le chemin de redirection général au niveau du serveur.

Restrictions de zones hébergées pour les transiteurs conditionnels

Vous ne pouvez pas créer un transiteur conditionnel pour un nom DNS qui correspond à une zone principale, secondaire ou stub hébergée par le même serveur DNS. Parce que le serveur DNS stocke un transiteur conditionnel comme zone de transiteur, le serveur ne peut pas héberger un autre type de zone ni un retraiteur conditionnel portant le même nom.

Par exemple, si le serveur héberge `contoso.com` comme une zone d'autorité, vous ne pouvez pas créer un transiteur conditionnel nommé `contoso.com` sur ce serveur. DNS Manager ou `Add-DnsServerConditionalForwarderZone` indique que la zone existe déjà, et le serveur continue de répondre aux requêtes pour `contoso.com` à partir de sa zone hébergée.

Si un autre serveur DNS doit résoudre tout l'espace de noms, migrez les données de la zone et supprimez la zone hébergée avant de créer le retraiteur conditionnel. Si d'autres serveurs DNS hébergent uniquement un espace de noms enfant, conservez la zone parente et créez une délégation pour cet espace de noms.

Repli et récursion du redirecteur conditionnel

Le paramètre **Utiliser la récursion** du transiteur conditionnel contrôle ce que le serveur DNS peut faire si les serveurs DNS cibles de la zone ne répondent pas ou ne retournent pas un résultat que le serveur DNS considère comme réessayable.

Agrandir le tableau

Utiliser la récursion	Comportement après absence de réponse terminale	Result
activé	Le serveur DNS ne peut essayer un autre chemin de résolution récursive que lorsque la configuration à l'échelle du serveur permet la récursion, qu'un chemin applicable existe et que le temps reste dans `RecursionTimeout`.	La résolution peut se poursuivre par un chemin récursif applicable.
Désactivé	Le serveur DNS n'essaie pas d'autres serveurs DNS.	La requête échoue si les serveurs DNS cibles configurés ne peuvent pas fournir de résultat terminal.

`ForwarderTimeout` contrôle la fenêtre de temporisation conditionnelle du transiteur et la planification des tentatives du serveur DNS cible. Le serveur DNS ne démarre pas une nouvelle tentative vers le redirecteur conditionnel une fois `ForwarderTimeout` écoulé. `RecursionTimeout` fournit une limite distincte à l'échelle du serveur sur le traitement récursif.

Délégation et transfert du serveur DNS

Si un serveur DNS héberge une zone parente et que le nom interrogé relève d'une délégation applicable, le serveur utilise cette délégation pour localiser les serveurs DNS autoritaires de la zone enfant. La délégation crée une coupure de zone : le serveur parent fait autorité pour les enregistrements de délégation mais ne l'est pas pour les données à l'intérieur de la zone enfant déléguée.

Si aucune délégation ne s'applique et que le nom demandé appartient à une zone hébergée par le serveur, le serveur fait autorité pour la requête. Si le nom ou le type d'enregistrement demandé n'existe pas, le serveur renvoie une réponse négative autoritaire telle que `NXDOMAIN` ou `NODATA`. Il n'envoie pas cette requête à un redirecteur conditionnel, à un redirecteur au niveau du serveur ou aux indications de racine.

Par exemple, si un serveur héberge `contoso.com` et d'autres serveurs hébergent `south.contoso.com`, créez une délégation pour `south` dans la `contoso.com` zone. La zone parent renvoie une référence aux serveurs autorisés de la zone enfant. Une délégation n'envoie pas de requête récursive et transférée.

Ce comportement de délégation s'applique lorsque `ForwardDelegations` est désactivé. Si votre environnement permet ce réglage, validez l'interaction résultante entre délégations et transiteurs avant de vous fier à cet ordre de résolution.

> **ⓘ Important**
>
> Si le serveur DNS héberge également une copie autoritaire de la zone enfant et que vous souhaitez déplacer l'espace de noms enfant vers d'autres serveurs, migrez et supprimez la copie locale de la zone enfant. Sinon, le serveur reste autoritaire pour cette copie.

Indications de racine du serveur DNS et résolution itérative

Les indications de la racine sont des enregistrements de ressources qui identifient les serveurs DNS faisant autorité sur la racine d'un espace de noms DNS. Le serveur DNS les utilise comme points de départ pour la résolution itérative. Un serveur racine renvoie généralement une réponse, une référence à des serveurs plus proches du nom demandé, ou une défaillance DNS ou une réponse négative.

Si vous ne configurez pas de forwarders au niveau serveur et qu'aucune délégation ou configuration de transfert plus spécifique ne fournit un point de départ, le serveur peut utiliser

des hints racines pour une requête non résolue. Si vous configurez des redirecteurs au niveau du serveur, celui-ci n'utilise les indications de racine comme solution de secours qu'après avoir épuisé les redirecteurs, et uniquement si la récursion, le délai d'expiration restant et `UseRootHint` permettent ce repli.

Si un serveur DNS fait autorité pour la racine d'un espace de noms privé, c'est un serveur racine pour cet espace de noms. Ne supposez pas que le transfert classique au niveau serveur ou les hints root publics sont appropriés pour une root privée. Utilisez des délégations ou concevez délibérément une configuration de transfert conditionnel entre les espaces de noms.

Délais d'expiration du serveur DNS et comportement de défaillance

Les paramètres de délai d'expiration déterminent si un serveur DNS contacte les redirecteurs suivants ou bascule vers les indications de racine. `RecursionTimeout` est le budget global de temps pour le traitement récursif. `ForwardingTimeout` et `ForwarderTimeout` planifient les tentatives individuelles pour les redirecteurs au niveau du serveur et les redirecteurs conditionnels respectivement, dans ce budget ; aucun des deux ne redémarre ni ne prolonge `RecursionTimeout`.

Agrandir le tableau

Setting	Scope	Purpose	Paramètre PowerShell
`RecursionTimeout`	Serveur DNS	Limite l'ensemble de la requête client récursive. Lorsque le délai expire, le traitement récursif s'arrête et le serveur retourne `SERVFAIL`.	`Set-DnsServerRecursion -Timeout`
`ForwardingTimeout`	Redirecteurs au niveau du serveur	Précise combien de temps le serveur DNS attend chaque retraiteur au niveau serveur avant d'essayer le retraiteur suivant.	`Set-DnsServerForwarder -Timeout`
`ForwarderTimeout`	Zone de redirecteur conditionnel	Contrôle la fenêtre temporelle du redirecteur conditionnel et la planification de chaque tentative vers chaque serveur DNS cible. Le serveur DNS ne lance aucune nouvelle tentative vers une autre cible de redirecteur conditionnel	`Add-DnsServerConditionalForwarderZone -ForwarderTimeout`

Setting	Scope	Purpose	Paramètre PowerShell
		une fois ce délai d'attente écoulé.	

Lorsqu'un transiteur renvoie une réponse terminale, le serveur renvoie cette réponse sans essayer un autre chemin de résolution. Lorsqu'un transiteur ne répond pas ou retourne un résultat que le serveur DNS considère comme réessayable, le serveur DNS peut essayer le serveur configuré suivant ou un chemin de secours disponible tant que le temps restant.

Parce que `RecursionTimeout` cela limite l'ensemble de l'opération, configurer de nombreux transiteurs ne garantit pas que le serveur interroge chaque transiteur ou tente des indices root. Si le délai d'expiration total expire en premier, le serveur renvoie `SERVFAIL`. Lorsque vous configurez trois forwarders ou plus, examinez les valeurs d'expiration et vérifiez le comportement efficace grâce à la surveillance et à la capture de paquets dans votre environnement.

Choisir une conception de transfert de serveur DNS

Choisissez une méthode de résolution en fonction du propriétaire de l'espace de noms et des serveurs DNS qui doivent recevoir les requêtes. Les scénarios suivants montrent comment chaque architecture affecte le transfert et le mécanisme de secours.

Agrandir le tableau

Scénario	Conception de la méthode de résolution	Décision de repli
Centralisation de la résolution DNS générale	Utilisez des transiteurs au niveau serveur afin que les serveurs DNS désignés gèrent des noms que les zones locales, le cache, les transiteurs conditionnels ou les délégations ne résolvent pas.	Gardez le repli des indications de racine lorsque la résolution itérative directe est acceptable. Désactivez-la lorsque la politique exige que toutes les requêtes non résolues restent dans la limite de retransmission, et faites respecter la frontière avec des contrôles réseau.
Connectez des espaces de noms internes administrés séparément	Utilisez un retraiteur conditionnel pour envoyer des noms dans un espace de noms, comme `south.contoso.com`, directement vers ses serveurs DNS sans héberger de zone secondaire.	**Activez Utiliser la récursion** uniquement si un autre chemin récursif est valide pour cet espace de noms.
Résoudre un espace de noms	Utilisez un retraiteur conditionnel pour l'espace de noms du partenaire	**Désactiver Utiliser la récursion** lorsque seuls les serveurs DNS désignés du partenaire doivent résoudre l'espace de noms.

Scénario	Conception de la méthode de résolution	Décision de repli
partenaire via des serveurs désignés	au lieu d'envoyer ces requêtes via la hiérarchie DNS publique.	
Séparer un espace de noms enfant d'une zone parent hébergée	Utilisez une délégation dans la zone mère pour identifier les serveurs DNS autoritaires de la zone enfant. Une délégation renvoie des renvois au lieu de transmettre des requêtes récursives.	Lorsque vous désactivez `ForwardDelegations`, la délégation contrôle la résolution, donc les forwarders au niveau serveur ne fournissent pas de solution de secours pour la requête déléguée.

Utilisez plusieurs redirecteurs sains lorsque la conception nécessite de la redondance, et assurez-vous que les délais d'expiration de transfert et de récursion laissent suffisamment de temps pour les atteindre. Surveillez séparément le temps de réponse, le taux de défaillance et la portée du réseau car le comportement de transfert ne remplace pas la surveillance de la santé. Les serveurs récursifs qui résolvent des noms internet utilisent généralement des indices root publics, tandis que les hiérarchies DNS privées nécessitent des informations root correspondant à l'espace de noms privé.

Ressources de transfert DNS associées

- Pour comprendre les requêtes DNS récursives et itératives, examinez les requêtes et les recherches DNS dans Windows et Windows Server.
- Configurez un redirecteur général ou spécifique à un espace de noms avec Set-DnsServerForwarder et Add-DnsServerConditionalForwarderZone.
- Utilisez Gérer les zones DNS en utilisant un serveur DNS dans Windows Server lorsque votre conception d'espace de noms nécessite une zone ou une délégation.
- Diagnostiquez les échecs de redirection avec Résoudre les échecs de résolution de noms DNS liés aux redirecteurs DNS et Délais d'attente de résolution des redirecteurs.

ⓘ**Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Dernière mise à jour : 01/10/2026

Dynamic update

29/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

La mise à jour dynamique permet aux ordinateurs clients DNS d'enregistrer et de mettre à jour leurs enregistrements de ressources auprès d'un serveur DNS à chaque fois que des modifications sont apportées. Cette fonctionnalité réduit la nécessité d'administration manuelle des enregistrements de zone, en particulier pour les clients qui se déplacent régulièrement ou changent fréquemment d'emplacement et utilisent DHCP pour obtenir une adresse IP.

The DNS Client and Server services support dynamic update, as described in RFC 2136. Le service DNS Server peut activer ou désactiver les mises à jour dynamiques par zone. Par défaut, le service client DNS Windows Server met à jour dynamiquement les enregistrements de ressources d'hôte (A) dans DNS lorsqu'il est configuré pour TCP/IP. Par défaut, le service DNS Server est configuré pour autoriser uniquement les mises à jour dynamiques sécurisées.

Protocol overview

La RFC 2136 introduit le format de message `UPDATE`, qui permet d'ajouter et de supprimer des enregistrements de ressources dans une zone spécifiée tout en vérifiant les conditions préalables. La mise à jour est atomique, ce qui signifie que toutes les conditions doivent être remplies pour qu'elle se produise.

La mise à jour de la zone doit être validée sur un serveur DNS principal pour cette zone. Le serveur DNS secondaire transmet une mise à jour à l'aide de la topologie de réplication jusqu'à atteindre le serveur DNS principal. Lorsque vous utilisez une zone intégrée à Active Directory, la mise à jour d'un enregistrement de ressource dans une zone peut être envoyée à n'importe quel serveur DNS s'exécutant sur un contrôleur de domaine Active Directory dont le magasin de données contient la zone.

Lorsqu'un processus de transfert de zone démarre, il verrouille la zone. Ce verrouillage garantit qu'un serveur DNS secondaire reçoit une vue cohérente de la zone lors du transfert des données. Pendant cette période, la zone ne peut pas accepter les mises à jour dynamiques. Si la zone est vaste et fréquemment verrouillée pour les transferts, cela peut priver les clients de la mise à jour dynamique et provoquer une instabilité du système. Pour éviter ce problème, le service DNS Server Windows Server met en file d'attente les demandes de mise à jour qui arrivent pendant le transfert de la zone et les traite une fois le transfert terminé.

Comment les ordinateurs mettent à jour leurs noms DNS

Par défaut, les ordinateurs configurés statiquement pour TCP/IP tentent d'enregistrer dynamiquement les enregistrements de ressources d'hôte (A) et de pointeur (PTR) pour les adresses IP configurées et utilisées par leurs connexions réseau installées. Tous les ordinateurs inscrivent les enregistrements en fonction de leur nom de domaine complet (FQDN).

Les clients DNS ne tentent pas la mise à jour dynamique des éléments suivants :

- Via un accès à distance ou une connexion VPN (Virtual Private Network). Pour changer cette configuration, vous pouvez modifier les paramètres TCP/IP avancés de la connexion réseau concernée ou modifier le registre.

- Zones de domaine de premier niveau (TLD). Toute zone nommée avec un nom en une partie est considérée comme une zone TLD, par exemple, `com`, `edu`, `blank`, `my-company`.

De même, toujours par défaut, la partie suffixe du DNS principal du nom de domaine complet d'un ordinateur est identique au nom du domaine Active Directory auquel l'ordinateur est joint. To allow different primary DNS suffixes, a domain administrator can create a restricted list of allowed suffixes by modifying the **msDS-AllowedDNSSuffixes** attribute in the domain object container. Un administrateur de domaine peut gérer l'attribut à l'aide des interfaces ADSI (Active Directory Service Interfaces) ou du protocole LDAP (Lightweight Directory Access Protocol). Les mises à jour dynamiques peuvent être envoyées pour l'une des raisons ou l'un des événements suivants :

- Une adresse IP est ajoutée, supprimée ou modifiée dans la configuration des propriétés TCP/IP pour l'une des connexions réseau installées.
- Au démarrage, lorsque l'ordinateur est allumé.
- Un serveur membre est promu en contrôleur de domaine.
- Un bail d'adresse IP est modifié ou renouvelé par le serveur DHCP pour l'une des connexions réseau installées, par exemple, au démarrage de l'ordinateur ou si la commande `ipconfig /renew` est utilisée.
- La commande `ipconfig /registerdns` permet de forcer manuellement l'actualisation de l'inscription du nom du client dans DNS.

> **ⓘ Important**
>
> Si vous utilisez `ipconfig /registerdns`, le service client DNS tente d'inscrire directement son enregistrement DNS, en contournant le serveur DHCP. Cette inscription se produit même si le serveur DHCP est configuré pour **mettre à jour toujours mettre à jour dynamiquement les enregistrements DNS A et PTR**. Si le client n'est pas autorisé à

mettre à jour son enregistrement de ressource, l'inscription échoue en mode silencieux. Si le client DNS dispose de cette autorisation, l'enregistrement de ressource est mis à jour. Les autorisations peuvent être réinitialisées de sorte que le serveur DHCP ne soit plus en mesure d'effectuer de mises à jour sur l'enregistrement de ressource.
La méthode recommandée pour mettre à jour l'inscription DNS pour les clients DHCP exécutant Windows consiste à utiliser `ipconfig /renew`. N'utilisez `ipconfig /registerdns` pas .

Lorsque l'un des événements précédents déclenche une mise à jour dynamique, le service client DNS envoie des mises à jour. Ce déclencheur est conçu de sorte que si une modification est apportée aux informations d'adresse IP, les mises à jour correspondantes dans DNS sont effectuées pour synchroniser les mappages nom-adresse pour l'ordinateur. Le service client DNS exécute cette fonction pour toutes les connexions réseau utilisées sur le système, y compris les connexions non configurées pour utiliser DHCP.

Ce processus de mise à jour part du principe que les paramètres d'installation par défaut sont appliqués pour les serveurs exécutant Windows Server. Les noms et le comportement de mise à jour sont ajustables lorsque les propriétés TCP/IP avancées sont configurées pour utiliser des paramètres DNS autres que ceux par défaut.

En plus du nom complet (ou nom principal) de l'ordinateur, les noms DNS spécifiques à la connexion peuvent être configurés et éventuellement enregistrés ou mis à jour dans DNS.

Fonctionnement de la mise à jour dynamique

Les mises à jour dynamiques sont généralement demandées lorsqu'un nom DNS ou une adresse IP change sur l'ordinateur. Par exemple, supposons qu'un client nommé `oldhost` soit d'abord configuré avec les noms suivants :

- **Computer name**: `oldhost`
- **Nom de domaine DNS**: `example.contoso.com`
- **Noms d'ordinateur complet**: `oldhost.example.contoso.com`

Dans cet exemple, aucun nom de domaine DNS spécifique à la connexion n'est configuré pour l'ordinateur. L'ordinateur est ensuite renommé de `oldhost` en `newhost`, ce qui entraîne les modifications de nom suivantes sur le système :

- **Computer name**: `newhost`
- **Nom de domaine DNS**: `example.contoso.com`
- **Noms d'ordinateur complet**: `newhost.example.contoso.com`

Une fois le changement de nom appliqué dans les propriétés système, vous êtes invité à redémarrer l'ordinateur. Lorsque l'ordinateur redémarre Windows, le service client DNS effectue la séquence suivante pour mettre à jour DNS :

1. Le service client DNS envoie une requête de type SOA à l'aide du nom de domaine DNS de l'ordinateur.

   L'ordinateur client utilise le nom de domaine complet actuellement configuré de l'ordinateur (par exemple, `newhost.example.contoso.com`) comme le nom spécifié dans cette requête.

2. Le serveur DNS faisant autorité pour la zone contenant le nom de domaine complet du client répond à la requête de type SOA.

   Pour les zones principales standard, le serveur principal (propriétaire) retourné dans la réponse à la requête SOA est fixe et statique. Il correspond toujours au nom DNS exact tel qu'il apparaît dans l'enregistrement de ressource SOA stocké avec la zone. Si la zone mise à jour est intégrée à l'annuaire, tout serveur DNS s'exécutant sur un contrôleur de domaine pour le domaine Active Directory dans le nom de domaine complet peut répondre. Il peut insérer dynamiquement son propre nom en tant que serveur principal (propriétaire) de la zone dans la réponse à la requête SOA.

3. Le service client DNS tente ensuite de contacter le serveur DNS principal.

   Le client traite la réponse à la requête SOA pour son nom afin de déterminer l'adresse IP du serveur DNS autorisé en tant que serveur principal pour accepter son nom. Il procède ensuite à l'exécution de la séquence d'étapes suivante, le cas échéant, pour contacter et mettre à jour dynamiquement son serveur principal :

   - Il envoie une requête de mise à jour dynamique au serveur principal déterminé dans la réponse à la requête SOA.
   - Si la mise à jour aboutit, aucune autre action n'est effectuée.
   - En cas d'échec de cette mise à jour, le client envoie ensuite une requête de type NS pour le nom de zone spécifié dans l'enregistrement SOA.
   - Lorsqu'il reçoit une réponse à cette requête, il envoie une requête SOA au premier serveur DNS répertorié dans la réponse.

   Une fois la requête SOA résolue, le client envoie une mise à jour dynamique au serveur spécifié dans l'enregistrement SOA retourné.

   - Si la mise à jour aboutit, aucune autre action n'est effectuée.
   - En cas d'échec de la mise à jour, le client répète le processus de requête SOA en envoyant une requête au serveur DNS suivant répertorié dans la réponse.

4. Une fois que le serveur DNS principal qui peut effectuer la mise à jour est contacté, le client envoie la requête de mise à jour et le serveur DNS la traite.

   Le contenu de la requête de mise à jour comprend des instructions permettant d'ajouter des enregistrements de ressources A (et éventuellement PTR) pour `newhost.example.contoso.com` et de supprimer ces mêmes types d'enregistrements pour `oldhost.example.contoso.com`, le nom précédemment inscrit.

   Le serveur DNS vérifie également que les mises à jour sont autorisées pour la requête du client. Pour les zones principales standard, les mises à jour dynamiques ne sont pas sécurisées, de sorte que toutes les tentatives de mise à jour du client aboutissent. Pour les zones intégrées à Active Directory, les mises à jour sont sécurisées et effectuées à l'aide des paramètres de sécurité basés sur l'annuaire. Pour plus d'informations, consultez la section Mise à jour dynamique sécurisée plus loin dans cet article.

Les mises à jour dynamiques sont envoyées ou actualisées régulièrement. Par défaut, les ordinateurs envoient une actualisation tous les sept jours. Si la mise à jour n'entraîne aucune modification des données de la zone, celle-ci reste dans sa version actuelle et aucune modification n'est écrite. Les mises à jour n'entraînent des modifications de la zone ou une augmentation des transferts de zone que lorsque les noms ou les adresses changent.

Les noms ne sont pas supprimés des zones DNS s'ils deviennent inactifs ou ne sont pas mis à jour dans l'intervalle d'actualisation (sept jours). DNS ne dispose pas d'un mécanisme pour libérer ou désactiver les noms. Cependant, les clients DNS tentent de supprimer les anciens enregistrements de nom lorsqu'un nouveau nom est appliqué. Les clients DNS tentent également de mettre à jour les enregistrements de noms lorsqu'un changement d'adresse se produit.

Lorsque le service Client DNS inscrit des enregistrements de ressources A et PTR pour un ordinateur, il utilise une durée de vie de mise en cache par défaut de 15 minutes pour les enregistrements hôtes. Cette durée de vie détermine la durée de mise en cache des enregistrements d'un ordinateur par d'autres serveurs et clients DNS lorsqu'ils sont inclus dans une réponse à une requête.

Durée de vie

Chaque fois qu'un client de mise à jour dynamique s'inscrit dans DNS, les enregistrements de ressources A et PTR associés incluent la durée de vie. Par défaut, la durée de vie est de 10 minutes pour les enregistrements inscrits par le service Netlogon. Pour les enregistrements inscrits par le service client DHCP, la durée de vie est de 15 minutes. Si le service DNS Server inscrit dynamiquement des enregistrements pour ses propres zones, la durée de vie par défaut est de 20 minutes. Vous pouvez modifier ce paramètre par défaut dans le registre. Une valeur

faible entraîne l'expiration plus rapide des entrées mises en cache, ce qui augmente le trafic DNS mais réduit le risque que les enregistrements mis en cache deviennent obsolètes. Faire expirer rapidement les entrées est utile pour les ordinateurs qui renouvellent fréquemment leurs baux DHCP. Les durées de conservation longues sont utiles pour les ordinateurs qui renouvellent peu souvent leurs baux DHCP.

Résolution de conflits de noms

Lorsque le service client DNS tente d'inscrire un enregistrement A, il vérifie si la zone du DNS faisant autorité contient déjà un enregistrement A pour le même nom, mais avec une adresse IP différente. Par défaut, le service client DNS tente de remplacer le ou les enregistrement(s) A existant(s) par le nouvel enregistrement A contenant l'adresse IP du client DNS. Par conséquent, n'importe quel ordinateur du réseau peut modifier l'enregistrement A existant, sauf en cas d'utilisation de la mise à jour dynamique sécurisée. Les zones configurées pour une mise à jour dynamique sécurisée permettent uniquement aux utilisateurs autorisés de modifier l'enregistrement de ressource.

Vous pouvez modifier le paramètre par défaut de telle sorte que le service client DNS mette fin au processus d'inscription et consigne l'erreur dans l'Observateur d'événements, au lieu de remplacer l'enregistrement A existant. Pour plus d'informations, consultez la section Mise à jour dynamique sécurisée plus loin dans cet article.

DNS et DHCP

Les clients DNS Windows prennent en charge les mises à jour dynamiques et peuvent lancer le processus de mise à jour dynamique. Un client DNS négocie le processus de mise à jour dynamique avec le serveur DHCP lorsque le client loue une adresse IP ou renouvelle le bail. Cette négociation permet de déterminer quel ordinateur met à jour les enregistrements de ressources A et PTR du client. Le client DNS et le serveur DHCP négocient qui met à jour les enregistrements. Le client et le serveur envoient des requêtes de mise à jour dynamique aux serveurs DNS principaux qui font autorité pour les noms à mettre à jour.

Le service serveur DHCP Windows Server peut mettre à jour les enregistrements DNS des clients qui ne prennent pas en charge l'option FQDN du service client DHCP. This functionality can be enabled in the **DNS** tab of the server properties for the DHCP console. Le serveur DHCP obtient d'abord le nom des clients hérités à partir du paquet `DHCP REQUEST`. Il ajoute ensuite le nom de domaine attribué pour cette étendue et inscrit les enregistrements de ressources A et PTR.

Dans certains cas, des enregistrements de ressources PTR ou A obsolètes peuvent apparaître sur les serveurs DNS à l'expiration du bail d'un client DHCP. Par exemple, lorsqu'un client DNS

tente de négocier une procédure de mise à jour dynamique avec un serveur DHCP, le client DNS doit inscrire lui-même les enregistrements de ressources A et PTR. Par la suite, si le client est supprimé de manière incorrecte du réseau, il ne peut pas annuler l'inscription de ses enregistrements de ressources A et PTR, qui deviennent alors obsolètes.

Si un enregistrement de ressource A obsolète apparaît dans une zone où seules les mises à jour dynamiques sécurisées sont autorisées, aucun ordinateur ne pourra enregistrer un autre enregistrement de ressource sous le nom associé à cet enregistrement A. Pour éviter les problèmes liés aux enregistrements de ressources PTR et A obsolètes, vous pouvez activer les fonctionnalités de vieillissement et de nettoyage. Pour en savoir plus sur la fonctionnalité de nettoyage et et de vieillissement, consultez Nettoyage et vieillissement DNS.

Pour assurer une tolérance aux pannes lors des mises à jour dynamiques, envisagez d'intégrer à Active Directory les zones qui acceptent les mises à jour dynamiques des clients Windows. Pour accélérer la découverte des serveurs DNS faisant autorité, vous pouvez configurer chaque client avec une liste de serveurs DNS par défaut et auxiliaires, qui sont principaux pour cette zone intégrée à l'annuaire. Si un client ne parvient pas à mettre à jour la zone via son serveur DNS préféré parce que celui-ci est indisponible, il peut tenter la mise à jour auprès d'un serveur auxiliaire. Lorsque le serveur DNS préféré redevient disponible, il charge la zone intégrée à l'annuaire mise à jour avec les informations du client.

Processus de mise à jour dynamique

Dans cette section, nous décrivons le processus de mise à jour dynamique pour les clients DHCP, les clients configurés de manière statique, les clients d'accès à distance et les clients multirésidents.

Processus client DHCP

Pour lancer le processus de mise à jour dynamique, le client DHCP envoie son nom de domaine complet au serveur DHCP dans le paquet `DHCPREQUEST` à l'aide de l'option de nom de domaine complet du service client DHCP. Le serveur DHCP répond ensuite au client DHCP en envoyant un message d'accusé de réception DHCP (`DHCPACK`) qui inclut l'option de nom de domaine complet (code d'option 81).

Le tableau suivant répertorie les champs de l'option de nom de domaine complet du paquet `DHCPREQUEST`.

Agrandir le tableau

Field	Explanation
Code	Spécifie le code de cette option (81).
Len	Spécifie la longueur, en octets, de cette option (minimum 4).
Flags	Peut avoir l'une des valeurs suivantes : 0. Le client souhaite inscrire l'enregistrement de ressource A et demande au serveur de mettre à jour l'enregistrement de ressource PTR. 1. Le client souhaite que le serveur inscrive les enregistrements de ressources A et PTR. 3. Le serveur DHCP inscrit les enregistrements de ressources A et PTR, quelle que soit la requête du client.
`RCODE1` et `RCODE2`	Le serveur DHCP utilise ces champs pour spécifier le code de réponse des enregistrements de ressources A et PTR effectués pour le compte du client et pour indiquer s'il a tenté la mise à jour avant l'envoi de `DHCPACK`.
Domain Name	Spécifie le nom de domaine complet du client.

Les conditions dans lesquelles les clients DHCP envoient l'option de nom de domaine complet dépendent du système d'exploitation exécuté par le client et de la configuration de celui-ci. Les actions entreprises par les serveurs DHCP dépendent également du système d'exploitation exécuté par le serveur et de la configuration de celui-ci.

Par défaut, le service client DHCP Windows utilise le processus suivant.

1. Le service client DHCP Windows envoie l'option de nom de domaine complet avec le champ Indicateurs défini sur 0. Cet indicateur demande au client de mettre à jour l'enregistrement de ressource A et au service serveur DHCP de mettre à jour l'enregistrement de ressource PTR.

2. Le client attend une réponse du serveur DHCP. À moins que le serveur DHCP ne définisse le champ Indicateurs sur 3, le client DNS lance alors une mise à jour pour l'enregistrement de la ressource A.

3. Si le serveur DHCP ne prend pas en charge ou n'est pas configuré pour l'inscription de l'enregistrement DNS, aucun nom de domaine complet n'est inclus dans la réponse. Dans ce cas, le client DNS tente d'inscrire les enregistrements de ressources A et PTR.

En fonction de la requête du client DHCP, le serveur DHCP peut effectuer différentes actions.

Si le client DHCP envoie un message `DHCPREQUEST` sans l'option de nom de domaine complet, le comportement dépend du type de serveur DHCP et de sa configuration. Le serveur DHCP met

à jour les deux enregistrements si vous le configurez pour mettre à jour les enregistrements au nom des clients DHCP qui ne prennent pas en charge l'option de nom de domaine complet.

Dans les cas suivants, le serveur DHCP n'effectue aucune action :

- Le serveur DHCP ne prend pas en charge la mise à jour dynamique.
- Le serveur DHCP est configuré pour ne pas effectuer de mises à jour dynamiques pour les clients qui ne prennent pas en charge l'option de nom de domaine complet.
- Le serveur DHCP est configuré pour ne pas inscrire les enregistrements de ressources DNS.

Si le client DHCP Windows demande au serveur de mettre à jour l'enregistrement de ressource PTR, mais pas l'enregistrement de ressource A, le comportement dépend du type de serveur DHCP et de sa configuration.

Le serveur peut effectuer l'une des actions suivantes :

- Si le serveur DHCP Windows est configuré pour ne pas effectuer de mises à jour dynamiques, il n'inclut pas l'option de nom de domaine complet dans sa réponse. Il ne met pas non plus à jour les enregistrements de ressources. Dans ce cas, s'il en est en mesure, le client DNS tente de mettre à jour les enregistrements de ressources A et PTR.
- Si le serveur DHCP Windows est configuré pour effectuer une mise à jour en fonction de la requête du client DHCP, le serveur tente de mettre à jour l'enregistrement de ressource PTR. Le serveur DHCP envoie un message `DHCPACK` au client DHCP. Ce message contient l'option de nom de domaine complet avec le champ Indicateurs défini sur `0`. Le message `DHCPACK` confirme que le serveur DHCP met à jour l'enregistrement PTR. S'il en est en mesure, le client DNS tente ensuite de mettre à jour l'enregistrement de ressource A.
- Si le serveur DHCP est configuré pour toujours mettre à jour les enregistrements A et PTR, il tente de mettre à jour ces deux enregistrements de ressources. Le message `DHCPACK` envoyé par le serveur DHCP au client DHCP contient l'option de nom de domaine complet avec le champ Indicateurs défini sur `3`, informant le client DHCP que le serveur DHCP met à jour les enregistrements A et PTR. Dans ce cas, le client DNS ne tente pas de mettre à jour ces enregistrements de ressources.

Processus de clients configurés statiquement et d'accès à distance

Les clients configurés de manière statique et les clients d'accès à distance ne dépendent pas du serveur DHCP pour l'inscription DNS. Les clients configurés de manière statique mettent à jour

dynamiquement leurs enregistrements de ressources A et PTR à chaque démarrage. Les clients effectuent également une mise à jour toutes les 24 heures afin d'actualiser les enregistrements dans la base de données DNS.

Les clients d'accès à distance peuvent mettre à jour dynamiquement les enregistrements de ressources A et PTR lorsqu'une connexion d'accès à distance est établie. Ils peuvent également tenter de retirer ou de désinscrire les enregistrements de ressources A et PTR lorsque l'utilisateur ferme explicitement la connexion. Les ordinateurs exécutant Windows Server avec une connexion réseau d'accès à distance tentent d'inscrire dynamiquement les enregistrements A et PTR pour l'adresse IP de cette connexion. Par défaut, le service client DNS sur le client Windows ne tente pas de mise à jour dynamique via un accès à distance ou une connexion VPN. Pour changer cette configuration, vous pouvez modifier les paramètres TCP/IP avancés de la connexion réseau concernée ou modifier le registre.

Dans tous les systèmes d'exploitation, si un client d'accès à distance ne reçoit pas de réponse positive à sa tentative de désinscription d'un enregistrement de ressource DNS, ou échoue pour toute autre raison à désinscrire un enregistrement de ressource dans un délai de quatre secondes, le client DNS ferme la connexion. Dans ce cas, la base de données DNS peut contenir un enregistrement obsolète.

Si le client d'accès à distance ne parvient pas à désinscrire un enregistrement de ressource DNS, il ajoute un message au journal des événements, que vous pouvez consulter à l'aide de l'Observateur d'événements. Le client d'accès à distance ne supprime jamais les enregistrements obsolètes, mais le serveur d'accès à distance tente de désinscrire l'enregistrement de ressource PTR lorsque le client est déconnecté.

Par défaut, le service client DNS Windows ne tente pas de mettre à jour automatiquement les enregistrements A et PTR pour les connexions d'accès à distance.

Processus client multirésident

Si un client de mise à jour dynamique est multirésident, c'est-à-dire qu'il dispose de plusieurs connexions réseau et d'une adresse IP associée, il inscrit toutes les adresses IP pour chaque connexion réseau. Si vous ne souhaitez pas que ces adresses IP soient inscrites, vous pouvez configurer la connexion réseau de telle sorte qu'elle n'inscrive pas les adresses IP.

Le client de mise à jour dynamique n'inscrit pas toutes les adresses IP auprès des serveurs DNS dans tous les espaces de noms auxquels l'ordinateur est connecté. Par exemple, un ordinateur multirésident, `client1.example.contoso.com`, est connecté à la fois à Internet et à l'intranet de l'entreprise. Le client est connecté à l'intranet par l'adaptateur A, un adaptateur DHCP dont l'adresse IP est `172.16.8.7`. Le client est également connecté à Internet par l'adaptateur B, un adaptateur d'accès à distance dont l'adresse IP est `10.3.3.9`. Le client résout les noms intranet

à l'aide d'un serveur de noms sur l'intranet et résout les noms Internet à l'aide d'un serveur de noms sur Internet.

Mise à jour dynamique sécurisée

La sécurité des mises à jour DNS n'est disponible que pour les zones intégrées à Active Directory. Lorsque vous intégrez une zone dans Active Directory, des listes de contrôle d'accès sont disponibles dans la console DNS pour vous permettre d'ajouter ou de supprimer des utilisateurs et des groupes de la liste de contrôle d'accès pour un enregistrement de zone ou de ressource spécifié. Les listes de contrôle d'accès sont uniquement destinées au contrôle d'accès d'administration DNS et n'ont aucune incidence sur la résolution des requêtes DNS.

Par défaut, la sécurité des mises à jour dynamiques pour les serveurs et les clients DNS est gérée comme suit :

- Les clients DNS tentent d'utiliser la mise à jour dynamique non sécurisée en premier. Si une mise à jour non sécurisée est refusée, les clients tentent d'utiliser la mise à jour sécurisée.

  La stratégie de mise à jour par défaut permet aux clients de tenter d'écraser un enregistrement de ressource précédemment inscrit, sauf s'il est bloqué.

- Une fois qu'une zone est intégrée à Active Directory, par défaut, les serveurs DNS exécutant Windows Server autorisent uniquement les mises à jour dynamiques sécurisées.

  Lorsque vous utilisez le stockage de zone basé sur des fichiers, le service DNS Server est configuré par défaut pour ne pas autoriser les mises à jour dynamiques sur ses zones. Pour les zones qui sont intégrées à l'annuaire ou qui utilisent un stockage standard basé sur des fichiers, vous pouvez modifier la zone afin d'autoriser toutes les mises à jour dynamiques. Ce paramètre permet d'accepter toutes les mises à jour.

Dynamic update is an addition to the DNS standard specification, defined in RFC 2136.

L'inscription dynamique des enregistrements de ressources DNS peut être limitée à l'aide d'entrées de registre.

Fonctionnement de la mise à jour dynamique sécurisée

Le processus de mise à jour dynamique sécurisée est décrit comme suit :

1. Pour lancer une mise à jour dynamique sécurisée, le client DNS lance d'abord le processus de négociation du contexte de sécurité, au cours duquel les jetons sont transmis entre le client et le serveur à l'aide d'enregistrements de ressources TKEY. À la fin du processus de négociation, le contexte de sécurité est établi.

2. Le client DNS envoie la requête de mise à jour dynamique au serveur DNS. Cette requête contient des enregistrements de ressources pour l'ajout, la suppression ou la modification de données.

   a. La requête est signée à l'aide du contexte de sécurité précédemment établi.

   b. La signature est transmise dans l'enregistrement de ressource TSIG, qui est inclus dans le paquet de mise à jour dynamique.

3. Le serveur tente de mettre à jour Active Directory à l'aide des informations d'identification du client et envoie le résultat de la mise à jour au client. Ces résultats sont également signés à l'aide du contexte de sécurité et de la signature transmise dans l'enregistrement de ressource TSIG inclus dans la réponse.

Processus de mise à jour dynamique sécurisée

Le processus de mise à jour dynamique sécurisée est décrit comme suit :

1. Le client DNS interroge le serveur DNS préféré afin de déterminer quel serveur DNS fait autorité pour le nom de domaine qu'il tente de mettre à jour. Le serveur DNS préféré répond avec le nom de la zone et le serveur DNS principal qui fait autorité pour la zone.

2. Le client DNS tente une mise à jour dynamique standard, et si la zone est configurée pour autoriser uniquement les mises à jour dynamiques sécurisées (configuration par défaut pour les zones intégrées à Active Directory), le serveur DNS refuse la mise à jour non sécurisée. Si la zone est configurée pour la mise à jour dynamique standard plutôt que pour la mise à jour dynamique sécurisée, le serveur DNS accepte la tentative du client DNS d'ajouter, de supprimer ou de modifier des enregistrements de ressources dans cette zone.

3. Le client DNS et le serveur DNS commencent la négociation TKEY.

   a. Le client DNS et le serveur DNS négocient un mécanisme de sécurité sous-jacent. Les clients de mise à jour dynamique Windows et les serveurs DNS peuvent uniquement utiliser le protocole Kerberos.

   b. À l'aide du mécanisme de sécurité, le client DNS et le serveur DNS vérifient leurs identités respectives et établissent le contexte de sécurité.

4. Le client DNS envoie la requête de mise à jour dynamique au serveur DNS, signée à l'aide du contexte de sécurité établi. La signature est incluse dans le champ de signature de l'enregistrement de ressource TSIG inclus dans le paquet de requête de mise à jour dynamique. Le serveur DNS vérifie l'origine du paquet de mise à jour dynamique à l'aide du contexte de sécurité et de la signature TSIG.

5. Le serveur DNS tente d'ajouter, de supprimer ou de modifier des enregistrements de ressources dans Active Directory. La mise à jour dépend de si le client DNS dispose des autorisations appropriées et les conditions préalables sont remplies.

6. Le serveur DNS envoie une réponse au client DNS indiquant s'il a été en mesure d'effectuer la mise à jour, signée à l'aide du contexte de sécurité établi. La signature est incluse dans le champ de signature de l'enregistrement de ressource TSIG inclus dans le paquet de réponse de mise à jour dynamique. Si le client DNS reçoit une réponse falsifiée, il l'ignore et attend une réponse signée.

Sécurité pour les clients DHCP qui ne prennent pas en charge l'option de nom de domaine complet

Les clients DHCP Windows qui ne prennent pas en charge l'option de nom de domaine complet (option 81) ne sont pas en mesure d'effectuer des mises à jour dynamiques. Si vous souhaitez que les enregistrements de ressources A et PTR de ces clients soient inscrits dynamiquement dans DNS, vous devez configurer le serveur DHCP pour effectuer des mises à jour dynamiques en leur nom.

Pour que le serveur DHCP effectue des mises à jour dynamiques sécurisées pour le compte des clients DHCP qui ne prennent pas en charge l'option de nom de domaine complet, une configuration supplémentaire est nécessaire afin d'éviter un problème d'autorisation. Lorsqu'un serveur DHCP effectue une mise à jour dynamique sécurisée sur un nom, il devient le propriétaire de ce nom. Seul ce serveur DHCP peut mettre à jour un enregistrement pour ce nom.

Supposons, par exemple, que le serveur DHCP DHCP1 a créé un objet pour le nom `host1.example.com`, puis a cessé de répondre, et que plus tard le serveur DHCP de sauvegarde, DHCP2, a essayé de mettre à jour un enregistrement portant le même nom, `host1.example.com`. Dans ce cas, DHCP2 n'est pas en mesure de mettre à jour le nom, car il n'en est pas le propriétaire.

To avoid this issue, use the built-in security group called *DnsUpdateProxy*. Si vous ajoutez tous les serveurs DHCP en tant que membres du groupe DnsUpdateProxy, un autre serveur peut mettre à jour les enregistrements d'un serveur en cas de défaillance du premier serveur. De plus, étant donné que tous les objets créés par les membres du groupe DnsUpdateProxy ne

sont pas sécurisés, le premier utilisateur à modifier l'ensemble d'enregistrements associé à un nom DNS en devient le propriétaire. Lorsque les clients hérités sont mis à niveau, ils peuvent prendre possession de leurs enregistrements de noms sur le serveur DNS. Si tous les serveurs DHCP inscrivant des enregistrements de ressources pour les anciens clients sont membres du groupe DnsUpdateProxy, les problèmes évoqués précédemment ne se produisent pas.

Sécurisation des enregistrements à l'aide du groupe DnsUpdateProxy

Lorsque le serveur DHCP est membre du groupe DnsUpdateProxy, il ne sécurise pas les noms de domaine DNS qu'il inscrit. Par conséquent, n'utilisez pas ce groupe dans une zone intégrée à Active Directory qui autorise uniquement les mises à jour dynamiques sécurisées sans prendre de mesures supplémentaires pour sécuriser les enregistrements créés par les membres du groupe.

Pour vous protéger contre les enregistrements non sécurisés ou pour permettre aux membres du groupe DnsUpdateProxy d'inscrire des enregistrements dans des zones qui autorisent uniquement les mises à jour dynamiques sécurisées, créez un compte d'utilisateur dédié. À l'aide des informations d'identification de ce compte utilisateur, configurez les serveurs DHCP pour qu'ils effectuent des mises à jour dynamiques DNS. Plusieurs serveurs DHCP peuvent utiliser les informations d'identification d'un même compte d'utilisateur dédié.

Le compte d'utilisateur dédié est un compte d'utilisateur standard utilisé uniquement pour fournir aux serveurs DHCP des informations d'identification pour l'inscription des mises à jour dynamiques DNS. Chaque serveur DHCP fournit ces informations d'identification lors de l'inscription de noms pour le compte de clients DHCP à l'aide de la mise à jour dynamique DNS. Le compte d'utilisateur dédié est créé dans la même forêt que celle où réside le serveur DNS principal de la zone à mettre à jour. Le compte d'utilisateur dédié peut également se trouver dans une autre forêt à condition que la forêt dans laquelle il réside ait une approbation de forêt établie avec la forêt contenant le serveur DNS principal pour la zone à mettre à jour.

Lorsqu'il est installé sur un contrôleur de domaine, le service serveur DHCP hérite des autorisations de sécurité du contrôleur de domaine. Cela signifie qu'il dispose du pouvoir de mettre à jour ou de supprimer tout enregistrement DNS inscrit dans une zone sécurisée intégrée à Active Directory. Les autres ordinateurs exécutant Windows Server, tels que les contrôleurs de domaine, inscrivent ces enregistrements de manière sécurisée. Lorsqu'il est installé sur un contrôleur de domaine, configurez le serveur DHCP avec les informations d'identification du compte d'utilisateur dédié afin d'empêcher le serveur d'hériter, et éventuellement d'utiliser à mauvais escient, les privilèges du contrôleur de domaine.

Configurez un compte d'utilisateur dédié ainsi que le service serveur DHCP avec les informations d'identification du compte dans les circonstances suivantes :

- Un contrôleur de domaine est configuré pour fonctionner comme un serveur DHCP.
- Le serveur DHCP est configuré pour effectuer des mises à jour dynamiques DNS pour le compte des clients DHCP.
- Le serveur DHCP met à jour les zones DNS qui sont configurées pour autoriser uniquement les mises à jour dynamiques sécurisées.

Après avoir créé un compte d'utilisateur dédié, vous pouvez configurer des serveurs DHCP avec les informations d'identification du compte d'utilisateur à l'aide de la console DHCP ou de la commande `netsh dhcp server set dnscredentials`.

Notes

- Si les informations d'identification fournies appartiennent à un objet qui est membre du groupe de sécurité DnsUpdateProxy, le prochain objet à inscrire le même enregistrement de nom dans DNS deviendra le propriétaire de l'enregistrement.
- Si vous spécifiez des informations d'identification pour le serveur DHCP à utiliser lors de l'inscription des ordinateurs clients DHCP dans DNS, ces informations d'identification ne sont pas sauvegardées. Après la restauration d'une base de données DHCP, de nouvelles informations d'identification doivent être configurées.

Vieillissement et nettoyage DNS

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Le vieillissement et la récupération DNS sont deux fonctionnalités du serveur DNS dans Windows Server qui fonctionnent ensemble pour détecter et supprimer au fil du temps les enregistrements de ressources dynamiques obsolètes des données de zone. Un enregistrement obsolète est celui qu'un client a enregistré automatiquement mais qui reste dans la zone après le départ du client.

Avec la mise à jour dynamique, les enregistrements de ressources sont ajoutés automatiquement aux zones, par exemple lorsque les ordinateurs se connectent au réseau. Mais seul un administrateur ou le processus de vieillissement et de récupération suppriment ces documents. Sans nettoyage, les archives obsolètes s'accumulent et causent des problèmes de résolution de noms.

Le vieillissement et le fouillis s'appliquent également aux zones intégrées à Active Directory. La réplication Active Directory seule ne supprime pas les enregistrements obsolètes, donc vous avez toujours besoin de ces fonctionnalités sur les zones intégrées.

Cet article explique la terminologie, les intervalles et le cycle de vie des enregistrements que le vieillissement et le nettoyage utilisent pour déterminer quand un enregistrement est périmé. Comprendre ces mécaniques vous permet d'activer ces fonctionnalités en toute confiance, sans supprimer les enregistrements encore utilisés.

Pourquoi les disques obsolètes posent problème

Si elles ne sont pas gérées, des archives de ressources obsolètes dans les données de zone peuvent causer les problèmes suivants :

- **Résolution de nom incorrecte.** Les serveurs DNS avec des enregistrements obsolètes peuvent utiliser des informations obsolètes pour répondre aux requêtes des clients, ce qui cause des problèmes de résolution de noms sur le réseau.
- **Stockage dans une zone supérieure et trafic de réplication.** Un grand nombre d'enregistrements obsols occupent de l'espace disque serveur, allongent les transferts de zone et ajoutent de la charge au réseau.
- **Dégradation des performances.** Des enregistrements obsolètes accumulés peuvent dégrader les performances et la réactivité des serveurs DNS.

> ⚠ **Avertissement**
>
> Par défaut, le vieillissement et le récupération sont désactivés pour le service serveur DNS. Activez-les seulement après avoir bien compris tous les paramètres. Une mauvaise configuration accidentelle peut supprimer des enregistrements légitimes, empêchant les utilisateurs de résoudre ces enregistrements DNS.

Le vieillissement et la récupération sont des mécanismes indépendants

Le vieillissement et la récupération sont deux mécanismes indépendants mais complémentaires. Vous devez activer les deux pour que le nettoyage automatique des dossiers obsolètes puisse s'effectuer.

Ce que fait le vieillissement

Le vieillissement détermine si une mise à jour dynamique entrante peut actualiser l'horodatage d'un enregistrement DNS. Le vieillissement utilise l'intervalle sans actualisation pour déterminer si une mise à jour de l'horodatage est autorisée. Si un rafraîchissement dynamique arrive avant l'horodatage de l'enregistrement plus l'intervalle sans rafraîchiment, le serveur le rejette. Le vieillissement seul ne supprime jamais les archives ; Il ne suit que les horodatages.

Le serveur DNS distingue deux types d'enregistrements par leur horodatage :

- **Enregistrements dynamiques (l'horodatage n'est pas zéro)** : Enregistrements ajoutés via une mise à jour dynamique. L'horodatage représente la date et l'heure du dernier rafraîchissement ou mise à jour autorisé.
- **Enregistrements statiques (l'horodatage est zéro)** : Les enregistrements ajoutés manuellement ou à partir d'un fichier de zone textuel reçoivent un horodatage de zéro, ils ne sont donc pas éligibles au récupération. Un tel enregistrement peut toujours recevoir des mises à jour dynamiques de ses données, comme une nouvelle adresse IP, mais son horodatage reste nul, il reste donc exclu de la récupération.

Vous pouvez aussi faire en sorte que le serveur traite un enregistrement statique comme un enregistrement dynamique en réglant manuellement son horodatage à une valeur non nulle.

Fonctionnement du nettoyage

Fouiller efface les archives obsolètes. Il examine les enregistrements de ressources et supprime ceux qu'il identifie comme obsolètes. Le nettoyage détermine si un enregistrement est obsolète en fonction de l'âge que le processus de vieillissement lui attribue.

Conditions pour récupérer un disque

Le fouillement ne supprime un enregistrement que lorsqu'il remplit les quatre conditions suivantes :

- Le fouillage est activé sur le serveur DNS (un réglage au niveau du serveur).
- Le vieillissement est activé sur la zone DNS où l'enregistrement existe.
- L'enregistrement de la ressource est éligible (il a un horodatage non nul).
- L'horodatage d'enregistrement plus l'intervalle sans rafraîchissement plus l'intervalle de rafraîchissement est antérieur à l'heure actuelle du serveur.

Le nettoyage s'exécute automatiquement selon la planification, même lorsque le vieillissement est désactivé, mais il ignore toute zone pour laquelle le vieillissement est désactivé et n'effectue aucune action sur les enregistrements de ces zones, même sur ceux dont les horodatages les feraient autrement considérer comme obsolètes.

Terminologie et intervalles

Les termes suivants s'appliquent lorsque vous parlez de vieillissement et de récupération.

Agrandir le tableau

Terme	Definition
Étendue de réplication Active Directory	Le paramètre qui définit quels serveurs DNS reçoivent une zone intégrée à Active Directory via la réplication AD DS. La zone peut se répliquer vers tous les serveurs DNS fonctionnant sur des contrôleurs de domaine dans le domaine ou la forêt, ou vers tous les contrôleurs de domaine du domaine pour assurer la compatibilité avec Windows 2000.
Disponible pour l'heure de nettoyage	Un attribut par zone qui représente le moment le plus précoce auquel la zone peut participer à un passage de nettoyage Lorsque vous activez le vieillissement ou modifiez ses paramètres, le serveur calcule cela comme : l'heure actuelle du serveur (arrondie à la baisse à l'heure la plus proche) + l'intervalle de rafraîchissement de la zone. Atteindre ce temps ne déclenche pas en soi un passage de fouille sur la zone ni ne garantit que le serveur supprime les enregistrements qu'elle contient. Pour la formule, voir Quand la récupération peut commencer.
Heure actuelle du serveur	La date et l'heure actuelles sur le serveur DNS. Il sert de point de référence pour tous les calculs de vieillissement.

Terme	Definition
Intervalle de sondage par annuaire	L'intervalle auquel le service serveur DNS interroge Active Directory pour détecter les modifications effectuées par d'autres contrôleurs de domaine. Le polling permet au serveur DNS de détecter et de charger les mises à jour qui se répliquent via Active Directory.
dnsNode	Un objet Active Directory qui représente un nom DNS au sein d'une zone intégrée à Active Directory. Un `dnsNode` peut contenir un ou plusieurs enregistrements DNS pour le même nom d'hôte. Par exemple, un `dnsNode` objet représente un hôte nommé `server1.contoso.com` et peut contenir des types d'enregistrements A, AAAA ou autres.
dnsRecord	Les données des enregistrements DNS stockées dans un `dnsNode` objet, telles que les enregistrements A, AAAA, CNAME, MX, et PTR. Les zones intégrées à Active Directory stockent les données d'enregistrement, les horodatages et les informations vieillissantes comme attributs de l'objet `dnsNode`.
dnsTombstoned	Un attribut Active Directory qui marque un `dnsNode` comme étant logiquement supprimé après que le nettoyage, un administrateur ou une mise à jour dynamique autorisée a supprimé son dernier enregistrement. Le service Serveur DNS définit l'attribut, puis services de domaine Active Directory (AD DS) réplique l'objet marqué comme supprimé avant de le supprimer définitivement.
Intervalle sans rafraîchissement	La période après que le serveur a défini l'horodatage d'un enregistrement, pendant laquelle le serveur n'accepte pas d'actualisation de l'horodatage. Cette période réduit le trafic de réplication inutile. Le serveur considère comme réussie une actualisation avec les mêmes données, mais aucune écriture dans la base de données n'a lieu et l'horodatage ne change pas. Le serveur continue d'écrire des mises à jour qui modifient les données d'enregistrement. La valeur par défaut est de 7 jours.
Renouvellement des enregistrements	Une mise à jour dynamique qui laisse le nom hôte et l'adresse IP inchangés et ne modifie que l'horodatage. Le serveur bloque les rafraîchissements pendant l'intervalle sans rafraîchissement.
Mise à jour des records	Une mise à jour dynamique dans laquelle les données de l'enregistrement changent, comme une nouvelle adresse IP. Le serveur accepte toujours les mises à jour, même pendant l'intervalle sans rafraîchissement, et ils réinitialisent l'horodatage.
Intervalle d'actualisation	La période qui commence après l'expiration de l'intervalle sans rafraîchissement, pendant laquelle le serveur accepte un rafraîchissement. Un disque devient obsolète s'il n'est pas rafraîchi avant la fin de cette période. La valeur par défaut est de 7 jours.
Horodatage de l'enregistrement de ressource	Valeur de date et d'heure apposée sur un enregistrement, à l'heure près, par le processus de vieillissement ou manuellement par un administrateur. Le nettoyage l'utilise pour déterminer si le disque est obsolète.
Période de nettoyage	L'intervalle entre les passes de nettoyage automatique successives sur un serveur DNS. Il se réinitialise dès que le service DNS redémarre. Le temps par défaut est de 7 jours et le minimum est d'1 heure.

Terme	Definition
Nettoyage des serveurs	Un paramètre de zone avancé optionnel qui configure quelles adresses IP des serveurs DNS peuvent effectuer le nettoyage de la zone. Par défaut, chaque serveur DNS qui héberge la zone peut la nettoyer.

Calcul des enregistrements obsolètes

Un enregistrement est obsolet et éligible à suppression par recyclage lorsque la condition suivante est vraie :

Horodatage de l'enregistrement + intervalle sans actualisation + intervalle d'actualisation < heure actuelle du serveur

Avec les réglages par défaut (7 jours plus 7 jours), un enregistrement qui n'est pas actualisé dans les 14 jours devient obsolète. Le nettoyage supprime l'enregistrement au passage suivant. Dans le pire des cas, un enregistrement obsolète peut donc persister pendant la durée cumulée des périodes de non-actualisation, d'actualisation et de nettoyage. Par exemple, cela peut atteindre jusqu'à 21 jours avec tous les paramètres par défaut.

Cycle de vie des archives de ressources

Pour comprendre le processus, considérez la durée de vie et les étapes d'un seul enregistrement de ressource sur un serveur et une zone où le vieillissement et la récupération sont activés. Les étapes suivantes décrivent la durée de vie complète d'un enregistrement dynamique :

1. **L'enregistrement est créé.** Un hôte, tel que `host-a.example.contoso.com`, enregistre son enregistrement de ressource hôte (A) auprès du serveur DNS. Le serveur horodate l'enregistrement avec l'heure actuelle du serveur, à l'heure près.

2. **Le record vit sans mises à jour.** Immédiatement après l'enregistrement, la période sans actualisation débute. Pendant cet intervalle, le serveur supprime les tentatives de rafraîchissement de l'enregistrement, ce qui réduit le trafic de réplication Active Directory. Le serveur accepte toujours les mises à jour qui modifient les données de l'enregistrement, comme une nouvelle adresse IP, et chaque mise à jour réinitialise l'horodatage de l'enregistrement.

3. **La fenêtre de rafraîchissement s'ouvre.** Après l'expiration de l'intervalle sans rafraîchissement, l'intervalle de rafraîchissement commence et le serveur accepte les rafraîchissements. Lorsque le serveur traite un rafraîchissement, il réinitialise l'horodatage et l'intervalle sans rafraîchissement recommence.

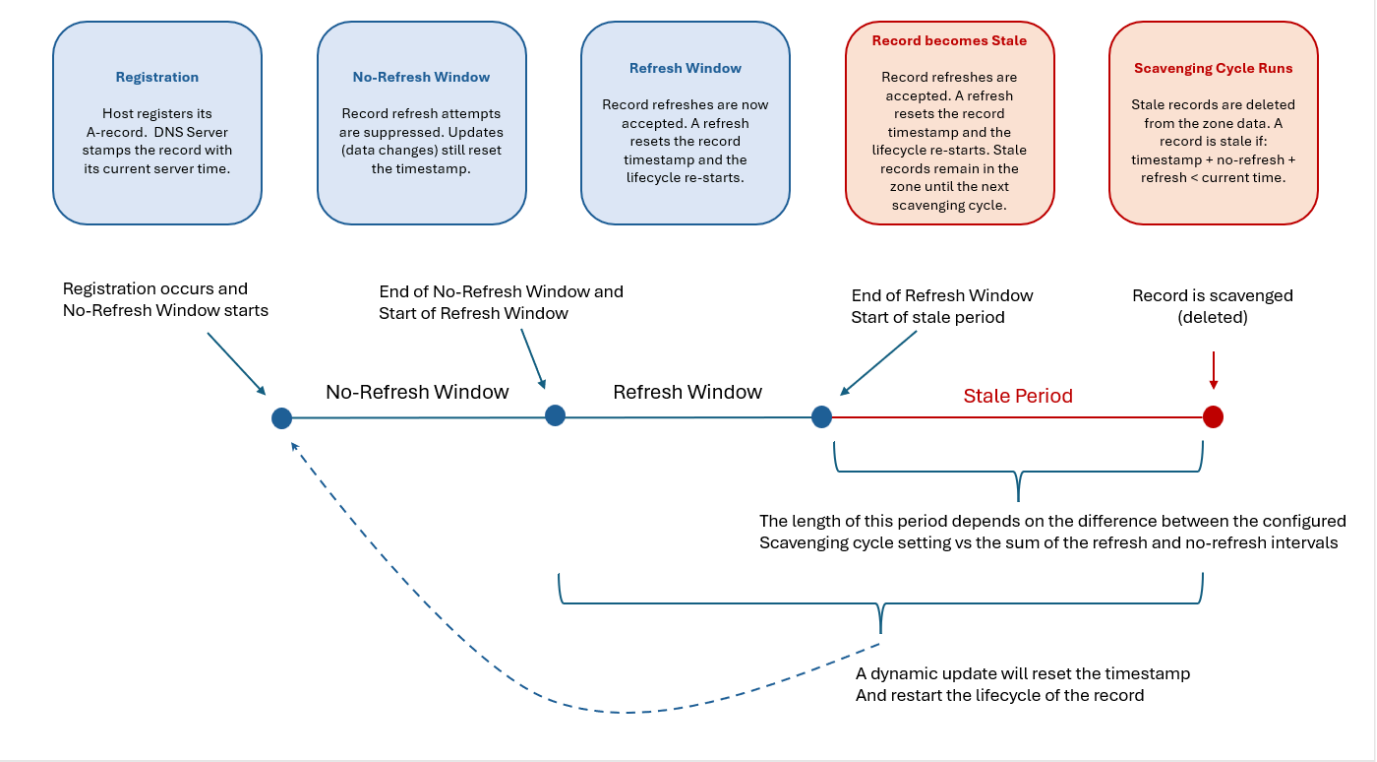
4. **Le disque devient fade.** Si le disque n'est pas rafraîchi pendant l'intervalle de rafraîchissement, il devient obsolète. L'enregistrement reste dans la zone jusqu'à ce que le prochain passage de nettoyage s'exécute.

5. **Le disque est nettoyé.** Lors d'un cycle de nettoyage, le serveur examine tous les enregistrements de toutes les zones éligibles au nettoyage. Pour chaque enregistrement ayant un horodatage non nul, le serveur compare l'heure actuelle du serveur à la somme suivante :

   Horodatage + intervalle d'absence de rafraîchissement + intervalle de rafraîchissement

   - Si la somme est supérieure à l'heure actuelle du serveur, le serveur n'agit pas et l'enregistrement continue de vieillir dans la zone.
   - Si la somme est inférieure au temps serveur actuel, le serveur supprime l'enregistrement des données de zone en mémoire serveur. Pour une zone intégrée à Active Directory, le serveur écrit la suppression dans AD DS, qui la réplique sur les autres serveurs DNS hébergeant la zone afin qu'ils suppriment leurs copies de l'enregistrement.

Le schéma suivant montre le cycle de vie d'un enregistrement de ressource au cours de l'intervalle sans rafraîchissement, de l'intervalle de rafraîchissement, de l'état obsolète et du nettoyage.



Quand le balayage peut commencer

Le nettoyage peut commencer pour une zone lorsque l'heure actuelle du serveur est postérieure à l'*heure de disponibilité de la zone pour le nettoyage*. Le délai de nettoyage disponible est une valeur propre à chaque zone qui indique le moment à partir duquel la zone peut participer à un cycle de nettoyage. Le serveur le calcule ainsi :

Temps disponible pour la récupération = heure actuelle du serveur (arrondie à l'heure inférieure) + intervalle d'actualisation

Lorsque vous activez pour la première fois le vieillissement sur une zone, ou que vous modifiez les paramètres de vieillissement de la zone, ce calcul accorde à la zone un intervalle d'actualisation de protection avant qu'elle ne devienne éligible au nettoyage.

Le fouillage automatique est un comportement à l'échelle du serveur DNS. Vous le contrôlez avec un bouton de récupération au niveau serveur et un intervalle de récupération, appelé la période de récupération. Lorsque vous activez la bascule, le serveur exécute un passage de récupération une fois par période de récupération.

Lorsque le nettoyage est déjà activé lorsque le service DNS démarre, le serveur planifie le premier cycle de nettoyage une période de nettoyage après le démarrage, puis planifie chaque cycle suivant une période de nettoyage après le précédent.

Lorsque vous activez le nettoyage alors que le service DNS est déjà en cours d'exécution et que le serveur n'a encore jamais effectué de nettoyage, un cycle est normalement exécuté lors du prochain contrôle périodique du serveur, en général dans les minutes qui suivent.

Vous pouvez également lancer manuellement une opération de nettoyage à l'aide du Gestionnaire DNS (MMC) ou de PowerShell. Une exécution manuelle contourne la planification, mais elle ne contourne pas les critères d'éligibilité de zone ni les exigences de vieillissement des enregistrements, et ne modifie pas la planification automatique.

Une passe de récupération saute une zone lorsque l'une des conditions suivantes s'applique :

- Le serveur n'est pas un serveur de nettoyage autorisé pour la zone.
- Le vieillissement est désactivé dans cette zone.
- L'heure actuelle du serveur est antérieure à l'heure à laquelle la zone devient disponible pour le nettoyage.
- La zone est en pause, est une zone de cache ou est une zone signée en mode hors ligne.
- La partition du répertoire Active Directory de la zone n'a pas été répliquée depuis le lancement du serveur DNS.

Le serveur réinitialise le temps disponible pour la récupération sur une zone chaque fois que l'un des événements suivants se produit :

- Vous activez les mises à jour dynamiques pour la zone.
- L'état de la case à cocher **Nettoyer les enregistrements de ressources obsolètes** change.
- Le service Serveur DNS démarre et charge une zone principale pour laquelle le nettoyage est activé.
- Une zone reprend le service après une pause.

Comportement dans les zones intégrées à Active Directory

Dans une zone intégrée à Active Directory, le serveur stocke les données de zone dans AD DS et les réplique via Active Directory plutôt que dans un fichier de zone local basé sur du texte. Le serveur utilise des transferts de zone standard (AXFR ou IXFR) uniquement lorsque vous configurez une zone intégrée Active Directory pour servir un serveur DNS secondaire conventionnel non intégré ; sinon, les données de zone ne se propagent que par réplication Active Directory. AD DS stocke tous les enregistrements de ressources portant le même nom, tels que les enregistrements A et AAAA pour `host.contoso.com`, dans un seul `dnsNode` objet sous forme de valeurs de son attribut multi-valeur `dnsRecord` .

La réplication propage les ajouts d'enregistrements, les mises à jour horodatages et les suppressions récupérées entre les serveurs DNS, mais elle ne supprime pas les enregistrements obsolètes à elle seule. Vous devez toujours utiliser le vieillissement et le nettoyage pour identifier et supprimer les enregistrements obsolètes dans une zone intégrée à Active Directory.

Le nettoyage et la mise en tombstone sont deux opérations distinctes :

- **Le nettoyage** supprime les valeurs obsolètes `dnsRecord`. Lorsque le serveur récupère un enregistrement obsolète, il supprime la valeur correspondante `dnsRecord` . Si d'autres `dnsRecord` valeurs restent pour le `dnsNode`, le nœud reste.
- **Tombstoning** est l'état de suppression dans Active Directory de l'objet `dnsNode` une fois son dernier enregistrement supprimé. Si le serveur supprime le dernier `dnsRecord`, le service Serveur DNS marque le `dnsNode` comme supprimé. AD DS réplique ce marquage afin que d'autres serveurs DNS hébergeant la zone cessent également de charger le `dnsNode`, et que le nettoyage normal du DNS et de l'AD DS supprime l'objet de répertoire plus tard.

Pourquoi nous recommandons un serveur de récupération par zone

Activez le nettoyage au niveau du serveur sur un seul serveur DNS par zone. Ne configurez pas plusieurs serveurs de récupération par zone car :

- Les événements de nettoyage et les données d'audit sont répartis sur plusieurs serveurs.
- Des calendriers de récupération différents rendent les suppressions plus difficiles à prédire et à retracer.
- Les problèmes de réplication ou de configuration deviennent plus difficiles à dépanner.

Utilisez le paramètre de zone `ScavengingServers` pour restreindre quelles adresses IP de serveur DNS peuvent récupérer la zone. Vous pouvez configurer plusieurs serveurs pour la redondance, mais ils sont généralement inutiles.

Contenu connexe

- Configurer le vieillissement et le nettoyage DNS

ⓘ**Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Dernière mise à jour : 23/09/2026

Recherche inversée

Article • 08/05/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Dans la plupart des recherches DNS, les clients effectuent généralement une recherche vers l'avant, qui est une recherche basée sur le nom DNS d'un autre ordinateur tel qu'il est stocké dans une adresse (A) RR. Ce type de requête attend une adresse IP en tant que données de ressource pour la réponse répondue.

DNS fournit également un processus de recherche inverse, permettant aux clients d'utiliser une adresse IP connue pendant une requête de nom et de rechercher un nom d'ordinateur en fonction de son adresse. Une recherche inversée prend la forme d'une question, telle que « Pouvez-vous me dire le nom DNS de l'ordinateur qui utilise l'adresse IP 192.168.1.20 ? »

Fonctionnement de la recherche inversée

Un domaine spécial appelé domaine `in-addr.arpa` a été défini dans les normes DNS. Ce domaine est réservé dans l'espace de noms DNS Internet pour fournir un moyen pratique et fiable d'effectuer des requêtes inversées. Pour créer l'espace de noms inverse, les sous-domaines du `in-addr.arpa` domaine sont formés à l'aide de l'ordre inverse des nombres dans la notation décimale en pointillés des adresses IP.

Lorsque les adresses IP sont lues de gauche à droite, elles sont interprétées de la manière opposée par rapport aux noms DNS. Cet ordre inversé des domaines pour chaque valeur d'octet est nécessaire. Lors de la lecture d'une adresse IP de gauche à droite, elle commence par l'adresse réseau et se termine par l'adresse de l'hôte. Pour cette raison, l'ordre des octets d'adresse IP doit être inversé lors de la génération de l'arborescence du `in-addr.arpa` domaine. Les adresses IP de l'arborescence DNS `in-addr.arpa` peuvent être déléguées aux entreprises, car elles reçoivent un ensemble spécifique ou limité d'adresses IP dans les classes d'adresses définies par Internet.

Enfin, l'arborescence du domaine in-addr.arpa, telle qu'elle est intégrée au DNS, nécessite qu'un autre type RR, le pointeur (PTR) RR, soit défini. Ce RR est utilisé pour créer un mappage dans la zone de recherche inversée qui correspond généralement à un hôte (A) nommé RR pour le nom d'ordinateur DNS d'un hôte dans sa zone de recherche directe.

Le domaine in-addr.arpa s'applique à une utilisation dans tous les réseaux TCP/IP basés sur l'adressage IPv4 (Internet Protocol version 4). L'Assistant Nouvelle zone suppose automatiquement que vous utilisez ce domaine lors de la création d'une zone de recherche inversée.

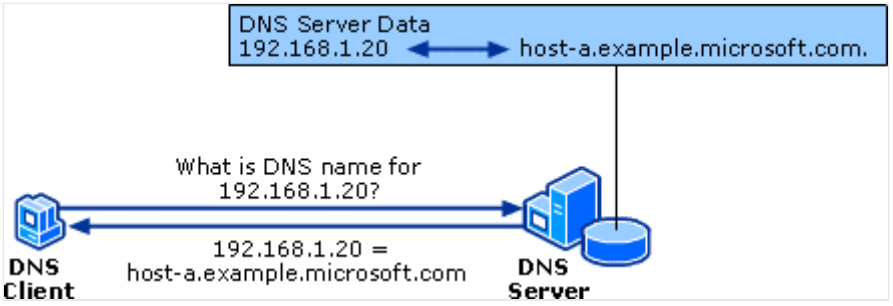
Si vous configurez des zones de recherche inversées pour un réseau IPv6 (Internet Protocol version 6), vous pouvez spécifier un nom exact à l'aide de l'Assistant Nouvelle zone. Cela vous permet de créer des zones de recherche inverse dans la console DNS qui peuvent être utilisées pour prendre en charge les réseaux IPv6. Les zones IPv6 utilisent un autre nom de domaine spécial, le `ip6.arpa` domaine.

Pour plus d'informations sur IPv6 et DNS, notamment des exemples de création et d'utilisation `ip6.arpa` de noms de domaine comme décrit dans RFC 1886 (« Extensions DNS pour prendre en charge IP version 6 »), consultez informations de référence DNS.

> ⓘ **Notes**
>
> La configuration des RR PTR et des zones de recherche inverse pour identifier les hôtes par requête inverse est strictement une partie facultative de l'implémentation standard DNS. Vous n'êtes pas obligé d'utiliser des zones de recherche inverse, bien que pour certaines applications en réseau, elles sont utilisées pour effectuer des vérifications de sécurité.

Exemple : requête inverse IPv4

La figure suivante montre un exemple de requête inversée lancée par un client DNS (host-b) pour apprendre le nom d'un autre hôte (host-a) en fonction de son adresse IP, 192.168.1.20.



Le processus de requête inverse, comme illustré dans cette figure, se produit dans les étapes suivantes :

1. Le client, `host-b` interroge le serveur DNS pour un pointeur (PTR) RR mappé à l'adresse IP de 192.168.1.20 pour `host-a`.

   Étant donné que la requête concerne les enregistrements PTR, le programme de résolution inverse l'adresse et ajoute le `in-addr.arpa` domaine à la fin de l'adresse inverse. Cette requête forme le nom de domaine complet (`20.1.168.192.in-addr.arpa.`) à rechercher dans une zone de recherche inverse.

2. Une fois l’enregistrement localisé, le serveur DNS faisant autorité pour `20.1.168.192.in-addr.arpa` peut répondre avec les informations de l'enregistrement de type PTR. Cette réponse inclut le nom de domaine DNS pour `host-a`, en effectuant la recherche inversée.

   Si le nom inversé interrogé n’est pas accessible à partir du serveur DNS, la résolution DNS normale (récursivité ou itération) peut être utilisée pour localiser un serveur DNS faisant autorité pour la zone de recherche inverse et qui contient le nom interrogé. Dans ce sens, le processus de résolution de noms utilisé dans une recherche inversée est identique à celui d’une recherche vers l’avant.

Intégration de recherche DNS WINS

Article • 30/04/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Le service WINS (Windows Internet Name Service) représente un service hérité d'inscription et de résolution de noms d'ordinateurs qui mappe les noms NetBIOS d'ordinateurs à des adresses IP. La prise en charge de l'utilisation du service WINS (Windows Internet Name Service) est fournie pour rechercher des noms DNS que l'espace de noms de domaine DNS ne peut pas résoudre. Pour effectuer une recherche WINS à l'aide du rôle serveur DNS sur Windows Server, deux types d'enregistrements de ressources spécifiques sont utilisés et peuvent être activés pour toutes les zones chargées par le service DNS :

- L'enregistrement de ressource WINS, qui peut être activé pour intégrer la recherche WINS dans les zones de recherche directe
- Enregistrement de ressource WINS-R, qui peut être activé pour intégrer la demande d'état de l'adaptateur de nœud pour les zones de recherche inverse

> **Conseil**
>
> Si vous avez déjà déployé WINS sur votre réseau, il est recommandé de migrer complètement votre réseau pour utiliser DNS exclusivement.

Enregistrement de ressource WINS

Les services WINS et DNS sont utilisés pour fournir la résolution de noms pour l'espace de noms NetBIOS et l'espace de noms de domaine DNS, respectivement. Bien que DNS et WINS puissent fournir un service de nom distinct et utile aux clients, WINS est nécessaire pour prendre en charge les clients et les programmes plus anciens qui nécessitent une prise en charge de l'affectation de noms NetBIOS.

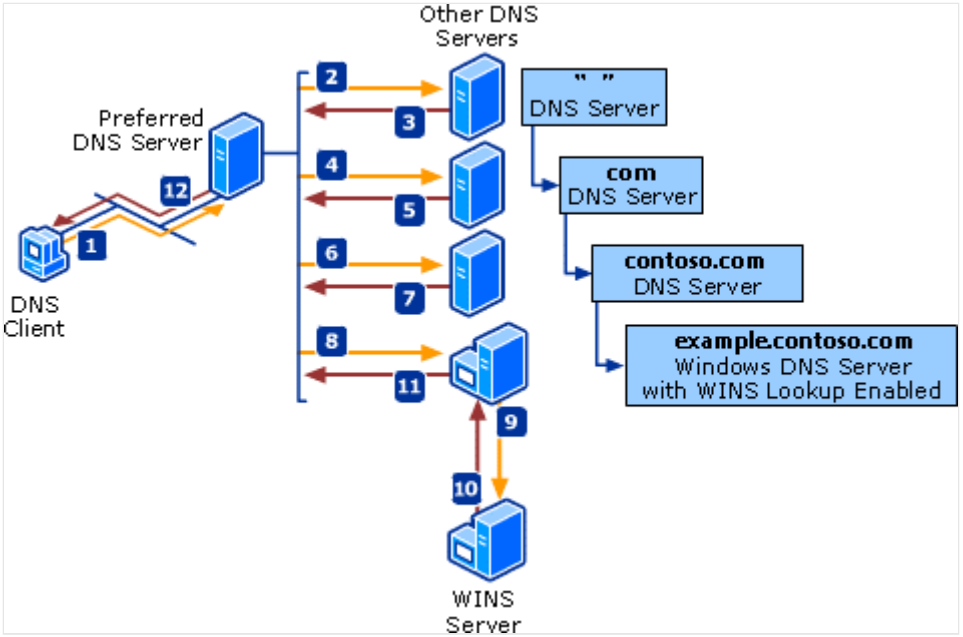
Toutefois, le service DNS peut travailler avec WINS pour fournir des recherches de noms combinées dans les deux espaces de noms lors de la résolution d'un nom de domaine DNS introuvable dans les informations de zone. Pour fournir cette interopérabilité, un nouvel enregistrement (l'enregistrement WINS) est défini dans le fichier de base de données de zone.

La présence d'un enregistrement de ressource WINS peut indiquer au service DNS d'utiliser WINS pour rechercher des requêtes vers l'avant pour les noms d'hôtes ou les noms introuvables dans la base de données de zone. Cette fonctionnalité est utile pour la résolution

de noms requise par les clients qui ne prennent pas en charge WINS. Par exemple, les noms des ordinateurs non inscrits auprès de DNS, tels que les clients UNIX ou Windows hérités.

Recherches

Le diagramme suivant est un exemple d'un client DNS interrogeant son serveur DNS dans une tentative de recherche de l'adresse d'un autre ordinateur.



À l'étape 1, le client interroge son serveur DNS préféré. Dans les étapes 2 à 8, le processus normal de récursivité se poursuit, car le serveur DNS préféré interroge d'autres serveurs DNS en succession pour le compte du client. Ce processus se termine à l'étape 8, lorsque le serveur DNS de la `example.contoso.com` zone se trouve via la chaîne précédente de réponses de référence.

Lorsque le serveur DNS de la `example.contoso.com` zone reçoit la requête de l'hôte, il recherche dans sa zone configurée pour voir si un enregistrement de ressource d'adresse correspondante (A) est trouvé. Si aucun enregistrement A n'est trouvé et que la zone est configurée pour utiliser la résolution WINS, le serveur DNS sépare la partie hôte du nom de domaine complet contenu dans la requête DNS.

La partie hôte du nom est le premier label du nom de domaine DNS interrogé, avant qu'un point ne soit utilisé dans le nom.

- Le serveur envoie ensuite une demande de nom NetBIOS au serveur WINS à l'aide du nom d'hôte.
- Si le serveur WINS peut résoudre le nom, il retourne l'adresse IP au serveur DNS.

- Le serveur DNS compile ensuite un enregistrement de ressource A à l'aide de l'adresse IP résolue via le serveur WINS. Elle retourne cet enregistrement au serveur DNS préféré d'origine interrogé par le client.
- Le serveur DNS préféré transmet ensuite la réponse de requête au client demandeur.

Recherches inversées

Une entrée de recherche inversée de type WINS-R ou WINS peut être activée et ajoutée aux zones de recherche inverse. Toutefois, étant donné que la base de données WINS n'est pas indexée à l'aide de l'adresse IP, le service DNS ne peut pas envoyer de recherche de nom inverse à WINS pour obtenir le nom d'un ordinateur en fonction de son adresse IP.

Étant donné que WINS ne fournit pas de fonctionnalité de recherche inversée, le service DNS envoie à la place une demande d'état de l'adaptateur de nœud directement à l'adresse IP implicite dans la requête inverse DNS. Lorsque le serveur DNS obtient le nom NetBIOS de la réponse d'état du nœud, il ajoute le nom de domaine DNS au nom NetBIOS fourni dans la réponse d'état du nœud et transfère le résultat au client demandeur.

> ⓘ **Notes**
>
> Les enregistrements de ressources WINS et WINS-R sont propriétaires du service DNS Server fourni par Windows. Vous pouvez empêcher ces enregistrements de ressources d'être inclus dans les transferts de zone vers d'autres implémentations de serveur DNS.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Qu’est-ce que DNSSEC ?

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Les extensions de sécurité du DNS (DNSSEC, Domain Name System Security Extensions) représentent une suite d’extensions qui renforcent la sécurité du protocole DNS en permettant la validation des réponses DNS. DNSSEC fournit l’autorité d’origine, l’intégrité des données et le déni d’existence authentifié. Avec DNSSEC, le protocole DNS est beaucoup moins vulnérable à certains types d’attaques, notamment aux tentatives d’usurpation DNS.

Fonctionnement de DNSSEC

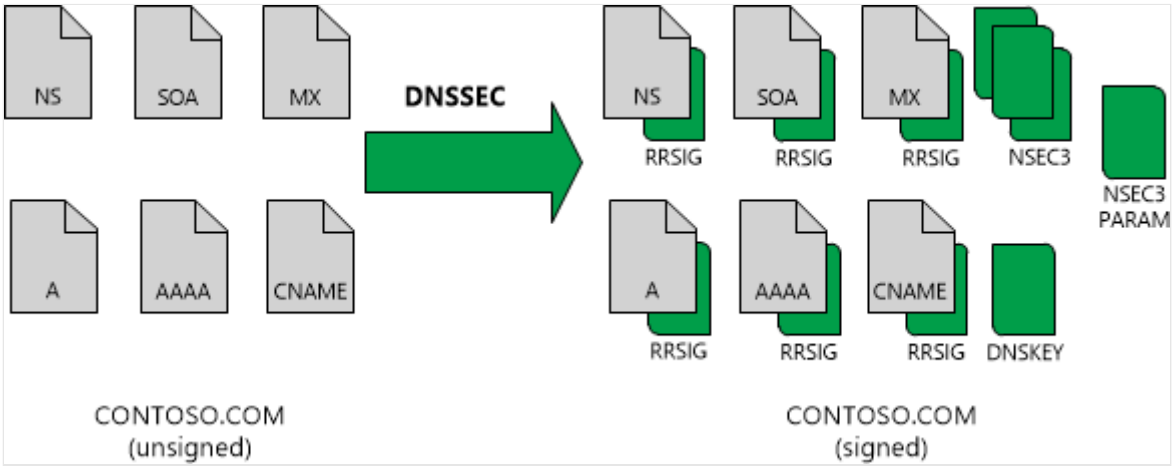
Les zones DNS peuvent être sécurisées avec DNSSEC grâce à un processus appelé signature de zone lorsqu’il est utilisé avec un serveur DNS faisant autorité qui prend en charge DNSSEC. Signer une zone avec DNSSEC ajoute la prise en charge de la validation à une zone sans modifier le mécanisme de base d’une requête DNS et de sa réponse.

La validation des réponses DNS repose sur les signatures numériques incluses avec les réponses DNS. Ces signatures numériques sont contenues dans les enregistrements de ressources liés à DNSSEC qui sont générés et ajoutés à la zone durant la signature de zone.

Les extensions DNSSEC de base sont spécifiées dans les documents RFC (Request For Comments) suivants.

- RFC 4033 : « Introduction et configuration requise de la sécurité DNS »
- RFC 4034 : « Enregistrements de ressources pour les extensions de sécurité DNS »
- RFC 4035 : « Modifications du protocole pour les extensions de sécurité DNS »

La figure suivante montre un exemple d’enregistrements de ressource DNS pour la zone contoso.com avant et après la signature de zone.



Pour plus d'informations sur chacun de ces enregistrements de ressources, consultez Enregistrements de ressources DNSSEC.

Enregistrements de ressources DNS

Le tableau suivant présente les types d'enregistrements de ressources utilisés avec DNSSEC.

Agrandir le tableau

Type d'enregistrement de ressource	Description
Signature d'enregistrement de ressource (RRSIG)	Les signatures qui sont générées avec DNSSEC sont contenues dans des enregistrements RRSIG. Chaque enregistrement RRSIG est mis en correspondance avec un autre enregistrement dans la zone pour laquelle il fournit une signature numérique. Lorsqu'un solveur émet une requête pour un nom, un ou plusieurs enregistrements RRSIG sont retournés dans la réponse.
Next Secure (NSEC)	Un enregistrement NSEC est utilisé pour prouver la non-existence d'un nom DNS. Les enregistrements NSEC empêchent les attaques par usurpation d'identité qui visent à tromper un client DNS en lui faisant croire qu'un nom DNS n'existe pas.
Next Secure 3 (NSEC3)	NSEC3 est un remplacement ou une alternative au NSEC qui empêche *la marche de zone*. L'énumération de zone est le processus qui consiste à répéter des requêtes NSEC afin de récupérer tous les noms d'une zone. Un serveur DNS exécutant Windows Server 2012 ou un système d'exploitation ultérieur prend en charge NSEC et NSEC3. Une zone peut être signée soit avec NSEC, soit avec NSEC3, mais pas avec les deux.
Paramètre Next Secure 3 (NSEC3PARAM)	L'enregistrement NSEC3PARAM permet de déterminer quels enregistrements NSEC3 inclure dans les réponses pour les noms DNS non existants.
Clé DNS (DNSKEY)	Un enregistrement de ressource DNSKEY stocke une clé de chiffrement publique qui sert à vérifier une signature. L'enregistrement DNSKEY est utilisé par un serveur DNS pendant le processus de validation. Les enregistrements DNSKEY peuvent stocker les clés publiques pour une clé de signature de zone (ZSK) ou une clé de signature de clé (KSK).
Signataire de délégation (DS)	Un enregistrement DS est un type d'enregistrement DNSSEC qui sert à sécuriser une délégation. Les enregistrements DS permettent de générer des chaînes d'authentification vers les zones enfants.

À l'exception de l'enregistrement DS, tous ces enregistrements sont ajoutés à une zone automatiquement lorsqu'elle est signée avec DNSSEC. L'enregistrement DS est un enregistrement spécifique qui peut être ajouté manuellement à une zone parente pour créer

une délégation sécurisée pour une zone enfant. Par exemple, la zone contoso.com peut contenir un enregistrement DS pour secure.contoso.com. Cependant, cet enregistrement doit être créé soit dans la zone parente, soit dans une zone enfant pour être ensuite propagée dans la zone parente. L'enregistrement DS n'est pas être automatiquement créé à la signature d'une zone.

Les enregistrements NSEC ou NSEC3 sont automatiquement ajoutés à une zone lors de la signature de zone. Toutefois, une zone signée ne peut pas avoir à la fois des enregistrements NSEC et des enregistrements NSEC3. Le type d'enregistrement (NSEC ou NSEC3) ajouté à la zone dépend de la configuration de la signature de zone. Dans l'exemple précédent, la zone est signée à l'aide de NSEC3.

Ancres de confiance

Les enregistrements de ressources DNSKEY et DS sont également appelés *ancres d'approbation* ou *points d'approbation*. Une ancre d'approbation doit être distribuée à tous les serveurs DNS ne faisant pas autorité qui assurent la validation DNSSEC des réponses DNS pour une zone signée. Si le serveur DNS s'exécute sur un contrôleur de domaine, les ancres d'approbation sont stockées dans une partition d'annuaire de forêt dans les services de domaine Active Directory (AD DS). Elles peuvent être répliquées dans tous les contrôleurs de domaine de la forêt. Sur des serveurs DNS autonomes, les ancres d'approbation sont stockées dans un fichier appelé `TrustAnchors.dns`.

Utilisez Windows PowerShell pour afficher les ancres d'approbation d'une zone à l'aide de la commande Get-DnsServerTrustAnchor . Pour afficher tous les points d'approbation actuels sur un serveur, utilisez la commande PowerShell Get-DnsServerTrustPoint . Un serveur DNS exécutant Windows Server 2012 ou un système d'exploitation ultérieur affiche également les ancres d'approbation configurées dans l'arborescence de la console du Gestionnaire DNS dans le conteneur **Points d'approbation** .

Étapes suivantes

Pour en savoir plus sur la façon dont DNSSEC utilise les enregistrements de ressources pour valider et sécuriser les réponses DNS, consultez Valider les réponses DNS.

Valider et sécuriser les réponses DNS à l'aide de DNSSEC

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Les enregistrements de ressources DNSSEC sont utilisés pour valider et sécuriser les réponses DNS. Les zones DNS sont sécurisées avec DNSSEC via la signature de zone. La signature d'une zone ajoute la prise en charge de la validation sans modifier le mécanisme de base d'une requête et d'une réponse DNS. Pour obtenir une présentation de DNSSEC pour le serveur DNS dans Windows Server, consultez Vue d'ensemble de DNSSEC.

Les signatures numériques sont incluses dans les réponses DNS pour assurer la validation. Ces signatures numériques sont contenues dans les enregistrements de ressources liés à DNSSEC qui sont générés et ajoutés à la zone durant la signature de zone.

DNS récursif

Lorsqu'un serveur DNS récursif ou de transfert prenant en charge DNSSEC reçoit une requête d'un client DNS pour une zone signée par DNSSEC, il demande que le serveur DNS faisant autorité envoie également des enregistrements DNSSEC pour valider la réponse DNS. Un serveur DNS récursif ou de transfert reconnaît que la zone prend en charge la technologie DNSSEC si elle possède un DNSKEY, également appelé « ancre d'approbation », pour cette zone.

> ⓘ **Important**
>
> Un serveur DNS ne faisant pas autorité peut utiliser la récursivité ou le transfert pour résoudre une requête DNS. Dans cette rubrique, le serveur ne faisant pas autorité est considéré comme un serveur DNS récursif ; si le serveur utilise le transfert, le processus utilisé pour la validation DNSSEC des réponses DNS est le même.

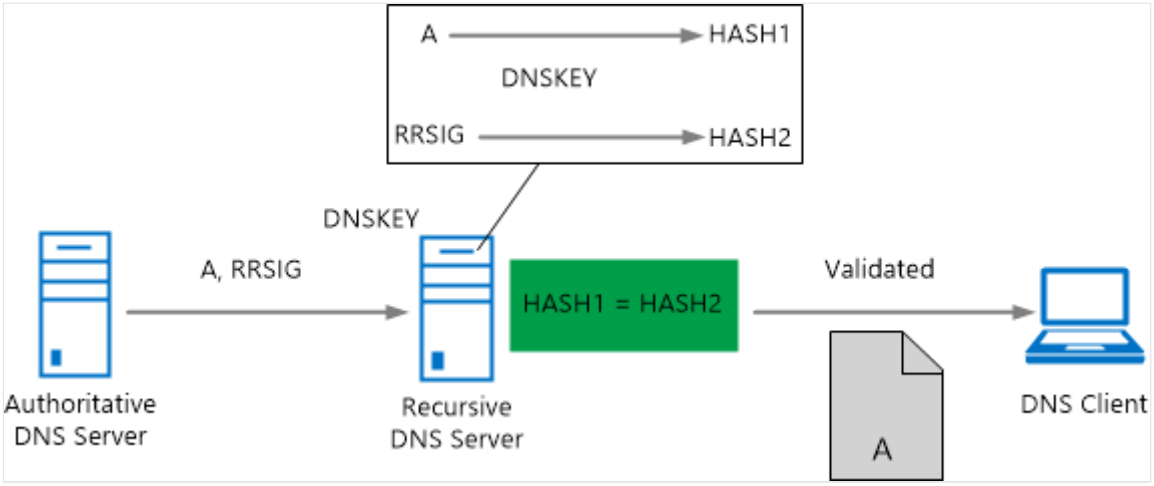
DNSKEY

Un serveur DNS récursif utilise l'enregistrement de ressource *DNSKEY* pour valider les réponses du serveur DNS faisant autorité. Pour valider les réponses, le serveur DNS déchiffre les signatures numériques contenues dans les enregistrements de ressources liés à DNSSEC et compare les valeurs de hachage. Si les valeurs de hachage sont identiques, il adresse une réponse au client DNS avec les données DNS qu'il a demandées, telles qu'un enregistrement

de ressource (A) hôte. Si les valeurs de hachage ne correspondent pas, il répond par un message `SERVFAIL`. De cette façon, un serveur DNS de résolution compatible avec la technologie DNSSEC et sur lequel une ancre d'approbation valide est installée vous protège contre les usurpation DNS, que les clients DNS prennent en charge la technologie DNSSEC ou non.

Si votre client DNS prend en charge DNSSEC, il peut être configuré pour exiger du serveur DNS qu'il effectue une validation DNSSEC.

Le graphique suivant illustre le processus de validation.



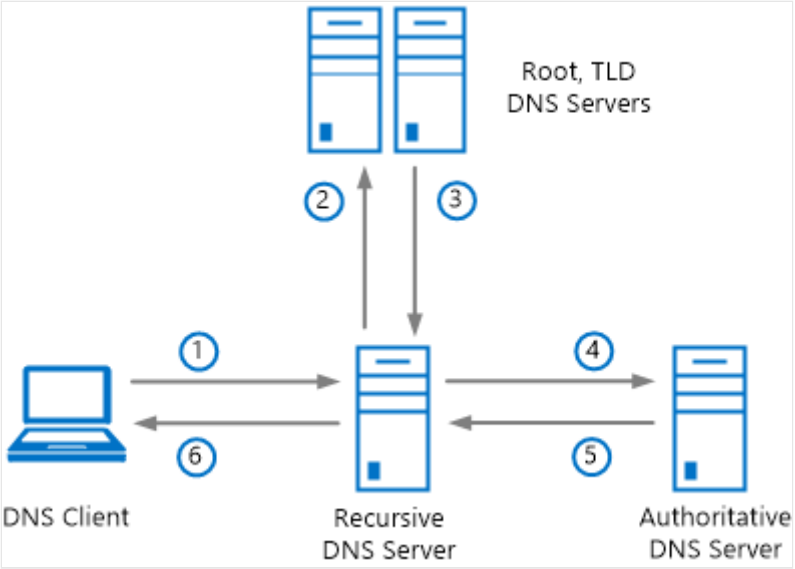
Les DNSKEY sont utilisées pour calculer les valeurs de hachage et déchiffrer les enregistrements RRSIG. La figure ne présente pas tous les processus de validation effectués. Une validation supplémentaire est également effectuée pour garantir la validité des DNSKEY et des enregistrements DS, le cas échéant (ne figurent pas dans la capture d'écran).

Processus de requête et de réponse DNS

Un exemple simple illustre comment vous pouvez incorporer DNSSEC dans le processus de requête et de réponse DNS pour assurer la validation.

Dans l'exemple suivant, un ordinateur client DNS interroge un serveur DNS (avec mise en cache) récursif, qui, à son tour, interroge les serveurs DNS faisant autorité avant de renvoyer une réponse. Cet exemple considère que les données DNS ne sont pas encore mises en cache sur le client ou le serveur. Les données DNSSEC ne valident l'authenticité des réponses DNS que lorsqu'une zone est signée et que vous utilisez des serveurs et des clients prenant en charge DNSSEC.

Le graphique suivant illustre le processus de requête DNS récursive.



Le tableau suivant indique les étapes d'une requête et d'une réponse DNS avec des données DNSSEC facultatives.

Agrandir le tableau

Step	Query-response	Données DNSSEC facultatives
1	Un client DNS envoie une requête DNS vers un serveur DNS récursif.	Le client DNS peut indiquer qu'il prend en charge DNSSEC (`DO=1`).
2	Le serveur DNS récursif envoie une requête DNS vers les serveurs DNS de la racine et du domaine de premier niveau (TLD).	Le serveur DNS récursif peut indiquer qu'il prend en charge DNSSEC (`DO=1`).
3	Les serveurs racine et TLD renvoient une réponse DNS vers le serveur DNS récursif en fournissant l'adresse IP du serveur DNS faisant autorité pour la zone.	Les serveurs faisant autorité pour la zone parente peuvent indiquer que la zone enfant est signée à l'aide de DNSSEC et qu'elle comprend une délégation sécurisée (enregistrement DS).
4	Le serveur DNS récursif envoie une requête DNS vers le serveur DNS faisant autorité pour la zone.	Le serveur DNS récursif peut indiquer qu'il prend en charge DNSSEC (`DO=1`) et qu'il peut valider les enregistrements de ressources signés (`CD=1`) à envoyer dans la réponse.
5	Le serveur DNS faisant autorité renvoie une réponse DNS vers le serveur DNS récursif, en fournissant les données d'enregistrement de ressource.	Le serveur DNS faisant autorité peut inclure des signatures DNSSEC sous la forme d'enregistrements RRSIG dans la réponse DNS pour les utiliser dans la validation.
6	Le serveur DNS récursif renvoie une réponse DNS vers le client DNS, en fournissant les données d'enregistrement de ressource.	Le serveur DNS récursif peut indiquer si la réponse DNS a été validée (`AD=1`) en utilisant DNSSEC.

Inclusion de données DNSSEC

Des indicateurs (bits) liés à DNSSEC sont utilisés dans une requête et une réponse DNS pour déterminer si des données DNSSEC sont incluses, et si la validation a été effectuée. Ces indicateurs sont définis par l'activation ou la désactivation de bits de données étendus dans l'en-tête de paquet DNS. Lorsque ces indicateurs sont activés, on parle de « définition » du bit (la valeur est définie sur 1). L'action qui consiste à désactiver un indicateur est appelée « effacement » du bit (la valeur est définie sur 0).

- **DO** : Le bit DO est inclus dans une requête DNS et est une abréviation de « DNSSEC OK ». Si le bit DO est défini (`DO=1`), le client prend en charge DNSSEC, et le serveur DNS peut retourner des données DNSSEC dans une réponse sans aucun risque. Si le bit DO n'est pas défini (`DO=0`), le client ne prend pas en charge DNSSEC, et le serveur DNS ne doit pas inclure de données DNSSEC dans une réponse DNS. Les clients DNS peuvent toujours être protégés avec DNSSEC, même s'ils ne prennent pas en charge DNSSEC. Dans ce contexte, un client DNS est un ordinateur qui envoie une requête DNS. Quand un serveur DNS récursif envoie une requête au serveur DNS faisant autorité, il doit indiquer qu'il prend en charge DNSSEC afin que le serveur DNS faisant autorité envoie des données DNSSEC dans la réponse.
- **AD** : Le bit AD est inclus dans une réponse DNS et est une abréviation pour les « données authentifiées ». Si le bit AD est défini (`AD=1`), cela signifie que la réponse DNS est authentique, car elle a été validée avec DNSSEC. Un ordinateur prenant en charge DNSSEC sans validation, comme un ordinateur exécutant Windows 8, n'effectue pas de validation DNSSEC mais peut être configuré pour exiger des réponses DNS authentiques. Si le bit AD n'est pas défini (`AD=0`), cela signifie que la réponse DNS n'a pas été validée. Cela peut être dû au fait que la validation n'a pas été tentée ou qu'elle a échoué.
- **CD** : le bit CD est inclus dans une requête DNS et est une abréviation de « vérification désactivée ». Si le bit CD est défini (`CD=1`) dans une requête, cela signifie qu'une réponse DNS doit être envoyée, que la validation ait abouti ou non. Si le bit CD n'est pas défini (`CD=0`), aucune réponse DNS n'est envoyée si la validation était requise et a échoué. Si le bit est effacé (`CD=0`), cela signifie que la vérification est activée et que la validation DNSSEC peut se produire. Le bit CD peut être défini (`CD=1`) dans une requête car l'hôte est capable d'effectuer la validation DNSSEC et ne nécessite pas de validation en amont, comme un serveur DNS récursif exécutant Windows Server 2012 ou une version ultérieure. Un résolveur de stub non validant, tel qu'un ordinateur exécutant un client DNS Windows, émet des requêtes avec le bit de CD effacé `CD=0`. Pour plus d'informations, consultez RFC4035, section 3.2.2 .

Un quatrième indicateur important (bit) pouvant appartenir à un en-tête de paquet DNS est le bit AA. Cet indicateur n'est pas nouveau pour DNSSEC, mais il peut être utilisé lorsque DNSSEC est déployé :

- **AA** : Le bit AA est inclus dans une réponse DNS et est une abréviation de « réponse faisant autorité ». Si le bit AA est défini, cela signifie que la réponse DNS est authentifiée, car elle provient directement d'un serveur DNS faisant autorité. Un client qui exige une validation DNSSEC (`AD=1`) accepte le bit AA (AA=1, `AD=0`) si le client interroge directement un serveur faisant autorité, car les réponses faisant autorité n'ont pas besoin d'être validées. Il serait redondant pour un serveur faisant autorité de valider sa propre réponse.

Exemples de requêtes DNS

Les exemples suivants affichent les résultats de requête DNS exécutés à partir d'un ordinateur client DNS exécutant Windows 8.1 à l'aide de l'applet de commande **Resolve-DnsName** . L'applet de commande Resolve-DnsName a été introduite dans Windows Server 2012 et Windows 8 et peut être utilisée pour afficher des requêtes DNS qui incluent des données DNSSEC.

> **Important**
>
> N'utilisez pas l'outil en ligne de commande `nslookup.exe` pour tester la prise en charge de la technologie DNSSEC pour une zone. L'outil `nslookup.exe` utilise un client DNS interne qui ne prend pas en charge DNSSEC.

Exemple 1 : Dans l'exemple suivant, une requête est envoyée à un serveur DNS récursif pour un enregistrement d'adresse (A) dans la zone signée **secure.contoso.com** avec `DO=0`.

PowerShell

```
Resolve-DnsName finance.secure.contoso.com –type A -server dns1.contoso.com
```

Output

```
Name Type TTL Section IPAddress

---- ---- --- ------- ---------

finance.secure.contoso.com A 2848 Answer 192.168.0.200
```

Le bit DO n'est pas défini, car le paramètre **dnssecok** n'a pas été inclus.

Exemple 2 : Dans l'exemple suivant, l'indicateur `DO=1` est défini en ajoutant le paramètre **dnssecok** .

PowerShell

```
Resolve-DnsName -name finance.secure.contoso.com -type A -server dns1.contoso.com
-dnssecok
```

Output

```
Name Type TTL Section IPAddress

---- ---- --- ------- ---------

finance.secure.contoso.com A 2848 Answer 192.168.0.200

Name : finance.secure.contoso.com

QueryType : RRSIG

TTL : 2848

Section : Answer

TypeCovered : A

Algorithm : 8

LabelCount : 4

OriginalTtl : 3600

Expiration : 10/18/2013 8:23:41 PM

Signed : 10/8/2013 7:23:41 PM

Signer : secure.contoso.com

Signature : {86, 229, 217, 39...}

Name : .

QueryType : OPT

TTL : 32768

Section : Additional

Data : {}
```

Lorsque `DO=0`, le serveur DNS n'envoie pas de données DNSSEC dans la réponse DNS. Lorsque `DO=1`, le client indique qu'il peut recevoir des données DNSSEC le cas échéant. Comme la zone `secure.contoso.com` est signée, un enregistrement de ressource RRSIG a été inclus dans la réponse DNS lorsque `DO=1`.

Dans les exemples 1 et 2, la validation n'est pas exigée pour la zone `secure.contoso.com`, car la table de stratégie de résolution de noms (NRPT) n'est pas configurée pour exiger une validation.

Vous pouvez utiliser l'applet de commande **Get-DnsClientNrptPolicy** pour afficher les règles NRPT actuelles. Pour plus d'informations, consultez Get-DnsClientNrptPolicy.

Exemple 3 : Dans l'exemple suivant, une règle NRPT s'affiche pour `secure.contoso.com`.

PowerShell

```
Get-DnsClientNrptPolicy
```

Output

```
Namespace : .secure.contoso.com

QueryPolicy :

SecureNameQueryFallback :

DirectAccessIPsecCARestriction :

DirectAccessProxyName :

DirectAccessDnsServers :

DirectAccessEnabled :

DirectAccessProxyType : NoProxy

DirectAccessQueryIPsecEncryption :

DirectAccessQueryIPsecRequired : False

NameServers :

DnsSecIPsecCARestriction :

DnsSecQueryIPsecEncryption :

DnsSecQueryIPsecRequired : False

DnsSecValidationRequired : False
```

```
NameEncoding : Utf8WithoutMapping
```

Dans cet exemple, la valeur de **DnsSecValidationRequired** est **False**. Lorsque la valeur est false, la validation DNSSEC n'est pas exigée.

Exemple 4 : Avec la validation DNSSEC activée pour `secure.contoso.com`, le NRPT affiche **True** pour **DnsSecValidationRequired**. Cet exemple affiche uniquement l'espace `secure.contoso.com` de noms et le paramètre **DnsSecValidationRequired** .

PowerShell

```
(Get-DnsClientNrptPolicy -NameSpace secure.contoso.com).DnsSecValidationRequired
```

Output

```
True
```

Si la valeur de **DnsSecValidationRequired** est **True** , les ordinateurs clients prenant en charge DNSSEC envoient toujours des requêtes avec `DO=1`, même si le paramètre **dnssecok** n'est pas inclus.

Exemple 5 : Lorsque la validation DNSSEC est requise dans la table de stratégie de résolution de noms (NRPT), le bit DNSSEC OK est automatiquement défini (`DO=1`) pour les clients prenant en charge DNSSEC.

PowerShell

```
Resolve-DnsName -name finance.secure.contoso.com -type A -server dns1.contoso.com
```

Output

```
Name Type TTL Section IPAddress

---- ---- --- ------- ---------

finance.secure.contoso.com A 2848 Answer 192.168.0.200

Name : finance.secure.contoso.com

QueryType : RRSIG

TTL : 2848

Section : Answer
```

```
TypeCovered : A

Algorithm : 8

LabelCount : 4

OriginalTtl : 3600

Expiration : 10/18/2013 8:23:41 PM

Signed : 10/8/2013 7:23:41 PM

Signer : secure.contoso.com

Signature : {86, 229, 217, 39...}

Name : .

QueryType : OPT

TTL : 32768

Section : Additional

Data : {}
```

Dans cet exemple, un enregistrement RRSIG est envoyé dans la réponse DNS afin de répondre aux exigences de validation de `secure.contoso.com`. Une ancre d'approbation valide est également configurée sur le serveur DNS récursif `dns1.contoso.com`.

Si un client DNS ne prend pas en charge DNSSEC, la règle NRPT ne s'applique pas et les requêtes sont envoyées avec `DO=0`, même si une règle NRPT existante exige une validation DNSSEC.

Exemple 6 : Dans l'exemple suivant, la même requête est effectuée comme dans l'exemple 5, mais sans ancre de confiance valide configurée sur `dns1.contoso.com`.

PowerShell

```
Resolve-DnsName -name finance.secure.contoso.com -type A -server dns1.contoso.com
```

Output

```
Resolve-DnsName : finance.secure.contoso.com : Unsecured DNS packet

At line:1 char:1
```

```
+ Resolve-DnsName -name finance.secure.contoso.com -type A -server dns1.contoso.co
...

+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ CategoryInfo : ResourceUnavailable: (finance.secure.contoso.com:String)
[Resolve-DnsName], Win32Excepti

on

+ FullyQualifiedErrorId :
DNS\_ERROR\_UNSECURE\_PACKET,Microsoft.DnsClient.Commands.ResolveDnsName
```

Dans cet exemple, la résolution DNS échoue avec le message DNS_ERROR_UNSECURE_PACKET. La résolution échoue, car la validation exigée dans la table NRPT ne peut pas être effectuée en raison de l'absence d'une ancre d'approbation valide pour la zone `secure.contoso.com`. L'applet de commande **Resolve-DnsName** signale des résultats détaillés pour le type d'échec rencontré. Si le client DNS tente de résoudre `finance.secure.contoso.com` afin de se connecter à cet hôte, il échoue.

Scénarios DNSSEC

DNSSEC pouvant être déployé dans divers environnements avec des paramètres de client et serveur uniques, il est important de comprendre comment les requêtes et les réponses DNS sont affectées.

Examinez les quatre instructions suivantes liées à DNSSEC. Chaque instruction affecte le fonctionnement de la technologie DNSSEC dans un scénario donné :

- L'enregistrement de ressource `finance.secure.contoso.com` est correctement signé avec DNSSEC.
- Un serveur DNS récursif est capable de valider les réponses à une requête pour `finance.secure.contoso.com`.
- Un client DNS prend en charge la technologie DNSSEC.
- Un client DNS est configuré pour exiger une validation pour toutes les requêtes dans l'espace de noms `secure.contoso.com`.

Examinons de plus près chacune de ces quatre instructions.

1. **Statut de signature DNSSEC** : DNSSEC signe tous les enregistrements de la zone. Cette condition fait référence à l'état de la zone `secure.contoso.com`, et pas seulement à l'enregistrement de ressource `finance.secure.contoso.com`. Vous ne pouvez pas signer

certains enregistrements et ne pas en signer d'autres. Par conséquent, l'état DNSSEC de `finance.secure.contoso.com` dépend de l'état DNSSEC de `secure.contoso.com`.

- **Signé correctement** : la `secure.contoso.com` zone peut être signée de manière valide, ce qui permet `finance.secure.contoso.com` d'être validée comme authentique. Pour être valide, la zone doit être signée avec des clés valides n'ayant pas expirés et tous les enregistrements de ressource DNSSEC liées doivent être présents.

- **Non signé** : la `secure.contoso.com` zone peut ne pas être signée, auquel cas aucun enregistrement RRSIG n'est associé `finance.secure.contoso.com`, et les réponses DNS aux requêtes pour `finance.secure.contoso.com` lesquelles vous ne pouvez pas être validées. Si un client exige une validation, une requête DNS envoyée à un serveur DNS récursif échoue, car le client DNS n'accepte pas de réponse non validée. Si un client interroge directement un serveur faisant autorité, la validation n'échoue pas, car la réponse est déjà considérée comme authentique.

- **Signature incorrecte** : la zone `secure.contoso.com` est peut-être signée, mais pas de manière valide. Par exemple, une ou plusieurs clés de signature DNSSEC peuvent avoir expiré. Après la signature initiale d'une zone, celle-ci doit être resignée de façon régulière avec de nouvelles clés avant que la période de validité de la clé de signature n'arrive à expiration, ceci afin de maintenir un état DNSSEC opérationnel sécurisé. La période de validité des clés de signature DNSSEC doit être suffisamment courte pour maintenir la sécurité, mais suffisamment longue pour faciliter l'administration. Dans Windows Server 2012 et Windows Server 2012 R2, DNSSEC prend en charge la substitution de clé automatique, ce qui favorise la sécurité et facilite l'administration de vos zones signées par DNSSEC.

2. **État de validation** : un serveur DNS récursif avec une ancre d'approbation valide (clé de chiffrement publique) pour la `secure.contoso.com` zone est capable de valider une réponse DNS pour l'enregistrement de ressource `finance.secure.contoso.com` . Un serveur DNS récursif doit également prendre en charge les normes DNSSEC et les algorithmes utilisés pour signer la zone.

   - **Peut valider** : si le serveur DNS récursif prend en charge tous les algorithmes de chiffrement utilisés pour signer la `secure.contoso.com` zone et qu'il dispose d'une ancre d'approbation valide qu'il peut utiliser pour déchiffrer la signature DNSSEC associée à l'enregistrement de ressource signé, elle peut valider l'enregistrement `finance.secure.contoso.com` de ressource comme authentique.

   - **Impossible de valider** : un serveur DNS NE prenant pas en compte DNSSEC n'est pas capable de la validation. De la même façon, un serveur DNS qui ne dispose pas

d'une ancre de validation valide pour la zone `secure.contoso.com` n'a pas les moyens de valider une réponse DNS pour `finance.secure.contoso.com`. Les ancres d'approbation doivent être mises à jour lors d'une nouvelle signature de zone, par exemple, au cours de la substitution de clé d'approbation. DNSSEC dans Windows Server 2012 et Windows Server 2012 R2 prend en charge la mise à jour automatique des ancres d'approbation sur la substitution de clé par RFC 5011, « Mises à jour automatisées des ancres de confiance DNS (DNSSEC) ».

3. **État prenant en compte DNSSEC** : l'état de prise en compte DNSSEC d'un client DNS dépend du système d'exploitation qu'il exécute. Le service Client DNS Windows de Windows 7 ou de Windows Server 2008 R2 et les systèmes d'exploitation ultérieurs sont des résolveurs de stub sans validation qui prennent en charge DNSSEC. Les systèmes d'exploitation Windows précédents ne sont pas compatibles avec la technologie DNSSEC. Le client DNS informe un serveur DNS qu'il prend en charge ou non DNSSEC au moment d'envoyer une requête DNS.

   - **Le client et le serveur sont tous deux compatibles DNSSEC** : si le client et le serveur sont tous deux compatibles DNSSEC, la réponse DNS du serveur au client inclut l'indicateur de données authentifiées DNSSEC (AD). Si la réponse DNS est validée avec DNSSEC, `AD=1` est envoyé. Si la réponse DNS n'est pas validée, `AD=0` est envoyé.

   - **Le serveur DNS n'est pas compatible DNSSEC** : si le serveur DNS n'est pas compatible DNSSEC, aucune validation n'est effectuée et l'indicateur AD n'est pas défini (`AD=0`), que le client DNS soit compatible DNSSEC ou non.

   - **Le client DNS n'est pas compatible DNSSEC** : si le client DNS n'est pas compatible DNSSEC, le serveur DNS ne définit pas l'indicateur AD dans sa réponse au client, même s'il comprend DNSSEC. En revanche, si le serveur DNS prend en charge DNSSEC et dispose d'une ancre d'approbation pour la zone, il tente de valider la réponse du serveur faisant autorité. Si la validation échoue, il retourne une erreur de serveur DNS au client DNS. Si la validation réussit, il retourne les résultats de la requête au client. Ainsi, un serveur DNS récursif prenant en charge la technologie DNSSEC peut protéger des clients DNS qui ne la prennent pas en charge. Dans ce scénario, si la zone n'est pas signée, aucune validation n'est tentée et la réponse est retournée normalement au client.

4. **Condition de validation** : ce paramètre détermine l'exigence d'un client DNSSEC prenant en charge DNS POUR les données DNSSEC (l'indicateur AD) dans une réponse d'un serveur DNS. Pour que le client DNS requière une validation, il doit prendre en charge la technologie DNSSEC. Les clients DNS qui ne prennent pas en charge DNSSEC ne peuvent pas être contraints d'exiger une validation DNSSEC. Si le client DNS interroge directement

un serveur DNS faisant autorité, la réponse est validée, même si la zone n'est pas signée. Ceci est dû au fait que les serveurs DNS faisant autorité renvoient toujours les réponses authentifiées.

- **La validation est requise** : si la validation est requise, le client doit recevoir `AD=1` (validation réussie) ou il rejette la réponse DNS. Si la validation a échoué ou n'a pas été tentée (`AD=0`), la résolution DNS échoue. Cela est vrai, même si la zone n'est pas signée. Cela s'applique uniquement aux requêtes adressées à un serveur DNS récursif ne faisant pas autorité.

- **La validation n'est pas requise** : si la validation n'est pas requise, le client accepte une réponse provenant d'un serveur DNS récursif non compatible DNSSEC. En revanche, si le serveur DNS récursif prend en charge DNSSEC et que la validation échoue, il retourne un basculement de serveur au client, même si le client n'exige pas de validation.

Étapes suivantes

Voici quelques articles pour en savoir plus sur DNSSEC pour serveur DNS.

- DNSSEC dans Windows Server
- DNSSEC dans le client DNS Windows
- Signature d'une zone DNS
- Types d'ancres de confiance
- Présentation de la table de stratégie de résolution de noms (NRPT)

Master de clé DNSSEC

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Dans cet article, vous allez découvrir ce que le maître de clé est, son rôle dans les déploiements DNS Security Extensions (DNSSEC) et comment le gérer efficacement.

Qu'est-ce qu'un maître de clé DNSSEC ?

Le maître de clés génère et gère les clés de chiffrement pour les zones signées DNSSEC, ce qui garantit l'intégrité et la sécurité de votre infrastructure DNS. Le rôle est essentiel pour maintenir la sécurité des zones DNS, en particulier dans les environnements nécessitant des niveaux élevés de confiance et de sécurité.

Le maître de clé est :

- Serveur DNS principal faisant autorité responsable de la génération et de la gestion des clés pour les zones signées DNSSEC.
- Sélectionné automatiquement comme maître de clé lors de l'utilisation des paramètres de signature de zone par défaut, sauf indication contraire.
- Transférable à un autre serveur DNS qui prend en charge la signature DNSSEC en ligne, ce qui permet une flexibilité dans la gestion des clés.
- Exclusif à un seul serveur DNS par zone, ce qui signifie qu'un seul serveur DNS peut servir de maître de clé pour une zone DNS spécifique à tout moment donné.

Ce composant est essentiel pour maintenir les opérations DNS sécurisées dans les environnements nécessitant des niveaux élevés de confiance et de sécurité.

Spécifications

Le maître de clé doit répondre à des exigences spécifiques pour fonctionner correctement.

Pour tous les types de zones, le maître de clé doit être un serveur principal faisant autorité pour la zone qui est également capable de signer des zones en ligne.

Les zones intégrées Active Directory et les zones sauvegardées par des fichiers ont certaines exceptions. Ces exceptions sont décrites dans les sections suivantes.

Zones intégrées Active Directory

Dans une zone intégrée Active Directory où il existe plusieurs serveurs DNS principaux faisant autorité, les exceptions suivantes sont possibles :

- Vous pouvez transférer le rôle Principal de clé vers un autre serveur de noms faisant autorité après avoir signé une zone DNS.
- Vous pouvez transférer le rôle Principal de clé si le maître de clé actuel est en ligne. Si le maître de clé actuel est hors connexion, vous pouvez également transférer le rôle dans le cadre d'un processus de récupération d'urgence.
- Un serveur faisant autorité peut être le maître de clé pour plusieurs zones.
- Différents serveurs faisant autorité peuvent être le maître de clé pour différentes zones.

Zones sauvegardées par fichier

Vous ne pouvez pas transférer le rôle principal de clé si une zone est sauvegardée par un fichier, car ces zones n'ont qu'un seul serveur DNS principal faisant autorité.

Considérations relatives à la sécurité

Les exigences de sécurité de votre clé principale dépendent de votre type de zone :

- **Zones intégrées à Active Directory** : le contrôleur de domaine est un contrôleur de domaine et bénéficie des mêmes considérations de sécurité améliorées que celles que vous utilisez pour les contrôleurs de domaine.

- **Zones sauvegardées par fichier** : le contrôleur de clé n'est peut-être pas un contrôleur de domaine. Dans ce scénario, prenez des précautions de sécurité supplémentaires pour protéger le maître de clé contre les attaques et protéger les matériaux de clé privée contre la compromission. Pour des raisons de sécurité, une clé principale qui n'est pas un contrôleur de domaine ne doit avoir que le rôle serveur DNS installé pour limiter sa surface d'attaque.

Signature de zone

Lorsque vous signez une zone avec DNSSEC, le maître de clés joue un rôle central dans le processus en générant et en gérant les clés de signature de chiffrement requises pour la signature de zone. La signature de zone ajoute des enregistrements de ressources spécifiques à DNSSEC à votre zone DNS qui fournissent une preuve de chiffrement de l'intégrité des données.

Le maître de clé gère le processus de signature différemment en fonction de votre type de zone :

- **Zones intégrées à Active Directory** : les clés de signature privées sont automatiquement répliquées sur tous les serveurs DNS principaux via la réplication Active Directory. Chaque maître de clé signe sa propre copie de la zone en mémoire pour des performances optimales.
- **Zones sauvegardées par fichier** : la zone signée est validée sur le disque sur le serveur DNS principal unique servant de maître de clé. Les clés de signature sont stockées dans le magasin de certificats local ou dans un module de sécurité matériel (HSM) s'ils sont configurés.

Pour obtenir des instructions détaillées sur la façon de signer des zones DNS avec DNSSEC, consultez DnsSec Sign DNS Zones.

Clés de signature

Le maître de clé génère toutes les clés pour la zone DNS et est responsable de la distribution des clés privées et des informations de signature de zone. Le maître de clé est également chargé d'effectuer toutes les substitutions de clé de signature de zone (ZSK) et de clé de signature de clé (KSK) et d'interroger les zones enfants afin de conserver les délégations signées up-to-date.

Zones non signées

Vous pouvez également affecter un maître de clé à une zone non signée. Toutes les zones ont un paramètre Key Master, qu'ils soient actuellement signés ou non. Une zone qui n'est pas signée n'a pas non plus de clé principale. Vous pouvez attribuer un maître de clé à l'avance à l'aide de PowerShell pour préparer la signature de zone.

Stockage de clés privées

Pour effectuer son rôle, le maître de clé doit avoir accès à une clé privée pour une zone signée DNSSEC. La clé privée peut être stockée de plusieurs façons :

- **Active Directory** : si le contrôleur de clé est un contrôleur de domaine, il peut stocker du matériel de clé privée dans Active Directory. L'utilisation d'Active Directory est l'option la plus sécurisée et permet une réplication et un accès faciles par d'autres serveurs DNS dans le domaine.

  Meilleur pour : Environnements dans lesquels DNS est intégré à Active Directory, car il fournit une sécurité forte et un accès facile aux clés privées.

- **Magasin de certificats** : si le contrôleur de clé n'est pas un contrôleur de domaine, il peut stocker du matériel de clé privée dans le magasin de certificats local. L'utilisation d'un magasin de certificats nécessite une gestion minutieuse pour garantir que les clés privées sont sécurisées et accessibles.

  Meilleur pour : Groupes de travail et environnements autonomes dans lesquels vous devez gérer des clés privées localement.

- **Module de sécurité matériel (HSM)** : pour les environnements à haute sécurité, les clés privées peuvent être stockées dans un HSM. Les modules HSM offrent une protection forte contre la compromission des clés, mais nécessitent une configuration et une gestion supplémentaires.

  Meilleur pour : Environnements haute sécurité où vous avez besoin d'une protection forte contre l'exfiltration et la compromission de clé.

Pour en savoir plus sur la création de clés de signature, consultez zones DNSSEC sign DNS.

Contenu connexe

- Vue d'ensemble de DNSSEC

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Chiffrement DNS à l'aide de DNS via HTTPS

S'applique à: ✅ Windows Server 2025, ✅ Windows 11

Le DNS traditionnel utilise des messages UDP ou TCP non chiffrés sur le port 53, qui expose le trafic DNS à la surveillance passive, à l'analyse du trafic et à la manipulation active par des attaquants. Le chiffrement DNS protège le trafic de requête et de réponse DNS d'être observé, modifié ou falsifié lors du transit sur un réseau.

DNS sur HTTPS (DoH) est un mécanisme basé sur des normes qui chiffre le trafic DNS en encapsulant des messages DNS dans HTTPS, fournissant la confidentialité et l'intégrité à l'aide du protocole TLS (Transport Layer Security). En chiffrant le trafic DNS, DoH permet d'empêcher l'écoute, les attaques man-in-the-middle et l'inspection non autorisée des requêtes et réponses DNS.

Fonctionnement du DNS via HTTPS

DNS sur HTTPS ne modifie pas le modèle de requête et de réponse DNS fondamental. Au lieu de cela, il modifie la façon dont les messages DNS sont transportés sur le réseau. Lorsque vous activez DoH sur un serveur DNS, DoH devient une option de communication chiffrée supplémentaire et le serveur DNS continue de répondre aux requêtes DNS traditionnelles, sauf si vous désactivez explicitement cette fonctionnalité.

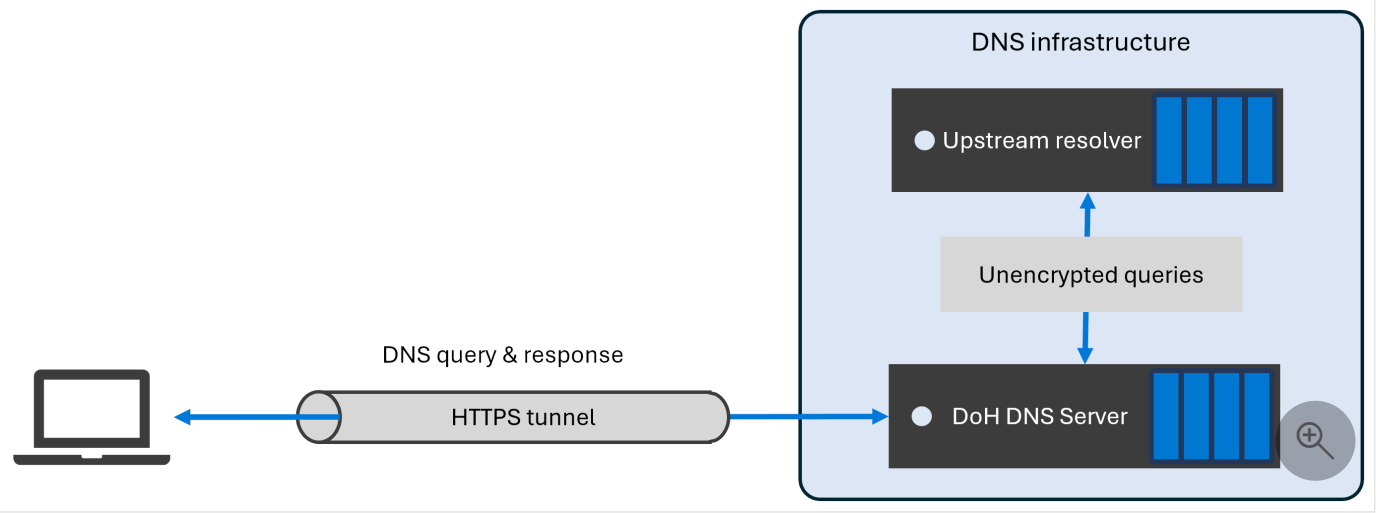
Lorsque vous activez DoH :

- Le serveur DNS écoute le trafic HTTPS.
- Vous configurez un client compatible DoH (par exemple, un client Windows 11) pour utiliser des requêtes chiffrées sur un serveur DNS.
- Le client DoH établit une connexion TLS au serveur DNS.
- Le client envoie des requêtes DNS à l'intérieur d'une requête HTTPS.
- Le serveur DNS traite la requête comme d'habitude.
- La réponse DNS est retournée à l'intérieur de la réponse HTTPS.

DNS sur HTTPS pour le serveur DNS

À compter de la mise à jour de sécurité 2026-06 (KB5094125) pour Windows Server 2025, vous pouvez activer DNS via HTTPS (DoH) sur le service serveur DNS pour chiffrer le trafic DNS entre les clients compatibles DoH et votre serveur DNS.

Un exemple de flux de communication DoH est illustré dans le diagramme suivant.



Lorsque vous configurez DNS sur HTTPS pour le serveur DNS, tenez compte des points suivants :

- La communication DNS en amont (redirecteurs, redirecteurs conditionnels, serveurs faisant autorité) reste non chiffrée.
- Les transferts de zone DNS restent non chiffrés.
- Les mises à jour dynamiques DNS restent non chiffrées par défaut.
- Vous ne pouvez pas créer un filtre de requête DNS qui correspond uniquement aux requêtes DoH.
- Les stratégies avec un filtre de requête de protocole de transport ne correspondent pas aux requêtes DoH. Par exemple, une stratégie avec le filtre de protocole de transport défini sur `EQ, TCP` ne correspond pas à DoH.

Avantages de sécurité du DNS via HTTPS

DNS sur HTTPS offre les avantages suivants en matière de sécurité et de confidentialité :

- **Confidentialité**. Les requêtes et réponses DNS sont chiffrées, ce qui empêche la surveillance passive.
- **Intégrité**. TLS protège les messages DNS contre la modification pendant le transit.

- **Authentication**. Les clients DNS peuvent valider l'identité du serveur DNS à l'aide de la validation de certificat HTTPS standard.
- **Résistance à l'analyse du trafic**. Le trafic DNS se mélange avec d'autres trafics HTTPS, ce qui réduit l'exposition au filtrage ou à la manipulation spécifiques au DNS. Cette approche améliore la confidentialité et la résistance à l'interception.

"Protocoles et normes de DNS sur HTTPS"

L'IETF définit DNS sur HTTPS dans RFC 8484 – Requêtes DNS sur HTTPS (DoH).

RFC 8484 spécifie comment envoyer et recevoir des messages DNS à l'aide de HTTP via TLS. La norme DoH prend en charge les méthodes GET et POST et définit des types de supports pour les messages DNS. Cette approche permet au trafic DNS de tirer parti des fonctionnalités HTTPS modernes telles que le chiffrement, l'authentification et la réutilisation des connexions.

En outre, la norme DoH permet aux implémentations de serveur de configurer l'URI et le port d'écoute du serveur, ce qui permet un déploiement flexible dans différents environnements réseau.

Chiffrement DNS et DNSSEC

Le chiffrement DNS, tel que DoH et DNSSEC, traitent différents modèles de menace et sont des technologies complémentaires. Le chiffrement DNS protège le trafic DNS sur le câble, tandis que DNSSEC garantit que les données DNS sont vérifiées par chiffrement pour l'intégrité et proviennent d'une source faisant autorité.

En utilisant DoH avec DNSSEC, vous bénéficiez d'une défense approfondie en combinant un transport chiffré avec des données DNS authentifiées. Pour plus d'informations sur DNSSEC, consultez Qu'est-ce que DNSSEC ?

Étapes suivantes

Activer DNS sur HTTPS sur Windows DNS Server

ⓘ**Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Last updated on 12/06/2026

Gérer les zones DNS à l'aide du serveur DNS dans Windows Server

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Créez des zones DNS primaires, secondaires, stub et inversées à l'aide du rôle serveur DNS dans Windows Server. Cet article vous montre également comment configurer les paramètres de transfert de zone et effectuer la délégation de zone.

Prerequisites

Avant de pouvoir gérer la zone DNS dans Windows Server, vous devez remplir les conditions préalables suivantes :

- Un serveur Windows avec le rôle serveur DNS installé et configuré. Consultez démarrage rapide : Installation et configuration du serveur DNS pour savoir comment commencer.
- Déterminez le type de zone que vous souhaitez créer, consultez les zones DNS pour en savoir plus.
- Un compte membre du groupe Administrateurs ou équivalent.
- Vous avez besoin du nom de domaine complet (FQDN) de la zone que vous souhaitez créer.
- Si vous souhaitez créer une zone secondaire ou stub, vous avez besoin de l'adresse IP du ou des serveurs DNS hébergeant la zone primaire.

Vous pouvez gérer à distance un serveur DNS Windows Server à l'aide de toutes les méthodes décrites dans cet article.

Créer une zone primaire

Créer une zone primaire intégrée Active Directory

Pour créer une zone primaire intégrée Active Directory, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer une zone DNS intégrée Active Directory à l'aide de la commande PowerShell Add-DnsServerPrimaryZone .

Créez une zone primaire pour `north.contoso.com` et définissez l'étendue de réplication, exécutez la commande suivante :

PowerShell

```
Add-DnsServerPrimaryZone -Name "north.contoso.com" -ReplicationScope "Forest"
-PassThru
```

Créer une zone primaire basée sur un fichier

Pour créer une zone primaire basée sur un fichier, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer une zone DNS basée sur un fichier à l'aide de la commande PowerShell Add-DnsServerPrimaryZone .

Pour ajouter la zone DNS basée sur un fichier `east.contoso.com` à l'aide du fichier `east.contoso.com.dns`, exécutez la commande suivante sur un ordinateur avec le rôle serveur DNS installé :

PowerShell

```
Add-DnsServerPrimaryZone -Name "east.contoso.com" -ZoneFile
"east.contoso.com.dns"
```

Créer une zone secondaire

Pour créer une zone secondaire, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer une zone DNS secondaire à l'aide de la commande PowerShell Add-DnsServerSecondaryZone .

Ajoutez la zone secondaire western.contoso.com à l'aide du nom de fichier de zone `south.contoso.dns` et à l'aide du serveur de zone principal à l'adresse IP `172.23.90.124` utilisez la commande suivante :

PowerShell

```
Add-DnsServerSecondaryZone -Name "south.contoso.com" -ZoneFile
"south.contoso.com.dns" -MasterServers 172.23.90.124
```

Créer une zone de stub

Pour créer une zone stub, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer une zone DNS secondaire à l'aide de la commande PowerShell Add-DnsServerStubZone .

Pour ajouter une zone stub pour la zone `west.contoso.com` à l'aide du serveur DNS faisant autorité `172.23.90.124`, exécutez la commande suivante :

PowerShell

```
Add-DnsServerStubZone -Name "west.contoso.com" -MasterServers "172.23.90.124"
-PassThru -ZoneFile "west.contoso.com.dns"
```

Créer une zone de recherche inversée

Pour créer une zone de recherche inversée, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer une zone DNS inversée Active Directory intégrée à l'aide de la commande PowerShell Add-DnsServerPrimaryZone .

Pour ajouter la zone de recherche inverse pour la plage d'adresses IPv4 `10.1.0.0/24` et définir l'étendue de réplication, exécutez la commande suivante.

PowerShell

```
Add-DnsServerPrimaryZone -NetworkID "10.1.0.0/24" -ReplicationScope "Forest"
```

Configurer les paramètres de transfert de zone

Pour configurer les paramètres de transfert de zone pour une zone DNS principale, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment définir les paramètres de transfert de zone pour une zone DNS existante à l'aide de la commande PowerShell Set-DnsServerPrimaryZone .

Pour configurer les transferts de zone pour qu'ils soient autorisés uniquement aux serveurs dans les enregistrements de serveurs de noms (NS) pour `west.contoso.com` zone DNS, exécutez la commande suivante.

PowerShell

```
Set-DnsServerPrimaryZone -name "west.contoso.com" -SecureSecondaries
"TransferToZoneNameServer" -PassThru
```

Effectuer la délégation de zone

Pour effectuer la délégation de zone pour un sous-domaine, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment déléguer le `south.west.contoso.com` sous-domaine à l'aide de la commande PowerShell Add-DnsServerZoneDelegation .

Pour déléguer le sous-domaine `south` au serveur de noms `west-ns01.contoso.com` à l'aide d'une adresse IP de `172.23.90.136`, exécutez la commande suivante.

PowerShell

```
Add-DnsServerZoneDelegation -Name "west.contoso.com" -ChildZoneName "south" -
NameServer "west-ns01.contoso.com" -IPAddress 172.23.90.136 -PassThru -Verbose
```

Étapes suivantes

Maintenant que vous avez créé une zone DNS, configuré des paramètres de transfert de zone et effectué la délégation de zone, voici d'autres articles à prendre en compte.

- Vue d’ensemble des stratégies DNS
- Référence DNS PowerShell
- Vue d'ensemble Anycast DNS

Gérer les enregistrements de ressources DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Créez, modifiez et supprimez des enregistrements de ressources DNS à l'aide du rôle serveur DNS dans Windows Server. Vous pouvez ajouter des enregistrements de ressources à l'aide du gestionnaire DNS, de Windows PowerShell ou automatiquement lorsque des clients Windows utilisant le protocole DHCP (Dynamic Host Configuration Protocol) rejoignent un réseau à l'aide d'une mise à jour dynamique.

Les enregistrements de ressources contiennent les informations qu'une zone conserve sur les ressources (telles que les hôtes). Les informations d'enregistrement de ressource incluent le type d'enregistrement, le nom du propriétaire, l'adresse de l'hôte et d'autres informations.

Prerequisites

Avant de pouvoir gérer les enregistrements de ressources DNS dans Windows Server, vous devez disposer des prérequis suivants :

- Un serveur Windows avec le rôle serveur DNS installé et configuré. Consultez Démarrage rapide : installation et configuration d'un serveur DNS pour de plus amples informations sur la façon de commencer.
- Déterminez le type d'enregistrement que vous souhaitez créer. Consultez Enregistrements de ressources DNS.
- Un compte membre du groupe Administrateurs ou équivalent.
- Vous avez besoin du nom de domaine complet (FQDN) et de l'adresse IP de l'enregistrement de ressource que vous souhaitez créer.

Créez des enregistrements de ressources

Vous pouvez ajouter des enregistrements de ressources à une zone existante à l'aide du module PowerShell DnsServer . Certains types d'enregistrements de ressources courants ont d'autres commandes PowerShell dans lesquelles vous n'avez pas besoin de spécifier le type d'enregistrement de ressource. Vous pouvez également ajouter les types d'enregistrements de ressources suivants à l'aide de la console du Gestionnaire DNS.

Les sections suivantes contiennent des étapes pour créer les types d'enregistrements de ressources suivants :

- Hôte (A ou AAAA)
- Alias (CNAME)
- Serveur de messagerie (MX)
- Pointeur (PTR)
- Localisateur de service (SRV)
- Texte (TXT)

Créez un enregistrement hôte

Pour créer un enregistrement hôte IPv4 (A), sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer un hôte IPv4 (A) à l'aide de la commande PowerShell Add-DnsServerResourceRecord .

Pour créer un enregistrement de ressource hôte pour `Host34` mappé à l'adresse IP `10.17.1.34` de la zone `contoso.com`, exécutez la commande suivante.

PowerShell

```
Add-DnsServerResourceRecordA -Name "Host34" -ZoneName "Contoso.com" -
IPv4Address "10.17.1.34" -TimeToLive 01:00:00
```

Vous pouvez également ajouter un enregistrement hôte IPv4 (A) à l'aide de la commande Add-DnsServerResourceRecord.

Enregistrement de ressource AAAA

Pour créer un enregistrement d'hôte IPv6 (AAAA), sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer un hôte IPv6 (AAAA) à l'aide de la commande PowerShell Add-DnsServerResourceRecordAAAA .

Pour ajouter l'enregistrement de ressource AAAA `Host36` à mapper à l'adresse IPv6 `3ffe::1`, utilisez la commande :

PowerShell

```
Add-DnsServerResourceRecordAAAA -Name "Host36" -ZoneName "contoso.com" -
IPv6Address "3ffe::1" -TimeToLive 01:00:00
```

Vous pouvez également ajouter un enregistrement d'hôte IPv6 (AAAA) à l'aide de Add-DnsServerResourceRecord.

Enregistrements CNAME

Pour créer un enregistrement d'alias (CNAME), sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer un enregistrement de ressource CNAME à l'aide de la commande PowerShell Add-DnsServerResourceRecordCName .

Pour que le CNAME `labhost34` soit créé dans la `contoso.com` zone et pointe vers l'enregistrement DNS `Host34.lab.contoso.com` existant, utilisez la commande PowerShell suivante :

PowerShell

```
Add-DnsServerResourceRecordCName -Name "labhost34" -HostNameAlias
"Host34.lab.contoso.com" -ZoneName "contoso.com" -TimeToLive 01:00:00
```

Enregistrements MX

Pour créer un enregistrement MX, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer un enregistrement de ressource MX à l'aide de la commande PowerShell Add-DnsServerResourceRecordMX .

Pour ajouter un enregistrement MX pour l'hôte `mail.contoso.com` avec une préférence définie sur `10` pour la zone `contoso.com`, utilisez la commande PowerShell suivante :

PowerShell

```
Add-DnsServerResourceRecordMX -Preference 10 -Name "." -TimeToLive 01:00:00 -
MailExchange "mail.contoso.com" -ZoneName "contoso.com"
```

Enregistrements PTR

Pour créer un enregistrement PTR, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer un enregistrement de ressource PTR à l'aide de la commande PowerShell Add-DnsServerResourceRecordPtr .

Pour ajouter un enregistrement de pointeur nommé `host77.contoso.com` pour l'adresse IP `192.168.0.77` dans la zone de recherche inverse `0.168.192.in-addr.arpa`, utilisez la commande PowerShell suivante :

PowerShell

```
Add-DnsServerResourceRecord -Name "77" -Ptr -ZoneName "0.168.192.in-addr.arpa"
-AllowUpdateAny -PtrDomainName "host77.contoso.com"
```

Enregistrements SRV

Pour créer un enregistrement SRV, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer un enregistrement de ressource SRV à l'aide de la commande PowerShell Add-DnsServerResourceRecord .

Pour ajouter un enregistrement de ressource de localisateur de service (SRV) pour le service `_sip` sur le port `5060` avec un poids et une priorité de `0` pour le domaine `contoso.com` pointant vers `sipserver1.contoso.com`, utilisez la commande PowerShell suivante :

PowerShell

```
Add-DnsServerResourceRecord -Srv -Name "sip" -ZoneName "contoso.com" -
DomainName "sipserver1.contoso.com" -Priority 0 -Weight 0 -Port 5060
```

Enregistrements TXT

Pour créer un enregistrement TXT, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment créer un enregistrement de ressource TXT à l'aide de la commande PowerShell Add-DnsServerResourceRecord .

Pour créer un enregistrement TXT nommé exemple avec la valeur de texte `Example DNS record text` dans la zone `contoso.com`, utilisez la commande PowerShell suivante :

PowerShell

```
$recordtext = "Example DNS record text"
Add-DnsServerResourceRecord -DescriptiveText $recordtext -Name example -
zonename contoso.com
```

Mettez à jour les enregistrements de ressources

Pour mettre à jour un enregistrement de ressource, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment modifier la durée de vie (TTL) d'un enregistrement de ressource DNS à l'aide des commandes PowerShell Get-DnsServerResourceRecord et Set-DnsServerResourceRecord .

L'exemple suivant met à jour l'enregistrement de ressource `host01.contoso.com` afin que la durée de vie soit désormais de 2 heures. Dans cet exemple, vous utilisez le paramètre **OldInputObject** pour spécifier un objet d'enregistrement de ressource que vous souhaitez modifier et le paramètre **NewInputObject** pour spécifier les valeurs mises à jour.

Pour mettre à jour l'enregistrement de ressource `host01.contoso.com` afin que la durée de vie soit désormais de 2 heures, exécutez les commandes PowerShell suivantes :

PowerShell

```
$OldObj = Get-DnsServerResourceRecord -Name "host01" -ZoneName "contoso.com" -
RRType "A"
$NewObj = [ciminstance]::new($OldObj)
$NewObj.TimeToLive = [System.TimeSpan]::FromHours(2)
```

```
Set-DnsServerResourceRecord -NewInputObject $NewObj -OldInputObject $OldObj -
ZoneName "contoso.com" -PassThru
```

La commande PowerShell Set-DnsServerResourceRecord ne peut pas modifier le **nom** ou le **type** d'un objet d'enregistrement de ressource de serveur DNS. Si vous souhaitez effectuer ces actions, supprimez l'enregistrement de ressource existant et créez-en un.

Supprimez les enregistrements de ressources

Pour supprimer un enregistrement de ressource, sélectionnez la méthode appropriée et suivez les étapes.

PowerShell

Voici comment supprimer un enregistrement de ressource DNS à l'aide de la commande PowerShell Remove-DnsServerResourceRecord .

Pour supprimer l'enregistrement DNS `example.contoso.com`, exécutez la commande suivante :

PowerShell

```
Remove-DnsServerResourceRecord -name "Example" -Zonename "contoso.com" -RRType
A
```

Configurer le vieillissement et le nettoyage DNS

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Le vieillissement et la récupération suppriment les archives de ressources obsolètes qui s'accumulent dans les zones au fil du temps. Sans eux, des enregistrements obsolètes s'accumulent, ce qui gaspille du stockage, ralentit les transferts de zones et fait que les clients reçoivent des réponses de résolution de noms obsolètes.

Dans cet article, vous activez le vieillissement sur vos zones, activez le nettoyage sur le serveur DNS, protégez les enregistrements critiques contre la suppression et vérifiez que le nettoyage s'exécute. Vous configurez tout en utilisant soit DNS Manager, soit le module PowerShell DnsServer.

Pour plus d'informations sur la façon dont le vieillissement et la récupération déterminent quand un enregistrement est obsolète, voir Le vieillissement et la récupération DNS. Cet article se concentre sur la configuration et les tâches opérationnelles.

Prerequisites

Avant que le vieillissement et le nettoyage puissent fonctionner, assurez-vous que les conditions préalables suivantes sont en place :

- Un serveur fonctionnant sous Windows Server avec le rôle DNS Server installé. Vous configurez ce serveur.
- Autorisations administratives pour gérer le serveur DNS : appartenance au groupe DnsAdmins ou au groupe local des Administrateurs sur le serveur DNS. Pour une zone intégrée à Active Directory, utilisez un compte membre du groupe Domain Admins.
- Les outils de gestion DNS pour la méthode que vous utilisez : DNS Manager, qui s'installe avec le rôle DNS Server ou via Remote Server Administration Tools (RSAT), et le module PowerShell DnsServer. Cet article documente ces deux méthodes.
- Recherche au niveau serveur activée sur chaque serveur DNS où vous le souhaitez. Ce réglage ne se reproduit pas, donc configurez-le individuellement sur chaque serveur qui doit récupérer.

- Vieillissement au niveau des zones activé sur vos zones. Pour une zone intégrée AD, activez le vieillissement une fois et le paramètre se réplique avec les données de la zone vers d'autres serveurs DNS qui hébergent la zone. Pour une zone non intégrée à AD, activez le vieillissement dans chaque zone individuellement. Pour une zone primaire standard, configurez le vieillissement sur le serveur DNS principal.
- Des enregistrements DNS avec un horodatage non nul. Les enregistrements ajoutés reçoivent automatiquement un horodatage. Les enregistrements ajoutés manuellement, depuis la console DNS ou un fichier de zone textuel, reçoivent un horodatage de zéro, ce qui les exclut de la récupération tant que vous n'attribuez pas un horodatage non nul.
- Un type de zone supportée. Le vieillissement et le nettoyage ne s'appliquent qu'aux zones primaires standard et aux zones intégrées à AD. Les zones secondaires et les zones de stub ne prennent pas en charge ces processus.

> ⚠ **Avertissement**
>
> Le vieillissement et la récupération sont désactivés par défaut. Activez-les uniquement lorsque vous comprenez chaque intervalle que vous avez défini. Une mauvaise configuration peut supprimer des enregistrements légitimes, ce qui empêche les utilisateurs de résoudre ces noms. Testez votre configuration en laboratoire et sauvegardez vos données de zone avant d'activer le nettoyage en production.

Configurez le vieillissement et le nettoyage

Configurez le vieillissement et le nettoyage à l'aide du Gestionnaire DNS ou du module PowerShell DnsServer. Choisissez la méthode qui correspond à votre façon de travailler.

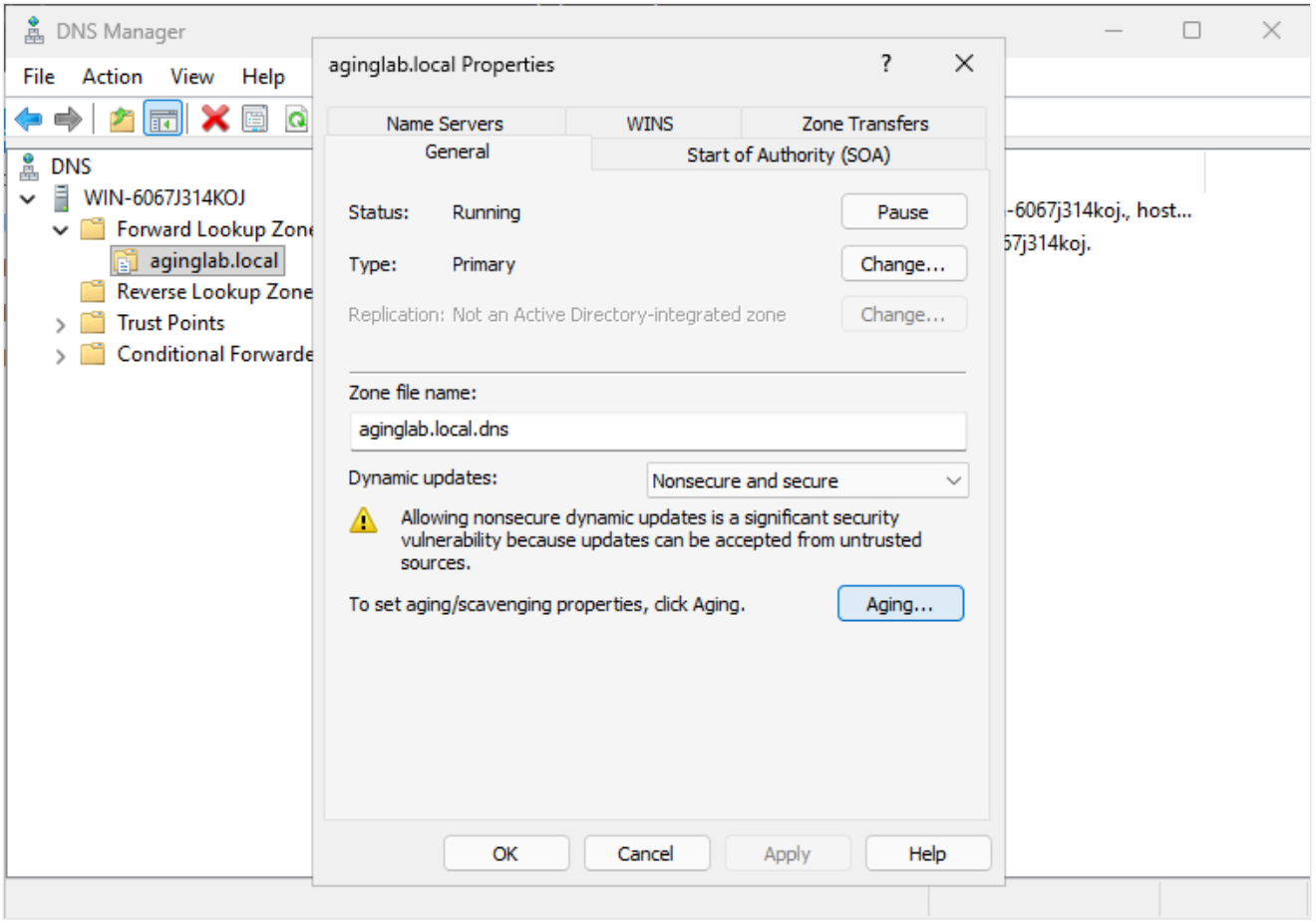
Gestionnaire DNS

Utilisez DNS Manager (`dnsmgmt.msc`) lorsque vous préférez une interface graphique. Les sections suivantes permettent d'activer le vieillissement sur une zone, d'appliquer des paramètres à toutes les zones, d'activer le nettoyage automatique sur le serveur et de protéger un enregistrement.

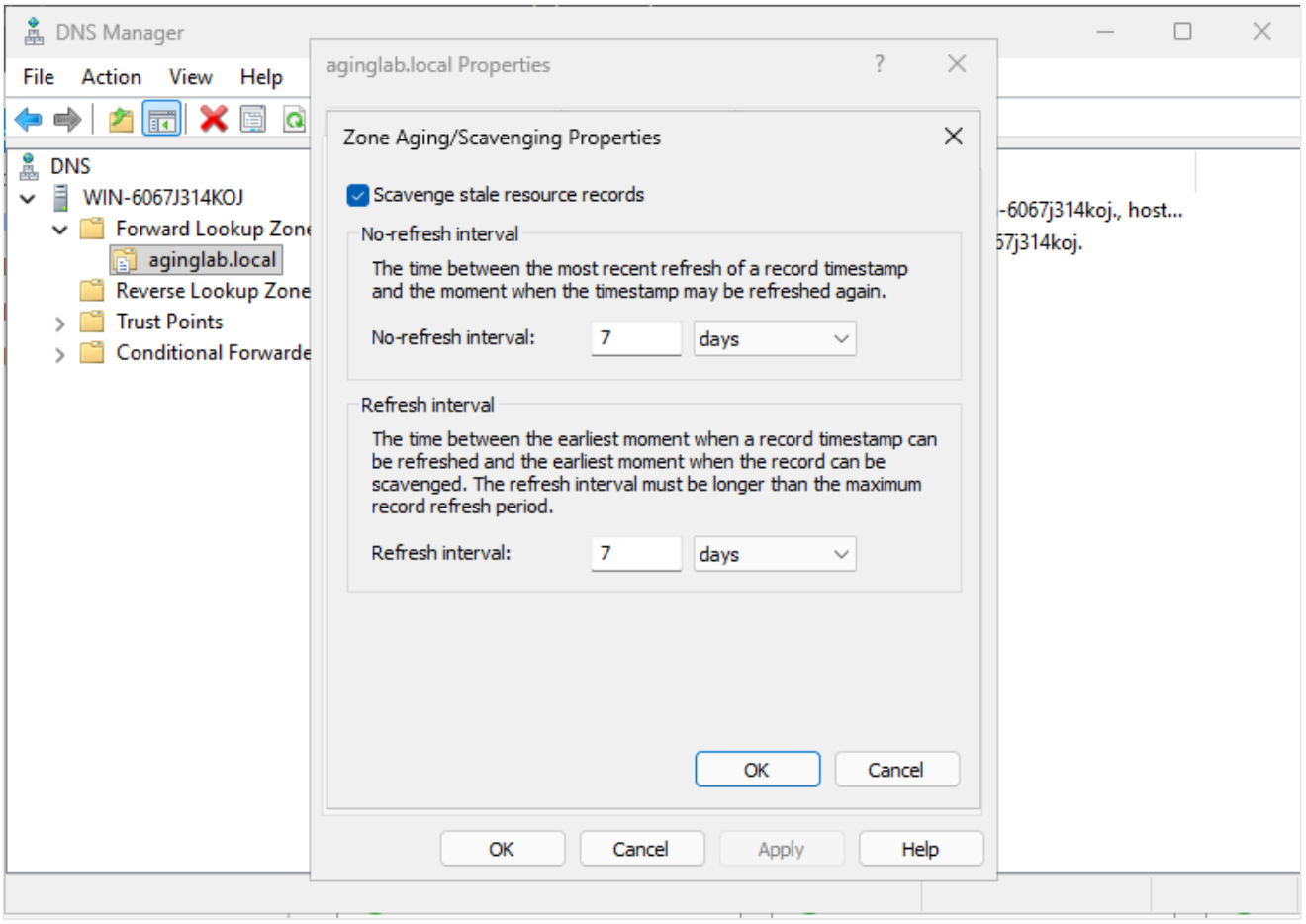
Activez le vieillissement sur une zone

1. Ouvrir le gestionnaire DNS (`dnsmgmt.msc`).
2. Sélectionnez et maintenez (ou faites un clic droit) sur la zone, sélectionnez **Propriétés**, puis **sélectionnez Vieillissement**.

3. **Sélectionnez Récupérer les archives de ressources obsolètes**.
4. Réglez **l'intervalle sans rafraîchissement** et **l'intervalle de rafraîchissement**. Le fait par défaut de sept jours par intervalle convient à la plupart des environnements.
5. Sélectionnez **OK**.



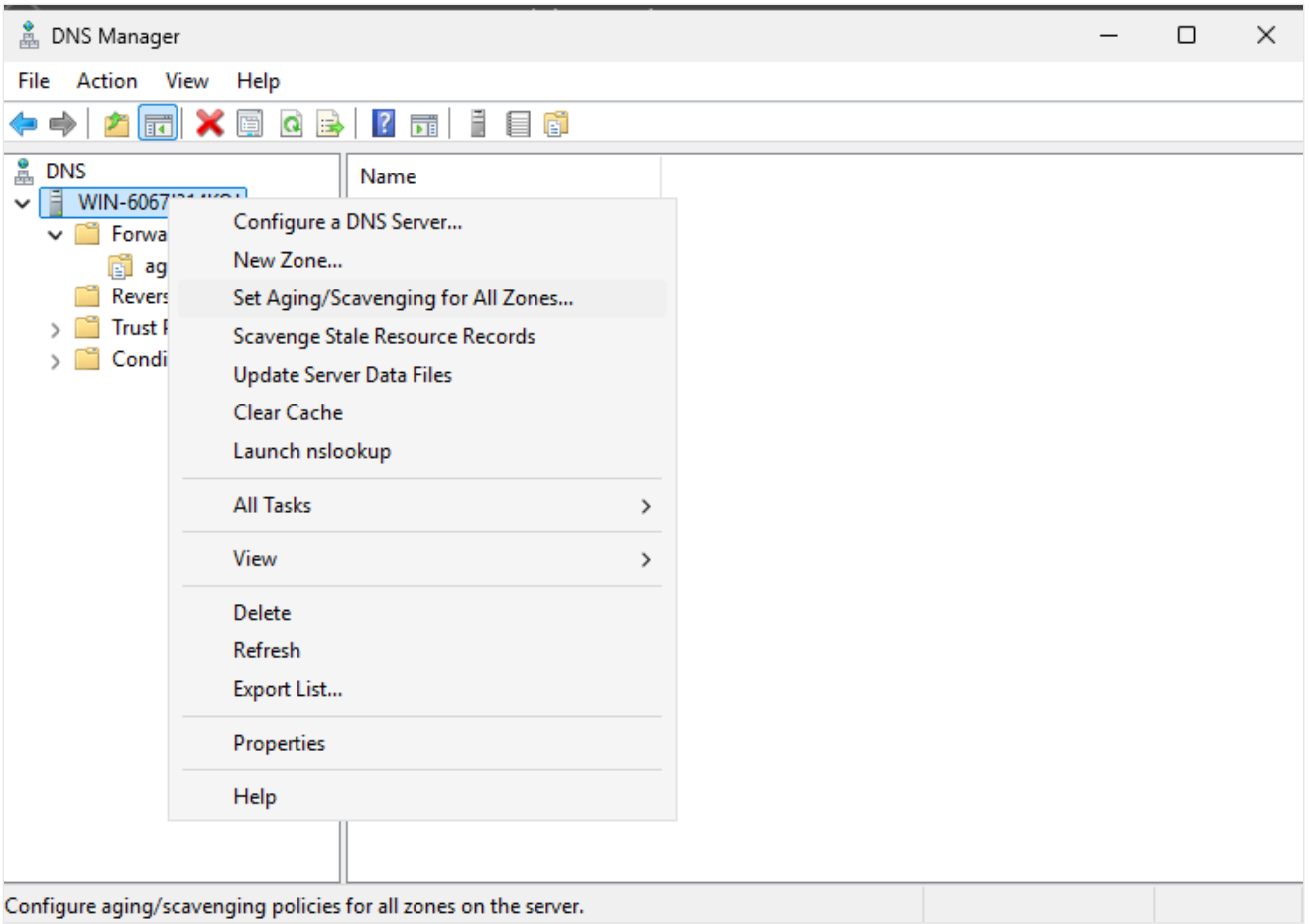
L'intervalle sans rafraîchissement supprime les mises à jour temporelles inutiles durant cette période. L'intervalle de rafraîchissement permet aux clients actifs de renouveler leurs horodatages pendant cette période. Un enregistrement devient éligible au récupération (c'est-à-dire que le serveur le considère comme obsolète) seulement après l'écoulement des deux intervalles, soit 14 jours avec les valeurs par défaut. Le prochain passage de nettoyage sur une zone éligible supprime tous les enregistrements obsolètes qu'il trouve. Des intervalles plus courts suppriment plus rapidement les enregistrements obsolètes mais augmentent le trafic de réplication et le risque de suppression des enregistrements pour les clients temporairement hors ligne.



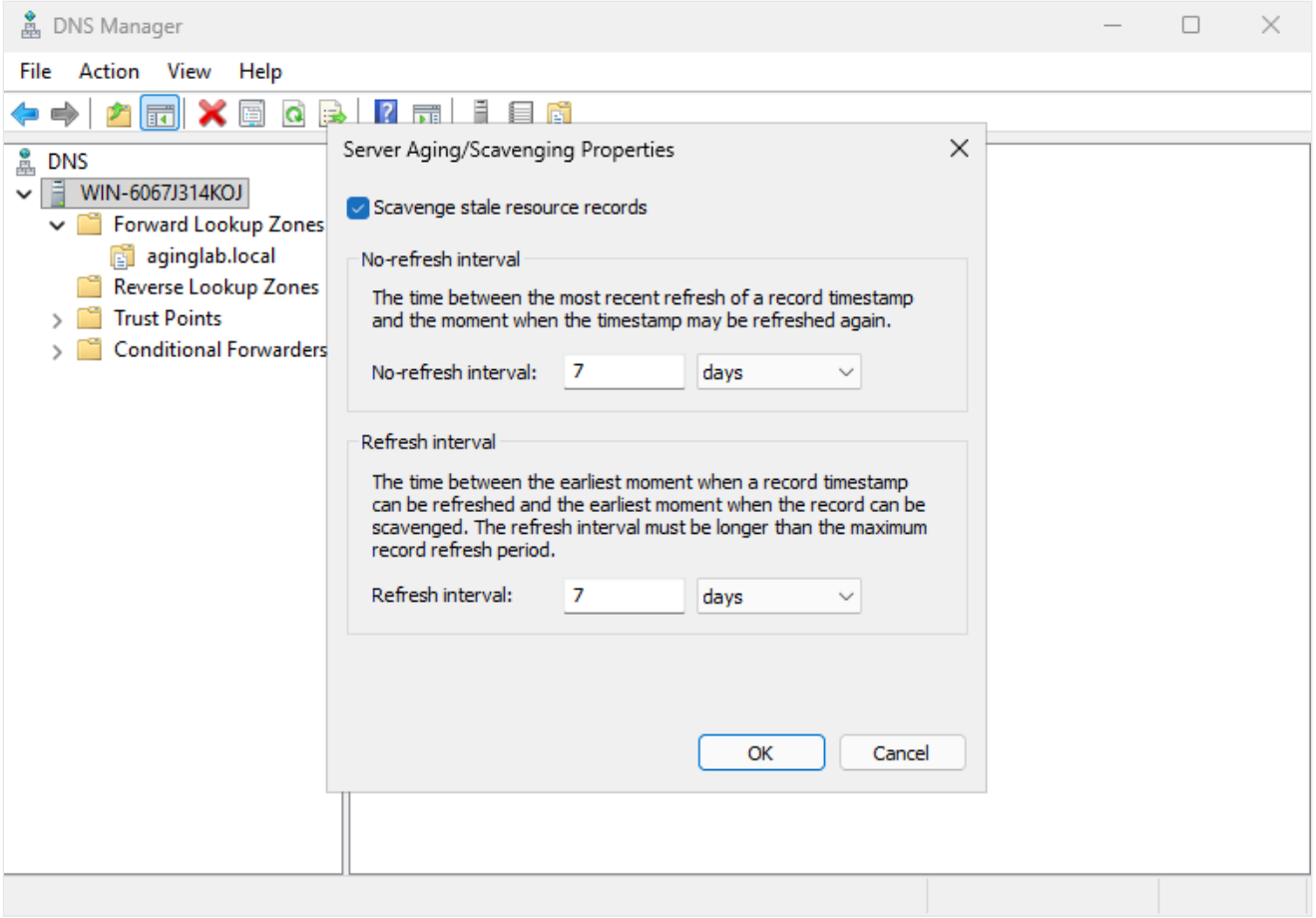
Définissez le vieillissement et le nettoyage pour toutes les zones

Utilisez cette tâche pour appliquer les paramètres de vieillissement à chaque zone simultanément, y compris les zones intégrées AD existantes.

1. Sélectionnez et maintenez (ou faites clic droit) sur le nom du serveur, sélectionnez **Définir vieillissement/Récupération pour toutes les zones**.
2. Sélectionnez **Nettoyer les enregistrements de ressources périmés** et définissez les intervalles.
3. Sélectionnez **OK**.
4. Sélectionnez **Appliquer ces paramètres aux zones intégrées à Active Directory existantes**, puis **sélectionnez OK**.



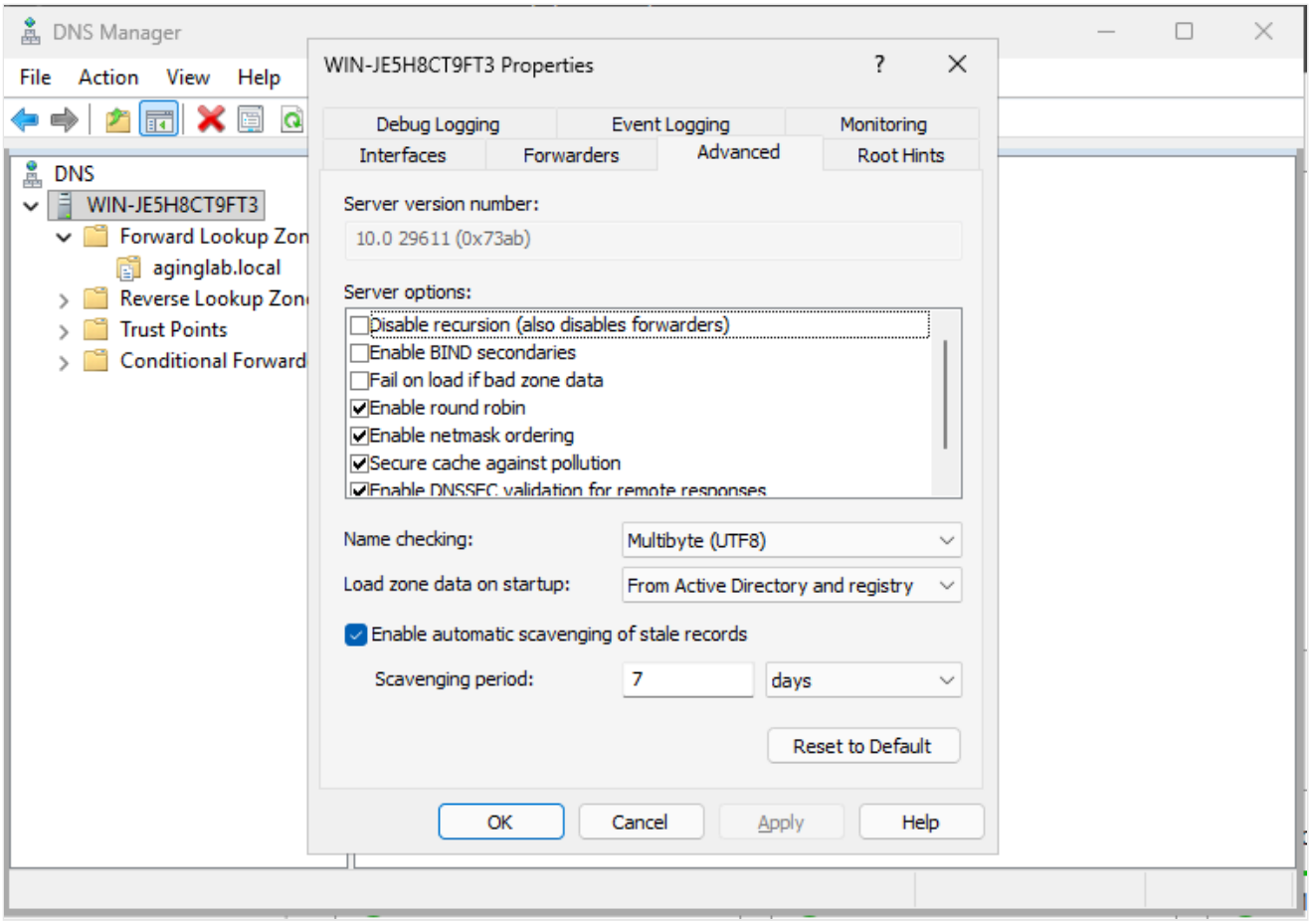
L'option Appliquer ces paramètres aux zones intégrées à Active Directory existante permet de faire vieillir les enregistrements dans les zones déjà existantes, par exemple après avoir converti une zone standard en AD-intégrée. Sans cette option, les nouveaux paramètres ne s'appliquent qu'aux zones créées par la suite.



> ⓘ **Remarque**
>
> Lorsque vous activez le vieillissement pour la première fois sur une zone, la zone bénéficie d'un intervalle de rafraîchissement pour protéger contre le charognardage. Cette période de grâce empêche le serveur de supprimer des enregistrements qui paraissent obsolètes à cause de l'horodatage mais que les clients auraient pu mettre à jour pendant que le vieillissement était désactivé, lorsque le serveur n'enregistrait pas ces horodatages. La période de grâce permet aux mises à jour dynamiques d'actualiser ces enregistrements avant que le nettoyage ne les supprime.

Activez le nettoyage automatique sur le serveur

1. Sélectionnez et maintenez (ou faites un clic droit) sur le serveur DNS, sélectionnez **Propriétés**, puis sélectionnez l'onglet **Avancé** .
2. Sélectionnez **Activer la récupération automatique des archives obsolètes**.
3. Définissez la **période de récupération**. La valeur par défaut et recommandée est de sept jours.
4. Sélectionnez **OK**.



La période de récupération détermine la fréquence à laquelle le serveur vérifie et supprime les enregistrements obsolètes éligibles. Cela ne détermine pas quand un disque devient obsolète.

Protéger un enregistrement contre la récupération

Pour protéger un dossier critique contre la fouille, effacez son horodatage :

1. Ouvrez les propriétés de l'enregistrement.
2. Effacer **Supprimer cet enregistrement lorsqu'il devient obsolète**.

Lorsque vous décochez cette case, l'horodatage de l'enregistrement est défini sur zéro, ce qui empêche le nettoyage.

> ⓘ **Remarque**
>
> Un enregistrement avec un horodatage zéro peut toujours recevoir des mises à jour dynamiques de ses données, comme une nouvelle adresse IP, mais son horodatage reste nul. L'enregistrement reste protégé contre le nettoyage. Le record ne redevient éligible à la récupération que si vous mettez un horodatage non nul.

Surveillez le nettoyage avec le journal d'événements

Une fois un cycle de nettoyage terminé, le serveur DNS inscrit l'un des événements suivants dans le journal des événements du serveur DNS. Examinez ces événements pour vérifier que le nettoyage est en cours et pour voir quels enregistrements il a retirés.

Agrandir le tableau

ID de l'événement	Meaning
2501	Un passage de nettoyage a été découvert et des disques **ont été** récupérés. Vérifiez quels enregistrements ont été supprimés par le nettoyage. Pour les zones intégrées à AD, les enregistrements supprimés peuvent être marqués comme supprimés et la modification se propage via la réplication AD.
2502	Un passage de récupération a été découvert, mais **aucun** enregistrement n'a été récupéré. Cet événement indique un état normal et sain lorsque tous les dossiers sont à jour.
4013	Le serveur DNS attend que services de domaine Active Directory s'initialise avant de charger les zones intégrées AD. Le serveur DNS retarde le fouillement jusqu'à la fin de l'initialisation AD DS.
4515	Le serveur DNS détecte une zone dupliquée dans Active Directory, ce qui peut empêcher la zone concernée de se charger ou d'être nettoyée correctement. Vérifiez la configuration des zones et l'état de la réplication AD.
4521	Le serveur DNS ne pouvait pas charger une zone intégrée AD, donc il ne peut pas récupérer la zone tant que vous n'avez pas résolu l'erreur sous-jacente. Consultez les journaux d'événements du serveur DNS et du service d'annuaire pour plus de détails.

Le serveur DNS programme le prochain passage automatique approximativement à l'heure de début du passage précédent plus l'intervalle de récupération configuré. L'ajout de la période de nettoyage à l'horodatage de l'événement 2501 ou 2502 fournit une estimation, mais l'horodatage de l'événement reflète l'achèvement de l'opération plutôt que son heure de début.

> **Conseil**
>
> Surveillez régulièrement l'ID d'événement 2501 pour confirmer que le nettoyage s'exécute et pour consulter les enregistrements qu'il supprime.

Pour les zones intégrées AD, surveillez également les journaux d'événements du serveur DNS et du service d'annuaire pour les événements 4013, 4515 et 4521, qui peuvent indiquer des problèmes de chargement de zone, de réplication ou de configuration. Lorsque vous enquêtez

sur les incohérences des enregistrements, interrogez chaque serveur DNS autoritaire directement avec `Resolve-DnsName`, et vérifiez l'état de réplication d'Active Directory avec `repadmin /replsummary` et `repadmin /showrepl`. Les réponses mises en cache peuvent persister dans le cache d'un client ou dans celui d'un serveur non autoritaire après la fin de la réplication, donc une réponse en cache obsolète n'indique pas nécessairement un échec de réplication.

Bonnes pratiques et erreurs courantes

Suivez les consignes suivantes pour effectuer les opérations de récupération en toute sécurité :

- **Testez d'abord en laboratoire.** Validez votre configuration dans un environnement non produit avant de l'activer en production.
- **Sauvegardez la configuration de votre serveur DNS.** Exportez la configuration de votre serveur avant de faire des modifications.
- **Sauvegardez vos données de zone.** Exportez les données des zones avant d'activer le vieillissement ou de déclencher le nettoyage.
- **Utilisez un serveur de récupération par zone.** Restreignez le fouillage à un seul serveur DNS avec le `-ScavengeServers` paramètre pour simplifier le dépannage.
- **Protégez les dossiers statiques critiques.** Créez des enregistrements pour serveurs, imprimantes, services web et contrôleurs de domaine sous forme d'enregistrements statiques, et assurez-vous de supprimer **cet enregistrement lorsqu'il devient obsolète**.
- **Surveiller l'ID d'événement 2501.** Consultez le journal des événements DNS pour confirmer les opérations de récupération et vérifier les enregistrements supprimés.
- **Vérifiez la réplication AD.** Pour les zones intégrées à AD, vérifiez la sortie de `repadmin /replsummary` et `repadmin /showrepl` avant d'activer le nettoyage ou de résoudre ses problèmes.

Évitez ces erreurs courantes :

- **Définir un intervalle de rafraîchissement trop court.** Si l'intervalle de rafraîchissement est plus court que le temps dont les clients ont besoin pour se réenregistrer, le nettoyage supprime des enregistrements valides. Alignez les intervalles « Sans rafraîchissement » et « Rafraîchissement » sur la durée de votre bail DHCP, de sorte que leur durée cumulée soit égale ou inférieure à celle du bail.
- **Nettoyer sur plusieurs serveurs sans coordination.** Le fait que plusieurs serveurs effectuent ce nettoyage indépendamment augmente le risque de situations de concurrence et rend plus difficile l'identification de l'origine des suppressions inattendues.
- **S'attendant à ce que des enregistrements statiques soient nettoyés.** Les enregistrements créés manuellement ont un horodatage zéro et ne s'effacent pas à moins que vous

n’attribuiez un horodatage non nul. Ce comportement est intentionnel.

Contenu connexe

- Vieillissement DNS et récupération
- Gérer les enregistrements de ressources DNS

ⓘ**Remarque :** L’auteur a créé cet article avec l’aide de l’IA. En savoir plus

---

Dernière mise à jour : 23/09/2026

Activer DNS sur HTTPS dans le serveur DNS

S'applique à: ✅ Windows Server 2025

Cet article explique comment activer DNS via HTTPS (DoH) dans le service serveur DNS s'exécutant sur Windows Server.

Le trafic DNS traditionnel n'est pas chiffré, ce qui expose les requêtes DNS à l'écoute, à l'interception et à la manipulation par des attaquants sur votre réseau. Si vous devez protéger la communication DNS entre les clients et votre serveur DNS, l'activation de DoH chiffre ce trafic à l'aide du protocole HTTPS, ce qui empêche l'observation ou la falsification non autorisées.

Pour plus d'informations sur le fonctionnement de DoH, consultez chiffrement DNS à l'aide de DNS via HTTPS.

Prerequisites

Avant de commencer, vérifiez que vous disposez des points suivants :

- Windows Server 2025 avec la mise à jour de sécurité 2026-06 (KB5094125) ou ultérieure installée
- Accès à une autorité de certification (CA) :
  - Microsoft Enterprise Certificate Authority avec des modèles de certificat publiés

  ou
  - Fournisseur de certificats tiers tel que DigiCert, Let's Encrypt ou Verisign
- Règles de pare-feu configurées pour autoriser les connexions entrantes sur le port TCP 443 pour DoH
- Accès administratif ou équivalent à Windows Server hébergeant le service serveur DNS

Les certificats DoH doivent répondre aux exigences suivantes :

- **Extension d'utilisation améliorée de la clé** : doit inclure l'identificateur d'objet Authentification du serveur (1.3.6.1.5.5.7.3.1)
- **Nom ou nom alternatif de l'objet** : certificat signé avec un nom alternatif de l'objet (SAN) et le nom de domaine entièrement qualifié ou l'adresse IP qui correspond à votre modèle d'URI DoH configuré.

- **Clé privée** : doit être présente dans le magasin de l'ordinateur local, correctement associée au certificat et ne doit pas avoir une protection forte de clé privée activée
- **Chaîne d'approbation** : doit être émise par une autorité de certification que le serveur DNS et les clients DNS approuvent

Pour connaître les configurations de certificats plus complexes, consultez Certificats et clés publiques et Utilisation des certificats.

Importer le certificat

Si vous disposez déjà d'un certificat sur le serveur, accédez à Lier le certificat. Sinon, importez votre certificat sur le serveur.

1. Placez le fichier du `.pfx` certificat (contenant à la fois le certificat et la clé privée) sur le serveur hébergeant le serveur DNS.
2. Ouvrez PowerShell en tant qu'administrateur et exécutez la commande suivante pour importer le certificat, en veillant à remplacer `<pfxpath>` par le chemin d'accès à votre `.pfx` fichier et `<pfxpassword>` par le mot de passe du `.pfx` fichier :

   PowerShell

   ```
   Import-PfxCertificate `
       -FilePath "<pfxpath>" `
       -CertStoreLocation "Cert:\LocalMachine\My" `
       -Password (Read-Host -AsSecureString "<pfxpassword>")
   ```

3. Lorsque vous y êtes invité, entrez le mot de passe de votre certificat.
4. Pour vérifier que le certificat a été importé avec succès, exécutez la commande suivante, en remplaçant `<subject-name>` par l'objet de votre certificat :

   PowerShell

   ```
   Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object { $_.Subject -match "
   <subject-name>" }
   ```

Lier le certificat

Après avoir importé le certificat, liez-le au port du serveur afin que le serveur DNS puisse l'utiliser pour les connexions HTTPS.

1. Générez un nouveau GUID et stockez-le dans une variable en exécutant la commande suivante :

   PowerShell
   ```
   $guid = New-Guid
   ```

2. Récupérez votre certificat et stockez-le dans une variable en exécutant la commande suivante. Remplacez `<subject-name>` par l'objet de votre certificat :

   PowerShell
   ```
   $cert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object { $_.Subject -
   match "<subject-name>" }
   ```

3. Liez le certificat au port du serveur en exécutant la commande suivante :

   PowerShell
   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=$($cert.Thumbprint) appid="
   {$guid}"
   ```

> **Conseil**
>
> Pour que le service serveur DNS réponde au trafic DoH sur une adresse IP spécifique au lieu de toutes les adresses, remplacez `0.0.0.0` par votre adresse IP souhaitée. L'adresse IP doit correspondre ou se résoudre à l'hôte spécifié dans le SAN de votre certificat. Vous pouvez également remplacer `443` par un autre numéro de port.

Vérifier la liaison de certificat

Vérifiez que votre certificat est correctement lié à l'adresse IP et au port appropriés.

1. Exécutez la commande suivante pour afficher les liaisons de certificat SSL :

   PowerShell
   ```
   netsh http show sslcert
   ```

2. Vérifiez que la sortie affiche votre adresse IP et votre port, et que le hachage de certificat correspond à votre empreinte numérique.

Configurer les règles de pare-feu

DoH utilise un port TCP différent du DNS non chiffré. Vous devez donc configurer votre pare-feu pour autoriser le trafic entrant sur le port que vous avez spécifié lors de la liaison du certificat. Par défaut, DoH utilise le port TCP 443, sauf si vous avez spécifié un autre port dans le modèle d'URI et les étapes de liaison de certificat.

Configurez le Pare-feu Windows pour autoriser les connexions entrantes sur le port DoH configuré en procédant comme suit :

1. Pour créer une règle de pare-feu qui autorise le trafic DoH entrant, exécutez la commande suivante :

   PowerShell
   ```
   New-NetFirewallRule -DisplayName "DNS over HTTPS" -Direction Inbound -Protocol
   TCP -LocalPort 443 -Action Allow
   ```

2. Vérifiez que la règle de pare-feu a été créée en exécutant la commande suivante :

   PowerShell
   ```
   Get-NetFirewallRule -DisplayName "DNS over HTTPS"
   ```

> **Remarque**
>
> Si vous avez configuré DoH pour utiliser un autre port, remplacez `443` par votre numéro de port personnalisé. Si vous utilisez un pare-feu matériel ou un groupe de sécurité réseau, vérifiez qu'il autorise également le trafic TCP entrant sur le même port.

Activer le DoH

Après avoir lié le certificat et configuré des règles de pare-feu, activez le DoH sur votre serveur DNS.

1. Activez DoH et définissez le modèle d'URI à l'aide de la commande Set-DnsServerEncryptionProtocol . Remplacez `dns.contoso.com` par le nom d'hôte (ou l'adresse IP) contenu dans le san de votre certificat :

   PowerShell

```
Set-DnsServerEncryptionProtocol -EnableDoh $true -UriTemplate
"https://dns.contoso.com:443/dns-query"
```

> ⓘ **Remarque**
>
> Vérifiez que le numéro de port dans le modèle d'URI correspond au numéro de port que vous avez utilisé lors de la liaison du certificat.

2. Redémarrez le service DNS pour appliquer les modifications :

PowerShell

```
Restart-Service -Name DNS
```

Vérifier la configuration DoH

Testez que DoH fonctionne correctement en vérifiant la configuration et le test à partir d'un client.

1. Vérifiez la configuration doH sur le serveur à l'aide de la commande Get-DnsServerEncryptionProtocol :

PowerShell

```
Get-DnsServerEncryptionProtocol
```

2. Ouvrez **l'Observateur d'événements** sur le serveur et accédez à **Journaux des applications et des services** > **Serveur DNS**.

3. Recherchez l'ID d'événement `822`, ce qui indique que le service DoH a démarré correctement.

Tester DoH à partir d'un client

Pour vérifier que DoH fonctionne correctement, testez la résolution DNS à partir d'un client compatible DoH.

1. Configurez un client DoH pour utiliser le chiffrement pour votre serveur DNS avec le même modèle d'URI que celui que vous avez configuré. Pour connaître les étapes de configuration du client, consultez Secure DNS Client over HTTPS (DoH).

2. À partir du client DoH configuré, testez la résolution DNS à l'aide de la commande Resolve-DnsName . Remplacez par `contoso.com` un domaine que vous souhaitez résoudre :

   PowerShell

   ```
   Resolve-DnsName -Name contoso.com -Type A
   ```

3. La requête DNS se résout correctement.

Pour vérifier davantage l'activité DoH, suivez l'article suivant pour surveiller DoH sur votre serveur DNS.

Étapes suivantes

Surveiller DNS sur HTTPS dans le serveur DNS

ⓘ**Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Last updated on 12/06/2026

Surveiller DNS sur HTTPS dans DNS Server (Aperçu)

S'applique à: ✅ Windows Server 2025

> ⓘ **Important**
>
> DNS sur HTTPS (DoH) pour le serveur DNS sur Windows Server est actuellement en préversion. Ces informations concernent un produit en version préliminaire qui peut être sensiblement modifié avant sa commercialisation. Microsoft n'offre aucune garantie, exprimée ou implicite, en ce qui concerne les informations fournies ici.

Cet article explique comment surveiller l'activité DNS sur HTTPS (DoH) sur le serveur DNS à l'aide des journaux d'événements et des compteurs de performances.

Lorsque vous activez DoH sur votre serveur DNS, vous avez besoin d'une visibilité sur le trafic DNS chiffré pour la planification de la capacité, l'analyse des performances et la sensibilisation opérationnelle. Étant donné que le trafic DoH est chiffré, les outils de surveillance réseau traditionnels ne peuvent pas inspecter les requêtes DNS. Les événements et compteurs de performances spécifiques à DoH décrits dans cet article vous aident à suivre l'activité de requête chiffrée, à mesurer le débit et à identifier les problèmes potentiels avec votre service DoH.

DoH chiffre le trafic DNS en encapsulant des messages DNS au sein du protocole HTTPS. Pour en savoir plus sur le fonctionnement de DoH, consultez le chiffrement DNS à l'aide de DNS via HTTPS.

Prerequisites

Avant de commencer, assurez-vous d'avoir :

- Windows Server 2025 avec la mise à jour de sécurité 2026-02 ((KB5075899)) ou ultérieure installée.
- DNS sur HTTPS activé et configuré sur votre serveur DNS (voir Activer DNS sur HTTPS dans le serveur DNS).
- Administrateur ou accès équivalent à Windows Server hébergeant le service serveur DNS.
- Compréhension de base de l'Observateur d'événements Windows et de l'Analyseur de performances.

Afficher les journaux du serveur

Le système active les journaux d'audit par défaut. Ces journaux d'activité n'affectent pas considérablement les performances du serveur DNS. Les événements d'audit du serveur DNS activent le démarrage, l'arrêt et le suivi des modifications sur le serveur DNS. Pour afficher les journaux DoH :

1. Sélectionnez le bouton **Démarrer** , tapez **l'Observateur d'événements** et ouvrez **l'Observateur** d'événements dans la liste de correspondances optimale.

2. Dans l'Observateur d'événements, accédez à **Applications et Services** > **Serveur DNS**.

3. Pour filtrer les événements spécifiques à DoH, cliquez avec le bouton droit sur **le serveur DNS**, sélectionnez **Filtrer le journal actuel** et, dans la boîte de dialogue de filtre, entrez les ID d'événement DoH suivants dans le champ **Tous les ID d'événement** : `597, 598, 599, 600, 601, 602, 603`. Sélectionnez **OK** pour appliquer le filtre.

Événements de serveur

Le tableau suivant récapitule les événements d'audit DoH.

Agrandir le tableau

ID de l'événement	Type	Catégorie	Level	Texte de l'événement
822	URL DoH inscrite	DNS sur HTTPS	Informational	`Successfully started HTTP server for DNS-over-HTTPS (DoH) server. The DoH server is listening on following URL(s): %1`
823	Échec de l'initialisation DoH	DNS sur HTTPS	Erreur	`The DNS server could not initialize the HTTP server for DNS-over-HTTPS (DoH) and failed with error code %1.`
824	Échec des sessions DoH	DNS sur HTTPS	Erreur	`The DNS server could not create the HTTP server session for DNS-over-HTTPS (DoH) and failed with error code %1.`
825	Échec de la création de l'URL DoH	DNS sur HTTPS	Erreur	`The DNS server could not register the URL: %1 for the DNS-over-HTTPS (DoH) server and failed with error code %2.`
826	Échec de la file d'attente de création	DNS sur HTTPS	Erreur	`The DNS server could not create the HTTP request queue for DNS-`

ID de l'événement	Type	Catégorie	Level	Texte de l'événement
	de requête DoH			`over-HTTPS (DoH) and failed with error code %1.`
827	Configuration DoH	DNS sur HTTPS	Informational	`The configuration for DNS-over-HTTPS (DoH) server are: %1`
828	Fermeture DoH	DNS sur HTTPS	Informational	`The DNS-over-HTTPS (DoH) server has shut down gracefully.`
829	Erreur de mise hors service DoH	DNS sur HTTPS	Erreur	`The DNS-over-HTTPS (DoH) server has shut down due to an error and failed with error code %1.`

Afficher les événements analytiques

Les événements analytiques ne sont pas activés par défaut, vous devez les activer pour afficher les événements analytiques spécifiques à DoH. Les événements analytiques DoH fournissent des informations détaillées sur les activités de requête et de réponse DNS chiffrées, telles que les noms de requête, les types, les codes de réponse et les temps de traitement. Vous pouvez afficher les événements spécifiques à DoH qui effectuent le suivi de l'activité de requête et de réponse chiffrées en procédant comme suit :

Pour activer la journalisation des diagnostics DNS :

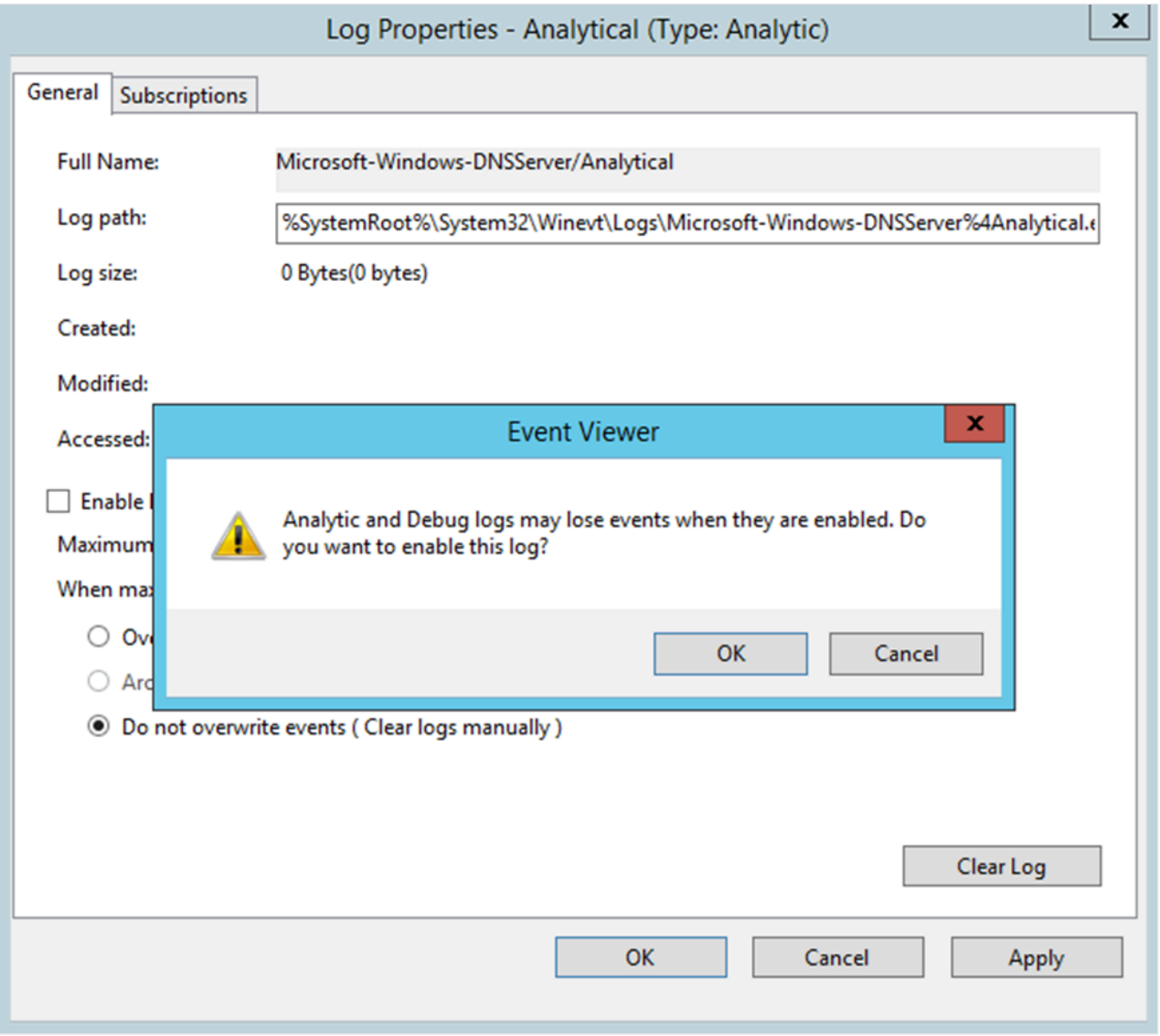
1. Dans le nœud **Journaux** > **des applications et services de Microsoft** > **Windows** > **DNS-Server**, faites un clic droit sur DNS-Server, sélectionnez **Affichage**, puis sélectionnez **Afficher les journaux d'analyse et de débogage**. Le journal analytique s'affiche.

2. Cliquez avec le bouton droit sur **Analytique** , puis sélectionnez **Propriétés**.

3. Si vous souhaitez interroger et afficher les journaux d'activité de l'observateur d'événements, choisissez **Lorsque la taille maximale du journal des événements est atteinte**, sélectionnez **Ne pas remplacer les événements (Effacer manuellement les journaux)**, cochez la case **Activer la journalisation**, puis cochez **OK** lorsque vous avez demandé si vous souhaitez activer ce journal.

4. Si vous souhaitez activer la journalisation circulaire, choisissez **Remplacer si nécessaire (les événements les plus anciens en premier)** et sélectionnez **Activer la journalisation**. Après avoir sélectionné **OK**, une erreur de requête s'affiche . La journalisation a lieu même si cette erreur s'affiche. L'erreur signifie uniquement que vous ne pouvez pas afficher les événements en cours de journalisation dans l'observateur d'événements.

5. Sélectionnez **OK** pour activer le journal des événements DNS Server Analytics.



Les journaux d'analyse sont écrits par défaut dans le fichier `%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.etl`. La section suivante explique les événements DoH affichés dans les journaux d'événements d'audit et d'analyse du serveur DNS.

Événements analytiques DNS sur HTTPS

Les événements analytiques DoH sont similaires aux événements analytiques DNS standard, mais ils suivent uniquement les requêtes et réponses chiffrées. Pour plus d'informations sur les journaux disponibles pour le service serveur DNS, consultez Activer la journalisation et les diagnostics DNS.

Le tableau suivant décrit les événements analytiques DoH :

Agrandir le tableau

ID de l'événement	Type	Catégorie	Texte de l'événement
597	Requête chiffrée reçue	Recherche	`QUERY_RECEIVED: Channel=%1; %2; InterfaceIP=%3; Source=%4; RD=%5; QNAME=%6; QTYPE=%7; XID=%8; Port=%9; Flags=%10; PacketData=%12; AdditionalInfo = VirtualizationInstanceOptionValue: %13; GUID=%14; %15`
598	Réponse chiffrée envoyée	Recherche	`RESPONSE_SUCCESS: Channel=%1; %2; InterfaceIP=%3; Destination=%4; AA=%5; AD=%6; QNAME=%7; QTYPE=%8; XID=%9; DNSSEC=%10; RCODE=%11; Port=%12; Flags=%13; Scope=%14; Zone=%15; PolicyName=%16; PacketData=%18; AdditionalInfo= %19; DataTag=%20; ElapsedTime=%21; GUID=%22; %23; %24;`
599	Échec de réponse chiffrée	Recherche	`RESPONSE_FAILURE: Channel=%1; %2; InterfaceIP=%3; Reason=%4; Destination=%5; QNAME=%6; QTYPE=%7; XID=%8; RCODE=%9; Port=%10; Flags=%11; Zone=%12; PolicyName=%13; PacketData=%15; AdditionalInfo = VirtualizationInstance: %14; ElapsedTime=%17; GUID=%18; %19`
600	Requête chiffrée rejetée	Recherche	`IGNORED_QUERY: Channel=%1; %2; InterfaceIP=%3; Source=%4; Reason=%5`
601	Échec du canal de réponse chiffré	Recherche	`IGNORED_QUERY: Channel=%1; %2; InterfaceIP=%3; Source=%4; Reason=%5`
602	Demande de mise à jour DDNS chiffrée reçue	Mise à jour dynamique	`DYN_UPDATE_RECV: Channel=%1; %2; InterfaceIP=%3; Source=%4; QNAME=%5; XID=%6; Port=%7; Flags=%8; SECURE=%9; PacketData=%11`
603	Réponse de mise à jour DDNS chiffrée envoyée	Mise à jour dynamique	`DYN_UPDATE_RESPONSE: Channel=%1; %2; InterfaceIP=%3; Destination=%4; QNAME=%5; XID=%6; ZoneScope=%7; Zone=%8; RCODE=%9; PolicyName=%10; PacketData=%12`

Le champ TCP n'est pas applicable à DoH. Le `Channel` champ (`%1`) le remplace et porte la valeur 2 pour le trafic DoH. Des informations complémentaires (`%2`) sur la demande ou la réponse suivent le `Channel` champ. Chaque événement inclut des informations détaillées telles que la version HTTP, l'ID de requête et les codes d'état. Pour les événements de requête, les informations complémentaires suivent ce format :

```text
HTTP=Version:HTTP/2; Verb:POST; RequestID:{4987238521587782}
```

Pour les événements de réponse, le format inclut l'état HTTP :

```text
HTTP=Version:HTTP/2; Verb:POST; RequestID:{4987238521587782}; Status:200
```

Superviser les performances

Le tableau suivant décrit les compteurs de performances DoH disponibles :

Agrandir le tableau

Nom du compteur	Catégorie	Descriptif
Demandes DoH reçues par seconde	DNS-over-HTTPS	Mesure le nombre de paquets de requête DoH que le serveur reçoit chaque seconde
Réponses DoH envoyées par secondes	DNS-over-HTTPS	Mesure le nombre de paquets de réponse DoH que le serveur envoie correctement chaque seconde, y compris les réponses provenant de données faisant autorité, les données mises en cache, les réponses transférées, les résultats de récursivité et les réponses avec des codes d'erreur HTTP ou DNS
Demandes DoH rejetées/s	DNS-over-HTTPS	Mesure le nombre de requêtes DoH entrantes supprimées par le serveur chaque seconde avant le traitement normal, en raison de limites de ressources du serveur, d'erreurs d'analyse de paquets, de limitation de débit, de congestion du réseau ou de stratégies de sécurité

Remarque

Les compteurs de performances sont réinitialisés lorsque le service serveur DNS redémarre.

Les compteurs de performances DoH mesurent l'activité de requête DNS chiffrée séparément du trafic DNS traditionnel. Pour surveiller les performances DoH, sélectionnez votre méthode préférée dans la section suivante.

Analyseur de performances

Pour surveiller les compteurs de performances DoH à l'aide de l'Analyseur de performances, procédez comme suit :

1. Sélectionnez **Démarrer**, tapez **Analyseur de performances**, puis sélectionnez **Analyseur de performances** dans les résultats.
2. Dans **l'Analyseur de performances**, sélectionnez le bouton **Ajouter** (signe plus vert) pour ajouter des compteurs.
3. Dans la liste **des compteurs disponibles**, dépliez **DNS sur HTTPS**.
4. Sélectionnez les compteurs DoH que vous souhaitez surveiller :
   - **Demandes DoH reçues par seconde**
   - **Réponses DoH envoyées/s**
   - **Demandes DoH supprimées/s**
5. Sélectionnez **Ajouter** pour ajouter les compteurs sélectionnés au graphique d'analyse.
6. Sélectionnez **OK** pour commencer à surveiller les compteurs.

Contenu connexe

- Activer DNS sur HTTPS dans le serveur DNS
- Chiffrement DNS à l'aide de DNS via HTTPS
- Activer la journalisation et les diagnostics DNS
- À propos du suivi d'événements

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Last updated on 12/02/2026

Sécuriser le client DNS via HTTPS (DoH)

16/08/2025

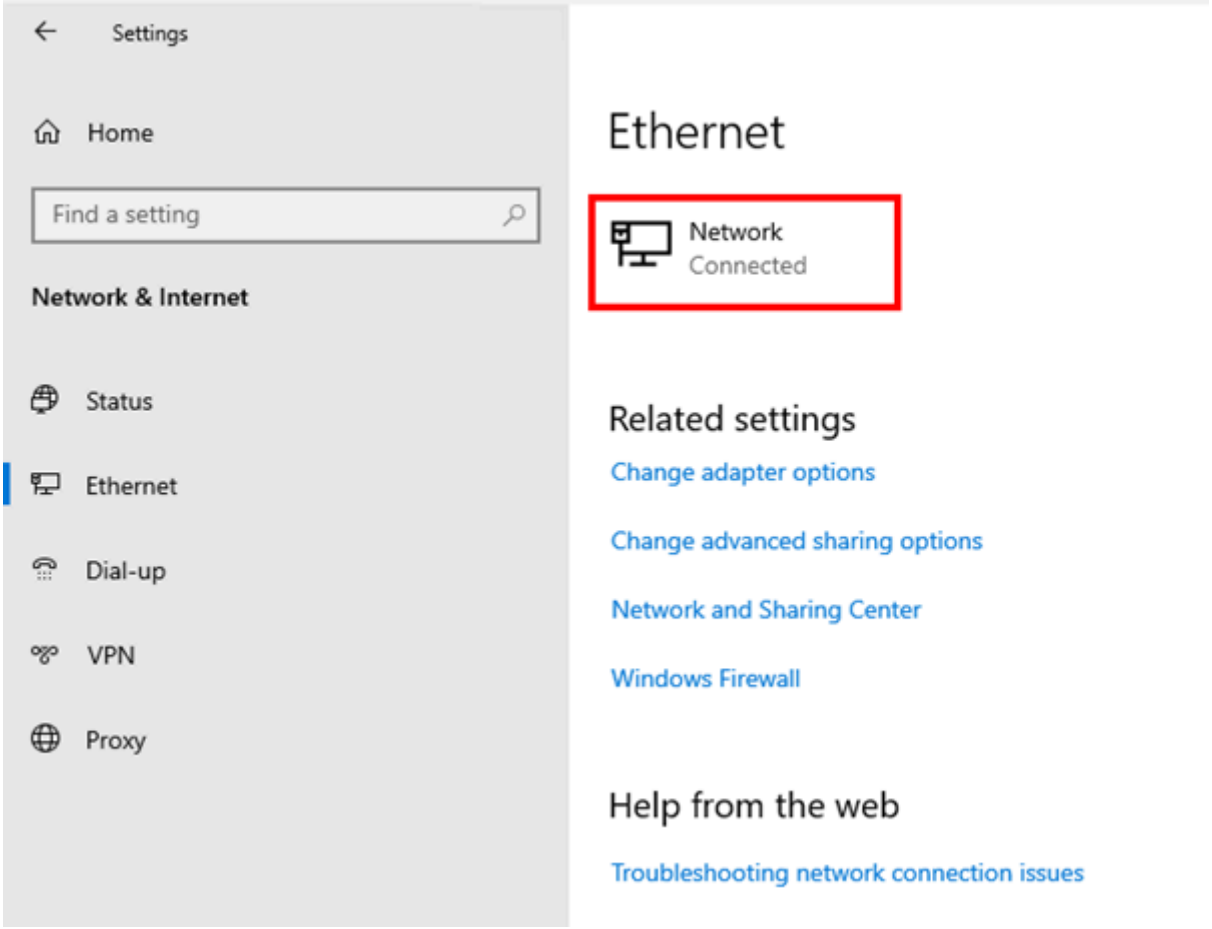
S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

À compter de Windows Server 2022, le client DNS prend en charge DNS-over-HTTPS (DoH). Lorsque Le doH est activé, les requêtes DNS entre le client DNS de Windows Server et le serveur DNS passent sur une connexion HTTPS sécurisée plutôt qu'en texte brut. En passant la requête DNS sur une connexion chiffrée, elle est protégée contre l'interception par des tiers non approuvés.

Configurer le client DNS pour prendre en charge DoH

Vous pouvez configurer le client Windows Server pour utiliser DoH uniquement si le serveur DNS principal ou secondaire sélectionné pour l'interface réseau figure dans la liste des serveurs DoH connus. Vous pouvez configurer le client DNS pour exiger DoH, demander DoH ou utiliser uniquement des requêtes DNS en texte brut traditionnelles. Pour configurer le client DNS pour prendre en charge DoH sur Windows Server avec Expérience de bureau, procédez comme suit :

1. Dans le panneau de configuration paramètres Windows, sélectionnez **Réseau et Internet**.
2. Dans la page Réseau et Internet, sélectionnez **Ethernet**.
3. Sur l'écran Ethernet, sélectionnez l'interface réseau que vous souhaitez configurer pour DoH.



4. Sur l'écran Réseau, faites défiler jusqu'aux **paramètres DNS** et sélectionnez le bouton **Modifier** .

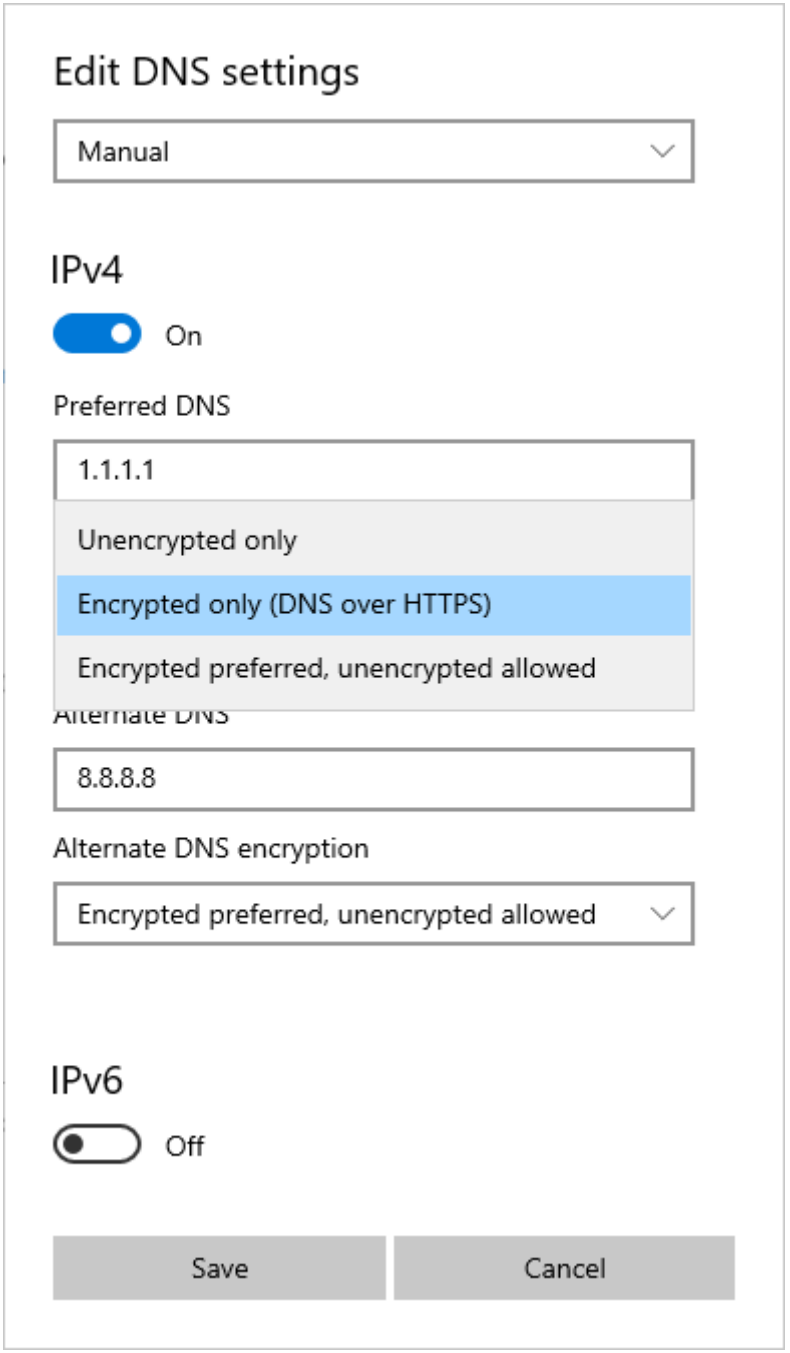
5. Dans l'écran Modifier les paramètres DNS, sélectionnez Manuel dans la liste déroulante des paramètres IP automatiques ou manuels. Ce paramètre vous permet de configurer le DNS préféré et d'autres serveurs DNS. Si les adresses de ces serveurs sont présentes dans la liste des serveurs DoH connus, la liste déroulante **de chiffrement DNS préférée** est activée. Vous pouvez choisir entre les paramètres suivants pour définir le chiffrement DNS préféré :

   - **Chiffré uniquement (DNS sur HTTPS)**. Lorsque ce paramètre est choisi, tout le trafic de requête DNS passe sur HTTPS. Ce paramètre offre la meilleure protection pour le trafic de requête DNS. Toutefois, cela signifie également que la résolution DNS ne se produit pas si le serveur DNS cible ne peut pas prendre en charge les requêtes DoH.

   - **Chiffrement préféré, non chiffré autorisé**. Lorsque ce paramètre est choisi, le client DNS tente d'utiliser DoH, puis revient aux requêtes DNS non chiffrées si cela n'est pas possible. Ce paramètre offre la meilleure compatibilité pour les serveurs DNS compatibles DoH, mais vous ne serez pas fourni avec une notification si les requêtes DNS sont passées du DoH au texte brut.

   - **Non chiffré uniquement**. Tout le trafic de requête DNS vers le serveur DNS spécifié n'est pas chiffré. Ce paramètre configure le client DNS pour qu'il utilise des requêtes

DNS de texte brut traditionnelles.



6. Sélectionnez **Enregistrer** pour appliquer les paramètres DoH au client DNS.

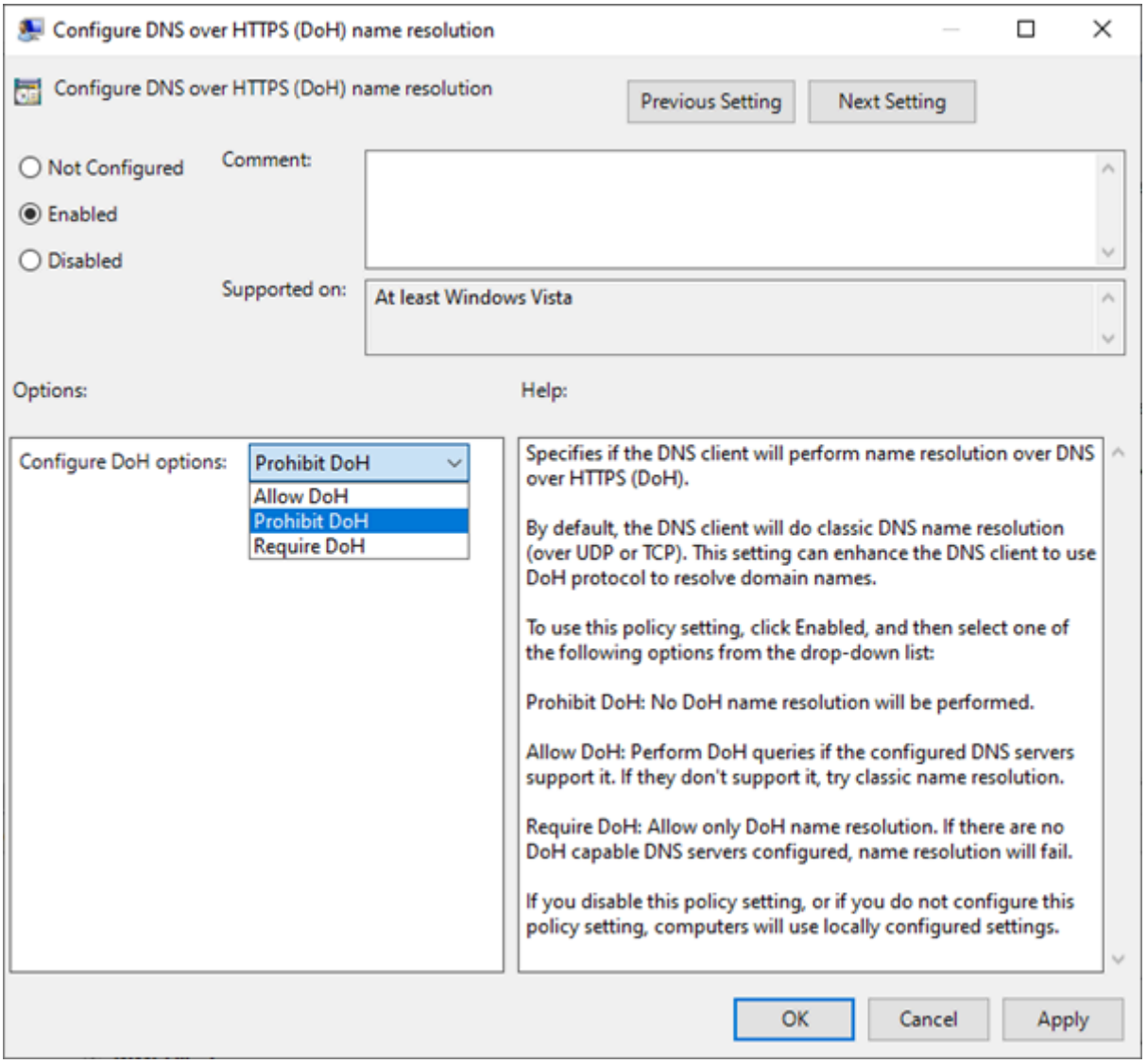
Si vous configurez l'adresse du serveur DNS pour un client via PowerShell à l'aide de l'applet de commande `Set-DNSClientServerAddress`, le paramètre DoH dépend du paramètre de secours du serveur dans la liste des serveurs DoH connus. Actuellement, vous ne pouvez pas configurer les paramètres DoH pour le client DNS sur Windows Server 2022 à l'aide de Windows Admin Center ou *de sconfig.cmd*.

Configuration de DoH via une stratégie de groupe

Les paramètres de stratégie de groupe locaux et de domaine Windows Server 2022 incluent la stratégie de résolution de noms **Configurer DNS sur HTTPS (DoH)**. Vous pouvez l'utiliser pour

configurer le client DNS pour utiliser DoH. Cette stratégie se trouve dans le nœud `Computer Configuration\Policies\Administrative Templates\Network\DNS Client`. Quand elle est activée, cette stratégie peut être configurée avec les paramètres suivants :

- **Autoriser DoH**. Les requêtes sont effectuées à l'aide de DoH si les serveurs DNS spécifiés prennent en charge le protocole. Si les serveurs ne prennent pas en charge DoH, des requêtes non chiffrées sont émises.
- **Interdire DoH**. Empêchera l'utilisation de DoH avec des requêtes client DNS.
- **Exiger DoH**. Nécessite que les requêtes soient effectuées à l'aide de DoH. Si les serveurs DNS configurés ne prennent pas en charge DoH, la résolution de noms échoue.



N'activez pas l'option Exiger le doH pour les ordinateurs joints à un domaine, car Les services de domaine Active Directory dépendent fortement du DNS, car le service Serveur DNS Windows Server ne prend pas en charge les requêtes DoH. Si vous avez besoin que le trafic de requête DNS sur le réseau des services de domaine Active Directory soit chiffré, envisagez d'implémenter des règles de sécurité de connexion basées sur IPsec pour protéger ce trafic.

Pour plus d'informations, consultez Sécurisation des connexions IPsec de bout en bout à l'aide de IKEv2 .

Déterminer les serveurs DoH figurant dans la liste des serveurs connus

Windows Server est fourni avec une liste de serveurs connus pour prendre en charge DoH. Vous pouvez déterminer quels serveurs DNS se trouvent dans cette liste à l'aide de l'applet `Get-DNSClientDohServerAddress` de commande PowerShell.

```
Administrator: Windows PowerShell
PS C:\> Get-DNSClientDohServerAddress

ServerAddress        AllowFallbackToUdp AutoUpgrade DohTemplate
-------------        ------------------ ----------- -----------
149.112.112.112      False              False       https://dns.quad9.net/dns-query
9.9.9.9              False              False       https://dns.quad9.net/dns-query
8.8.8.8              False              False       https://dns.google/dns-query
8.8.4.4              False              False       https://dns.google/dns-query
1.1.1.1              False              False       https://cloudflare-dns.com/dns-query
1.0.0.1              False              False       https://cloudflare-dns.com/dns-query
2001:4860:4860::8844 False              False       https://dns.google/dns-query
2001:4860:4860::8888 False              False       https://dns.google/dns-query
2606:4700:4700::1001 False              False       https://cloudflare-dns.com/dns-query
2606:4700:4700::1111 False              False       https://cloudflare-dns.com/dns-query
2620:fe::fe          False              False       https://dns.quad9.net/dns-query
2620:fe::fe:9        False              False       https://dns.quad9.net/dns-query


PS C:\>
```

La liste par défaut des serveurs DoH connus est la suivante :

Agrandir le tableau

Propriétaire du serveur	Adresses IP du serveur DNS
Cloudflare	1.1.1.1 1.0.0.1 2606:4700:4700::1111 2606:4700:4700::1001
Google	8.8.8.8 8.8.4.4 2001:4860:4860::8888 2001:4860:4860::8844
Quad 9	9.9.9.9 149.112.112.112 2620:fe::fe 2620:fe::fe:9

Ajouter un nouveau serveur DoH à la liste des serveurs connus

Vous pouvez ajouter de nouveaux serveurs DoH à la liste des serveurs connus à l'aide de l'applet `Add-DnsClientDohServerAddress` de commande PowerShell. Spécifiez l'URL du modèle DoH et indiquez si vous autoriserez le client à revenir à une requête non chiffrée si la requête sécurisée échoue. La syntaxe de cette commande est la suivante :

PowerShell

```
Add-DnsClientDohServerAddress -ServerAddress '<resolver-IP-address>' -DohTemplate
'<resolver-DoH-template>' -AllowFallbackToUdp $False -AutoUpgrade $True
```

Utiliser la table de stratégie de résolution de noms avec DoH

Vous pouvez utiliser la table de stratégie de résolution de noms (NRPT) pour configurer des requêtes sur un espace de noms DNS spécifique pour utiliser un serveur DNS spécifique. Si le serveur DNS est connu pour prendre en charge DoH, les requêtes liées à ce domaine sont effectuées à l'aide de DoH plutôt que d'une manière non chiffrée.

Activer la journalisation et les diagnostics DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Découvrez comment activer la journalisation, l'audit et les événements analytiques DNS améliorés pour le rôle serveur DNS dans Windows Server. La journalisation et les diagnostics DNS fournissent des informations détaillées sur les opérations de serveur DNS, notamment les modifications de zone, les mises à jour dynamiques et les opérations DNSSEC. La journalisation et les diagnostics DNS peuvent vous aider à surveiller les performances du serveur DNS, à résoudre les problèmes DNS et à suivre l'activité du serveur DNS.

Prerequisites

Avant d'activer la journalisation et les diagnostics DNS, vérifiez que vous disposez des points suivants :

- Un serveur Windows avec le rôle serveur DNS installé, y compris les outils d'administration de serveur distant DNS (RSAT).
- Privilèges d'administration sur le serveur.
- Compréhension de base des opérations de serveur DNS.

Afficher les journaux du serveur DNS

Les journaux d'audit DNS sont activés par défaut et n'affectent pas considérablement les performances du serveur DNS. Les événements d'audit du serveur DNS activent le suivi des modifications sur le serveur DNS. Un événement d'audit est journalisé chaque fois que les paramètres d'enregistrement de serveur, de zone ou de ressource sont modifiés. Les événements d'audit incluent des événements opérationnels tels que les mises à jour dynamiques, les transferts de zones, ainsi que la signature et l'annulation de signature de zone DNSSEC. Pour afficher les journaux du serveur DNS :

1. Sélectionnez le bouton **Démarrer**, tapez Observateur d'événements, ouvrez **l'Observateur** d'événements dans la liste de correspondances optimale.
2. Dans l'Observateur d'événements, accédez à **Applications et services** > **Journaux** > **Microsoft** > **Windows** > **Serveur DNS**.

3. Sélectionnez **Audit** dans le volet de navigation pour afficher les journaux d'audit DNS.

Événements d'audit

Le tableau suivant récapitule les événements d'audit du serveur DNS.

Agrandir le tableau

ID de l'événement	Type	Category	Level	Texte de l'événement
513	`Zone delete`	Opérations de zone	Informational	`The zone %1 was deleted.`
514	`Zone updated`	Opérations de zone	Informational	`The zone %1 was updated. The %2 setting has been set to %3.`
515	`Record create`	Opérations de zone	Informational	`A resource record of type %1, name %2, TTL %3 and RDATA %5 was created in scope %7 of zone %6.`
516	`Record delete`	Opérations de zone	Informational	`A resource record of type %1, name %2 and RDATA %5 was deleted from scope %7 of zone %6.`
517	`RRSET delete`	Opérations de zone	Informational	`All resource records of type %1, name %2 were deleted from scope %4 of zone %3.`
518	`Node delete`	Opérations de zone	Informational	`All resource records at Node name %1 were deleted from scope %3 of zone %2.`
519	`Record create - dynamic update`	Mise à jour dynamique	Informational	`A resource record of type %1, name %2, TTL %3 and RDATA %5 was created in scope %7 of zone %6 via dynamic update from IP Address %8.`
520	`Record delete - dynamic update`	Mise à jour dynamique	Informational	`A resource record of type %1, name %2 and RDATA %5 was deleted from scope %7 of zone %6 via dynamic update from IP Address %8.`
521	`Record scavenge`	Aging	Informational	`A resource record of type %1, name %2, TTL %3 and RDATA %5 was scavenged from scope %7 of zone %6.`
522	`Zone scope create`	Opérations de zone	Informational	`The scope %1 was created in zone %2.`

ID de l'événement	Type	Category	Level	Texte de l'événement
523	`Zone scope delete`	Opérations de zone	Informational	`The scope %1 was created in zone %2.`
525	`Zone sign`	Signature en ligne	Informational	`The zone %1 was signed with following properties...`
526	`Zone unsign`	Signature en ligne	Informational	`The zone %1 was unsigned.`
527	`Zone re-sign`	Signature en ligne	Informational	`The zone %1 was re-signed with following properties...`
528	`Key rollover start`	Opérations DNSSEC	Informational	`Rollover was started on the type %1 with GUID %2 of zone %3.`
529	`Key rollover end`	Opérations DNSSEC	Informational	`Rollover was completed on the type %1 with GUID %2 of zone %3.`
530	`Key retire`	Opérations DNSSEC	Informational	`The type %1 with GUID %2 of zone %3 was marked for retiral. The key will be removed after the rollover completion.`
531	`Key rollover triggered`	Opérations DNSSEC	Informational	`Manual rollover was triggered on the type %1 with GUID %2 of zone %3.`
533	`Key poke rollover`	Opérations DNSSEC	Warning	`The keys signing key with GUID %1 on zone %2 that was waiting for a Delegation Signer(DS) update on the parent has been forced to move to rollover completion.`
534	`Export DNSSEC`	Opérations DNSSEC	Informational	`DNSSEC setting metadata was exported %1 key signing key metadata from zone %2.`
535	`Import DNSSEC`	Opérations DNSSEC	Informational	`DNSSEC setting metadata was imported on zone %1.`
536	`Cache purge`	Opérations DNSSEC	Informational	`A record of type %1, QNAME %2 was purged from scope %3 in cache.`
537	`Forwarder reset`	Opérations de cache	Informational	`The forwarder list on scope %2 has been reset to %1.`
540	`Root hints`	Configuration	Informational	`The root hints have been modified.`

ID de l'événement	Type	Category	Level	Texte de l'événement
541	`Server setting`	Configuration	Informational	`The setting %1 on scope %2 has been set to %3.`
542	`Server scope create`	Configuration	Informational	`The scope %1 of DNS server was created.`
543	`Server scope delete`	Configuration	Informational	`The scope %1 of DNS server was deleted.`
544	`Add trust point DNSKEY`	Configuration	Informational	`The DNSKEY with Key Protocol %2, Base64 Data %4 and Crypto Algorithm %5 has been added at the trust point %1.`
545	`Add trust point DS`	Configuration	Informational	`The DS with Key Tag: %2, Digest Type: %3, Digest: %5 and Crypto Algorithm: %6 has been added at the trust point %1.`
546	`Remove trust point`	Configuration	Informational	`The trust point at %1 of type %2 has been removed.`
547	`Add trust point root`	Opérations DNSSEC	Informational	`The trust anchor for the root zone has been added.`
548	`Restart server`	Opérations DNSSEC	Informational	`A request to restart the DNS server service has been received.`
549	`Clear debug logs`	Opérations DNSSEC	Informational	`The debug logs have been cleared from %1 on DNS server.`
550	`Write dirty zones`	Opérations DNSSEC	Informational	`The in-memory contents of all the zones on DNS server have been flushed to their respective files.`
551	`Clear statistics`	Opérations de serveur	Informational	`All the statistical data for the DNS server has been cleared.`
552	`Start scavenging`	Opérations de serveur	Informational	`A resource record scavenging cycle has been started on the DNS Server.`
553	`Enlist directory partition`	Opérations de serveur	Informational	`1%`

ID de l'événement	Type	Category	Level	Texte de l'événement
554	`Abort scavenging`	Opérations de serveur	Informational	`The resource record scavenging cycle has been terminated on the DNS Server.`
555	`Prepare for demotion`	Opérations de serveur	Informational	`The DNS server has been prepared for demotion by removing references to it from all zones stored in the Active Directory.`
556	`Write root hints`	Opérations de serveur	Informational	`The information about the root hints on the DNS server has been written back to the persistent storage.`
557	`Listen address`	Opérations de serveur	Informational	`The addresses on which DNS server will listen has been changed to %1.`
558	`Active refresh trust points`	Opérations de serveur	Informational	`An immediate RFC 5011 active refresh has been scheduled for all trust points.`
559	`Pause zone`	Opérations de serveur	Informational	`The zone %1 is paused.`
560	`Resume zone`	Opérations de serveur	Informational	`The zone %1 is resumed.`
561	`Reload zone`	Opérations DNSSEC	Informational	`The data for zone %1 has been reloaded from %2.`
562	`Refresh zone`	Opérations de zone	Informational	`The data for zone %1 has been refreshed from the primary server %2.`
563	`Expire zone`	Opérations de zone	Informational	`The secondary zone %1 has been expired and new data has been requested from the primary server %2.`
564	`Update from DS`	Opérations de zone	Informational	`The zone %1 has been reloaded from the Active Directory.`
565	`Write and notify`	Opérations de zone	Informational	`The content of the zone %1 has been written to the disk and the notification has been sent to all the notify servers.`
566	`Force aging`	Opérations de zone	Informational	`All DNS records at the node %1 in the zone %2 will have their aging time stamp set to the current time.%3`

ID de l'événement	Type	Category	Level	Texte de l'événement
567	`Scavenge servers`	Opérations de zone	Informational	`The Active Directory-integrated zone %1 has been updated. Only %2 can run scavenging.`
568	`Transfer primary key server`	Opérations de zone	Informational	`The key management role for zone %1 has been %2.%3`
569	`Add SKD`	Opérations de zone	Informational	`A %1 singing key (%2) descriptor has been added on the zone %3 with following properties: KeyId=%4; KeyType=%5; CurrentState=%6; KeyStorageProvider=%7; StoreKeysInAD=%8; CryptoAlgorithm=%9; KeyLength=%10; DnsKeySignatureValidityPeriod=%11; DSSignatureValidityPeriod=%12; ZoneSignatureValidityPeriod=%13; InitialRolloverOffset=%14; RolloverPeriod=%15; RolloverType=%16; NextRolloverAction=%17; LastRolloverTime=%18; NextRolloverTime=%19; CurrentRolloverStatus=%20; ActiveKey=%21; StandbyKey=%22; NextKey=%23. The zone will be resigned with the %2 generated with these properties.`
570	`Modify SKD`	Opérations de zone	Informational	`A %1 singing key (%2) descriptor with GUID %3 has been updated on the zone %4. The properties of this %2 descriptor have been set to: KeyId=%5; KeyType=%6; CurrentState=%7; KeyStorageProvider=%8; StoreKeysInAD=%9; CryptoAlgorithm=%10; KeyLength=%11; DnsKeySignatureValidityPeriod=%12; DSSignatureValidityPeriod=%13; ZoneSignatureValidityPeriod=%14; InitialRolloverOffset=%15; RolloverPeriod=%16; RolloverType=%17; NextRolloverAction=%18; LastRolloverTime=%19; NextRolloverTime=%20; CurrentRolloverStatus=%21; ActiveKey=%22; StandbyKey=%23; NextKey=%24. The zone`

ID de l'événement	Type	Category	Level	Texte de l'événement
				`will be resigned with the %2 generated with these properties.`
571	`Delete SKD`	Opérations DNSSEC	Informational	`A %1 singing key (%2) descriptor %4 has been removed from the zone %3.`
572	`Modify SKD state`	Opérations DNSSEC	Informational	`The state of the %1 signing key (%2) %3 has been modified on zone %4. The new active key is %5, standby key is %6 and next key is %7.`
573	`Add delegation`	Opérations DNSSEC	Informational	`A delegation for %1 in the scope %2 of zone %3 with the name server %4 has been added.`
574	`Create client subnet record`	Opérations DNSSEC	Informational	`The client subnet record with name %1 value %2 has been added to the client subnet map.`
575	`Delete client subnet record`	Opérations DNSSEC	Informational	`The client subnet record with name %1 has been deleted from the client subnet map.`
576	`Update client subnet record`	Opérations de zone	Informational	`The client subnet record with name %1 has been updated from the client subnet map. The new client subnets that it refers to are %2.`
577	`Create server level policy`	Opérations de stratégie	Informational	`A server level policy %6 for %1 has been created on server %2 with following properties: ProcessingOrder:%3; Criteria:%4; Action:%5.`
578	`Create zone level policy`	Opérations de stratégie	Informational	`A zone level policy %8 for %1 has been created on zone %6 on server %2 with following properties: ProcessingOrder:%3; Criteria:%4; Action:%5; Scopes:%7.`
579	`Create forwarding policy`	Opérations de stratégie	Informational	`A forwarding policy %6 has been created on server %2 with following properties: ProcessingOrder:%3; Criteria:%4; Action:%5; Scope:%1.`
580	`Delete server`	Opérations de stratégie	Informational	`The server level policy %1 has been deleted from server %2.`

ID de l'événement	Type	Category	Level	Texte de l'événement
	`level policy`			
581	`Delete zone level policy`	Opérations de stratégie	Informational	`The zone level policy %1 has been deleted from zone %3 on server %2.`
582	`Delete forwarding policy`	Opérations de stratégie	Informational	`The forwarding policy %1 has been deleted from server %2.`

Activer la journalisation des événements analytiques

La journalisation et les diagnostics DNS améliorés dans Windows Server incluent les événements d'audit DNS et les événements DNS Analytics. Les journaux d'audit DNS sont activés par défaut et n'affectent pas considérablement les performances du serveur DNS.

Les journaux analytiques DNS ne sont pas activés par défaut et affectent généralement uniquement les performances du serveur DNS à des taux de requête DNS élevés. Par exemple, un serveur DNS s'exécutant sur du matériel moderne qui reçoit 100 000 requêtes par seconde (QPS) peut rencontrer une dégradation des performances de 5% lorsque les journaux analytiques sont activés. Il n'existe aucun impact apparent sur les performances pour les taux de requête de 50 000 QPS et inférieurs. Toutefois, nous vous recommandons de surveiller les performances du serveur DNS chaque fois que la journalisation est activée.

Pour activer la journalisation des diagnostics DNS :

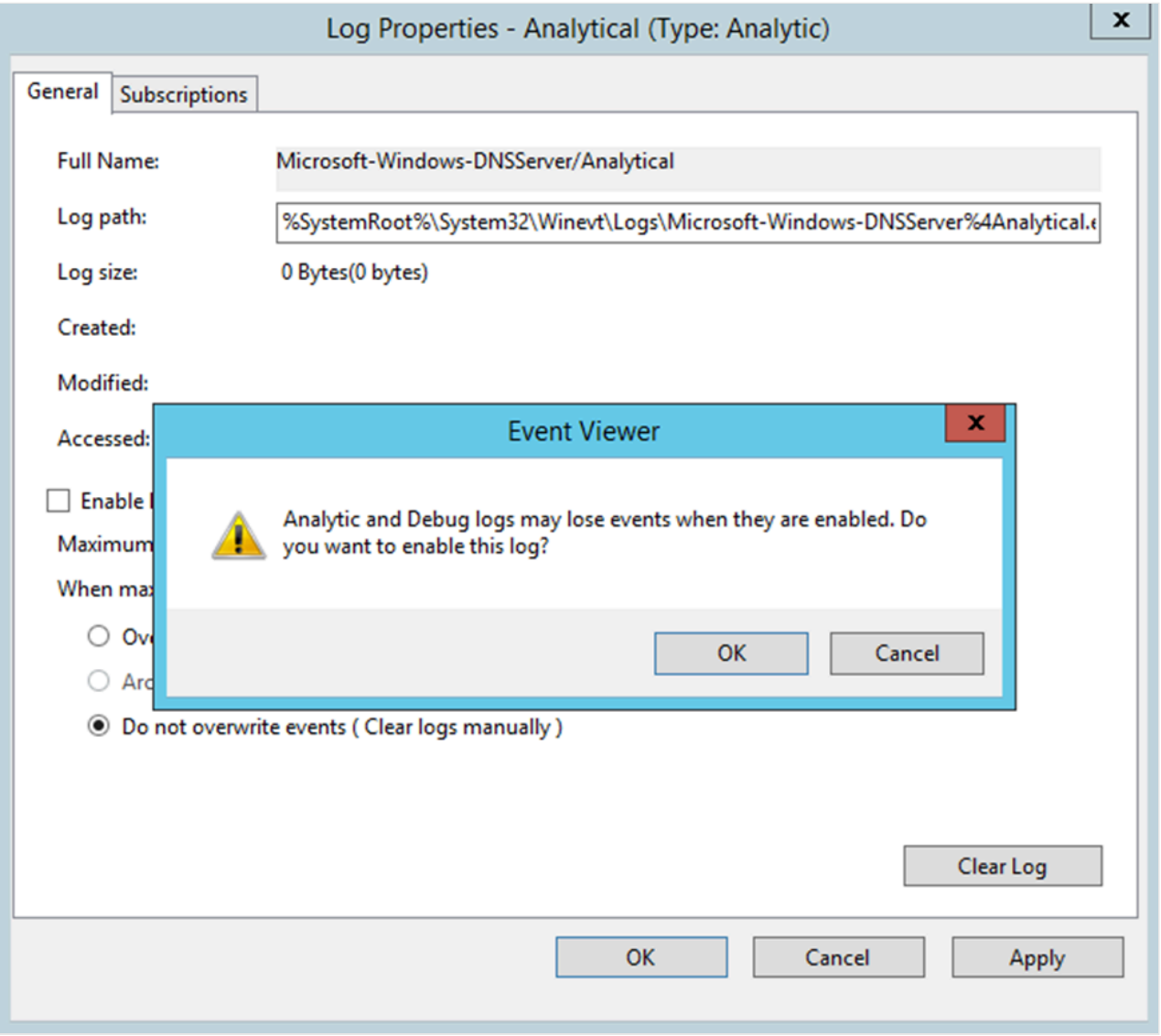
1. Dans le nœud **Applications et services** > **Journaux** > **Microsoft** > **Windows** > **Serveur DNS**, sélectionnez Serveur DNS avec le bouton droit de la souris, sélectionnez **Afficher**, puis **Afficher les journaux d'analyse et de débogage**. Le journal analytique s'affiche.

2. Cliquez avec le bouton droit sur **Analytique** , puis sélectionnez **Propriétés**.

3. Si vous souhaitez interroger et afficher les journaux d'activité de l'observateur d'événements, choisissez **Lorsque la taille maximale du journal des événements est atteinte**, sélectionnez **Ne pas remplacer les événements (Effacer manuellement les journaux)**, cochez la case **Activer la journalisation**, puis cochez **OK** lorsque vous avez demandé si vous souhaitez activer ce journal.

4. Si vous souhaitez activer la journalisation circulaire, choisissez **Remplacer si nécessaire (les événements les plus anciens en premier)** et sélectionnez **Activer la journalisation**. Après avoir sélectionné **OK**, une erreur de requête s'affiche. La journalisation a lieu même si cette erreur s'affiche. L'erreur signifie uniquement que vous ne pouvez pas afficher les événements en cours de journalisation dans l'observateur d'événements.

5. Sélectionnez **OK** pour activer le journal des événements DNS Server Analytics.



Les journaux d'analyse sont écrits par défaut dans le fichier `%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.etl`. Les événements affichés dans les journaux d'événements d'audit et d'analyse du serveur DNS sont traités dans la section suivante.

Événements analytiques

Les événements analytiques de serveur DNS activent le suivi des activités sur le serveur DNS. Un événement analytique est journalisé chaque fois que le serveur envoie ou reçoit des informations DNS. Le tableau suivant récapitule les événements analytiques du serveur DNS.

Agrandir le tableau

ID de l'événement	Type	Category	Level	Texte de l'événement
257	`Response success`	Lookup	Informational	`RESPONSE_SUCCESS: TCP=%1; InterfaceIP=%2; Destination=%3; AA=%4; AD=%5; QNAME=%6; QTYPE=%7; XID=%8; DNSSEC=%9; RCODE=%10; Port=%11; Flags=%12; Scope=%13; Zone=%14; PolicyName=%15; PacketData=%17`
258	`Response failure`	Lookup	Error	`RESPONSE_FAILURE: TCP=%1; InterfaceIP=%2; Reason=%3; Destination=%4; QNAME=%5; QTYPE=%6; XID=%7; RCODE=%8; Port=%9; Flags=%10; Zone=%11; PolicyName=%12; PacketData=%14`
259	`Ignored query`	Lookup	Error	`IGNORED_QUERY: TCP=%1; InterfaceIP=%2; Reason=%3; QNAME=%4; QTYPE=%5; XID=%6; Zone=%7; PolicyName=%8`
260	`Query out`	Requête récursive	Informational	`RECURSE_QUERY_OUT: TCP=%1; Destination=%2; InterfaceIP=%3; RD=%4; QNAME=%5; QTYPE=%6; XID=%7; Port=%8; Flags=%9; ServerScope=%10; CacheScope=%11; PolicyName=%12; PacketData=%14`
261	`Response in`	Requête récursive	Informational	`RECURSE_RESPONSE_IN: TCP=%1; Source=%2; InterfaceIP=%3; AA=%4; AD=%5; QNAME=%6; QTYPE=%7; XID=%8; Port=%9; Flags=%10; ServerScope=%11; CacheScope=%12; PacketData=%14`
262	`Recursive query`	Error	`RECURSE_QUERY_TIMEOUT: TCP=%1; InterfaceIP=%2; Destination=%3;`	

ID de l'événement	Type	Category	Level	Texte de l'événement
			`QNAME=%4; QTYPE=%5; XID=%6; Port=%7; Flags=%8; ServerScope=%9; CacheScope=%10`	
263	`Update in`	Mise à jour dynamique	Informational	`DYN_UPDATE_RECV: TCP=%1; InterfaceIP=%2; Source=%3; QNAME=%4; XID=%5; Port=%6; Flags=%7; SECURE=%8; PacketData=%10`
264	`Update response`	Mise à jour dynamique	Informational	`DYN_UPDATE_RESPONSE: TCP=%1; InterfaceIP=%2; Destination=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; RCODE=%8; PolicyName=%9; PacketData=%11`
265	`IXFR request out`	Zone XFR	Informational	`IXFR_REQ_OUT: TCP=%1; InterfaceIP=%2; Source=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; PacketData=%9`
266	`IXFR request in`	Zone XFR	Informational	`IXFR_REQ_RECV: TCP=%1; InterfaceIP=%2; Source=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; PacketData=%9`
267	`267 IXFR response out`	Zone XFR	Informational	`IXFR_RESP_OUT: TCP=%1; InterfaceIP=%2; Destination=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; RCODE=%8; PacketData=%10`
268	`IXFR response in`	Zone XFR	Informational	`IXFR_RESP_RECV: TCP=%1; InterfaceIP=%2; Destination=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; RCODE=%8; PacketData=%10`
269	`AXFR request out`	Zone XFR	Informational	`AXFR_REQ_OUT: TCP=%1; Source=%2; InterfaceIP=%3; QNAME=%4; XID=%5;`

ID de l'événement	Type	Category	Level	Texte de l'événement
				`ZoneScope=%6; Zone=%7; PacketData=%9`
270	`AXFR request in`	Zone XFR	Informational	`AXFR_REQ_RECV: TCP=%1; Source=%2; InterfaceIP=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; PacketData=%9`
271	`AXFR response out`	Zone XFR	Informational	`AXFR_RESP_OUT: TCP=%1; InterfaceIP=%2; Destination=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; RCODE=%8`
272	`AXFR response in`	Zone XFR	Informational	`AXFR_RESP_RECV: TCP=%1; InterfaceIP=%2; Destination=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; RCODE=%8`
273	`XFR notification in`	Zone XFR	Informational	`XFR_NOTIFY_RECV: Source=%1; InterfaceIP=%2; QNAME=%3; ZoneScope=%4; Zone=%5; PacketData=%7`
274	`XFR notification out`	Zone XFR	Informational	`XFR_NOTIFY_OUT: Destination=%1; InterfaceIP=%2; QNAME=%3; ZoneScope=%4; Zone=%5; PacketData=%7`
275	`XFR notify ACK in`	Zone XFR	Informational	`XFR_NOTIFY_ACK_IN: Source=%1; InterfaceIP=%2; PacketData=%4`
276	`XFR notify ACK out`	Zone XFR	Informational	`XFR_NOTIFY_ACK_OUT: Destination=%1; InterfaceIP=%2; Zone=%3; PacketData=%5`
277	`Update forward`	Mise à jour dynamique	Informational	`DYN_UPDATE_FORWARD: TCP=%1; ForwardInterfaceIP=%2; Destination=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; RCODE=%8; PacketData=%10`

ID de l'événement	Type	Category	Level	Texte de l'événement
278	`Update response in`	Mise à jour dynamique	Informational	`DYN_UPDATE_RESPONSE_IN: TCP=%1; InterfaceIP=%2; Source=%3; QNAME=%4; XID=%5; ZoneScope=%6; Zone=%7; RCODE=%8; PacketData=%10`
279	`Internal lookup CNAME`	Lookup	Informational	`INTERNAL_LOOKUP_CNAME: TCP=%1; InterfaceIP=%2; Source=%3; RD=%4; QNAME=%5; QTYPE=%6; Port=%7; Flags=%8; XID=%9; PacketData=%11`
280	`Internal lookup`	Lookup	Informational	`INTERNAL_LOOKUP_ADDITIONAL: TCP=%1; InterfaceIP=%2; Source=%3; RD=%4; QNAME=%5; QTYPE=%6; Port=%7; Flags=%8; XID=%9; PacketData=%11`

Suivi d'événements

Les journaux DNS sont compatibles avec le suivi des événements pour les applications grand public Windows (ETW), telles que logman, tracelog et analyseur de messages. Pour plus d'informations sur l'utilisation du suivi d'événements, consultez À propos du suivi d'événements.

Vous pouvez utiliser les consommateurs ETW tels que `tracelog.exe` avec l'audit du serveur DNS et les événements analytiques en spécifiant un GUID de `{EB79061A-A566-4698-9119-3ED2807060E7}`.

Vous pouvez obtenir `tracelog.exe` en téléchargeant et en installant le Kit de pilotes Windows (WDK). `Tracelog.exe` est inclus lorsque vous installez wdK, Visual Studio et le Kit de développement logiciel (SDK) Windows pour les applications de bureau. Pour plus d'informations sur le téléchargement des kits, consultez Téléchargements matériels Windows. Par exemple, lorsque vous téléchargez et installez windows Driver Kit (WDK) et acceptez le chemin d'installation par défaut, `tracelog.exe` est disponible sur : `C:\Program Files (x86)\WindowsKits\10\bin\10.0.26100.0\x64\tracelog.exe`.

Pour plus d'informations sur l'utilisation de `tracelog.exe`, consultez syntaxe de commande Tracelog.

Les exemples suivants montrent comment utiliser `tracelog.exe` avec les journaux d'événements d'audit et d'analyse DNS :

La commande suivante active à la fois la journalisation analytique et d'audit :

PowerShell

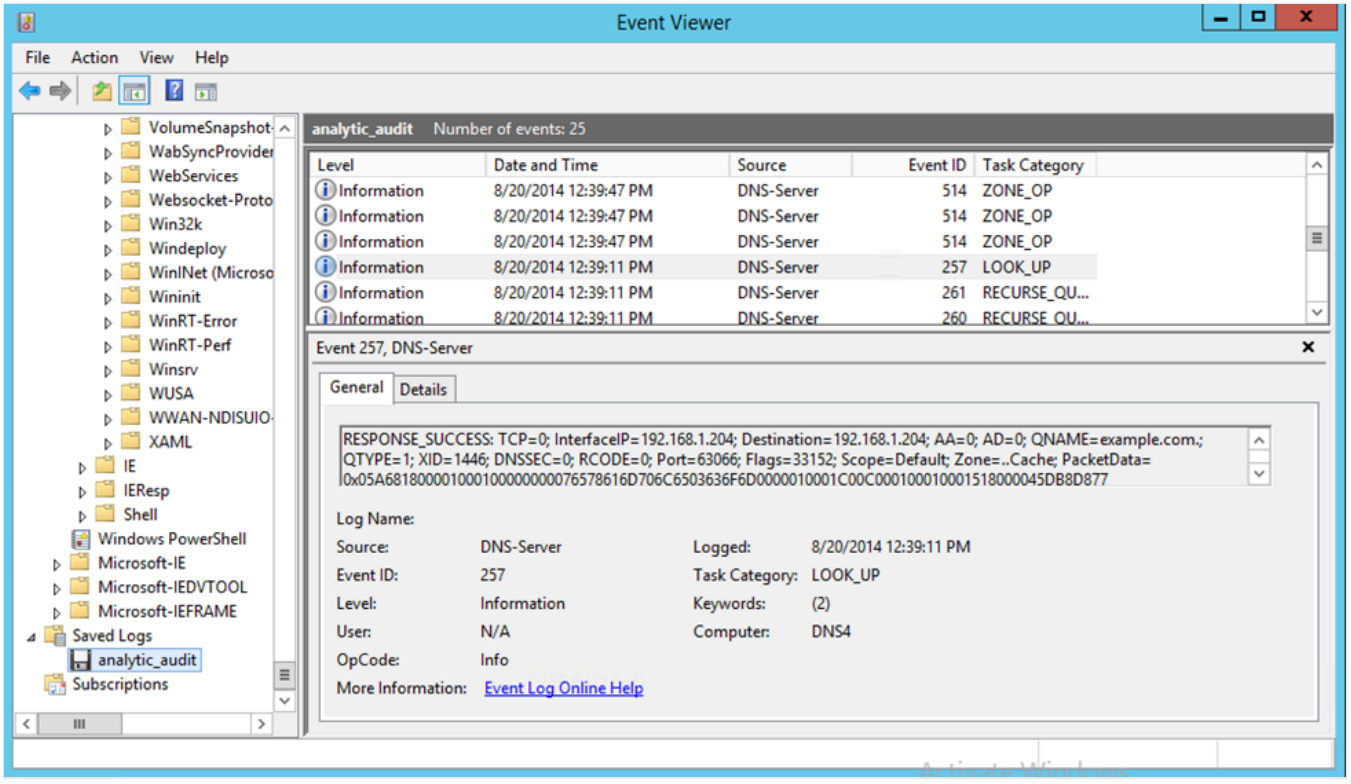
```
tracelog.exe -start Dns -guid #{EB79061A-A566-4698-9119-3ED2807060E7} -level 5 -
matchanykw 0xFFFFFFFF -f C:\analytic_audit.etl
```

Pendant que la trace est active, tous les événements d'analyse et d'audit sont enregistrés dans le fichier **C :\analytic_audit.etl** spécifié sur la ligne de commande. Vous pouvez arrêter le suivi en émettant une commande d'arrêt :

Invite de commandes Windows

```
tracelog –stop Dns
```

Après avoir arrêté la trace, vous pouvez afficher le fichier .etl dans l'Observateur d'événements en sélectionnant **Action** , puis en sélectionnant **Ouvrir le journal enregistré**.



L'exemple suivant active uniquement le canal analytique et correspond uniquement aux mots clés à `0x7FFFF` :

Invite de commandes Windows

```
tracelog.exe -start Dns -guid #{EB79061A-A566-4698-9119-3ED2807060E7} -level 5 -
matchanykw 0x7FFFF -f C:\analytic.etl
```

Un niveau de journalisation de 5 est utilisé dans les exemples précédents. Le tableau suivant présente les niveaux de journalisation disponibles.

Agrandir le tableau

Niveau de journalisation	Description
0 (Aucun)	Journalisation OFF
1 (Critique)	Seuls les événements critiques sont enregistrés, par exemple la sortie ou l'arrêt du processus. Si aucun niveau de journalisation n'est donné, le niveau 1 est utilisé par défaut.
2 (Erreur)	Seuls les événements d'erreur graves sont enregistrés, par exemple les échecs d'exécution d'une tâche requise.
3 (Avertissement)	Erreurs pouvant entraîner un problème de service, mais qui sont acceptables ou récupérables. Par exemple, la première tentative de contact avec un redirecteur échoue.
4 (Information)	Les événements de haut niveau sont enregistrés dans le journal des événements. Ces événements peuvent inclure un message pour chaque tâche majeure effectuée par le service. Utilisez ce paramètre pour commencer une enquête lorsque l'emplacement du problème est en doute. Par exemple, un thread de nettoyage a été lancé.
5 (détaillé)	Tous les événements sont enregistrés. Le niveau 5 fournit un journal complet de l'opération du service. Utilisez ce niveau lorsque le problème est suivi d'une catégorie particulière ou d'un petit ensemble de catégories.

Considérations relatives aux performances

Les performances du serveur DNS peuvent être affectées lorsque la journalisation est activée, mais la fonctionnalité de journalisation et de diagnostic DNS améliorée dans Windows Server est conçue pour réduire l'impact sur les performances. Cet article traite des considérations relatives aux performances du serveur DNS lorsque la journalisation est activée.

Journalisation du débogage

Avant l'introduction des journaux d'analyse DNS, la journalisation du débogage DNS était une méthode disponible pour surveiller les transactions DNS. La journalisation de débogage DNS n'est pas la même que la fonctionnalité améliorée de journalisation et de diagnostic DNS présentée dans cet article. La journalisation de débogage est un outil qui peut également être utilisé pour la journalisation et les diagnostics DNS. Le journal de débogage DNS fournit des données détaillées sur toutes les informations DNS envoyées et reçues par le serveur DNS. Les informations collectées sont similaires aux données qui peuvent être collectées à l'aide d'outils de capture de paquets tels que le moniteur réseau.

Par défaut, toutes les options de journalisation de débogage sont désactivées. Lorsqu'il est activé de manière sélective, le service serveur DNS peut effectuer la journalisation au niveau du suivi des types d'événements ou de messages sélectionnés pour la résolution des problèmes et le débogage généraux du serveur.

La journalisation du débogage peut être gourmande en ressources, affectant les performances globales du serveur et consommant de l'espace disque. Par conséquent, elle ne doit être utilisée temporairement que lorsque des informations plus détaillées sur les performances du serveur sont nécessaires.

> **Conseil**
>
> `Dns.log` contient les logs de débogage. Par défaut, le journal de débogage DNS se trouve dans le `%windir%\system32\dns` répertoire.

Vous pouvez activer la journalisation du débogage à l'aide de l'expérience utilisateur ou de PowerShell. Utilisez les méthodes suivantes pour activer la journalisation des événements de diagnostic et modifier d'autres paramètres du journal des événements. Sélectionnez la méthode qui correspond le mieux à vos besoins.

Expérience de bureau

Les étapes suivantes montrent comment activer la journalisation du débogage à l'aide de l'expérience de bureau. Pour sélectionner et activer les options de journalisation de débogage sur le serveur DNS, procédez comme suit :

1. Sélectionnez **Démarrer**, tapez **le Gestionnaire DNS**, puis sélectionnez **Le Gestionnaire DNS** dans la liste de correspondances optimale.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur le serveur DNS applicable, puis sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Débogage de journalisation** .

4. Dans la boîte de dialogue **Propriétés** , cochez les **paquets de journal pour le débogage** , puis sélectionnez les événements que vous souhaitez enregistrer pour la journalisation du débogage.

Les options de journalisation de débogage DNS suivantes sont disponibles :

- **Direction des paquets**

  Envoi : les paquets envoyés par le serveur DNS sont enregistrés dans le fichier journal du serveur DNS.

  Réception : les paquets reçus par le serveur DNS sont enregistrés dans le fichier journal.

- Contenu **des paquets**

  Requêtes standard : spécifie que les paquets contenant des requêtes standard (par RFC 1034) sont enregistrés dans le fichier journal du serveur DNS.

  Mises à jour : spécifie que les paquets contenant des mises à jour dynamiques (par RFC 2136) sont enregistrés dans le fichier journal du serveur DNS.

  Notifications : spécifie que les paquets contenant des notifications (par RFC 1996) sont enregistrés dans le fichier journal du serveur DNS.

- **Protocole de transport**

  UDP : spécifie que les paquets envoyés et reçus via UDP sont enregistrés dans le fichier journal du serveur DNS.

  TCP : spécifie que les paquets envoyés et reçus via TCP sont enregistrés dans le fichier journal du serveur DNS.

- **type de paquets**

  Requête : spécifie que les paquets de requête sont enregistrés dans le fichier journal du serveur DNS (un paquet de requête est caractérisé par un bit QR défini sur 0 dans l'en-tête du message DNS).

  Réponse : spécifie que les paquets de réponse sont enregistrés dans le fichier journal du serveur DNS (un paquet de réponse est caractérisé par un bit QR défini sur 1 dans l'en-tête du message DNS).

- **Activer le filtrage en fonction de l'adresse IP** Fournit le filtrage des paquets enregistrés dans le fichier journal du serveur DNS. Cette option permet la

journalisation des paquets envoyés à partir d'adresses IP spécifiques à un serveur DNS ou d'un serveur DNS vers des adresses IP spécifiques.

- **Nom de fichier** : vous permet de spécifier le nom et l'emplacement du fichier journal du serveur DNS.

  Par exemple:

  - **dns.log** spécifie que le fichier journal du serveur DNS doit être enregistré en tant que **dns.log** dans le `<systemroot>zSystem32Dns directory`. N'oubliez pas de remplacer `<systemroot>` par le chemin d'accès réel au répertoire Windows sur votre ordinateur.

  - **temp\dns.log** spécifie que le fichier journal du serveur DNS doit être enregistré en tant que **dns.log** dans le `<systemroot>\Temp directory`. N'oubliez pas de remplacer `<systemroot>` par le chemin d'accès réel au répertoire Windows sur votre ordinateur.

- **limite de taille maximale du fichier journal** vous permet de définir la taille de fichier maximale pour le fichier journal du serveur DNS. Lorsque la taille maximale spécifiée du fichier journal du serveur DNS est atteinte, le serveur DNS remplace les informations de paquet les plus anciennes avec de nouvelles informations. Remarque : Si elle n'est pas spécifiée, la taille du fichier journal du serveur DNS peut prendre une grande quantité d'espace disque.

Transférer le rôle principal de clé

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Cet article explique comment transférer le rôle maître de clé DNSSEC entre les serveurs DNS faisant autorité dans les environnements Windows DNS Server. DnsSEC Key Master est le serveur DNS responsable de la génération et de la gestion des clés pour une zone signée DNSSEC. Pour une compréhension complète du rôle Principal de clé, de ses exigences et des concepts de gestion des clés, consultez DNSSEC Key Master.

Vous souhaiterez peut-être transférer dans les scénarios suivants :

- Vous souhaitez remplacer le maître de clé par un autre serveur DNS faisant autorité à des fins d'équilibrage de charge ou d'administration.
- Vous effectuez une maintenance sur le maître de clé actuel et devez transférer temporairement le rôle vers un autre serveur.
- Vous migrez vers un nouveau serveur DNS et souhaitez transférer le rôle Principal de clé dans le cadre du processus de migration.

Si le maître de clé actuel est hors connexion et que vous devez gérer les opérations de signature DNSSEC, vous devez saisir le rôle Principal de clé pour garantir la continuité du service.

Prerequisites

Pour transférer le rôle principal de clé, votre environnement doit répondre aux exigences suivantes :

- Les serveurs DNS faisant autorité principale doivent prendre en charge la signature de zone.
- Les serveurs DNS principaux et secondaires faisant autorité doivent prendre en charge l'hébergement de zones signées.
- Les serveurs DNS récursifs ou de transfert doivent prendre en charge la validation DNSSEC des réponses DNS.
- Un autre serveur DNS éligible doit être disponible sur le réseau.
- Vous devez disposer de privilèges d'administration sur le serveur DNS où vous souhaitez transférer le rôle principal de clé.
- (Facultatif) Vous devez disposer de droits de groupe Administrateurs de domaine ou être membre d'un groupe disposant d'autorisations équivalentes pour qu'il apparaisse dans la liste des maîtres de clés disponibles.

> **Important**
>
> Vous ne pouvez pas transférer le rôle principal de clé si une zone est basée sur des fichiers, car ces zones n'ont qu'un seul serveur DNS principal faisant autorité. Dans ce scénario, il est recommandé de prendre d'autres précautions de sécurité pour protéger le maître de clé contre les attaques et pour protéger le matériel de clé privée de devenir compromis ou perdu. Pour des raisons de sécurité, une clé principale qui n'est pas un contrôleur de domaine ne doit avoir que le rôle serveur DNS installé pour limiter sa surface d'attaque.

Rechercher le maître de clé actuel

Pour rechercher le maître de clé actuel pour une zone DNS, vous pouvez utiliser le Gestionnaire DNS ou Windows PowerShell. Sélectionnez votre méthode préférée.

Gestionnaire DNS

Pour rechercher le masque de clés à l'aide du Gestionnaire DNS, procédez comme suit :

1. Ouvrez le Gestionnaire DNS sur un serveur DNS principal faisant autorité ou connectez-vous à un serveur DNS principal faisant autorité à partir d'un autre emplacement à l'aide du Gestionnaire DNS.
2. Dans l'arborescence de la console, développez **Zones de recherche vers l'avant** ou **les zones de recherche inverse**.
3. Cliquez avec le bouton droit sur la zone pour laquelle vous souhaitez rechercher le masque de clé, développez **DNSSEC**, puis sélectionnez **Propriétés**.
4. Le nom du masque de clé s'affiche dans le champ **Maître** de clé s'affiche sous l'onglet **Maître** de clé de la page des propriétés DNSSEC.

Transférer le masque de clé

Lorsque le maître de clé est en ligne, vous pouvez transférer le rôle Principal de clé vers un autre serveur DNS. Ce processus nécessite qu'un autre serveur DNS éligible soit disponible sur le réseau.

Une zone non signée peut également être affectée à une clé principale. Toutes les zones signées ont un paramètre Key Master, qu'elles soient actuellement signées ou non. Une zone

qui n'a jamais été signée n'a généralement pas de clé principale. Toutefois, vous pouvez affecter une clé principale à l'avance à l'aide de Windows PowerShell pour préparer la signature de zone.

Vous pouvez transférer le rôle Principal de clé vers un autre serveur DNS à l'aide du Gestionnaire DNS ou de Windows PowerShell. Sélectionnez votre méthode préférée.

Gestionnaire DNS

Pour déplacer le rôle principal de clé à l'aide du Gestionnaire DNS, procédez comme suit :

1. Ouvrez le Gestionnaire DNS sur un serveur DNS principal faisant autorité ou connectez-vous à un serveur DNS principal faisant autorité à partir d'un autre emplacement à l'aide du Gestionnaire DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone pour laquelle vous envisagez de déplacer le rôle Principal de clé, pointez sur **DNSSEC**, puis sélectionnez **Propriétés**.
3. Sous l'onglet Maître de la **clé** , sélectionnez **Utiliser le serveur DNS suivant comme maître de clé**.
4. Sélectionnez la liste déroulante, puis sélectionnez **Oui** dans la fenêtre contextuelle qui s'affiche. Le serveur DNS local crée une liste de serveurs DNS capables d'être le nouveau maître de clé pour la zone.
5. Choisissez un serveur DNS dans la liste pour le nouveau maître de clé, puis sélectionnez **OK**.
6. Sélectionnez **Oui** dans la boîte de dialogue qui s'affiche pour déplacer le rôle principal de clé vers le serveur DNS qui a été choisi. Si vous sélectionnez **Non**, l'opération est annulée et la clé principale reste inchangée.
7. Vérifiez que **la clé principale de la zone** `<zone name>` **a été mise à jour** correctement s'affiche, puis sélectionnez **OK**.

La procédure modifie immédiatement la clé principale. Vous n'avez pas besoin d'attendre la réplication Active Directory ou de réinscrire la zone.

Saisie du rôle principal de clé (transfert hors connexion)

Si la clé principale est hors connexion et que vous ne pouvez pas la ramener en ligne facilement, vous pouvez transférer le rôle Principal de clé vers un autre serveur DNS. Ce processus est appelé *saisie* du rôle Principal de clé. Ne saisissez pas le rôle principal de clé et transférez-le hors connexion, sauf s'il est inévitable, par exemple dans un scénario de récupération d'urgence.

Vous pouvez saisir le rôle Principal de clé à l'aide du Gestionnaire DNS ou de Windows PowerShell. Sélectionnez votre méthode préférée.

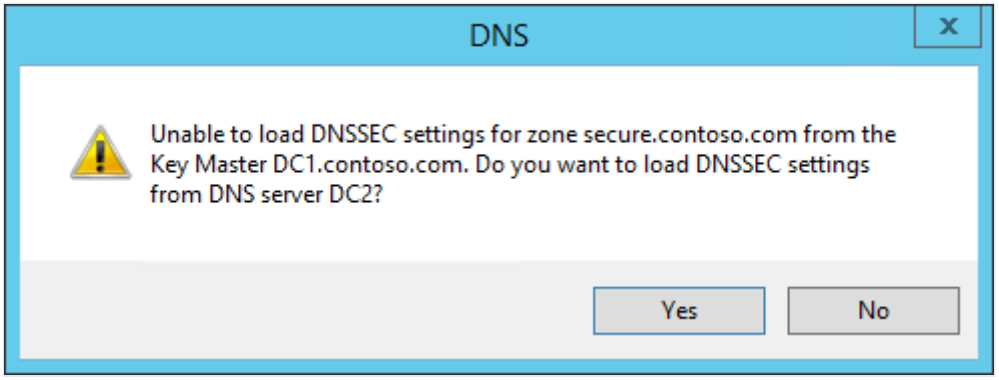
Gestionnaire DNS

Pour saisir le rôle Principal de clé à l'aide du Gestionnaire DNS

1. Ouvrez le Gestionnaire DNS sur un serveur DNS principal faisant autorité ou connectez-vous à un serveur DNS principal faisant autorité à partir d'un autre emplacement à l'aide du Gestionnaire DNS.

2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone pour laquelle vous envisagez de déplacer le rôle Principal de clé, pointez sur **DNSSEC**, puis sélectionnez **Propriétés**.

3. Une alerte s'affiche indiquant que les paramètres DNSSEC de la zone n'ont pas pu être chargés à partir du maître de clé, sélectionnez **Oui**.



> **Attention**
>
> Si vous ne voyez pas d'alerte, vérifiez que la clé principale est hors connexion. Si le maître de clé est en ligne et que vous souhaitez toujours déplacer le rôle Principal de clé, consultez la section Transférer une clé principale en ligne. Ne saisissez pas le rôle Principal de clé.

4. Sous l'onglet Maître de la **clé** , sélectionnez **Utiliser le serveur DNS suivant comme maître de clé**.

5. Sélectionnez la liste déroulante, puis sélectionnez **Oui** dans la fenêtre contextuelle qui s'affiche. Le serveur DNS local crée une liste de serveurs DNS capables d'être le nouveau maître de clé pour la zone.

6. Choisissez un serveur DNS dans la liste pour le nouveau maître de clé, puis sélectionnez **OK**.

7. Sélectionnez **Oui** dans la boîte de dialogue qui s'affiche pour déplacer le rôle principal de clé vers le serveur DNS choisi. Si vous sélectionnez **Non**, l'opération est annulée et la clé principale reste inchangée.

8. Si vous voyez un avertissement de boîte de dialogue indiquant que le maître de clé ne peut pas être contacté pour transférer du matériel de clé privée, le serveur DNS actuel n'a pas accès aux clés de signature. Pour en savoir plus sur ce scénario, consultez la section Transfert sans accès aux clés de signature.

9. Vérifiez que **la clé principale de la zone `<zone name>` a été mise à jour** correctement s'affiche, puis sélectionnez **OK**.

La procédure modifie immédiatement le masque de clé. Vous n'avez pas besoin d'attendre la réplication Active Directory ou de réinscrire la zone.

Transférer sans accès aux clés de signature

Si le maître de clé actuel est hors connexion et que le nouveau maître de clé ne peut pas accéder aux clés privées, vous devez générer de nouvelles clés et signer à nouveau la zone. Pour plus d'informations sur les options de stockage de clés privées, consultez Clés de signature.

Pour éviter une situation où le maître de clé est hors connexion et que vous ne pouvez pas accéder au matériel de clé privée, il est recommandé de stocker du matériel de clé privée dans Active Directory. De cette façon, si le maître de clé passe hors connexion, vous pouvez saisir le rôle principal de clé sur un autre serveur DNS qui a accès au matériel de clé privée. Lors de la signature de la zone, utilisez la **réplication de cette clé privée sur tous les serveurs DNS faisant autorité pour cette** option de zone dans les paramètres de clé de signature de clé (KSK). Cette option garantit que le matériel de clé privée est répliqué sur tous les serveurs DNS faisant autorité pour la zone, le rendant disponible pour une utilisation par l'un de ces serveurs.

Si vous ne souhaitez pas stocker de matériel de clé privée dans Active Directory, vous pouvez également fournir l'accès au matériel de clé privée à l'aide d'un certificat ou d'un appareil de module de stockage matériel (HSM). Pour en savoir plus sur les options de stockage du matériel de clé privée, consultez Clés de signature.

Une fois que vous avez saisi le rôle Principal de clé, procédez comme suit :

1. Si le matériel de clé privée n'est pas stocké dans Active Directory ou un appareil externe, exécutez la commande New-SelfSignedCertificate dans PowerShell pour stocker ce matériel dans un certificat sur l'ordinateur local.

   PowerShell

   ```
   New-SelfSignedCertificate `
     -DnsName "YourDNSName" `
     -CertStoreLocation "Cert:\LocalMachine\MS-DNSSEC" `
     -KeyExportPolicy Exportable
   ```

2. Réinscrire la zone à l'aide des nouvelles clés. Pour en savoir plus sur la réinscrire la zone, consultez Signer des zones DNS avec DNSSEC.

3. Si la zone a des ancres d'approbation, vous devez également les remplacer. Pour en savoir plus sur la distribution d'ancres d'approbation, consultez Distribuer des ancres d'approbation dans Active Directory.

Si la clé principale d'origine devient disponible avant la nouvelle signature de la zone, vous pouvez transférer le rôle principal de clé vers ce serveur sans avoir à signer à nouveau la zone et redistribuer les ancres d'approbation.

Contenu connexe

- En savoir plus sur le maître de clé DNSSEC
- Vue d'ensemble de DNSSEC

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Signer des zones DNS avec DNSSEC

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

DNSSEC (Extensions de sécurité du système de noms de domaine) protège les zones DNS contre la falsification et garantit l'intégrité des données en ajoutant des signatures de chiffrement aux enregistrements DNS. Cet article guide les administrateurs DNS tout au long du processus de signature de zones DNS avec DNSSEC sur Windows Server.

La signature d'une zone avec DNSSEC ajoute plusieurs nouveaux enregistrements de ressources associés à DNSSEC. Ces nouveaux enregistrements de ressources peuvent être envoyés en réponse aux requêtes DNS pour la zone, ainsi que les enregistrements de ressources traditionnels non liés à DNSSEC. Les serveurs DNS doivent demander spécifiquement que les enregistrements DNSSEC soient inclus dans les réponses DNS. Par conséquent, les serveurs qui ne prennent pas en charge DNSSEC reçoivent uniquement les enregistrements de ressources traditionnels dans une réponse DNS.

Une zone signée peut être une zone de recherche vers l'avant ou inverse, une zone statique ou dynamique et peut être intégrée à Active Directory ou sauvegardée par un fichier. Si la zone est intégrée à Active Directory, les clés de signature de zone privée sont répliquées automatiquement sur tous les serveurs DNS principaux de clé principale via la réplication Active Directory. Chaque serveur qui fonctionne comme Key Master signe sa propre copie de la zone lorsqu'il reçoit la clé. Pour optimiser les performances et empêcher l'augmentation de la taille du fichier de base de données Active Directory, la copie signée de la zone reste en mémoire pour les zones intégrées à Active Directory. Une zone signée DNSSEC est validée uniquement sur le disque pour les zones sauvegardées par fichier.

Paramètres de signature

Avant de pouvoir signer une zone avec DNSSEC, vous devez choisir les valeurs de paramètre DNSSEC utilisées pour la signature. Les paramètres que vous choisissez déterminent la façon dont la zone est signée et la façon dont DNSSEC fonctionne pour la zone.

Choisir d'utiliser les paramètres ou paramètres par défaut d'une zone existante ignore les pages de paramètres personnalisées. Certaines valeurs de paramètre peuvent également être modifiées une fois la zone signée si vous le souhaitez.

Les options suivantes sont disponibles pour spécifier les valeurs de paramètre DNSSEC utilisées pour la signature de zone :

- Personnaliser les paramètres de signature de zone (option par défaut)

  Si vous choisissez cette option, l'Assistant affiche plusieurs pages que vous pouvez utiliser pour des valeurs de paramètres différentes et vous fournit des valeurs par défaut pour chaque paramètre. Ces valeurs peuvent également être modifiées en n'importe quelle valeur dans une plage acceptable. Si la zone a été précédemment signée, puis non signée, les paramètres qui ont été utilisés le plus récemment sont fournis comme valeurs par défaut.

- Paramètres existants

  Pour utiliser cette option, le serveur DNS doit déjà faire autorité pour une ou plusieurs zones signées DNSSEC. Si vous choisissez cette option, vous devez fournir le nom d'une zone signée à utiliser comme modèle pour signer la zone active. Si la zone a été précédemment signée, les paramètres utilisés pour signer la zone sont fournis comme valeurs par défaut.

- Paramètres par défaut

  Si vous choisissez cette option, la zone est signée avec les paramètres par défaut. Ces paramètres apparaissent par défaut lorsque vous choisissez de personnaliser les paramètres de signature de zone. Si la zone a été signée avant avec différents paramètres, les paramètres les plus récents sont affichés à la place. Si vous choisissez de signer la zone avec les paramètres par défaut, l'Assistant passe à la page récapitulative.

Algorithmes de chiffrement et méthodes NSEC

Si vous utilisez des paramètres personnalisés pour signer une zone avec DNSSEC, vous devez choisir les algorithmes de chiffrement et les méthodes sécurisées suivantes (NSEC) utilisées pour la signature de clés. L'algorithme de chiffrement détermine la façon dont les clés sont générées et utilisées, tandis que la méthode NSEC détermine la façon dont le déni d'existence authentifié est fourni dans la zone signée.

Plusieurs algorithmes de chiffrement sont disponibles pour une utilisation dans une clé KSK ou ZSK. Vous pouvez utiliser différents algorithmes pour les clés de signature de clés (KSK) et les clés de signature de zone (ZSK). Toutefois, vous ne pouvez pas signer de zone si une clé utilise l'algorithme RSA/SHA-1 (NSEC3), tandis qu'une autre clé utilise l'algorithme RSA/SHA-1. Ces deux algorithmes de chiffrement sont incompatibles.

Le tableau suivant présente les algorithmes de chiffrement et les méthodes NSEC compatibles.

Agrandir le tableau

Algorithm	Méthodes NSEC compatibles
ECDSAP256/SHA-256	NSEC, NSEC3
ECDSAP384/SHA-384	NSEC, NSEC3
RSA/SHA-1	NSEC
RSA/SHA-1 (NSEC3)	NSEC3
RSA/SHA-256	NSEC, NSEC3
RSA/SHA-512	NSEC, NSEC3

Notes

Vous ne pouvez pas utiliser NSEC pour refuser l'existence authentifiée si vous avez choisi RSA/SHA-1 (NSEC3) comme algorithme de chiffrement dans n'importe quel KSK ou ZSK. Vous ne pouvez pas également utiliser NSEC3 si vous utilisez RSA/SHA-1 avec une clé de signature.

Vous devez avoir au moins un (1) KSK et un (1) ZSK. Vous pouvez avoir jusqu'à trois (3) KSK et trois (3) ZSK qui utilisent le même algorithme de chiffrement, et vous avez plusieurs algorithmes de chiffrement.

Pour prendre en charge la substitution automatique des clés, une autre clé de signature est générée pour chaque ZSK et KSK ajouté à la zone. Pour la substitution automatique de KSK, seule la méthode de substitution de signature double est prise en charge. Pour la substitution ZSK automatique, seule la méthode de substitution de prépublier est prise en charge.

En règle générale, une zone est signée avec une seule zone ZSK et une seule KSK. Vous pouvez utiliser plusieurs touches pour signer une zone dans les circonstances suivantes :

1. Tous les validateurs DNS ne prennent pas en charge un seul algorithme de chiffrement.
2. Vous effectuez la transition de l'infrastructure DNS pour utiliser de nouvelles propriétés de clé de signature.
3. Vous fusionnez des zones DNS ou des éléments réseau qui utilisent différentes propriétés de clé de signature.

Chaque clé de signature supplémentaire et algorithme de chiffrement que vous ajoutez augmente le temps et le coût de calcul de la signature de zone.

Prerequisites

Avant de pouvoir signer une zone avec DNSSEC, vous devez respecter les conditions préalables suivantes :

- Le rôle serveur DNS doit être installé et configuré.
- Les outils d'administration à distance du serveur DNS doivent être installés sur l'ordinateur que vous utilisez pour signer la zone.
- Le serveur DNS doit être un serveur DNS principal faisant autorité pour la zone que vous souhaitez signer. Les enregistrements de ressources liés à DNSSEC sont transférés vers des serveurs secondaires, mais vous ne pouvez pas signer, afficher ou modifier les propriétés DNSSEC d'une zone secondaire.
- La zone DNS doit être non signée. Si la zone est déjà signée, vous devez l'annuler avant de pouvoir la signer à nouveau.
- Vous devez disposer de privilèges d'administration sur le serveur DNS pour signer une zone. Si le serveur DNS est intégré à Active Directory, vous devez également disposer d'informations d'identification d'administrateur de domaine ou équivalentes pour signer une zone.

Signature d'une zone

Sur un serveur DNS exécutant Windows Server, vous pouvez utiliser le Gestionnaire DNS ou Windows PowerShell pour signer une zone.

- Gestionnaire DNS. L'Assistant Signature de zone fournit une interface pas à pas pour entrer les paramètres DNSSEC et lancer la signature de zone. Si la zone est déjà signée, vous pouvez également afficher ou modifier des paramètres et réinscrire une zone à l'aide de la page de propriétés DNSSEC. Un Assistant zone unsign est également fourni pour supprimer les enregistrements signés DNSSEC d'une zone.

- Windows PowerShell. De nombreuses applets de commande sont disponibles pour signer et annuler l'attribution de zones DNS et pour afficher ou modifier des paramètres DNSSEC.

Les deux méthodes pour la signature de zone sont compatibles entre elles. Vous pouvez signer une zone avec le Gestionnaire DNS et afficher ou modifier les paramètres avec Windows PowerShell, et vice versa.

Conseil

- Dans l'arborescence de la console du Gestionnaire DNS, les zones signées avec DNSSEC sont indiquées avec une icône de verrouillage.

- La durée nécessaire pour signer une zone dépend des paramètres que vous spécifiez et de la taille de la zone.

Pour commencer à signer une zone, sélectionnez votre méthode préférée :

Gestionnaire DNS

Pour signer une zone DNS à l'aide du Gestionnaire DNS, procédez comme suit :

1. Ouvrez le Gestionnaire DNS sur un serveur DNS principal faisant autorité.
2. Pour démarrer **l'Assistant Signature** de zone dans le Gestionnaire DNS, cliquez avec le bouton droit sur une zone DNS directe ou inversée sur un serveur DNS principal faisant autorité, pointez sur **DNSSEC**, puis choisissez **Signer la zone**.
3. Dans la page d'accueil de l'Assistant Signature de zone, passez en revue les informations DNSSEC, puis sélectionnez **Suivant**.
4. Sélectionnez l'une des trois options de signature, puis sélectionnez **Suivant**. Les étapes suivantes supposent que vous choisissez la première option, **Personnaliser les paramètres de signature de zone**.
   - Personnaliser les paramètres de signature de zone (sélectionnés par défaut)
   - Signer la zone avec un nouvel ensemble de paramètres de signature de zone
   - Utiliser les paramètres par défaut pour signer la zone
5. Pour sélectionner le maître de clé, vérifiez que le serveur DNS actuel est sélectionné comme maître de clé. Vous pouvez également sélectionner **un autre serveur principal comme maître de clé** et choisir un autre serveur dans la liste déroulante. Cliquez sur **Suivant**.
6. Passez en revue les détails de KSK sur la page d'informations clé de signature (KSK), puis sélectionnez **Suivant**.
7. Pour créer une clé de signature de clé (KSK), sélectionnez **Ajouter**, renseignez les informations suivantes :

Agrandir le tableau

Paramètre	Valeur
Génération de clés	Sélectionnez l'une des options suivantes : - Générer de nouvelles clés de signature (par défaut)

Paramètre	Valeur
	- Utiliser des clés prégénérées. Si vous utilisez des clés prédéfinies, vous devez spécifier une clé active et de secours disponible à l'aide du GUID. Utilisez l'applet de commande **Get-DnsServerSigningKey** pour afficher les clés disponibles. Le GUID est également appelé KeyId.
Algorithme de chiffrement	Sélectionnez l'une des options suivantes : - RSA/SHA-256 (par défaut) - ECDSAP256/SHA-256 - ECDSAP384/SHA-384 - RSA/SHA-1 - RSA/SHA-1 (NSEC3) - RSA/SHA-512
Longueur de clé (bits)	Sélectionnez l'une des valeurs dans le menu déroulant. La valeur par défaut est 2048 bits. La longueur de la clé doit être comprise entre 1024 et 4 096 bits par incréments de 64 bits. Pour les clés ECDSA, la longueur de la clé est fixe à 256 bits ou 384 bits.
Fournisseur de stockage de clés	Sélectionnez l'une des options suivantes : - Fournisseur de stockage de clés logicielles Microsoft (par défaut) - Fournisseur de stockage de clés Microsoft Passport - Fournisseur de chiffrement de plateforme Microsoft - Fournisseur de stockage de clés de carte à puce Microsoft Si vous envisagez de distribuer les clés à l'aide des services de domaine Active Directory, vous devez choisir **le fournisseur de stockage de clés logicielles Microsoft**.
Période de validité de la signature DNSKEY RRSET (heures)	Sélectionnez l'une des options suivantes : - 168 heures (par défaut)

Paramètre	Valeur
	- 6 - 720 heures
Répliquer cette clé privée sur tous les serveurs DNS faisant autorité pour cette zone	Cochez la case pour activer cette option (par défaut). Cette option est activée par défaut. Si vous désactivez cette option, la clé privée est stockée uniquement sur le maître de la clé.
Activer la substitution de clé	Cochez la case pour activer la substitution automatique (valeur par défaut). Entrez les valeurs souhaitées - Fréquence de substitution (jours) : 755 jours (valeur par défaut) - Retarder la première substitution par (jours) : 0 jours (par défaut)

Conseil

- Un minimum d'une KSK est requis. Jusqu'à trois KSK peuvent être ajoutés pour chacun des algorithmes de chiffrement disponibles.
- Si la zone a été signée, puis non signée, les KSK et les paramètres utilisés pour signer précédemment la zone sont automatiquement fournis à nouveau.

Après avoir entré les paramètres KSK, sélectionnez **OK** pour ajouter la clé KSK à la zone. Sélectionnez **Suivant** pour continuer.

8. Dans la page d'informations de la clé de signature de zone (ZSK), passez en revue les détails de ZSK, puis sélectionnez **Suivant**.
9. Pour créer une clé de signature de zone (ZSK), sélectionnez **Ajouter**, renseignez les informations suivantes :

Agrandir le tableau

Paramètre	Valeur
Algorithme de chiffrement	Sélectionnez l'une des options suivantes : - RSA/SHA-256 (par défaut)

Paramètre	Valeur
	- ECDSAP256/SHA-256 - ECDSAP384/SHA-384 - RSA/SHA-1 - RSA/SHA-1 (NSEC3) - RSA/SHA-512
Longueur de clé (bits)	Sélectionnez l'une des valeurs dans le menu déroulant. La valeur par défaut est 1 024 bits. La longueur de la clé doit être comprise entre 1024 et 4 096 bits par incréments de 64 bits. Pour les clés ECDSA, la longueur de la clé est fixe à 256 bits ou 384 bits.
Fournisseur de stockage de clés	Sélectionnez l'une des options suivantes : - Fournisseur de stockage de clés logicielles Microsoft (par défaut) - Fournisseur de stockage de clés Microsoft Passport - Fournisseur de chiffrement de plateforme Microsoft - Fournisseur de stockage de clés de carte à puce Microsoft Si vous envisagez de distribuer les clés à l'aide des services de domaine Active Directory, vous devez choisir **le fournisseur de stockage de clés logicielles Microsoft**.
Période de validité de signature DNSKEY (heures)	Sélectionnez l'une des options suivantes : - 168 heures (par défaut) - 6 - 720 heures
Période de validité de la signature DS (heures)	Sélectionnez l'une des options suivantes : - 168 heures (par défaut) - 6 - 720 heures

Paramètre	Valeur
Période de validité des enregistrements de zone (heures)	Sélectionnez l'une des options suivantes : - 240 heures (par défaut) - 6 - 720 heures
Activer la substitution de clé	Cochez la case pour activer la substitution automatique. La substitution est activée par défaut. Entrez les valeurs souhaitées - Fréquence de substitution (jours) : 6 - 1825 jours, 90 jours est la valeur par défaut - Retarder la première substitution par (jours) : 0 à 30 jours, 0 jours est la valeur par défaut

Conseil

- Un minimum d'une ZSK est requis. Jusqu'à trois ZSK peuvent être ajoutés pour chacun des algorithmes de chiffrement disponibles.
- Si la zone a été signée, puis non signée, les KSK et les paramètres utilisés pour signer précédemment la zone sont automatiquement fournis à nouveau.

Après avoir entré les paramètres ZSK, sélectionnez **OK** pour ajouter la ZSK à la zone. Sélectionnez **Suivant** pour continuer.

10. Si vous devez ajouter une nouvelle instance ZSK, configurez les propriétés de clé dans la boîte de dialogue Nouvelle clé de signature de zone (ZSK), puis sélectionnez **OK**.
11. Dans la page Suivant Sécurisé (NSEC), sélectionnez Utiliser NSEC3 (recommandé) ou Utiliser NSEC, configurez les itérations et la longueur de sel si vous utilisez NSEC3, puis sélectionnez **Suivant**.
12. Dans la page Ancres d'approbation (TAs), sélectionnez éventuellement **Activer la distribution des ancres d'approbation pour cette zone** et **activez la mise à jour**

automatique des ancres d'approbation sur la substitution de clé, puis sélectionnez **Suivant**.

13. Dans la page Paramètres de signature et d'interrogation, renseignez les informations suivantes :

Agrandir le tableau

Paramètre	Valeur
Algorithme de génération d'enregistrements DS	Sélectionnez l'une des options suivantes : -Tout -Aucun - SHA-1 - SHA-1 et SHA-256 (par défaut) - SHA-1 et SHA-384 - SHA-256 - SHA-256 et SHA-384 - SHA-384
Durée de vie d'enregistrement DS (secondes)	Entrez une valeur comprise entre 0 et 604800 secondes. La valeur par défaut est de 3 600 secondes.
Durée de vie de l'enregistrement DNSKEY (secondes)	Entrez une valeur comprise entre 0 et 604800 secondes. La valeur par défaut est de 3 600 secondes.
Période d'interrogation de délégation sécurisée (heures)	Entrez une valeur comprise entre 1 et 168 heures. La valeur par défaut est 12 heures.
Création de signature (heures)	Entrez une valeur comprise entre 0 et 168 heures. La valeur par défaut est 1 heure.

Après avoir entré les paramètres de signature et d'interrogation, sélectionnez **Suivant** pour continuer.

14. Pour signer la zone, passez en revue la page récapitulative qui affiche tous les paramètres DNSSEC. Si vous avez besoin d'apporter des modifications, sélectionnez

Retour pour revenir à la page appropriée et modifier les paramètres. Si tout semble correct, sélectionnez **Suivant**.

15. Dans la page finale, lorsque la zone est correctement signée, sélectionnez **Terminer** pour fermer l'Assistant.

Assistant Annuler l'affectation de zone

Pour supprimer DNSSEC d'une zone signée, vous pouvez utiliser l'Assistant **Annuler l'affectation de zone** dans le Gestionnaire DNS ou à l'aide de PowerShell. L'Assistant unsign zone supprime tous les enregistrements de ressources liés à DNSSEC de la zone, y compris les enregistrements DNSKEY, DS et RRSIG. Une fois qu'une zone n'est pas signée, elle peut être modifiée ou supprimée comme toute autre zone non signée.

Pour annuler l'affectation d'une zone, sélectionnez votre méthode préférée :

Gestionnaire DNS

Pour annuler l'attribution d'une zone à l'aide du Gestionnaire DNS, procédez comme suit :

1. Ouvrez le Gestionnaire DNS sur un serveur DNS principal faisant autorité.
2. Dans l'arborescence de la console du Gestionnaire DNS, cliquez avec le bouton droit sur la zone signée que vous souhaitez annuler, pointez sur **DNSSEC**, puis choisissez **Annuler l'attribution de la zone**.

La zone est immédiatement non signée et tous les enregistrements de ressources liés à DNSSEC sont supprimés de la zone. Vous pouvez annuler l'attribution d'une zone sur n'importe quel serveur DNS principal faisant autorité qui héberge une version signée de la zone ; il n'est pas obligé d'être le maître de clé.

Lorsque vous annulez l'attribution d'une zone, les paramètres utilisés pour la signature de zone sont enregistrés afin de pouvoir les utiliser à nouveau. Pour réinscrire une zone à l'aide des mêmes paramètres utilisés précédemment, choisissez **Personnaliser les paramètres de signature de zone** et utilisez les valeurs fournies pour chaque paramètre. Les kits KSK et ZSK utilisés pour signer la zone précédemment, ainsi que les valeurs de tous les paramètres DNSSEC personnalisés sont automatiquement renseignés dans **l'Assistant Signature** de zone. Si vous ne souhaitez pas utiliser les mêmes paramètres, vous avez également la possibilité de les modifier.

Si vous utilisez Windows PowerShell, vous pouvez réutiliser les mêmes paramètres en spécifiant le paramètre **DoResign** avec l'applet de commande **Invoke-DnsServerZoneSign** . Pour utiliser les paramètres par défaut, vous pouvez spécifier le paramètre **SignWithDefault** .

Modification des propriétés DNSSEC

Une fois qu'une zone est signée, certaines propriétés DNSSEC peuvent être modifiées. Par exemple, les clés peuvent être ajoutées une fois la zone signée. Si vous ajoutez une nouvelle clé de signature, la zone est immédiatement signée avec cette clé et toutes les autres clés qui sont toujours présentes dans la zone. Les clés de signature actives ne peuvent pas être supprimées, mais vous pouvez mettre hors service une clé de signature si ce n'est pas le dernier KSK ou ZSK dans la zone.

Certaines propriétés peuvent être modifiées sans signature et réinscrire la zone. Toutefois, ces paramètres ne sont pas utilisés immédiatement. Par exemple, les modifications apportées aux paramètres KSK ne prennent effet qu'à la prochaine substitution KSK. Ce comportement inclut les paramètres de signature et d'interrogation sous l'onglet **Avancé** de la page de propriétés DNSSEC. De même, les modifications apportées aux paramètres ZSK ne prennent effet qu'à la prochaine substitution ZSK.

Certains paramètres DNSSEC ne peuvent pas être modifiés lorsqu'une zone est signée. La modification de ces paramètres nécessite que la zone soit d'abord non signée, puis signée à nouveau. Dans ce scénario, toutes les ancres d'approbation qui ont été distribuées pour résoudre les serveurs DNS doivent être mises à jour manuellement.

Contenu connexe

- Vue d'ensemble de DNSSEC

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Configurer des règles DNSSEC à l'aide de la table de stratégie de résolution de noms

13/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Cet article explique comment configurer la table de stratégie de résolution de noms (NRPT) dans Windows Server pour appliquer des stratégies de sécurité DNS pour des espaces de noms spécifiques. Le NRPT permet aux administrateurs système d'implémenter des exigences de validation DNSSEC, garantissant ainsi la résolution de noms sécurisée pour les domaines critiques de votre organisation.

La table de stratégie de résolution de noms (NRPT) dans Windows Server vous permet d'appliquer des stratégies de résolution de noms sur les clients DNS prenant en compte la sécurité. Vous pouvez créer des règles NRPT pour exiger la validation DNSSEC pour des espaces de noms spécifiques, ce qui est essentiel pour sécuriser les requêtes et réponses DNS. Dans cet article, découvrez comment configurer le NRPT à l'aide de la stratégie de groupe ou de Windows PowerShell. Le NRPT peut être utilisé pour créer différents types de règles en choisissant l'un des quatre onglets disponibles. Cet article traite uniquement des règles DNSSEC.

Espaces de noms NRPT

Lorsque le service client DNS effectue la résolution de noms DNS, il vérifie le NRPT avant d'envoyer une requête DNS. Si une requête DNS correspond à une entrée dans le NRPT, le service le traite en fonction des paramètres de la stratégie. Les requêtes qui ne correspondent pas à une entrée NRPT sont traitées normalement. Vous pouvez utiliser le NRPT pour appliquer la validation DNSSEC. Cette validation s'applique aux réponses DNS pour les requêtes. Vous pouvez spécifier les espaces de noms où ces règles s'appliquent.

Le tableau suivant présente les options que vous pouvez utiliser pour configurer l'espace de noms auquel une stratégie s'applique.

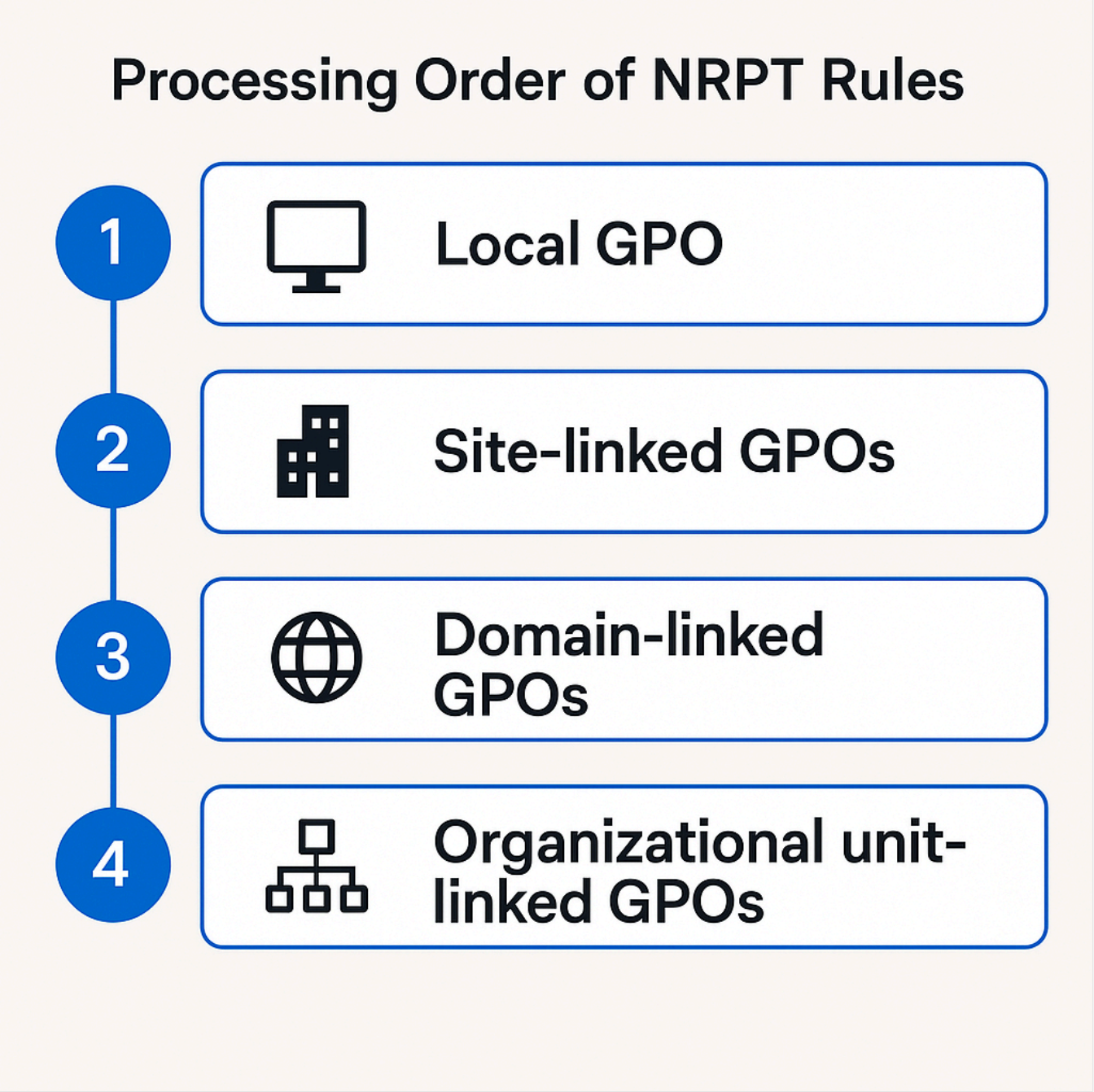
Agrandir le tableau

Choix	Utilisation
suffixe	La stratégie s'applique à tout nom qui se termine `.contoso.com` et inclut des domaines enfants.

Choix	Utilisation
Préfixe	La stratégie s'applique uniquement à un nom d'hôte. Cette stratégie est déclenchée uniquement si la partie nom d'hôte d'une requête DNS correspond au nom plat configuré dans la règle. Par exemple, si la règle spécifie `server1`, elle s'applique aux requêtes comme `server1.contoso.com` et `server1.nwtraders.com`.
FQDN	La stratégie s'applique uniquement à l'hôte spécifié. Ce nom de domaine complet (FQDN) n'est pas le nom de domaine complet d'un domaine, mais un nom de domaine complet d'un ordinateur hôte.
Sous-réseau (IPv4)	Cette option configure une stratégie, qui s'applique aux requêtes de recherche IPv4 inversées.
Sous-réseau (IPv6)	Cette option configure une stratégie, qui s'applique aux requêtes de recherche IPv6 inversées.
Quelconque	Cette option configure la stratégie par défaut.

Traitement des règles NRPT

Les règles NRPT peuvent être configurées dans un objet de stratégie de groupe lié à un objet de stratégie de groupe lié à local, site, domaine ou organisationnelle. Les règles de traitement de stratégie de groupe normales s'appliquent. À compter de l'objet de stratégie de groupe local, des objets de stratégie de groupe liés au site, des objets de stratégie de groupe liés au domaine et enfin des objets de stratégie de groupe liés à l'unité organisationnelle. Un exemple de l'ordre de traitement est illustré dans le diagramme suivant.



Si les règles NRPT sont présentes dans plusieurs objets de stratégie de groupe qui s'appliquent au même utilisateur ou ordinateur, les règles sont fusionnées, avec des règles plus discrètes qui sont prioritaires sur des règles plus générales. Par exemple, une règle qui s'applique à un espace de noms enfant est prioritaire sur une règle pour l'espace de noms parent, comme indiqué dans le tableau suivant.

Agrandir le tableau

Nom de l'objet de stratégie de groupe	Namespace	DNSSEC activé	Validation requise
Stratégie de domaine par défaut	`contoso.com`	✅	❌
NRPT_settings	`secure.contoso.com`	✅	✅

Dans cet exemple, la validation DNSSEC est requise pour les requêtes DNS qui ont un suffixe de `secure.contoso.com`, par exemple `www.secure.contoso.com`. La validation inclut des requêtes dans un domaine enfant, par exemple `www.corp.secure.contoso.com`. Toutefois, la validation n'est pas requise pour `*.contoso.com` ou `*.corp.contoso.com`. Par conséquent, si les domaines parent et enfant nécessitent une stratégie de résolution de noms différente, vous devez créer explicitement des stratégies pour l'espace de noms enfant.

> ⚠ **Avertissement**
>
> Les règles NRPT ne remplacent pas les unes les autres. Si deux règles sont créées dans deux objets de stratégie de groupe différents qui s'appliquent au même espace de noms pour le même utilisateur ou ordinateur, un conflit se produit. Par conséquent, aucune règle n'est appliquée. Si les règles s'appliquent au même utilisateur ou ordinateur pour différents espaces de noms, elles sont fusionnées. Toutefois, cette règle ne s'applique pas à la stratégie de groupe locale. Si des paramètres NRPT sont configurés dans la stratégie de groupe de domaine, tous les paramètres NRPT de stratégie de groupe local sont ignorés.

Le NRPT peut être configuré pour exiger ou non une validation pour des segments spécifiques de votre espace de noms. Par exemple, vous pouvez utiliser un redirecteur conditionnel pour désactiver la validation DNSSEC. À l'aide de cette conception, vous pouvez implémenter un redirecteur conditionnel qui dirige les ordinateurs clients vers un domaine externe non signé pour un espace de noms spécifique, tel qu'un nom de domaine complet. Si le nom transféré se trouve dans un espace de noms signé dans votre organisation, la validation peut être nécessaire, sauf si vous la désactivez spécifiquement pour ce nom de domaine complet.

Par exemple, vous pouvez avoir un domaine interne signé, `contoso.com` et vous disposez également d'un site web `www.contoso.com` externe qui n'est pas signé. Dans ce scénario, les domaines internes et externes utilisent différents serveurs faisant autorité. Un redirecteur conditionnel est utilisé pour résoudre le nom `www.contoso.com`. Le NRPT peut être configuré comme suit pour s'assurer que les ordinateurs clients sont en mesure d'atteindre le site web externe sans nécessiter de validation DNSSEC :

Agrandir le tableau

Nom	Redirecteur conditionnel	DNSSEC activé	Validation requise
`contoso.com`	Aucune	✅	✅
`www.contoso.com`	`10.10.10.10`	❌	❌

Dans cet exemple, d'autres noms dans l'espace `contoso.com` de noms, tels que `finance.contoso.com`, nécessitent toujours la validation, car ils ne correspondent pas à la règle de nom de domaine complet NRPT pour `www.contoso.com`.

Filtrer la stratégie NRPT

Par défaut, les nouveaux objets de stratégie de groupe liés au domaine s'appliquent au groupe Utilisateurs authentifiés. Vous pouvez appliquer la stratégie NRPT à des groupes, utilisateurs et ordinateurs sélectionnés en supprimant le groupe Utilisateurs authentifiés du **filtrage de sécurité** , puis en ajoutant un utilisateur, un groupe ou un ordinateur personnalisé.

Conditions préalables

Pour configurer le NRPT, vous devez disposer des conditions préalables suivantes.

- L'appartenance au groupe **Administrateurs** ou équivalent est la condition minimale requise pour effectuer ces procédures.
- Vous devez avoir installé la fonctionnalité de la console de gestion des stratégies de groupe sur l'ordinateur sur lequel vous souhaitez configurer le NRPT à l'aide de la stratégie de groupe.
- Vous devez disposer de droits pour créer ou modifier un objet de stratégie de groupe (GPO) existant dans le domaine dans lequel vous souhaitez configurer le NRPT.

Configurer le NRPT

Utilisez les procédures suivantes pour configurer la table de stratégie de résolution de noms (NRPT). Les exemples fournis montrent comment ajouter une règle dans un objet de stratégie de groupe (GPO) existant qui nécessite la validation DNSSEC pour un espace de noms (zone).

Vous pouvez configurer le NRPT à l'aide de la console de gestion des stratégies de groupe ou de Windows PowerShell. Sélectionnez la méthode qui convient le mieux à votre environnement et à vos préférences administratives.

Console de gestion des stratégies de groupe

Pour configurer les règles NRPT à l'aide de la console de gestion des stratégies de groupe (GPMC), procédez comme suit.

1. Connectez-vous à un ordinateur avec la fonctionnalité gestion des stratégies de groupe installée.

2. Ouvrez la console Gestion des stratégies de **groupe** en sélectionnant **Outils** dans le menu Gestionnaire de serveur, puis en sélectionnant **Gestion des stratégies de groupe**.
3. Accédez à l'objet de stratégie de groupe (GPO) que vous souhaitez configurer dans l'arborescence de la console de gestion des stratégies de groupe. Cliquez avec le bouton droit sur l'objet de stratégie de groupe, puis sélectionnez **Modifier**.
4. Dans l'arborescence de l'éditeur de gestion des stratégies de groupe, accédez à la stratégie de **résolution des noms des paramètres Windows des stratégies > de configuration >> ordinateur**.
5. Pour créer une règle, sous **Créer des règles**, sélectionnez la partie de l'espace de noms auquel la règle s'applique dans la liste déroulante. Par exemple, choisissez **Suffixe** pour créer une règle qui s'applique à tous les noms qui se terminent par le texte que vous fournissez.
6. Sélectionnez le type d'espace de noms dans la liste déroulante et entrez l'espace de noms auquel la règle s'applique. Par exemple, pour appliquer une règle à tous les appareils de l'espace `secure.contoso.com` de noms DNS, choisissez **Suffixe** et type `secure.contoso.com`.
7. Activez la validation DNSSEC en sélectionnant **activer DNSSEC dans cette case** à cocher, puis activez la case à cocher Exiger que les **clients DNS vérifient que ce nom et les données d'adresse ont été validés par la case à cocher du serveur DNS** .
8. Sélectionnez **Créer** en bas de cette section du NRPT pour créer la règle.
9. Faites défiler vers le bas pour afficher les règles configurées dans la section Table de stratégie **de résolution de noms** et vérifiez que la nouvelle règle s'affiche.

Afficher la stratégie NRPT actuelle

Vous pouvez utiliser l'applet de commande Get-DnsClientNrptPolicy pour afficher les stratégies NRPT. Consultez l'exemple qui suit.

```
PS C:\> Get-DnsClientNrptPolicy -Effective

Namespace                        : .contoso.com
QueryPolicy                      : QueryIPv6Only
SecureNameQueryFallback          : FallbackPrivate
DirectAccessIPsecCARestriction   :
DirectAccessProxyName            :
DirectAccessDnsServers           :
DirectAccessEnabled              : False
DirectAccessProxyType            :
DirectAccessQueryIPsecEncryption :
```

```
DirectAccessQueryIPsecRequired   :
NameServers                      :
DnsSecIPsecCARestriction         :
DnsSecQueryIPsecEncryption       :
DnsSecQueryIPsecRequired         : False
DnsSecValidationRequired         : False
NameEncoding                     :

Namespace                        : .secure.contoso.com
QueryPolicy                      : QueryIPv6Only
SecureNameQueryFallback          : FallbackPrivate
DirectAccessIPsecCARestriction   :
DirectAccessProxyName            :
DirectAccessDnsServers           :
DirectAccessEnabled              : False
DirectAccessProxyType            :
DirectAccessQueryIPsecEncryption :
DirectAccessQueryIPsecRequired   :
NameServers                      :
DnsSecIPsecCARestriction         :
DnsSecQueryIPsecEncryption       :
DnsSecQueryIPsecRequired         : False
DnsSecValidationRequired         : True
NameEncoding                     :
```

L'applet **de commande Get-DnsClientNrptPolicy** obtient la stratégie qui s'applique à l'ordinateur local. Dans cet exemple, la sortie indique que la validation DNSSEC est requise pour `*.secure.contoso.com`, et n'est pas requise pour `*.contoso.com`.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Guide de scénario de stratégie DNS

30/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Ce guide est destiné aux administrateurs DNS, réseau et système.

La stratégie DNS est une nouvelle fonctionnalité pour DNS dans Windows Server® 2016. Vous pouvez utiliser ce guide pour apprendre à utiliser la stratégie DNS pour contrôler la façon dont un serveur DNS traite les requêtes de résolution de noms en fonction des différents paramètres que vous définissez dans les stratégies.

Ce guide contient des informations de vue d'ensemble des stratégies DNS, ainsi que des scénarios de stratégie DNS spécifiques qui vous fournissent des instructions sur la configuration du comportement du serveur DNS pour atteindre vos objectifs, notamment la gestion du trafic basée sur la géolocalité pour les serveurs DNS principaux et secondaires, la haute disponibilité des applications, le DNS « split-brain », etc.

Ce guide contient les sections suivantes.

- Présentation des stratégies DNS
- Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des serveurs principaux
- Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des déploiements principal-secondaire
- Utiliser une stratégie DNS pour des réponses DNS intelligentes basées sur l'heure
- Réponses DNS basées sur l'heure avec un serveur d'applications cloud Azure
- Utiliser une stratégie DNS pour le déploiement DNS Split-Brain
- Utilisation de la stratégie DNS pour le DNS Split-Brain dans Active Directory
- Utilisation de la stratégie DNS pour appliquer des filtres aux requêtes DNS
- Utilisation de la stratégie DNS pour l'équilibrage de charge des applications
- Utilisation de la stratégie DNS pour l'équilibrage de charge des applications avec prise en charge de la géolocalisation

Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des serveurs principaux

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour savoir comment configurer la stratégie DNS pour permettre aux serveurs DNS principaux de répondre aux requêtes client DNS en fonction de l'emplacement géographique du client et de la ressource à laquelle le client tente de se connecter, en fournissant au client l'adresse IP de la ressource la plus proche.

> ⓘ **Important**
>
> Ce scénario montre comment déployer une stratégie DNS pour la gestion du trafic basée sur la géolocalisation lorsque vous utilisez uniquement des serveurs DNS principaux. Vous pouvez également effectuer une gestion du trafic basée sur la géolocalisation lorsque vous disposez de serveurs DNS principaux et secondaires. Si vous avez un déploiement principal-secondaire, commencez par effectuer les étapes décrites dans cette rubrique, puis suivez les étapes fournies dans la rubrique Utiliser la stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des déploiements Principal-Secondaire.

Avec de nouvelles stratégies DNS, vous pouvez créer une stratégie DNS qui permet au serveur DNS de répondre à une requête client demandant l'adresse IP d'un serveur Web. Les instances du serveur Web peuvent se trouver dans différents centres de données à différents emplacements physiques. DNS peut évaluer les emplacements du client et du serveur Web, puis répondre à la demande du client en fournissant au client une adresse IP de serveur Web pour un serveur Web physiquement situé plus près du client.

Vous pouvez utiliser les paramètres de stratégie DNS suivants pour contrôler les réponses du serveur DNS aux requêtes des clients DNS.

- **Sous-réseau client**. Nom d'un sous-réseau client prédéfini. Permet de vérifier le sous-réseau à partir duquel la requête a été envoyée.
- **Protocole de transport**. Protocole de transport utilisé dans la requête. Les entrées possibles sont **UDP** et **TCP**.
- **Protocole Internet**. Protocole réseau utilisé dans la requête. Les entrées possibles sont **IPv4** et **IPv6**.

- **Adresse IP de l'interface serveur**. Adresse IP de l'interface réseau du serveur DNS qui a reçu la requête DNS.
- **FQDN**. Nom de domaine complet (FQDN) de l'enregistrement dans la requête, avec la possibilité d'utiliser une carte générique.
- **Type de requête**. Type d'enregistrement interrogé (A, SRV, TXT, etc.)
- **Heure du jour**. Heure de la réception de la requête.

Vous pouvez combiner les critères suivants avec un opérateur logique (AND/OR) pour formuler des expressions de stratégie. Lorsque ces expressions correspondent, les stratégies sont censées effectuer l'une des actions suivantes.

- **Ignore**. Le serveur DNS supprime silencieusement la requête.
- **Deny**. Le serveur DNS répond à cette requête avec une réponse d'échec.
- **Allow**. Le serveur DNS répond en retour avec une réponse gérée par le trafic.

Exemple de Gestion du trafic basée sur la géolocalisation

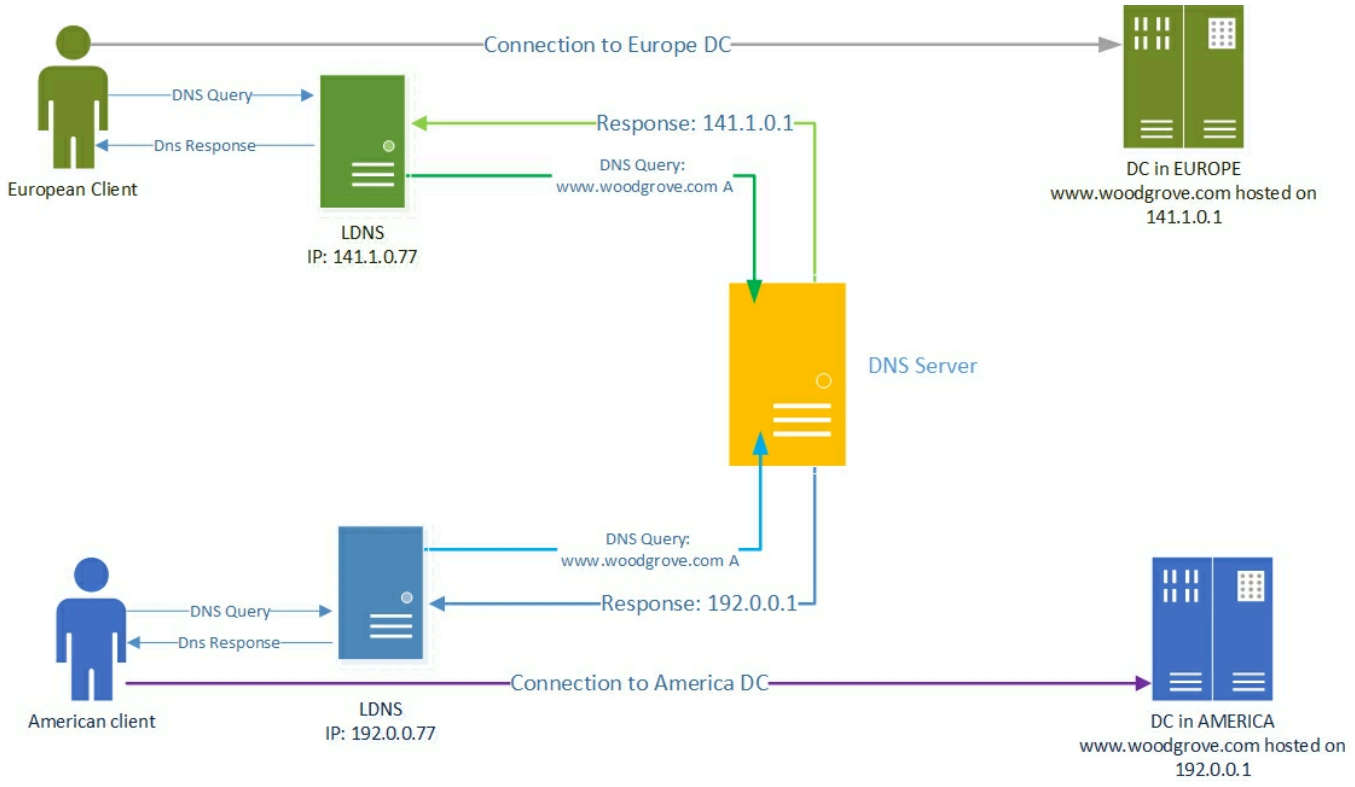
Voici un exemple de la façon dont vous pouvez utiliser la stratégie DNS pour obtenir la redirection du trafic sur la base de l'emplacement physique du client qui exécute une requête DNS.

Cet exemple utilise deux sociétés fictives : Contoso Cloud Services, qui fournit des solutions d'hébergement web et d'hébergement de domaine, et Woodgrove Food Services, qui fournit des services de livraison de nourriture dans plusieurs villes à travers le monde, et qui dispose d'un site Web nommé woodgrove.com.

Contoso Cloud Services dispose de deux centres de données, l'un aux États-Unis et l'autre en Europe. Le centre de données européen héberge un portail de commandes alimentaires pour woodgrove.com.

Pour s'assurer que les clients woodgrove.com bénéficient d'une expérience réactive à partir de leur site web, Woodgrove souhaite que les clients européens soient dirigés vers le centre de données européen et les clients américains vers le centre de données américain. Les clients situés ailleurs dans le monde peuvent être dirigés vers l'un des centres de données.

L'illustration suivante représente ce scénario.



Fonctionnement du processus de résolution de noms DNS

Pendant le processus de résolution de noms, l'utilisateur tente de se connecter à www.woodgrove.com. Il en résulte une demande de résolution de noms DNS qui est envoyée au serveur DNS configuré dans les propriétés de connexion réseau sur l'ordinateur de l'utilisateur. En règle générale, il s'agit du serveur DNS fourni par le FAI local agissant en tant que programme de résolution de mise en cache, et est appelé LDNS.

Si le nom DNS n'est pas présent dans le cache local de LDNS, le serveur LDNS transfère la requête au serveur DNS qui fait autorité pour woodgrove.com. Le serveur DNS faisant autorité répond avec l'enregistrement demandé (www.woodgrove.com) au serveur LDNS, qui met à son tour en cache l'enregistrement localement avant de l'envoyer à l'ordinateur de l'utilisateur.

Étant donné que Contoso Cloud Services utilise des stratégies de serveur DNS, le serveur DNS faisant autorité qui héberge contoso.com est configuré pour retourner des réponses gérées du trafic basées sur la géolocalisation. Cela se traduit par la direction des clients européens vers le centre de données européen et la direction des clients américains vers le centre de données américain, comme illustré dans l'illustration.

Dans ce scénario, le serveur DNS faisant autorité voit généralement la demande de résolution de noms provenant du serveur LDNS et, très rarement, de l'ordinateur de l'utilisateur. Pour cette raison, l'adresse IP source dans la demande de résolution de noms, telle que vue par le serveur DNS faisant autorité, est celle du serveur LDNS et non celle de l'ordinateur de

l'utilisateur. Toutefois, l'utilisation de l'adresse IP du serveur LDNS lorsque vous configurez des réponses de requête géolocalisée fournit une estimation juste de l'emplacement géographique de l'utilisateur, car l'utilisateur interroge le serveur DNS de son FAI local.

> **Notes**
>
> Les stratégies DNS utilisent l'adresse IP de l'expéditeur dans le paquet UDP/TCP qui contient la requête DNS. Si la requête atteint le serveur principal via plusieurs tronçons de programme de résolution/LDNS, la stratégie prend uniquement en compte l'adresse IP du dernier programme de résolution à partir duquel le serveur DNS reçoit la requête.

Comment configurer une stratégie DNS pour les réponses de requête basées sur la géolocalisation

Pour configurer la stratégie DNS pour les réponses de requête basées sur la géolocalisation, vous devez effectuer les étapes suivantes.

1. Créer les sous-réseaux clients DNS
2. Créer les étendues de la zone
3. Ajouter des enregistrements aux étendues de zone
4. Créer les stratégies

> **Notes**
>
> Vous devez effectuer ces étapes sur le serveur DNS faisant autorité pour la zone que vous souhaitez configurer. L'appartenance à **DnsAdmins** ou équivalent est nécessaire pour effectuer les procédures suivantes.

Les sections suivantes fournissent des instructions de configuration détaillées.

> **Important**
>
> Les sections suivantes incluent des exemples de commandes Windows PowerShell qui contiennent des exemples de valeurs pour de nombreux paramètres. Veillez à remplacer les exemples de valeurs dans ces commandes par des valeurs appropriées à votre déploiement avant d'exécuter ces commandes.

Créer les sous-réseaux clients DNS

La première étape consiste à identifier les sous-réseaux ou l'espace d'adressage IP des régions pour lesquelles vous souhaitez rediriger le trafic. Par exemple, si vous souhaitez rediriger le trafic vers les États-Unis et l'Europe, vous devez identifier les sous-réseaux ou les espaces d'adressage IP de ces régions.

Vous pouvez obtenir ces informations à partir de cartes géo-IP. En fonction de ces distributions géo-IP, vous devez créer les « sous-réseaux clients DNS ». Un sous-réseau client DNS est un regroupement logique de sous-réseaux IPv4 ou IPv6 à partir desquels les requêtes sont envoyées à un serveur DNS.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer des sous-réseaux clients DNS.

PowerShell

```
Add-DnsServerClientSubnet -Name "USSubnet" -IPv4Subnet "192.0.0.0/24"
Add-DnsServerClientSubnet -Name "EuropeSubnet" -IPv4Subnet "141.1.0.0/24"
```

Pour plus d'informations, consultez Add-DnsServerClientSubnet.

Créer des étendues de zone

Une fois les sous-réseaux clients configurés, vous devez partitionner la zone dont vous souhaitez rediriger le trafic dans deux étendues de zone différentes, une étendue pour chacun des sous-réseaux clients DNS que vous avez configurés.

Par exemple, si vous souhaitez rediriger le trafic pour le nom DNS www.woodgrove.com, vous devez créer deux étendues de zone différentes dans la zone woodgrove.com, une pour les États-Unis et une pour l'Europe.

Une étendue de zone est une instance unique de la zone. Une zone DNS peut avoir plusieurs étendues de zone, chacune d'elles contenant son propre jeu d'enregistrements DNS. Le même enregistrement peut être présent dans plusieurs étendues, avec des adresses IP différentes ou les mêmes adresses IP.

> **Notes**
>
> Par défaut, une étendue de zone existe sur les zones DNS. Cette étendue de zone porte le même nom que la zone, et les opérations DNS héritées fonctionnent sur cette étendue.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer des étendues de zone.

PowerShell

```
Add-DnsServerZoneScope -ZoneName "woodgrove.com" -Name "USZoneScope"
Add-DnsServerZoneScope -ZoneName "woodgrove.com" -Name "EuropeZoneScope"
```

Pour plus d'informations, consultez Add-DnsServerZoneScope.

Ajouter des enregistrements aux étendues de zone

Vous devez maintenant ajouter les enregistrements représentant l'hôte du serveur web dans les deux étendues de zone.

Par exemple, **USZoneScope** et **EuropeZoneScope**. Dans USZoneScope, vous pouvez ajouter l'enregistrement www.woodgrove.com avec l'adresse IP 192.0.0.1, qui se trouve dans un centre de données américain ; et en EuropeZoneScope, vous pouvez ajouter le même enregistrement (www.woodgrove.com) avec l'adresse IP 141.1.0.1 dans le centre de données européen.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour ajouter des enregistrements aux étendues de zone.

PowerShell

```
Add-DnsServerResourceRecord -ZoneName "woodgrove.com" -A -Name "www" -IPv4Address
"192.0.0.1" -ZoneScope "USZoneScope"
Add-DnsServerResourceRecord -ZoneName "woodgrove.com" -A -Name "www" -IPv4Address
"141.1.0.1" -ZoneScope "EuropeZoneScope"
```

Dans cet exemple, vous devez également utiliser les commandes Windows PowerShell suivantes pour ajouter des enregistrements dans l'étendue de zone par défaut afin que le reste du monde puisse toujours accéder au serveur web woodgrove.com à partir de l'un des deux centres de données.

PowerShell

```
Add-DnsServerResourceRecord -ZoneName "woodgrove.com" -A -Name "www" -IPv4Address
"192.0.0.1"
Add-DnsServerResourceRecord -ZoneName "woodgrove.com" -A -Name "www" -IPv4Address
"141.1.0.1"
```

Le paramètre **ZoneScope** n'est pas inclus lorsque vous ajoutez un enregistrement dans l'étendue par défaut. Cela équivaut à ajouter des enregistrements à une zone DNS standard.

Pour plus d'informations, consultez Add-DnsServerResourceRecord.

Créer les stratégies

Après avoir créé les sous-réseaux, les partitions (étendues de zone) et ajouté des enregistrements, vous devez créer des stratégies qui connectent les sous-réseaux et les partitions, de sorte que lorsqu'une requête provient d'une source dans l'un des sous-réseaux clients DNS, la réponse à la requête est retournée à partir de l'étendue correcte de la zone. Aucune stratégie n'est requise pour le mappage de l'étendue de zone par défaut.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer une stratégie DNS qui lie les sous-réseaux du client DNS et les étendues de zone.

PowerShell

```
Add-DnsServerQueryResolutionPolicy -Name "USPolicy" -Action ALLOW -ClientSubnet
"eq,USSubnet" -ZoneScope "USZoneScope,1" -ZoneName "woodgrove.com"
Add-DnsServerQueryResolutionPolicy -Name "EuropePolicy" -Action ALLOW -
ClientSubnet "eq,EuropeSubnet" -ZoneScope "EuropeZoneScope,1" -ZoneName
"woodgrove.com"
```

Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

À présent, le serveur DNS est configuré avec les stratégies DNS requises pour rediriger le trafic en fonction de l'emplacement géographique.

Lorsque le serveur DNS reçoit des requêtes de résolution de noms, le serveur DNS évalue les champs de la requête DNS par rapport aux stratégies DNS configurées. Si l'adresse IP source dans la demande de résolution de noms correspond à l'une des stratégies, l'étendue de zone associée est utilisée pour répondre à la requête et l'utilisateur est dirigé vers la ressource qui est géographiquement la plus proche d'elle.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des déploiements principaux/secondaires

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour apprendre à créer une stratégie DNS pour la gestion du trafic basée sur la géolocalisation lorsque votre déploiement DNS inclut à la fois des serveurs DNS primaires et secondaires.

Le scénario précédent, Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des serveurs primaires, fournissait des instructions pour la configuration de la stratégie DNS pour la gestion du trafic basée sur la géolocalisation sur un serveur DNS primaire. Dans l'infrastructure Internet, toutefois, les serveurs DNS sont largement déployés dans un modèle primaire-secondaire, où la copie accessible en écriture d'une zone est stockée sur des serveurs primaires sélectionnés et sécurisés, et les copies en lecture seule de la zone sont conservées sur plusieurs serveurs secondaires.

Les serveurs secondaires utilisent les protocoles de transfert de zone faisant autorité (AXFR) et de transfert de zone incrémentiel (IXFR) pour demander et recevoir des mises à jour de zone qui incluent de nouvelles modifications apportées aux zones sur les serveurs DNS primaires.

> **Notes**
>
> Pour plus d'informations sur AXFR, consultez l'Internet Engineering Task Force (IETF) Requête pour commentaires 5936. Pour plus d'informations sur IXFR, consultez l'Internet Engineering Task Force (IETF) Requête pour commentaires 1995.

Exemple de gestion du trafic basée sur la géolocalisation primaire et secondaire

Voici un exemple de la façon dont vous pouvez utiliser la stratégie DNS dans un déploiement primaire-secondaire pour obtenir la redirection du trafic sur la base de l'emplacement physique du client qui exécute une requête DNS.

Cet exemple utilise deux sociétés fictives : Contoso Cloud Services, qui fournit des solutions d'hébergement web et d'hébergement de domaine, et Woodgrove Food Services, qui fournit

des services de livraison de nourriture dans plusieurs villes à travers le monde, et qui dispose d'un site Web nommé woodgrove.com.

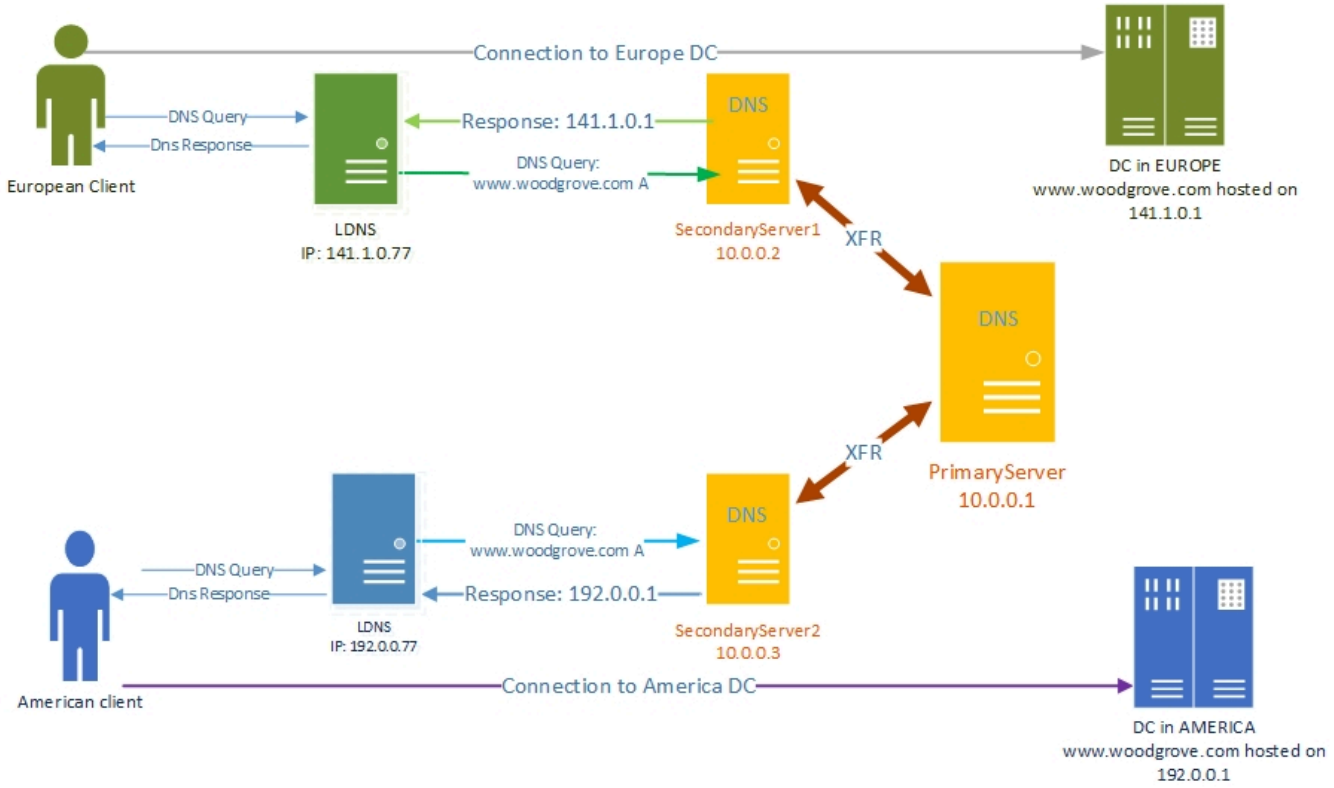
Pour s'assurer que les clients woodgrove.com bénéficient d'une expérience réactive à partir de leur site web, Woodgrove souhaite que les clients européens soient dirigés vers le centre de données européen et les clients américains vers le centre de données américain. Les clients situés ailleurs dans le monde peuvent être dirigés vers l'un des centres de données.

Contoso Services cloud dispose de deux centres de données, l'un aux États-Unis et l'autre en Europe, sur lesquels Contoso héberge son portail de commandes alimentaires pour woodgrove.com.

Le déploiement DNS contoso comprend deux serveurs secondaires : **SecondaryServer1**, avec l'adresse IP 10.0.0.2 ; et **SecondaryServer2**, avec l'adresse IP 10.0.0.3. Ces serveurs secondaires agissent en tant que serveurs de noms dans les deux régions différentes, SecondaryServer1 situé en Europe et SecondaryServer2 situé aux États-Unis.

Il existe une copie de zone accessible en écriture principale sur **PrimaryServer** (adresse IP 10.0.0.1), où les modifications de zone sont apportées. Avec des transferts de zone réguliers vers les serveurs secondaires, les serveurs secondaires sont toujours à jour avec les nouvelles modifications apportées à la zone sur le serveur primaire.

L'illustration suivante représente ce scénario.



Fonctionnement du système primaire et secondaire du DNS

Lorsque vous déployez la gestion du trafic basée sur la géolocalisation dans un déploiement DNS primaire-secondaire, il est important de comprendre comment se produisent les transferts normaux de zone primaire-secondaire avant d'en savoir plus sur les transferts au niveau de l'étendue de zone. Les sections suivantes fournissent des informations sur les transferts au niveau de la zone et de l'étendue de la zone.

- Transferts de zone dans un déploiement DNS primaire-secondaire
- Transferts au niveau de l'étendue de la zone dans un déploiement DNS primaire-secondaire

Transferts de zone dans un déploiement DNS primaire-secondaire

Vous pouvez créer un déploiement DNS primaire-secondaire et synchroniser les zones en suivant les étapes suivantes.

1. Lorsque vous installez DNS, la zone primaire est créée sur le serveur DNS primaire.
2. Sur le serveur secondaire, créez les zones et spécifiez les serveurs primaires.
3. Sur les serveurs primaires, vous pouvez ajouter les serveurs secondaires en tant que serveurs secondaires approuvés sur la zone primaire.
4. Les zones secondaires effectuent une requête de transfert de zone complète (AXFR) et reçoivent la copie de la zone.
5. Si nécessaire, les serveurs primaires envoient des notifications aux serveurs secondaires concernant les mises à jour de la zone.
6. Les serveurs secondaires effectuent une requête de transfert de zone incrémentielle (IXFR). Pour cette raison, les serveurs secondaires restent synchronisés avec le serveur primaire.

Transferts au niveau de l'étendue de la zone dans un déploiement DNS primaire-secondaire

Le scénario de gestion du trafic nécessite des étapes supplémentaires pour diviser les zones en différents périmètres. Pour cette raison, des étapes supplémentaires sont nécessaires pour transférer les données à l'intérieur des étendues de zone vers les serveurs secondaires et pour transférer des stratégies et des sous-réseaux clients DNS vers les serveurs secondaires.

Après avoir configuré votre infrastructure DNS avec des serveurs primaires et secondaires, les transferts au niveau de l'étendue de la zone sont effectués automatiquement par DNS, à l'aide

des processus suivants.

Pour garantir le transfert au niveau de l'étendue de la zone, les serveurs DNS utilisent les mécanismes d'extension pour DNS (EDNS0) OPT RR. Toutes les requêtes de transfert de zone (AXFR ou IXFR) des zones avec étendues proviennent d'un EDNS0 OPT RR, dont l'ID d'option est défini sur « 65433 » par défaut. Pour plus d'informations sur EDNSO, consultez la Requête de commentaires 6891 de l'IETF.

La valeur d'OPT RR est le nom d'étendue de zone pour lequel la requête est envoyée. Lorsqu'un serveur DNS primaire reçoit ce paquet d'un serveur secondaire approuvé, il interprète la requête comme étant destinée à cette étendue de zone.

Si le serveur primaire dispose de cette zone, il répond avec les données de transfert (XFR) de cette étendue. La réponse contient un RR OPT avec le même ID d'option « 65433 » et la même valeur définie pour la même étendue de zone. Les serveurs secondaires reçoivent cette réponse, récupèrent les informations d'étendue de la réponse et mettent à jour cette étendue particulière de la zone.

Après ce processus, le serveur primaire gère une liste de fichiers secondaires approuvés qui ont envoyé une requête d'étendue de zone de ce type pour les notifications.

Pour toute mise à jour supplémentaire dans une étendue de zone, une notification IXFR est envoyée aux serveurs secondaires, avec le même OPT RR. L'étendue de zone recevant cette notification effectue la requête IXFR contenant cette OPT RR et le même processus que celui décrit ci-dessus s'ensuit.

Comment configurer une stratégie DNS pour la gestion du trafic basée sur la géolocalisation primaire et secondaire

Avant de commencer, vérifiez que vous avez effectué toutes les étapes de la rubrique Utiliser la stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec les serveurs primaires, et que votre serveur DNS primaire est configuré avec des zones, des étendues de zone, des sous-réseaux client DNS et une stratégie DNS.

> **Notes**
>
> Les instructions de cette rubrique pour copier les sous-réseaux client DNS, les étendues de zone et les stratégies DNS des serveurs principaux DNS vers des serveurs secondaires DNS concernent la configuration et la validation DNS initiales. À l'avenir, vous souhaiterez peut-être modifier les paramètres des sous-réseaux du client DNS, des étendues de zone

et des stratégies sur le serveur primaire. Dans ce cas, vous pouvez créer des scripts d'automatisation pour maintenir la synchronisation des serveurs secondaires avec le serveur primaire.

Pour configurer la stratégie DNS pour les réponses de requête basées sur la géolocalisation primaire-secondaire, vous devez effectuer les étapes suivantes.

- Créer les zones secondaires
- Configurer les paramètres de transfert de zone sur la zone primaire
- Copier les sous-réseaux clients DNS
- Créer les étendues de zone sur le serveur secondaire
- Configurer une stratégie DNS :

Les sections suivantes fournissent des instructions de configuration détaillées.

> **Important**
>
> Les sections suivantes incluent des exemples de commandes Windows PowerShell qui contiennent des exemples de valeurs pour de nombreux paramètres. Veillez à remplacer les exemples de valeurs dans ces commandes par des valeurs appropriées à votre déploiement avant d'exécuter ces commandes.
>
> L'appartenance à **DnsAdmins** ou équivalent est nécessaire pour effectuer les procédures suivantes.

Créez les zones secondaires

Vous pouvez créer la copie secondaire de la zone à répliquer sur SecondaryServer1 et SecondaryServer2 (en supposant que les applets de commande sont exécutées à distance à partir d'un seul client de gestion).

Par exemple, vous pouvez créer la copie secondaire de www.woodgrove.com sur SecondaryServer1 et SecondaryServer2.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer les zones secondaires.

PowerShell

```
Add-DnsServerSecondaryZone -Name "woodgrove.com" -ZoneFile "woodgrove.com.dns" -
MasterServers 10.0.0.1 -ComputerName SecondaryServer1
```

```
Add-DnsServerSecondaryZone -Name "woodgrove.com" -ZoneFile "woodgrove.com.dns" -
MasterServers 10.0.0.1 -ComputerName SecondaryServer2
```

Pour plus d'informations, consultez Add-DnsServerSecondaryZone.

Configurez les paramètres de transfert de zone sur la zone primaire

Vous devez configurer les paramètres de zone primaire afin que :

1. Les transferts de zone du serveur primaire vers les serveurs secondaires spécifiés sont autorisés.
2. Les notifications de mise à jour de zone sont envoyées par le serveur primaire aux serveurs secondaires.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour configurer les paramètres de transfert de zone sur la zone primaire.

> **Notes**
>
> Dans l'exemple de commande suivant, le paramètre **-Notify** spécifie que le serveur principal envoie des notifications sur les mises à jour apportées à la liste de sélection des secondaires.

PowerShell

```
Set-DnsServerPrimaryZone -Name "woodgrove.com" -Notify Notify -SecondaryServers
"10.0.0.2,10.0.0.3" -SecureSecondaries TransferToSecureServers -ComputerName
PrimaryServer
```

Pour plus d'informations, consultez Set-DnsServerPrimaryZone.

Copiez les sous-réseaux clients DNS

Vous devez copier les sous-réseaux clients DNS du serveur primaire vers les serveurs secondaires.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour copier les sous-réseaux sur les serveurs secondaires.

PowerShell

```
Get-DnsServerClientSubnet -ComputerName PrimaryServer | Add-DnsServerClientSubnet
-ComputerName SecondaryServer1
Get-DnsServerClientSubnet -ComputerName PrimaryServer | Add-DnsServerClientSubnet
-ComputerName SecondaryServer2
```

Pour plus d'informations, consultez Add-DnsServerClientSubnet.

Créez les étendues de zone sur le serveur secondaire

Vous devez créer les étendues de zone sur les serveurs secondaires. Dans DNS, les étendues de zone commencent également à demander des XFR auprès du serveur principal. En cas de modification des étendues de zone sur le serveur primaire, une notification contenant les informations d'étendue de zone est envoyée aux serveurs secondaires. Les serveurs secondaires peuvent ensuite mettre à jour leurs étendues de zone avec une modification incrémentielle.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer les étendues de zone sur les serveurs secondaires.

PowerShell

```
Get-DnsServerZoneScope -ZoneName "woodgrove.com" -ComputerName PrimaryServer|Add-
DnsServerZoneScope -ZoneName "woodgrove.com" -ComputerName SecondaryServer1 -
ErrorAction Ignore
Get-DnsServerZoneScope -ZoneName "woodgrove.com" -ComputerName PrimaryServer|Add-
DnsServerZoneScope -ZoneName "woodgrove.com" -ComputerName SecondaryServer2 -
ErrorAction Ignore
```

Notes

Dans ces exemples de commandes, le paramètre **-ErrorAction Ignore** est inclus, car une étendue de zone par défaut existe sur chaque zone. L'étendue de zone par défaut ne peut pas être créée ou supprimée. Le traitement en pipeline entraînera une tentative de création de cette étendue, qui échouera. Vous pouvez également créer des étendues de zone autres que les étendues par défaut sur deux zones secondaires.

Pour plus d'informations, consultez Add-DnsServerZoneScope.

Configurez la stratégie DNS

Après avoir créé les sous-réseaux, les partitions (étendues de zone) et ajouté des enregistrements, vous devez créer des stratégies qui connectent les sous-réseaux et les

partitions, de sorte que lorsqu'une requête provient d'une source dans l'un des sous-réseaux clients DNS, la réponse à la requête est retournée à partir de l'étendue correcte de la zone. Aucune stratégie n'est requise pour le mappage de l'étendue de zone par défaut.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer une stratégie DNS qui lie les sous-réseaux du client DNS et les étendues de zone.

PowerShell

```
$policy = Get-DnsServerQueryResolutionPolicy -ZoneName "woodgrove.com" -
ComputerName PrimaryServer
$policy | Add-DnsServerQueryResolutionPolicy -ZoneName "woodgrove.com" -
ComputerName SecondaryServer1
$policy | Add-DnsServerQueryResolutionPolicy -ZoneName "woodgrove.com" -
ComputerName SecondaryServer2
```

Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

À présent, les serveurs DNS secondaires sont configurés avec les stratégies DNS requises pour rediriger le trafic en fonction de la géolocalisation.

Lorsque le serveur DNS reçoit des requêtes de résolution de noms, le serveur DNS évalue les champs de la requête DNS par rapport aux stratégies DNS configurées. Si l'adresse IP source dans la demande de résolution de noms correspond à l'une des stratégies, l'étendue de zone associée est utilisée pour répondre à la requête et l'utilisateur est dirigé vers la ressource qui est géographiquement la plus proche d'elle.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Utiliser une stratégie DNS pour les réponses DNS intelligentes basées sur l'heure du jour

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour apprendre à distribuer le trafic d'application entre différentes instances distribuées géographiquement d'une application à l'aide de stratégies DNS basées sur l'heure de la journée.

Ce scénario est utile dans les situations où vous souhaitez diriger le trafic dans un fuseau horaire vers d'autres serveurs d'applications, tels que des serveurs Web, qui se trouvent dans un autre fuseau horaire. Cela vous permet d'équilibrer la charge du trafic entre les instances d'application pendant les périodes de pointe lorsque vos serveurs principaux sont surchargés de trafic.

Exemple des réponses DNS intelligentes basées sur l'heure du jour

Voici un exemple de la façon dont vous pouvez utiliser la stratégie DNS pour équilibrer le trafic d'application en fonction de l'heure de la journée.

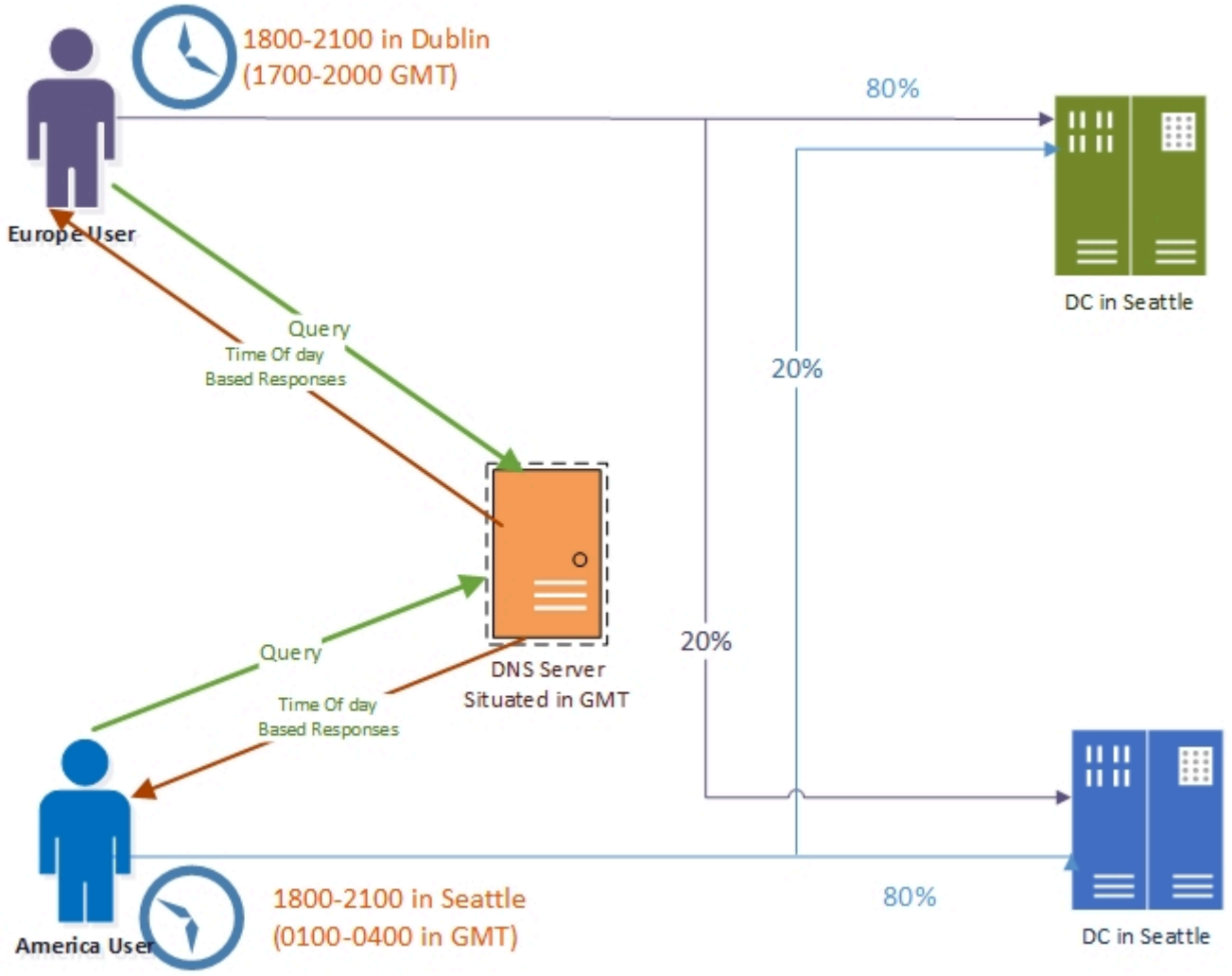
Cet exemple utilise une société fictive, Contoso Gift Services, qui fournit des solutions de cadeaux en ligne dans le monde entier via son site Web, contosogiftservices.com.

Le site Web contosogiftservices.com est hébergé dans deux centres de données, l'un à Seattle (Amérique du Nord) et l'autre à Dublin (Europe). Les serveurs DNS sont configurés pour envoyer des réponses prenant en charge la géolocalisation à l'aide d'une stratégie DNS. Avec une récente augmentation de l'activité, contosogiftservices.com a un plus grand nombre de visiteurs chaque jour, et certains clients ont signalé des problèmes de disponibilité du service.

Contoso Gift Services effectue une analyse de site et découvre que tous les soirs entre 18h00 et 21h00, le trafic vers les serveurs Web augmente. Les serveurs Web ne peuvent pas être mis à l'échelle pour gérer l'augmentation du trafic à ces heures de pointe, ce qui entraîne un déni de service pour les clients. La même surcharge de trafic aux heures de pointe se produit dans les centres de données européens et américains. À d'autres moments de la journée, les serveurs gèrent des volumes de trafic bien inférieurs à leur capacité maximale.

Pour s'assurer que contosogiftservices.com clients bénéficient d'une expérience réactive à partir du site Web, Contoso Gift Services souhaite rediriger une partie du trafic de Dublin vers les serveurs d'applications de Seattle entre 18 h et 21 h à Dublin ; et ils veulent rediriger du trafic de Seattle vers les serveurs d'applications Dublin entre 18h00 et 21h00 à Seattle.

L'illustration suivante représente ce scénario.



Comment les Réponses DNS intelligentes basées sur l'heure du jour fonctionnent

Lorsque le serveur DNS est configuré avec la stratégie DNS d'heure de la journée, entre 18h00 et 21h00 à chaque emplacement géographique, le serveur DNS effectue les opérations suivantes.

- Répond aux quatre premières requêtes qu'il reçoit avec l'adresse IP du serveur Web dans le centre de données local.
- Répond à la cinquième requête qu'il reçoit avec l'adresse IP du serveur Web dans le centre de données distant.

Ce comportement basé sur des stratégies décharge vingt pour cent de la charge de trafic du serveur Web local vers le serveur Web distant, ce qui facilite la pression sur le serveur d'applications local et améliore les performances du site pour les clients.

Pendant les heures creuses, les serveurs DNS effectuent une gestion du trafic basée sur des emplacements géographiques normaux. En outre, les clients DNS qui envoient des requêtes à partir d'emplacements autres que Amérique du Nord ou l'Europe, le serveur DNS équilibre la charge du trafic entre les centres de données de Seattle et de Dublin.

Lorsque plusieurs stratégies DNS sont configurées dans DNS, il s'agit d'un ensemble ordonné de règles et elles sont traitées par DNS de la priorité la plus élevée à la priorité la plus faible. DNS utilise la première stratégie qui correspond aux circonstances, y compris l'heure de la journée. Pour cette raison, les stratégies plus spécifiques doivent avoir une priorité plus élevée. Si vous créez des stratégies d'heure de la journée et que vous leur accordez une priorité élevée dans la liste des stratégies, DNS traite et utilise d'abord ces stratégies si elles correspondent aux paramètres de la requête cliente DNS et aux critères définis dans la stratégie. Si elles ne correspondent pas, DNS descend la liste des stratégies pour traiter les stratégies par défaut jusqu'à ce qu'il trouve une correspondance.

Pour plus d'informations sur les types et les critères de stratégie, consultez Vue d'ensemble des stratégies DNS.

Comment configurer une stratégie DNS pour les réponses DNS intelligentes basées sur l'heure du jour

Pour configurer la stratégie DNS pour les réponses de requête basées sur l'équilibrage de charge de l'application à l'heure de la journée, vous devez effectuer les étapes suivantes.

- Créer les sous-réseaux clients DNS
- Créer les étendues de zone
- Ajouter des enregistrements aux étendues de zone
- Créer les stratégies DNS

> **Notes**
>
> Vous devez effectuer ces étapes sur le serveur DNS faisant autorité pour la zone que vous souhaitez configurer. L'adhésion à **DnsAdmins**, ou un équivalent, est nécessaire pour effectuer les procédures suivantes.

Les sections suivantes fournissent des instructions de configuration détaillées.

> **Important**
>
> Les sections suivantes incluent des exemples de commandes Windows PowerShell qui contiennent des exemples de valeurs pour de nombreux paramètres. Veillez à remplacer les exemples de valeurs dans ces commandes par des valeurs appropriées à votre déploiement avant d'exécuter ces commandes.

Créer les sous-réseaux clients DNS

La première étape consiste à identifier les sous-réseaux ou l'espace d'adressage IP des régions pour lesquelles vous souhaitez rediriger le trafic. Par exemple, si vous souhaitez rediriger le trafic vers les États-Unis et l'Europe, vous devez identifier les sous-réseaux ou les espaces d'adressage IP de ces régions.

Vous pouvez obtenir ces informations à partir de cartes géo-IP. En fonction de ces distributions géo-IP, vous devez créer les « sous-réseaux clients DNS ». Un sous-réseau client DNS est un regroupement logique de sous-réseaux IPv4 ou IPv6 à partir desquels les requêtes sont envoyées à un serveur DNS.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer des sous-réseaux clients DNS.

PowerShell

```
Add-DnsServerClientSubnet -Name "AmericaSubnet" -IPv4Subnet "192.0.0.0/24",
"182.0.0.0/24"

Add-DnsServerClientSubnet -Name "EuropeSubnet" -IPv4Subnet "141.1.0.0/24",
"151.1.0.0/24"
```

Pour plus d'informations, consultez Add-DnsServerClientSubnet.

Créer les étendues de zone

Une fois les sous-réseaux clients configurés, vous devez partitionner la zone dont vous souhaitez rediriger le trafic dans deux étendues de zone différentes, une étendue pour chacun des sous-réseaux clients DNS que vous avez configurés.

Par exemple, si vous souhaitez rediriger le trafic pour le nom `www.contosogiftservices.com` DNS, vous devez créer deux étendues de zone différentes dans la zone contosogiftservices.com, une pour les États-Unis et une pour l'Europe.

Une étendue de zone est une instance unique de la zone. Une zone DNS peut avoir plusieurs étendues de zone, chacune d'elles contenant son propre jeu d'enregistrements DNS. Le même enregistrement peut être présent dans plusieurs étendues, avec des adresses IP différentes ou les mêmes adresses IP.

> **Notes**
>
> Par défaut, une étendue de zone existe sur les zones DNS. Cette étendue de zone porte le même nom que la zone, et les opérations DNS héritées fonctionnent sur cette étendue.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer des étendues de zone.

PowerShell

```
Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name
"SeattleZoneScope"

Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name "DublinZoneScope"
```

Pour plus d'informations, consultez Add-DnsServerZoneScope.

Ajouter des enregistrements aux étendues de zone

Vous devez maintenant ajouter les enregistrements représentant l'hôte du serveur web dans les deux étendues de zone.

Par exemple, dans **SeattleZoneScope**, l'enregistrement **www.contosogiftservices.com** est ajouté avec l'adresse IP 192.0.0.1, qui se trouve dans un centre de données de Seattle. De même, dans **DublinZoneScope**, l'enregistrement **www.contosogiftservices.com** est ajouté avec l'adresse IP 141.1.0.3 dans le centre de données de Dublin

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour ajouter des enregistrements aux étendues de zone.

PowerShell

```
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name "www" -
IPv4Address "192.0.0.1" -ZoneScope "SeattleZoneScope"

Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name "www" -
IPv4Address "141.1.0.3" -ZoneScope "DublinZoneScope"
```

Le paramètre ZoneScope n'est pas inclus lorsque vous ajoutez un enregistrement dans l'étendue par défaut. Cela équivaut à ajouter des enregistrements à une zone DNS standard.

Pour plus d'informations, consultez Add-DnsServerResourceRecord.

Créer les stratégies DNS

Après avoir créé les sous-réseaux, les partitions (étendues de zone) et ajouté des enregistrements, vous devez créer des stratégies qui connectent les sous-réseaux et les partitions, de sorte que lorsqu'une requête provient d'une source dans l'un des sous-réseaux clients DNS, la réponse à la requête est retournée à partir de l'étendue correcte de la zone. Aucune stratégie n'est requise pour le mappage de l'étendue de zone par défaut.

Après avoir configuré ces stratégies DNS, le comportement du serveur DNS est le suivant :

1. Les clients DNS européens reçoivent l'adresse IP du serveur web dans le centre de données de Dublin dans leur réponse à la requête DNS.
2. Les clients DNS américains reçoivent l'adresse IP du serveur Web dans le centre de données de Seattle dans leur réponse à la requête DNS.
3. Entre 6 h et 9 h à Dublin, 20 % des requêtes des clients européens reçoivent l'adresse IP du serveur Web dans le centre de données Seattle dans leur réponse de requête DNS.
4. Entre 6 h et 9 h à Seattle, 20 % des requêtes des clients américains reçoivent l'adresse IP du serveur Web dans le centre de données de Dublin dans leur réponse de requête DNS.
5. La moitié des requêtes du reste du monde reçoivent l'adresse IP du centre de données de Seattle et l'autre moitié reçoivent l'adresse IP du centre de données de Dublin.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer une stratégie DNS qui lie les sous-réseaux du client DNS et les étendues de zone.

> **Notes**
>
> Dans cet exemple, le serveur DNS étant dans le fuseau horaire GMT, les heures de pointe doivent être exprimées dans l'heure GMT équivalente.

PowerShell

```
Add-DnsServerQueryResolutionPolicy -Name "America6To9Policy" -Action ALLOW -
ClientSubnet "eq,AmericaSubnet" -ZoneScope "SeattleZoneScope,4;DublinZoneScope,1"
-TimeOfDay "EQ,01:00-04:00" -ZoneName "contosogiftservices.com" -ProcessingOrder 1

Add-DnsServerQueryResolutionPolicy -Name "Europe6To9Policy" -Action ALLOW -
ClientSubnet "eq,EuropeSubnet" -ZoneScope "SeattleZoneScope,1;DublinZoneScope,4" -
TimeOfDay "EQ,17:00-20:00" -ZoneName "contosogiftservices.com" -ProcessingOrder 2
```

```
Add-DnsServerQueryResolutionPolicy -Name "AmericaPolicy" -Action ALLOW -
ClientSubnet "eq,AmericaSubnet" -ZoneScope "SeattleZoneScope,1" -ZoneName
"contosogiftservices.com" -ProcessingOrder 3

Add-DnsServerQueryResolutionPolicy -Name "EuropePolicy" -Action ALLOW -
ClientSubnet "eq,EuropeSubnet" -ZoneScope "DublinZoneScope,1" -ZoneName
"contosogiftservices.com" -ProcessingOrder 4

Add-DnsServerQueryResolutionPolicy -Name "RestOfWorldPolicy" -Action ALLOW -
ZoneScope "DublinZoneScope,1;SeattleZoneScope,1" -ZoneName
"contosogiftservices.com" -ProcessingOrder 5
```

Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

À présent, le serveur DNS est configuré avec les stratégies DNS requises pour rediriger le trafic en fonction de l'emplacement géographique et de l'heure de la journée.

Lorsque le serveur DNS reçoit des requêtes de résolution de noms, le serveur DNS évalue les champs de la requête DNS par rapport aux stratégies DNS configurées. Si l'adresse IP source dans la demande de résolution de noms correspond à l'une des stratégies, l'étendue de zone associée est utilisée pour répondre à la requête et l'utilisateur est dirigé vers la ressource qui est géographiquement la plus proche d'elle.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Réponses DNS basées sur l'heure du jour avec un serveur d'applications Azure Cloud

Article • 14/04/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Vous pouvez utiliser cette rubrique pour apprendre à distribuer le trafic d'application entre différentes instances distribuées géographiquement d'une application à l'aide de stratégies DNS basées sur l'heure de la journée.

Ce scénario est utile dans les situations où vous souhaitez diriger le trafic dans un fuseau horaire vers d'autres serveurs d'applications, tels que des serveurs Web qui sont hébergés sur Microsoft Azure, se trouvant dans un autre fuseau horaire. Cela vous permet d'équilibrer la charge du trafic entre les instances d'application pendant les périodes de pointe lorsque vos serveurs principaux sont surchargés de trafic.

Notes

Pour savoir comment utiliser une stratégie DNS pour des réponses DNS intelligentes sans utiliser Azure, consultez **Utiliser la stratégie DNS pour les réponses DNS intelligentes en fonction de l'heure de la journée**.

Exemple des réponses DNS intelligentes basées sur l'heure du jour avec le serveur d'application Azure Cloud

Voici un exemple de la façon dont vous pouvez utiliser la stratégie DNS pour équilibrer le trafic d'application en fonction de l'heure de la journée.

Cet exemple utilise une société fictive, Contoso Gift Services, qui fournit des solutions de cadeaux en ligne dans le monde entier via son site Web, contosogiftservices.com.

Le site web contosogiftservices.com est hébergé uniquement dans un seul centre de données local à Seattle (avec l'adresse IP publique 192.68.30.2).

Le serveur DNS se trouve également dans le centre de données local.

Avec une récente augmentation de l’activité, contosogiftservices.com a un plus grand nombre de visiteurs chaque jour, et certains clients ont signalé des problèmes de disponibilité du service.

Contoso Gift Services effectue une analyse de site et découvre que tous les soirs entre 18h00 et 21h00, le trafic vers le serveur Web de Seattle augmente. Le serveur Web ne peut pas être mis à l’échelle pour gérer l’augmentation du trafic à ces heures de pointe, ce qui entraîne un déni de service pour les clients.

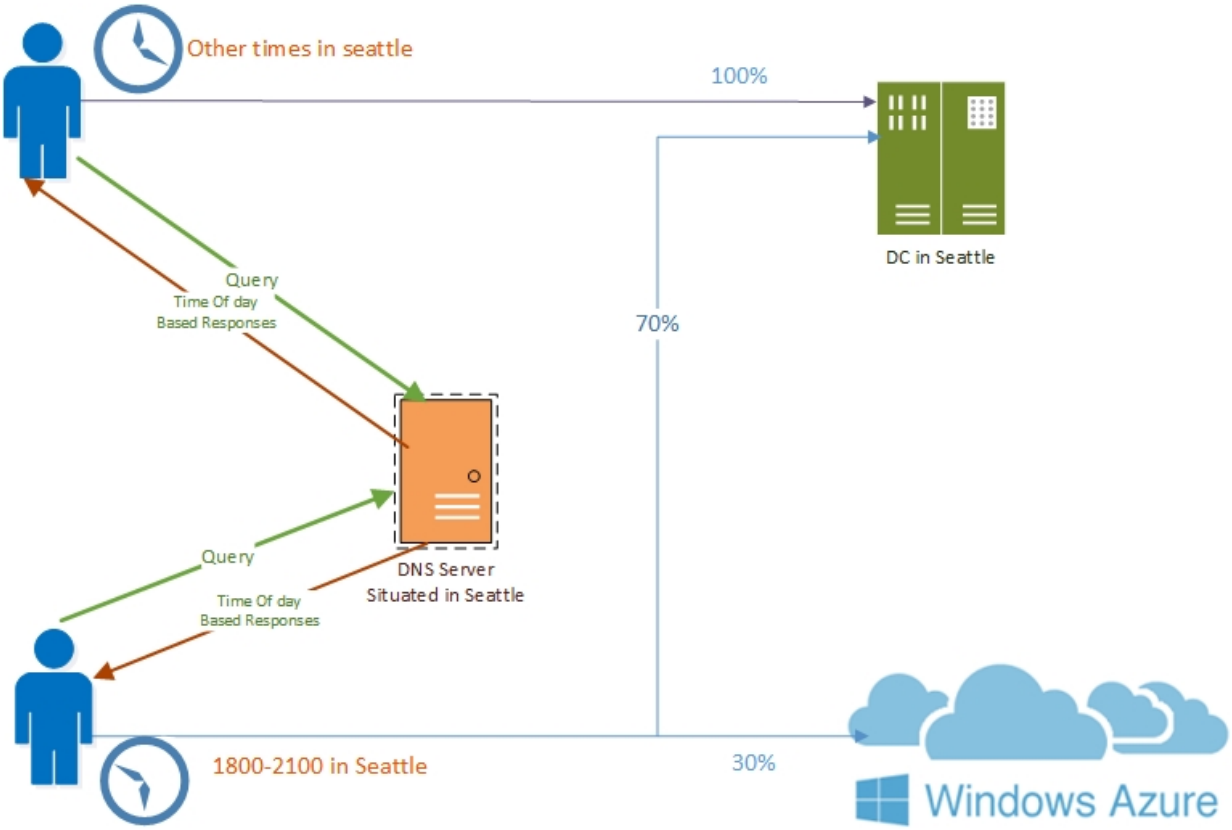
Pour s’assurer que les clients contosogiftservices.com bénéficient d’une expérience réactive à partir du site Web, pendant ces heures Contoso Gift Services décide de louer une machine virtuelle sur Microsoft Azure pour héberger une copie de son serveur Web.

Contoso Gift Services obtient une adresse IP publique d’Azure pour la machine virtuelle (192.68.31.44) et développe l’automatisation pour déployer le serveur web tous les jours sur Azure entre 17 h et 22 h, ce qui permet d’activer une période d’urgence d’une heure.

> ⓘ **Notes**
>
> Pour plus d'informations sur les machines virtuelles Azure, consultez **Documentation sur les machines virtuelles**.

Les serveurs DNS sont configurés avec des étendues de zone et des stratégies DNS afin que 30 % des requêtes soient envoyées à l’instance du serveur Web qui s’exécute dans Azure entre 17 h et 21 h chaque jour.

L’illustration suivante représente ce scénario.



Comment les réponses DNS intelligentes basées sur l'heure du jour avec le serveur d'application Azure fonctionnent

Cet article explique comment configurer le serveur DNS pour répondre aux requêtes DNS avec deux adresses IP de serveur d'applications différentes : un serveur web se trouve à Seattle et l'autre dans un centre de données Azure.

Après la configuration d'une nouvelle stratégie DNS basée sur les heures de pointe de 18 h à 21 h à Seattle, le serveur DNS envoie 70 % des réponses DNS aux clients contenant l'adresse IP du serveur Web Seattle, et trente pour cent des réponses DNS aux clients contenant l'adresse IP du serveur Web Azure, redirigeant ainsi le trafic client vers le nouveau serveur web Azure et empêchant la surcharge du serveur web Seattle.

À tous les autres moments de la journée, le traitement normal des requêtes a lieu et les réponses sont envoyées à partir de l'étendue de zone par défaut qui contient un enregistrement pour le serveur web dans le centre de données local.

La durée de vie de 10 minutes sur l'enregistrement Azure garantit que l'enregistrement a expiré à partir du cache LDNS avant la suppression de la machine virtuelle d'Azure. L'un des avantages de cette mise à l'échelle est que vous pouvez conserver vos données

DNS localement et continuer à effectuer un scale-out vers Azure en fonction de la demande.

Comment configurer une stratégie DNS pour les réponses DNS intelligentes basées sur l'heure du jour avec le serveur d'application Azure

Pour configurer la stratégie DNS pour les réponses de requête basées sur l'équilibrage de charge de l'application à l'heure de la journée, vous devez effectuer les étapes suivantes.

- Créer les étendues de zone
- Ajouter des enregistrements aux étendues de zone
- Créer les stratégies DNS

> **Notes**
>
> Vous devez effectuer ces étapes sur le serveur DNS faisant autorité pour la zone que vous souhaitez configurer. L'adhésion à DnsAdmins, ou un équivalent, est nécessaire pour effectuer les procédures suivantes.

Les sections suivantes fournissent des instructions de configuration détaillées.

> **Important**
>
> Les sections suivantes incluent des exemples de commandes Windows PowerShell qui contiennent des exemples de valeurs pour de nombreux paramètres. Veillez à remplacer les exemples de valeurs dans ces commandes par des valeurs appropriées à votre déploiement avant d'exécuter ces commandes.

Créer les étendues de zone

Une étendue de zone est une instance unique de la zone. Une zone DNS peut avoir plusieurs étendues de zone, chacune d'elles contenant son propre jeu d'enregistrements DNS. Le même enregistrement peut être présent dans plusieurs étendues, avec différentes adresses IP ou les mêmes adresses IP.

> **Notes**
>
> Par défaut, une étendue de zone existe sur les zones DNS. Cette étendue de zone a le même nom que la zone, et les opérations DNS héritées fonctionnent sur cette étendue.

Vous pouvez utiliser l'exemple de commande suivant pour créer une étendue de zone pour héberger les enregistrements Azure.

```
Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name
"AzureZoneScope"
```

Pour plus d'informations, consultez Add-DnsServerZoneScope

Ajouter des enregistrements aux étendues de zone

L'étape suivante consiste à ajouter les enregistrements représentant l'hôte du serveur web dans les étendues de zone.

Dans AzureZoneScope, l'enregistrement www.contosogiftservices.com est ajouté avec l'adresse IP 192.68.31.44, qui se trouve dans le cloud public Azure.

De même, dans l'étendue de zone par défaut (contosogiftservices.com), un enregistrement (www.contosogiftservices.com) est ajouté avec l'adresse IP 192.68.30.2 du serveur Web exécuté dans le centre de données local de Seattle.

Dans la deuxième applet de commande ci-dessous, le paramètre –ZoneScope n'est pas inclus. Pour cette raison, les enregistrements sont ajoutés dans zoneScope par défaut.

En outre, la durée de vie de l'enregistrement pour les machines virtuelles Azure est conservée à 600 s (10 minutes) afin que le LDNS ne le mette pas en cache plus longtemps, ce qui interférerait avec l'équilibrage de charge. En outre, les machines virtuelles Azure sont disponibles pendant 1 heure supplémentaire en cas d'urgence pour garantir que même les clients avec des enregistrements mis en cache sont en mesure de résoudre.

```
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name
"www" -IPv4Address "192.68.31.44" -ZoneScope "AzureZoneScope" –TimeToLive
600
```

```
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name
"www" -IPv4Address "192.68.30.2"
```

Pour plus d'informations, consultez Add-DnsServerResourceRecord.

Créer les stratégies DNS

Une fois les étendues de zone créées, vous pouvez créer des stratégies DNS qui distribuent les requêtes entrantes entre ces étendues afin que les opérations suivantes se produisent.

1. De 18 h à 21 h tous les jours, 30 % des clients reçoivent l'adresse IP du serveur Web dans le centre de données Azure dans la réponse DNS, tandis que 70 % des clients reçoivent l'adresse IP du serveur Web local de Seattle.
2. À tous les autres moments, tous les clients reçoivent l'adresse IP du serveur Web local de Seattle.

L'heure du jour doit être exprimé en heure locale du serveur DNS.

Vous pouvez utiliser l'exemple de commande suivant pour créer la stratégie DNS.

```
Add-DnsServerQueryResolutionPolicy -Name "Contoso6To9Policy" -Action ALLOW -
ZoneScope "contosogiftservices.com,7;AzureZoneScope,3" –TimeOfDay “EQ,18:00-
21:00” -ZoneName "contosogiftservices.com" –ProcessingOrder 1
```

Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

À présent, le serveur DNS est configuré avec les stratégies DNS requises pour rediriger le trafic vers le serveur Web Azure basé sur l'heure du jour.

Notez l'expression :

`-ZoneScope "contosogiftservices.com,7;AzureZoneScope,3" –TimeOfDay “EQ,18:00-21:00”`

Cette expression configure le serveur DNS avec une combinaison ZoneScope et de poids qui indique au serveur DNS d'envoyer l'adresse IP du serveur Web Seattle 70 % du temps, tout en envoyant l'adresse IP du serveur Web Azure 30 % du temps.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Utiliser une stratégie DNS pour un déploiement DNS Split-Brain dans Active Directory

30/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour tirer parti des fonctionnalités de gestion du trafic des stratégies DNS pour les déploiements de cerveau partagé avec des zones DNS intégrées Active Directory dans Windows Server 2016.

Dans Windows Server 2016, la prise en charge des stratégies DNS est étendue aux zones DNS intégrées à Active Directory. L'intégration d'Active Directory fournit des fonctionnalités de haute disponibilité multi-maître au serveur DNS.

Jusqu'à maintenant, ce scénario imposait aux administrateurs DNS de gérer deux serveurs DNS différents, chacun fournissant des services à chaque ensemble d'utilisateurs, interne et externe. Si quelques enregistrements à l'intérieur de la zone avaient fait l'objet d'un déploiement Split-Brain, ou si les deux instances de la zone (interne et externe) avaient été déléguées au même domaine parent, cela devenait un casse-tête de gestion.

> ⓘ **Notes**
>
> - Les déploiements DNS sont fractionnés lorsqu'il existe deux versions d'une seule zone, une version pour les utilisateurs internes sur l'intranet de l'organisation et une version pour les utilisateurs externes, qui sont généralement des utilisateurs sur Internet.
> - La rubrique **Utiliser une stratégie DNS pour Split-Brain déploiement DNS** explique comment utiliser des stratégies DNS et des étendues de zone pour déployer un système DNS à cerveau partagé sur un serveur DNS unique Windows Server 2016.

Exemple DNS Split-Brain dans Active Directory

Cet exemple utilise une société fictive, Contoso, qui gère un site web de carrière à l'adresse `www.career.contoso.com`.

Le site existe en deux versions. La première version s'adresse aux utilisateurs internes et propose des offres d'emploi en interne. Ce site interne est disponible à l'adresse IP locale

10.0.0.39.

La deuxième version est la version publique du même site, disponible à l'adresse IP publique 65.55.39.10.

En l'absence de stratégie DNS, l'administrateur doit héberger ces deux zones sur des serveurs DNS Windows Server distincts, et les gérer séparément.

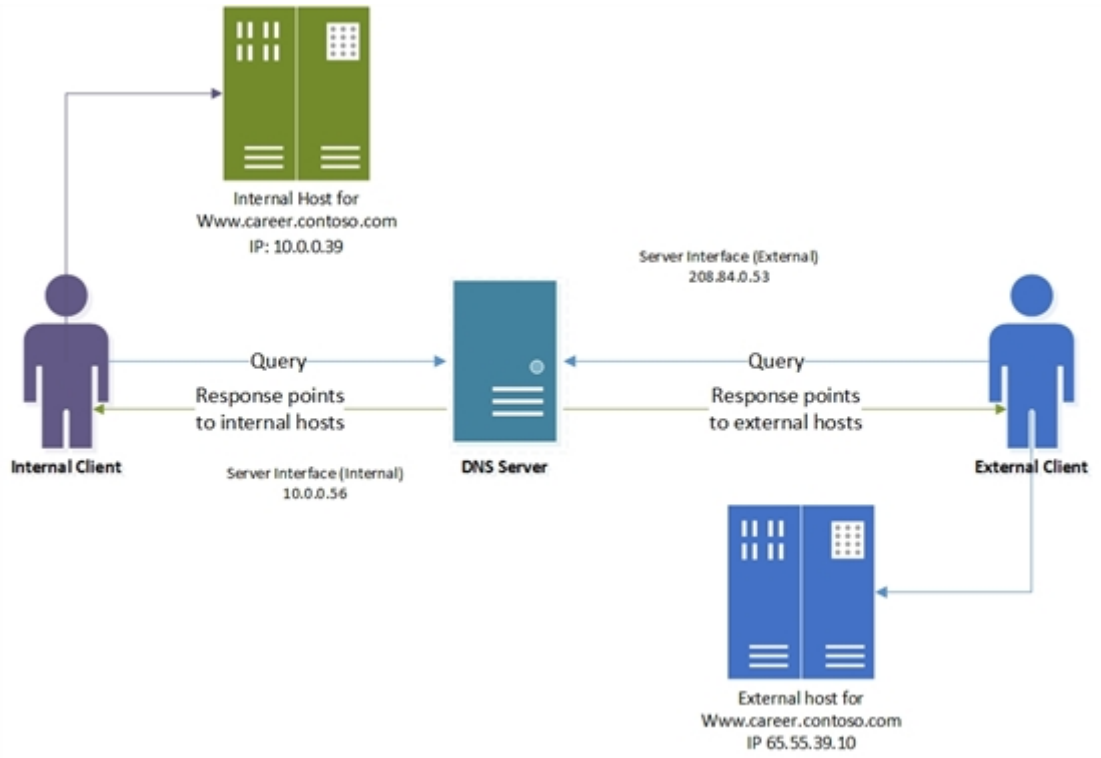
À l'aide de stratégies DNS, ces zones peuvent désormais être hébergées sur le même serveur DNS.

Si le serveur DNS pour contoso.com est intégré à Active Directory et écoute deux interfaces réseau, l'administrateur DNS de Contoso peut suivre les étapes décrites dans cette rubrique pour obtenir un déploiement à cerveau partagé.

L'administrateur DNS configure les interfaces du serveur DNS avec les adresses IP suivantes.

- La carte réseau accessible sur Internet est configurée avec une adresse IP publique 208.84.0.53 pour les requêtes externes.
- La carte réseau intranet est configurée avec une adresse IP privée 10.0.0.56 pour les requêtes internes.

L'illustration suivante représente ce scénario.



Fonctionnement de la stratégie DNS pour Split-Brain DNS dans Active Directory

Quand le serveur DNS est configuré avec les stratégies DNS nécessaires, chaque requête de résolution de noms est évaluée par rapport aux stratégies du serveur DNS.

L'interface serveur est utilisée dans cet exemple en tant que critère pour différencier les clients internes et externes.

Si l'interface serveur sur laquelle la requête est reçue correspond à l'une des stratégies, l'étendue de zone associée est utilisée pour répondre à la requête.

Par conséquent, dans notre exemple, les requêtes DNS pour `www.career.contoso.com` lesquelles elles sont reçues sur l'adresse IP privée (10.0.0.56) reçoivent une réponse DNS qui contient une adresse IP interne ; et les requêtes DNS reçues sur l'interface réseau publique reçoivent une réponse DNS qui contient l'adresse IP publique dans l'étendue de la zone par défaut (il s'agit de la même chose que la résolution de requête normale).

La prise en charge des mises à jour et du balayage dns dynamique (DDNS) est prise en charge uniquement sur l'étendue de zone par défaut. Étant donné que les clients internes sont approvisionnés par l'étendue de zone par défaut, les administrateurs DNS de Contoso peuvent continuer à utiliser les mécanismes existants (DNS dynamique ou statique) pour mettre à jour les enregistrements dans contoso.com. Pour les étendues de zone autres que les étendues par défaut (telles que l'étendue externe dans cet exemple), la prise en charge de DDNS ou de récupération n'est pas disponible.

Haute disponibilité des stratégies

Les stratégies DNS ne sont pas intégrées à Active Directory. Pour cette raison, les stratégies DNS ne sont pas répliquées sur les autres serveurs DNS qui hébergent la même zone intégrée Active Directory.

Les stratégies DNS sont stockées sur le serveur DNS local. Vous pouvez facilement exporter des stratégies DNS d'un serveur à un autre à l'aide de l'exemple suivant des commandes Windows PowerShell.

PowerShell

```
$policies = Get-DnsServerQueryResolutionPolicy -ZoneName "contoso.com" -
ComputerName Server01
$policies |  Add-DnsServerQueryResolutionPolicy -ZoneName "contoso.com" -
ComputerName Server02
```

Pour plus d'informations, consultez les rubriques de référence Windows PowerShell suivantes.

- Get-DnsServerQueryResolutionPolicy
- Add-DnsServerQueryResolutionPolicy

Guide pratique pour configurer une stratégie DNS pour Split-Brain DNS dans Active Directory

Pour configurer le déploiement Split-Brain DNS à l'aide d'une stratégie DNS, vous devez utiliser les sections suivantes, qui fournissent des instructions de configuration détaillées.

Ajouter la zone intégrée Active Directory

Vous pouvez utiliser l'exemple de commande suivant pour ajouter la zone de contoso.com intégrée Active Directory au serveur DNS.

PowerShell

```
Add-DnsServerPrimaryZone -Name "contoso.com" -ReplicationScope "Domain" -PassThru
```

For more information, see Add-DnsServerPrimaryZone.

Créer les étendues de la zone

Vous pouvez utiliser cette section pour partitionner la zone contoso.com créer une étendue de zone externe.

Une étendue de zone est une instance unique de la zone. Une zone DNS peut avoir plusieurs étendues de zone, chacune d'elles contenant son propre jeu d'enregistrements DNS. Le même enregistrement peut être présent dans plusieurs étendues, avec des adresses IP différentes ou les mêmes adresses IP.

Étant donné que vous ajoutez cette nouvelle étendue de zone dans une zone intégrée Active Directory, l'étendue de zone et les enregistrements qu'elle contient sont répliqués via Active Directory sur d'autres serveurs réplicas du domaine.

Par défaut, une étendue de zone existe dans chaque zone DNS. Cette étendue de zone porte le même nom que la zone, et les opérations DNS héritées fonctionnent sur cette étendue. Cette étendue de zone par défaut hébergera la version interne de `www.career.contoso.com`.

Vous pouvez utiliser l'exemple de commande suivant pour créer l'étendue de zone sur le serveur DNS.

PowerShell

```
Add-DnsServerZoneScope -ZoneName "contoso.com" -Name "external"
```

For more information, see Add-DnsServerZoneScope.

Ajouter des enregistrements aux étendues de zone

L'étape suivante consiste à ajouter les enregistrements représentant l'hôte du serveur web dans les deux étendues de zone : externe et par défaut (pour les clients internes).

Dans l'étendue de zone interne par défaut, l'enregistrement `www.career.contoso.com` est ajouté avec l'adresse IP 10.0.0.39, qui est une adresse IP privée ; et dans l'étendue de zone externe, le même enregistrement (www.career.contoso.com) est ajouté avec l'adresse IP publique 65.55.39.10.

Les enregistrements (à la fois dans l'étendue de zone interne par défaut et l'étendue de zone externe) sont automatiquement répliqués sur le domaine avec leurs étendues de zone respectives.

Vous pouvez utiliser l'exemple de commande suivant pour ajouter des enregistrements aux étendues de zone sur le serveur DNS.

PowerShell

```
Add-DnsServerResourceRecord -ZoneName "contoso.com" -A -Name "www.career" -
IPv4Address "65.55.39.10" -ZoneScope "external"
Add-DnsServerResourceRecord -ZoneName "contoso.com" -A -Name "www.career" -
IPv4Address "10.0.0.39”
```

> ⓘ **Notes**
>
> The **–ZoneScope** parameter is not included when the record is added to the default zone scope. Cette action est identique à l'ajout d'enregistrements à une zone normale.

For more information, see Add-DnsServerResourceRecord.

Créer les stratégies DNS

Une fois que vous avez identifié les interfaces serveur du réseau externe et du réseau interne, et que vous avez créé les étendues de zone, vous devez créer des stratégies DNS qui connectent les étendues de zone interne et externe.

> ⓘ **Notes**

Cet exemple utilise l'interface du serveur (le paramètre -ServerInterface dans l'exemple de commande ci-dessous) comme critères pour différencier les clients internes et externes. Une autre méthode permet de différencier les clients externes et internes : elle consiste à utiliser des sous-réseaux clients en tant que critères. Si vous pouvez identifier les sous-réseaux auxquels appartiennent les clients internes, vous pouvez configurer la stratégie DNS de différenciation basée sur le sous-réseau client. Pour plus d'informations sur la configuration de la gestion du trafic à l'aide de critères liés aux sous-réseaux clients, consultez Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des serveurs primaires.

Après avoir configuré des stratégies, lorsqu'une requête DNS est reçue sur l'interface publique, la réponse est retournée à partir de l'étendue externe de la zone.

> **Notes**
>
> Aucune stratégie n'est requise pour le mappage de l'étendue de zone interne par défaut.

PowerShell

```
Add-DnsServerQueryResolutionPolicy -Name "SplitBrainZonePolicy" -Action ALLOW -
ServerInterface "eq,208.84.0.53" -ZoneScope "external,1" -ZoneName contoso.com
```

> **Notes**
>
> 208.84.0.53 est l'adresse IP sur l'interface réseau publique.

For more information, see Add-DnsServerQueryResolutionPolicy.

À présent, le serveur DNS est configuré avec les stratégies DNS requises pour un serveur de noms à cerveau partagé avec une zone DNS intégrée Active Directory.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Utiliser une stratégie DNS pour un déploiement DNS Split-Brain

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique afin de découvrir comment configurer une stratégie DNS dans Windows Server® 2016 pour les déploiements DNS Split-Brain, où il existe deux versions d'une seule zone : l'une pour les utilisateurs internes situés sur l'intranet de votre organisation, et l'autre pour les utilisateurs externes, qui sont généralement des utilisateurs situés sur Internet.

> ⓘ **Notes**
>
> Pour plus d'informations sur l'utilisation d'une stratégie DNS dans le cadre d'un déploiement DNS Split-Brain avec des zones DNS intégrées à Active Directory, consultez **Utiliser une stratégie DNS pour un déploiement DNS Split-Brain dans Active Directory**.

Jusqu'à maintenant, ce scénario imposait aux administrateurs DNS de gérer deux serveurs DNS différents, chacun fournissant des services à chaque ensemble d'utilisateurs, interne et externe. Si quelques enregistrements à l'intérieur de la zone avaient fait l'objet d'un déploiement Split-Brain, ou si les deux instances de la zone (interne et externe) avaient été déléguées au même domaine parent, cela devenait un casse-tête de gestion.

Le contrôle de récursivité sélective pour la résolution de noms DNS est un autre scénario de configuration du déploiement Split-Brain. Parfois, les serveurs DNS d'entreprise sont censés effectuer une résolution récursive via Internet pour les utilisateurs internes. En même temps, ils doivent également agir en tant que serveurs de noms faisant autorité pour les utilisateurs externes, et bloquer la récursivité dans ce cas.

Cette rubrique contient les sections suivantes.

- Exemple de déploiement DNS Split-Brain
- Exemple de contrôle de récursivité sélective DNS

Exemple de déploiement DNS Split-Brain

Vous trouverez ci-dessous un exemple de la façon dont vous pouvez utiliser la stratégie DNS pour mettre en œuvre le scénario de DNS Split-Brain décrit plus haut.

Cette section contient les rubriques suivantes :

- Fonctionnement du déploiement DNS Split-Brain
- Guide pratique pour configurer le déploiement DNS Split-Brain

Cet exemple utilise une société fictive, Contoso, qui gère un site web de carrière à l'adresse `www.career.contoso.com`.

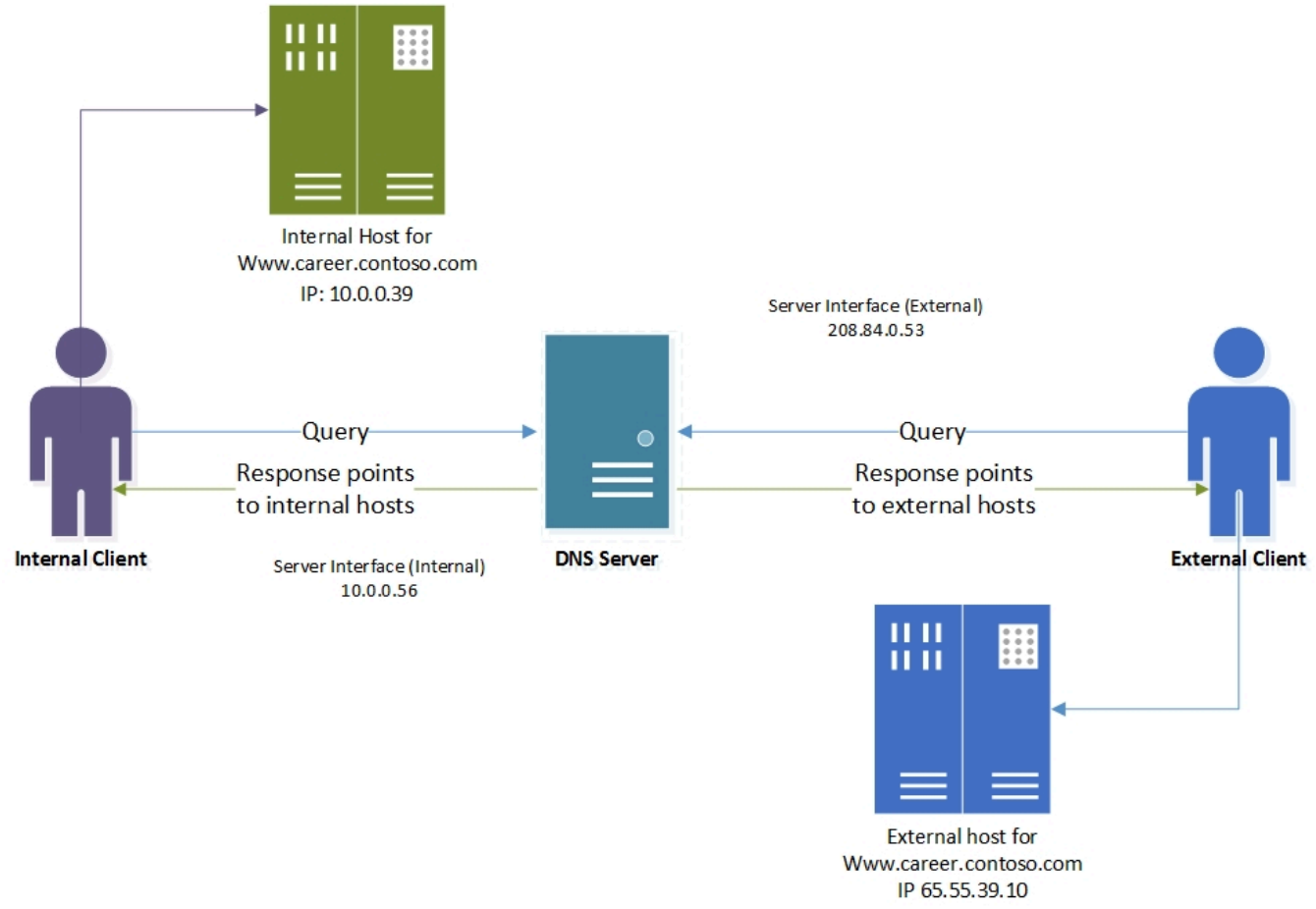
Le site existe en deux versions. La première version s'adresse aux utilisateurs internes et propose des offres d'emploi en interne. Ce site interne est disponible à l'adresse IP locale 10.0.0.39.

La deuxième version est la version publique du même site, disponible à l'adresse IP publique 65.55.39.10.

En l'absence de stratégie DNS, l'administrateur doit héberger ces deux zones sur des serveurs DNS Windows Server distincts, et les gérer séparément.

À l'aide de stratégies DNS, ces zones peuvent désormais être hébergées sur le même serveur DNS.

L'illustration suivante représente ce scénario.



Fonctionnement du déploiement DNS Split-Brain

Quand le serveur DNS est configuré avec les stratégies DNS nécessaires, chaque requête de résolution de noms est évaluée par rapport aux stratégies du serveur DNS.

L'interface serveur est utilisée dans cet exemple en tant que critère pour différencier les clients internes et externes.

Si l'interface serveur sur laquelle la requête est reçue correspond à l'une des stratégies, l'étendue de zone associée est utilisée pour répondre à la requête.

Par conséquent, dans notre exemple, les requêtes DNS pour `www.career.contoso.com` lesquelles elles sont reçues sur l'adresse IP privée (10.0.0.56) reçoivent une réponse DNS qui contient une adresse IP interne ; et les requêtes DNS reçues sur l'interface réseau publique reçoivent une réponse DNS qui contient l'adresse IP publique dans l'étendue de la zone par défaut (il s'agit de la même chose que la résolution de requête normale).

Guide pratique pour configurer le déploiement DNS Split-Brain

Pour configurer le déploiement DNS Split-Brain à l'aide d'une stratégie DNS, vous devez suivre les étapes ci-dessous.

- Créer les étendues de zone
- Ajouter des enregistrements aux étendues de zone
- Créer les stratégies DNS

Les sections suivantes fournissent des instructions de configuration détaillées.

> **Important**
>
> Les sections suivantes incluent des exemples de commandes Windows PowerShell qui contiennent des exemples de valeurs pour de nombreux paramètres. Veillez à remplacer les exemples de valeurs dans ces commandes par des valeurs appropriées à votre déploiement avant d'exécuter ces commandes.

Créer les étendues de zone

Une étendue de zone est une instance unique de la zone. Une zone DNS peut avoir plusieurs étendues de zone, chacune d'elles contenant son propre jeu d'enregistrements DNS. Le même

enregistrement peut être présent dans plusieurs étendues, avec des adresses IP différentes ou les mêmes adresses IP.

> ⓘ **Notes**
>
> Par défaut, une étendue de zone existe sur les zones DNS. Cette étendue de zone porte le même nom que la zone, et les opérations DNS héritées fonctionnent sur cette étendue. Cette étendue de zone par défaut hébergera la version externe de `www.career.contoso.com`.

Vous pouvez utiliser l'exemple de commande suivant pour partitionner l'étendue de zone contoso.com afin de créer une étendue de zone interne. L'étendue de zone interne sera utilisée pour conserver la version interne de `www.career.contoso.com`.

```
Add-DnsServerZoneScope -ZoneName "contoso.com" -Name "internal"
```

Pour plus d'informations, consultez Add-DnsServerZoneScope

Ajouter des enregistrements aux étendues de zone

L'étape suivante consiste à ajouter les enregistrements représentant l'hôte du serveur web aux deux étendues de zone : interne et par défaut (pour les clients externes).

Dans l'étendue de zone interne par défaut, l'enregistrement **www.career.contoso.com** est ajouté avec l'adresse IP 10.0.0.39, qui est une adresse IP privée. Dans l'étendue de zone externe par défaut, le même enregistrement, **www.career.contoso.com**, est ajouté avec l'adresse IP publique 65.55.39.10.

Aucun paramètre **-ZoneScope** n'est fourni dans les exemples de commandes suivants quand l'enregistrement est ajouté à l'étendue de zone par défaut. L'opération est similaire à l'ajout d'enregistrements à une zone standard.

```
Add-DnsServerResourceRecord -ZoneName "contoso.com" -A -Name "www.career" -IPv4Address "65.55.39.10" Add-DnsServerResourceRecord -ZoneName "contoso.com" -A -Name "www.career" -IPv4Address "10.0.0.39” -ZoneScope "internal"
```

Pour plus d'informations, consultez Add-DnsServerResourceRecord.

Créer les stratégies DNS

Une fois que vous avez identifié les interfaces serveur du réseau externe et du réseau interne, et que vous avez créé les étendues de zone, vous devez créer des stratégies DNS qui

connectent les étendues de zone interne et externe.

> ⓘ **Notes**
>
> Cet exemple utilise l'interface serveur en tant que critère pour différencier les clients internes et externes. Une autre méthode permet de différencier les clients externes et internes : elle consiste à utiliser des sous-réseaux clients en tant que critères. Si vous pouvez identifier les sous-réseaux auxquels appartiennent les clients internes, vous pouvez configurer la stratégie DNS de différenciation basée sur le sous-réseau client. Pour plus d'informations sur la configuration de la gestion du trafic à l'aide de critères liés aux sous-réseaux clients, consultez **Utiliser une stratégie DNS pour la gestion du trafic basée sur la géolocalisation avec des serveurs primaires**.

Quand le serveur DNS reçoit une requête sur l'interface privée, la réponse à la requête DNS est retournée à partir de l'étendue de zone interne.

> ⓘ **Notes**
>
> Aucune stratégie n'est requise pour le mappage de l'étendue de zone par défaut.

Dans l'exemple de commande suivant, 10.0.0.56 est l'adresse IP sur l'interface réseau privée, comme le montre l'illustration précédente.

```
Add-DnsServerQueryResolutionPolicy -Name "SplitBrainZonePolicy" -Action ALLOW -
ServerInterface "eq,10.0.0.56" -ZoneScope "internal,1" -ZoneName contoso.com
```

Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

Exemple de contrôle de récursivité sélective DNS

Vous trouverez ci-dessous un exemple de la façon dont vous pouvez utiliser la stratégie DNS pour mettre en œuvre le scénario de contrôle de récursivité sélective DNS décrit ci-dessus.

Cette section contient les rubriques suivantes :

- Fonctionnement du contrôle de récursivité sélective DNS
- Guide pratique pour configurer le contrôle de récursivité sélective DNS

Cet exemple utilise la même société fictive que dans l'exemple précédent, Contoso, qui gère un site web de carrière à l'adresse `www.career.contoso.com`.

Dans l'exemple de déploiement DNS Split-Brain, le même serveur DNS répond aux clients externes et internes, et leur fournit des réponses différentes.

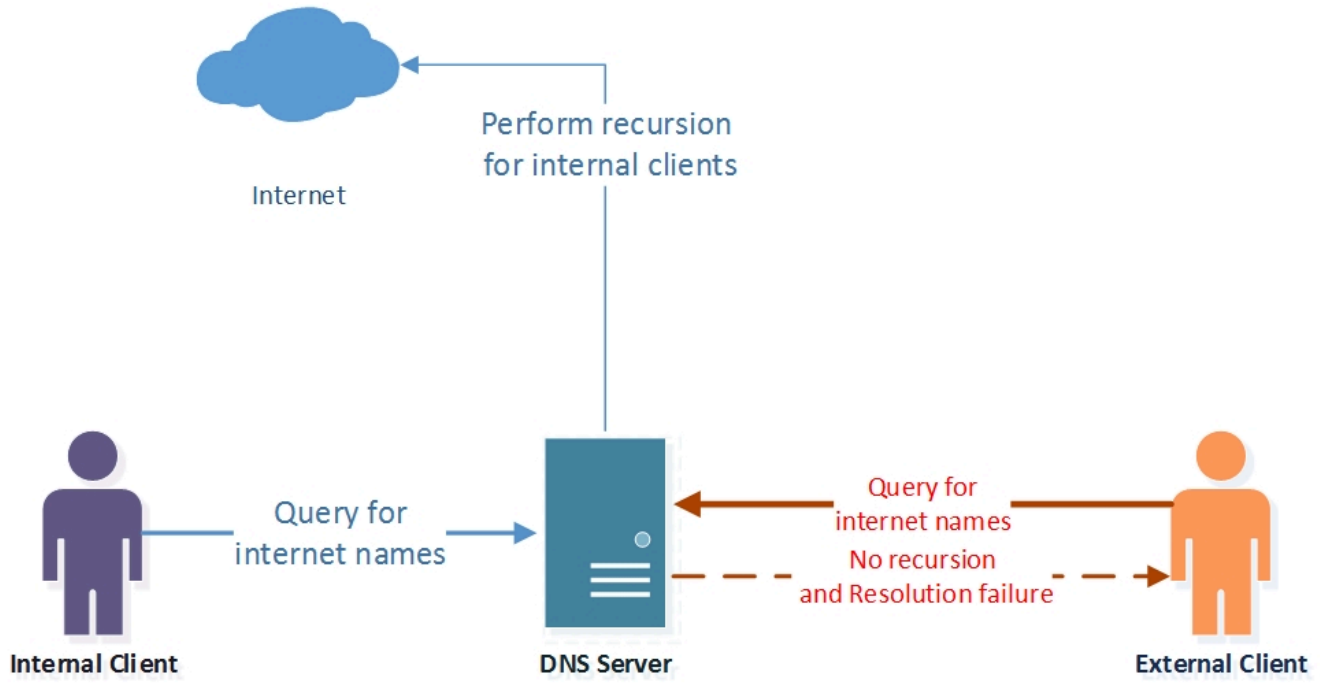
Certains déploiements DNS peuvent nécessiter le même serveur DNS pour effectuer une résolution de noms récursive pour les clients internes, en plus de servir de serveur de noms faisant autorité pour les clients externes. Ce cas de figure est appelé contrôle de récursivité sélective DNS.

Dans les versions précédentes de Windows Server, l'activation de la récursivité signifiait qu'elle était activée sur l'ensemble du serveur DNS pour toutes les zones. Dans la mesure où le serveur DNS écoute également les requêtes externes, la récursivité est activée pour les clients internes et externes, ce qui fait du serveur DNS un programme de résolution ouvert.

Un serveur DNS configuré en tant que programme de résolution ouvert peut être vulnérable à l'épuisement des ressources. Des clients malveillants peuvent s'en servir pour créer des attaques par réflexion.

C'est la raison pour laquelle les administrateurs DNS de Contoso ne souhaitent pas que le serveur DNS de contoso.com effectue la résolution de noms récursive pour les clients externes. Un contrôle de récursivité est uniquement nécessaire pour les clients internes, vous pouvez le bloquer pour les clients externes.

L'illustration suivante représente ce scénario.



Fonctionnement du contrôle de récursivité sélective DNS

Si une requête pour laquelle le serveur DNS Contoso ne fait pas autorité est reçue, par exemple dans le cas de https://www.microsoft.com, la requête de résolution de noms est évaluée par rapport aux stratégies du serveur DNS.

Dans la mesure où ces requêtes n'appartiennent à aucune zone, les stratégies au niveau de la zone (définies dans l'exemple de déploiement Split-Brain) ne sont pas évaluées.

Le serveur DNS évalue les stratégies de récursivité, et vérifie si les requêtes reçues sur l'interface privée correspondent à **SplitBrainRecursionPolicy**. Cette stratégie pointe vers une étendue de récursivité où la récursivité est activée.

Le serveur DNS effectue ensuite une récursivité afin d'obtenir la réponse pour https://www.microsoft.com à partir d'Internet, puis met en cache la réponse localement.

Si la requête est reçue sur l'interface externe, aucune stratégie DNS ne correspond, et le paramètre de récursivité par défaut (dans ce cas **Disabled**) est appliqué.

Cela empêche le serveur d'agir en tant que programme de résolution ouvert pour les clients externes, alors qu'il agit en tant que programme de résolution de cache DNS pour les clients internes.

Guide pratique pour configurer le contrôle de récursivité sélective DNS

Pour configurer le contrôle de récursivité sélective DNS à l'aide de la stratégie DNS, vous devez suivre les étapes ci-dessous.

- Créer des étendues de récursivité DNS
- Créer des stratégies de récursivité DNS

Créer des étendues de récursivité DNS

Les étendues de récursivité sont des instances uniques d'un groupe de paramètres qui contrôlent la récursivité sur un serveur DNS. Une étendue de récursivité contient une liste de redirecteurs et indique si la récursivité est activée. Un serveur DNS peut comporter de nombreuses étendues de récursivité.

Le paramètre de récursivité hérité et la liste des redirecteurs sont désignés sous le nom d'étendue de récursivité par défaut. Vous ne pouvez pas ajouter ou supprimer l'étendue de récursivité par défaut, identifiée par le nom « . » (point).

Dans cet exemple, le paramètre de récursivité par défaut est désactivé, tandis qu'une nouvelle étendue de récursivité pour les clients internes est créée là où la récursivité est activée.

PowerShell

```
Set-DnsServerRecursionScope -Name . -EnableRecursion $False
Add-DnsServerRecursionScope -Name "InternalClients" -EnableRecursion $True
```

Pour plus d'informations, consultez Add-DnsServerRecursionScope

Créer des stratégies de récursivité DNS

Vous pouvez créer des stratégies de récursivité de serveur DNS afin de choisir une étendue de récursivité pour un ensemble de requêtes correspondant à des critères spécifiques.

Si le serveur DNS ne fait pas autorité pour certaines requêtes, les stratégies de récursivité du serveur DNS vous permettent de contrôler le mode de résolution des requêtes.

Dans cet exemple, l'étendue de récursivité interne avec activation de la récursivité, est associée à l'interface réseau privée.

Vous pouvez utiliser l'exemple de commande suivant pour configurer des stratégies de récursivité DNS.

PowerShell

```
Add-DnsServerQueryResolutionPolicy -Name "SplitBrainRecursionPolicy" -Action ALLOW
-ApplyOnRecursion -RecursionScope "InternalClients" -ServerInterfaceIP
"EQ,10.0.0.39"
```

Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

Le serveur DNS est désormais configuré avec les stratégies DNS nécessaires pour un serveur de noms Split-Brain ou un serveur DNS avec contrôle de récursivité sélective activé pour les clients internes.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Pour plus d'informations, consultez le Guide de scénario de stratégie DNS.

Utiliser une stratégie DNS pour l'application de filtres sur les requêtes DNS

08/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique pour apprendre à configurer une stratégie DNS dans Windows Server® 2016 afin de créer des filtres de requête basés sur les critères que vous fournissez.

Les filtres de requête dans la stratégie DNS vous permettent de configurer le serveur DNS pour répondre de manière personnalisée en fonction de la requête DNS et du client DNS qui envoie la requête DNS.

Par exemple, vous pouvez configurer une stratégie DNS avec une liste de blocages de filtre de requête qui bloque les requêtes DNS à partir de domaines malveillants connus, ce qui empêche DNS de répondre aux requêtes de ces domaines. Étant donné qu'aucune réponse n'est envoyée à partir du serveur DNS, la requête DNS du membre de domaine malveillant expire.

Un autre exemple consiste à créer une liste verte de filtre de requête qui autorise uniquement un ensemble spécifique de clients à résoudre certains noms.

Critères de filtre de requête

Vous pouvez créer des filtres de requête avec n'importe quelle combinaison logique (ET/OU/PAS) des critères suivants.

Agrandir le tableau

Name	Description
Sous-réseau client	Nom d'un sous-réseau client prédéfini. Permet de vérifier le sous-réseau à partir duquel la requête a été envoyée.
Protocole de transfert	Protocole de transport utilisé dans la requête. Les valeurs possibles sont UDP et TCP.
Internet Protocol	Protocole réseau utilisé dans la requête. Les valeurs possibles sont IPv4 et IPv6.
Adresse IP de l'interface serveur	Adresse IP de l'interface réseau du serveur DNS qui a reçu la requête DNS.

Name	Description
FQDN	Nom de domaine complet de l'enregistrement dans la requête, avec la possibilité d'utiliser un caractère générique.
Type de requête	Type d'enregistrement interrogé (A, SRV, TXT, etc.)
Heure de la journée	Heure de la réception de la requête.

Les exemples suivants vous montrent comment créer des filtres pour la stratégie DNS qui bloquent ou autorisent les requêtes de résolution de noms DNS.

> ⓘ **Notes**
>
> Les exemples de commandes de cette rubrique utilisent la commande Windows PowerShell **Add-DnsServerQueryResolutionPolicy**. Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

Bloquer les requêtes d'un domaine

Dans certains cas, vous pouvez bloquer la résolution de noms DNS pour les domaines que vous avez identifiés comme malveillants ou pour les domaines qui ne sont pas conformes aux instructions d'utilisation de votre organisation. Vous pouvez effectuer des requêtes de blocage pour des domaines à l'aide d'une stratégie DNS.

La stratégie que vous configurez dans cet exemple n'est pas créée sur une zone particulière. Au lieu de cela, vous créez une stratégie au niveau du serveur qui est appliquée à toutes les zones configurées sur le serveur DNS. Les stratégies au niveau du serveur sont les premières à être évaluées et sont donc les premières à être mises en correspondance lorsqu'une requête est reçue par le serveur DNS.

L'exemple de commande suivant configure une stratégie au niveau du serveur pour bloquer toutes les requêtes avec le **suffixe de domaine contosomalicious.com**.

```
Add-DnsServerQueryResolutionPolicy -Name "BlockListPolicy" -Action IGNORE -FQDN "EQ,*.contosomalicious.com" -PassThru
```

> ⓘ **Notes**
>
> Lorsque vous configurez le paramètre **Action** avec la valeur **IGNORE**, le serveur DNS est configuré pour supprimer les requêtes sans aucune réponse. Le client DNS dans le domaine malveillant expire alors.

Bloquer les requêtes à partir d’un sous-réseau

Avec cet exemple, vous pouvez bloquer les requêtes à partir d’un sous-réseau s’il est infecté par un programme malveillant et tente de contacter des sites malveillants à l’aide de votre serveur DNS.

' Add-DnsServerClientSubnet -Name « MaliciousSubnet06 » -IPv4Subnet 172.0.33.0/24 -PassThru

Add-DnsServerQueryResolutionPolicy -Name « BlockListPolicyMalicious06 » -Action IGNORER -ClientSubnet « EQ, MaliciousSubnet06 » -PassThru '

L’exemple suivant montre comment utiliser les critères de sous-réseau en combinaison avec les critères de nom de domaine complet pour bloquer les requêtes de certains domaines malveillants provenant de sous-réseaux infectés.

```
Add-DnsServerQueryResolutionPolicy -Name "BlockListPolicyMalicious06" -Action IGNORE -ClientSubnet "EQ,MaliciousSubnet06" –FQDN “EQ,*.contosomalicious.com” -PassThru
```

Bloquer un type de requête

Vous devrez peut-être bloquer la résolution de noms pour certains types de requêtes sur vos serveurs. Par exemple, vous pouvez bloquer la requête « ANY », qui peut être utilisée de manière malveillante pour créer des attaques d’amplification.

```
Add-DnsServerQueryResolutionPolicy -Name "BlockListPolicyQType" -Action IGNORE -QType "EQ,ANY" -PassThru
```

Autoriser les requêtes uniquement à partir d’un domaine

Vous pouvez non seulement utiliser la stratégie DNS pour bloquer les requêtes, mais également les utiliser pour approuver automatiquement des requêtes provenant de domaines ou de sous-réseaux spécifiques. Lorsque vous configurez des listes d’autorisation, le serveur DNS traite uniquement les requêtes provenant de domaines autorisés, tout en bloquant toutes les autres requêtes provenant d’autres domaines.

L’exemple de commande suivant autorise uniquement les ordinateurs et les appareils des domaines contoso.com et enfants à interroger le serveur DNS.

```
Add-DnsServerQueryResolutionPolicy -Name "AllowListPolicyDomain" -Action IGNORE -FQDN "NE,*.contoso.com" -PassThru
```

Autoriser les requêtes uniquement à partir d'un sous-réseau

Vous pouvez également créer des listes vertes pour les sous-réseaux IP, afin que toutes les requêtes qui ne proviennent pas de ces sous-réseaux soient ignorées.

```
Add-DnsServerClientSubnet -Name "AllowedSubnet06" -IPv4Subnet 172.0.33.0/24 -PassThru
Add-DnsServerQueryResolutionPolicy -Name "AllowListPolicySubnet" -Action IGNORE -ClientSubnet "NE, AllowedSubnet06" -PassThru
```

Autoriser uniquement certains QTYPE

Vous pouvez appliquer des listes vertes à QTYPE.

Par exemple, si vous avez des clients externes qui interrogent l'interface de serveur DNS 164.8.1.1, seuls certains QTYPE sont autorisés à être interrogés, tandis qu'il existe d'autres QTYPE, comme les enregistrements SRV ou TXT, qui sont utilisés par les serveurs internes à des fins de résolution de noms ou à des fins de surveillance.

```
Add-DnsServerQueryResolutionPolicy -Name "AllowListQType" -Action IGNORE -QType "NE,A,AAAA,MX,NS,SOA" –ServerInterface "EQ,164.8.1.1" -PassThru
```

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Utiliser une stratégie DNS pour l'équilibrage de charge des applications

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez utiliser cette rubrique afin de découvrir comment configurer une stratégie DNS pour effectuer l'équilibrage de charge des applications.

Les versions précédentes du DNS Windows Server fournissaient uniquement l'équilibrage de charge à l'aide de réponses tourniquet (round robin). Avec DNS dans Windows Server 2016, vous pouvez cependant configurer une stratégie DNS pour l'équilibrage de charge des applications.

Lorsque vous avez déployé plusieurs instances d'une application, vous pouvez utiliser une stratégie DNS pour équilibrer la charge du trafic entre les différentes instances d'application, en allouant dynamiquement la charge de trafic pour l'application.

Exemple d'équilibrage de charge d'application

Voici un exemple d'utilisation de la stratégie DNS pour l'équilibrage de charge des applications.

Cet exemple utilise une société fictive - Contoso Gift Services - qui fournit des services de cadeaux en ligne, et qui a un site Web nommé **contosogiftservices.com**.

Le site Web contosogiftservices.com est hébergé dans plusieurs centres de données qui ont chacun des adresses IP différentes.

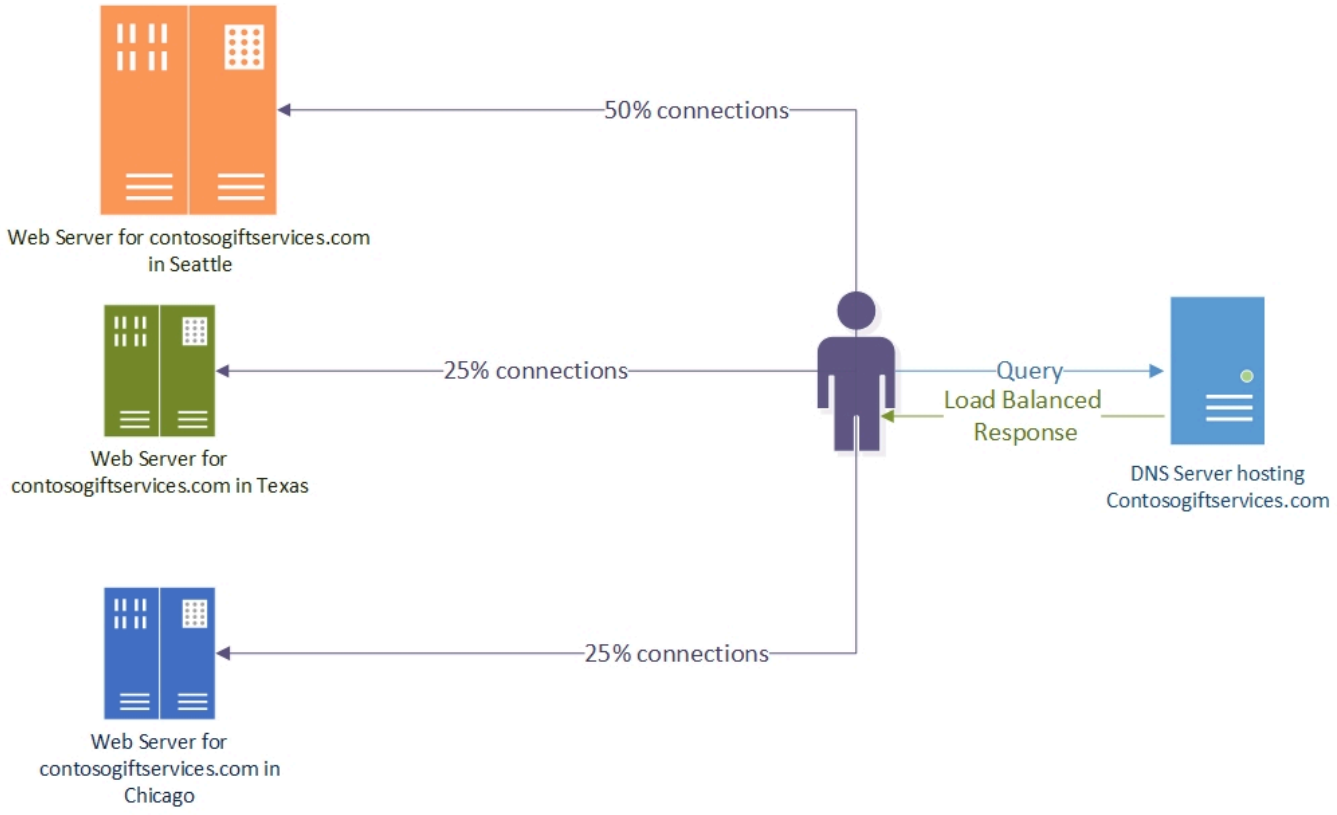
En Amérique du Nord, marché principal de Contoso Gift Services, le site Web est hébergé dans trois centres de données : Chicago, dans l'Illinois, Dallas, dans le Texas et Seattle, dans l'État de Washington.

Le serveur Web de Seattle possède la meilleure configuration matérielle et peut gérer deux fois plus de charge que les deux autres sites. Contoso Gift Services souhaite que le trafic d'application soit dirigé de la manière suivante.

- Étant donné que le serveur Web de Seattle inclut plus de ressources, la moitié des clients de l'application sont dirigés vers ce serveur
- Un quart des clients de l'application sont dirigés vers le centre de données de Dallas, dans le Texas

- Un quart des clients de l'application sont dirigés vers le centre de données de Chicago, dans l'Illinois

L'illustration suivante représente ce scénario.



Fonctionnement de l'équilibrage de charge des applications

Une fois que vous avez configuré le serveur DNS avec la stratégie DNS pour l'équilibrage de charge des applications à l'aide de cet exemple de scénario, le serveur DNS répond 50 % du temps avec l'adresse du serveur Web de Seattle, 25 % du temps avec l'adresse du serveur Web de Dallas et 25 % du temps avec l'adresse du serveur Web de Chicago.

Ainsi, pour quatre requêtes reçues par le serveur DNS, celui-ci répond avec deux réponses pour Seattle, une pour Dallas et une pour Chicago.

L'un des problèmes possibles liés à l'équilibrage de charge avec la stratégie DNS est la mise en cache des enregistrements DNS par le client DNS et le programme de résolution / LDNS, ce qui peut interférer avec l'équilibrage de charge, car le client ou le programme de résolution n'envoie pas de requête au serveur DNS.

Vous pouvez atténuer l'effet de ce comportement en utilisant une valeur de durée de vie (TTL) faible pour les enregistrements DNS qui doivent être équilibrés en charge.

Comment configurer l'équilibrage de charge des applications

Les sections suivantes vous montrent comment configurer une stratégie DNS pour l'équilibrage de charge des applications.

Créer les étendues de zone

Vous devez d'abord créer les étendues de la zone contosogiftservices.com pour les centres de données où elles sont hébergées.

Une étendue de zone est une instance unique de la zone. Une zone DNS peut avoir plusieurs étendues de zone, chacune d'elles contenant son propre jeu d'enregistrements DNS. Le même enregistrement peut être présent dans plusieurs étendues, avec des adresses IP différentes ou les mêmes adresses IP.

> ⓘ **Notes**
>
> Par défaut, une étendue de zone existe sur les zones DNS. Cette étendue de zone porte le même nom que la zone, et les opérations DNS héritées fonctionnent sur cette étendue.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer des étendues de zone.

PowerShell

```
Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name
"SeattleZoneScope"
Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name "DallasZoneScope"
Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name
"ChicagoZoneScope"
```

Pour plus d'informations, consultez Add-DnsServerZoneScope

Ajouter des enregistrements aux étendues de zone

Vous devez maintenant ajouter les enregistrements représentant l'hôte du serveur web dans les deux étendues de zone.

Dans **SeattleZoneScope**, vous pouvez ajouter l'enregistrement `www.contosogiftservices.com` avec l'adresse IP 192.0.0.1, qui se trouve dans le centre de données de Seattle.

Dans **ChicagoZoneScope**, vous pouvez ajouter le même enregistrement (www.contosogiftservices.com) avec l'adresse IP 182.0.0.1 dans le centre de données de Chicago.

De même, dans **DallasZoneScope**, vous pouvez ajouter un enregistrement (www.contosogiftservices.com) avec l'adresse IP 162.0.0.1 dans le centre de données de Chicago.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour ajouter des enregistrements aux étendues de zone.

PowerShell

```
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name "www" -
IPv4Address "192.0.0.1" -ZoneScope "SeattleZoneScope"
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name "www" -
IPv4Address "182.0.0.1" -ZoneScope "ChicagoZoneScope"
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name "www" -
IPv4Address "162.0.0.1" -ZoneScope "DallasZoneScope"
```

Pour plus d'informations, consultez Add-DnsServerResourceRecord.

Créer les stratégies DNS

Une fois que vous avez créé les partitions (étendues de zone) et ajouté des enregistrements, vous devez créer des stratégies DNS qui distribuent les requêtes entrantes dans ces étendues afin que 50 % des requêtes pour contosogiftservices.com soient traitées avec l'adresse IP du serveur Web du centre de données de Seattle et que le reste soit réparti de manière égale entre les centres de données de Chicago et de Dallas.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer une stratégie DNS qui équilibre le trafic des applications entre ces trois centres de données.

> **Notes**
>
> Dans l'exemple de commande ci-dessous, l'expression –ZoneScope "SeattleZoneScope,2; ChicagoZoneScope,1; DallasZoneScope,1" configure le serveur DNS avec un tableau qui inclut la combinaison de paramètres `<ZoneScope>`, `<weight>`.

PowerShell

```
Add-DnsServerQueryResolutionPolicy -Name "AmericaPolicy" -Action ALLOW -ZoneScope
"SeattleZoneScope,2;ChicagoZoneScope,1;DallasZoneScope,1" -ZoneName
"contosogiftservices.com"
```

Pour plus d'informations, consultez Add-DnsServerQueryResolutionPolicy.

Vous avez maintenant créé une stratégie DNS qui permet l'équilibrage de charge des applications sur les serveurs Web de trois centres de données différents.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Utiliser une stratégie DNS pour l'équilibrage de charge des applications avec connaissance de la géolocalisation

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Vous pouvez vous servir de cette rubrique pour découvrir comment configurer une stratégie DNS pour équilibrer la charge d'une application avec la reconnaissance de l'emplacement géographique.

La rubrique précédente de ce guide, Utiliser une stratégie DNS pour l'équilibrage de charge des applications, utilise un exemple de société fictive, Contoso Gift Services, qui fournit des services de cadeaux en ligne et qui a un site Web nommé contosogiftservices.com. Contoso Gift Services équilibre la charge de son application web en ligne entre les serveurs des centres de données nord-américains situés à Seattle, WA, Chicago et Dallas.

> ⓘ **Notes**
>
> Il est recommandé de vous familiariser avec la rubrique **Utiliser la stratégie DNS pour l'équilibrage de charge des applications** avant d'exécuter les instructions de ce scénario.

Cette rubrique utilise la même entreprise fictive et l'infrastructure réseau comme base pour un nouvel exemple de déploiement qui inclut la reconnaissance de la géolocalisation.

Dans cet exemple, Contoso Gift Services étend avec succès sa présence dans le monde entier.

À l'instar de Amérique du Nord, l'entreprise dispose désormais de serveurs web hébergés dans des centres de données européens.

Les administrateurs DNS de Contoso Gift Services souhaitent configurer l'équilibrage de charge des applications pour les centres de données européens, comme la stratégie DNS a pu être mise en œuvre aux États-Unis, avec le trafic d'application distribué entre les serveurs Web situés à Dublin en Irlande, à Amsterdam aux Pays-Bas et ailleurs.

Les administrateurs DNS souhaitent également que toutes les requêtes provenant d'autres emplacements dans le monde soient distribuées de façon égale entre tous leurs centres de données.

Dans les sections suivantes, vous allez découvrir comment atteindre des objectifs similaires à ceux des administrateurs DNS de Contoso sur votre propre réseau.

Comment configurer l'équilibrage de charge des applications avec la reconnaissance géographique

Les sections suivantes vous montrent comment configurer une stratégie DNS pour l'équilibrage de charge des applications avec la reconnaissance géographique.

> **Important**
>
> Les sections suivantes incluent des exemples de commandes Windows PowerShell qui contiennent des exemples de valeurs pour de nombreux paramètres. Veillez à remplacer les exemples de valeurs dans ces commandes par des valeurs appropriées à votre déploiement avant d'exécuter ces commandes.

Créer les sous-réseaux clients DNS

Vous devez d'abord identifier les sous-réseaux ou l'espace d'adressage IP des régions Amérique du Nord et Europe.

Vous pouvez obtenir ces informations à partir de cartes géo-IP. En fonction de ces distributions géo-IP, vous devez créer les sous-réseaux clients DNS.

Un sous-réseau du client est un regroupement logique de sous-réseaux IPv4 ou IPv6 à partir desquels les requêtes sont envoyées à un serveur DNS.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer des sous-réseaux clients DNS.

PowerShell

```
Add-DnsServerClientSubnet -Name "AmericaSubnet" -IPv4Subnet
192.0.0.0/24,182.0.0.0/24
Add-DnsServerClientSubnet -Name "EuropeSubnet" -IPv4Subnet
141.1.0.0/24,151.1.0.0/24
```

Pour plus d'informations, consultez Add-DnsServerClientSubnet.

Créer les étendues de zone

Une fois les sous-réseaux clients en place, vous devez partitionner la zone contosogiftservices.com en différentes étendues de zone, chacune pour un centre de données.

Une étendue de zone est une instance unique de la zone. Une zone DNS peut avoir plusieurs étendues de zone, chacune d'elles contenant son propre jeu d'enregistrements DNS. Le même enregistrement peut être présent dans plusieurs étendues, avec des adresses IP différentes ou les mêmes adresses IP.

> ⓘ **Notes**
>
> Par défaut, une étendue de zone existe sur les zones DNS. Cette étendue de zone porte le même nom que la zone, et les opérations DNS héritées fonctionnent sur cette étendue.

Le scénario précédent sur l'équilibrage de charge des applications montre comment configurer trois étendues de zone pour les centres de données en Amérique du Nord.

Avec les commandes ci-dessous, vous pouvez créer deux étendues de zone supplémentaires, une chacune pour les centres de données de Dublin et Amsterdam.

Vous pouvez ajouter ces étendues de zone sans aucune modification aux trois étendues de zone Amérique du Nord existantes dans la même zone. En outre, après avoir créé ces étendues de zone, vous n'avez pas besoin de redémarrer votre serveur DNS.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour créer des étendues de zone.

PowerShell

```
Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name "DublinZoneScope"
Add-DnsServerZoneScope -ZoneName "contosogiftservices.com" -Name
"AmsterdamZoneScope"
```

Pour plus d'informations, consultez Add-DnsServerZoneScope

Ajouter des enregistrements aux étendues de zone

Vous devez maintenant ajouter les enregistrements représentant l'hôte du serveur web dans les deux étendues de zone.

Les enregistrements des centres de données américains ont été ajoutés dans le scénario précédent. Vous pouvez utiliser les commandes Windows PowerShell suivantes pour ajouter des enregistrements aux étendues de zone pour les centres de données européens.

PowerShell

```
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name "www" -
IPv4Address "151.1.0.1" -ZoneScope "DublinZoneScope”
Add-DnsServerResourceRecord -ZoneName "contosogiftservices.com" -A -Name "www" -
IPv4Address "141.1.0.1" -ZoneScope "AmsterdamZoneScope"
```

Pour plus d’informations, consultez Add-DnsServerResourceRecord.

Créer les stratégies DNS

Après avoir créé les partitions (étendues de zone) et ajouté des enregistrements, vous devez créer des stratégies DNS qui distribuent les requêtes entrantes entre ces étendues.

Pour cet exemple, la distribution des requêtes entre les serveurs d’applications dans différents centres de données répond aux critères suivants.

1. Lorsque la requête DNS est reçue d’une source dans un sous-réseau client nord-américain, 50 % des réponses DNS pointent vers le centre de données de Seattle, 25 % des réponses pointent vers le centre de données de Chicago et les 25 % restants pointent vers le centre de données de Dallas.
2. Lorsque la requête DNS est reçue à partir d’une source dans un sous-réseau client européen, 50 % des réponses DNS pointent vers le centre de données de Dublin et 50 % des réponses DNS pointent vers le centre de données d’Amsterdam.
3. Lorsque la requête provient de n’importe où dans le monde, les réponses DNS sont réparties entre les cinq centres de données.

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour implémenter ces stratégies DNS.

PowerShell

```
Add-DnsServerQueryResolutionPolicy -Name "AmericaLBPolicy" -Action ALLOW -
ClientSubnet "eq,AmericaSubnet" -ZoneScope "SeattleZoneScope,2;ChicagoZoneScope,1;
TexasZoneScope,1" -ZoneName "contosogiftservices.com" –ProcessingOrder 1
Add-DnsServerQueryResolutionPolicy -Name "EuropeLBPolicy" -Action ALLOW -
ClientSubnet "eq,EuropeSubnet" -ZoneScope "DublinZoneScope,1;AmsterdamZoneScope,1"
-ZoneName "contosogiftservices.com" -ProcessingOrder 2
Add-DnsServerQueryResolutionPolicy -Name "WorldWidePolicy" -Action ALLOW -FQDN
"eq,*.contoso.com" -ZoneScope "SeattleZoneScope,1;ChicagoZoneScope,1;
TexasZoneScope,1;DublinZoneScope,1;AmsterdamZoneScope,1" -ZoneName
"contosogiftservices.com" -ProcessingOrder 3
```

Pour plus d’informations, consultez Add-DnsServerQueryResolutionPolicy.

Vous avez maintenant créé une stratégie DNS qui assure l’équilibrage de charge des applications entre les serveurs Web situés dans cinq centres de données différents sur plusieurs continents.

Vous pouvez créer des milliers de stratégies DNS en fonction de vos exigences de gestion du trafic, et toutes les nouvelles stratégies sont appliquées dynamiquement, sans redémarrer le serveur DNS, sur les requêtes entrantes.

Résolution des problèmes liés à DNS (Domain Name System)

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Essayez notre agent virtuel : il peut vous aider à identifier et à résoudre rapidement les problèmes courants liés au protocole DNS (Server Message Block).

Les problèmes de résolution de nom de domaine peuvent être divisés en deux catégories : les problèmes côté client et les problèmes côté serveur. Il est généralement conseillé de commencer par les problèmes côté client, sauf si vous déterminez au cours de la phase de délimitation que le problème se produit définitivement côté serveur.

- Résolution des problèmes liés aux clients DNS
- Résolution des problèmes liés aux serveurs DNS

Collecte de données

Nous vous recommandons de collecter simultanément les données côté client et côté serveur quand le problème se produit. Toutefois, en fonction du problème réel, vous pouvez démarrer votre collecte à partir d'un jeu de données unique sur le client DNS ou le serveur DNS.

Pour collecter un diagnostic réseau Windows à partir d'un client affecté et de son serveur DNS configuré, effectuez les étapes suivantes :

1. Démarrez les captures réseau sur le client et le serveur :

   Invite de commandes Windows

   ```
   netsh trace start capture=yes tracefile=c:\%computername%_nettrace.etl
   ```

2. Exécutez la commande suivante pour effacer le cache DNS sur le client DNS :

   Invite de commandes Windows

   ```
   ipconfig /flushdns
   ```

3. Reproduisez le problème.

4. Arrêtez et enregistrez les traces :

Invite de commandes Windows

```
netsh trace stop
```

5. Enregistrez les fichiers Nettrace.cab de chaque ordinateur. Ces informations vous seront utiles quand vous contacterez le support Microsoft.

Résolution des problèmes liés aux clients DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Cet article explique comment résoudre les problèmes des clients DNS.

Vérifier la configuration IP

1. Ouvrez une fenêtre d'invite de commandes en tant qu'administrateur sur l'ordinateur client.
2. Exécutez la commande suivante:

   Invite de commandes Windows

   ```
   ipconfig /all
   ```

3. Vérifiez que le client a une adresse IP valide, un masque de sous-réseau et une passerelle par défaut pour le réseau auquel il est attaché et utilisé.
4. Vérifiez les serveurs DNS répertoriés dans la sortie et vérifiez que les adresses IP répertoriées sont correctes.
5. Vérifiez le suffixe DNS spécifique à la connexion dans la sortie et vérifiez qu'il est correct.

Si le client n'a pas de configuration TCP/IP valide, utilisez l'une des méthodes suivantes :

- Pour les clients configurés dynamiquement, utilisez la `ipconfig /renew` commande pour forcer manuellement le client à renouveler sa configuration d'adresse IP avec le serveur DHCP.
- Pour les clients configurés statiquement, modifiez les propriétés TCP/IP du client pour utiliser des paramètres de configuration valides ou terminez sa configuration DNS pour le réseau.

Vérifier la connexion réseau

Test ping

Vérifiez que le client peut contacter un serveur DNS préféré (ou un autre) en effectuant un test ping sur le serveur DNS préféré par son adresse IP.

Par exemple, si le client utilise un serveur DNS préféré de 10.0.0.1, exécutez cette commande à l'invite de commandes :

Invite de commandes Windows

```
ping 10.0.0.1
```

Si aucun serveur DNS configuré ne répond à un test ping direct de son adresse IP, cela indique que la source du problème est plus susceptible d'être connectée au réseau entre le client et les serveurs DNS. Si c'est le cas, suivez les étapes de résolution des problèmes de réseau TCP/IP de base pour résoudre le problème. N'oubliez pas que le trafic ICMP doit être autorisé via le pare-feu pour que la commande ping fonctionne.

Tests de requête DNS

Si le client DNS peut effectuer un test ping sur l'ordinateur serveur DNS, essayez d'utiliser les commandes suivantes `nslookup` pour tester si le serveur peut répondre aux clients DNS. Étant donné que nslookup n'utilise pas le cache DNS du client, la résolution de noms utilise le serveur DNS configuré du client.

Tester un client

Invite de commandes Windows

```
nslookup <client>
```

Par exemple, si l'ordinateur client est nommé **client1**, exécutez cette commande :

Invite de commandes Windows

```
nslookup client1
```

Si une réponse réussie n'est pas retournée, essayez d'exécuter la commande suivante :

Invite de commandes Windows

```
nslookup <fqdn of client>
```

Par exemple, si le nom de domaine complet est **client1.corp.contoso.com**, exécutez cette commande :

Invite de commandes Windows

```
nslookup client1.corp.contoso.com.
```

> **Notes**
>
> Vous devez inclure le point de fin quand vous exécutez ce test.

Si Windows trouve correctement le nom de domaine complet, mais ne trouve pas le nom court, vérifiez la configuration du suffixe DNS sous l'onglet DNS des paramètres TCP/IP avancés de la carte réseau. Pour plus d'informations, consultez Configuration de la résolution DNS.

Tester le serveur DNS

Invite de commandes Windows

```
nslookup <DNS Server>
```

Par exemple, si le serveur DNS est nommé DC1, exécutez cette commande :

Invite de commandes Windows

```
nslookup dc1
```

Si les tests précédents ont réussi, ce test doit également réussir. Si ce test n'a pas réussi, vérifiez la connectivité au serveur DNS.

Tester l'enregistrement défaillant

Invite de commandes Windows

```
nslookup <failed internal record>
```

Par exemple, si l'enregistrement défaillant a été **app1.corp.contoso.com**, exécutez cette commande :

Invite de commandes Windows

```
nslookup app1.corp.contoso.com
```

Tester une adresse Internet publique

Invite de commandes Windows

```
nslookup <external name>
```

Par exemple:

Invite de commandes Windows

```
nslookup bing.com
```

Si ces quatre tests ont réussi, exécutez `ipconfig /displaydns` puis vérifiez la sortie pour le nom qui a échoué. Si vous voyez « Nom n'existe pas » sous le nom défaillant, une réponse négative a été retournée à partir d'un serveur DNS et a été mise en cache sur le client.

Pour résoudre le problème, effacez le cache en exécutant `ipconfig /flushdns`.

Étape suivante

Si la résolution de noms échoue toujours, accédez à la section Résolution des problèmes des serveurs DNS .

Résolution des problèmes liés aux serveurs DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Essayez notre agent virtuel : il peut vous aider à identifier et à résoudre rapidement les problèmes courants liés au protocole DNS (Server Message Block).

Cet article explique comment résoudre les problèmes sur les serveurs DNS.

Vérifier la configuration IP

1. Exécutez `ipconfig /all` dans une invite de commande et vérifiez l'adresse IP, le masque de sous-réseau et la passerelle par défaut.

2. Vérifiez si le serveur DNS fait autorité pour le nom recherché. Si c'est le cas, consultez Vérification des problèmes liés aux données faisant autorité.

3. Exécutez la commande suivante:

   Invite de commandes Windows

   ```
   nslookup <name> <IP address of the DNS server>
   ```

   Par exemple:

   Invite de commandes Windows

   ```
   nslookup app1 10.0.0.1
   ```

   Si vous recevez une réponse d'échec ou de délai d'attente, consultez Vérification des problèmes de récursivité.

4. Videz le cache du programme de résolution. Pour ce faire, exécutez la commande suivante dans une fenêtre d'invite de commandes d'administration :

   Invite de commandes Windows

   ```
   dnscmd /clearcache
   ```

Ou, dans une fenêtre PowerShell d'administration, exécutez l'applet de commande suivante :

PowerShell

```
Clear-DnsServerCache
```

> **Notes**
>
> Si le serveur fonctionne en tant que client DNS (par exemple, quand il doit résoudre les noms de ses propres opérations), utilisez cette option `Clear-DnsClientCache` pour effacer le cache du client DNS local. Si vous résolvez des problèmes liés au rôle du serveur en tant que serveur DNS (qui sert des enregistrements DNS à d'autres clients), utilisez cette option `Clear-DnsServerCache` pour effacer le cache faisant autorité du serveur et l'empêcher de fournir des informations DNS obsolètes.

5. Répétez l'étape 3.

Vérifier les problèmes de serveur DNS

Journal des événements

Vérifiez les journaux suivants pour déterminer s'il existe des erreurs enregistrées :

- Application
- System
- Serveur DNS

Tester à l'aide de la requête nslookup

Exécutez la commande suivante et vérifiez si le serveur DNS est accessible à partir des ordinateurs clients.

Invite de commandes Windows

```
nslookup <client name> <server IP address>
```

- Si le programme de résolution retourne l'adresse IP du client, le serveur n'a aucun problème.

- Si le programme de résolution retourne une réponse « Échec du serveur » ou « Requête refusée », la zone est probablement mise en pause ou le serveur est éventuellement surchargé. Vous pouvez savoir s'il est mis en pause en vérifiant l'onglet Général des propriétés de zone dans la console DNS.

Si le programme de résolution retourne la réponse « Requête au serveur expirée » ou « Pas de réponse du serveur », le service DNS ne fonctionne probablement pas. Essayez de redémarrer le service serveur DNS en entrant ce qui suit à l'invite de commandes sur le serveur :

Invite de commandes Windows

```
net start DNS
```

Si le problème se produit lorsque le service est en cours d'exécution, il se peut que le serveur n'écoute pas l'adresse IP que vous avez utilisée dans votre requête nslookup. Sous l'onglet **Interfaces** de la page propriétés du serveur dans la console DNS, les administrateurs peuvent restreindre l'écoute d'un serveur DNS uniquement sur les adresses sélectionnées. Si le serveur DNS a été configuré pour limiter le service à une liste spécifique de ses adresses IP configurées, il est possible que l'adresse IP utilisée pour contacter le serveur DNS ne figure pas dans la liste. Vous pouvez essayer une autre adresse IP dans la liste ou ajouter l'adresse IP à la liste.

Dans de rares cas, le serveur DNS peut avoir une configuration avancée de sécurité ou de pare-feu. Si le serveur se trouve sur un autre réseau accessible uniquement via un hôte intermédiaire (tel qu'un routeur de filtrage de paquets ou un serveur proxy), le serveur DNS peut utiliser un port non standard pour écouter et recevoir des demandes clientes. Par défaut, nslookup envoie des requêtes aux serveurs DNS sur le port UDP 53. Par conséquent, si le serveur DNS utilise un autre port, les requêtes nslookup échouent. Si vous pensez que cela peut être le problème, vérifiez si un filtre intermédiaire est intentionnellement utilisé pour bloquer le trafic sur les ports DNS connus. Si ce n'est pas le cas, essayez de modifier les filtres de paquets ou les règles de port sur le pare-feu pour autoriser le trafic sur le port UDP/TCP 53.

Vérification des problèmes liés aux données faisant autorité

Vérifiez si le serveur qui retourne la réponse incorrecte est un serveur principal pour la zone (le serveur principal standard pour la zone ou un serveur qui utilise l'intégration Active Directory pour charger la zone) ou un serveur qui héberge une copie secondaire de la zone.

Si le serveur est un serveur principal

Le problème peut être dû à une erreur utilisateur lorsque les utilisateurs entrent des données dans la zone. Ou bien, cela peut être dû à un problème qui affecte la réplication Active Directory ou la mise à jour dynamique.

Si le serveur héberge une copie secondaire de la zone

1. Examinez la zone sur le serveur principal (le serveur à partir duquel ce serveur récupère les transferts de zone).

   > ⓘ **Notes**
   >
   > Vous pouvez déterminer quel serveur est le serveur principal en examinant les propriétés de la zone secondaire dans la console DNS.

   Si le nom n'est pas correct sur le serveur principal, passez à l'étape 4.

2. Si le nom est correct sur le serveur principal, vérifiez si le numéro de série sur le serveur principal est inférieur ou égal au numéro de série sur le serveur secondaire. Si tel est le cas, modifiez le serveur principal ou le serveur secondaire afin que le numéro de série sur le serveur principal soit supérieur au numéro de série sur le serveur secondaire.

3. Sur le serveur secondaire, forcez un transfert de zone à partir de la console DNS ou en exécutant la commande suivante :

   Invite de commandes Windows

   ```
   dnscmd /zonerefresh <zone name>
   ```

   Par exemple, si la zone est corp.contoso.com, entrez : `dnscmd /zonerefresh corp.contoso.com`.

4. Examinez à nouveau le serveur secondaire pour voir si la zone a été transférée correctement. Si ce n'est pas le cas, vous avez probablement un problème de transfert de zone. Pour plus d'informations, consultez Problèmes de transfert de zone.

5. Si la zone a été transférée correctement, vérifiez si les données sont maintenant correctes. Si ce n'est pas le cas, les données sont incorrectes dans la zone primaire. Le problème peut être dû à une erreur utilisateur lorsque les utilisateurs entrent des données dans la zone. Ou bien, cela peut être dû à un problème qui affecte la réplication Active Directory ou la mise à jour dynamique.

Vérification des problèmes de récursivité

Pour que la récursivité fonctionne correctement, tous les serveurs DNS utilisés dans le chemin d'une requête récursive doivent être en mesure de répondre et de transférer des données correctes. Si ce n'est pas le cas, une requête récursive peut échouer pour l'une des raisons suivantes :

- La requête expire avant de pouvoir être terminée.
- Un serveur utilisé pendant la requête ne répond pas.
- Un serveur utilisé pendant la requête fournit des données incorrectes.

Démarrez la résolution des problèmes sur le serveur utilisé dans votre requête d'origine. Vérifiez si ce serveur transfère des requêtes vers un autre serveur en examinant l'onglet **Redirecteurs** dans les propriétés du serveur dans la console DNS. Si la case **Activer les redirecteurs** est cochée et qu'un ou plusieurs serveurs sont répertoriés, ce serveur transfère les requêtes.

Si ce serveur transfère des requêtes à un autre serveur, vérifiez les problèmes qui affectent le serveur auquel ce serveur transfère les requêtes. Pour rechercher des problèmes, consultez Vérifier les problèmes de serveur DNS. Lorsque cette section vous indique d'effectuer une tâche sur le client, effectuez-la sur le serveur à la place.

Si le serveur est sain et peut transférer des requêtes, répétez cette étape et examinez le serveur vers lequel ce serveur transfère les requêtes.

Si ce serveur ne transfère pas les requêtes à un autre serveur, vérifiez si ce serveur peut interroger un serveur racine. Pour ce faire, exécutez la commande suivante :

Invite de commandes Windows

```
nslookup
server <IP address of server being examined>
set q=NS
```

- Si le programme de résolution retourne l'adresse IP d'un serveur racine, vous avez probablement une délégation rompue entre le serveur racine et le nom ou l'adresse IP que vous essayez de résoudre. Suivez la procédure Test d'une délégation défaillante pour identifier l'emplacement d'une délégation défaillante.
- Si le programme de résolution retourne une réponse « La requête au serveur a expiré », vérifiez si les indications racines pointent vers des serveurs racines fonctionnels. Pour ce faire, suivez la procédure Pour afficher les indications de racine actuelles. Si les indicateurs

racines pointent vers le fonctionnement des serveurs racines, vous pouvez rencontrer un problème réseau ou le serveur peut utiliser une configuration de pare-feu avancée qui empêche le programme de résolution d'interroger le serveur, comme décrit dans la section Vérifier les problèmes du serveur DNS . Il est également possible que la valeur par défaut du délai d'attente récursive soit trop courte.

Tester une délégation rompue

Commencez les tests de la procédure suivante en interrogeant un serveur racine valide. Le test vous guide à travers un processus complet d'interrogation de tous les serveurs DNS, depuis la racine principale jusqu'au serveur que vous testez pour une délégation défaillante.

1. À l'invite de commandes sur le serveur que vous testez, entrez les éléments suivants :

   Invite de commandes Windows

   ```
   nslookup
   server <server IP address>
   set norecursion
   set querytype= <resource record type>
   <FQDN>
   ```

   > ⓘ **Notes**
   >
   > Le type d'enregistrement de ressource est celui que vous avez demandé dans votre requête d'origine, et le nom de domaine complet est celui pour lequel vous avez fait la requête (terminé par un point).

2. Si la réponse inclut une liste d'enregistrements de ressources « NS » et « A » pour les serveurs délégués, répétez l'étape 1 pour chaque serveur et utilisez l'adresse IP des enregistrements de ressources « A » comme adresse IP du serveur.

   - Si la réponse ne contient pas d'enregistrement de ressource « NS », une délégation est rompue.
   - Si la réponse contient des enregistrements de ressources « NS », mais aucun enregistrement de ressource « A », entrez **la récursivité définie** et interrogez individuellement les enregistrements de ressources « A » des serveurs répertoriés dans les enregistrements « NS ». Si vous ne trouvez pas au moins une adresse IP valide d'un enregistrement de ressource « A » pour chaque enregistrement de ressource NS dans une zone, vous disposez d'une délégation rompue.

3. Si vous déterminez que vous avez une délégation rompue, corrigez-la en ajoutant ou en mettant à jour un enregistrement de ressource « A » dans la zone parente à l'aide d'une adresse IP valide pour un serveur DNS correct pour la zone déléguée.

Pour afficher les indications de racine actuelles

1. Démarrez la console DNS.
2. Ajoutez ou connectez-vous au serveur DNS qui a échoué à une requête récursive.
3. Cliquez avec le bouton droit sur le serveur, puis sélectionnez **Propriétés**.
4. Cliquez sur Root Hints.

Vérifiez la connectivité de base aux serveurs racines.

- Si les indications racine semblent être configurées correctement, vérifiez que le serveur DNS utilisé en cas d'échec de résolution de noms peut pinguer les serveurs racines par leur adresse IP.
- Si les serveurs racines ne répondent pas au test ping par adresse IP, les adresses IP des serveurs racines peuvent avoir changé. Toutefois, il est rare de voir une reconfiguration des serveurs racines.

Problèmes de transfert de zone

Exécutez les vérifications suivantes :

- Vérifiez l'Observateur d'événements pour le serveur DNS principal et secondaire.
- Vérifiez si le serveur principal refuse d'envoyer le transfert pour la sécurité.
- Vérifiez l'onglet **Transferts** de zone des propriétés de zone dans la console DNS. Si le serveur restreint les transferts de zone à une liste de serveurs, tels que ceux répertoriés sous l'onglet **Serveurs de noms** des propriétés de zone, assurez-vous que le serveur secondaire figure sur cette liste. Vérifiez que le serveur est configuré pour envoyer des transferts de zone.
- Vérifiez que le serveur principal rencontre des problèmes en suivant les étapes décrites dans la section Vérifier les problèmes du serveur DNS . Lorsque vous êtes invité à effectuer une tâche sur le client, effectuez la tâche sur le serveur secondaire à la place.
- Vérifiez si le serveur secondaire exécute une autre implémentation de serveur DNS, telle que BIND. Si c'est le cas, le problème peut avoir l'une des causes suivantes :

- Le serveur principal Windows peut être configuré pour envoyer des transferts de zones rapides, mais le serveur secondaire tiers peut ne pas prendre en charge les transferts de zone rapide. Si c'est le cas, désactivez les transferts de zone rapides sur le serveur principal à partir de la console DNS en cochant la case **Activer la liaison des secondaires** sous l'onglet **Avancé** des propriétés de votre serveur.

- Si une zone de recherche vers l'avant sur le serveur Windows contient un type d'enregistrement (par exemple, un enregistrement SRV) que le serveur secondaire ne prend pas en charge, le serveur secondaire peut rencontrer des problèmes lors de l'extraction de la zone.

Vérifiez si le serveur principal exécute une autre implémentation de serveur DNS, telle que BIND. Dans ce cas, il est possible que la zone sur le serveur principal inclut des enregistrements de ressources incompatibles que Windows ne reconnaît pas.

Si le serveur maître ou le serveur secondaire exécute une autre implémentation de serveur DNS, vérifiez les deux serveurs pour vous assurer qu'ils prennent en charge les mêmes fonctionnalités. Vous pouvez vérifier le serveur Windows dans la console DNS sous l'onglet **Avancé** de la page des propriétés du serveur. En plus de la zone Activer les fichiers secondaires De liaison, cette page inclut la liste déroulante **Vérification de nom** . Cela vous permet de sélectionner l'application de la conformité RFC stricte pour les caractères dans les noms DNS.

Résoudre les problèmes dns sur HTTPS dans le serveur DNS (préversion)

S'applique à: ✅ Windows Server 2025

> ⓘ **Important**
>
> DNS sur HTTPS (DoH) pour le serveur DNS sur Windows Server est actuellement en préversion. Ces informations concernent un produit en version préliminaire qui peut être sensiblement modifié avant sa commercialisation. Microsoft n'offre aucune garantie, exprimée ou implicite, en ce qui concerne les informations fournies ici.

Vos clients ne peuvent-ils pas se connecter à votre serveur DNS à l'aide de DoH ou les requêtes DNS chiffrées échouent-elles sans raison claire ? Cet article vous aide à identifier et résoudre les problèmes DNS courants sur HTTPS (DoH) sur Windows DNS Server. Que vous soyez confronté à des erreurs de liaison de certificat, à des conflits de ports ou à des problèmes de performances, vous trouverez des instructions pas à pas pour que DoH fonctionne correctement.

Commencez par la liste de contrôle de résolution des problèmes pour identifier rapidement votre problème, puis suivez les sections spécifiques aux symptômes pour obtenir des étapes de résolution détaillées. Cet article s'applique à Windows Server 2025 et versions ultérieures avec la fonctionnalité d'évaluation DoH activée.

Prerequisites

Avant de résoudre les problèmes de DoH, assurez-vous de disposer de :

- Windows Server 2025 avec la mise à jour de sécurité 2026-02 ((KB5075899)) ou ultérieure installée.
- Le DNS sur HTTPS dans le service de serveur DNS est activé à l'aide des instructions fournies après avoir demandé l'accès en utilisant DoH sur Windows DNS Server : Inscription à la préversion publique .
- Accès administratif ou équivalent à Windows Server hébergeant le service serveur DNS.

Les certificats DoH doivent répondre aux exigences suivantes :

- **Extension d'utilisation améliorée de la clé** : doit inclure l'identificateur d'objet Authentification du serveur (1.3.6.1.5.5.7.3.1)

- **Nom ou nom alternatif de l'objet** : certificat signé avec un nom alternatif de l'objet (SAN) et le nom de domaine entièrement qualifié ou l'adresse IP qui correspond à votre modèle d'URI DoH configuré.
- **Clé privée** : doit être présente dans le magasin de l'ordinateur local, correctement associée au certificat et ne doit pas avoir une protection forte de clé privée activée
- **Chaîne d'approbation** : doit être émise par une autorité de certification approuvée par les clients DNS

Liste de contrôle pour la résolution des problèmes

Parcourez cette liste de contrôle pour identifier votre problème DoH. Chaque vérification contient des liens vers des étapes de résolution détaillées.

1. Vérifier l'état DoH

✅ DoH est activé : `Get-DnsServerEncryptionProtocol` affiche `EnableDoh : True`

✅ Le service DNS est en cours d'exécution : `Get-Service DNS` affiche `Running`

✅ Le port configuré est à l'écoute : `netstat -an | findstr :<port>` affiche `LISTENING`. Le port par défaut est 443.

Pour résoudre les problèmes de configuration de service, consultez Symptôme : DoH non configuré ou en cours d'exécution.

2. Vérifier l'initialisation DoH

✅ L'ID d'événement 822 apparaît dans le journal des événements du serveur DNS après le redémarrage du service

✅ Aucun événement d'erreur (823, 824, 825, 826) dans le journal des événements

✅ Le certificat est lié à votre port configuré : `netsh http show sslcert`

Pour résoudre les échecs d'initialisation, consultez Symptôme : Échec de l'initialisation du doH.

3. Vérifier la connectivité du client

✅ Les clients peuvent atteindre le serveur DNS sur le port DoH configuré (test à l'aide d'un navigateur), par défaut 443

✅ Le pare-feu autorise le trafic TCP entrant sur le port DoH configuré

✅ Les clients approuvent le certificat de serveur (aucun avertissement de certificat)

Pour résoudre les problèmes de connectivité, consultez Symptôme : Les clients ne peuvent pas se connecter à l'aide de DoH.

4. Vérifier le traitement des requêtes

✅ L'ID d'événement 597 (requêtes reçues) apparaît dans le journal analytique.

✅ L'ID d'événement 598 (réponses envoyées) apparaît dans le journal analytique

✅ Aucun ID d'événement 599 (échecs de réponse) ou ID d'événement 600 (requêtes rejetées)

Pour résoudre les problèmes de traitement des requêtes, consultez Symptôme : Les requêtes DoH échouent ou expirent.

> 💡 **Conseil**
>
> Si l'ID d'événement 597 n'apparaît pas, résolvez d'abord la connectivité du client. Voir **symptôme : Les clients ne peuvent pas se connecter à l'aide de DoH**.

5. Vérifier les performances

✅ Compteur de requêtes DoH abandonnées par seconde = 0

✅ Réponses DoH envoyées/s ≈ demandes DoH reçues/s

✅ La latence des requêtes est acceptable

Pour résoudre les problèmes de performances, consultez Symptôme : Problèmes de performances DoH.

Symptôme : DoH non configuré ou en cours d'exécution

Vous tentez d'utiliser DoH, mais les clients continuent à utiliser un DNS non chiffré, ou vous ne pouvez pas vérifier que DoH est activé sur le serveur.

Causes courantes :

- DoH non activé sur le serveur

- Service DNS arrêté
- Erreur de configuration dans les paramètres DoH

Comment diagnostiquer :

Pour vérifier la configuration doH, exécutez la commande suivante :

PowerShell

```
Get-DnsServerEncryptionProtocol
```

Si DoH est correctement configuré, vous devez voir :

Output

```
EnableDoh   : True
UriTemplate : https://dns.contoso.com:443/dns-query
```

Pour vérifier l'état du service DNS, exécutez la commande suivante :

PowerShell

```
Get-Service DNS
```

La sortie doit afficher `Status: Running`.

Pour vérifier que votre port configuré écoute, exécutez la commande suivante. Remplacez `443` par votre port configuré si différent :

Invite de commandes Windows

```
netstat -an | findstr :443
```

Vous devriez voir les entrées TCP dans l'état `LISTENING`.

Pour obtenir des procédures de surveillance détaillées, consultez Surveiller DNS sur HTTPS.

Résolution du problème :

Si `EnableDoh` `False` est le cas, afin d'activer DoH, exécutez la commande suivante :

PowerShell

```
Set-DnsServerEncryptionProtocol -EnableDoh $true -UriTemplate
"https://dns.contoso.com:443/dns-query"
```

Remplacez `dns.contoso.com` par le nom de domaine complet de votre serveur DNS qui correspond à votre san de certificat.

Pour redémarrer le service serveur DNS, exécutez la commande suivante :

PowerShell

```
Restart-Service -Name DNS
```

Si DoH n'a pas été précédemment configuré, consultez Activer DNS sur HTTPS sur Windows DNS Server pour obtenir des instructions d'installation complètes, notamment les exigences de certificat.

Symptôme : Échec de l'initialisation du doH

Vous activez DoH, mais le service ne s'initialise pas correctement. Les clients ne peuvent pas se connecter à l'aide de DoH.

Causes courantes :

- Problèmes de liaison de certificat (ID d'événement 823).
- Conflits de ports (ID d'événement 825, 826).
- Configuration du modèle d'URI non valide.

Comment diagnostiquer :

Consultez l'Observateur d'événements Windows pour les événements DNS Server. Accédez au**serveur DNS**>.

Pour plus d'informations sur les événements, consultez Surveiller DNS sur HTTPS - Événements de serveur.

Recherchez ces événements spécifiques :

- **ID d'événement 823 (DNS_EVENT_HTTP_SERVER_INIT_FAILED)** : échec de l'initialisation du serveur HTTP, généralement en raison de problèmes de liaison de certificat ou de conflits de port.
- **ID d'événement 824 (DNS_EVENT_HTTP_SERVER_SESSION_FAILED)** : échec de la création de session de serveur HTTP, généralement en raison de contraintes de ressources.

- **ID d'événement 825 (DNS_EVENT_HTTP_CREATE_URL_FAILED)** : échec de l'inscription d'URL en raison d'un format d'URI ou d'un port non valide.

Recherchez l'ID d'événement 822 (DNS_EVENT_HTTP_URL_REGISTERED), qui indique une initialisation réussie. Si cet événement est manquant après le redémarrage du service, l'initialisation a échoué.

Résolution du problème :

Problèmes de liaison des certificats

Si vous voyez l'ID d'événement 823, exécutez la commande suivante pour vérifier la liaison de certificat :

Invite de commandes Windows

```
netsh http show sslcert
```

Recherchez une entrée qui correspond à votre adresse IP et à votre port (par exemple, `0.0.0.0:443`). Vérifiez qu'elle affiche l'empreinte numérique du certificat de votre serveur DNS.

Si le certificat n'est pas lié ou affiche une empreinte incorrecte, consultez Lier le certificat pour connaître les étapes de liaison du certificat approprié.

Vérifiez que le certificat répond à ces exigences :

- Certificat SSL/TLS valide dans le `LocalMachine\My store`
- Le Nom alternatif du sujet (SAN) correspond au FQDN dans votre URI DoH.
- La clé privée est installée
- Non expiré

Pour obtenir une configuration détaillée du certificat, consultez Activer DNS sur HTTPS sur Windows DNS Server.

Conflits de ports

Si vous voyez l'ID d'événement 825 ou 826, un autre service peut utiliser le port 443. Pour vérifier ce qui utilise le port, exécutez la commande suivante :

Invite de commandes Windows

```
netstat -ano | findstr :443
```

Si un autre processus utilise le port 443, effectuez les opérations suivantes :

- Arrêter le service en conflit ou
- Pour configurer DoH pour utiliser un autre port, exécutez la commande suivante :

PowerShell

```
Set-DnsServerEncryptionProtocol -EnableDoh $true -UriTemplate
"https://dns.contoso.com:8443/dns-query"
```

Ensuite, liez votre certificat au nouveau port et mettez à jour les règles de pare-feu en conséquence.

Erreurs de configuration

Vérifiez que votre modèle d'URI est correctement mis en forme :

- Commence par `https://`
- Inclut le FQDN qui correspond à votre SAN du certificat
- Inclut le chemin d'accès `/dns-query`
- Exemple : `https://dns.contoso.com:443/dns-query`

Pour vérifier la configuration actuelle du modèle d'URI, exécutez la commande suivante :

PowerShell

```
Get-DnsServerEncryptionProtocol | Select-Object UriTemplate
```

Si le modèle d'URI est incorrect ou manquant, exécutez la commande suivante pour la reconfigurer :

PowerShell

```
Set-DnsServerEncryptionProtocol -EnableDoh $true -UriTemplate
"https://dns.contoso.com:443/dns-query"
```

Remplacez `dns.contoso.com` par le nom de domaine complet de votre serveur DNS. Vérifiez que le nom de domaine complet correspond exactement au nom d'alternative de l'objet (SAN) dans votre certificat.

Après avoir résolu les problèmes, exécutez la commande suivante pour redémarrer le service DNS. Recherchez l'ID d'événement 822 pour confirmer l'initialisation réussie.

PowerShell

```
Restart-Service -Name DNS
```

Symptôme : Les clients ne peuvent pas se connecter à l'aide de DoH

Vous configurez et démarrez DoH sur le serveur, mais les clients ne peuvent pas se connecter ou obtenir des erreurs de certificat.

Causes courantes :

- Réseau ou pare-feu bloquant le port DoH configuré, qui est 443 par défaut.
- Problèmes d'approbation de certificat.
- Client utilisant un URI ou une configuration incorrects.

Comment diagnostiquer :

Testez la connectivité à partir d'une machine cliente en ouvrant un navigateur web et en accédant à votre URI DoH (par exemple). `https://dns.contoso.com/dns-query` Vous devez voir l'un des résultats suivants :

- Une page vierge ou une réponse minimale indique que le serveur écoute et que la connectivité réseau fonctionne.
- Une erreur de certificat indique des problèmes d'approbation de certificat, mais confirme que la connectivité réseau et les règles de pare-feu sont correctes.
- Un délai d'expiration de connexion indique des problèmes de réseau ou de pare-feu qui empêchent l'accès au serveur DNS à l'aide de DoH.

Pour vérifier les règles de pare-feu sur le serveur DNS, exécutez la commande suivante :

PowerShell

```
Get-NetFirewallRule | Where-Object {$_.DisplayName -like "*DNS*" -or $_.DisplayName
-like "*443*"} | Format-Table DisplayName, Enabled, Direction, Action
```

Vérifiez l'approbation du certificat client en examinant les détails du certificat dans le navigateur. Vérifiez si la chaîne de certificats est valide et approuvée.

Résolution du problème :

Connectivité réseau

Tout d'abord, vérifiez la connectivité réseau du client au serveur DNS via HTTPS. Exécutez la commande suivante, en remplaçant le port si vous avez configuré un port non défini :

PowerShell

```
Test-NetConnection -ComputerName dns.contoso.com -Port 443
```

Si `TcpTestSucceeded` retourne `False`, vérifiez le routage réseau et les règles de pare-feu entre le client et le serveur.

Pour créer une règle de pare-feu Windows sur le serveur pour autoriser les connexions entrantes, exécutez la commande suivante. Remplacez `443` par votre port configuré si différent :

PowerShell

```
New-NetFirewallRule -DisplayName "DNS over HTTPS" -Direction Inbound -Protocol TCP -
LocalPort 443 -Action Allow
```

Si vous utilisez un pare-feu matériel ou un groupe de sécurité réseau, vérifiez qu'il autorise le trafic TCP entrant sur votre port DoH configuré sur le serveur DNS.

Confiance des certificats

Si vous utilisez une autorité de certification privée (CA) :

1. Assurez-vous que vos clients DNS approuvent cette autorité de certification.
2. Installez le certificat racine sur les ordinateurs clients.
3. Vérifiez que la chaîne de certificats est terminée sur le serveur.

Vous pouvez également utiliser un certificat signé par une autorité de certification approuvée publiquement que les clients approuvent déjà.

Pour tester la connectivité réseau au port DoH du serveur DNS à partir d'un client, exécutez la commande suivante. Remplacez `443` par votre port configuré si différent :

PowerShell

```
Test-NetConnection -ComputerName dns.contoso.com -Port 443
```

Pour vérifier que le certificat est approuvé par le client, ouvrez un navigateur web et accédez à `https://dns.contoso.com/dns-query`. Si le navigateur affiche un avertissement de certificat, le client n'approuve pas la chaîne de certificats.

Pour obtenir des conseils sur le déploiement de certificats, consultez Activer DNS sur HTTPS sur Windows DNS Server.

Configuration du client

Vérifiez que la configuration DoH du client correspond exactement à l'URI de votre serveur :

- Windows 11 : Paramètres réseau et Internet > [Connexion] > Paramètres > DNS
- Le modèle DoH doit correspondre à : `https://dns.contoso.com:443/dns-query`
- Si vous utilisez un port nondefault, vérifiez que les clients le spécifient.

Si vous configurez des clients mais qu'ils utilisent toujours un DNS non chiffré, vérifiez que l'adresse IP du serveur DNS dans les paramètres réseau client correspond à votre serveur DNS avec DoH activé.

Symptôme : Les requêtes DoH échouent ou expirent

Les clients se connectent au serveur DNS, mais les requêtes échouent ou ne reçoivent pas de réponses.

Causes courantes :

- Problèmes de résolution DNS en amont (ID d'événement 599)
- Incompatibilité du protocole client (ID d'événement 600)
- Problèmes de configuration du DoH client
- Problèmes de configuration du serveur DNS

Comment diagnostiquer :

Activez la journalisation analytique pour capturer des événements détaillés par requête :

1. Ouvrez l'Observateur d'événements et accédez aux **journaux**> des applications et services**Microsoft**>**Windows**>**DNS-Server**.

2. Cliquez avec le bouton droit sur **Analytique** et sélectionnez **Activer le journal**.

Pour obtenir des procédures détaillées de journalisation analytique, consultez Surveiller DNS sur HTTPS - Événements analytiques.

Vérifiez ces événements clés :

- **ID d'événement 597** : Requête DoH reçue - confirme que les requêtes DNS chiffrées atteignent le serveur
- **ID d'événement 598** : Réponse DoH envoyée - confirme les réponses réussies
- **ID d'événement 599** : Échec de la réponse DoH : indique que le serveur a essayé de répondre mais n'a pas pu (probablement résoudre le problème de résolution en amont)
- **ID d'événement 600** : requête DoH rejetée : le serveur supprime activement certaines requêtes DoH
- **ID d'événement 601** : Échec du canal DoH - peut accompagner 600 ou 599 dans certains cas d'erreur

Recherchez des modèles :

- Plusieurs entrées d'ID d'événement 597, mais aucune entrée d'ID d'événement 598 suggère que le serveur ne peut pas résoudre les requêtes.
- Les entrées d'ID d'événement 600 peuvent indiquer une incompatibilité de version HTTP ou des requêtes incorrectes.
- L'ID d'événement 599 avec `SERVFAIL RCODE` indique des problèmes de redirecteur en amont.

Résolution du problème :

Problèmes DNS en amont (ID d'événement 599)

Si vous voyez l'ID d'événement 599 avec `SERVFAIL` ou des erreurs similaires, vérifiez la configuration DNS en amont sur le serveur DNS. Exécutez la commande suivante:

PowerShell

```
Get-DnsServerForwarder
```

Pour tester la connectivité aux redirecteurs, exécutez la commande suivante :

PowerShell

```
Test-NetConnection -ComputerName <forwarder-ip> -Port 53
```

Si les redirecteurs sont inaccessibles ou mal configurés, essayez d'autres redirecteurs à l'aide de la commande suivante :

PowerShell

```
Set-DnsServerForwarder -IPAddress <new-forwarder-ip>
```

Pour tester la résolution manuellement, exécutez la commande suivante :

PowerShell

```
Resolve-DnsName -Name microsoft.com -Server localhost
```

Pour la résolution des problèmes DNS classique, consultez Résolution des problèmes liés aux serveurs DNS.

Rejet de requête (ID d'événement 600)

L'ID d'événement 600 indique les requêtes rejetées. Les causes courantes sont les suivantes :

- **Incompatibilité de requête HTTP** : le serveur DNS rejette la requête en raison de caractéristiques de requête HTTP non prises en charge ou non valides.
- **Requêtes incorrectes** : la requête n'est pas conforme à la norme RFC 8484.
- **Restrictions de stratégie DNS** : une stratégie DNS peut supprimer des requêtes.
- **Conditions requises pour les demandes côté serveur non remplies** : DoH n'est pas activé sur l'interface de réception ou il existe une incompatibilité de modèle d'URI ou une validation côté serveur, une configuration ou des vérifications de stratégie.

Vérifiez les détails de l'événement pour la raison du rejet. Si les clients utilisent des versions HTTP incompatibles, mettez à jour le logiciel client ou utilisez différentes applications clientes DoH.

Pour vérifier qu'aucune stratégie DNS n'interfère, exécutez la commande suivante :

PowerShell

```
Get-DnsServerQueryResolutionPolicy
```

Configuration du DoH du client

Si les requêtes échouent à partir de clients spécifiques, mais fonctionnent à partir d'autres utilisateurs, vérifiez la configuration DoH du client. Voici quelques problèmes courants :

- Modèle d'URI DoH incorrect
- Adresse IP du serveur DNS ne correspondant pas au serveur DNS utilisé pour DoH
- Client non configuré pour utiliser DoH

Pour obtenir des conseils sur la configuration du client, consultez Secure DNS Client over HTTPS (DoH).

Configurer le serveur

Si les requêtes échouent pour des raisons autres que celles répertoriées précédemment dans cet article, consultez la configuration générale du serveur DNS :

- Vérifiez que les hints racine sont configurés correctement.
- Vérifiez le chargement de zone pour les zones faisant autorité.
- Passez en revue les paramètres de récursivité si le serveur doit effectuer une résolution récursive.

Pour une résolution complète des problèmes DNS, consultez Résoudre les problèmes liés aux serveurs DNS.

Pour éviter une génération d'événements excessive, désactivez le journal analytique lorsque la résolution des problèmes est terminée.

Symptôme : Problèmes de performance DoH

DoH fonctionne, mais vous voyez une latence élevée, des requêtes supprimées ou des performances médiocres par rapport au DNS non chiffré.

Causes courantes :

- Limites de capacité du serveur
- Surcharge de négociation TLS
- Congestion du réseau ou utilisation élevée du processeur

Comment diagnostiquer :

Activez l'analyse pour les compteurs suivants à l'aide de Monitor DNS sur HTTPS - Surveiller les performances :

- Demandes DoH reçues par seconde
- Réponses DoH envoyées par secondes
- Demandes DoH rejetées/s

Indicateurs clés des problèmes de performances :

- **Requêtes DoH supprimées/s > 0** : le serveur ignore les requêtes.
- **Demandes reçues/s beaucoup plus élevées que les réponses envoyées/s** : de nombreuses requêtes ne reçoivent pas de réponses.
- **Utilisation élevée ou intensive du processeur** pendant le traitement des requêtes DoH.

Surveillez également les ressources système :

- Utilisation du processeur
- Utilisation de la mémoire
- Débit réseau

Si seules certaines requêtes sont lentes, le problème peut être externe à DoH. Par exemple, la récursivité lente vers les serveurs en amont pour des domaines spécifiques. Pour isoler la surcharge DoH des retards DNS généraux, comparez les performances DoH et DNS non chiffré pour les mêmes requêtes. Si les deux sont lents, le problème est probablement d'origine amont plutôt que spécifique à DoH.

Résolution du problème :

Requêtes supprimées

Si `DoH Requests Dropped/sec` la valeur est supérieure à 0, procédez comme suit :

1. Mettre en corrélation avec l'ID d'événement 600 dans les journaux du serveur DNS pour identifier la cause des chutes.
2. Vérifiez si le serveur est limité aux ressources.

PowerShell

```
Get-Counter '\Processor(_Total)\% Processor Time'
Get-Counter '\Memory\Available MBytes'
```

3. Si le processeur ou la mémoire est constamment élevé, tenez compte des points suivants :

    - Effectuer un scale-up du serveur avec davantage de ressources processeur ou RAM.
    - Ajout de serveurs DNS supplémentaires pour distribuer la charge.
    - Implémentation de l'équilibrage de charge DNS.

Latence élevée

La surcharge de négociation TLS peut augmenter la latence des requêtes par rapport au DNS non chiffré. Pour diagnostiquer les problèmes de latence :

- Comparez les temps de requête DoH aux bases de référence DNS non chiffrées pour les mêmes requêtes.
- Utilisez les outils côté client pour mesurer le temps de requête DoH de bout en bout.
- Si le DoH et le DNS non chiffré sont lents pour les mêmes requêtes, le problème est lié à la résolution en amont plutôt que spécifique au DoH.

Pour réduire la latence spécifique à DoH :

1. **Vérifiez la capacité du processeur du serveur** : les opérations TLS sont gourmandes en uc. Pour vérifier si le processeur est un goulot d'étranglement pendant le trafic DoH, exécutez la commande suivante :

    PowerShell
    ```
    Get-Counter '\Processor(_Total)\% Processor Time' -SampleInterval 1 -MaxSamples
    30
    ```

    Si le processeur dépasse constamment 70 à 80 % pendant le trafic DoH, envisagez de mettre à niveau les ressources du serveur ou de distribuer la charge.

2. **Passer en revue la longueur de la chaîne de certificats** : les chaînes de certificats plus courtes valident plus rapidement. Vérifiez que les certificats intermédiaires sont correctement configurés pour éviter les recherches supplémentaires.

3. **Vérifier les chemins réseau** : une latence réseau élevée entre les clients et le serveur DNS affecte directement le temps de requête. Utilisez `Test-NetConnection` ou `traceroute` pour rechercher des goulots d'étranglement réseau.

Contraintes de ressources

Si le serveur est sous-approvisionné :

1. Surveillez l'utilisation des ressources de référence pendant les opérations normales.
2. Identifiez les pics d'utilisation et mettez-les en corrélation avec le volume de requête.
3. Considérer:
    - Mise à l'échelle verticale (une machine virtuelle ou un serveur physique plus volumineux).
    - Mise à l'échelle horizontale (plusieurs serveurs DNS derrière un équilibreur de charge).
    - Optimisation des configurations de zone DNS pour réduire la surcharge de transfert de zone.

Pour surveiller les tendances à long terme et planifier la capacité, exécutez la commande suivante :

PowerShell

```
Get-Counter '\DNS-over-HTTPS\DoH Requests Received/sec' -Continuous
```

Pour obtenir des conseils sur la planification de la capacité, consultez Surveiller dns sur HTTPS - Surveiller les performances.

Diagnostic avancé

Lorsque la résolution des problèmes de base ne résout pas le problème, utilisez ces techniques avancées pour collecter des informations de diagnostic détaillées.

Activer la journalisation analytique

Le journal analytique du serveur DNS capture des événements détaillés par requête, y compris les opérations spécifiques à DoH. Lorsque vous activez le journal, il enregistre les ID d'événement 597-600 pour chaque requête DoH, réponse, échec et rejet.

Pour obtenir des instructions pas à pas sur l'activation et l'utilisation de la journalisation analytique, consultez Surveiller DNS sur HTTPS - Événements analytiques.

> ⓘ **Important**

Désactivez la journalisation analytique lorsque vous avez terminé, car elle génère un grand volume d'événements sur des serveurs occupés.

Analyse détaillée des événements

Lorsque vous passez en revue les événements DoH, examinez ces champs d'événements pour obtenir des indices de diagnostic :

- **QNAME** : Nom de domaine interrogé. Ce champ vous aide à identifier si les problèmes sont spécifiques au domaine.
- **QTYPE** : type d'enregistrement DNS, tel que A, AAAA, MX et autres.
- **RCODE** : Code de réponse, tel que NOERROR, SERVFAIL, NXDOMAIN et autres.
- **Raison** : Pour l'ID d'événement 600, ce champ fournit la raison du rejet.
- **Adresse IP du client** : source de la requête. Ce champ vous aide à identifier les clients problématiques.

Mettre en corrélation les événements au fil du temps :

- Recherchez des modèles. Les défaillances se produisent-ils à des moments spécifiques ?
- Vérifiez si plusieurs clients rencontrent le même problème.
- Identifiez si les défaillances correspondent à des périodes de charge élevées.

Effectuer une référence croisée avec d'autres logs :

- Journal des erreurs TLS Schannel pour le système.
- Journal opérationnel du serveur DNS pour les problèmes de zone et de redirecteur.
- Journal d'application pour les erreurs de niveau de service.

Analyse des performances

Pour une analyse approfondie des performances :

1. Établissez des métriques de référence pendant les opérations normales.
2. Comparez les performances actuelles à la base de référence.
3. Identifier les écarts et mettre en corrélation les événements ou les modifications de configuration.

Compteurs de performances clés à surveiller au fil du temps :

PowerShell

```
Get-Counter -Counter @(
    '\DNS-over-HTTPS\DoH Requests Received/sec',
    '\DNS-over-HTTPS\DoH Responses Sent/sec',
    '\DNS-over-HTTPS\DoH Requests Dropped/sec',
    '\Processor(_Total)\% Processor Time',
    '\Memory\Available MBytes'
) -SampleInterval 5 -MaxSamples 60
```

Cette commande échantillonne les compteurs toutes les 5 secondes pendant 5 minutes, fournissant des données de tendance.

Analyser les tendances :

- Les performances se dégradent-ils au fil du temps ?
- Certains moments de la journée présentent-ils des problèmes ?
- Les performances sont-ils corrélées avec le volume de requête ?

Utilisez ces données pour :

- Planifiez les mises à niveau de capacité.
- Identifiez les goulots d'étranglement de configuration.
- Optimisez les paramètres du serveur DNS.

Pour obtenir des conseils complets sur la surveillance des performances, consultez Surveiller dns sur HTTPS.

Contenu connexe

- Activer DNS sur HTTPS sur Windows DNS Server
- Surveiller DNS sur HTTPS
- Résoudre les problèmes liés aux serveurs DNS
- Journalisation et diagnostics DNS

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Last updated on 12/02/2026

Qu’est-ce que le serveur DHCP (Dynamic Host Configuration Protocol) dans Windows Server ?

Article • 13/05/2025 •

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Le serveur DHCP (Dynamic Host Configuration Protocol) dans Windows Server automatise l’affectation et la gestion des adresses IP et des configurations réseau associées. En centralisant ces tâches, le serveur DHCP réduit les efforts manuels, réduit les erreurs et garantit une utilisation efficace des ressources d’adresse IP sur votre réseau.

Windows Server inclut le serveur DHCP comme rôle de serveur de mise en réseau facultatif que vous pouvez déployer pour gérer et offrir des baux d’adresses IP et d’autres informations sur les clients DHCP. Tous les systèmes d’exploitation clients Windows incluent le client DHCP dans le cadre de TCP/IP, et le client DHCP est activé par défaut.

La fonction Dynamic Host Configuration Protocol (DHCP) est un protocole client/serveur qui fournit automatiquement une adresse Internet Protocol (IP) et d’autres informations de configuration pertinentes à un hôte IP (par exemple, masque de sous-réseau et passerelle par défaut). Les RFC 2131 et 2132 définissent DHCP comme une norme IETF (Internet Engineering Task Force) basée sur bootstrap Protocol (BOOTP), un protocole avec lequel DHCP partage de nombreux détails d’implémentation. DHCP permet aux hôtes d’obtenir les informations de configuration TCP/IP requises à partir d’un serveur DHCP.

Pourquoi utiliser DHCP ?

Chaque appareil sur un réseau TCP/IP doit avoir une adresse IP unique pour accéder au réseau et à ses ressources. Sans DHCP, les adresses IP des nouveaux ordinateurs ou ordinateurs qui sont déplacés d’un sous-réseau à un autre doivent être configurées manuellement ; les adresses IP des ordinateurs supprimés du réseau doivent être récupérées manuellement.

Avec DHCP, l’ensemble de ce processus est automatisé et géré de manière centralisée. Le serveur DHCP gère un pool d’adresses IP et loue une adresse à n’importe quel client avec DHCP lorsqu’il démarre sur le réseau. Étant donné que les adresses IP sont dynamiques (louées) plutôt que statiques (affectées de manière permanente), les adresses qui ne sont plus utilisées sont automatiquement retournées au pool pour la réaffectation.

L’administrateur réseau établit des serveurs DHCP qui conservent les informations de configuration TCP/IP et fournissent la configuration de l’adresse aux clients avec DHCP sous la

forme d'une offre de bail. Le serveur DHCP stocke les informations de configuration dans une base de données qui comprend :

- Les paramètres de configuration TCP/IP valides pour tous les clients du réseau.
- Adresses IP valides, conservées dans un pool pour l'affectation aux clients, ainsi que les adresses exclues.
- Les adresses IP réservées associées à des clients DHCP particuliers. Cela permet l'attribution cohérente d'une adresse IP unique à un seul client DHCP.
- Durée du bail ou durée pendant laquelle l'adresse IP peut être utilisée avant qu'un renouvellement de bail soit requis.

Un client avec DHCP, lors de l'acceptation d'une offre de bail, reçoit :

- Adresse IP valide pour le sous-réseau à laquelle il se connecte.
- Options DHCP demandées, qui sont des paramètres supplémentaires qu'un serveur DHCP est configuré pour être affecté aux clients. Parmi les exemples d'options DHCP, citons Routeur (passerelle par défaut), Serveurs DNS et Nom de domaine DNS.

Avantages du serveur DHCP

DHCP procure les avantages suivants.

- **Configuration d'adresse IP de confiance**. DHCP réduit les erreurs de configuration causées par la configuration manuelle des adresses IP, telles que les erreurs typographiques, ou les conflits d'adresses causés par l'attribution d'une adresse IP à plusieurs ordinateurs en même temps.
- **Administration réseau réduite**. DHCP inclut les fonctionnalités suivantes pour réduire l'administration réseau :
    - Configuration TCP/IP centralisée et automatisée.
    - Possibilité de définir des configurations TCP/IP à partir d'un emplacement central.
    - Possibilité d'affecter une plage complète de valeurs de configuration TCP/IP supplémentaires au moyen d'options DHCP.
    - Gestion efficace des modifications d'adresse IP pour les clients qui doivent être mis à jour fréquemment, comme ceux des appareils portables qui se déplacent à différents emplacements sur un réseau sans fil.

- Transfert des messages DHCP initiaux à l'aide d'un agent de relais DHCP, ce qui élimine le besoin d'un serveur DHCP sur chaque sous-réseau.

Fonctionnalités du serveur DHCP

Le serveur DHCP dans Windows Server inclut les fonctionnalités suivantes :

- **Stratégies DHCP**. Cette fonctionnalité vous permet de créer des stratégies qui appliquent des options DHCP et des paramètres en fonction des caractéristiques du client, telles que l'adresse MAC ou la classe de fournisseur.
- **Journalisation d'audit DHCP**. Cette fonctionnalité vous permet de suivre l'activité du serveur DHCP, y compris les affectations de bail et les renouvellements.
- **Gestion du serveur DHCP**. Cette fonctionnalité vous permet de gérer des serveurs DHCP à l'aide de Windows PowerShell, de la console DHCP ou de Windows Admin Center.
- **Autorisation du serveur DHCP**. Cette fonctionnalité vous permet d'autoriser les serveurs DHCP dans Active Directory, ce qui empêche les serveurs non autorisés de fournir des adresses IP aux clients.
- **Intégration du serveur DHCP à DNS**. Le DNS dynamique met automatiquement à jour les enregistrements DNS lorsque des baux DHCP sont attribués ou renouvelés, ce qui garantit que les clients peuvent résoudre les noms d'hôte en adresses IP.
- **Intégration du serveur DHCP à IPv4 et IPv6**. Cette fonctionnalité vous permet d'affecter à la fois des adresses IPv4 et IPv6 aux clients à l'aide de DHCP, ce qui permet de prendre en charge les deux normes d'adressage IP.
- **Basculement DHCP**. Cette fonctionnalité permet à deux serveurs DHCP de partager une seule étendue, ce qui fournit une redondance et un équilibrage de charge.
- **Intégration du serveur DHCP à IPAM**. Cette fonctionnalité vous permet de gérer les serveurs DHCP à l'aide de la gestion des adresses IP (IPAM), en fournissant un emplacement centralisé pour la gestion des affectations d'adresses IP et des baux.

Commencez à utiliser DHCP

Pour savoir comment installer et configurer DHCP dans Windows Server, consultez Démarrage rapide : Installer et configurer le serveur DHCP.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Démarrage rapide : Installer et configurer un serveur DHCP

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans ce guide de démarrage rapide, vous installez un serveur DHCP (Dynamic Host Configuration Protocol) sur Windows Server. Tout d'abord, vous devez installer le rôle serveur DHCP, autoriser le serveur dans votre domaine Active Directory, puis configurer une étendue pour affecter automatiquement des adresses IP DHCP et des options aux clients DHCP IPv4.

Prérequis

Avant de pouvoir installer votre serveur DHCP, vous devez respecter les prérequis suivants :

- Un ordinateur exécutant une version de Windows Server prise en charge.
- Une adresse IPv4 statique.
- Une plage d'adresses IP pour votre étendue DHCP.
- Un compte membre du groupe Administrateurs ou équivalent.

Installer le serveur DHCP

L'installation du serveur DHCP implique l'ajout du rôle Serveur DHCP à un serveur Windows Server existant.

Installer le rôle serveur DHCP

Installez le rôle serveur DHCP en tant que serveur autonome à l'aide de PowerShell ou du Gestionnaire de serveur. Sélectionnez votre méthode et suivez les étapes décrites dans cette section pour installer le rôle.

PowerShell

Voici comment installer DHCP à l'aide de la commande Install-WindowsFeature.

1. Exécutez PowerShell sur votre ordinateur dans une session avec élévation de privilèges.

2. Exécutez la commande suivante :

PowerShell

```
Install-WindowsFeature DHCP -IncludeManagementTools
```

L'installation ne nécessite pas de redémarrage.

Configurer un server DHCP

Une fois que vous avez correctement installé le rôle serveur DHCP, vous devez autoriser et configurer votre serveur DHCP.

Autoriser le serveur DHCP dans Active Directory

Si vous installez DHCP dans un environnement de domaine, vous devez effectuer les étapes suivantes pour autoriser le serveur DHCP à fonctionner dans le domaine.

> **Notes**
>
> Les serveurs DHCP non autorisés installés dans des domaines Active Directory ne peuvent pas fonctionner correctement et ne louent pas d'adresses IP aux clients DHCP. La désactivation automatique des serveurs DHCP non autorisés est une fonctionnalité de sécurité qui empêche les serveurs DHCP non autorisés d'attribuer des adresses IP incorrectes aux clients de votre réseau.

Pour autoriser votre serveur DHCP dans un environnement de domaine :

PowerShell

1. Exécutez la commande suivante pour ajouter le serveur DHCP à la liste des serveurs DHCP autorisés dans Active Directory.

   > **Notes**
   >
   > Si vous n'avez pas d'environnement de domaine, n'exécutez pas cette commande.

   PowerShell

```
Add-DhcpServerInDC -DnsName DHCP1.corp.contoso.com -IPAddress 10.0.0.3
```

2. Pour vérifier que le serveur DHCP est autorisé dans Active Directory, exécutez la commande suivante :

   PowerShell

   ```
   Get-DhcpServerInDC
   ```

   L'exemple suivant montre la sortie que vous devriez voir dans Windows PowerShell.

   PowerShell

   ```
   IPAddress      DnsName
   ---------      -------
   10.0.0.3       DHCP1.corp.contoso.com
   ```

Pour plus d'informations sur ces commandes, consultez les articles suivants :

- Add-DhcpServerInDC
- Get-DhcpServerInDC

Configurer une étendue IPv4

Une fois que vous avez autorisé votre serveur DHCP, vous pouvez procéder à la création d'une étendue DHCP. Les étendues sont utilisées pour indiquer la plage d'adresses IP de votre serveur DHCP et de ses clients.

Pour en savoir plus sur la planification de vos plages d'étendues, consultez Étendues DHCP pour obtenir des conseils.

Pour créer une étendue DHCP IPv4, sélectionnez la méthode appropriée et suivez les instructions.

PowerShell

Voici comment créer une étendue à l'aide de la commande PowerShell Add-DhcpServerv4Scope.

1. Exécutez PowerShell sur votre ordinateur dans une session avec élévation de privilèges.

2. Pour configurer une nouvelle étendue DHCP nommée `Contoso network` avec une plage de `10.10.10.100` à `10.10.10.200` et un masque de sous-réseau de `255.255.255.0`, exécutez la commande suivante.

PowerShell

```
Add-DhcpServerv4Scope -Name "Contoso network" -StartRange 10.10.10.100 -
EndRange 10.10.10.200 -SubnetMask 255.255.255.0
```

Gérer les options d'étendue

Après avoir configuré votre nouvelle étendue, vous pouvez gérer les options d'étendue à l'aide de la console DHCP ou de PowerShell.

PowerShell

Vous pouvez modifier les options d'étendue DHCP à l'aide de PowerShell avec l'applet de commande **Set-DhcpServerv4OptionValue**. Par exemple, pour définir l'option Serveur DNS pour l'étendue `192.168.15.0` et définir les serveurs DNS avec les valeurs `192.168.15.10` et `192.168.15.11`, exécutez la commande suivante :

PowerShell

```
Set-DhcpServerv4OptionValue -ScopeId 192.168.15.0 -OptionId 6 -Value
"192.168.15.10", "192.168.15.11"
```

Gérer les réservations

Avec les réservations clientes, vous pouvez réserver une adresse IP pour une utilisation permanente par un client DHCP. Les réservations sont stockées en utilisant l'adresse MAC d'une carte d'interface réseau (NIC) et garantissent que le serveur DHCP loue exclusivement une adresse IP spécifique à une adresse MAC spécifique.

PowerShell

Vous pouvez créer des réservations à l'aide de l'applet de commande PowerShell **Add-DhcpServerv4Reservation**. Par exemple, pour ajouter une réservation à une étendue DHCP avec un ID d'étendue `192.168.15.0`, une adresse IP `192.168.15.100` et l'adresse Mac `00-11-22-33-44-55`, exécutez la commande PowerShell suivante :

PowerShell

```
Add-DhcpServerv4Reservation -ScopeId 192.168.15.0 -IPAddress 192.168.15.100 -
ClientId "00-11-22-33-44-55"
```

Gérer les exclusions

Voici comment gérer les plages d'exclusions dans le serveur DHCP.

PowerShell

Vous pouvez exécuter l'applet de commande **Add-DhcpServerv4ExclusionRange** pour ajouter une plage d'exclusion à une étendue DHCP à l'aide de PowerShell. Par exemple, pour ajouter la plage d'exclusion de `192.168.15.1` à `192.168.15.10` à l'étendue `192.168.15.0`, exécutez la commande suivante :

PowerShell

```
Add-DhcpServerv4ExclusionRange -ScopeId 192.168.15.0 -StartRange 192.168.15.1
-EndRange 192.168.15.10
```

Contenu connexe

- Principes de base DHCP
- Options de sélection du sous-réseau DHCP

Options de sélection du sous-réseau DHCP

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Vous pouvez utiliser cette rubrique pour plus d'informations sur les nouvelles options de sélection du sous-réseau DHCP.

DHCP prend désormais en charge l'option 82 (sous-option 5). Vous pouvez utiliser ces options pour autoriser les clients proxy DHCP et les agents de relais à demander une adresse IP pour un sous-réseau spécifique, ainsi qu'à partir d'une plage d'adresses IP et d'une étendue spécifiques. Pour plus d'informations, consultez **Option 82 sous-option 5** : RFC 3527 Sous-option Sélection de lien pour l'option Informations sur l'agent de relais pour DHCPv4.

Si vous utilisez un agent de relais DHCP configuré avec l'option DHCP 82, sous-option 5, l'agent de relais peut demander un bail d'adresse IP pour les clients DHCP à partir d'une plage d'adresses IP spécifique.

Option 82 sous-option 5 : Sous-option Sélection de lien

La sous-option Sélection de lien de l'agent de relais de relais permet à un agent de relais DHCP de spécifier un sous-réseau IP à partir duquel le serveur DHCP doit attribuer des adresses IP et des options.

En règle générale, les agents de relais DHCP s'appuient sur le champ Adresse IP de la passerelle (GIADDR) pour communiquer avec les serveurs DHCP. Toutefois, l'adresse GIADDR est limitée par ses deux fonctions opérationnelles :

1. Pour informer le serveur DHCP du sous-réseau sur lequel réside le client DHCP qui demande le bail d'adresse IP.
2. Pour informer le serveur DHCP de l'adresse IP à utiliser pour communiquer avec l'agent de relais.

Dans certains cas, l'adresse IP que l'agent de relais utilise pour communiquer avec le serveur DHCP peut être différente de la plage d'adresses IP à partir de laquelle l'adresse IP du client DHCP doit être allouée.

La sous-option Sélection de lien de l'option 82 est utile dans ce cas, ce qui permet à l'agent de relais d'indiquer explicitement le sous-réseau à partir duquel il souhaite que l'adresse IP soit allouée sous la forme de l'option 82 sous-option 5 de DHCP v4.

> **Notes**
>
> Toutes les adresses IP de l'agent de relais (GIADDR) doivent faire partie d'une plage d'adresses IP d'étendue DHCP active. Toute adresse GIADDR en dehors des plages d'adresses IP d'étendue DHCP est considérée comme un relais non autorisé et Windows DHCP Server n'accuse pas réception des demandes client DHCP de ces agents de relais.
>
> Une étendue spéciale peut être créée pour « autoriser » les agents de relais. Créez une étendue avec l'adresse GIADDR (ou plusieurs si les adresses GIADDR sont des adresses IP séquentielles), excluez la ou les adresses GIADDR de la distribution, puis activez l'étendue. Cela autorise les agents de relais tout en empêchant l'attribution des adresses GIADDR.

Cas d'utilisation

Dans ce scénario, un réseau d'organisation comprend à la fois un serveur DHCP et un point d'accès sans fil (AP) pour les utilisateurs invités. Les adresses IP des clients invités sont attribuées à partir du serveur DHCP de l'organisation. Toutefois, en raison des restrictions de la stratégie de pare-feu, le serveur DHCP ne peut pas accéder au réseau sans fil invité ou aux clients sans fil avec des messages en majuscules.

Pour résoudre cette restriction, l'AP est configuré avec la sous-option Sélection de lien 5 pour spécifier le sous-réseau à partir duquel il souhaite que l'adresse IP soit allouée aux clients invités, tandis que dans l'adresse GIADDR, il spécifie également l'adresse IP de l'interface interne qui mène au réseau d'entreprise.

Commentaires

Cette page a-t-elle été utile ? Yes No

Événements de journalisation DHCP pour les inscriptions DNS

Article • 17/04/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Les journaux d'événements du serveur DHCP fournissent désormais des informations détaillées sur les échecs d'inscription DNS.

Notes

Dans de nombreux cas, les échecs d'inscription d'enregistrements DNS par les serveurs DHCP sont causés par une zone de recherche inversée DNS configurée de manière incorrecte ou non configurée du tout.

Les nouveaux événements DHCP suivants vous aident à identifier facilement quand les inscriptions DNS échouent en raison d'une zone de recherche inversée DNS mal configurée ou manquante.

id	Événement	Valeur
20317	DHCPv4.ForwardRecordDNSFailure	L'inscription de l'enregistrement de transfert pour l'adresse IPv4 %1 et le nom de domaine complet %2 a échoué avec l'erreur %3. Cela est probablement dû au fait que la zone de recherche directe pour cet enregistrement n'existe pas sur le serveur DNS.
20318	DHCPv4.ForwardRecordDNSTimeout	L'inscription de l'enregistrement de transfert pour l'adresse IPv4 %1 et le nom de domaine complet %2 a échoué avec l'erreur %3.
20319	DHCPv4.PTRRecordDNSFailure	L'inscription de l'enregistrement de transfert pour l'adresse IPv4 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3. Cela est probablement dû au fait que la zone de recherche inversée pour cet enregistrement n'existe pas sur le serveur DNS.
20320	DHCPv4.PTRRecordDNSTimeout	L'inscription de l'enregistrement de transfert pour l'adresse IPv4 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3.

id	Événement	Valeur
20321	DHCPv6.ForwardRecordDNSFailure	L'inscription de l'enregistrement de transfert pour l'adresse IPv6 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3. Cela est probablement dû au fait que la zone de recherche directe pour cet enregistrement n'existe pas sur le serveur DNS.
20322	DHCPv6.ForwardRecordDNSTimeout	L'inscription de l'enregistrement de transfert pour l'adresse IPv6 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3.
20323	DHCPv6.PTRRecordDNSFailure	L'inscription de l'enregistrement de transfert pour l'adresse IPv6 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3. Cela est probablement dû au fait que la zone de recherche inversée pour cet enregistrement n'existe pas sur le serveur DNS.
20324	DHCPv6.PTRRecordDNSTimeout	L'inscription de l'enregistrement de transfert pour l'adresse IPv6 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3.
20325	DHCPv4.ForwardRecordDNSError	L'inscription de l'enregistrement de transfert pour l'adresse IPv4 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3 (%4).
20326	DHCPv6.ForwardRecordDNSError	L'inscription de l'enregistrement de transfert pour l'adresse IPv6 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3 (%4)
20327	DHCPv6.PTRRecordDNSError	L'inscription de l'enregistrement de transfert pour l'adresse IPv6 %1 et le nom de domaine complet (FQDN) %2 a échoué avec l'erreur %3 (%4).

DHCP scopes

30/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Une étendue DHCP (Dynamic Host Configuration Protocol) est un regroupement administratif d'adresses IP pour les ordinateurs sur un sous-réseau que le serveur DHCP peut louer aux clients. Lorsque vous définissez une ou plusieurs étendues sur votre serveur DHCP, le serveur peut gérer la distribution et l'attribution d'adresses IP aux clients DHCP.

Les étendues vous permettent de configurer des paramètres réseau pour tous les clients, tels que les serveurs DNS (Domain Name System) et les passerelles réseau. Les étendues filtrent les hôtes par nom, adresse MAC et même système d'exploitation avant d'attribuer une adresse IP. Vous pouvez configurer la stratégie pour chaque étendue.

Cet article explique les différents types d'étendues, leur option et comment planifier la création de votre étendue. Si vous recherchez des informations sur la création et la configuration d'une étendue DHCP, consultez démarrage rapide : Installer et configurer le serveur DHCP à la place. Avant de créer votre nouvelle étendue, vous devez également planifier la plage d'adresses IP qu'elle doit utiliser.

Types d'étendues

Le serveur DHCP inclut les types d'étendues suivants :

- Single scope.
- Multicast scope.
- DHCP Superscopes.

Single scope

Une seule étendue est la configuration la plus simple possible dans DHCP. Une étendue unique est une plage d'adresses IP et d'options de configuration associées allouées aux clients DHCP dans un sous-réseau spécifique.

En outre, une étendue DHCP classique a les propriétés suivantes :

- une plage d'adresses IP où inclure ou exclure les adresses utilisées pour les offres de bail de service DHCP ;
- un masque de sous-réseau, qui détermine le préfixe de sous-réseau correspondant à une adresse IP donnée ;

- Nom de portée qui est automatiquement attribué lorsque vous créez la portée.
- des valeurs de durée de bail, qui sont affectées aux clients DHCP recevant des adresses IP allouées de manière dynamique ;
- Toutes les options d'étendue DHCP configurées pour l'affectation aux clients DHCP, telles que le serveur DNS, le routeur et les adresses IP de passerelle par défaut.
- des réservations, utilisées de manière optionnelle pour s'assurer qu'un client DHCP reçoit toujours la même adresse IP.

Avant de déployer votre serveur DHCP, répertoriez vos sous-réseaux et la plage d'adresses IP que vous souhaitez utiliser pour chaque sous-réseau.

D'autres types d'étendues disponibles dans un serveur DHCP IPv4 autorisé peuvent fournir des fonctionnalités étendues, en fonction des besoins et des considérations de déploiement de vos utilisateurs.

Multicast scope

La multidiffusion dans Windows est le processus d'envoi d'un message à un groupe de destinataires, contrairement à un message envoyé à un destinataire spécifique. Dans une configuration à étendue unique, DHCP affecte à chaque client une adresse IP unique à partir d'une plage d'adresses IP que vous avez planifiées et configurées avant d'activer l'étendue. En revanche, une étendue de multidiffusion est un groupe d'adresses réseau de multidiffusion IP que le serveur DHCP peut distribuer à d'autres ordinateurs de votre réseau à l'aide du protocole MADCAP (Multicast Address Dynamic Client Allocation Protocol). MADCAP contrôle la façon dont le serveur DHCP affecte dynamiquement des adresses IP. For more information about how MADCAP works, see RFC2730 .

DHCP Superscopes

Les superscopes DHCP sont une fonctionnalité d'administration du serveur DHCP que vous pouvez utiliser pour regrouper plusieurs étendues en tant qu'entité administrative unique. Les étendues globales permettent d'identifier facilement quelles étendues résident dans quels réseaux. Dans un environnement avec plusieurs sous-réseaux définis sur un seul réseau physique, les superscopes permettent à votre serveur DHCP d'attribuer des baux aux clients sur ces plusieurs sous-réseaux. See DHCP Superscopes to learn more about how to enable DHCP Superscopes.

Scope options

Les options d'étendue que vous configurez au niveau du serveur sont appliquées à tous les clients DHCP, quel que soit le sous-réseau sur lequel ils sont activés. Si vous souhaitez que certaines fonctionnalités soient disponibles sur tous les clients DHCP, vous devez la configurer au niveau du serveur. Ces options standard sont les suivantes :

- Default gateway.
- Noms de domaine et serveurs DNS.
- Serveurs WINS (Windows Internet Name Service).

Outre les options standard, vous pouvez configurer des classes spécifiques à l'utilisateur ou à un fournisseur.

Définir une étendue DHCP

Chaque sous-réseau ne peut avoir qu'une seule étendue DHCP avec une seule plage continue d'adresses IP. Pour utiliser plusieurs plages d'adresses dans une étendue ou un sous-réseau unique pour le service DHCP, vous devez d'abord définir l'étendue, puis définir les plages d'exclusion requises. Les sections suivantes décrivent comment planifier les plages d'exclusion.

Planifier les plages d'adresses

La planification des plages d'adresses IP sur plusieurs étendues sur un serveur DHCP IPv4 autorisé est essentielle pour comprendre le fonctionnement des étendues et la création réussie de nouvelles étendues.

Chaque sous-réseau doit avoir sa propre plage d'adresses IP unique. La plage d'adresses IP spécifie les adresses IP à inclure ou exclure pour l'affectation aux clients DHCP. En d'autres termes, une plage d'adresses IP vous permet de sélectionner les adresses que les appareils connectés à votre DHCP peuvent utiliser. Les plages d'adresses IP sont représentées sur un serveur DHCP en tant qu'étendues ou regroupements d'adresses IP sur le sous-réseau qui utilise le service DHCP. Vous pouvez également exclure des adresses IP spécifiques que vous ne souhaitez pas que les clients utilisent.

Lorsque vous définissez votre plage d'adresses IP pour chaque étendue, vous devez utiliser la plage complète d'adresses IP consécutives qui composent le sous-réseau local de votre service DHCP. Nous vous recommandons vivement d'établir l'ensemble de la plage d'adresses avant d'identifier les adresses IP statiques au sein de votre plage. Après avoir établi la plage, il est plus facile d'identifier les adresses IP restantes disponibles pour les clients DHCP à louer.

Vous devez planifier les plages d'adresses IP avant de configurer des étendues. Pour en savoir plus sur la création de nouvelles étendues sur un serveur DHCP IPv4 autorisé, consultez Installer le serveur DHCP.

Reservations

Votre réseau comprend des serveurs, des routeurs, des commutateurs, des imprimantes et d'autres appareils qui peuvent nécessiter des adresses IP réservées (statiques). Il est judicieux de faire une liste de ces appareils, y compris des adresses de réserve supplémentaires que vous pourrez utiliser au fur et à mesure que vos besoins augmentent. Une réservation DHCP est une adresse IP prédéfinie fournie par votre serveur DHCP et donnée à une carte d'interface réseau lorsqu'une carte réseau appelle un serveur DHCP pour une adresse IP. N'oubliez pas qu'un appareil doit prendre en charge DHCP pour utiliser des réservations.

Vous pouvez utiliser des réservations pour affecter une adresse IP à un appareil client (NIC) spécifique en fonction de son adresse MAC. L'appareil reçoit toujours la même adresse IP et l'adresse ne change jamais. L'appareil dépend de votre serveur DHCP après avoir configuré la réservation. Si le serveur DHCP rencontre des problèmes et s'arrête, l'appareil de réservation DHCP devient également indisponible.

Les réservations vous permettent de modifier facilement les adresses IP sans avoir à se connecter à un appareil. Vous pouvez également gérer les adresses IP des appareils tiers s'ils sont définis sur DHCP.

Exclusion ranges

Il existe certains scénarios où vous devrez peut-être configurer manuellement des serveurs ou d'autres appareils avec des adresses IP statiques à partir de la même plage d'adresses IP que le serveur DHCP. Dans ces situations, il est possible de créer involontairement un conflit d'adresse IP dans lequel vous et le serveur DHCP attribuez la même adresse IP à différents appareils.

Pour éviter les conflits d'adresses, vous pouvez créer une plage d'exclusion pour l'étendue DHCP. Une plage d'exclusion est une plage contiguë d'adresses IP dans la plage d'adresses IP de l'étendue que le serveur DHCP n'est pas autorisé à utiliser. Si vous créez une plage d'exclusion, le serveur DHCP n'affecte pas d'adresses à cette plage, ce qui vous permet d'affecter manuellement ces adresses sans créer de conflit d'adresses IP.

Vous devez utiliser des exclusions pour tous les appareils configurés avec une adresse IP statique. Les adresses exclues doivent inclure toutes les adresses IP que vous avez attribuées manuellement à d'autres serveurs, clients non DHCP, stations de travail sans disque ou routage et accès à distance et clients PPP (Point à Point Protocol).

Nous vous recommandons de configurer votre plage d'exclusion avec des adresses d'espace réservé supplémentaires afin de prendre en compte la croissance future du réseau. Le tableau suivant fournit un exemple de plage d'exclusion pour une étendue avec une plage d'adresses IP de 10.0.0.1 à 10.0.0.254 et un masque de sous-réseau de 255.255.255.0.

Agrandir le tableau

Configuration items	Example values
Adresse IP de début de la plage d'exclusion	10.0.0.1
Adresse IP de fin de la plage d'exclusion	10.0.0.25

Next steps

En savoir plus sur les étendues DHCP aux ressources suivantes :

- Principes de base du protocole DHCP (Dynamic Host Configuration Protocol)
- Options de sélection de sous-réseau DHCP
- Démarrage rapide : Installer et configurer le serveur DHCP

Déploiement de DHCP à l'aide de Windows PowerShell

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Ce guide fournit des instructions sur l'utilisation de Windows PowerShell pour déployer un serveur DHCP (Dynamic Host Configuration Protocol) IP (Internet Protocol) version 4 qui affecte automatiquement des adresses IP et des options DHCP aux clients DHCP IPv4 connectés à un ou plusieurs sous-réseaux de votre réseau.

> ⓘ **Notes**
>
> Pour télécharger ce document au format Word à partir de TechNet Gallery, consultez Déployer DHCP à l'aide de Windows PowerShell dans Windows Server 2016.

L'utilisation de serveurs DHCP pour attribuer des adresses IP permet de réduire la surcharge administrative, car vous n'avez pas besoin de configurer manuellement les paramètres TCP/IP v4 pour chaque carte réseau de chaque ordinateur de votre réseau. Avec DHCP, la configuration TCP/IP v4 est effectuée automatiquement lorsqu'un ordinateur ou un autre client DHCP est connecté à votre réseau.

Vous pouvez déployer votre serveur DHCP dans un groupe de travail en tant que serveur autonome ou dans le cadre d'un domaine Active Directory.

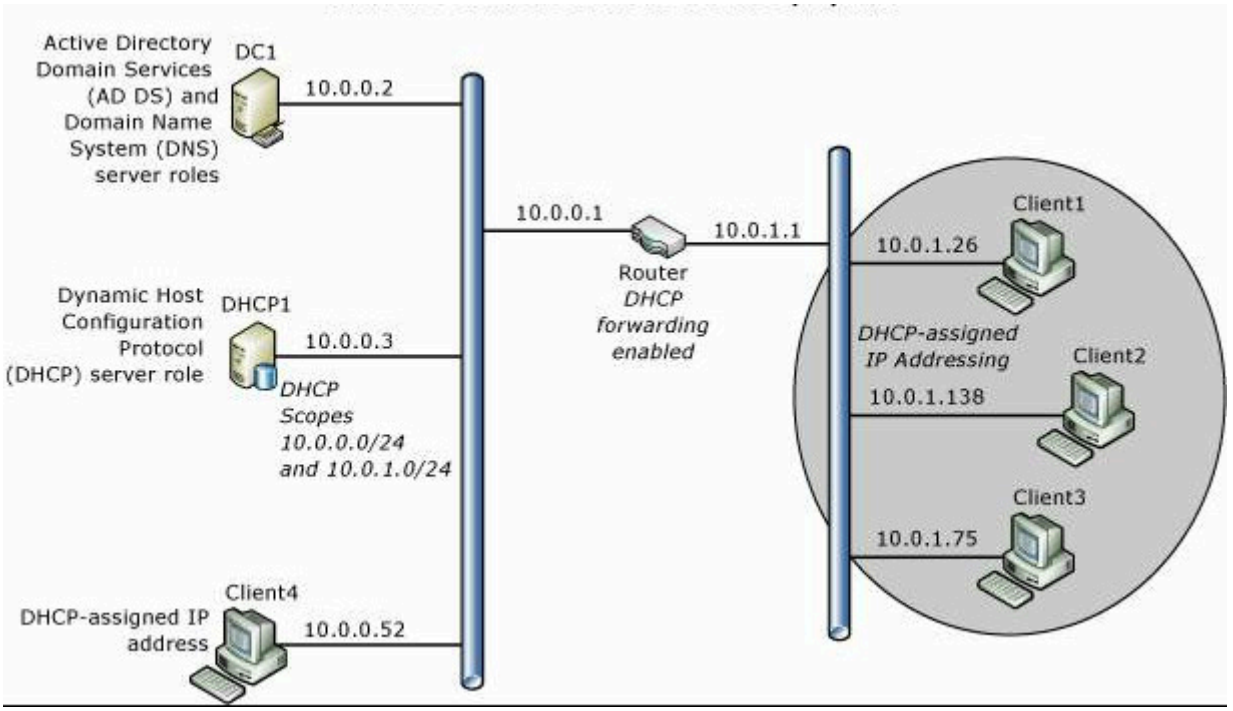
Ce guide contient les sections suivantes.

- Vue d'ensemble du déploiement DHCP
- Vue d'ensemble des technologies
- Planifier le déploiement DHCP
- Utilisation de ce guide dans un laboratoire de test
- Déployer DHCP
- Vérifier la fonctionnalité du serveur
- Commandes Windows PowerShell pour DHCP
- Liste des commandes Windows PowerShell dans ce guide

Vue d'ensemble du déploiement DHCP

L'illustration suivante illustre le scénario que vous pouvez déployer à l'aide de ce guide. Le scénario inclut un serveur DHCP dans un domaine Active Directory. Le serveur est configuré

pour fournir des adresses IP aux clients DHCP sur deux sous-réseaux différents. Les sous-réseaux sont séparés par un routeur sur lequel le transfert DHCP est activé.



Vue d’ensemble des technologies

Les sections suivantes fournissent une brève vue d’ensemble de DHCP et TCP/IP.

Vue d’ensemble du protocole DHCP

DHCP est une norme IP permettant de simplifier la gestion de la configuration IP de l’hôte. Cette norme permet d’utiliser des serveurs DHCP comme moyen de gérer l’allocation dynamique d’adresses IP et d’autres informations de configuration pour les clients DHCP sur votre réseau.

DHCP vous permet d’utiliser un serveur DHCP pour attribuer dynamiquement une adresse IP à un ordinateur ou un autre périphérique, tel qu’une imprimante, sur votre réseau local, plutôt que de configurer manuellement chaque appareil avec une adresse IP statique.

Chaque ordinateur d’un réseau TCP/IP doit avoir une adresse IP unique, car cette adresse et son masque de sous-réseau associé sont utilisés pour identifier l’ordinateur hôte et le sous-réseau auquel l’ordinateur est joint. Avec le protocole DHCP, vous avez l’assurance que tous les ordinateurs configurés en tant que clients DHCP reçoivent une adresse IP correspondant à leur emplacement réseau et leur sous-réseau. De plus, en utilisant les options DHCP, telles qu’une passerelle par défaut et des serveurs DNS, vous fournissez automatiquement aux clients DHCP les informations dont ils ont besoin pour fonctionner correctement sur votre réseau.

Pour les réseaux TCP/IP, le réseau DHCP réduit la complexité et le travail d'administration nécessaires pour configurer les ordinateurs.

Vue d'ensemble du protocole TCP/IP

Par défaut, toutes les versions des systèmes d'exploitation Windows Server et clients Windows ont des paramètres TCP/IP pour les connexions réseau IP version 4 configurées pour obtenir automatiquement une adresse IP et d'autres informations, appelées options DHCP, à partir d'un serveur DHCP. À ce titre, vous n'avez pas besoin de configurer manuellement les paramètres TCP/IP, sauf s'il s'agit d'un ordinateur serveur ou d'un autre appareil qui nécessite une adresse IP statique configurée manuellement.

Par exemple, il est recommandé de configurer manuellement l'adresse IP du serveur DHCP, ainsi que les adresses IP des serveurs DNS et des contrôleurs de domaine qui exécutent les Active Directory Domain Services (AD DS).

TCP/IP dans Windows Server 2016 est le suivant :

- un logiciel réseau reposant sur des protocoles réseau standard ;
- un protocole réseau d'entreprise routable qui prend en charge la connexion de votre ordinateur Windows aux environnements de réseau local (LAN, Local Area Network) et de réseau étendu (WAN, Wide Area Network) ;
- un ensemble de technologies et d'utilitaires centraux permettant de connecter votre ordinateur Windows à des systèmes hétérogènes pour le partage d'informations ;
- une base pour pouvoir accéder aux services Internet globaux, comme les serveurs Web et FTP (File Transfer Protocol).
- une infrastructure client/serveur interplateforme, évolutive et robuste.

TCP/IP propose des utilitaires TCP/IP de base qui permettent aux ordinateurs Windows de se connecter à d'autres systèmes d'exploitation Microsoft et non-Microsoft pour partager des informations, notamment :

- Windows Server 2016
- Windows 10
- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012

- Windows 8
- Windows Server 2008 R2
- Windows 7
- Windows Server 2008
- Windows Vista
- Hôtes Internet
- Systèmes Apple Macintosh
- Ordinateurs mainframes IBM
- Systèmes UNIX et Linux
- Systèmes Open VMS
- Imprimantes prêtes pour le réseau
- Tablettes et téléphones cellulaires avec activation de la technologie filaire Ethernet ou sans fil 802.11

Planifier le déploiement DHCP

Cette section décrit les principales étapes de planification qui doivent être suivies avant d'installer le rôle serveur DHCP.

Planification des serveurs DHCP et de l'acheminement DHCP

Les messages DHCP étant des messages de diffusion, ils ne sont pas acheminés entre les sous-réseaux par les routeurs. Si vous avez plusieurs sous-réseaux et souhaitez proposer le service DHCP sur chacun d'eux, vous devez procéder comme suit :

- Installez un serveur DHCP sur chaque sous-réseau.
- Configurez les routeurs pour qu'ils acheminent les messages de diffusion DHCP dans les sous-réseaux et configurez plusieurs étendues sur le serveur DHCP, à raison d'une étendue par sous-réseau.

En règle générale, il est économiquement plus avantageux de configurer des routeurs pour qu'ils acheminent les messages de diffusion DHCP plutôt que de déployer un serveur DHCP sur chaque segment physique du réseau.

Planification de plages d’adresses IP

Chaque sous-réseau doit avoir sa propre plage d’adresses IP unique. Ces plages sont représentées sur un serveur DHCP avec des étendues.

Une étendue est un groupement administratif des adresses IP des ordinateurs d’un sous-réseau qui utilisent le service DHCP. L’administrateur crée d’abord une étendue pour chaque sous-réseau physique, puis utilise l’étendue pour définir les paramètres utilisés par les clients.

Une étendue possède les propriétés suivantes :

- une plage d’adresses IP où inclure ou exclure les adresses utilisées pour les offres de bail de service DHCP ;
- un masque de sous-réseau, qui détermine le préfixe de sous-réseau correspondant à une adresse IP donnée ;
- un nom affecté à l’étendue lors de sa création ;
- des valeurs de durée de bail, qui sont affectées aux clients DHCP recevant des adresses IP allouées de manière dynamique ;
- des options d’étendue DHCP configurées pour être affectées aux clients DHCP, telles que l’adresse IP d’un serveur DNS et l’adresse IP d’un routeur/d’une passerelle par défaut ;
- des réservations, utilisées de manière optionnelle pour s’assurer qu’un client DHCP reçoit toujours la même adresse IP.

Avant de déployer vos serveurs, dressez la liste de vos sous-réseaux et des plages d’adresses IP à utiliser pour chaque sous-réseau.

Planification des masques de sous-réseaux

Au sein d’une adresse IP, les ID de réseau et les ID d’hôte sont différenciés à l’aide d’un masque de sous-réseau. Chaque masque de sous-réseau est un nombre de 32 bits qui utilise des groupes de bits consécutifs composés uniquement de 1 pour identifier l’ID de réseau et composés uniquement de 0 pour identifier les parties de l’adresse IP relatives à l’ID d’hôte.

Par exemple, un masque de sous-réseau normalement utilisé avec l’adresse IP 131.107.16.200 correspond au nombre binaire de 32 bits suivant :

```
11111111 11111111 00000000 00000000
```

Ce numéro de masque de sous-réseau est formé de 16 bits de valeur 1, suivis de 16 bits de valeur zéro, indiquant que les sections ID de réseau et ID d'hôte de cette adresse IP ont toutes deux une longueur de 16 bits. Ce masque de sous-réseau est affiché en notation décimale séparée par des points sous la forme 255.255.0.0.

Le tableau ci-dessous indique les masques de sous-réseau des classes d'adresses Internet.

Agrandir le tableau

Classe Address	Bits du masque de sous-réseau	Masque de sous-réseau
Classe A	11111111 00000000 00000000 00000000	255.0.0.0
Classe B	11111111 11111111 00000000 00000000	255.255.0.0
Classe C	11111111 11111111 11111111 00000000	255.255.255.0

Lorsque vous créez une étendue dans DHCP et que vous entrez la plage d'adresses IP de cette étendue, DHCP fournit ces valeurs de masque de sous-réseau par défaut. Les valeurs de masque de sous-réseau par défaut conviennent généralement pour la plupart des réseaux qui ne nécessitent aucune configuration particulière et où chaque segment de réseau IP correspond au même réseau physique.

Dans d'autres cas, vous pourrez utiliser des masques de sous-réseau personnalisés pour implémenter la mise en sous-réseau IP. Dans le cadre de la mise en sous-réseau IP, vous pouvez subdiviser la partie ID d'hôte par défaut d'une adresse IP pour spécifier des sous-réseaux, qui sont des sous-divisions de l'ID de réseau basé sur la classe.

En personnalisant la longueur du masque de sous-réseau, vous pouvez réduire le nombre de bits utilisés pour l'ID d'hôte.

Pour éviter les problèmes d'adressage et de routage, vous devez veiller à ce que tous les ordinateurs TCP/IP d'un segment réseau utilisent le même masque de sous-réseau et que chaque ordinateur ou périphérique possède une adresse IP unique.

Planification des plages d'exclusion

Lorsque vous définissez une étendue sur un serveur DHCP, vous spécifiez une plage d'adresses IP qui inclut toutes les adresses IP que le serveur DHCP est autorisé à louer aux clients DHCP, tels que les ordinateurs et autres périphériques. Si, par la suite, vous configurez manuellement certains serveurs et autres périphériques avec des adresses IP statiques de la même plage d'adresses IP que le serveur DHCP utilise, vous risquez involontairement d'attribuer à un périphérique une adresse IP qui a déjà été attribuée à un autre périphérique par le serveur DHCP, et de générer ainsi un conflit d'adresse IP.

Vous pouvez éviter ce problème en créant une plage d'exclusion pour l'étendue DHCP. Une plage d'exclusion est une séquence d'adresses IP, au sein de la plage d'adresses IP de l'étendue, qui ne peuvent pas être utilisées par le serveur DHCP. Si vous créez une plage d'exclusion, le serveur DHCP ne peut attribuer aucune des adresses de cette plage. Vous pouvez alors attribuer manuellement ces adresses sans risque de générer un conflit d'adresse IP.

Vous pouvez exclure des adresses IP de la distribution par le serveur DHCP en créant une plage d'exclusion pour chaque étendue. Vous devez utiliser des exclusions pour tous les périphériques configurés avec une adresse IP statique. Dans les adresses exclues doivent figurer toutes les adresses IP que vous avez attribuées manuellement à d'autres serveurs DHCP, clients non DHCP, stations de travail sans disque ou clients de routage et d'accès à distance et clients PPP.

Il est recommandé de configurer votre plage d'exclusion avec des adresses supplémentaires afin de prendre en compte la croissance future du réseau. Le tableau suivant présente un exemple de plage d'exclusion pour une étendue définie avec une plage d'adresses IP de 10.0.0.1 à 10.0.0.254 et un masque de sous-réseau de 255.255.255.0.

Agrandir le tableau

Éléments de configuration	Exemples de valeurs
Adresse IP de début de la plage d'exclusion	10.0.0.1
Adresse IP de fin de la plage d'exclusion	10.0.0.25

Planification de la configuration TCP/IP statique

Certains périphériques, comme les routeurs, les serveurs DHCP et les serveurs DNS doivent être configurés avec une adresse IP statique. Par ailleurs, vous voudrez peut-être garantir que des périphériques supplémentaires, comme des imprimantes, disposent toujours de la même adresse IP. Dressez la liste des périphériques que vous souhaitez configurer de manière statique pour chaque sous-réseau, puis planifiez la plage d'exclusion que vous voulez utiliser sur le serveur DHCP pour faire en sorte que le serveur DHCP ne loue pas l'adresse IP d'un périphérique configuré de manière statique. Une plage d'exclusion est une séquence limitée d'adresses IP au sein d'une étendue, qui est exclue des offres du service DHCP. Les plages d'exclusion garantissent qu'aucune adresse figurant dans ces plages n'est offerte par le serveur aux clients DHCP sur votre réseau.

Par exemple, si la plage d'adresses IP d'un sous-réseau est 192.168.0.1 à 192.168.0.254 et que vous avez dix appareils que vous souhaitez configurer avec une adresse IP statique, vous

pouvez créer une plage d'exclusion pour la version 192.168.0. étendue *x* incluant dix adresses IP ou plus : 192.168.0.1 à 192.168.0.15.

Dans cet exemple, vous utilisez dix des adresses IP exclues pour configurer des serveurs et autres périphériques avec des adresses IP statiques. Il reste cinq adresses IP pour configurer de manière statique de nouveaux périphériques que vous voudrez peut-être ajouter plus tard. Avec cette plage d'exclusion, le serveur DHCP dispose d'un pool d'adresses allant de 192.168.0.16 à 192.168.0.254.

Le tableau suivant fournit des exemples d'éléments de configuration supplémentaires pour les services de domaine Active Directory et DNS :

Agrandir le tableau

Éléments de configuration	Exemples de valeurs
Liaisons de connexion réseau	Ethernet
Paramètres du serveur DNS	DC1.corp.contoso.com
Adresse IP du serveur DNS préféré	10.0.0.2
Valeurs d'étendue 1. Nom de l'étendue 2. Adresse IP de début 3. Adresse IP de fin 4. Masque de sous-réseau 5. Passerelle par défaut (facultatif) 6. Durée du bail	1. Sous-réseau principal 2. 10.0.0.1 3. 10.0.0.254 4. 255.255.255.0 5. 10.0.0.1 6. 8 jours
Mode d'opération du serveur DHCP IPv6	Non activé

Utilisation de ce guide dans un laboratoire de test

Vous pouvez utiliser ce guide pour déployer DHCP dans un laboratoire de test avant de déployer dans un environnement de production.

> **Notes**
>
> Si vous ne souhaitez pas déployer DHCP dans un laboratoire de test, vous pouvez passer à la section Déployer DHCP.

Les conditions requises pour votre laboratoire varient selon que vous utilisez des serveurs physiques ou des machines virtuelles et que vous utilisez un domaine Active Directory ou que

vous déployez un serveur DHCP autonome.

Vous pouvez utiliser les informations suivantes pour déterminer les ressources minimales dont vous avez besoin pour tester le déploiement DHCP à l'aide de ce guide.

Configuration requise du laboratoire de test avec des machines virtuelles

Pour déployer DHCP dans un laboratoire de test avec des machines virtuelles, vous avez besoin des ressources suivantes.

Pour le déploiement de domaine ou le déploiement autonome, vous avez besoin d'un serveur configuré en tant qu'hôte Hyper-V.

Déploiement de domaine

Ce déploiement nécessite un serveur physique, un commutateur virtuel, deux serveurs virtuels et un client virtuel :

Sur votre serveur physique, dans le Gestionnaire Hyper-V, créez les éléments suivants.

1. Un commutateur virtuel **interne** . Ne créez pas de commutateur virtuel **externe** , car si votre hôte Hyper-V se trouve sur un sous-réseau qui inclut un serveur DHCP, vos machines virtuelles de test recevront une adresse IP de votre serveur DHCP. En outre, le serveur DHCP de test que vous déployez peut affecter des adresses IP à d'autres ordinateurs sur le sous-réseau où l'hôte Hyper-V est installé.
2. Une machine virtuelle exécutant Windows Server 2016 configurée en tant que contrôleur de domaine avec Active Directory Domain Services connecté au commutateur virtuel interne que vous avez créé. Pour correspondre à ce guide, ce serveur doit avoir une adresse IP configurée statiquement de 10.0.0.2. Pour plus d'informations sur le déploiement d'AD DS, consultez la section **Déploiement de DC1** dans le Guide réseau principal de Windows Server 2016.
3. Une machine virtuelle exécutant Windows Server 2016 que vous allez configurer en tant que serveur DHCP à l'aide de ce guide et qui est connectée au commutateur virtuel interne que vous avez créé.
4. Une machine virtuelle exécutant un système d'exploitation client Windows connecté au commutateur virtuel interne que vous avez créé et que vous allez utiliser pour vérifier que votre serveur DHCP alloue dynamiquement des adresses IP et des options DHCP aux clients DHCP.

Déploiement de serveurs DHCP autonomes

Ce déploiement nécessite un serveur physique, un commutateur virtuel, un serveur virtuel et un client virtuel :

Sur votre serveur physique, dans le Gestionnaire Hyper-V, créez les éléments suivants.

1. Un commutateur virtuel **interne** . Ne créez pas de commutateur virtuel **externe** , car si votre hôte Hyper-V se trouve sur un sous-réseau qui inclut un serveur DHCP, vos machines virtuelles de test recevront une adresse IP de votre serveur DHCP. En outre, le serveur DHCP de test que vous déployez peut affecter des adresses IP à d'autres ordinateurs sur le sous-réseau où l'hôte Hyper-V est installé.
2. Une machine virtuelle exécutant Windows Server 2016 que vous allez configurer en tant que serveur DHCP à l'aide de ce guide et qui est connectée au commutateur virtuel interne que vous avez créé.
3. Une machine virtuelle exécutant un système d'exploitation client Windows connecté au commutateur virtuel interne que vous avez créé et que vous allez utiliser pour vérifier que votre serveur DHCP alloue dynamiquement des adresses IP et des options DHCP aux clients DHCP.

Configuration requise du laboratoire de test avec des serveurs physiques

Pour déployer DHCP dans un laboratoire de test avec des serveurs physiques, vous avez besoin des ressources suivantes.

Déploiement de domaine

Ce déploiement nécessite un hub ou un commutateur, deux serveurs physiques et un client physique :

1. Un hub Ethernet ou un commutateur auquel vous pouvez connecter les ordinateurs physiques avec des câbles Ethernet
2. Un ordinateur physique exécutant Windows Server 2016 configuré en tant que contrôleur de domaine avec Active Directory Domain Services. Pour correspondre à ce guide, ce serveur doit avoir une adresse IP configurée statiquement de 10.0.0.2. Pour plus d'informations sur le déploiement d'AD DS, consultez la section **Déploiement de DC1** dans le Guide réseau principal de Windows Server 2016.
3. Un ordinateur physique exécutant Windows Server 2016 que vous allez configurer en tant que serveur DHCP à l'aide de ce guide.
4. Un ordinateur physique exécutant un système d'exploitation client Windows que vous utiliserez pour vérifier que votre serveur DHCP alloue dynamiquement des adresses IP et des options DHCP aux clients DHCP.

> ⓘ **Notes**
>
> Si vous n'avez pas suffisamment de machines de test pour ce déploiement, vous pouvez utiliser une seule machine de test pour AD DS et DHCP. Toutefois, cette configuration n'est pas recommandée pour un environnement de production.

Déploiement de serveurs DHCP autonomes

Ce déploiement nécessite un hub ou un commutateur, un serveur physique et un client physique :

1. Un hub Ethernet ou un commutateur auquel vous pouvez connecter les ordinateurs physiques avec des câbles Ethernet
2. Un ordinateur physique exécutant Windows Server 2016 que vous allez configurer en tant que serveur DHCP à l'aide de ce guide.
3. Un ordinateur physique exécutant un système d'exploitation client Windows que vous utiliserez pour vérifier que votre serveur DHCP alloue dynamiquement des adresses IP et des options DHCP aux clients DHCP.

Déployer DHCP

Cette section fournit des exemples de commandes Windows PowerShell que vous pouvez utiliser pour déployer DHCP sur un serveur. Avant d'exécuter ces exemples de commandes sur votre serveur, vous devez modifier les commandes pour qu'elles correspondent à votre réseau et à votre environnement.

Par exemple, avant d'exécuter les commandes, vous devez remplacer les exemples de valeurs dans les commandes pour les éléments suivants :

- Noms d'ordinateur
- Plage d'adresses IP pour chaque étendue que vous souhaitez configurer (1 étendue par sous-réseau)
- Masque de sous-réseau pour chaque plage d'adresses IP que vous souhaitez configurer
- Nom de l'étendue pour chaque étendue
- Plage d'exclusion pour chaque étendue
- Valeurs d'option DHCP, telles que la passerelle par défaut, le nom de domaine et les serveurs DNS ou WINS
- Noms d'interface

> ⓘ **Important**

Examinez et modifiez chaque commande de votre environnement avant d'exécuter la commande.

Où installer DHCP, sur un ordinateur physique ou une machine virtuelle ?

Vous pouvez installer le rôle serveur DHCP sur un ordinateur physique ou sur une machine virtuelle installée sur un hôte Hyper-V. Si vous installez DHCP sur une machine virtuelle et que vous souhaitez que le serveur DHCP fournisse des attributions d'adresses IP aux ordinateurs sur le réseau physique auquel l'hôte Hyper-V est connecté, vous devez connecter la carte réseau virtuelle de la machine virtuelle à un commutateur virtuel Hyper-V **externe**.

Pour plus d'informations, consultez la section **Créer un commutateur virtuel avec le Gestionnaire Hyper-V** dans la rubrique Créer un réseau virtuel.

Exécutez Windows PowerShell en tant qu'administrateur

Vous pouvez utiliser la procédure suivante pour exécuter Windows PowerShell avec des privilèges d'administrateur.

1. Sur un ordinateur exécutant Windows Server 2016, cliquez sur **Démarrer**, puis cliquez avec le bouton droit sur l'icône Windows PowerShell. Un menu s'affiche.
2. Dans le menu, cliquez sur **Plus**, puis sur **Exécuter en tant qu'administrateur**. Si vous y êtes invité, tapez les informations d'identification d'un compte disposant de privilèges d'administrateur sur l'ordinateur. Si le compte d'utilisateur avec lequel vous êtes connecté à l'ordinateur est un compte de niveau administrateur, vous ne recevrez pas d'invite d'informations d'identification.
3. Windows PowerShell s'ouvre avec des privilèges d'administrateur.

Renommer le serveur DHCP et configurer une adresse IP statique

Si ce n'est déjà fait, vous pouvez utiliser les commandes Windows PowerShell suivantes pour renommer le serveur DHCP et configurer une adresse IP statique pour le serveur.

Configurer une adresse IP statique

Vous pouvez utiliser les commandes suivantes pour affecter une adresse IP statique au serveur DHCP et configurer les propriétés TCP/IP du serveur DHCP avec l'adresse IP du serveur DNS

correcte. Remplacez les noms d'interface et les adresses IP utilisés dans cet exemple par les valeurs de configuration souhaitées pour votre ordinateur.

```
New-NetIPAddress -IPAddress 10.0.0.3 -InterfaceAlias "Ethernet" -DefaultGateway
10.0.0.1 -AddressFamily IPv4 -PrefixLength 24
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.2
```

Pour plus d'informations sur ces commandes FTP, consultez les rubriques suivantes.

- New-NetIPAddress
- Set-DnsClientServerAddress

Renommer l'ordinateur

Vous pouvez utiliser les commandes suivantes pour renommer puis redémarrer l'ordinateur.

```
Rename-Computer -Name DHCP1
Restart-Computer
```

Pour plus d'informations sur ces commandes FTP, consultez les rubriques suivantes.

- Rename-Computer
- Restart-Computer

Joignez l'ordinateur au domaine (facultatif)

Si vous installez votre serveur DHCP dans un environnement de domaine Active Directory, vous devez joindre l'ordinateur au domaine. Ouvrez Windows PowerShell avec des privilèges d'administrateur, puis exécutez la commande suivante après avoir remplacé le nom NetBios du domaine **CORP** par une valeur appropriée pour votre environnement.

```
Add-Computer CORP
```

Lorsque vous y êtes invité.e, tapez les identifiants pour un compte d'utilisateur de domaine disposant de l'autorisation pour joindre un ordinateur au domaine.

```
Restart-Computer
```

Pour plus d'informations sur la commande Add-Computer, consultez la rubrique suivante.

- Add-Computer

Installer DHCP

Une fois l'ordinateur redémarré, ouvrez Windows PowerShell avec des privilèges d'administrateur, puis installez DHCP en exécutant la commande suivante.

```
Install-WindowsFeature DHCP -IncludeManagementTools
```

Pour plus d'informations sur cette commande, consultez la rubrique suivante.

- Install-WindowsFeature

Créer des groupes de sécurité DHCP

Pour créer des groupes de sécurité, vous devez exécuter une commande Network Shell (netsh) dans Windows PowerShell, puis redémarrer le service DHCP, afin que les nouveaux groupes deviennent actifs.

Lorsque vous exécutez la commande netsh suivante sur le serveur DHCP, les **administrateurs DHCP** et les groupes de sécurité **utilisateurs DHCP** sont créés dans **les utilisateurs et groupes locaux** sur le serveur DHCP.

```
netsh dhcp add securitygroups
```

La commande suivante redémarre le service DHCP sur l'ordinateur local.

```
Restart-Service dhcpserver
```

Pour plus d'informations sur ces commandes FTP, consultez les rubriques suivantes.

- Interpréteur de commande réseau (Netsh)

- Restart-Service

Autoriser le serveur DHCP dans Active Directory (facultatif)

Si vous installez DHCP dans un environnement de domaine, vous devez effectuer les étapes suivantes pour autoriser le serveur DHCP à fonctionner dans le domaine.

> ⓘ **Notes**
>
> Les serveurs DHCP non autorisés installés dans les domaines Active Directory ne peuvent pas fonctionner correctement et ne louent pas d'adresses IP aux clients DHCP. La désactivation automatique des serveurs DHCP non autorisés est une fonctionnalité de sécurité qui empêche les serveurs DHCP non autorisés d'attribuer des adresses IP incorrectes aux clients de votre réseau.

Vous pouvez utiliser la commande suivante pour ajouter le serveur DHCP à la liste des serveurs DHCP autorisés dans Active Directory.

> ⓘ **Notes**
>
> Si vous n'avez pas d'environnement de domaine, n'exécutez pas cette commande.

```
Add-DhcpServerInDC -DnsName DHCP1.corp.contoso.com -IPAddress 10.0.0.3
```

Pour vérifier que le serveur DHCP est autorisé dans Active Directory, vous pouvez utiliser la commande suivante.

```
Get-DhcpServerInDC
```

Voici des exemples de résultats affichés dans Windows PowerShell.

```
IPAddress   DnsName
---------   -------
10.0.0.3    DHCP1.corp.contoso.com
```

Pour plus d'informations sur ces commandes FTP, consultez les rubriques suivantes.

- Add-DhcpServerInDC
- Get-DhcpServerInDC

Notifier le Gestionnaire de serveur que la configuration DHCP post-installation est terminée (facultatif)

Une fois que vous avez effectué des tâches post-installation, telles que la création de groupes de sécurité et l'autorisation du serveur DHCP dans Active Directory, le Gestionnaire de serveur peut toujours afficher une alerte dans l'interface utilisateur indiquant que les étapes post-installation doivent être effectuées à l'aide de l'Assistant Configuration post-installation DHCP.

Vous pouvez empêcher l'affichage de ce message désormais inutile et incorrect dans le Gestionnaire de serveur en configurant la clé de registre suivante à l'aide de cette commande Windows PowerShell.

```
Set-ItemProperty –Path
registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 –Name
ConfigurationState –Value 2
```

Pour plus d'informations sur cette commande, consultez la rubrique suivante.

- Set-ItemProperty

Définir les paramètres de configuration de mise à jour dynamique DNS au niveau du serveur (facultatif)

Si vous souhaitez que le serveur DHCP effectue des mises à jour dynamiques DNS pour les ordinateurs clients DHCP, vous pouvez exécuter la commande suivante pour configurer ce paramètre. Il s'agit d'un paramètre au niveau du serveur, et non d'un paramètre de niveau d'étendue. Il affecte donc toutes les étendues que vous configurez sur le serveur. Cet exemple de commande configure également le serveur DHCP pour supprimer les enregistrements de ressources DNS pour les clients lorsque le client expire le moins.

```
Set-DhcpServerv4DnsSetting -ComputerName "DHCP1.corp.contoso.com" -DynamicUpdates
"Always" -DeleteDnsRRonLeaseExpiry $True
```

Vous pouvez utiliser la commande suivante pour configurer les informations d'identification utilisées par le serveur DHCP pour inscrire ou annuler l'inscription des enregistrements clients sur un serveur DNS. Cet exemple enregistre des informations d'identification sur un serveur DHCP. La première commande utilise **Get-Credential** pour créer un objet **PSCredential** , puis stocke l'objet dans la variable **$Credential** . La commande vous invite à entrer un nom d'utilisateur et un mot de passe. Assurez-vous donc de fournir les informations d'identification d'un compte qui est autorisé à mettre à jour les enregistrements de ressources sur votre serveur DNS.

```
$Credential = Get-Credential
Set-DhcpServerDnsCredential -Credential $Credential -ComputerName
"DHCP1.corp.contoso.com"
```

Pour plus d'informations sur ces commandes FTP, consultez les rubriques suivantes.

- Set-DhcpServerv4DnsSetting
- Set-DhcpServerDnsCredential

Configurer l'étendue Corpnet

Une fois l'installation DHCP terminée, vous pouvez utiliser les commandes suivantes pour configurer et activer l'étendue Corpnet, créer une plage d'exclusion pour l'étendue et configurer la passerelle par défaut des options DHCP, l'adresse IP du serveur DNS et le nom de domaine DNS.

```
Add-DhcpServerv4Scope -name "Corpnet" -StartRange 10.0.0.1 -EndRange 10.0.0.254 -
SubnetMask 255.255.255.0 -State Active
Add-DhcpServerv4ExclusionRange -ScopeID 10.0.0.0 -StartRange 10.0.0.1 -EndRange
10.0.0.15
Set-DhcpServerv4OptionValue -OptionID 3 -Value 10.0.0.1 -ScopeID 10.0.0.0 -
ComputerName DHCP1.corp.contoso.com
Set-DhcpServerv4OptionValue -DnsDomain corp.contoso.com -DnsServer 10.0.0.2
```

Pour plus d'informations sur ces commandes FTP, consultez les rubriques suivantes.

- Add-DhcpServerv4Scope
- Add-DhcpServerv4ExclusionRange
- Set-DhcpServerv4OptionValue

Configurer l'étendue Corpnet2 (facultatif)

Si vous avez un deuxième sous-réseau connecté au premier sous-réseau avec un routeur où le transfert DHCP est activé, vous pouvez utiliser les commandes suivantes pour ajouter une deuxième étendue, nommée Corpnet2 pour cet exemple. Cet exemple configure également une plage d'exclusion et l'adresse IP pour la passerelle par défaut (l'adresse IP du routeur sur le sous-réseau) du sous-réseau Corpnet2.

```
Add-DhcpServerv4Scope -name "Corpnet2" -StartRange 10.0.1.1 -EndRange 10.0.1.254 -
SubnetMask 255.255.255.0 -State Active
Add-DhcpServerv4ExclusionRange -ScopeID 10.0.1.0 -StartRange 10.0.1.1 -EndRange
10.0.1.15
Set-DhcpServerv4OptionValue -OptionID 3 -Value 10.0.1.1 -ScopeID 10.0.1.0 -
ComputerName DHCP1.corp.contoso.com
```

Si vous avez des sous-réseaux supplémentaires qui sont mis en service par ce serveur DHCP, vous pouvez répéter ces commandes, en utilisant des valeurs différentes pour tous les paramètres de commande, pour ajouter des étendues pour chaque sous-réseau.

> **Important**
>
> Assurez-vous que tous les routeurs entre vos clients DHCP et votre serveur DHCP sont configurés pour le transfert de messages DHCP. Pour plus d'informations sur la configuration du transfert DHCP, consultez la documentation de votre routeur.

Vérifier la fonctionnalité du serveur

Pour vérifier que votre serveur DHCP fournit une allocation dynamique d'adresses IP aux clients DHCP, vous pouvez connecter un autre ordinateur à un sous-réseau avec service. Une fois que vous avez connecté le câble Ethernet à la carte réseau et mis sous tension l'ordinateur, il demande une adresse IP à votre serveur DHCP. Vous pouvez vérifier la configuration réussie à l'aide de la commande **ipconfig /all** et examiner les résultats, ou en effectuant des tests de connectivité, tels que la tentative d'accès aux ressources Web avec votre navigateur ou partages de fichiers avec l'Explorateur Windows ou d'autres applications.

Si le client ne reçoit pas d'adresse IP de votre serveur DHCP, effectuez les étapes de dépannage suivantes.

1. Vérifiez que le câble Ethernet est branché à la fois à l'ordinateur et au commutateur Ethernet, au hub ou au routeur.
2. Si vous avez branché l'ordinateur client à un segment réseau séparé du serveur DHCP par un routeur, vérifiez que le routeur est configuré pour transférer les messages DHCP.

3. Vérifiez que le serveur DHCP est autorisé dans Active Directory en exécutant la commande suivante pour récupérer la liste des serveurs DHCP autorisés à partir d'Active Directory. Get-DhcpServerInDC.
4. Vérifiez que vos étendues sont activées en ouvrant la console DHCP (Gestionnaire de serveur, **Outils**, **DHCP**), en développant l'arborescence du serveur pour passer en revue les étendues, puis en cliquant avec le bouton droit sur chaque étendue. Si le menu résultant inclut la sélection **Activer**, cliquez sur **Activer**. (Si l'étendue est déjà activée, la sélection de menu lit **Désactiver**.)

Commandes Windows PowerShell pour DHCP

La référence suivante fournit des descriptions de commandes et une syntaxe pour toutes les commandes de serveur DHCP Windows PowerShell pour Windows Server 2016. La rubrique répertorie les commandes par ordre alphabétique en fonction du verbe au début des commandes, telles que **Get** ou **Set**.

> ⓘ **Notes**
>
> Vous ne pouvez pas utiliser Windows Server 2016 commandes dans Windows Server 2012 R2.

- DhcpServer Module

La référence suivante fournit des descriptions de commandes et une syntaxe pour toutes les commandes de serveur DHCP Windows PowerShell pour Windows Server 2012 R2. La rubrique répertorie les commandes par ordre alphabétique en fonction du verbe au début des commandes, telles que **Get** ou **Set**.

> ⓘ **Notes**
>
> Vous pouvez utiliser Windows Server 2012 commandes dans Windows Server 2016 R2.

- Applets de commande du serveur DHCP dans Windows PowerShell

Liste des commandes Windows PowerShell dans ce guide

Voici une liste simple de commandes et d'exemples de valeurs utilisés dans ce guide.

```
New-NetIPAddress -IPAddress 10.0.0.3 -InterfaceAlias "Ethernet" -DefaultGateway
10.0.0.1 -AddressFamily IPv4 -PrefixLength 24
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.2
Rename-Computer -Name DHCP1
Restart-Computer

Add-Computer CORP
Restart-Computer

Install-WindowsFeature DHCP -IncludeManagementTools
netsh dhcp add securitygroups
Restart-Service dhcpserver

Add-DhcpServerInDC -DnsName DHCP1.corp.contoso.com -IPAddress 10.0.0.3
Get-DhcpServerInDC

Set-ItemProperty –Path
registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 –Name
ConfigurationState –Value 2

Set-DhcpServerv4DnsSetting -ComputerName "DHCP1.corp.contoso.com" -DynamicUpdates
"Always" -DeleteDnsRRonLeaseExpiry $True

$Credential = Get-Credential
Set-DhcpServerDnsCredential -Credential $Credential -ComputerName
"DHCP1.corp.contoso.com"

rem At prompt, supply credential in form DOMAIN\user, password

rem Configure scope Corpnet
Add-DhcpServerv4Scope -name "Corpnet" -StartRange 10.0.0.1 -EndRange 10.0.0.254 -
SubnetMask 255.255.255.0 -State Active
Add-DhcpServerv4ExclusionRange -ScopeID 10.0.0.0 -StartRange 10.0.0.1 -EndRange
10.0.0.15
Set-DhcpServerv4OptionValue -OptionID 3 -Value 10.0.0.1 -ScopeID 10.0.0.0 -
ComputerName DHCP1.corp.contoso.com
Set-DhcpServerv4OptionValue -DnsDomain corp.contoso.com -DnsServer 10.0.0.2

rem Configure scope Corpnet2
Add-DhcpServerv4Scope -name "Corpnet2" -StartRange 10.0.1.1 -EndRange 10.0.1.254 -
SubnetMask 255.255.255.0 -State Active
Add-DhcpServerv4ExclusionRange -ScopeID 10.0.1.0 -StartRange 10.0.1.1 -EndRange
10.0.1.15
Set-DhcpServerv4OptionValue -OptionID 3 -Value 10.0.1.1 -ScopeID 10.0.1.0 -
ComputerName DHCP1.corp.contoso.com
```

Installer un agent de relais DHCP

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cet article explique comment installer et configurer un agent de relais du protocole DHCP (Dynamic Host Configuration Protocol) sur un ordinateur exécutant Windows Server. Un agent de relais DHCP fonctionne en tant qu'intermédiaire entre les clients DHCP et les serveurs DHCP qui ne se trouvent pas sur le même sous-réseau ou sur le même réseau local. L'agent de relais DHCP transfère les messages de diffusion DHCP des clients vers un serveur distant, ce qui permet aux clients d'obtenir des adresses IP et d'autres informations de configuration réseau depuis un serveur DHCP situé sur un autre sous-réseau.

Pour installer l'agent de relais DHCP sur Windows Server, vous devez déployer le rôle serveur *d'accès à distance* . L'agent de relais DHCP est une fonctionnalité de l'accès à distance et n'est pas inclus dans le rôle serveur DHCP.

Prerequisites

Avant de pouvoir installer votre agent de relais DHCP, vous devez disposer des éléments suivants :

- Un ordinateur exécutant Windows Server sur le sous-réseau distant où vous souhaitez installer l'agent de relais DHCP.
- Un serveur DHCP avec une étendue DHCP configurée pour le sous-réseau distant.

Installer et configurer le rôle serveur

Voici la procédure à suivre pour installer et configurer le routage LAN dans le cadre du rôle serveur Accès à distance depuis le bureau Windows.

1. Connectez-vous à l'ordinateur sur lequel vous souhaitez installer l'agent de relais DHCP, puis ouvrez le **Gestionnaire de serveur**.

2. Dans la console Gestionnaire de serveur, sélectionnez **Ajouter des rôles et des fonctionnalités**.

3. Dans le menu **Ajouter des rôles et des fonctionnalités**, sélectionnez **Suivant** jusqu'à atteindre la page **Rôles serveur**.

4. Développez le rôle **d'accès à distance** en cochant la case ou la flèche associée.

5. Dans **Services de rôle**, sélectionnez **Routage**, puis **Ajoutez des fonctionnalités** lorsque vous y êtes invité.

6. Sélectionnez **Suivant** jusqu'à atteindre la page **Confirmer les sélections d'installation** .

7. Sélectionnez **Installer** pour commencer l'installation. Une fois l'installation terminée, sélectionnez **Ouvrir l'Assistant Prise en main**.

8. Dans la console MMC (Microsoft Management Console) de routage et d'accès à distance, cliquez avec le bouton droit de la souris sur le serveur, puis sélectionnez *Configurer et activer le routage et l'accès à distance* pour ouvrir l'Assistant Installation du serveur de routage et d'accès à distance.

9. Dans l'Assistant Bienvenue dans l'Assistant Installation du serveur de routage et d'accès à distance, sélectionnez **Suivant**.

10. Dans **Configuration**, sélectionnez *routage LAN*, puis sélectionnez **Suivant**.

11. Dans **Configuration personnalisée**, sélectionnez *l'accès VPN*, puis sélectionnez **Suivant** pour ouvrir l'Assistant Exécution de l'Assistant Routage et Installation du serveur d'accès à distance.

12. Sélectionnez **Terminer** pour fermer l'Assistant, puis **Démarrer le service** lorsque vous y êtes invité.

Configurer l'agent de relais DHCP

Voici la procédure à suivre pour installer le rôle Agent de relais DHCP depuis la console MMC de routage et d'accès à distance.

1. Dans le volet gauche, développez le nom du serveur, puis cliquez avec le bouton droit sur **Général** sous **IPv4** ou **IPv6**, puis sélectionnez **Nouveau protocole de routage**.

2. Dans le volet de gauche, cliquez avec le bouton droit sur **Agent de relais DHCP** sous **IPv4** ou **IPv6**, puis sélectionnez **Nouvelle interface**.

3. Sélectionnez l'interface réseau que vous souhaitez utiliser pour l'agent de relais DHCP. Cliquez sur **OK**.

4. Dans le volet de gauche, cliquez avec le bouton droit sur **Agent de relais DHCP** sous **IPv4** ou **IPv6**, puis sélectionnez **Propriétés**.

5. Entrez l'adresse IP du serveur DHCP auquel vous souhaitez relayer les requêtes DHCP, puis sélectionnez **Ajouter**.

6. Sélectionnez **OK** pour enregistrer vos paramètres.

L'agent de relais DHCP est désormais installé et configuré sur votre serveur Windows.

Étapes suivantes

- Principes de base DHCP
- Options de sélection de sous-réseau DHCP

Migrer une installation de serveur DHCP vers un autre serveur Windows Server

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

La migration du serveur DHCP implique le déplacement des paramètres de votre serveur DHCP existant vers un nouveau serveur DHCP sur le réseau. L'objectif de cette migration de serveur est d'installer le rôle serveur DHCP sur le système d'exploitation Windows Server afin qu'il fournit des baux DHCP sur un réseau sans aucune modification perceptible sur les ordinateurs clients DHCP.

Ce guide décrit les étapes de migration des paramètres de serveur DHCP existants vers un serveur exécutant Windows Server. À l'aide de ce guide pour migrer un serveur DHCP, vous pouvez simplifier la migration, réduire le temps de migration, augmenter la précision du processus de migration et éliminer les conflits possibles susceptibles d'avoir lieu lors de la migration DHCP. Ce guide ne contient pas d'instructions pour la migration lorsque le serveur source exécute plusieurs rôles. Si votre serveur exécute plusieurs rôles, nous vous recommandons de concevoir une procédure de migration personnalisée spécifique à votre environnement serveur. Quelques notes sur la migration :

- Les migrations entre les systèmes d'exploitation physiques et les systèmes d'exploitation virtuels sont prises en charge.
- La migration d'un serveur source vers un serveur de destination exécutant un système d'exploitation dans un autre langage d'interface utilisateur système que le serveur source n'est pas pris en charge.
- La migration est recommandée au lieu d'une mise à niveau même si le matériel est natif x64.

Ce guide est destiné aux administrateurs informatiques, aux professionnels de l'informatique et à d'autres travailleurs des connaissances responsables de l'opération et du déploiement de serveurs DHCP dans un environnement managé. L'administrateur du serveur peut choisir les composants d'une installation existante à migrer. Avec le rôle serveur, ces composants incluent généralement la configuration, les données, l'identité système et les paramètres du système d'exploitation.

Prerequisites

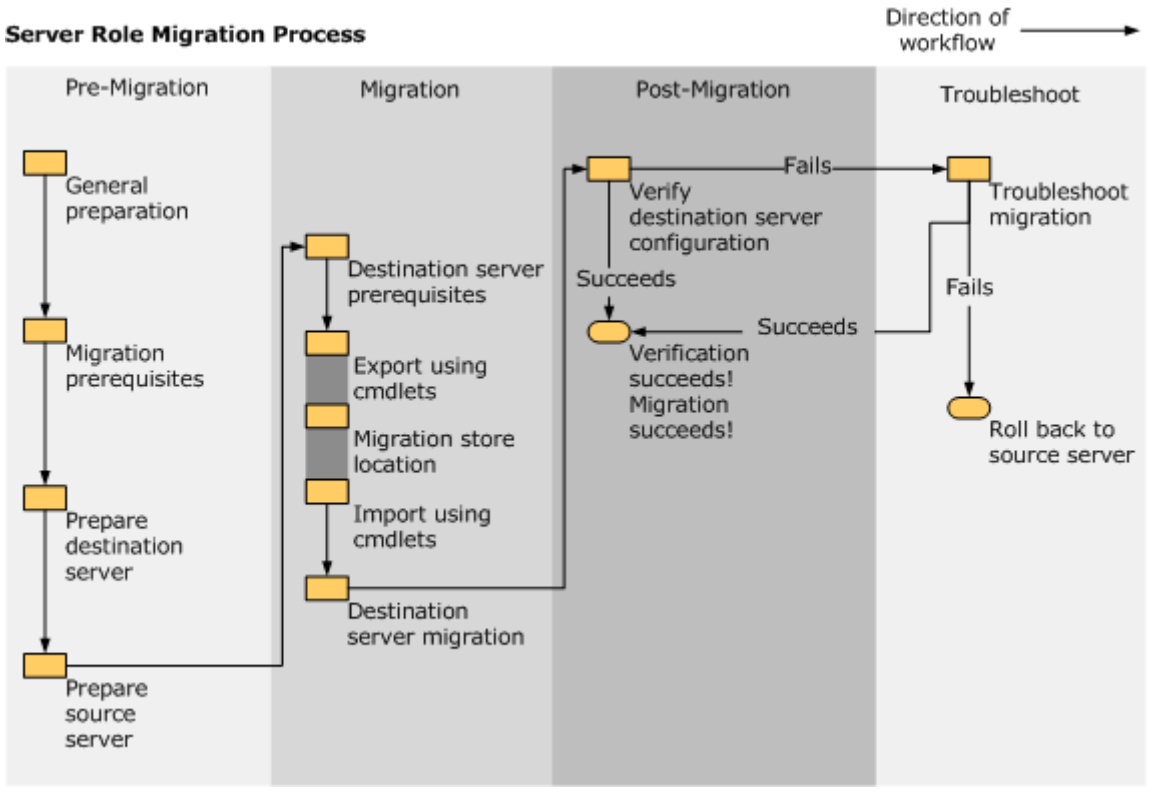
- Un serveur DHCP existant configuré et en cours d'exécution

- Les autorisations suivantes sont requises sur le serveur source et sur le serveur de destination :
  - Droits d'administration de domaine requis pour autoriser le serveur DHCP.
  - Les droits d'administration locaux sont requis pour installer ou gérer le serveur DHCP.
  - Des autorisations en écriture sont requises sur l'emplacement du magasin de migration.

Processus de migration de serveur

La migration du serveur DHCP est divisée en sections principales suivantes :

- Préparer la migration : le processus de prémigration implique la collecte manuelle de données, suivie des étapes de préparation des serveurs sources et de destination.
- Migrer le rôle serveur DHCP : le processus de migration inclut des procédures de serveur source et de destination qui utilisent les applets de commande Export et Import pour collecter, stocker et migrer automatiquement les paramètres du rôle serveur.
- Vérifiez la migration : vérifiez que le serveur de destination a correctement remplacé le serveur source.
- Effectuer des tâches post-migration : Mettre hors service ou réutiliser le serveur source. Résolvez les problèmes de migration en cas d'échec et revenez en arrière si nécessaire.



Préparer la migration

- **Identifiez vos serveurs source et de destination DHCP.**

- **Déterminez le domaine, le nom du serveur et les mots de passe sur le serveur source.** Pour identifier le domaine du serveur d'origine, affichez les paramètres système à partir du Panneau de configuration.
- **Avant la migration, installez toutes les mises à jour critiques et service packs sur le serveur source.** Il est recommandé d'installer toutes les mises à jour critiques actuelles et les Service Packs sur les serveurs source et de destination.
- **Comptez le nombre de cartes réseau dans les serveurs source et de destination et assurez-vous qu'elles sont égales en nombre.** Si le serveur source qui exécute le serveur DHCP a plusieurs cartes réseau et que le service DHCP est lié à toutes ces cartes et sert des adresses IP sur différents sous-réseaux, le serveur de destination qui exécute le serveur DHCP doit également avoir plusieurs cartes réseau afin de pouvoir desservir les mêmes sous-réseaux que le serveur source.
- **Préparez un emplacement pour le fichier de stockage de migration.** L'emplacement du magasin doit être accessible à partir du serveur source pendant l'exportation et à partir du serveur de destination pendant l'importation. Utilisez un lecteur commun qui peut contenir toutes les informations relatives au serveur DHCP à partir du serveur source. L'emplacement de stockage doit être similaire à ce qui suit : \\fileserver\users\username\.

Installer les outils de migration

Si ce n'est déjà fait, installez Les outils de migration Windows Server sur les serveurs de destination et sources. Les outils de migration peuvent être installés à l'aide de PowerShell ou du Gestionnaire de serveur.

Pour PowerShell, utilisez l'applet de commande Install-WindowsFeature :

PowerShell

```
Install-WindowsFeature -Name Migration -ComputerName Server1
```

Utilisez le Gestionnaire de serveur et ouvrez l'Assistant Ajout de rôles et de fonctionnalités. Recherchez et installez la fonctionnalité : **Outils de migration Windows Server**.

Préparer le serveur de destination

Pour installer le serveur DHCP sur le serveur de destination, effectuez le processus d'installation piloté par le menu. Effectuez la procédure suivante pour préparer le serveur de destination.

Pour préparer le serveur de destination

1. Installez Windows Server et configurez le serveur de destination.

2. Assurez-vous qu'il existe suffisamment d'espace disque pour stocker la base de données du serveur DHCP. L'espace disque nécessaire varie selon chaque installation et doit être égal ou supérieur à l'espace de la base de données du serveur DHCP.

3. Ajoutez le serveur de destination en tant que serveur membre dans le domaine du serveur source en cours de remplacement.

4. Vérifiez que le serveur de destination peut résoudre les noms des utilisateurs de domaine membres du groupe local pendant l'opération d'importation. Si les serveurs source et de destination se trouvent dans différents domaines, le serveur de destination doit être en mesure de contacter un serveur de catalogue global pour la forêt dans laquelle se trouvent les comptes d'utilisateur de domaine source.

5. Sur un ordinateur exécutant Windows Server, ouvrez Windows PowerShell en tant qu'administrateur.

6. Chargez le module Gestionnaire de serveur dans votre session Windows PowerShell. Pour charger le module Gestionnaire de serveur, entrez la commande :

   PowerShell

   ```
   Import-Module -Name ServerManager
   ```

   Notes

   Il n'est pas obligatoire que le serveur DHCP soit installé sur le serveur de destination avant d'importer les paramètres. Si le rôle n'est pas installé sur le serveur de destination, il est installé automatiquement pendant le processus d'importation. Toutefois, étant donné que l'installation du rôle pendant l'importation peut prolonger le temps d'arrêt, nous vous recommandons d'installer le serveur DHCP à l'aide de la console du Gestionnaire de serveur sur le serveur de destination dans le cadre de votre préparation à la migration.

7. Sur le serveur de destination, pour installer le serveur DHCP, exécutez la commande suivante :

   PowerShell

   ```
   Install-WindowsFeature -Name DHCP
   ```

Vous pouvez également installer manuellement le serveur DHCP à l'aide du Gestionnaire de serveur. Pour plus d'informations, consultez Installer et configurer le serveur DHCP.

1. À la fin du processus de migration, le serveur de destination doit avoir une adresse IP statique. Bien que vous ne modifiez pas l'adresse IP du serveur de destination maintenant, tenez compte des scénarios suivants en vue de la modifier lorsque la migration est terminée.

   - Si votre scénario de migration nécessite que vous désaffectiez et déconnectez le serveur source du réseau, vous pouvez uniquement rendre l'adresse IP sur le serveur de destination identique à l'adresse IP sur le serveur source. Le serveur source doit être déconnecté du réseau ou arrêté afin qu'il n'y ait aucun conflit d'adresse IP entre le serveur source et le serveur de destination. Toutefois, le serveur de destination peut toujours servir les clients qui recherchent le serveur hérité (source) qui exécutait le serveur DHCP.

   - Si votre scénario de migration appelle la poursuite de l'exécution du serveur source sur le réseau à d'autres fins non DHCP, vous devez affecter au serveur de destination une adresse IP non allouée dans le même sous-réseau que le serveur source pour éviter les conflits d'adresses IP.

   - Les clients du serveur DHCP qui tentent de renouveler un bail d'adresse IP envoient la demande de renouvellement à l'adresse IP précédente du serveur DHCP. Si le serveur source a été désactivé, puis déconnecté du réseau et que le nouveau serveur de destination DHCP fonctionne avec une adresse IP différente, cette requête échoue initialement en raison de l'adresse IP modifiée. Toutefois, les clients essaient de redécouvrir l'adresse IP du serveur DHCP sur le réseau et par conséquent de récupérer à partir de cette défaillance temporaire.

   > ⚠ **Avertissement**
   >
   > Si le serveur source exécute plusieurs rôles, le changement de nom du serveur source ou la modification de son adresse IP peut entraîner l'échec d'autres rôles qui s'exécutent sur le serveur source.

2. Si le chemin d'accès à la base de données du serveur DHCP ne correspond pas au chemin d'accès par défaut, vous devez vous assurer que le serveur de destination possède un disque avec la même lettre de lecteur que celle affichée dans le chemin de base de données du serveur DHCP du serveur source.

Le serveur de destination est maintenant préparé pour la migration.

Préparer le serveur source

Suivez ces étapes pour préparer le serveur source pour la migration.

1. Sauvegardez le serveur source. La sauvegarde doit être une sauvegarde spécifique au serveur DHCP, et non une sauvegarde Windows. (Une sauvegarde Windows sauvegarde le système d'exploitation complet.) Vous pouvez créer la sauvegarde spécifique au serveur DHCP à l'aide de l'outil en ligne de commande Netsh ou de la console MMC (Microsoft Management Console).

2. S'il est en cours d'exécution, arrêtez le service serveur DHCP. Dans une session ouverte comme décrit à l'étape 5 de la préparation du serveur de destination, entrez :

   PowerShell

   ```
   Stop-Service -Name "DHCPserver"
   ```

3. Si le chemin d'accès à la base de données du serveur DHCP ne correspond pas au chemin d'accès par défaut, vérifiez que le serveur de destination a un disque avec la même lettre de lecteur que dans le chemin de base de données du serveur DHCP du serveur source.

Vous êtes maintenant prêt à commencer la migration du serveur DHCP.

Migrer le rôle serveur DHCP

Dans cette section, vous allez migrer le serveur DHCP vers le serveur de destination à partir du serveur source. L'appartenance aux administrateurs de domaine ou équivalente est la condition minimale requise pour effectuer ces procédures.

Migrer le serveur DHCP vers le serveur de destination

1. S'il n'est pas déjà installé, installez le serveur DHCP sur le serveur de destination.

2. Si elle est en cours d'exécution, arrêtez le service serveur DHCP en exécutant la commande suivante :

   PowerShell

   ```
   Stop-Service -Name "DHCPserver"
   ```

Migrer le serveur DHCP à partir du serveur source

Suivez les étapes de cette section pour migrer le serveur DHCP à partir du serveur source.

> ⓘ **Important**
>
> Avant d'exécuter les applets de commande **Import-SmigServerSetting, Export-SmigServerSetting** ou **Get-SmigServerFeature**, vérifiez qu'au cours de la migration, les serveurs source et de destination peuvent contacter le contrôleur de domaine associé aux utilisateurs ou groupes de domaine qui sont membres de groupes locaux sur le serveur source. Avant d'exécuter les applets de commande **Send-SmigServerData** ou **Receive-SmigServerData** , vérifiez qu'au cours de la migration, les serveurs source et de destination peuvent contacter le contrôleur de domaine associé à ces utilisateurs de domaine qui possèdent des fichiers ou des partages en cours de migration.

1. Sur un ordinateur exécutant Windows Server, ouvrez Windows PowerShell en tant qu'administrateur.

2. Chargez les outils de migration Windows Server dans votre session.

   Si vous avez ouvert la session active à l'aide du raccourci Outils de migration Windows Server dans le menu **Démarrer** , ignorez cette étape et passez à l'étape 3. Chargez uniquement le composant logiciel enfichable Outils de migration de Windows Server dans une session ouverte d'une autre façon, et dans laquelle ce composant logiciel enfichable n'est pas déjà chargé. Pour charger les outils de migration Windows Server, tapez ce qui suit, puis **appuyez sur Entrée**.

   PowerShell
   ```
   Add-PSSnapin Microsoft.Windows.ServerManager.Migration
   ```

3. Collectez des données à partir du serveur source en exécutant l'applet de commande **Export-SmigServerSetting** en tant qu'administrateur. Les paramètres d'applet de commande **Export-SmigServerSetting** peuvent collecter toutes les données de serveur DHCP sources dans un seul fichier (Svrmig.mig). Ou l'applet de commande **Export-SmigServerSetting** peut être exécutée plusieurs fois, chaque itération utilisant un ou plusieurs paramètres pour collecter et stocker des données dans plusieurs fichiers Svrmig.mig. Avant d'exécuter cette commande, passez en revue les éléments suivants :

   - Lorsque vous exécutez la commande à l'étape 4, vous êtes invité à fournir un mot de passe pour chiffrer les données du magasin de migration. Vous devez fournir ce même mot de passe au moment de l'importation à partir du magasin de migration.

- Le paramètre **de chemin d'accès** peut être un répertoire vide ou aucunmpty. Le fichier de données réel dans le répertoire (Svrmig.mig) est créé par l'applet de commande **Export-SmigServerSetting** . Par conséquent, l'utilisateur n'a pas besoin de spécifier un nom de fichier.

- Si le chemin d'accès n'est pas un emplacement partagé à partir duquel le serveur de destination peut lire, vous devez copier manuellement le magasin de migration vers le serveur de destination ou un emplacement auquel le serveur de destination peut accéder.

- Si un emplacement de magasin de migration existe déjà et que vous souhaitez réexécuter l'applet de commande **Export-SmigServerSetting** , vous devez déplacer le fichier Svrmig.mig à partir de cet emplacement et le stocker ailleurs, renommer ou supprimer d'abord le magasin de migration.

- Vous pouvez effectuer simultanément une migration IP et DHCP Server à partir d'une invite Windows PowerShell à l'aide de l'applet de commande **Export-SmigServerSetting** combinée avec le commutateur **IPConfig** , sur une seule ligne de commande.

- Informations supplémentaires sur les paramètres de ligne de commande :

  - **-Utilisateurs** et **-Paramètres de groupe**

    Le paramètre **-Users** doit être spécifié uniquement si le groupe Administrateurs DHCP inclut des utilisateurs locaux. Sinon, vous pouvez utiliser le paramètre **-Group** et tous les membres des administrateurs DHCP seront migrés. Les membres du groupe Administrateur peuvent inclure des utilisateurs de domaine.

    > ⓘ **Important**
    >
    > Si le serveur source est un contrôleur de domaine, mais que le serveur de destination n'est pas, les groupes locaux de domaine sont migrés en tant que groupes locaux et les utilisateurs du domaine sont migrés en tant qu'utilisateurs locaux.

  - Le paramètre **-IPConfig** collecte des informations IP lorsqu'il est utilisé avec l'applet de commande **Export-SmigServerSetting** sur le serveur source ; le paramètre **-IPConfig** applique les paramètres lorsque l'applet **de commande Import-SmigServerSetting** est utilisée sur le serveur de destination.

    Si le serveur DHCP source a plusieurs cartes réseau et que le service de serveur DHCP est lié à plusieurs cartes réseau et sert des adresses IP sur différents sous-

réseaux, le serveur DHCP de destination doit également avoir plusieurs cartes réseau afin qu'il puisse servir les mêmes sous-réseaux que le serveur DHCP source. Étant donné que les détails de configuration IP seront utilisés ultérieurement lors de l'importation des paramètres de configuration IP sur le serveur de destination, il est recommandé d'enregistrer les paramètres de configuration IP à l'aide de la commande suivante : `IPConfig /all > IPSettings.txt`

L'applet **de commande Import-SmigServerSetting** vous oblige à mapper l'adresse physique source à l'adresse physique de destination.

> ⓘ **Notes**
>
> Le serveur de destination peut être affecté à la même adresse IP statique que le serveur source, sauf si d'autres rôles sur le serveur source doivent continuer à s'exécuter dessus. Dans ce cas, l'adresse IP statique du serveur de destination peut être n'importe quelle adresse IP statique non allouée dans le même sous-réseau que le serveur source.

4. Sur le serveur source, exécutez l'applet de commande **Export-SmigServerSetting** , où <*storepath*> est le chemin d'accès qui contient le fichier Svrmig.mig une fois cette étape terminée. Un exemple de chemin d'accès est \\fileserver\users\username\dhcpstore.

```
PowerShell

Export-SmigServerSetting -featureID DHCP -User All -Group -IPConfig -path
<storepath> -Verbose
```

5. Sur le serveur source, supprimez l'autorisation DHCP pour le serveur DHCP source en exécutant la commande suivante, où le nom de domaine *complet* du serveur est le nom de domaine complet (FQDN) du serveur DHCP et *l'adresse IP* du serveur est l'adresse IP du serveur. Les paramètres de commande respectent la casse et doivent apparaître exactement comme indiqué.

```
PowerShell

Netsh DHCP delete server <Server FQDN> <Server IPAddress>
```

Terminer la migration sur le serveur de destination

Revenez au serveur de destination et suivez ces étapes pour effectuer la migration.

1. Avant d'utiliser l'applet **de commande Import-SmigServerSetting** pour importer les paramètres du serveur DHCP, tenez compte des conditions suivantes :

    - Vous pouvez utiliser une seule ligne de commande avec tous les paramètres pour importer des paramètres DHCP (comme lorsque vous exportez des données à partir du serveur source) ou vous pouvez utiliser l'applet de commande plusieurs fois pour importer des données d'un paramètre à la fois.

    - Si vous décidez d'exécuter l'applet de commande **Import-SmigServerSetting** séparément pour importer les paramètres IP, utilisez le fichier source IPSettings.txt, référencé à l'étape 3 de la procédure précédente. Vous mappez les adresses physiques sources aux adresses physiques de destination à l'étape 3 de cette procédure. Si vous envisagez d'importer des paramètres de rôle et d'adresse IP séparément, vous devez d'abord importer des paramètres IP pour éviter tout conflit d'adresses IP. Vous pouvez ensuite importer le rôle DHCP.

    - Si le groupe Administrateurs DHCP inclut des utilisateurs locaux, utilisez le paramètre **-Users** combiné au paramètre **-Group** pour importer des utilisateurs locaux dans le groupe Administrateurs DHCP. S'il contient uniquement des utilisateurs de domaine, utilisez uniquement le paramètre **-Group** .

    > ⓘ **Notes**
    >
    > Si le serveur source est un serveur membre de domaine, mais que le serveur de destination est un contrôleur de domaine, les utilisateurs locaux importés sont élevés aux utilisateurs de domaine et les groupes locaux importés deviennent des groupes locaux de domaine sur le serveur de destination.

    - Si le rôle serveur DHCP que vous migrez n'a pas été installé sur le serveur de destination, l'applet de commande **Import-SmigServerSetting** installe ce rôle de serveur DHCP et ses dépendances. Vous devrez peut-être redémarrer l'ordinateur de destination pour terminer l'installation une fois le rôle serveur DHCP installé par l'applet de commande. Ensuite, pour terminer l'opération d'importation après avoir redémarré l'ordinateur, vous devez réexécuter l'applet **de commande Import-SmigServerSetting** avec le paramètre **-Force** .

2. Sur le serveur de destination, exécutez la commande suivante, où <*storepath*> est le chemin d'accès disponible qui contient le fichier Svrmig.mig, <*SourcePhysicalAddress-1*> et <*SourcePhysicalAddress-2*> sont des listes séparées par des virgules des adresses physiques de la carte réseau source, et <*TargetPhysicalAddress-1*> et <*TargetPhysicalAddress-2*> sont des listes séparées par des virgules des adresses physiques de la carte réseau de destination :

PowerShell

```
Import-SmigServerSetting -FeatureID 'DHCP' -User All -Group -IPConfig <All |
Global | NIC>
    -SourcePhysicalAddress <SourcePhysicalAddress-1>,<SourcePhysicalAddress-
2>
    -TargetPhysicalAddress <TargetPhysicalAddress-1>,<TargetPhysicalAddress-
2>
    -Force -Path <storepath> -Verbose
```

Le commutateur **-IPConfig** doit être utilisé avec la valeur **All** au cas où l'utilisateur souhaite importer tous les paramètres sources.

> **Important**
>
> Si vous importez l'adresse IP du serveur source sur le serveur cible avec le rôle DHCP sans déconnecter ni modifier l'adresse IP du serveur source, un conflit d'adresses IP se produit.

3. Exécutez la commande suivante pour démarrer le service DHCP : `Start-Service -Name "DHCPServer"`

4. Autorisez le serveur de destination. Les paramètres de commande respectent la casse et doivent apparaître exactement comme indiqué. Sur le serveur de destination, exécutez la commande suivante où le *nom* de domaine complet du serveur est le nom de domaine complet du serveur DHCP et l'adresse IP du serveur est l'adresse *IP* du serveur :

PowerShell

```
netsh DHCP add server <Server FQDN> <Server IPAddress>
```

Une fois cette migration terminée, les ordinateurs clients sur le serveur réseau sont servis par le nouveau serveur de destination x64 exécutant Windows Server. La migration est terminée lorsque le serveur de destination est prêt à servir des adresses IP sur le réseau.

Vérifier la migration

Une fois toutes les étapes de migration terminées, vous pouvez utiliser la procédure suivante pour vérifier que la migration du rôle serveur DHCP a réussi. Si la migration a échoué, vous pouvez revenir à la configuration valide précédente en suivant les étapes décrites dans Tâches post-migration.

Vérifier la configuration du serveur de destination

Suivez ces étapes pour vérifier que le serveur de destination DHCP sert désormais le domaine.

1. Vérifiez que le serveur de destination est autorisé en exécutant la commande suivante dans une fenêtre Windows PowerShell :

   PowerShell
   ```
   netsh DHCP show server
   ```

   La sortie de cette commande doit contenir le nom du serveur de destination DHCP.

2. Vérifiez si le serveur DHCP s'exécute sur le serveur de destination. Dans le Gestionnaire des tâches, sous l'onglet **Services** , l'état du serveur DHCP doit être **démarré**. Vous utilisez également le Gestionnaire des tâches pour vérifier que l'état du serveur source est **arrêté**.

3. Vérifiez que les ordinateurs clients reçoivent correctement des adresses IP à la demande en exécutant les commandes suivantes à l'invite de commandes sur un ordinateur client :

   PowerShell
   ```
   ipconfig /release

   ipconfig /renew
   ```

   Si l'adresse IP du serveur DHCP n'a pas changé, vous n'avez pas besoin d'exécuter la commande **ipconfig /release** . L'exécution **d'ipconfig /renew** doit être suffisante.

   La sortie de ces commandes doit indiquer que l'ordinateur client a reçu une adresse IP.

4. Utilisez la console DHCP pour vérifier que les étendues et les autres paramètres ont été migrés. Pour vous connecter au serveur de destination, sélectionnez **Action**, sélectionnez **Ajouter** un serveur, puis tapez l'adresse IP ou le nom d'hôte du serveur DHCP. Dans l'arborescence de la console, développez le nœud serveur, puis les nœuds IPv4 et IPv6 pour confirmer que les étendues ont été migrées. Localisez ensuite les répertoires des étendues et affichez la plage d'adresses, les réservations, les options d'étendue et les baux actifs pour vérifier ces informations. Vous pouvez également accéder au dossier Options du serveur et vérifier les options de serveur migrées.

Tâches post-migration

Ces tâches post-migration pour le serveur source sont facultatives, en fonction de votre scénario de migration.

La migration est terminée après avoir vérifié que le serveur de destination, et non le serveur source, sert désormais le réseau.

Mettre hors service DHCP sur votre serveur source

Après avoir vérifié la migration, vous pouvez déconnecter, réaffecter ou mettre hors service le serveur source. Si le serveur source exécute d'autres rôles de serveur, il doit être laissé sur le réseau. Si vous n'avez pas besoin d'utiliser cet ordinateur, vous pouvez le stocker en tant que sauvegarde si vous devez revenir à votre configuration DHCP précédente.

Si votre scénario de migration inclut un serveur DHCP autonome, ce serveur source a été mis hors connexion après la création du fichier d'exportation. Dans ce scénario, le service DHCP a été interrompu à partir du moment où il a été arrêté jusqu'à ce que la migration soit terminée sur le nouveau serveur.

Si votre scénario de migration inclut plusieurs serveurs DHCP dans un domaine, une sauvegarde ou un autre serveur DHCP continue de servir des adresses IP pendant la migration afin que les services aux clients ne soient jamais interrompus. La migration est terminée sur le nouveau serveur lorsque l'adresse IP du serveur source est migrée vers le serveur de destination.

Mettre hors service votre serveur source

Une fois que vous avez confirmé que le serveur de destination exécute les fonctions précédemment gérées par le serveur source, vous pouvez mettre hors service ou réaffecter le serveur source, en fonction de vos besoins. Suivez la stratégie de votre organisation concernant la désaffectation du serveur. Pour plus d'informations sur la désaffectation d'un contrôleur de domaine, consultez Rétrogradation des contrôleurs de domaine et des domaines.

Restaurer DHCP en cas d'échec de la migration

Si la migration du serveur DHCP échoue, vous avez les options suivantes :

- Si le serveur source n'a pas été réaffecté, un administrateur peut réaffecter les paramètres de configuration IP, réauthoriser le serveur et redémarrer le service DHCP sur le serveur d'origine.
- Utilisez les fichiers de sauvegarde créés sur le serveur source pour restaurer le serveur DHCP sur le serveur DHCP d'origine.

Dépanner une migration basée sur des applets de commande

Le fichier journal du déploiement des outils de migration Windows Server se trouve à %*windir*%\Logs\SmigDeploy.log. D'autres fichiers journaux des outils de migration Windows Server sont créés aux emplacements suivants.

- % *windir*%\Logs\ServerMigration.log
- % *localappdata*%\SvrMig\Log

Si les fichiers journaux de migration ne peuvent pas être créés dans les emplacements précédents, **ServerMigration.log** et **SmigDeploy.log** sont créés dans %%*temporaire* , et d'autres journaux sont créés dans %*windir*%\System32.

Pour obtenir des conseils de dépannage spécifiques à DHCP, consultez Résoudre les problèmes sur les serveurs DHCP.

Si les connexions entre les serveurs source ou de destination et les contrôleurs de domaine ou les serveurs de catalogue global ne peuvent pas être restaurées

1. Avant d'exécuter **Export-SmigServerSetting**, **Import-SmigServerSetting** ou **Get-SmigServerFeature** , supprimez à nouveau tous les utilisateurs ou groupes de domaine non résolus qui sont membres de groupes locaux du serveur sur lequel vous exécutez l'applet de commande.
2. Avant d'exécuter **à nouveau Send-SmigServerData** ou **Receive-SmigServerData** , supprimez tous les utilisateurs ou groupes de domaine non résolus disposant de droits d'utilisateur pour les fichiers, dossiers ou partages sur le serveur source de migration.

Afficher le contenu des objets de résultats des outils de migration Windows Server

Toutes les applets de commande outils de migration Windows Server retournent les résultats sous forme d'objets. Vous pouvez enregistrer des objets de résultat et les interroger pour plus d'informations sur les paramètres et les données qui ont été migrés. Vous pouvez également utiliser des objets de résultat comme entrée pour d'autres commandes et scripts Windows PowerShell.

Descriptions d'objets de résultat

Les applets de commande **Import-SmigServerSetting** et **Export-SmigServerSetting** des outils de migration Windows Server retournent une liste d'objets **MigrationResult** . Chaque objet **MigrationResult** contient des informations sur les données ou les paramètres que l'applet de commande traite, le résultat de l'opération et les messages d'erreur ou d'avertissement associés. Le tableau suivant décrit les propriétés d'un objet **MigrationResult** .

Agrandir le tableau

Nom de la propriété	Type	Definition
ItemType	Enum	Type d'élément en cours de migration. Les valeurs incluent **General**, **WindowsFeatureInstallation**, **WindowsFeature** et **OSSetting**.
ID	String	ID de l'élément migré. Parmi les exemples de valeurs, citons **l'utilisateur local**, **le groupe local** et **DHCP**.
Success	Boolean	La valeur **True** s'affiche si la migration a réussi ; sinon, **False** s'affiche.
DetailsList	`List<MigrationResultDetails>`	Liste des objets **MigrationResultDetails** .

Les applets de commande **Send-SmigServerData** et **Receive-SmigServerData** retournent des résultats dans une liste d'objets **MigrationDataResult**. Chaque objet **MigrationDataResult** contient des informations sur les données ou le partage que l'applet de commande traite, le résultat de l'opération, les messages d'erreur ou d'avertissement et d'autres informations connexes. Le tableau suivant décrit les propriétés d'un objet **MigrationDataResult** .

Agrandir le tableau

Nom de la propriété	Type	Definition
ItemType	Enum	Type d'élément migré. Les valeurs incluent **fichier**, **dossier**, **partage** et **fichier chiffré**.
SourceLocation	String	Emplacement source de l'élément, affiché sous la forme d'un chemin d'accès.
DestinationLocation	String	Emplacement de destination de l'élément, affiché sous la forme d'un chemin d'accès.
Success	Boolean	La valeur **True** s'affiche si la migration a réussi ; sinon, **False** s'affiche.
Size	Integer	Taille de l'élément, en octets.

Nom de la propriété	Type	Definition
ErrorDetails	`List<MigrationResultDetails>`	Liste des objets **MigrationResultDetails** .
Error	Enum	Énumération d'erreurs pour les erreurs qui se sont produites.
WarningMessageList	`List<String>`	Liste des messages d'avertissement.

Le tableau suivant décrit les propriétés des objets dans l'objet **MigrationResultDetails** qui sont communs aux objets **MigrationResult** et **MigrationDataResult** .

Agrandir le tableau

Nom de la propriété	Type	Definition
FeatureId	String	Nom du paramètre de migration lié à l'élément. Voici quelques exemples de valeurs : **IPConfig** et **DNS**. Cette propriété est vide pour la migration de données.
Messages	`List<String>`	Liste des messages d'événement détaillés.
DetailCode	Integer	Code d'erreur ou d'avertissement associé à chaque message d'événement.
Severity	Enum	Gravité d'un événement, si des événements se sont produits. Voici quelques exemples de valeurs : **Informations**, **Erreur** et **Avertissement**.
Title	String	Titre de l'objet de résultat. Il peut s'agir de l'adresse physique de la carte réseau en cas de configuration IP, ou du nom d'utilisateur en cas de migration d'un utilisateur local.

Vue d’ensemble du basculement DHCP

Article • 05/05/2025 •

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Le basculement DHCP permet à deux serveurs DHCP Microsoft de partager des informations de disponibilité, ce qui garantit une haute disponibilité en répliquant les baux d’adresses IP et les paramètres entre un serveur principal et son partenaire de basculement.

Toutes les informations d’étendue sont partagées entre les deux serveurs DHCP, y compris les baux actifs. Cela permet à l’un ou l’autre serveur DHCP de prendre en charge les clients DHCP si l’autre serveur n’est plus disponible.

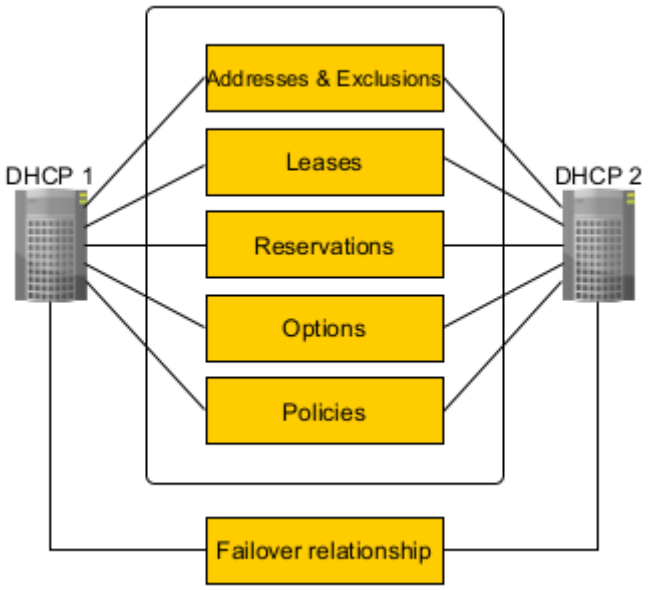
Cet article fournit une vue d’ensemble du basculement DHCP.

Présentation du basculement DHCP

Avec le basculement DHCP, les étendues DHCPv4 sont répliquées à partir d’un serveur DHCP principal vers un serveur DHCP partenaire, ce qui permet la redondance et l’équilibrage de charge des services DHCP. Les serveurs DHCP qui partagent une étendue DHCP activée pour le basculement sont appelés **partenaires de basculement**. L’implémentation du basculement DHCP par Microsoft est basée sur l’ébauche du protocole de basculement DHCP de l’IETF (Internet Engineering Task Force).

Lorsque deux serveurs DHCP sont configurés pour le basculement, ils partagent des informations d’étendue, y compris tous les baux actifs. Cela permet aux deux serveurs DHCP de fournir des baux au même sous-réseau à des fins d’équilibrage de charge ou de redondance. Les paramètres d’étendue sont répliqués lors de la première configuration du basculement DHCP et peuvent être répliqués ultérieurement si des modifications de configuration sont apportées.

La figure suivante illustre la façon dont les composants et les paramètres d'une étendue DHCP activée pour le basculement sont partagés entre deux serveurs DHCP.



Les étendues et les paramètres utilisés avec les serveurs DHCP configurés pour le basculement DHCP sont partagés à l'aide d'un nouvel objet appelé **relation de basculement DHCP**. Plusieurs options de configuration sont disponibles avec le basculement DHCP. Vous pouvez configurer le basculement sur toutes les étendues qui existent sur un serveur DHCP ou uniquement sur certaines étendues. Vous pouvez également utiliser facilement les mêmes paramètres de basculement DHCP pour de nombreuses étendues en les ajoutant à la même relation de basculement. Une relation de basculement est toujours entre deux serveurs DHCP uniquement. Toutefois, un serveur peut avoir de nombreuses relations de basculement, et chaque relation de basculement peut être avec un autre serveur DHCP.

> ⓘ **Important**
>
> Si des modifications sont apportées à une étendue activée pour le basculement, vous devez répliquer manuellement ces modifications sur le serveur partenaire afin de synchroniser les étendues sur les deux serveurs DHCP. La réplication copie les paramètres d'étendue du serveur DHCP où elle est lancée vers le serveur partenaire, remplaçant ainsi ses paramètres existants. Par conséquent, il est important de toujours lancer la réplication à partir du serveur qui a des paramètres d'étendue DHCP que vous souhaitez utiliser.

Spécifications de basculement DHCP

Les spécifications suivantes s'appliquent au basculement DHCP.

Étendues DHCP :

- Vous ne pouvez pas configurer le basculement DHCP sur une étendue DHCP pour inclure plus de deux serveurs DHCP.

- Le basculement DHCP prend uniquement en charge les étendues DHCPv4. Les étendues DHCPv6 ne peuvent pas être activées pour le basculement.
- Si les paramètres d'une étendue avec basculement sont modifiés, ces paramètres doivent être répliqués manuellement sur le serveur DHCP partenaire.
- La réplication des paramètres d'étendue peut être lancée à partir d'un serveur DHCP vers son serveur partenaire de basculement.

Client/serveur DHCP :

- Les clients DHCP doivent pouvoir communiquer avec les deux serveurs partenaires de basculement DHCP, directement ou à l'aide d'un relais DHCP.
- Lorsque le basculement DHCP est activé, un bail client DHCP peut être renouvelé par un serveur différent de celui qui l'a émis à l'origine.
- Deux bases de données de bail client synchronisées distinctes sont conservées indépendamment par chaque serveur partenaire de basculement DHCP.
- Les serveurs DHCP configurés en tant que partenaires de basculement peuvent se trouver sur différents sous-réseaux, mais cela n'est pas obligatoire.
- Le protocole DHCP en cluster est pris en charge conjointement avec le basculement DHCP. À des fins de basculement, un cluster DHCP est considéré comme un seul serveur DHCP.
- Le basculement DHCP peut être configuré et les paramètres peuvent être modifiés sans avoir à suspendre, arrêter ou redémarrer le service serveur DHCP.

Partenaires de basculement DHCP :

- Les partenaires de basculement DHCP doivent exécuter au moins Windows Server 2016.
- Deux serveurs DHCP configurés en tant que partenaires de basculement tentent de maintenir une connexion TCP/IP persistante.
- Les serveurs DHCP configurés en tant que partenaires de basculement connaissent tous les deux l'état du service DHCP sur l'autre serveur et sont informés de toute modification de cet état avec un délai minimal.
- Si deux serveurs DHCP configurés en tant que partenaires de basculement ne peuvent pas communiquer, les précautions sont prises pour éviter que le même bail d'adresse IP soit émis à deux clients DHCP différents.

- Si un serveur DHCP devient indisponible avant de pouvoir synchroniser correctement toutes les informations du client DHCP avec son partenaire de basculement, des précautions sont prises pour garantir la continuité du bail DHCP pour les clients DHCP.
- Deux bases de données de bail client synchronisées distinctes sont conservées indépendamment par chaque serveur partenaire de basculement DHCP.

> **Important**
>
> Lors de la réplication des paramètres entre les serveurs partenaires de basculement DHCP qui ont différentes versions du système d'exploitation, modifiez toujours les paramètres et lancez la réplication à partir du serveur DHCP avec la version la plus récente du système d'exploitation. Cela garantit que les paramètres sont reconnus par les partenaires de basculement et répliqués de manière cohérente.

Vous pouvez configurer le basculement DHCP à l'aide du Gestionnaire de serveur ou de Windows PowerShell. Pour plus d'informations sur l'utilisation de Windows PowerShell, consultez applets de commande du serveur DHCP dans Windows PowerShell. Pour obtenir des instructions sur la configuration du protocole DHCP dans le Gestionnaire de serveur, consultez ce guide pas à pas.

Basculement DHCP et IPv6

Le basculement DHCP n'est pas pris en charge pour les étendues IPv6 (Internet Protocol version 6). Les cartes réseau utilisant IPv6 déterminent généralement leur propre adresse IPv6 à l'aide de la configuration automatique IP sans état. Dans ce mode, le serveur DHCP fournit uniquement la configuration de l'option DHCP et le serveur ne conserve aucune information d'état de bail. Un déploiement à haute disponibilité pour le DHCPv6 sans état est possible en installant deux serveurs avec des options identiques. L'étendue fractionnée représente une solution viable de haute disponibilité car les étendues ne fonctionnent pas en cas d'utilisation intense d'adresse, même dans le cadre du déploiement DHCPv6 à états.

Modes de basculement DHCP

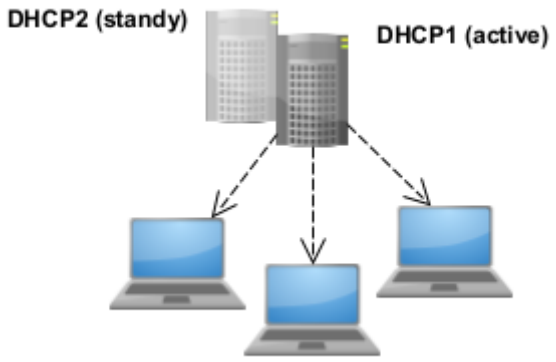
Deux modes de basculement DHCP sont disponibles lorsque vous créez une relation de basculement DHCP :

- **Mode de secours à chaud** : ce mode fournit une redondance pour les services DHCP.
- **Mode d'équilibrage de charge** : ce mode alloue des baux clients DHCP sur deux serveurs.

Vous pouvez basculer entre le mode de veille à chaud et le mode d'équilibrage de charge si vous le souhaitez, mais vous ne pouvez utiliser qu'un seul mode à la fois avec une seule étendue DHCP. Vous pouvez également utiliser les deux modes sur le même serveur DHCP si vous configurez plusieurs relations de basculement. Personnalisez votre déploiement en fonction de l'architecture physique de votre réseau.

Mode du serveur de secours

Dans ce mode, deux serveurs entretiennent une relation de basculement dans laquelle un serveur actif est responsable de louer les adresses IP et les informations de configuration à tous les clients dans une étendue ou un sous-réseau. Le serveur partenaire assume un rôle de secours, avec la responsabilité d'émettre des baux aux clients DHCP uniquement si le serveur actif devient indisponible. Le mode de secours à chaud est idéal pour les scénarios où le partenaire de basculement est destiné à être utilisé temporairement lorsque le serveur actif n'est pas disponible.



Un serveur est actif ou en veille dans le contexte d'une relation de basculement. Par exemple, un serveur qui a le rôle d'actif pour une relation donnée peut être un serveur de secours pour une autre relation. Par défaut, le serveur utilisé pour créer la relation de basculement est le serveur actif, mais ce n'est pas nécessaire.

Lorsque vous choisissez le secours à chaud, vous devez également configurer le pourcentage des adresses IP du serveur actif réservées pour une utilisation sur le serveur de secours si le serveur actif ne répond pas. Par défaut, ce pourcentage de réserve est de 5%.

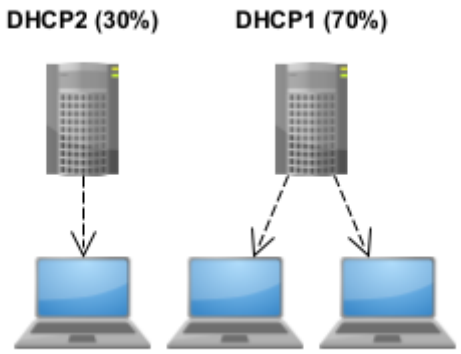
Le pourcentage de réserve est utilisé pour les nouveaux baux DHCP. Si un client DHCP tente de renouveler un bail DHCP avec le serveur de secours qui ne parvient pas à contacter le serveur actif, la même adresse IP qui a été précédemment affectée au client DHCP est renouvelée. Dans ce cas, un bail temporaire est accordé pour la durée maximale du délai d'exécution du client (MCLT), et non pour la durée totale du bail.

Si le serveur de secours émet tous ses baux de pourcentage de réserve disponibles pour les nouveaux clients DHCP avant l'expiration du MCLT, il refuse d'émettre de nouveaux baux DHCP et continue de renouveler les baux existants. Une fois le MCLT expiré, le serveur de secours est autorisé à utiliser l'intégralité du pool d'adresses IP disponibles pour les nouveaux baux DHCP. Si le serveur est toujours en état d'interruption des communications, il n'utilise pas l'intégralité du pool d'adresses IP disponibles pour les nouveaux baux DHCP.

En mode de secours à chaud, un bureau central ou un serveur de centre de données joue généralement le rôle de serveur de sauvegarde de secours. Ce serveur fournit une redondance pour un serveur DHCP local sur un site distant, qui sert directement les clients DHCP. Dans ces déploiements, le serveur de secours doit uniquement traiter les clients si le serveur DHCP local devient indisponible.

Mode d'équilibrage de charge

Le mode d'équilibrage de charge est le mode par défaut du déploiement. Dans ce mode, deux serveurs DHCP servent simultanément des adresses IP et des options aux clients sur un sous-réseau donné. Les demandes du client DHCP sont équilibrées et partagées entre les deux serveurs DHCP. Le rapport d'équilibrage de charge par défaut entre les deux serveurs est de 50:50, mais il peut être personnalisé à n'importe quel rapport compris entre 0% et 100%.



Le mécanisme d'équilibrage de charge est défini dans RFC 3074, dans lequel un hachage est calculé à partir de l'adresse MAC contenue dans chaque requête du client DHCP. Une plage de valeurs de hachage (également appelée compartiment de hachage) est affectée à chaque serveur DHCP en fonction des pourcentages d'équilibrage de charge configurés. Les serveurs déterminent s'ils sont désignés pour répondre au client en fonction de leur compartiment de hachage affecté.

En mode d'équilibrage de charge, lorsqu'un serveur DHCP perd le contact avec son partenaire de basculement, il commence à accorder des baux à tous les clients DHCP. S'il reçoit une demande de renouvellement de bail d'un client DHCP affecté à son partenaire de basculement, il renouvelle temporairement le même bail d'adresse IP pendant la durée du MCLT. S'il reçoit

une demande d'un client qui n'a pas été précédemment affecté à un bail, il accorde un nouveau bail à partir de son pool d'adresses IP gratuites jusqu'à ce qu'il soit épuisé, puis commence à utiliser le pool d'adresses IP gratuites de son partenaire de basculement. Si le serveur DHCP passe à l'état « partenaire indisponible », il attend la durée MCLT, puis prend en charge 100 % du pool d'adresses IP.

Le mode de fonctionnement avec équilibrage de charge est particulièrement adapté aux déploiements dans lesquels les deux serveurs en relation de basculement sont situés sur le même site physique. Les deux serveurs répondent aux demandes du client DHCP en fonction du ratio de distribution de charge configuré par l'administrateur.

Basculement DHCP et clustering de basculement Windows

Le basculement DHCP est pris en charge avec DHCP en cluster dans les configurations suivantes :

- Un seul serveur DHCP peut avoir une relation de basculement avec un cluster de basculement DHCP.
- Un cluster de basculement DHCP peut avoir une relation de basculement avec un autre cluster de basculement DHCP.

Dans les deux cas, vous devez configurer le basculement DHCP pour utiliser le nom ou l'adresse IP du cluster, et non le nom ou l'adresse IP d'un nœud de cluster. Si un nœud de cluster individuel est configuré en tant que partenaire de basculement, le serveur principal entre dans un état d'interruption des communications si le service serveur DHCP passe à un autre nœud du cluster.

> **Important**
>
> Si vous utilisez un secret partagé, vous devez répliquer manuellement le secret partagé sur tous les nœuds de cluster. Vous pouvez répliquer le secret partagé sur le nœud de cluster actif à l'aide de l'applet de commande PowerShell Set-DhcpServerv4Failover.

Basculement DHCP et mises à jour dynamiques DNS

Si les serveurs DHCP sont configurés pour effectuer des mises à jour dynamiques DNS pour le compte de l'ordinateur client, les deux serveurs DHCP dans une relation de basculement DHCP

doivent utiliser les mêmes informations d'identification DNS pour mettre à jour les enregistrements DNS. Si le partenaire de basculement tente d'utiliser différentes informations d'identification pour mettre à jour les enregistrements de ressources DNS, cette mise à jour échoue.

Les étapes suivantes décrivent comment les mises à jour dynamiques DNS peuvent échouer lorsqu'un ordinateur client utilise un autre serveur DHCP :

1. Un serveur DHCP Windows effectue une mise à jour dynamique pour le compte d'un client DHCP.
2. Le serveur DHCP crée le nom DNS du client et devient le propriétaire de ce nom.
3. Désormais, seul le serveur DHCP lui-même peut mettre à jour les enregistrements DNS pour le nom du client.
4. Le serveur d'origine échoue et un deuxième serveur DHCP de sauvegarde est en ligne ; le deuxième serveur ne peut pas mettre à jour le nom du client, car il n'est pas le propriétaire du nom.

Consultez également la propriété d'enregistrement DNS et le groupe DnsUpdateProxy pour une discussion sur ce scénario.

Points à prendre en considération pour le déploiement

Avant de déployer le basculement DHCP, tenez compte des éléments suivants :

Synchronisation de l'heure

Pour que le basculement DHCP fonctionne correctement, l'heure doit être synchronisée entre les deux serveurs qui entretiennent une relation de basculement. La synchronisation de l'heure peut être gérée par le déploiement du protocole NTP (Network Time Protocol) ou tout autre mécanisme alternatif. Lorsque l'Assistant Configuration de basculement est exécuté, il compare l'heure actuelle sur les serveurs en cours de configuration pour le basculement. Si la différence de temps entre les serveurs est supérieure à une minute, le processus de basculement s'arrêtera avec une erreur critique et demandera la synchronisation de l'heure sur les serveurs.

Chaque message de protocole de basculement inclut un champ de temps rempli avec l'heure utc (Temps universel coordonné) lorsque le serveur source a transmis le message. Pour chaque message, le serveur de réception effectue une vérification de la différence de temps entre le champ horodatage dans le paquet et l'heure au serveur de réception. Si cette différence de

temps est supérieure à une minute, le serveur de réception enregistre un événement critique indiquant que les deux serveurs ne sont pas synchronisés.

Affectation basée sur une stratégie

Windows Server inclut une fonctionnalité d'attribution d'adresse IP basée sur une stratégie, qui permet à un administrateur DHCP Windows de regrouper les clients DHCP par un attribut spécifique du client, tel que la classe de fournisseur, la classe d'utilisateur, l'identificateur client ou l'adresse MAC. Les administrateurs regroupent les clients en fonction de ces attributs et peuvent affecter des paramètres tels que l'adresse IP, la passerelle par défaut, le serveur DNS et d'autres options DHCP à un regroupement spécifique de clients. Cela permet à l'administrateur d'exercer un meilleur contrôle sur les paramètres de configuration remis aux hôtes finaux. Cette fonctionnalité introduit le concept de plusieurs plages d'adresses IP dans une seule étendue. Pour ce faire, la distribution d'adresses de basculement DHCP en mode de partage de charge est effectuée en fonction de la plage d'adresses IP.

Pare-feu Windows

Le basculement DHCP utilise le port TCP 647 pour écouter les messages de basculement entre deux serveurs partenaires de basculement. Pour que ce trafic soit autorisé par le Pare-feu Windows, les règles de pare-feu entrantes et sortantes suivantes sont ajoutées, puis vous installez le rôle serveur DHCP :

- Microsoft-Windows-DHCP-Failover-TCP-In
- Microsoft-Windows-DHCP-Failover-TCP-Out

Agents de relais

Les messages DHCPDISCOVER initiaux sont diffusés par les clients DHCP sur le sous-réseau auquel ils appartiennent. Étant donné que les routeurs ne transfèrent généralement pas le trafic de diffusion, un mécanisme est nécessaire pour permettre aux clients DHCP de communiquer avec des serveurs DHCP si le serveur DHCP n'est pas situé sur le même sous-réseau. Les agents de relais (généralement fournis sur un routeur) sont conçus pour effectuer cette fonction, relayer des messages DHCP et BOOTP entre les clients et les serveurs sur différents sous-réseaux. Les agents de relais sont généralement configurés sur un appareil réseau, ou vous pouvez configurer le relais DHCP sur un serveur Windows server avec le rôle d'accès à distance installé. Pour plus d'informations, consultez Déployer l'agent de relais DHCP.

Si votre relais DHCP est configuré sur un appareil réseau, consultez la documentation de votre fournisseur pour plus d'informations. La commande **d'adresse d'assistance** est couramment

utilisée pour configurer le relais DHCP sur un appareil réseau, par exemple : `ip helper-address 10.0.1.1`.

Lorsque vous déployez un basculement DHCP, une seule adresse de relais DHCP peut ne pas suffire, car les clients DHCP doivent toujours être en mesure de communiquer avec le serveur DHCP principal et le serveur partenaire de basculement. Si les deux serveurs DHCP se trouvent sur un sous-réseau différent des clients DHCP, cela nécessite au moins deux agents de relais DHCP. Par exemple : `ip helper-address 10.0.1.1`, `ip helper-address 10.0.1.2`.

Dans cet exemple, les deux serveurs DHCP se trouvent sur le même sous-réseau (10.0.1.0/24). L'adresse IP du serveur DHCP principal est 10.0.1.1 et 10.0.1.2 est l'adresse IP du serveur partenaire de basculement. Si les deux serveurs DHCP se trouvent sur le même sous-réseau, vous pouvez également configurer l'adresse de diffusion du sous-réseau (par exemple, 10.0.1.255) en tant que relais DHCP unique. L'utilisation d'une adresse de diffusion de sous-réseau en tant que relais DHCP unique n'est pas possible si les serveurs DHCP se trouvent sur des sous-réseaux distincts.

Agents de relais dupliqués

Virtual Router Redundancy Protocol (VRRP) est un autre protocole de basculement utilisé pour activer la redondance sur les appareils réseau. Un exemple de VRRP inclut le protocole HSRP (Hot Standby Router Protocol), qui est un VRRP propriétaire cisco. Si VRRP/HSRP est configuré sur un appareil réseau qui est également configuré avec un ou plusieurs relais DHCP, cela peut entraîner l'envoi de messages de relais DHCP en double au même serveur de basculement DHCP.

Si un serveur DHCP unique configuré pour le basculement DHCP reçoit des demandes de bail en double, cela peut entraîner des durées de bail client incohérentes et les clients peuvent louer des adresses IP appartenant à d'autres clients. Consultez la documentation de votre fournisseur pour déterminer si le protocole de redondance du routeur nécessite une configuration spécifique pour prendre en charge le relais DHCP. Par exemple, Cisco fournit la prise en charge du relais DHCP pour le protocole HSRP à l'aide de groupes de routeurs virtuels.

Gérer les relations de basculement DHCP dans Windows Server

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Les relations de basculement sont des paramètres utilisés par deux serveurs DHCP pour partager une ou plusieurs étendues DHCP avec basculement.

Dans cet article, suivez les étapes pour créer, afficher, modifier et supprimer des relations de basculement DHCP dans Windows Server.

Prerequisites

- Au moins Windows Server 2012
- Le rôle serveur DHCP est installé
- Comprendre comment fonctionnent les relations de basculement. Pour plus d'informations sur les relations de basculement DHCP, consultez Vue d'ensemble du basculement DHCP.
- Deux serveurs DHCP connectés au réseau qui peuvent communiquer entre eux
- Au moins une étendue DHCP IPv4 est configurée sur le serveur DHCP principal.

Configurer les relations de basculement

Pour créer une relation de basculement sur un serveur DHCP, vous pouvez utiliser PowerShell ou la console DHCP. Suivez les étapes de la méthode de votre choix.

Quelques points à prendre en compte pour créer une relation de basculement :

- Le mode de basculement DHCP par défaut est l'équilibrage de charge avec 50 % des baux affectés par le serveur local et 50 % affectés par le serveur partenaire.
- L'authentification est activée par défaut, mais ce paramètre n'est pas obligatoire. Si l'authentification est activée, vous devez également fournir un secret partagé.
- L'ID d'étendue fourni doit correspondre à une étendue configurée sur le serveur local qui n'est pas déjà activée pour le basculement et n'existe pas déjà sur le serveur partenaire.

- Si le basculement DHCP est configuré à distance, le serveur local fait référence au serveur spécifié sur la ligne de commande ou ajouté à la console de gestion.
- Vous ne pouvez pas activer le basculement DHCP sur une étendue DHCP si l'étendue existe déjà sur les deux serveurs DHCP dans une relation de basculement, comme cela peut se produire dans une configuration d'étendue fractionnée.
- Si une étendue DHCP existe sur le serveur DHCP partenaire, elle doit être supprimée avant de configurer le basculement DHCP.

PowerShell

Pour configurer une relation de basculement en utilisant PowerShell, procédez comme suit :

1. Sur le bureau Windows, sélectionnez le bouton Démarrer et tapez une partie du nom **Windows PowerShell**.

2. Cliquez avec le bouton droit sur Windows PowerShell, puis sélectionnez **Run as Administrator**.

3. Utilisez l'applet de commande PowerShell Add-DhcpServerv4Failover pour ajouter une relation de basculement IPv4 sur le service serveur DHCP. Exécutez la commande suivante pour créer une relation de **basculement d'équilibrage de charge** :

PowerShell

```
Add-DhcpServerv4Failover -ComputerName "dhcp1.contoso.com" -Name "dc1-dhcp1" -
PartnerServer "dhcp2.contoso.com" -ScopeId 10.10.10.0,10.20.20.0 -SharedSecret
"sEcReT"
```

Cette commande crée une **relation de basculement d'équilibrage de charge** entre **dhcp1.contoso.com** et **dhcp2.contoso.com**. Le basculement concerne les plages d'adresses 10.10.10.0 et 10.20.20.0 qui sont présentes sur **dhcp1.contoso.com**. Ces étendues sont créées sur le service serveur DHCP partenaire qui s'exécute sur l'ordinateur nommé **dhcp2.contoso.com** dans le cadre de la création de la relation de basculement. L'authentification de message est activée pour l'échange de messages serveur à serveur avec le secret partagé spécifié.

Pour créer une **relation de basculement en veille à chaud**, utilisez la commande :

PowerShell

```
Add-DhcpServerv4Failover -ComputerName "dhcp1.contoso.com" -Name "dc1-dhcp1" -
PartnerServer "dhcp2.contoso.com" -ServerRole Standby -ScopeId
```

```
10.10.10.0,10.20.20.0
```

dhcp2.contoso.com est en service en tant que serveur DHCP de secours, et **dhcp1.contoso.com** est en service en tant que serveur DHCP actif dans la relation de basculement.

Afficher les relations de basculement

Vous pouvez afficher les relations de basculement sur un serveur DHCP à l'aide de Windows PowerShell ou de la console DHCP.

PowerShell

Pour afficher les relations de basculement sur un serveur DHCP, vous pouvez utiliser l'applet de commande Get-DhcpServerv4Failover à l'aide d'une invite Windows PowerShell avec élévation de privilèges.

1. Sur le bureau Windows, sélectionnez le bouton Démarrer et tapez une partie du nom **Windows PowerShell**.
2. Cliquez avec le bouton droit sur Windows PowerShell, puis sélectionnez **Run as Administrator**.
3. Exécutez la commande suivante:

PowerShell

```
Get-DhcpServerv4Failover
```

Sortie

```
Name                : dc1.contoso.com-192.168.0.254
PartnerServer       : 192.168.0.254
Mode                : HotStandby
LoadBalancePercent  :
ServerRole          : Active
ReservePercent      : 5
MaxClientLeadTime   : 01:00:00
StateSwitchInterval :
State               : Normal
ScopeId             : {192.168.50.0, 192.168.0.0}
AutoStateTransition : False
EnableAuth          : False
```

```
    Name                : dhcp1-dc1 load balance
    PartnerServer       : dhcp1.contoso.com
    Mode                : LoadBalance
    LoadBalancePercent  : 50
    ServerRole          :
    ReservePercent      :
    MaxClientLeadTime   : 01:00:00
    StateSwitchInterval :
    State               : Normal
    ScopeId             :
    AutoStateTransition : False
    EnableAuth          : False
```

Un avantage d'utiliser Windows PowerShell pour visualiser les relations de basculement est que vous pouvez afficher plus de propriétés de la relation de basculement DHCP que dans la console DHCP.

Modifier les relations de basculement

Pour modifier les relations de basculement sur un serveur DHCP, vous pouvez utiliser PowerShell ou la console DHCP.

PowerShell

Pour modifier les relations de basculement sur un serveur DHCP, vous pouvez utiliser l'applet de commande Set-DhcpServerv4Failover.

1. Sur le bureau Windows, sélectionnez le bouton Démarrer et tapez une partie du nom **Windows PowerShell**.
2. Cliquez avec le bouton droit sur Windows PowerShell, puis sélectionnez **Run as Administrator**.
3. Exécutez la commande suivante:

PowerShell

```
Set-DhcpServerv4Failover -Name "dhcp1-dc1" -LoadBalancePercent 70
```

Cette commande modifie la relation de basculement **dhcp1-dc1** afin de traiter 70 % des requêtes client gérées par le serveur DHCP.

Supprimer les relations de basculement

Pour supprimer une relation de basculement sur un serveur DHCP, vous pouvez utiliser PowerShell ou la console DHCP.

PowerShell

Pour modifier les relations de basculement sur un serveur DHCP, vous pouvez utiliser l'applet de commande Remove-DhcpServerv4Failover.

1. Sur le bureau Windows, sélectionnez le bouton Démarrer et tapez une partie du nom **Windows PowerShell**.
2. Cliquez avec le bouton droit sur Windows PowerShell, puis sélectionnez **Run as Administrator**.
3. Exécutez la commande suivante:

PowerShell

```
Remove-DhcpServerv4Failover -Name dhcp1.contoso.com-dhcp2-dns1.contoso.com
```

Contenu connexe

Vue d'ensemble du basculement DHCP

Last updated on 20/04/2026

Migrer un déploiement de tolérance de panne DHCP (Dynamic Host Configuration Protocol) existant

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

La migration d'un déploiement de basculement DHCP existant vers une version plus récente de Windows Server garantit que votre infrastructure réseau reste up-to-date, sécurisée et efficace. Ce guide complet vous guide tout au long du processus de migration, en commençant par rompre la relation de basculement sur vos serveurs actuels, l'exportation et l'importation des paramètres DHCP et la configuration du basculement sur les nouveaux serveurs. En suivant ce guide, les administrateurs informatiques peuvent migrer leur configuration de basculement DHCP vers le dernier environnement Windows Server, ce qui garantit un temps d'arrêt minimal et des services réseau ininterrompus.

Prerequisites

- Au moins Windows Server 2012 installé.
- Le rôle serveur DHCP est installé.
- Une relation de basculement existante existe.
- L'appartenance au groupe **Administrateurs** ou équivalent est la condition minimale requise pour effectuer ces procédures.

Détails du serveur

Les étapes décrites dans ce guide sont valides pour les versions de Windows Server à partir de Windows Server 2012.

Dans ce guide, envisagez le scénario où le déploiement de reprise DHCP est migré de Windows Server 2022 à Windows Server 2025. Les serveurs suivants sont utilisés dans ce scénario de migration :

- **DHCP-2022-1** : serveur DHCP initial en ligne avec des étendues actives.
- **DHCP-2022-2** : serveur partenaire de basculement DHCP initial pour DHCP-2022-1.
- **DHCP-2025-1** : serveur DHCP sur Windows Server 2025 qui remplace DHCP-2022-1.
- **DHCP-2025-2** : serveur DHCP sur Windows Server 2025 qui remplace DHCP-2022-2.

Supprimer la relation de basculement entre DHCP-2022-1 et DHCP-2022-2

Vous pouvez supprimer la relation de basculement à l'aide de PowerShell ou de la console DHCP. La suppression d'une relation de basculement supprime toutes les étendues membres de la relation de basculement du serveur DHCP partenaire.

PowerShell

1. À une invite Windows PowerShell avec élévation de privilèges sur DHCP-2022-1, utilisez l'applet de commande Remove-DhcpServerv4Failover pour supprimer une relation de basculement nommée **DHCP-2022-1-DHCP-2022-2**. Tapez la commande suivante, puis appuyez sur Entrée :

   PowerShell

   ```
   Remove-DhcpServerv4Failover -Name DHCP-2022-1-DHCP-2022-2
   ```

   Remplacez *DHCP-2022-1-DHCP-2022-2* par le nom de la relation de basculement DHCP que vous souhaitez supprimer.

2. Utilisez l'applet de commande Get-DhcpServerv4Failover pour obtenir les relations de basculement configurées sur le serveur DHCP actuel. Tapez la commande suivante, puis appuyez sur Entrée :

   PowerShell

   ```
   Get-DhcpServerv4Failover
   ```

   Vérifiez que le nom de la relation de basculement DHCP n'est pas affiché dans la sortie de la commande, ce qui indique qu'il est supprimé avec succès.

Notes

Les étendues DHCP de la relation de basculement sont supprimées du serveur DHCP partenaire. Les étendues restent sur le serveur où vous avez saisi la commande Remove-DhcpServerv4Failover (DHCP-2022-1 dans cet exemple).

Exporter les paramètres DHCP vers un nouveau serveur

Utilisez la procédure suivante pour exporter les paramètres de niveau serveur à partir du serveur DHCP qui a des étendues que vous souhaitez activer pour le basculement DHCP, en préparation de l'importation vers vos nouveaux serveurs DHCP sur Windows Server 2025. Seule la configuration au niveau du serveur DHCP est exportée et importée, car la base de données de bail est répliquée de DHCP-2022-1 vers DHCP-2025-2 lorsque la relation de basculement est établie.

> ⓘ **Notes**
>
> Si vous utilisez DHCP en cluster, vous devez uniquement exporter les paramètres DHCP à partir du nœud actif.

Exporter les paramètres DHCP

Suivez les étapes pour exporter les paramètres DHCP à partir de DHCP-2022-1.

1. Sur **DHCP-2025-1**, ouvrez une invite Windows PowerShell avec élévation de privilèges, entrez les commandes suivantes :

   PowerShell

   ```
   mkdir C:\export
   mkdir C:\backup
   Export-DhcpServer –ComputerName DHCP-2022-1 –File C:\export\DHCP-2022-
   1exp.xml -Verbose
   ```

2. **Connectez-vous à DHCP-2025-2** et, dans une invite Windows PowerShell avec élévation de privilèges, exécutez ce qui suit :

   PowerShell

   ```
   mkdir C:\export
   mkdir C:\backup
   Export-DhcpServer –ComputerName DHCP-2022-1 –File C:\export\DHCP-2022-
   1exp.xml -Verbose
   ```

Les paramètres de configuration DHCP sont exportés à partir d'un serveur DHCP distant, **DHCP-2022-1**, vers un fichier sur le serveur local, **DHCP-2025-1** et **DHCP-2025-2**.

Vous pouvez également exporter vers un fichier sur DHCP-2022-1, puis copier le fichier de paramètres sur le réseau vers DHCP-2025-2 et DHCP-2025-1.

Importer les paramètres DHCP

La procédure suivante suppose que les paramètres DHCP sont enregistrés dans le fichier **C:\export\DHCP-2022-1exp.xml** sur un serveur DHCP avec un nom d'hôte **DHCP-2025-1**. Remplacez les noms de fichier et d'hôte par des noms utilisés dans votre environnement. Ne répétez pas cette procédure sur DHCP-2025-2.

Importer des paramètres DHCP et des baux sur un nouveau serveur

Suivez les étapes pour importer les paramètres ET les baux DHCP vers DHCP-2025-1.

1. À une invite de commandes Windows PowerShell avec des droits élevés, entrez les commandes suivantes :

   PowerShell

   ```
   Import-DhcpServer –ComputerName DHCP-2025-1 –File C:\export\DHCP-2022-1exp.xml -BackupPath C:\backup\ -ServerConfigOnly -Verbose -Force
   ```

Cette commande importe uniquement la configuration au niveau du serveur de DHCP-2022-1 vers DHCP-2025-1. Les paramètres au niveau du serveur sont les suivants :

- Classes de fournisseur personnalisées et classes utilisateur
- Définitions d'options personnalisées
- Valeurs d'option au niveau du serveur
- Stratégies au niveau du serveur
- Filtres d'adresses MAC
- Paramètres de détection de conflit personnalisés

Ces paramètres au niveau du serveur doivent également être importés vers le nouveau serveur partenaire de basculement DHCP (DHCP-2025-2) avec la même procédure.

> ⓘ **Notes**
>
> Le paramètre **–BackupPath** est utilisé pour spécifier un chemin d'accès dans lequel la base de données du serveur DHCP actuel est sauvegardée avant d'apporter des modifications

de configuration dans le cadre de l'opération d'importation. Pour restaurer l'opération d'importation, utilisez l'applet de commande Restore-DhcpServer et spécifiez **C :\backup** pour la valeur du paramètre **-Path** .

> ⓘ **Important**
>
> Vérifiez que les options et les paramètres sur DHCP-2025-1 sont corrects avant de continuer.

Importer des paramètres DHCP sur un nouveau serveur partenaire de basculement

Suivez les étapes pour importer les paramètres DHCP dans DHCP-2025-2.

1. À une invite de commandes Windows PowerShell avec des droits élevés, entrez les commandes suivantes :

   PowerShell

   ```
   Import-DhcpServer –ComputerName DHCP-2025-2 –File C:\export\DHCP-2022-1exp.xml -BackupPath C:\backup\ -ServerConfigOnly -Verbose -Force
   ```

Configurer le basculement DHCP entre DHCP-2022-1 et DHCP-2025-1

Ensuite, configurez le basculement DHCP pour les étendues souhaitées sur DHCP-2022-1, en indiquant DHCP-2025-1 comme serveur partenaire de basculement. Pour connaître les procédures de configuration du basculement DHCP à l'aide de PowerShell ou de la console DHCP, consultez Configurer le basculement DHCP.

Cette étape réplique les étendues et les baux vers DHCP-2025-1 en préparation de la mise en mode hors ligne de DHCP-2022-1.

Supprimer la relation de basculement DHCP sur DHCP-2025-1

Supprimez la relation de basculement DHCP sur DHCP-2025-1.

PowerShell

1. Dans une invite Windows PowerShell élevée sur DHCP-2025-1, entrez la commande suivante :

   PowerShell

   ```
   Remove-DhcpServerv4Failover -Name DHCP-2022-1-DHCP-2025-1
   ```

   Dans la procédure précédente, remplacez *DHCP-2022-1-DHCP-2025-1* par le nom de la relation de basculement DHCP que vous avez créée dans la procédure précédente.

2. Tapez la commande suivante, puis appuyez sur Entrée :

   PowerShell

   ```
   Get-DhcpServerv4Failover
   ```

   Vérifiez que le nom de la relation de basculement DHCP n'est pas affiché dans la sortie de la commande, ce qui indique qu'il est supprimé avec succès.

> **Notes**
>
> Les étendues DHCP ajoutées à la relation de basculement SONT supprimées du serveur DHCP partenaire. Les étendues restent sur le serveur où vous avez entré la commande Remove-DhcpServerv4Failover (DHCP-2025-1 dans cette procédure).

Configurer le basculement DHCP entre DHCP-2025-1 et DHCP-2025-2

Ensuite, configurez le basculement DHCP pour toutes les étendues souhaitées sur DHCP-2025-1, en désignant DHCP-2025-2 comme serveur partenaire de basculement. Pour connaître les procédures de configuration du basculement DHCP à l'aide de PowerShell ou de la console DHCP, consultez Configurer le basculement DHCP.

Mettre à jour les agents de relais DHCP et terminer la migration

Enfin, mettez à jour les agents de relais DHCP pour utiliser les nouveaux serveurs DHCP et effectuer la migration DHCP.

Une fois les baux et les paramètres répliqués vers DHCP-2025-1 et DHCP-2025-2, les paramètres sont vérifiés et les relais DHCP sont mis à jour, vous pouvez arrêter le service serveur DHCP sur DHCP-2022-1 et DHCP-2022-2 afin que les nouveaux baux DHCP soient émis uniquement à partir de DHCP-2025-1 ou DHCP-2025-2.

Contenu connexe

- Vue d'ensemble du basculement DHCP
- Gérer les relations de basculement DHCP

Migrer vers le mécanisme de basculement DHCP

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Ce guide fournit des conseils pour la migration de votre déploiement de serveur DHCP existant vers une configuration de basculement DHCP dans Windows Server. Que vous effectuez une transition à partir d'une configuration DHCP fractionnée ou en cluster, ce document décrit les étapes nécessaires pour garantir une migration fluide.

Prerequisites

- Le rôle serveur DCHP est installé sur les deux serveurs DHCP utilisés pour configurer la relation de basculement. Pour installer le rôle serveur DHCP, suivez les étapes décrites dans Installer et configurer le serveur DHCP.
- Un serveur DHCP existant configuré et en cours d'exécution.

Exporter les paramètres et les baux DHCP

Si vous utilisez DHCP en cluster, vous devez uniquement exporter les paramètres DHCP à partir du serveur DHCP actuellement actif. Procédez comme suit pour le serveur DHCP actif et le serveur de sauvegarde uniquement si vous utilisez une conception à étendue fractionnée et que vous devez répliquer des baux DHCP à partir des deux serveurs DHCP.

> ⓘ **Important**
>
> Vous ne pouvez pas importer de baux DHCP pour la même étendue à partir de deux serveurs DHCP différents. Vous devez consolider les fichiers exportés dans un seul fichier.

Exporter les paramètres et les baux DHCP

1. Sur le serveur DHCP qui sera utilisé pour configurer initialement le basculement DHCP, **dhcp-failover-server.contoso.com**, ouvrez une invite Windows PowerShell avec élévation de privilèges, tapez les commandes suivantes, puis appuyez sur Entrée :

   ```
   PowerShell
   ```

```
    mkdir C:\export
    mkdir C:\backup
    Export-DhcpServer -ComputerName "dhcp-server.contoso.com" -File
"C:\exportdir\dhcpexport.xml"
```

Cet exemple exporte toutes les configurations du serveur DHCP, DHCPv4 et DHCPv6, y compris les étendues présentes sur le service serveur DHCP vers le fichier d'exportation spécifié au format de fichier XML.

2. Si nécessaire, effectuez à nouveau l'étape d'exportation en spécifiant un nom d'ordinateur de **dhcp-server-2.contoso.com** et en exportant vers le fichier **C:\exportdir\dhcpexport2.xml**. Lorsque vous avez terminé, vous disposez d'un fichier XML pour chaque serveur DHCP qui a des baux que vous souhaitez importer dans **dhcp-failover-server.contoso.com**.

3. Si vous avez plusieurs fichiers qui contiennent des baux pour le même ID d'étendue, ces fichiers doivent être consolidés avant d'importer des données dans **dhcp-failover-server.contoso.com**.

Importer les paramètres et les baux DHCP sur le serveur de basculement DHCP

Avant d'effectuer cette procédure, vérifiez que vous avez consolidé et enregistré des baux et des paramètres à partir de vos serveurs DHCP actuels dans un fichier sur le nouveau serveur DHCP. La procédure suivante suppose que les paramètres et les baux DHCP sont enregistrés dans le fichier **C:\export\dhcpexport.xml** sur un serveur DHCP avec un nom d'hôte de **dhcp-failover-server.contoso.com**.

Importer les paramètres et les baux DHCP

- À l'invite de commandes élevée de Windows PowerShell, tapez les commandes suivantes, puis appuyez sur Entrée :

  PowerShell

  ```
  Import-DhcpServer -ComputerName "dhcp-failover-server.contoso.com" -File
  "C:\exports\dhcpexport.xml" -BackupPath "C:\dhcpbackup\"
  ```

  Cet exemple importe les données de configuration dans le fichier spécifié sur le service de serveur de basculement DHCP nommé **dhcp-failover-server.contoso.com**. Le fichier peut contenir des données de configuration DHCPv4 et DHCPv6.

Par défaut, toutes les étendues sont importées. Une étendue ne sera pas importée si elle existe déjà sur le serveur de destination. Pour spécifier uniquement certaines étendues pour l'importation, utilisez le paramètre **–ScopeId** . Par exemple:

PowerShell

```
Import-DhcpServer -ComputerName "dhcp-failover-server.contoso.com" -File
"C:\exports\dhcpexport.xml" -BackupPath "C:\dhcpbackup\" -ScopeId
10.10.10.0,10.20.20.0
```

Cet exemple importe les données de configuration des étendues 10.10.10.0 et 10.20.20.0 à partir du fichier spécifié sur le service serveur DHCP qui s'exécute sur l'ordinateur nommé **dhcp-failover-server.contoso.com**. Si le fichier d'exportation contient des étendues en plus de 10.10.10.0 et 10.20.20.0, ces étendues sont ignorées. Les données de configuration au niveau du serveur DHCPv4, si elles sont présentes dans le fichier d'exportation, sont également importées sur le service de serveur DHCP.

> ⓘ **Important**
>
> Vérifiez que les options et les paramètres sur le serveur de basculement sont corrects avant de continuer. Les options telles que les serveurs DNS, les réservations ou les filtres peuvent également être mises à jour sur le serveur de basculement.

Importer des paramètres de niveau serveur vers le serveur partenaire de basculement DHCP

Procédez comme suit pour importer des paramètres au niveau du serveur de **dhcp-server.contoso.com** vers le serveur partenaire de basculement **dhcp-failover-server-2.contoso.com**.

Importer les paramètres au niveau du serveur

- À une invite Windows PowerShell avec élévation de privilèges sur le serveur partenaire de basculement, tapez les commandes suivantes, puis appuyez sur Entrée :

  PowerShell

  ```
  mkdir C:\dhcpbackup\
  Import-DhcpServer -ComputerName "dhcp-failover-server-2.contoso.com" -File
  "C:\exports\dhcpexport.xml" -BackupPath "C:\dhcpbackup\"
  ```

La base de données du serveur DHCP est sauvegardée localement sur le même serveur que celui sur lequel le service serveur DHCP s'exécute même si vous exécutez l'applet de commande **Import-DhcpServer** à distance.

Configurer le basculement DHCP

Ensuite, configurez le basculement DHCP pour certaines étendues sur **dhcp-failover-server.contoso.com**, en spécifiant **dhcp-failover-server-2.contoso.com** en tant que serveur partenaire de basculement. Pour connaître les étapes de configuration du basculement DHCP, consultez Configurer le basculement DHCP à l'aide de PowerShell ou du Gestionnaire de serveur.

Mettre à jour les agents de relais DHCP et terminer la migration

Enfin, mettez à jour les agents de relais DHCP pour utiliser les nouveaux serveurs DHCP et effectuer la migration DHCP.

Une fois les baux et les paramètres importés sur les serveurs de basculement DHCP, les paramètres sont vérifiés et les relais DHCP sont mis à jour, la migration est terminée. Vous pouvez arrêter le service serveur DHCP sur **dhcp-server.contoso.com** et **dhcp-server-2.contoso.com** afin que les nouveaux baux DHCP soient émis uniquement à partir des serveurs de basculement DHCP.

Contenu connexe

- Vue d'ensemble du basculement DHCP
- Gérer les relations de basculement DHCP

Répliquer le basculement DHCP

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

La réplication est le processus de copie des paramètres d'une ou plusieurs étendues DHCP avec basculement sur un serveur DHCP vers le serveur du partenaire de basculement.

Trois types de réplication sont disponibles :

- **Réplication du serveur** : ce type de réplication copie la configuration de toutes les étendues activées pour le basculement sur le serveur local vers ses serveurs partenaires de basculement.
- **Réplication de relation** : ce type de réplication copie la configuration de toutes les étendues DHCP qui font partie d'une relation de basculement sélectionnée vers le serveur partenaire de basculement.
- **Réplication de l'étendue** : ce type de réplication copie la configuration d'une étendue DHCP sélectionnée vers le serveur partenaire de basculement.

Suivez les étapes pour le type de réplication que vous souhaitez effectuer, à l'aide de la console DHCP ou de Windows PowerShell.

Prerequisites

- Au moins Windows Server 2012
- Le rôle serveur DHCP est installé
- Un travail de relations de basculement existant existe
- L'appartenance au groupe **Administrateurs** ou équivalent est la condition minimale requise pour effectuer ces procédures.

> ⓘ **Important**
>
> La réplication peut être lancée à partir de chaque DHCP dans une relation de basculement. Les paramètres du serveur partenaire de basculement sont remplacés par les paramètres configurés sur le serveur où la réplication est lancée. Par conséquent, il est important de toujours s'assurer que la réplication est lancée sur le serveur configuré avec les paramètres que vous souhaitez utiliser.

Répliquer les paramètres de basculement au niveau du serveur

Pour répliquer les paramètres de basculement au niveau du serveur, procédez comme suit.

Console DHCP

1. Sur un serveur DHCP, ouvrez le Gestionnaire de serveur, sélectionnez **Outils**, **puis DHCP.**
2. Dans la console DHCP, cliquez avec le bouton droit sur **IPv4**, puis sélectionnez **Répliquer les étendues de basculement**.
3. Sélectionnez **OK** dans l'alerte qui s'affiche.
4. Dans la boîte de dialogue **Réplication de configuration de l'étendue de basculement** , vérifiez que la réplication a réussi, puis sélectionnez **Fermer**.

Répliquer les paramètres de basculement au niveau de la relation

Pour répliquer les paramètres de basculement au niveau de la relation, procédez comme suit.

Console DHCP

1. Sur un serveur DHCP, ouvrez le Gestionnaire de serveur, sélectionnez **Outils**, **puis DHCP.**
2. Dans la console DHCP, cliquez avec le bouton droit sur toute étendue avec fonctionnalité de basculement, puis sélectionnez **Répliquer la relation de basculement**.
3. Sélectionnez **OK** dans l'alerte qui s'affiche.
4. Dans la boîte de dialogue **Réplication de configuration de l'étendue de basculement** , vérifiez que la réplication a réussi, puis sélectionnez **Fermer**.

Répliquer les paramètres de basculement au niveau de l'étendue

Pour répliquer les paramètres de basculement au niveau de l'étendue, procédez comme suit :

Console DHCP

1. Sur un serveur DHCP, ouvrez le Gestionnaire de serveur, sélectionnez **Outils**, **puis DHCP.**
2. Dans la console DHCP, cliquez avec le bouton droit sur n'importe quelle étendue avec basculement activé, puis sélectionnez **Répliquer l'étendue**.
3. Dans la boîte de dialogue **Réplication de configuration de l'étendue de basculement** , vérifiez que la réplication a réussi, puis sélectionnez **Fermer**.

Contenu connexe

- Vue d'ensemble du basculement DHCP

Evénements de basculement DHCP dans Windows Server

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Windows Server dispose de compteurs de performances et de journalisation des événements pour prendre en charge la surveillance et la résolution des problèmes pour le basculement DHCP. Les événements de basculement DHCP sont également enregistrés dans le journal d'audit DHCP.

Dans le basculement DHCP, les messages clients qui sont diffusés sont reçus par les deux serveurs de basculement DHCP. Toutefois, un seul serveur répond aux messages clients. En mode équilibreur de charge, les serveurs hachent l'adresse MAC d'un client DHCP pour établir lequel d'entre eux doit répondre. En mode de secours à chaud, seul le serveur actif répond. Dans les deux cas, le serveur DHCP qui ne répond pas au client enregistre ce message dans le journal d'audit.

Canaux d'événements de serveur DHCP pour le basculement DHCP

Les canaux d'événements du serveur DHCP suivants sont disponibles à l'aide de l'Observateur d'événements avec le chemin d'accès : **applications et journaux des services\Microsoft\Windows\DHCP-Server**. Il existe deux canaux d'événements dans lesquels vous pouvez afficher les événements de basculement DHCP.

- **Canal d'administration** (Microsoft-Windows-DHCP Server Events/Admin) : ce canal fournit la journalisation des événements d'administration du serveur DHCP. Par exemple, les événements sont enregistrés dans ce canal si un état de basculement DHCP d'un serveur change.
- **Canal opérationnel** (Microsoft-Windows-DHCP Server Events/Operational) : ce canal fournit un audit de configuration DHCP. Par exemple, un événement est enregistré si une étendue sur le serveur DHCP est ajoutée ou supprimée d'une relation de basculement DHCP.

Journalisation des événements d'administration

Les événements du Suivi des événements pour Windows (ETW) sont enregistrés pour le changement d'état du serveur local ou de son serveur partenaire. Ces événements sont enregistrés sur le canal **d'administration** du serveur DHCP. Les données suivantes sont fournies dans le cadre de chaque événement de modification d'état.

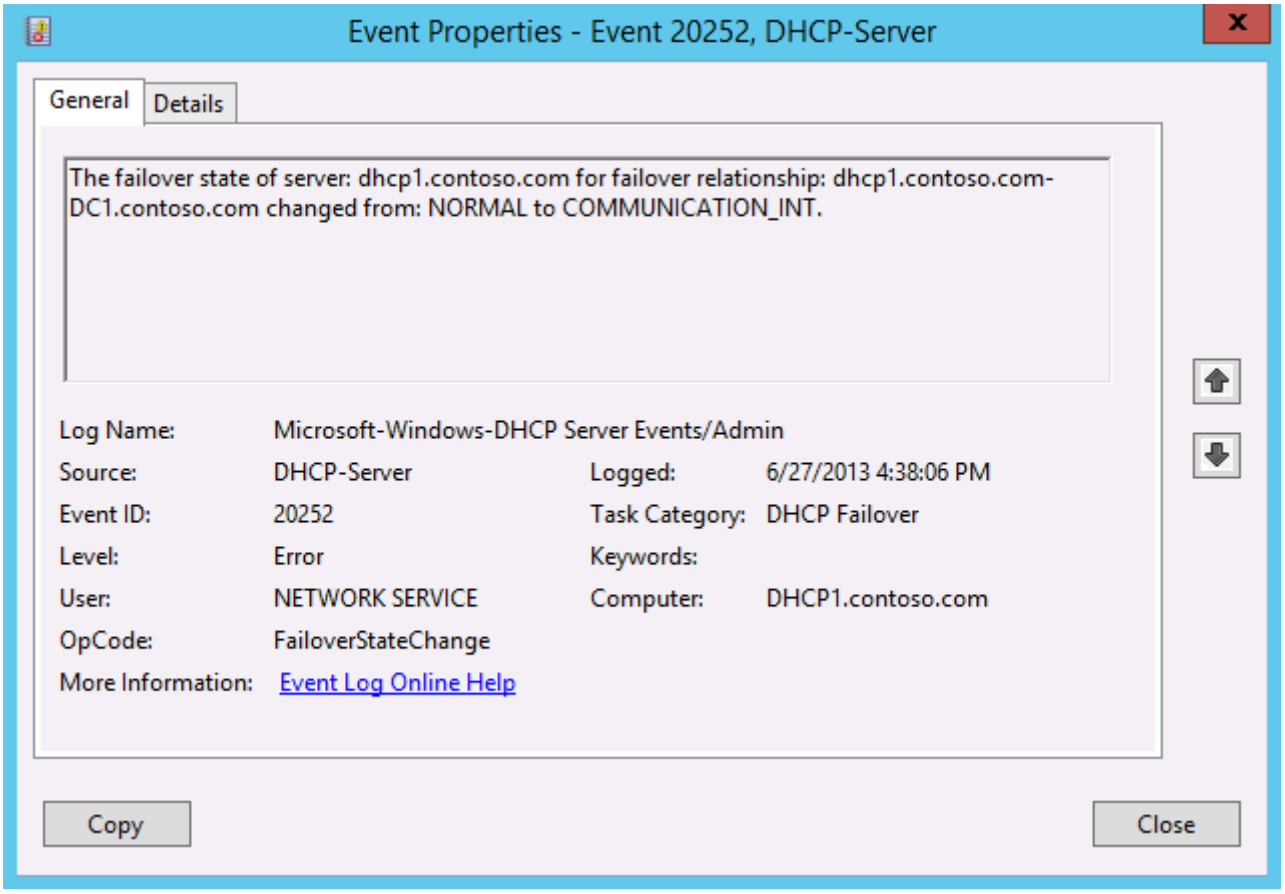
- État précédent du serveur.
- État actuel du serveur.
- Nom de la relation de basculement.
- Nom d'hôte du serveur ou adresse IP.

Outre la journalisation de sa propre modification d'état, le serveur enregistre les modifications dans l'état de son serveur partenaire de basculement. Ces informations sont communiquées par les messages d'état du partenaire de basculement. Le tableau suivant répertorie les valeurs remplies pour les différents champs du journal des événements.

Agrandir le tableau

Champ d'événement	**Value**
ID de l'événement	20252 (exemple d'ID)
Date et heure	Heure du changement d'état
Computer	Nom d'hôte du serveur DHCP ou adresse IP
User	SERVICE RÉSEAU
Description	État de basculement du serveur : `<host name>` pour la relation de basculement : `<relationship name>` passe de : `<previous state>` à `<current state>`. L'adresse IP du serveur ou le nom d'hôte correspond au serveur qui a changé d'état. Il peut s'agir du nom d'hôte ou de l'adresse IP du serveur DHCP local ou du partenaire de basculement. Si l'état précédent du serveur n'est pas connu, la description suivante s'affiche pour l'événement : État de basculement du serveur : `<host name>` pour la relation de basculement modifiée en `<current state>`.
OpCode	FailoverStateChange
Catégorie de tâche	Basculement DHCP
Level	- Erreur : En cas de transition hors de l'état NORMAL ou d'entrée dans l'état PARTNER DOWN. - Informations : En cas de transition vers l'état NORMAL. - Avertissement : pour les transitions entre d'autres états.

Consultez l'exemple d'événement suivant.



Le type de données d'événement suivant est journalisé lorsqu'un serveur détecte qu'il n'est pas en synchronisation temporelle avec son serveur partenaire.

Agrandir le tableau

Champ d'événement	Value
ID de l'événement	20253
Date et heure	Heure de détection du délai non synchronisé avec le serveur partenaire
Computer	Nom d'hôte du serveur DHCP
User	SERVICE RÉSEAU
Description	Le serveur a détecté qu'il n'est pas synchronisé avec le serveur partenaire : `<host name>` pour la relation de basculement : `<relationship name>`. Le délai d'attente est non synchronisé de : `<# of seconds>` secondes.
OpCode	TimeOutOfSync
Catégorie de tâche	Basculement DHCP

Champ d'événement	Value
Level	Error

Un événement est également enregistré lorsqu'une connexion est établie et qu'une connexion est perdue entre les partenaires de basculement DHCP.

Agrandir le tableau

Level	Opcode	Catégorie de tâche	Description
Error	CommDown	Basculement DHCP	Le serveur a perdu le contact avec le serveur partenaire de basculement : `<host name>` pour la relation : `<relationship name>`.
Information	CommUp	Basculement DHCP	Le serveur a établi un contact avec le serveur partenaire de basculement : `<host name>` pour la relation : `<relationship name>`.

Journalisation des événements opérationnels

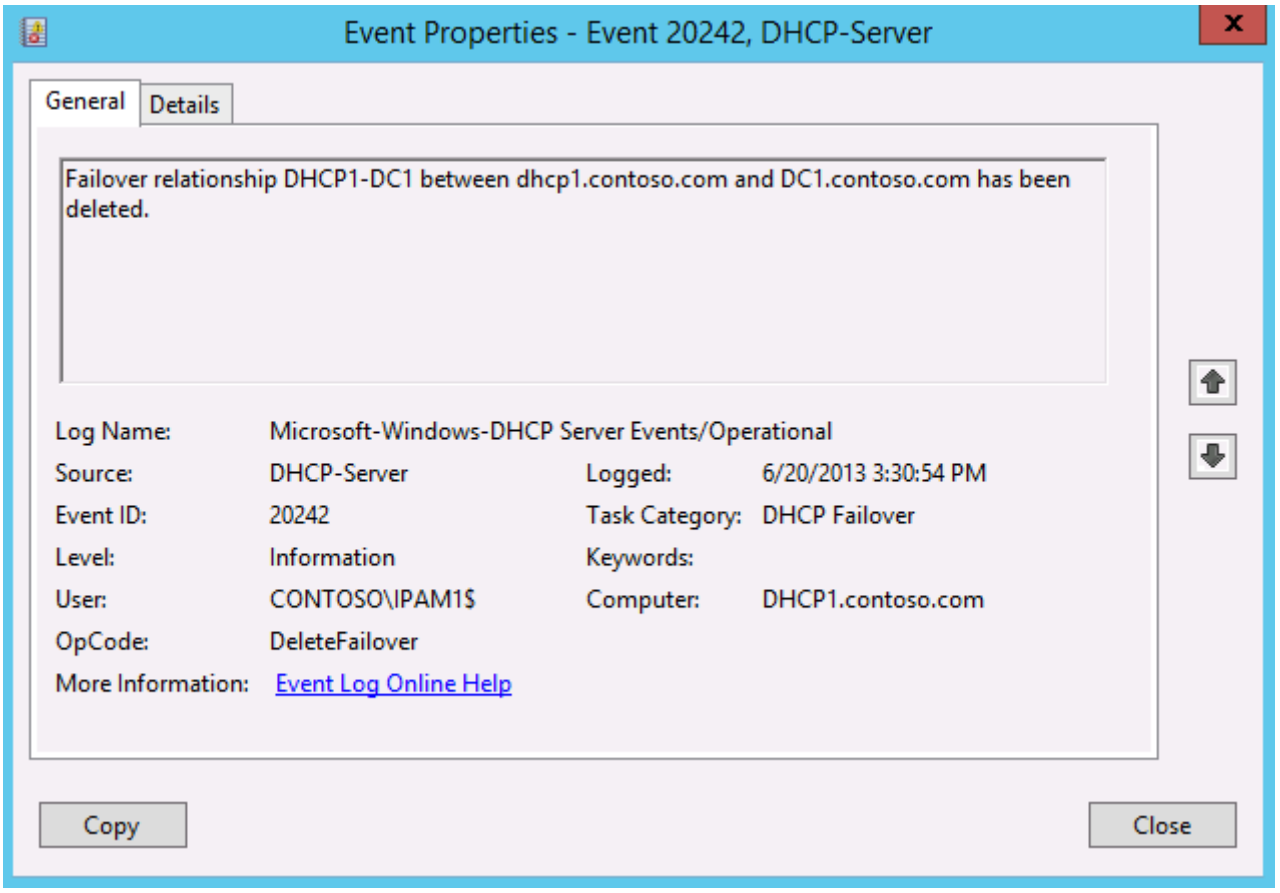
Les événements d'audit de configuration au niveau des informations suivants sont enregistrés sur le canal **opérationnel** du serveur DHCP.

Agrandir le tableau

Type d'événement	OpCode	Description
Création d'une relation de basculement	CreateFailover	Une relation de basculement est créée entre les serveurs : `<host name>` et `<host name>` avec les paramètres de configuration suivants : Nom : Mode `<value>` : `<mode>`, Délai maximum du prospect du client : `<value>` secondes, pourcentage d'équilibrage de charge sur ce serveur/pourcentage d'adresse de réserve sur le serveur de secours : `<value>`, intervalle de basculement d'état automatique : `<value>` secondes en mode serveur de secours : `<host name>`
Suppression de la relation de basculement	DeleteFailover	La relation de basculement `<relationship name>` entre `<host name>` et `<host name>` est supprimée.

Type d'événement	OpCode	Description
Ajout d'une étendue à une relation de basculement existante	AddFailoverScope	L'étendue `<scope ID>` est ajoutée à la relation de basculement `<relationship name>` avec le serveur `<host name>`
Suppression de l'étendue d'une relation de basculement existante	RemoveFailoverScope	L'étendue `<scope ID>` est supprimée de la relation de basculement `<relationship name>` avec le serveur `<host name>`
Modifier MCLT	ChangeFailoverConfig	Le paramètre de configuration de basculement MCLT pour la relation de basculement `<relationship name>` avec le serveur `<host name>` est passé de `<old value>` secondes à `<new value>` secondes
Modifier l'intervalle de basculement d'état automatique	ChangeFailoverConfig	L'intervalle de basculement d'état automatique du paramètre de la relation de basculement `<relationship name>` avec le serveur `<host name>` passe de `<old value>` secondes à `<new value>` secondes.
Modifier le pourcentage d'adresses de réserve	ChangeFailoverConfig	Le paramètre de configuration du basculement Pourcentage de réserve d'adresses sur le serveur de secours pour la relation de basculement `<relationship name>` avec le serveur `<host name>` passe de `<old value>` à `<new value>`
Modifier le mode de relation de basculement	ChangeFailoverConfig	Le mode de paramètre de configuration de la relation de basculement `<relationship name>` avec le serveur `<host name>` passe de `<old value>` à `<new value>`
Modifier le pourcentage d'équilibrage de charge	ChangeFailoverConfig	Le pourcentage d'équilibrage de charge du paramètre de configuration de la relation de basculement `<relationship name>` avec le serveur `<host name>` passe de `<old value>` à `<new value>` sur ce serveur.

Consultez l'exemple d'événement suivant.



Compteurs de performance

Windows Server dispose des compteurs de performances liés au basculement DHCP suivants pour les compteurs de serveur DHCP :

- Rapports de liaison envoyés par minute
- Rapports de liaison reçus par minute
- Liaison d'accusés de réception reçus par minute
- Liaison d'accusés de réception envoyés par minute
- Nombre de mises à jour de liaison sortante en attente sur ce serveur
- Nombre de transitions dans l'état COMMUNICATION INTERRUPTED
- Nombre de transitions dans l'état PARTNER DOWN
- Nombre de transitions dans l'état RECOVER
- Nombre de files d'attente de mise à jour de la liaison fonctionnant à 90 % de la taille maximale de la file d'attente
- Nombre de mises à jour de la liaison supprimées

Contenu connexe

- Vue d’ensemble du basculement DHCP
- Événements de serveur DHCP

Guide de résolution des problèmes de protocole DHCP (Dynamic Host Configuration Protocol)

16/08/2025

Pour tout appareil (tel qu'un ordinateur ou un téléphone) pouvant fonctionner dans un réseau, il doit être affecté à une adresse IP. Vous pouvez affecter une adresse IP manuellement ou automatiquement. L'attribution automatique est gérée par le service DHCP (Microsoft ou un serveur tiers).

Dans cet article, nous aborderons les étapes de dépannage générales du client et du serveur DHCP Microsoft IPv4.

Plus d'informations

La procédure pour l'attribution d'adresses IPv4 implique généralement trois composants principaux :

- Un appareil client DHCP qui doit obtenir une adresse IP
- Un service DHCP qui fournit des adresses IP au client en fonction de paramètres spécifiques
- Un agent de relais DHCP/Assistance IP pour envoyer des demandes de diffusion DHCP à un autre segment réseau

Une communication client à serveur DHCP se compose de trois types d'interaction entre les deux homologues :

- **DORA basé sur la diffusion** (Découverte, Offre, Demande, Accusé de réception). Le processus se déroule comme suit :
    - Le client DHCP envoie une demande de diffusion DHCP Discover à tous les serveurs DHCP disponibles dans la plage.
    - Une réponse de diffusion de l'offre DHCP est reçue du serveur DHCP, offrant un bail d'adresse IP disponible.
    - La demande de diffusion du client DHCP demande le bail d'adresse IP proposée et l'accusé de réception de diffusion DHCP à la fin.

    - Si le client et le serveur DHCP se trouvent dans différents segments de réseau logique, un agent de relais DHCP agit comme un redirecteur, en envoyant les paquets de diffusion DHCP entre homologues.

- **Demandes de renouvellement DHCP unicast** : celles-ci sont envoyées directement au serveur DHCP à partir du client DHCP pour renouveler l'attribution d'adresse IP après 50 % de la durée du bail d'adresse IP.

- **Requêtes de redéfinition DHCP** : elles sont envoyées à tous les serveurs DHCP à portée du client. Celles-ci sont envoyées après 87,5 % de la durée du bail d'adresse IP, car cela indique que la demande de monodiffusion dirigée n'a pas fonctionné. Comme pour le processus DORA, ce processus implique une communication de l'agent de relais DHCP.

Si un client DHCP Microsoft ne reçoit pas d'adresse IPv4 DHCP valide, le client est probablement configuré pour utiliser une adresse APIPA. Pour plus d'informations, consultez l'article suivant de la Base de connaissances : 220874 Comment utiliser l'adressage TCP/IP automatique sans serveur DHCP

Toutes les communications sont effectuées sur les ports UDP 67 et 68. Pour plus d'informations, consultez l'article suivant de la Base de connaissances : 169289 principes de base du protocole DHCP (Dynamic Host Configuration Protocol).

Principes de base du protocole DHCP (Dynamic Host Configuration Protocol)

16/08/2025

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole standard défini par RFC 1541 (qui est remplacé par RFC 2131) qui permet à un serveur de distribuer dynamiquement l'adressage IP et les informations de configuration aux clients. Normalement, le serveur DHCP fournit au client au moins ces informations de base :

- Adresse IP
- Masque de sous-réseau
- Passerelle par défaut

D'autres informations peuvent également être fournies, telles que les adresses de serveur DNS (Domain Name Service) et les adresses du serveur WINS (Windows Internet Name Service). L'administrateur système configure le serveur DHCP avec les options qui sont fournies au client après traitement.

Plus d'informations

Les produits Microsoft suivants fournissent des fonctionnalités client DHCP :

- Windows NT Server versions 3.5, 3.51 et 4.0
- Windows NT Workstation versions 3.5, 3.51 et 4.0
- Windows 95
- Microsoft Network Client version 3.0 pour MS-DOS
- Client Microsoft LAN Manager version 2.2c pour MS-DOS
- Microsoft TCP/IP-32 pour Windows for Workgroups versions 3.11, 3.11a et 3.11b

Différents clients DHCP prennent en charge différentes options qu'ils peuvent recevoir du serveur DHCP.

Les systèmes d'exploitation microsoft server suivants fournissent des fonctionnalités de serveur DHCP :

- Windows NT Server version 3.5

- Windows NT Server version 3.51
- Windows NT Server version 4.0

Lorsqu'un client est initialisé pour la première fois après qu'il a été configuré pour recevoir des informations DHCP, il lance une conversation avec le serveur.

Vous trouverez ci-dessous un tableau récapitulatif de la conversation entre le client et le serveur, suivi d'une description au niveau du paquet du processus :

```
Source Dest Source Dest Packet
 MAC addr MAC addr IP addr IP addr Description
 ----------------------------------------------------------------
 Client Broadcast 0.0.0.0 255.255.255.255 DHCP Discover
 DHCPsrvr Broadcast DHCPsrvr 255.255.255.255 DHCP Offer
 Client Broadcast 0.0.0.0 255.255.255.255 DHCP Request
 DHCPsrvr Broadcast DHCPsrvr 255.255.255.255 DHCP ACK
```

La conversation détaillée entre le client DHCP et le serveur DHCP est la suivante :

DHCPDISCOVER

Le client envoie un paquet DHCPDISCOVER. Voici un extrait d'une capture de moniteur réseau montrant les parties IP et DHCP d'un paquet DHCPDISCOVER. Dans la section IP, vous pouvez voir que l'adresse de destination est 255.255.255.255 et que l'adresse source est 0.0.0.0. La section DHCP identifie le paquet comme un paquet de découverte et identifie le client à deux endroits à l'aide de l'adresse MAC de la carte réseau. Notez les valeurs dans le champ CHADDR et le champ DHCP : Identificateur du client sont identiques.

```
IP: ID = 0x0; Proto = UDP; Len: 328
 IP: Version = 4 (0x4)
 IP: Header Length = 20 (0x14)
 IP: Service Type = 0 (0x0)
 IP: Precedence = Routine
 IP: ...0.... = Normal Delay
 IP: ....0... = Normal Throughput
 IP: .....0.. = Normal Reliability
 IP: Total Length = 328 (0x148)
 IP: Identification = 0 (0x0)
 IP: Flags Summary = 0 (0x0)
 IP: .......0 = Last fragment in datagram
 IP: ......0. = May fragment datagram if necessary
 IP: Fragment Offset = 0 (0x0) bytes
```

```
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x39A6
  IP: Source Address = 0.0.0.0
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)

 DHCP: Discover (xid=21274A1D)
  DHCP: Op Code (op) = 1 (0x1)
  DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
  DHCP: Hardware Address Length (hlen) = 6 (0x6)
  DHCP: Hops (hops) = 0 (0x0)
  DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
  DHCP: Seconds (secs) = 0 (0x0)
  DHCP: Flags (flags) = 0 (0x0)
  DHCP: 0............... = No Broadcast
  DHCP: Client IP Address (ciaddr) = 0.0.0.0
  DHCP: Your IP Address (yiaddr) = 0.0.0.0
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay IP Address (giaddr) = 0.0.0.0
  DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
  DHCP: Server Host Name (sname) = <Blank>
  DHCP: Boot File Name (file) = <Blank>
  DHCP: Magic Cookie = [OK]
  DHCP: Option Field (options)
  DHCP: DHCP Message Type = DHCP Discover
  DHCP: Client-identifier = (Type: 1) 08 00 2b 2e d8 5e
  DHCP: Host Name = JUMBO-WS
  DHCP: Parameter Request List = (Length: 7) 01 0f 03 2c 2e 2f 06
  DHCP: End of this option field
```

DHCPOFFER

Le serveur DHCP répond en envoyant un paquet DHCPOFFER. Dans la section IP de l'extrait de capture ci-dessous, l'adresse source est désormais l'adresse IP du serveur DHCP et l'adresse de destination est l'adresse de diffusion 255.255.255.255. La section DHCP identifie le paquet en tant qu'offre. Le champ YIADDR est rempli avec l'adresse IP que le serveur offre au client. Notez que le champ CHADDR contient toujours l'adresse physique du client demandeur. En outre, nous voyons dans la section Champ d'option DHCP les différentes options envoyées par le serveur, ainsi que l'adresse IP. Dans ce cas, le serveur envoie le masque de sous-réseau, la passerelle par défaut (routeur), le délai de bail, l'adresse du serveur WINS (service de nom NetBIOS) et le type de nœud NetBIOS.

```
 IP: ID = 0x3C30; Proto = UDP; Len: 328
  IP: Version = 4 (0x4)
```

```
  IP: Header Length = 20 (0x14)
  IP: Service Type = 0 (0x0)
  IP: Precedence = Routine
  IP: ...0.... = Normal Delay
  IP: ....0... = Normal Throughput
  IP: .....0.. = Normal Reliability
  IP: Total Length = 328 (0x148)
  IP: Identification = 15408 (0x3C30)
  IP: Flags Summary = 0 (0x0)
  IP: .......0 = Last fragment in datagram
  IP: ......0. = May fragment datagram if necessary
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x2FA8
  IP: Source Address = 157.54.48.151
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)

 DHCP: Offer (xid=21274A1D)
  DHCP: Op Code (op) = 2 (0x2)
  DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
  DHCP: Hardware Address Length (hlen) = 6 (0x6)
  DHCP: Hops (hops) = 0 (0x0)
  DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
  DHCP: Seconds (secs) = 0 (0x0)
  DHCP: Flags (flags) = 0 (0x0)
  DHCP: 0............... = No Broadcast
  DHCP: Client IP Address (ciaddr) = 0.0.0.0
  DHCP: Your IP Address (yiaddr) = 157.54.50.5
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay IP Address (giaddr) = 0.0.0.0
  DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
  DHCP: Server Host Name (sname) = <Blank>
  DHCP: Boot File Name (file) = <Blank>
  DHCP: Magic Cookie = [OK]
  DHCP: Option Field (options)
  DHCP: DHCP Message Type = DHCP Offer
  DHCP: Subnet Mask = 255.255.240.0
  DHCP: Renewal Time Value (T1) = 8 Days, 0:00:00
  DHCP: Rebinding Time Value (T2) = 14 Days, 0:00:00
  DHCP: IP Address Lease Time = 16 Days, 0:00:00
  DHCP: Server Identifier = 157.54.48.151
  DHCP: Router = 157.54.48.1
  DHCP: NetBIOS Name Service = 157.54.16.154
  DHCP: NetBIOS Node Type = (Length: 1) 04
  DHCP: End of this option field
```

DHCPREQUEST

Le client répond au DHCPOFFER en envoyant un DHCPREQUEST. Dans la section IP de la capture ci-dessous, l’adresse source du client est toujours 0.0.0.0 et la destination du paquet est toujours 255.255.255.255.255. Le client conserve 0.0.0.0 car il n'a pas reçu de confirmation du serveur pour pouvoir commencer à utiliser l'adresse proposée. La destination est toujours diffusée, car plusieurs serveurs DHCP ont peut-être répondu et peuvent conserver une réservation pour une offre faite au client. Cela permet à ces autres serveurs DHCP de savoir qu’ils peuvent libérer leurs adresses proposées et les renvoyer à leurs pools disponibles. La section DHCP identifie le paquet en tant que requête et vérifie l’adresse proposée à l’aide du champ Dhcp : Adresse demandée. Le champ DHCP : Identificateur de serveur affiche l’adresse IP du serveur DHCP offrant le bail.

```
IP: ID = 0x100; Proto = UDP; Len: 328
 IP: Version = 4 (0x4)
 IP: Header Length = 20 (0x14)
 IP: Service Type = 0 (0x0)
 IP: Precedence = Routine
 IP: ...0.... = Normal Delay
 IP: ....0... = Normal Throughput
 IP: .....0.. = Normal Reliability
 IP: Total Length = 328 (0x148)
 IP: Identification = 256 (0x100)
 IP: Flags Summary = 0 (0x0)
 IP: .......0 = Last fragment in datagram
 IP: ......0. = May fragment datagram if necessary
 IP: Fragment Offset = 0 (0x0) bytes
 IP: Time to Live = 128 (0x80)
 IP: Protocol = UDP - User Datagram
 IP: Checksum = 0x38A6
 IP: Source Address = 0.0.0.0
 IP: Destination Address = 255.255.255.255
 IP: Data: Number of data bytes remaining = 308 (0x0134)

DHCP: Request (xid=21274A1D)
 DHCP: Op Code (op) = 1 (0x1)
 DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
 DHCP: Hardware Address Length (hlen) = 6 (0x6)
 DHCP: Hops (hops) = 0 (0x0)
 DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
 DHCP: Seconds (secs) = 0 (0x0)
 DHCP: Flags (flags) = 0 (0x0)
 DHCP: 0............... = No Broadcast
 DHCP: Client IP Address (ciaddr) = 0.0.0.0
 DHCP: Your IP Address (yiaddr) = 0.0.0.0
 DHCP: Server IP Address (siaddr) = 0.0.0.0
 DHCP: Relay IP Address (giaddr) = 0.0.0.0
 DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
 DHCP: Server Host Name (sname) = <Blank>
 DHCP: Boot File Name (file) = <Blank>
```

```
 DHCP: Magic Cookie = [OK]
 DHCP: Option Field (options)
 DHCP: DHCP Message Type = DHCP Request
 DHCP: Client-identifier = (Type: 1) 08 00 2b 2e d8 5e
 DHCP: Requested Address = 157.54.50.5
 DHCP: Server Identifier = 157.54.48.151
 DHCP: Host Name = JUMBO-WS
 DHCP: Parameter Request List = (Length: 7) 01 0f 03 2c 2e 2f 06
 DHCP: End of this option field
```

DHCPACK

Le serveur DHCP répond à DHCPREQUEST avec un DHCPACK, ce qui termine le cycle d'initialisation. L'adresse source est l'adresse IP du serveur DHCP et l'adresse de destination est toujours 255.255.255.255. Le champ YIADDR contient l'adresse du client et les champs CHADDR et DHCP : les champs Identificateur du client sont l'adresse physique de la carte réseau dans le client demandeur. La section Option DHCP identifie le paquet en tant qu'ACK.

```
IP: ID = 0x3D30; Proto = UDP; Len: 328
 IP: Version = 4 (0x4)
 IP: Header Length = 20 (0x14)
 IP: Service Type = 0 (0x0)
 IP: Precedence = Routine
 IP: ...0.... = Normal Delay
 IP: ....0... = Normal Throughput
 IP: .....0.. = Normal Reliability
 IP: Total Length = 328 (0x148)
 IP: Identification = 15664 (0x3D30)
 IP: Flags Summary = 0 (0x0)
 IP: .......0 = Last fragment in datagram
 IP: ......0. = May fragment datagram if necessary
 IP: Fragment Offset = 0 (0x0) bytes
 IP: Time to Live = 128 (0x80)
 IP: Protocol = UDP - User Datagram
 IP: Checksum = 0x2EA8
 IP: Source Address = 157.54.48.151
 IP: Destination Address = 255.255.255.255
 IP: Data: Number of data bytes remaining = 308 (0x0134)

DHCP: ACK (xid=21274A1D)
 DHCP: Op Code (op) = 2 (0x2)
 DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
 DHCP: Hardware Address Length (hlen) = 6 (0x6)
 DHCP: Hops (hops) = 0 (0x0)
 DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
 DHCP: Seconds (secs) = 0 (0x0)
 DHCP: Flags (flags) = 0 (0x0)
```

```
  DHCP: 0............... = No Broadcast
  DHCP: Client IP Address (ciaddr) = 0.0.0.0
  DHCP: Your IP Address (yiaddr) = 157.54.50.5
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay IP Address (giaddr) = 0.0.0.0
  DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
  DHCP: Server Host Name (sname) = <Blank>
  DHCP: Boot File Name (file) = <Blank>
  DHCP: Magic Cookie = [OK]
  DHCP: Option Field (options)
  DHCP: DHCP Message Type = DHCP ACK
  DHCP: Renewal Time Value (T1) = 8 Days, 0:00:00
  DHCP: Rebinding Time Value (T2) = 14 Days, 0:00:00
  DHCP: IP Address Lease Time = 16 Days, 0:00:00
  DHCP: Server Identifier = 157.54.48.151
  DHCP: Subnet Mask = 255.255.240.0
  DHCP: Router = 157.54.48.1
  DHCP: NetBIOS Name Service = 157.54.16.154
  DHCP: NetBIOS Node Type = (Length: 1) 04
  DHCP: End of this option field
```

Si le client a déjà eu une adresse IP affectée PAR DHCP et qu'il est redémarré, le client demande spécifiquement l'adresse IP précédemment louée dans un paquet DHCPREQUEST spécial. L'adresse source est 0.0.0.0 et la destination est l'adresse de diffusion 255.255.255.255.255. Les clients Microsoft remplissent le champ d'option DHCP : Adresse demandée avec l'adresse précédemment affectée. Les clients strictement conformes à la RFC remplissent le champ CIADDR avec l'adresse demandée. Le serveur DHCP Microsoft accepte l'un ou l'autre.

```
 IP: ID = 0x0; Proto = UDP; Len: 328
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Service Type = 0 (0x0)
  IP: Precedence = Routine
  IP: ...0.... = Normal Delay
  IP: ....0... = Normal Throughput
  IP: .....0.. = Normal Reliability
  IP: Total Length = 328 (0x148)
  IP: Identification = 0 (0x0)
  IP: Flags Summary = 0 (0x0)
  IP: .......0 = Last fragment in datagram
  IP: ......0. = May fragment datagram if necessary
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x39A6
  IP: Source Address = 0.0.0.0
```

```
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)

 DHCP: Request (xid=2757554E)
  DHCP: Op Code (op) = 1 (0x1)
  DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
  DHCP: Hardware Address Length (hlen) = 6 (0x6)
  DHCP: Hops (hops) = 0 (0x0)
  DHCP: Transaction ID (xid) = 660034894 (0x2757554E)
  DHCP: Seconds (secs) = 0 (0x0)
  DHCP: Flags (flags) = 0 (0x0)
  DHCP: 0............... = No Broadcast
  DHCP: Client IP Address (ciaddr) = 0.0.0.0
  DHCP: Your IP Address (yiaddr) = 0.0.0.0
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay IP Address (giaddr) = 0.0.0.0
  DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
  DHCP: Server Host Name (sname) = <Blank>
  DHCP: Boot File Name (file) = <Blank>
  DHCP: Magic Cookie = [OK]
  DHCP: Option Field (options)
  DHCP: DHCP Message Type = DHCP Request
  DHCP: Client-identifier = (Type: 1) 08 00 2b 2e d8 5e
  DHCP: Requested Address = 157.54.50.5
  DHCP: Host Name = JUMBO-WS
  DHCP: Parameter Request List = (Length: 7) 01 0f 03 2c 2e 2f 06
  DHCP: End of this option field
```

À ce stade, le serveur peut ou non répondre. Le comportement du serveur DHCP Windows NT dépend de la version du système d'exploitation utilisée, ainsi que d'autres facteurs tels que le superscoping. Si le serveur détermine que le client peut toujours utiliser l'adresse, il reste silencieux ou ACK la DHCPREQUEST. Si le serveur détermine que le client ne peut pas avoir l'adresse, il envoie un NACK.

```
 IP: ID = 0x3F1A; Proto = UDP; Len: 328
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Service Type = 0 (0x0)
  IP: Precedence = Routine
  IP: ...0.... = Normal Delay
  IP: ....0... = Normal Throughput
  IP: .....0.. = Normal Reliability
  IP: Total Length = 328 (0x148)
  IP: Identification = 16154 (0x3F1A)
  IP: Flags Summary = 0 (0x0)
  IP: .......0 = Last fragment in datagram
  IP: ......0. = May fragment datagram if necessary
  IP: Fragment Offset = 0 (0x0) bytes
```

```
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x2CBE
  IP: Source Address = 157.54.48.151
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)

 DHCP: NACK (xid=74A005CE)
  DHCP: Op Code (op) = 2 (0x2)
  DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
  DHCP: Hardware Address Length (hlen) = 6 (0x6)
  DHCP: Hops (hops) = 0 (0x0)
  DHCP: Transaction ID (xid) = 1956644302 (0x74A005CE)
  DHCP: Seconds (secs) = 0 (0x0)
  DHCP: Flags (flags) = 0 (0x0)
  DHCP: 0............... = No Broadcast
  DHCP: Client IP Address (ciaddr) = 0.0.0.0
  DHCP: Your IP Address (yiaddr) = 0.0.0.0
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay IP Address (giaddr) = 0.0.0.0
  DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
  DHCP: Server Host Name (sname) = <Blank>
  DHCP: Boot File Name (file) = <Blank>
  DHCP: Magic Cookie = [OK]
  DHCP: Option Field (options)
  DHCP: DHCP Message Type = DHCP NACK
  DHCP: Server Identifier = 157.54.48.151
  DHCP: End of this option field
```

Le client commence ensuite le processus de découverte, mais le paquet DHCPDISCOVER tente toujours de louer la même adresse. Dans de nombreux cas, le client obtient la même adresse, mais peut-être pas.

```
 IP: ID = 0x100; Proto = UDP; Len: 328
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Service Type = 0 (0x0)
  IP: Precedence = Routine
  IP: ...0.... = Normal Delay
  IP: ....0... = Normal Throughput
  IP: .....0.. = Normal Reliability
  IP: Total Length = 328 (0x148)
  IP: Identification = 256 (0x100)
  IP: Flags Summary = 0 (0x0)
  IP: .......0 = Last fragment in datagram
  IP: ......0. = May fragment datagram if necessary
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
```

```
  IP: Checksum = 0x38A6
  IP: Source Address = 0.0.0.0
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)

 DHCP: Discover (xid=3ED14752)
  DHCP: Op Code (op) = 1 (0x1)
  DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
  DHCP: Hardware Address Length (hlen) = 6 (0x6)
  DHCP: Hops (hops) = 0 (0x0)
  DHCP: Transaction ID (xid) = 1053902674 (0x3ED14752)
  DHCP: Seconds (secs) = 0 (0x0)
  DHCP: Flags (flags) = 0 (0x0)
  DHCP: 0............... = No Broadcast
  DHCP: Client IP Address (ciaddr) = 0.0.0.0
  DHCP: Your IP Address (yiaddr) = 0.0.0.0
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay IP Address (giaddr) = 0.0.0.0
  DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
  DHCP: Server Host Name (sname) = <Blank>
  DHCP: Boot File Name (file) = <Blank>
  DHCP: Magic Cookie = [OK]
  DHCP: Option Field (options)
  DHCP: DHCP Message Type = DHCP Discover
  DHCP: Client-identifier = (Type: 1) 08 00 2b 2e d8 5e
  DHCP: Requested Address = 157.54.51.5
  DHCP: Host Name = JUMBO-WS
  DHCP: Parameter Request List = (Length: 7) 01 0f 03 2c 2e 2f 06
  DHCP: End of this option field
```

Les informations DHCP obtenues par le client à partir d'un serveur DHCP ont une durée de bail associée. Le délai de bail définit la durée pendant laquelle le client peut utiliser les informations affectées par DHCP. Lorsque le bail atteint certains jalons, le client tente de renouveler ses informations DHCP.

Pour afficher des informations IP sur un client Windows ou Windows for Workgroups, utilisez l'utilitaire IPCONFIG. Si le client est Windows 95, utilisez WINIPCFG.

références

Pour plus d'informations sur DHCP, consultez RFC1541 et RFC2131. Les RFC peuvent être obtenus via Internet sur de nombreux sites, par exemple : http://www.rfc-editor.org/ http://www.tech-nic.qc.ca/

Résoudre les problèmes sur le serveur DHCP

16/08/2025

Essayez notre agent virtuel : il peut vous aider à identifier et à résoudre rapidement les problèmes courants liés au protocole DHCP (Server Message Block).

Cet article explique comment résoudre les problèmes qui se produisent sur le serveur DHCP.

Liste de contrôle de résolution des problèmes

Vérifiez les paramètres suivants :

- Le service Serveur DHCP est démarré et en cours d'exécution. Pour vérifier ce paramètre, exécutez la `net start` commande et recherchez le **serveur DHCP**.
- Le serveur DHCP est autorisé. Consultez Autorisation de serveur DHCP Windows dans un scénario de jonction à un domaine.
- Vérifiez que les baux d'adresses IP sont disponibles dans l'étendue du serveur DHCP pour le sous-réseau sur lequel s'exécute le client DHCP. Pour vérifier la disponibilité, consultez la statistique de l'étendue appropriée dans la console d'administration du serveur DHCP.
- Vérifiez si des listes BAD_ADDRESS se trouvent dans Baux d'adresses.
- Vérifiez si les appareils du réseau ont des adresses IP statiques qui n'ont pas été exclues de l'étendue DHCP.
- Vérifiez que le serveur DHCP se lie à au moins une adresse IP et que cette adresse IP appartient au sous-réseau des étendues à partir desquelles les adresses IP doivent être louées, sauf si vous utilisez un relais DHCP. Pour effectuer cette vérification, exécutez l'applet de commande `Get-DhcpServerv4Binding` ou `Get-DhcpServerv6Binding`. Les liaisons de connexion au serveur sont configurées dans la console de gestion du serveur DHCP sous **Propriétés avancées IPv4/IPv6**.
- Vérifiez que seul le serveur DHCP écoute sur le port UDP 67 et 68 en exécutant la commande `netstat -anb`. Aucun autre processus ou autre service, tel que WDS ou PXE, ne doit occuper ces ports.
- Vérifiez que l'exemption IPsec du serveur DHCP a été ajoutée si vous êtes dans un environnement déployé par IPsec.

- Vérifiez que l'adresse IP de l'agent de relais peut faire l'objet d'une commande Ping à partir du serveur DHCP.
- Énumérez et vérifiez les stratégies et les filtres DHCP configurés.

Collecte de données

Journal du serveur DHCP

Les journaux de débogage du service de serveur DHCP fournissent des informations supplémentaires sur l'attribution du bail d'adresse IP et les mises à jour dynamiques DNS effectuées par le serveur DHCP. Par défaut, ces journaux sont stockés sous %windir%\System32\Dhcp. Pour plus d'informations, consultez Analyser les fichiers journaux du serveur DHCP.

Trace réseau

Une trace réseau de corrélation peut indiquer ce que le serveur DHCP faisait au moment où l'événement a été consigné. Pour créer une telle trace à l'aide des outils de résolution des problèmes Windows, suivez les instructions fournies dans les Conseils de dépannage DHCP - Collecte des données.

Voir aussi

- Instructions pour la résolution des problèmes DHCP
- Guide de résolution des problèmes de protocole DHCP (Dynamic Host Configuration Protocol)
- Introduction à l'ensemble d'outils TroubleShootingScript (TSS)

Événements de serveur DHCP

Article • 27/03/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local, versions 23H2 and 22H2

Le serveur DHCP journalise les événements pour toutes les modifications apportées. Dans cet article, découvrez où afficher les événements de serveur DHCP et voir l'ID, la catégorie et le texte de chaque événement.

Afficher les journaux des événements du serveur DHCP

Les journaux d'audit DHCP sont activés par défaut et n'affectent pas considérablement les performances du serveur DNS. Pour afficher les journaux d'événements du serveur DHCP :

1. Sélectionnez le bouton Démarrer, tapez Observateur d'événements, ouvrez l'Observateur d'événements à partir de la liste des correspondances les plus proches.
2. Dans l'Observateur d'événements, accédez à **Journaux des applications et des services**>**Microsoft**>**Windows**>**Serveur DHCP**.
3. Selon le type de problème, un événement est enregistré sur l'un des canaux d'événements suivants :

- événements opérationnels du serveur DHCP
- événements d'administration du serveur DHCP
- Événements système du serveur DHCP
- Événements de notification de filtre du serveur DHCP
- Événements d'audit du serveur DHCP

Événements opérationnels du serveur DHCP

Les événements opérationnels du serveur DHCP consignent les informations sur l'opération du serveur. Chaque fois qu'une étendue est modifiée, un événement est ajouté.

▼ Pour afficher tous les événements opérationnels du serveur, développez cette section.

Agrandir le tableau

ID d'événement	Catégorie d'événement	Texte de l'événement
70	DHCPv4.ScopeConfigured	Étendue : %1 pour IPv4 est configuré par %2.
71	DHCPv4.ScopeModified	Étendue : %1 pour IPv4 est modifié par %2.
72	DHCPv4.ScopeDeleted	Étendue : %1 pour IPv4 est supprimé par %2.
73	DHCPv4.ScopeActivated	Étendue : %1 pour IPv4 est activé par %2.
74	DHCPv4.ScopeDeActivated	Étendue : %1 pour IPv4 est désactivé par %2.
75	DHCPv4.ScopeLeaseUpdate	Étendue : %1 pour IPv4 est mis à jour avec la durée de bail de %2 secondes par %3. La durée de bail configurée précédente était : %4 secondes.
76	DHCPv4.ScopeOptionUpdate	Étendue : %1 pour IPv4 est mis à jour avec les paramètres d'option %2 par %3
77	DHCPv4.ScopeDNSEnable	Étendue : %1 pour IPv4 est activé pour les mises à jour dynamiques DNS par %2.
78	DHCPv4.ScopeDNSDisable	Étendue : %1 pour IPv4 est désactivé pour les mises à jour dynamiques DNS par %2.
79	DHCPv4.ScopeDNSUpdate_Req_by_Client	Étendue : %1 pour IPv4 est mise à jour avec les paramètres DNS par %2: pour mettre à jour dynamiquement les enregistrements DNS A et PTR à la demande des clients DHCP.
80	DHCPv4.ScopeDNSUpdate_Always	Étendue : %1 pour IPv4 est mis à jour avec les paramètres DNS par %2, ce qui permet de toujours mettre à jour dynamiquement les enregistrements DNS A et PTR.
81	DHCPv4.ScopeDNSEnable_Discard	Étendue : %1 pour IPv4 est activé pour les paramètres DNS par %2, ce qui permet d'ignorer les enregistrements DNS A et PTR lorsque le bail est supprimé.
82	DHCPv4.ScopeDNSDisable_Discard	Étendue : %1 pour IPv4 est désactivé pour les paramètres DNS par %2, ce qui permet d'ignorer les enregistrements DNS A et PTR lorsque le bail est supprimé.

ID d’événement	Catégorie d’événement	Texte de l’événement
83	DHCPv4.ScopeDNSEnable_Update_Client_NoReq	Étendue : %1 pour IPv4 est activé pour les paramètres DNS par %2: pour mettre à jour dynamiquement les enregistrements DNS A et PTR pour les clients DHCP qui ne demandent pas de mises à jour.
84	DHCPv4.ScopeDNSDisable_Update_Client_NoReq	Étendue : %1 pour IPv4 est désactivé pour les paramètres DNS par %2: pour mettre à jour dynamiquement les enregistrements DNS A et PTR pour les clients DHCP qui ne demandent pas de mises à jour.
85	DHCPv4.ScopePBA_Désactivé	L’affectation basée sur la politique a été désactivée pour l’étendue %1.
86	DHCPv4.ScopePBA_Activated	L’affectation basée sur la stratégie a été activée pour l’étendue %1.
87	DHCPv4.ScopeDHCIDEnable	Le paramètre de protection du nom est activé sur l'étendue %1 pour IPv4 par %2.
88	DHCPv4.ScopeDHCIDDisable	Le paramètre de protection du nom est désactivé sur l'étendue %1 pour IPv4 par %2.
89	DHCPv4.ScopeSupportType	Étendue : %1 pour IPv4 est mis à jour avec le type de support : %2 par %3. L’état configuré précédent était : %4.
90	DHCPv4.ScopeNAPEnabled	La contrainte de mise en conformité NAP est activée sur l'étendue %1 pour IPv4 par %2.
91	DHCPv4.ScopeNAPDisabled	La contrainte de mise en conformité NAP est désactivée sur l'étendue %1 pour IPv4 par %2.
92	DHCPv4.ScopeNAPProfileConfigured	Le profil NAP est configuré dans l’étendue %1 pour IPv4 avec le profil NAP suivant : %2 par %3.
93	DHCPv4.ScopeNAPProfileModified	Le profil NAP est mis à jour dans l’étendue %1 pour IPv4 avec le profil NAP suivant : %2 par %3. Le profil NAP configuré précédent était : %4.
94	DHCPv4.ScopeNAPProfileDeleted	Le profil NAP suivant : %1 est supprimé dans l'étendue %2 par %3.
95	DHCPv4.MulticastScopeConfigured	Étendue : %1 pour IPv4 de multidiffusion est configuré par %2.
96	DHCPv4.MulticastScopeDeleted	Étendue : %1 pour IPv4 de multidiffusion est supprimé par %2.
98	DHCPv4.SuperScopeConfigured	SuperScope : %1 pour IPv4 est configuré par %2.
99	DHCPv4.SuperScopeDeleted	SuperScope : %1 pour IPv4 est supprimé par %2.
100	DHCPv4.SuperScopeActivated	Étendue : %1 dans SuperScope : %2 pour IPv4 est activé par %3.
101	DHCPv4.SuperScopeDésactivé	Étendue : %1 dans SuperScope : %2 pour IPv4 est Désactivé par %3.
102	DHCPv4.SuperScopeDeleteTemp	Étendue : %1 pour IPv4 est supprimé dans l'étendue globale : %2 par %3. Toutefois, le Scope existe en dehors du Superscope.
1:03	DHCPv4.SuperScopeDeletePerm	Étendue : %1 pour IPv4 est supprimé dans l'étendue globale : %2 et supprimé définitivement par %3.
105	DHCPv4.ServerOptionUpdate	L’option de niveau serveur %1 pour IPv4 a été mise à jour par %2.
01:23:06 AM	DHCPv4.ReservationConfigured	Réservation : %1 pour IPv4 est configuré sous l'étendue %2 par %3.
107	DHCPv4.ReservationDeleted	Réservation : %1 pour IPv4 est supprimé sous l'étendue %2 par %3.
1:08	DHCPv4.ReservationDNSEnable	Réservation : %1 pour IPv4 sous l'étendue %2 est activé pour les mises à jour dynamiques DNS par %3.
109	DHCPv4.ReservationDNSDisable	Réservation : %1 pour IPv4 sous l'étendue %2 est désactivé pour les mises à jour dynamiques DNS par %3.
110	DHCPv4.ReservationDNSUpdate_Req_by_Client	Réservation : %1 pour IPv4 sous l'étendue %2 a été mis à jour avec les paramètres DNS par %3, ce qui permet de mettre à jour dynamiquement les enregistrements DNS A et PTR à la demande des clients DHCP.
01:23:11 AM	DHCPv4.ReservationDNSUpdate_Always	Réservation : %1 pour IPv4 sous l'étendue %2 a été mis à jour par %3 avec les paramètres DNS, ce qui permet de toujours mettre à jour dynamiquement les enregistrements DNS A et PTR.
112	DHCPv4.ReservationDNSEnable_Discard	Réservation : %1 pour IPv4 sous l'étendue %2 est activé pour les paramètres DNS par %3, ce qui permet d'ignorer les enregistrements DNS A et PTR lorsque le bail est supprimé.
113	DHCPv4.ReservationDNSDisable_Discard	Réservation : %1 pour IPv4 sous l'étendue %2 est désactivé pour les paramètres DNS par %3, ce qui permet d'ignorer les enregistrements DNS A et PTR lorsque le bail est

ID d'événement	Catégorie d'événement	Texte de l'événement
		supprimé.
114	DHCPv4.ReservationDNSEnableUpdate_No_Req_by_Client	Réservation : %1 pour IPv4 sous l'étendue %2 est activé pour les paramètres DNS par %3, ce qui permet la mise à jour dynamique des enregistrements DNS A et PTR pour les clients DHCP qui ne demandent pas de mises à jour.
115	DHCPv4.ReservationDNSDisableUpdate_No_Req_by_Client	Réservation : %1 pour IPv4 sous l'étendue %2 est désactivé pour les paramètres DNS par %3, ce qui permet la mise à jour dynamique des enregistrements DNS A et PTR pour les clients DHCP qui ne demandent pas de mises à jour.
116	DHCPv4.ReservationOptionUpdate	Réservation : %1 pour IPv4 sous l'étendue %2 est mis à jour avec le paramètre d'option %3 par %4.
117	DHCPv4.ServerPBA_DeActivated	L'affectation basée sur la stratégie a été désactivée au niveau du serveur.
1:18	DHCPv4.ServerPBA_Activated	L'attribution basée sur la stratégie a été activée au niveau du serveur.
01:19:48 AM	DHCPv4.ScopeExclusionAdded	Ajout de la plage d'adresses IP d'exclusion %1 dans le pool d'adresses pour IPv4 sous l'étendue %2 par %3.
01:20:21	DHCPv4.ScopeExclusionDeleted	Suppression de la plage d'adresses IP d'exclusion %1 dans le pool d'adresses pour IPv4 sous l'étendue %2 par %3.
121	DHCPv4.ScopeEnableAllow	Le filtrage basé sur la couche de liaison est activé dans la liste d'adresses autorisées d'IPv4 par %1
122	DHCPv4.ScopeDisableAllow	Le filtrage basé sur la couche de liaison est désactivé dans la liste d'adresses autorisées d'IPv4 par %1
123	DHCPv4.ScopeAllow_AddFilter	Filtre pour l'adresse physique %1, type de matériel %3 ajouté à la liste d'adresses autorisées d'IPv4 par %2.
124	DHCPv4.ScopeAllow_DeleteFilter	Filtre pour l'adresse physique : %1, type de matériel : %3 supprimé de la liste d'autorisation IPv4 par %2.
125	DHCPv4.ScopeEnableDeny	Le filtrage basé sur la couche de liens est activé dans la liste de blocs de l'IPv4 par %1
126	DHCPv4.ScopeDisableDeny	Le filtrage basé sur la couche de liens est désactivé dans la liste de blocs de l'IPv4 par %1
1:27	DHCPv4.ScopeDeny_AddFilter	Filtre pour l'adresse physique : %1, type de matériel : %3 ajouté à la liste de blocs IPv4 par %2.
128	DHCPv4.ScopeDeny_DeleteFilter	Filtre pour l'adresse physique : %1, type de matériel : %3 supprimé de la liste de blocs IPv4 par %2.
130	DHCPv6.ScopeDeleted	Étendue : %1 pour IPv6 est supprimé par %2.
131	DHCPv6.ScopeActivated	Étendue : %1 pour IPv6 est activé par %2.
1:32	DHCPv6.ScopeDeActivated	Étendue : %1 pour IPv6 est désactivé par %2.
133	DHCPv6.ScopeLeasePreferredUpdate	Étendue : %1 pour IPv6 est mis à jour avec la durée de vie préférée du bail %2 par %3. La durée de vie préférée de bail configurée précédemment était la suivante : %4.
1:34	DHCPv6.ScopeLeaseValidUpdate	Étendue : %1 pour IPv6 est mis à jour avec la durée de vie valide du bail %2 par %3. La durée de vie valide du bail précédemment configurée était la suivante : %4.
135	DHCPv6.ScopeOptionUpdate	Étendue : %1 pour IPv6 est mis à jour avec les paramètres d'option %2 par %3.
136	DHCPv6.ScopeDNSEnable	Étendue : %1 pour IPv6 est activé pour les mises à jour dynamiques DNS par %2.
137	DHCPv6.ScopeDNSDisable	Étendue : %1 pour IPv6 est désactivée pour les mises à jour DNS dynamiques par %2.
138	DHCPv6.ScopeDNSUpdate_Req_by_Client	Étendue : %1 pour IPv6 est mise à jour avec les paramètres DNS par %2: pour mettre à jour dynamiquement les enregistrements DNS AAAA et PTR à la demande des clients DHCP.
139	DHCPv6.ScopeDNSUpdate_Always	Étendue : %1 pour IPv6 est mis à jour avec les paramètres DNS par %2, ce qui permet de toujours mettre à jour dynamiquement les enregistrements DNS A et AAAA.
140	DHCPv6.ScopeDNSEnable_Discard	Étendue : %1 pour IPv6 est activé pour les paramètres DNS par %2, ce qui permet d'ignorer les enregistrements DNS A et AAAA lorsque le bail est supprimé.
01:21:41 AM	DHCPv6.ScopeDNSDisable_Discard	Étendue : %1 pour IPv6 est désactivé pour les paramètres DNS par %2, ce qui permet d'ignorer les enregistrements DNS A et AAAA lorsque le bail est supprimé.

ID d’événement	Catégorie d’événement	Texte de l’événement
1:42	DHCPv6.ScopeDHCIDEnable	Le paramètre de protection du nom est activé sur l'étendue %1 pour IPv6 par %2.
143	DHCPv6.ScopeDHCIDDisable	Le paramètre de protection du nom est désactivé sur l'étendue %1 pour IPv6 par %2.
145	DHCPv6.ReservationConfigured	Réservation : %1 pour IPv6 est configuré sous l'étendue %2 par %3.
147	DHCPv6.ReservationDeleted	Réservation : %1 pour IPv6 est supprimé sous l'étendue %2 par %3.
148	DHCPv6.ReservationDNSEnable	Réservation : %1 pour IPv6 sous l'étendue %2 est activé pour les mises à jour dynamiques DNS par %3.
149	DHCPv6.ReservationDNSDisable	Réservation : %1 pour IPv6 sous l'étendue %2 est désactivé pour les mises à jour dynamiques DNS par %3.
150	DHCPv6.ReservationDNSUpdate_Req_by_Client	Réservation : %1 pour IPv6 sous l'étendue %2 a été mis à jour avec les paramètres DNS par %3, ce qui permet de mettre à jour dynamiquement les enregistrements DNS AAAA et PTR à la demande des clients DHCP.
151	DHCPv6.ReservationDNSUpdate_Always	Réservation : %1 pour IPv6 sous l'étendue %2 a été mis à jour par %3 avec les paramètres DNS, ce qui permet de toujours mettre à jour dynamiquement les enregistrements DNS AAAA et PTR.
152	DHCPv6.ReservationDNSEnable_Discard	Réservation : %1 pour IPv6 sous l'étendue %2 est activé pour les paramètres DNS par %3, ce qui permet d'ignorer les enregistrements DNS AAAA et PTR lorsque le bail est supprimé.
153	DHCPv6.ReservationDNSDisable_Discard	Réservation : %1 pour IPv6 sous l'étendue %2 est désactivé pour les paramètres DNS par %3, ce qui permet d'ignorer les enregistrements DNS AAAA et PTR lorsque le bail est supprimé.
154	DHCPv6.ReservationOptionUpdate	Réservation : %1 pour IPv6 sous l'étendue %2 est mis à jour avec le paramètre d’option %3 par %4.
1:55	DHCPv6.ScopeExclusionAdded	Ajout de la plage d’adresses IP d’exclusion %1 dans le pool d’adresses pour IPv6 sous l'étendue %2 par %3.
1:56	DHCPv6.ScopeExclusionDeleted	Suppression de la plage d’adresses IP d’exclusion %1 dans le pool d’adresses pour IPv6 sous l'étendue %2 par %3.
1:57	DHCPv6.ScopeModified	Étendue : %1 pour IPv6 est modifié par %2.
158	DHCPv6.ScopeStatelessEnabled	L'inventaire des clients sans état DHCPv6 a été activé pour l'étendue %1.
1:59	DHCPv6.ScopeStatelessDisabled	L'inventaire des clients sans état DHCPv6 a été désactivé pour l'étendue %1.
160	DHCPv6.ServerStatelessEnabled	L'inventaire des clients sans état DHCPv6 a été activé pour le serveur.
161	DHCPv6.ServerStatelessDisabled	L'inventaire des clients sans état DHCPv6 a été désactivé pour le serveur.
162	DHCPv6.ScopeStatelessPurgeInterval	L'intervalle de temps de vidage pour l'inventaire des clients sans état DHCPv6 dans l'étendue %1 a été défini sur %2 heures.
163	DHCPv6.ServerStatelessPurgeInterval	L'intervalle de temps de vidage pour l'inventaire des clients sans état DHCPv6 sur le serveur a été défini sur %1 heures.
165	DHCPv4.ScopeDNSDisable_DisablePtrUpdates	Étendue : %1 pour IPv4 est désactivée pour les paramètres DNS par %2: pour désactiver les mises à jour dynamiques des enregistrements PTR DNS.
166	DHCPv6.ServerOptionUpdate	L’option de niveau serveur %1 pour IPv6 a été mise à jour par %2.
20220	DHCPv4.UpdateServerPolicyState	La politique %2 pour le serveur est %1.
20221	DHCPv4.UpdateScopePolicyState	La stratégie %2 pour l’étendue %3 est %1.
20222	DHCPv4.UpdateServerPolicyExpr	Les conditions de la stratégie de serveur %3 ont été définies sur %1. Les conditions sont regroupées par opérateur logique %2.
20223	DHCPv4.UpdateScopePolicyExpr	Les conditions de la stratégie %3 pour l'étendue %4 ont été définies sur %1. Les conditions sont regroupées par opérateur logique %2.
20226	DHCPv4.DeleteServerPolicy	La stratégie %1 a été supprimée du serveur.
20227	DHCPv4.DeleteScopePolicy	La politique %1 a été supprimée du périmètre %2.
20228	DHCPv4.SetScopePolicyRange	La plage d’adresses IP de %1 a été définie pour la stratégie %2 de l'étendue %3.

ID d'événement	Catégorie d'événement	Texte de l'événement
20229	DHCPv4.RemoveScopePolicyRange	La plage d'adresses IP de %1 a été supprimée de la stratégie %2 de l'étendue %3.
20230	DHCPv4.SetServerPolicyOption	La valeur %2 a été définie pour l'option %1 pour la stratégie de serveur %3.
20231	DHCPv4.SetScopePolicyOption	La valeur %2 a été définie pour l'option %1 de la stratégie %3 de l'étendue %4.
20232	DHCPv4.UnsetServerPolicyOption	La valeur %2 a été supprimée de l'option %1 pour la stratégie de serveur %3.
20233	DHCPv4.UnsetScopePolicyOption	La valeur %2 a été supprimée de l'option %1 dans le cadre de l'étendue %4 de la stratégie %3.
20234	DHCPv4.UpdateServerPolicyName	La stratégie de serveur %2 a été renommée %1.
20235	DHCPv4.UpdateScopePolicyName	La stratégie %2 de l'étendue %3 a été renommée %1.
20236	DescriptionDeLaStratégieDeMiseÀJourDuServeurDHCPv4	La description de la stratégie de serveur %2 a été définie sur %1.
20237	DHCPv4.UpdateScopePolicyDescription	La description de la stratégie %2 de l'étendue %3 a été définie sur %1.
20238	DHCPv4.UpdateServerPolicyProcOrder	L'ordre de traitement de la stratégie de serveur %3 a été changé de %2à %1.
20239	DHCPv4.UpdateScopePolicyProcOrder	L'ordre de traitement de la stratégie %3 de l'étendue %4 a été modifié, passant de %2 à %1.
20241	DHCPv4.CreateFailoverRelationshipHotStandby	Une relation de basculement a été créée entre les serveurs %1 et les %2 avec les paramètres de configuration suivants : nom : %3, mode : veille à chaud, délai maximal du client : %4 secondes, pourcentage d'adresse de réserve sur le serveur de secours : %5, intervalle de basculement d'état automatique : %6 secondes, serveur de secours : %7.
20242	DHCPv4.DeleteFailoverRelationship	La relation de basculement %1 entre %2 et %3 a été supprimée.
20243	DHCPv4.AddScopeRelationship	L'étendue %1 a été ajoutée à la relation de basculement %2 avec le serveur %3.
20244	DHCPv4.DeleteScopeRelationship	L'étendue %1 a été supprimée de la relation de basculement %2 avec le serveur %3.
20245	DHCPv4.UpdateRelationshipParamMclt	Le paramètre de configuration de basculement MCLT pour la relation de basculement %1 avec le serveur %2 a été modifié, passant de %3 secondes à %4 secondes.
20246	DHCPv4.UpdateRelationshipParamAutoSwitchOverInterval	Dans les paramètres de configuration du basculement, l'intervalle de commutation automatique pour la relation de basculement %1 avec le serveur %2 a été modifié, passant de %3 secondes à %4 secondes.
20247	DHCPv4.UpdateRelationshipParamPercentageHS	Le pourcentage d'adresses de réserve du paramètre de configuration de basculement pour la relation de basculement %1 avec le serveur %2 a été passé de %3 à %4.
20248	DHCPv4.UpdateRelationshipParamPercentageLB	Dans les paramètres de configuration du basculement, le pourcentage d'équilibrage de charge pour la relation de basculement %1 avec le serveur %2 a été modifié, passant de %3 à %4 sur ce serveur.
20249	DHCPv4.UpdateRelationshipParamModeHStoLB	Dans les paramètres de configuration du basculement, le mode pour la relation de basculement %1 avec le serveur %2 a été modifié, passant de serveur de secours à équilibre de charge.
20250	DHCPv4.UpdateRelationshipParamModeLBtoHS	Dans les paramètres de configuration du basculement, le mode pour la relation de basculement %1 avec le serveur %2 a été modifié, passant d'équilibre de charge à serveur de secours.
20311	DHCPv4.UpdateSharedSecret	Le secret partagé pour la relation de basculement %2 avec le serveur %1 a été modifié.
20312	DHCPv4.EnabledSharedSecret	L'authentification des messages pour la relation de basculement %2 avec le serveur %1 a été activée.
20313	DHCPv4.DisabledSharedSecret	L'authentification des messages pour la relation de basculement %2 avec le serveur %1 a été désactivée.
20315	DHCPv4.UpdateScopePolicyDNSSuffix	Le DNSSuffix de la stratégie %2 de l'étendue %3 a été défini sur %1.
20316	DHCPv4.UpdateServerPolicyDNSSuffix	Le DNSSuffix de la stratégie de serveur %2 a été définie sur %1.

Événements d'administration du serveur DHCP

Les événements d'administration du serveur DHCP consignent les informations sur les tâches d'administration effectuées sur le serveur DHCP.

▼ Pour afficher tous les événements administratifs du serveur, développez cette section.

Agrandir le tableau

ID d'événement	Catégorie d'événement	Texte de l'événement
1000	EVENT_SERVER_UNKNOWN_OPTION	Le service DHCP a reçu l'option inconnue %1, avec une longueur de %2. Les donn brute sont indiquées ci-dessous.
1 001	EVENT_SERVER_FAILED_REGISTER_SC	Le service DHCP n'a pas pu s'inscrire auprès du contrôleur de service. L'erreur suiv produite : %n%1.
1002	EVENT_SERVER_INIT_DATA_FAILED	Le service DHCP n'a pas pu initialiser ses paramètres globaux. L'erreur suivante s'e %n%1
1003	EVENT_SERVER_INIT_REGISTRY_FAILED	Le service DHCP n'a pas pu initialiser ses paramètres de Registre. L'erreur suivante produite : %n%1
1004	EVENT_SERVER_INIT_DATABASE_FAILED	Le service DHCP n'a pas pu initialiser la base de données. L'erreur suivante s'est pr %n%1
1005	EVENT_SERVER_INIT_WINSOCK_FAILED	Le service DHCP n'a pas pu initialiser le démarrage de Winsock. L'erreur suivante s : %n%1
1006	EVENT_SERVER_INIT_RPC_FAILED	Le service DHCP n'a pas pu démarrer en tant que serveur RPC. L'erreur suivante s'e %n%1
1007	EVENT_SERVER_INIT_SOCK_FAILED	Le service DHCP n'a pas pu initialiser les données Winsock. L'erreur suivante s'est %n%1
1008	EVENT_SERVER_SHUTDOWN	Le service DHCP s'arrête en raison de l'erreur suivante : %n%1
1009	EVENT_SERVER_CLIENT_CLEANUP	Le service DHCP a rencontré l'erreur suivante lors du nettoyage des enregistremer attente : %n%1
1010	EVENT_SERVER_DATABASE_CLEANUP	Le service DHCP a rencontré l'erreur suivante lors du nettoyage de la base de don
1011	EVENT_SERVER_LEASE_NACK	Le service DHCP a émis un NACK (message d'accusé de réception négatif) au clien l'adresse, %1.
1012	EVENT_SERVER_LEASE_DECLINED	Le client DHCP, %2, a refusé l'adresse %1.
1013	EVENT_SERVER_LEASE_RELEASE	Le client DHCP, %2, a publié l'adresse %1.
1016	EVENT_SERVER_DATABASE_BACKUP	Le service DHCP a rencontré l'erreur suivante lors de la sauvegarde de la base de d %n%1
1017	EVENT_SERVER_CONFIG_BACKUP	Le service DHCP a rencontré l'erreur suivante lors de la sauvegarde de la configura Registre : %n%1
1018	EVENT_SERVER_DATABASE_RESTORE_FAILED	Le service DHCP n'a pas pu restaurer la base de données. L'erreur suivante s'est pr %n%1
1019	EVENT_SERVER_CONFIG_RESTORE_FAILED	Le service DHCP n'a pas pu restaurer la configuration du Registre DHCP. L'erreur s produite : %n%1
1020	EVENT_SERVER_LOW_ADDRESS_WARNING	L'étendue %1 est complète à %2 % avec seulement %3 adresses IP restantes.
1021	EVENT_SERVER_LOAD_JET_FAILED	Le service DHCP n'a pas pu charger correctement la bibliothèque de base de donr
1022	EVENT_SERVER_JET_CONV_REQUIRED	Le service DHCP n'a pas pu utiliser la base de données. Si ce service a été démarré première fois après la mise à niveau à partir de NT 3.51 ou version antérieure, vou exécuter l'utilitaire, upg351db.exe, sur la base de données DHCP pour la convertir format de base de données JET. Redémarrez le service DHCP après avoir mis à niv de données.
1023	EVENT_SERVER_JET_CONV_IN_PROGRESS	Le service DHCP se termine maintenant, car la base de données existante a besoin conversion au format Windows 2000. La conversion via le processus jetconv a dém redémarrez pas ou arrêtez le processus jetconv. La conversion peut prendre jusqu minutes en fonction de la taille de la base de données. Terminez DHCP maintenan sur OK. Cela est nécessaire pour que la conversion de base de données réussisse. le service DHCP est redémarré automatiquement une fois la conversion terminée. l'état de la conversion, examinez le journal des événements de l'application pour l jetconv.
1024	EVENT_SERVER_INIT_AND_READY	Le service DHCP a initialisé et est prêt

ID d'événement	Catégorie d'événement	Texte de l'événement
1025	EVENT_SERVER_BOOT_FILE_TABLE	Le service DHCP n'a pas pu lire la table de fichiers BOOTP à partir du Registre. Le s ne peut pas répondre aux demandes BOOTP qui spécifient le nom du fichier de dé
1026	EVENT_SERVER_BOOT_FILE_NAME	Le service DHCP n'a pas pu lire le nom de fichier BOOTP global à partir du Registre
1027	EVENT_SERVER_AUDIT_LOG_APPEND_FAILED	Impossible d'ajouter le fichier journal d'audit.
1028	EVENT_SERVER_INIT_AUDIT_LOG_FAILED	Le service DHCP n'a pas pu initialiser le journal d'audit. L'erreur suivante s'est prod
1029	EVENT_SERVER_PING_FAILED	Le service DHCP n'a pas pu effectuer un test ping pour une nouvelle adresse IP. L'a louée au client.
1030	EVENT_SERVER_MOVE_AUDIT_LOG_FAILED	Impossible de sauvegarder le fichier journal d'audit. L'erreur suivante s'est produit
1031	EVENT_SERVER_CALLOUT_UNHANDLED_EXCEPTION	Le fichier de légende serveur installé .dll a causé une exception. L'exception était : serveur a ignoré cette exception. Toutes les autres exceptions seront ignorées.
1032	EVENT_SERVER_CALLOUT_LOAD_EXCEPTION	Le fichier de légende serveur installé .dll a causé une exception. L'exception était : serveur a ignoré cette exception et le fichier .dll n'a pas pu être chargé.
1033	EVENT_SERVER_CALLOUT_LOAD_SUCCESS	Le service DHCP a correctement chargé une ou plusieurs DLL de légende.
10:34	EVENT_SERVER_READ_ONLY_GROUP_ERROR	Échec du chargement d'une ou plusieurs DLL de légende par le service DHCP. L'er suivante s'est produite : %n%1
1035	EVENT_SERVER_READ_ONLY_GROUP_ERROR	Le service DHCP n'a pas pu créer ou rechercher le groupe local utilisateurs DHCP s ordinateur. Le code d'erreur se trouve dans les données.
1036	EVENT_SERVER_ADMIN_GROUP_ERROR	Le serveur DHCP n'a pas pu créer ou rechercher le groupe local Administrateurs D ordinateur. Le code d'erreur se trouve dans les données.
1037	EVENT_SERVER_CLEANUP_STARTED	Le service DHCP a commencé à nettoyer la base de données.
1038	EVENT_SERVER_IPCLEANUP_FINISHED	Le service DHCP a nettoyé la base de données pour les adresses IP monodiffusion %1 ont été récupérés et %2 enregistrements ont été supprimés de la base de don
1039	EVENT_SERVER_MCASTCLEANUP_FINISHED	Le service DHCP a nettoyé la base de données pour les adresses IP de multidiffusi baux%1 ont expiré (ont été marqués pour suppression) et les enregistrements %2 supprimés de la base de données.
1040	EVENT_SERVER_DATABASE_RESTORE_SUCCEEDED	Le service DHCP a correctement restauré la base de données.
1041	DHCP_ROGUE_EVENT_NO_NETWORK	Le service DHCP ne traite pas de clients DHCPv4, car aucune des interfaces réseau configuré statiquement des adresses IPv4 ou il n'existe aucune interface active.
1042	DHCP_ROGUE_EVENT_UNAUTHORIZED_INFO	Le service DHCP/BINL exécuté sur cet ordinateur a détecté un serveur sur le réseau serveur n'appartient à aucun domaine, le domaine est répertorié comme vide. L'ad serveur est répertoriée entre parenthèses. %1
1043	DHCP_ROGUE_EVENT_STARTED	Le service DHCP/BINL sur l'ordinateur local a déterminé qu'il est autorisé à démarr actuellement au service des clients.
1044	DHCP_ROGUE_EVENT_STARTED_DOMAIN	Le service DHCP/BINL sur l'ordinateur local, appartenant au domaine d'administra Windows %2, a déterminé qu'il est autorisé à démarrer. Il sert maintenant des clie
10:45	DHCP_ROGUE_EVENT_STOPPED	Le service DHCP/BINL sur l'ordinateur local a déterminé qu'il n'est pas autorisé à d cessé de servir les clients. Voici quelques raisons possibles : %n%tThis machine ap groupe de travail et a rencontré un autre serveur DHCP (appartenant à un domain d'administration Windows) qui entretient le même réseau. %n%n%tAn erreur rése inattendue s'est produite.
1046	DHCP_ROGUE_EVENT_STOPPED_DOMAIN	Le service DHCP/BINL sur l'ordinateur local, appartenant au domaine d'administra Windows %2, a déterminé qu'il n'est pas autorisé à démarrer. Il a cessé de fournir aux clients. Voici quelques raisons possibles : %n%tThis machine fait partie d'une e service d'annuaire et n'est pas autorisée dans le même domaine. Pour plus d'infor consultez l'outil de gestion des services DHCP. %n%n%tThis machine ne peut pas son entreprise de service d'annuaire et elle a rencontré un autre service DHCP sur appartenant à une entreprise de service d'annuaire sur laquelle l'ordinateur local n autorisé. %n%n%tSome erreur réseau inattendue s'est produite.
1047	DHCP_ROGUE_EVENT_JUST_UPGRADED	Le service DHCP/BINL sur l'ordinateur local a déterminé qu'il est autorisé à démarr maintenant au service des clients. %nThe service DHCP/BINL a déterminé que la m récemment mise à niveau. Si la machine est destinée à appartenir à un service d'ar d'entreprise, le service DHCP doit être autorisé par le service d'annuaire pour com

ID d'événement	Catégorie d'événement	Texte de l'événement
		servir les clients. (Consultez l'aide sur l'outil de gestion des services DHCP pour au serveur).
1048	DHCP_ROGUE_EVENT_JUST_UPGRADED_DOMAIN	Le service DHCP/BINL sur l'ordinateur local, appartenant au domaine Windows %2 déterminé qu'il est autorisé à démarrer. Il sert maintenant les clients. Il a détermin l'ordinateur a été récemment mis à niveau. Il a également déterminé qu'il n'existe entreprise de service d'annuaire pour le domaine ou que l'ordinateur n'est pas aut service d'annuaire. Tous les services DHCP appartenant à une entreprise de service doivent être autorisés dans le service d'annuaire aux clients de service. (Consultez l'outil de gestion des services DHCP pour autoriser un service DHCP dans le servic d'annuaire).
1049	Événement DHCP Rogue : Impossible de trouver le domaine.	Le service DHCP/BINL sur l'ordinateur local a rencontré une erreur lors de la tentat recherche du domaine de l'ordinateur local. L'erreur était : %3.
1050	DHCP_ROGUE_EVENT_NETWORK_FAILURE	Le service DHCP/BINL sur l'ordinateur local a rencontré une erreur réseau. L'erreur
1051	DHCP_ROGUE_EVENT_UNAUTHORIZED (événement DHCP rogue non autorisé)	Le service DHCP/BINL a déterminé qu'il n'est pas autorisé à traiter les clients sur ce pour le domaine Windows : %2. Tous les services DHCP appartenant à une entrepr service d'annuaire doivent être autorisés dans le service d'annuaire aux clients de s (Consultez l'aide sur l'outil de gestion des services DHCP pour autoriser un serveu le service d'annuaire).
1052	DHCP_ROGUE_EVENT_OTHER_SERVER	Le service DHCP/BINL sur ce serveur de groupe de travail a rencontré un autre ser l'adresse IP, %1, appartenant au domaine %2.
1053	DHCP_ROGUE_EVENT_SAM_OTHER_SERVER	Le service DHCP/BINL a rencontré un autre serveur sur ce réseau avec adresse IP, % appartenant au domaine : %2.
1054	DHCP_ROGUE_EVENT_SHUTDOWN	Le service DHCP/BINL sur cet ordinateur est arrêté. Consultez les messages précéc journal des événements pour connaître les raisons.
1055	DHCP_EVENT_DNS_REGPARAMS_FAILURE	Le service DHCP n'a pas pu emprunter les informations d'identification nécessaires enregistrements DNS : %n%1. Les informations d'identification système locales so
1056	DHCP_EVENT_NO_DNSCREDENTIALS_ON_DC	Le service DHCP a détecté qu'il s'exécute sur un contrôleur de domaine et qu'il n'a d'informations d'identification configurées pour une utilisation avec les inscription dynamiques lancées par le service DHCP. Il ne s'agit pas d'une configuration de sé recommandée. Les informations d'identification des inscriptions DNS dynamiques être configurées à l'aide de la ligne de commande ou via l'outil d'administration D
1057	EVENT_SERVER_DATABASE_CONVERSION	Le service DHCP n'a pas pu convertir la base de données temporaire au format ES
1058	EVENT_SERVER_INIT_CONFIG_FAILED	Le service DHCP n'a pas pu initialiser ses paramètres de configuration. L'erreur sui produite : %n%1
1 059	VENT_SERVER_COULDNT_SEE_DS	Le service DHCP n'a pas pu trouver un serveur de répertoires pour l'autorisation.
1060	EVENT_SERVER_AUDITLOG_PATH_NOT_ACCESSIBLE	Le service DHCP n'a pas pu accéder au chemin spécifié pour le journal d'audit.
1061	EVENT_SERVER_BACKUP_PATH_NOT_ACCESSIBLE	Le service DHCP n'a pas pu accéder au chemin spécifié pour les sauvegardes de ba données.
1062	EVENT_SERVER_DB_PATH_NOT_ACCESSIBLE	Le service DHCP n'a pas pu accéder au chemin spécifié pour la base de données
1063	EVENT_SERVER_SCOPE_FULL	Il n'existe aucune adresse IP disponible à louer dans l'étendue ou l'étendue global
1064	EVENT_SERVER_BOOTP_FULL	Il n'existe aucune adresse IP disponible pour les clients BOOTP dans l'étendue ou l globale %1.
1065	EVENT_SERVER_ORPHONED_ENTRIES_DELETED	Certaines entrées orphelines ont été supprimées dans la configuration en raison d suppression d'une classe ou d'une définition d'option. Vérifiez à nouveau la config serveur.
1144	EVENT_SERVER_NEED_STATIC_IP	Cet ordinateur a au moins une adresse IP affectée dynamiquement. Pour une opér serveur DHCP fiable, vous devez utiliser uniquement des adresses IP statiques.
1338	EVENT_SERVER_OFFER_QUEUE_FULL	Le nombre de messages DHCPOFFER en attente pour la transmission différée au c dépassé la capacité du serveur de 1 000 messages en attente. Le serveur DHCP su les messages DHCPDISCOVER suivants pour lesquels la réponse du message DHCI être retardée conformément à la configuration du serveur. Le serveur DHCP contir traiter les messages DHCPDISCOVER pour lesquels les réponses de message DHCP n'ont pas besoin d'être retardées. Le serveur DHCP reprend le traitement de tous l DHCPDISCOVER une fois le nombre de messages DHCPOFFER en attente pour la t différée au client est inférieur à la capacité du serveur.

ID d'événement	Catégorie d'événement	Texte de l'événement
1339	EVENT_SERVER_OFFER_QUEUE_FUNCTIONAL	Le nombre de messages DHCPOFFER en attente pour la transmission différée au c désormais inférieur à la capacité du serveur de 1 000. Le serveur DHCP reprend dé traitement de tous les messages DHCPDISCOVER.
1340	EVENT_SERVER_DNSDHCID_FAIL	L'inscription DNS pour l'adresse IP du client DHCPv4 %1, le nom de domaine com DHCID %3 a été refusé, car il existe probablement un client existant avec le même domaine complet déjà inscrit auprès du DNS.
1341	EVENT_SERVER_POLICY_RANGES_FULL	Aucune adresse IP n'est disponible pour la location dans la ou les plages d'adresse stratégie %1 dans l'étendue %2.
1342	EVENT_SERVER_RESIDUAL_RANGES_FULL	La plage d'adresses IP de l'étendue %1 n'a plus d'adresses IP disponibles.
1343	EVENT_SERVER_POLICY_RANGES_LOW_ADDRESS_WARNING	Les plages d'adresses IP de la stratégie %2 pour l'étendue %1 sont remplies à %3 reste que %4 adresses IP disponibles.
1344	EVENT_SERVER_DNS_VALIDATION_FAILED	L'adresse IP DNS %1 n'est pas une adresse de serveur DNS valide.
1376	EVENT_SERVER_RESIDUAL_RANGES_LOW_ADDRESS_WARNING	La plage d'adresses IP de l'étendue %1 est remplie à %2 % avec seulement %3 adr disponibles.
1377	EVENT_SERVER_SUPERSCOPE_LOW_ADDRESS_WARNING	L'étendue globale %1 est complète à %2 % avec seulement %3 adresses IP restant superscope a les plages suivantes %4
10 000	EVENT_DHCPV6_ADDERESS_NACKED	La confirmation DHCPv6 a été refusée, car l'adresse n'était pas appropriée pour le demande de renouvellement DHCPv6 a une durée de vie zéro pour l'adresse clien
10001	EVENT_DHCPV6_REQUEST_RECEIVED_FOR_ADDRESSES_NOT_LEASED	Renouvelez, reconnectez ou validez la réception des adresses IPv6 %1 pour lesque n'existe pas de bail actif disponible.
10002	EVENT_DHCPV6_SERVER_UNKNOWN_OPTION	Le service DHCPv6 a reçu l'option inconnue %1, avec une longueur de %2. Les dor d'option brute sont indiquées ci-dessous.
10003	EVENT_DHCPV6_SERVER_SCOPE_FULL	Il n'existe aucune adresse IPv6 disponible à attribuer dans l'étendue qui dessert le le préfixe %1.
10004	EVENT_DHCPV6_SERVER_LEASE_DECLINED	Le client DHCPv6, %2, a refusé l'adresse %1.
10005	EVENT_DHCPV6_SERVER_LOW_ADDRESS_WARNING	L'étendue DHCPv6 servant le réseau avec le préfixe %1est %2 pour cent pleine ave uniquement %3 adresses IP restantes.
10006	EVENT_DHCPV6_CLIENT_DELETE	Un client DHCPV6 %1 a été supprimé de la base de données DHCPV6.
10007	EVENT_DHCPV6_DROP_TIMEOUT	Un message DHCPV6 qui était dans la file d'attente pendant plus de 30 secondes supprimé, car il est trop ancien pour traiter.
10008	EVENT_DHCPV6_DROP_INVALID	Un message DHCPV6 non valide a été supprimé.
10009	EVENT_DHCPV6_DROP_WRONG_SERVER	Un message DHCPV6 qui n'a pas été destiné à ce serveur a été supprimé.
10010	EVENT_DHCPV6_DROP_UNICAST	Le message DHCV6 a été supprimé, car il a été reçu sur une adresse monodiffusio en charge de la monodiffusion est désactivée sur le serveur.
10011	EVENT_DHCPV6_SERVER_AUDIT_LOG_APPEND_FAILED	Le fichier de journalisation d'audit DHCPV6 ne peut pas être ajouté, code d'erreur %1.
10012	EVENT_DHCPV6_DROP_UNAUTH	Un message DHCPV6 a été supprimé, car le serveur n'est pas autorisé à traiter le n
10013	EVENT_DHCPv6_SERVER_INIT_AUDIT_LOG_FAILED	Le service DHCPv6 n'a pas pu initialiser le journal d'audit. L'erreur suivante s'est pr %n%1
10014	EVENT_DHCPV6_SERVER_MOVE_AUDIT_LOG_FAILED	Impossible de sauvegarder le fichier journal d'audit DHCPv6. Code d'erreur %1
10015	EVENT_DHCPV6_SERVER_AUDITLOG_PATH_NOT_ACCESSIBLE	Le service DHCPv6 n'a pas pu accéder au chemin spécifié pour le journal d'audit.
10016	EVENT_DHCPV6_SERVER_INIT_WINSOCK_FAILED	Le service DHCPv6 n'a pas pu initialiser le démarrage de Winsock. L'erreur suivante produite %1.
10017	EVENT_DHCPV6_NO_DNSCREDENTIALS_ON_DC	Le service DHCPv6 a détecté qu'il s'exécute sur un contrôleur de domaine et qu'il d'informations d'identification configurées pour une utilisation avec les inscription dynamiques lancées par le service DHCPv6. Il ne s'agit pas d'une configuration de recommandée.
10018	EVENT_DHCPV6_SERVER_INTERFACE_NOTIFICATION	Le serveur DHCPv6 n'a pas pu recevoir de notification de modifications de liste d'i Certaines interfaces ne seront pas activées dans le service DHCPv6.

ID d'événement	Catégorie d'événement	Texte de l'événement
10019	EVENT_DHCPV6_SERVER_INIT_CONFIG_FAILED	Le service DHCPv6 n'a pas pu initialiser ses paramètres de configuration. L'erreur s produite : %n%1.
10020	EVENT_DHCPV6_SERVER_NEED_STATIC_IP	Cet ordinateur a au moins une adresse IPv6 affectée dynamiquement. Pour une op serveur DHCPv6 fiable, vous devez utiliser uniquement des adresses IPv6 statiques
10021	EVENT_DHCPV6_SERVER_INIT_DATABASE_FAILED	Le service DHCPv6 n'a pas pu initialiser la base de données. L'erreur suivante s'est %n%1.
10022	EVENT_DHCPV6_SERVER_INIT_AND_READY	Le service DHCPv6 a initialisé et est prêt à servir.
10023	EVENT_DHCPV6_PORT_UNAVAILABLE	Le serveur DHCPv6 n'est pas en mesure de lier le numéro de port UDP %1 tel qu'il par une autre application. Ce port doit être mis à la disposition du serveur DHCPv6 démarrer la maintenance des clients.
10024	ERROR_LAST_DHCPV6_SERVER_ERROR	ERROR_LAST_DHCPV6_SERVER_ERROR
10025	EVENT_DHCPV6_DNSDHCID_FAIL	L'inscription DNS pour l'adresse IPv6 du client DHCPv6 %1, le nom de domaine co le DHCID %3 ont été refusés, car il existe probablement un client existant avec le n de domaine complet déjà inscrit auprès du DNS.
20090	EVENT_DHCP_PORT_UNAVAILABLE	Le serveur DHCP ne peut pas lier le numéro de port UDP %1 car il est utilisé par u application. Ce port doit être mis à la disposition du serveur DHCP pour démarrer maintenance des clients.
20098	EVENT_FILTER_EMPTY_ALLOW_LIST	Aucun client DHCP n'est servi, car la liste verte est vide et le serveur a été configur fournir des services DHCP aux clients dont les adresses matérielles sont présentes verte.
20251	DHCPv4.ChangeFailoverRelationState	L'état de basculement du serveur %1 pour la relation de basculement %2 a change %3 à %4.
20252	DHCPv4.ChangeFailoverRelationStateError	L'état de basculement du serveur %1 pour la relation de basculement %2 a change %3 à %4.
20253	DHCPv4.FailoverServerTimeSync	Le serveur a détecté qu'il n'est pas synchronisé avec le serveur partenaire : %1 pou de basculement %2. L'heure est désynchronisée de : %3 secondes.
20254	DHCPv4.FailoverCommUp	Le serveur a établi le contact avec le serveur de basculement partenaire %1 pour la %2.
20255	DHCPv4.FailoverCommDown	Le serveur a perdu le contact avec le serveur de basculement partenaire %1 pour l %2.
20256	DHCPv4.AuthFailedBndUpdMsgDigestFailedToCompare	Le message de protocole de basculement BINDING-UPDATE du serveur %1 pour l basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20257	DHCPv4.AuthFailedBndUpdMsgDigestNotConfigured	Le message de protocole de basculement BINDING-UPDATE du serveur %1 pour l basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20258	DHCPv4.AuthFailedBndUpdMsgDigestNotPresent	Le message de protocole de basculement BINDING-UPDATE du serveur %1 pour l basculement %2 a été rejeté car le condensat de message n'était pas présent.
20259	DHCPv4.ChangeFailoverRelationStateNoPrevState	L'état de basculement du serveur %1 pour la relation de basculement a été change %2 à %3.
20260	DHCPv4.ChangeFailoverRelationStateErrorNoPrevState	L'état de basculement du serveur %1 pour la relation de basculement a été change %2 à %3.
20261	DHCPv4.AuthFailedBndAckMsgDigestFailedToCompare	Le message de protocole de basculement BINDING-ACK du serveur %1 pour la rel basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20262	DHCPv4.AuthFailedBndAckMsgDigestNotConfigured	Le message de protocole de basculement BINDING-ACK du serveur %1 pour la rel basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20263	DHCPv4.AuthFailedBndAckMsgDigestNotPresent	Le message de protocole de basculement BINDING-ACK du serveur %1 pour la rel basculement %2 a été rejeté car le condensat de message n'était pas présent.
20264	DHCPv4.AuthFailedConnectMsgDigestFailedToCompare	Le message de protocole de basculement CONNECT du serveur %1 pour la relatio basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20265	DHCPv4.AuthFailedConnectMsgDigestNotConfigured	Le message de protocole de basculement CONNECT du serveur %1 pour la relatio basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20266	DHCPv4.AuthFailedConnectMsgDigestNotPresent	Le message de protocole de basculement CONNECT du serveur %1 pour la relatio

ID d'événement	Catégorie d'événement	Texte de l'événement
		basculement %2 a été rejeté car le condensat de message n'était pas présent.
20267	DHCPv4.AuthFailedConnectAckMsgDigestFailedToCompare	Le message de protocole de basculement CONNECTACK du serveur %1 pour la re basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20268	DHCPv4.AuthFailedConnectAckMsgDigestNotConfigured	Le message de protocole de basculement CONNECTACK du serveur %1 pour la re basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20269	DHCPv4.AuthFailedConnectAckMsgDigestNotPresent	Le message de protocole de basculement CONNECTACK du serveur %1 pour la re basculement %2 a été rejeté car le condensat de message n'était pas présent.
20270	DHCPv4.AuthFailedUpdReqAllMsgDigestFailedToCompare	Le message de protocole de basculement UPDREQALL du serveur %1 pour la relat basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20271	DHCPv4.AuthFailedUpdReqAllMsgDigestNotConfigured	Le message de protocole de basculement UPDREQALL du serveur %1 pour la relat basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20272	DHCPv4.AuthFailedUpdReqAllMsgDigestNotPresent	Le message de protocole de basculement UPDREQALL du serveur %1 pour la relat basculement %2 a été rejeté car le condensat de message n'était pas présent.
20273	DHCPv4.AuthFailedUpdDoneMsgDigestFailedToCompare	Le message de protocole de basculement UPDDONE du serveur %1 pour la relatic basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20274	DHCPv4.AuthFailedUpdDoneMsgDigestNotConfigured	Le message de protocole de basculement UPDDONE du serveur %1 pour la relatic basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20275	DHCPv4.AuthFailedUpdDoneMsgDigestNotPresent	Le message de protocole de basculement UPDDONE du serveur %1 pour la relatic basculement %2 a été rejeté car le condensat de message n'était pas présent.
20276	DHCPv4.AuthFailedUpdReqMsgDigestFailedToCompare	Le message de protocole de basculement UPDREQ du serveur %1 pour la relation basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20277	DHCPv4.AuthFailedUpdReqMsgDigestNotConfigured	Le message de protocole de basculement UPDREQ du serveur %1 pour la relation basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20278	DHCPv4.AuthFailedUpdReqMsgDigestNotPresent	Le message de protocole de basculement UPDREQ du serveur %1 pour la relation basculement %2 a été rejeté car le condensat de message n'était pas présent.
20279	DHCPv4.AuthFailedStateMsgDigestFailedToCompare	Le message de protocole de basculement STATE du serveur %1 pour la relation de basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20280	DHCPv4.AuthFailedStateMsgDigestNotConfigured	Le message de protocole de basculement STATE du serveur %1 pour la relation de basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20281	DHCPv4.AuthFailedStateMsgDigestNotPresent	Le message de protocole de basculement STATE du serveur %1 pour la relation de basculement %2 a été rejeté car le condensat de message n'était pas présent.
20282	DHCPv4.AuthFailedContactMsgDigestFailedToCompare	Le message de protocole de basculement CONTACT du serveur %1 pour la relatio basculement %2 a été rejeté car le condensat de message n'a pas pu être compare
20283	DHCPv4.AuthFailedContactMsgDigestNotConfigured	Le message de protocole de basculement CONTACT du serveur %1 pour la relatio basculement %2 a été rejeté car le condensat de message n'était pas configuré.
20284	DHCPv4.AuthFailedContactMsgDigestNotPresent	Le message de protocole de basculement CONTACT du serveur %1 pour la relatio basculement %2 a été rejeté car le condensat de message n'était pas présent.
20285	DHCPv4.InvalidAlgorithmProvider	Un algorithme de chiffrement non valide %1 a été spécifié pour l'authentification messages de basculement dans FailoverCryptoAlgorithm sous la clé de registre HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parame L'opération est arrêtée.
20286	DHCPv4.FailoverClientLeaseDropped	Le message BINDING UPDATE pour l'adresse IP %1 n'a pas pu être répliqué sur le partenaire %2 de relation de basculement %3 car la file d'attente BINDING UPDAT complète.
20287	DHCPv4.ClientRequestDropped	La demande du client DHCP de %1 a été rejetée, car les plages d'adresses IP appli l'étendue/le superscope %2 sont en dehors de la disponibilité des adresses IP. Cel dû au fait qu'il n'y a plus d'adresses IP disponibles dans les plages d'adresses IP d' stratégie.
20291	DHCPv4.SendBndAckMessageRejectReason	Un message BINDING-ACK avec l'ID de transaction %1 a été envoyé à l'adresse IP raison de rejet (%3) à destination du serveur partenaire %4 pour la relation de bas %5.
20292	DHCPv4.RecvBndAckMessageRejectReason	Un message BINDING-ACK avec l'ID de transaction %1 a été reçu à l'adresse IP %2 raison de rejet (%3) en provenance du serveur partenaire %4 pour la relation de b

ID d'événement	Catégorie d'événement	Texte de l'événement
		%5.

Événements système du serveur DHCP

Les événements du système du serveur DHCP consignent des informations sur le système de serveur DHCP.

▼ Pour afficher tous les événements système du serveur, développez cette section.

Agrandir le tableau

ID d'événement	Catégorie d'événement	Texte de l'événement
20035	EVENT_SERVER_INTERFACE_NOTIFICATION	%1 %3
20058	DHCPv4HA.BndUpd	%1 %3
20059	DHCPv4HA.BndAck	%1 %3
20060	DHCPv4HA.Connect	%1 %3
20061	DHCPv4HA.ConnectAck	%1 %3
20062	DHCPv4HA.UpdReqAll	%1 %3
20063	DHCPv4HA.UpdDone	%1 %3
20064	DHCPv4HA.UpdReq	%1 %3
20065	DHCPv4HA.State	%1 %3
20066	DHCPv4HA.Contact	%1 %3
20067	DHCPv4HA.Disconnect	%1 %3
20068	DHCPv4HA.ScavengerStart	Scavenger a démarré.
20069	DHCPv4HA.ScavengerEnd	Le jeu Scavenger est terminé.
20161	DHCPv4HA.AddrAllocationTriggered	Allocation d'adresses déclenchée pour la relation de basculement %1.
20163	DHCPv4Stateless.ScavengerEnd	Scavenger a terminé de purger les entrées sans état.
20164	DHCPv4HA.TotalLeasesDeleted	Le total des baux supprimés dans le nettoyeur est %1
20165	DHCPv4HA.FailoverScopeDeleted	L'étendue %1, qui faisait partie de la relation de basculement %2, n'a pas été trouvée dans la base de données du serveur DHCP. Restaurez la base de données du serveur DHCP.

Événements de notification de filtre de serveur DHCP

Les événements de notification du filtre du serveur DHCP consignent des informations sur le filtrage basé sur la couche de liaison.

▼ Pour afficher tous les événements de notification de filtre de serveur, détaillez cette section.

Agrandir le tableau

ID d'événement	Catégorie d'événement	Texte de l'événement
20096	EVENT_FILTER_DENIED_IN_DENY_LIST	Services DHCP refusés à l'ordinateur avec une adresse matérielle %1, un type de matériel %4et un nom de domaine complet/nom d'hôte %2, car il correspond à l'entrée %3 dans la liste de blocs.
20097	EVENT_FILTER_DENIED_NOT_IN_ALLOW_LIST	Les services DHCP ont été refusés à l'ordinateur avec une adresse matérielle %1, un type de matériel %3et un nom de domaine complet/nom d'hôte %2 car il ne correspond pas à une entrée dans la liste d'autorisation.
20099	EVENT_FILTER_DENIED_IN_DENY_LIST_UNSPECIFIED	Services DHCP refusés à l'ordinateur avec une adresse matérielle %1, un type de matériel %4et un nom de domaine complet/nom d'hôte non spécifié%2 car il

ID d'événement	Catégorie d'événement	Texte de l'événement
		correspond à l'entrée %3 dans la liste de blocs.
20100	EVENT_FILTER_DENIED_NOT_IN_ALLOW_LIST_UNSPECIFIED	Les services DHCP ont été refusés à la machine avec une adresse matérielle %1, un type de matériel %3 et un FQDN/nom d'hôte %2 non spécifié car cela ne correspondait à aucune entrée dans la liste d'autorisation.

Événements d'audit du serveur DHCP

Les informations du journal des événements d'audit du serveur DHCP sur les événements liés à la sécurité.

▼ Pour afficher tous les événements d'audit du serveur, développez cette section.

Agrandir le tableau

ID d'événement	Catégorie d'événement	Texte de l'événement
20289	DHCPv4.SendBndUpdMessage	Un message BINDING-UPDATE a été envoyé avec l'ID de transaction %1 à l'adresse IP %2 avec l'état de liaison %3 à destination du serveur partenaire %4 pour la relation de basculement %5.
20290	DHCPv4.RecvBndUpdMessage	Un message BINDING-UPDATE a été reçu avec l'ID de transaction %1 à l'adresse IP %2 avec l'état de liaison %3 en provenance du serveur partenaire %4 pour la relation de basculement %5.
20293	DHCPv4.SendUpdReqMessage	Un message UPDREQ a été envoyé avec l'ID de transaction %1 à destination du serveur partenaire %2 pour la relation de basculement %3.
20294	DHCPv4.RecvUpdReqMessage	Un message UPDREQ a été reçu avec l'ID de transaction %1 en provenance du serveur partenaire %2 pour la relation de basculement %3.
20295	DHCPv4.SendUpdDoneMessage	Un message UPDDONE a été envoyé avec l'ID de transaction %1 à destination du serveur partenaire %2 pour la relation de basculement %3.
20296	DHCPv4.RecvUpdDoneMessage	Un message UPDDONE a été reçu avec l'ID de transaction %1 en provenance du serveur partenaire %2 pour la relation de basculement %3.
20297	DHCPv4.SendUpdReqAllMessage	Un message UPDREQALL a été envoyé avec l'ID de transaction %1 à destination du serveur partenaire %2 pour la relation de basculement %3.
20298	DHCPv4.RecvUpdReqAllMessage	Un message UPDREQALL a été reçu avec l'ID de transaction %1 en provenance du serveur partenaire %2 pour la relation de basculement %3.
20299	DHCPv4.SendContactMessage	Un message CONTACT a été envoyé avec l'ID de transaction %1 à destination du serveur partenaire %2 pour la relation de basculement %3.
20300	DHCPv4.RecvContactMessage	Un message CONTACT a été reçu avec l'ID de transaction %1 en provenance du serveur partenaire %2 pour la relation de basculement %3.
20301	DHCPv4.SendConnectMessage	Un message CONNECT a été envoyé avec l'ID de transaction %1 à destination du serveur partenaire %2 pour la relation de basculement %3.
20302	DHCPv4.RecvConnectMessage	Un message CONNECT a été reçu avec l'ID de transaction %1 en provenance du serveur partenaire %2 pour la relation de basculement %3.
20303	DHCPv4.SendStateMessage	Un message STATE a été envoyé avec l'ID de transaction %1 à destination du serveur partenaire %2 concernant la relation de basculement %3, avec l'état %4 et l'heure de début d'état %5.
20304	DHCPv4.RecvStateMessage	Un message STATE a été reçu avec l'ID de transaction %1 en provenance du serveur partenaire %2 concernant la relation de basculement %3, avec l'état %4 et l'heure de début d'état %5.
20305	DHCPv4.SendConnectAckMessage	Un message CONNECTACK a été envoyé avec l'ID de transaction %1 à destination du serveur partenaire %2 pour la relation de basculement %3.
20306	DHCPv4.RecvConnectAckMessage	Un message CONNECTACK a été reçu avec l'ID de transaction %1 en provenance du serveur partenaire %2 pour la relation de basculement %3.
20307	DHCPv4.SendBndAckMessageNoRejectReason	Un message BINDING-ACK a été envoyé avec l'ID de transaction %1 à l'adresse IP %2 à destination du serveur partenaire %3 pour la relation de basculement %4.
20308	DHCPv4.RecvBndAckMessageNoRejectReason	Un message BINDING-ACK a été reçu avec l'ID de transaction %1 à l'adresse IP %2 en provenance du serveur partenaire %3 pour la relation de basculement %4.

ID d’événement	Catégorie d’événement	Texte de l’événement
20309	DHCPv4.SendConnectAckMessageRejectReason	Un message CONNECTACK a été envoyé avec l’ID de transaction %1 à destination du serveur partenaire %2 pour la relation de basculement %3 avec la raison de rejet %4.
20310	DHCPv4.RecvConnectAckMessageRejectReason	Un message CONNECTACK a été reçu avec l’ID de transaction %1 en provenance du serveur partenaire %2 pour la relation de basculement %3 avec la raison de rejet %4.

Présentation de Network ATC

> S'applique à Windows Server 2025

Le déploiement et le fonctionnement de la mise en réseau de cluster Windows Server peuvent être un processus complexe et sujette aux erreurs. En raison de la flexibilité de configuration fournie avec la pile de mise en réseau de l'hôte, il existe de nombreux éléments mobiles qui peuvent être facilement mal configurés ou négligés. Il est également difficile de rester à jour avec les dernières meilleures pratiques, car des améliorations ont été apportées en continu aux technologies sous-jacentes. Network ATC applique une configuration de cohérence entre les nœuds de cluster Windows Server pour créer une expérience plus fiable. Comme Network ATC est conçu pour les clusters Windows Server, il nécessite l'édition Datacenter de Windows Server et la fonctionnalité de clustering de basculement.

> **Remarque**
>
> Network ATC est le nom complet du produit et n'est pas un acronyme ou une abréviation.

Network ATC peut vous aider à :

- Réduire le temps de déploiement de la mise en réseau de l'hôte, la complexité et les erreurs
- Déployer les dernières pratiques recommandées et validées par Microsoft
- Garantir la cohérence de la configuration au sein du cluster
- Supprimer une dérive de configuration

Fonctionnalités

Network ATC fournit les fonctionnalités suivantes :

- **Déploiement** de Windows Admin Center : Network ATC est intégré à Windows Admin Center pour offrir une expérience facile à utiliser pour déployer la mise en réseau de l'hôte.

- **Symétrie** réseau : Network ATC configure et optimise toutes les cartes de façon identique en fonction de votre configuration. Network ATC vérifie également la taille, le modèle et la vitesse de votre carte réseau pour garantir la symétrie du réseau sur tous les nœuds du cluster.

- **Configuration de la carte** de stockage : Network ATC configure automatiquement les composants suivants pour votre réseau de stockage.
  - Propriétés de l'adaptateur physique
  - Data Center Bridging
  - Détermine si un commutateur virtuel est nécessaire et, le cas échéant, crée les cartes virtuelles requises
  - Mappe les adaptateurs virtuels à l'adaptateur physique approprié
  - Assigne des réseaux locaux virtuels
  - Network ATC affecte automatiquement des adresses IP pour les cartes de stockage.

- **Nommage** du réseau de cluster : Network ATC nomme automatiquement les réseaux de cluster en fonction de leur utilisation. Par exemple, le réseau de stockage peut être nommé *storage_compute(Storage_VLAN711)*.

- **Recommandations pour Live Migration** : Network ATC vous informe des lignes directrices recommandées pour Live Migration selon la version du système d'exploitation (il est toujours possible de les modifier). Network ATC gère les paramètres de migration dynamique suivants :
  - Nombre maximal de migrations en direct simultanées
  - Le réseau de migration dynamique
  - Transport de migration dynamique
  - Quantité maximale de bande passante SMBDirect (RDMA) utilisée pour la migration dynamique

- **Configuration** du proxy : Network ATC peut vous aider à configurer tous les nœuds de cluster avec les mêmes informations de configuration de proxy si votre environnement l'exige.

- **Prise en charge du cluster Stretch S2D** : Network ATC déploie la configuration requise pour les réseaux de réplication de stockage. Étant donné que ces adaptateurs doivent être acheminés entre les sous-réseaux, Network ATC n'affecte aucune adresse IP. Vous devez donc affecter l'adresse IP.

- **Détection du contexte** : Network ATC détecte automatiquement si vous exécutez la commande sur un nœud de cluster. Cela signifie que vous n'avez pas besoin d'utiliser le `-ClusterName` paramètre, car il détecte automatiquement le cluster sur lequel vous êtes activé.

Terminologie

Pour comprendre Network ATC, vous devez comprendre certains concepts de base. Voici une terminologie utilisée par Network ATC :

Intention: il s'agit d'une définition de la façon dont vous envisagez d'utiliser les cartes physiques dans votre système. Une intention a un nom convivial, identifie un ou plusieurs adaptateurs physiques, et inclut un ou plusieurs types d'intention.

Une carte physique individuelle ne peut être incluse que dans une seule intention. Par défaut, un adaptateur n'a pas d'intention (il n'y a pas d'état spécial ou de propriété donné aux adaptateurs qui n'ont pas d'intention). Vous pouvez avoir plusieurs intentions ; le nombre d'adaptateurs de votre système limite le nombre d'intentions que vous avez.

Type d'intention : chaque intention requiert un ou plusieurs types d'intention. N'importe quelle combinaison de types d'intention peut être spécifiée pour une intention unique spécifique. Voici les types d'intentions actuellement pris en charge et le nombre maximal d'intentions qu'ils peuvent être définis dans :

Gestion : les adaptateurs sont utilisés pour l'accès de gestion aux nœuds. Ce type d'intention ne peut être défini que dans une seule intention au maximum. Calcul : les adaptateurs sont utilisés pour connecter le trafic de machine virtuelle au réseau physique. Ce type d'intention peut être défini dans des intentions illimitées. Stockage : les adaptateurs sont utilisés pour le trafic SMB, y compris les espaces de stockage direct. Ce type d'intention ne peut être défini que dans une seule intention au maximum. Étendu : les cartes sont configurées de la même façon qu'une intention de stockage, sauf que RDMA ne peut pas être utilisé avec des intentions d'étendu. Ce type d'intention ne peut être défini que dans une seule intention au maximum.

Remplacement : par défaut, Network ATC déploie la configuration la plus courante, avec le moins d'entrées de la part de l'utilisateur. Les remplacements vous permettent de personnaliser si nécessaire votre déploiement. Par exemple, vous pouvez choisir de modifier les réseaux locaux virtuels utilisés pour les adaptateurs de stockage à partir des valeurs par défaut.

Network ATC vous permet de modifier toute la configuration que le système d'exploitation autorise. Cependant, le système d'exploitation limite certaines modifications du système d'exploitation et Network ATC respecte ces limitations. Par exemple, un commutateur virtuel n'autorise pas la modification de SR-IOV après son déploiement.

Exemple de déploiement

La vidéo suivante fournit une vue d'ensemble de Network ATC à l'aide de la commande Copy-NetIntent pour copier une intention d'un cluster vers un autre. Pour en savoir plus sur la

démonstration, consultez notre article Tech Community Déploiement de 100 clusters de production en quelques minutes.

https://www.youtube-nocookie.com/embed/AZBE_3LCiHQ

Étapes suivantes

Pour bien démarrer avec Network ATC, consultez les articles suivants :

- Passez en revue les valeurs par défaut de Network ATC et les exemples d'options de déploiement. Consultez Déployer un réseau hôte avec Network ATC.
- Configurez Network ATC à l'aide de PowerShell. Consultez Étape 4 : Configurer la mise en réseau des hôtes.
- Gérez Network ATC après le déploiement. Consultez Gérer la mise en réseau des hôtes à l'aide de Network ATC.
- Migrez un cluster existant vers Network ATC.
- Pour en savoir plus sur les dernières annonces de mise en réseau, créez vos compétences et connectez-vous à la communauté Microsoft Edge Networking, consultez le blog Tech Community Networking.

Dernière mise à jour : 15/09/2026

Déployer un réseau hôte avec Network ATC

S'applique à: ✅ Windows Server 2025, ✅ Azure Local 2311.2 and later

Cet article décrit les exigences, les bonnes pratiques et le déploiement de Network ATC. Network ATC simplifie le déploiement et la gestion de la configuration réseau pour les clusters Windows Server et Azure Local. L'ATC réseau fournit une approche basée sur les intentions pour le déploiement du réseau hôte. En spécifiant une ou plusieurs intentions (gestion, calcul ou stockage) pour une carte réseau, vous pouvez automatiser le déploiement de la configuration prévue. Pour plus d'informations sur Network ATC, notamment une vue d'ensemble et des définitions, consultez Vue d'ensemble de Network ATC.

Si vous avez des commentaires ou rencontrez des problèmes, passez en revue les exigences et la section bonnes pratiques, consultez le journal des événements Network ATC et collaborez avec votre équipe de support Technique Microsoft.

Prerequisites

Remplissez les conditions préalables suivantes pour utiliser Network ATC :

- Tous les serveurs du cluster doivent exécuter Windows Server 2025 ou version ultérieure pour Windows Server, et la version 2311.2 ou ultérieure pour les environnements locaux Azure.
- Doit utiliser des hôtes physiques certifiés pour Windows Server ou Azure Local. Pour le matériel certifié pour le serveur de base sécurisé, consultez le catalogue Windows Server. Pour les nœuds validés ou supérieurs pour Azure Local, consultez le catalogue Azure Local.
- Les adaptateurs de la même intention Network ATC doivent être symétriques (de même marque, de même modèle, de même vitesse et de même configuration) et disponibles sur chaque nœud du cluster.
  - Les adaptateurs asymétriques entraînent l'échec du déploiement d'une intention. Network ATC confirme automatiquement la symétrie de l'adaptateur pour tous les nœuds du cluster avant de déployer une intention.
  - Pour plus d'informations sur la symétrie de l'adaptateur, consultez Switch Embedded Teaming (SET).
- Chaque adaptateur physique spécifié dans une intention doit utiliser le même nom sur tous les nœuds du cluster.

- Vérifiez que chaque carte réseau affiche l'état « Up » (Actif) à l'aide de l'applet de commande PowerShell `Get-NetAdapter`.

- Chaque nœud doit avoir les fonctionnalités Windows Server suivantes installées :
  - Réseau ATC
  - Hyper-V
  - Clustering de basculement
  - Réseautage des centres de données
  - Cluster de basculement - Bande passante SMB (FS-SMBBW)

  Voici un exemple d'installation des fonctionnalités requises via PowerShell :

  PowerShell
  ```
  Install-WindowsFeature -Name NetworkATC, Hyper-V, 'Failover-Clustering', 'Data-Center-Bridging', FS-SMBBW -IncludeManagementTools
  ```

- Insérez chaque adaptateur dans les mêmes emplacements PCI dans chaque hôte. Cette pratique permet de faciliter les conventions d'affectation de noms automatisées par les systèmes d'imagerie.

- Configurez le réseau physique (commutateurs) avant réseau ATC, y compris les réseaux locaux virtuels, MTU et la configuration DCB. Pour plus d'informations, consultez Configuration réseau physique requise.

> **Important**
>
> Le déploiement d'ATC réseau dans des machines virtuelles peut être utilisé uniquement à des fins de test et de validation. Le déploiement basé sur une machine virtuelle nécessite un remplacement des paramètres d'adaptateur par défaut pour désactiver la propriété NetworkDirect. Pour plus d'informations sur la soumission d'un remplacement, consultez : Remplacer les paramètres réseau par défaut.

Commandes Network ATC courantes

Pour identifier les commandes Network ATC disponibles, exécutez l'applet `Get-Command -ModuleName NetworkATC` de commande dans PowerShell. Vérifiez que PowerShell est exécuté en tant qu'administrateur.

La cmdlet `Remove-NetIntent` supprime une intention du nœud ou du cluster local. Cette commande ne détruit pas la configuration appelée.

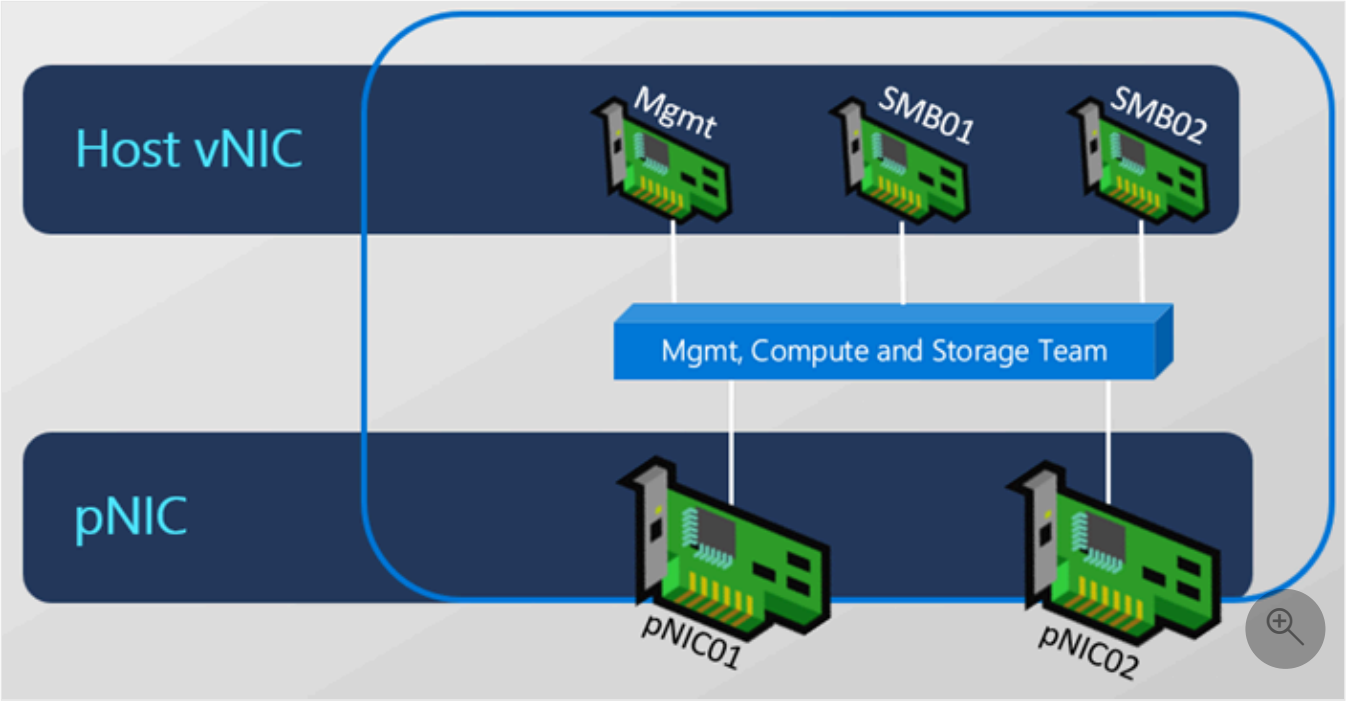
Exemples d'intentions

Network ATC modifie la manière dont vous déployez la mise en réseau de l'ordinateur hôte, et non ce que vous déployez. Vous pouvez déployer plusieurs scénarios tant que chaque scénario est un scénario pris en charge par Microsoft. Voici quelques exemples d'options de déploiement courantes et les commandes PowerShell nécessaires. Ces scénarios ne sont pas les seules combinaisons disponibles, mais elles doivent vous donner une idée des possibilités.

Par souci de simplicité, nous ne montrons que deux adaptateurs physiques par équipe SET, mais il est possible d'en ajouter d'autres. Pour plus d'informations, consultez Plan de mise en réseau de l'hôte.

Intention entièrement convergée

Pour cette intention, les réseaux de calcul, de stockage et de gestion sont déployés et gérés sur tous les nœuds du cluster.

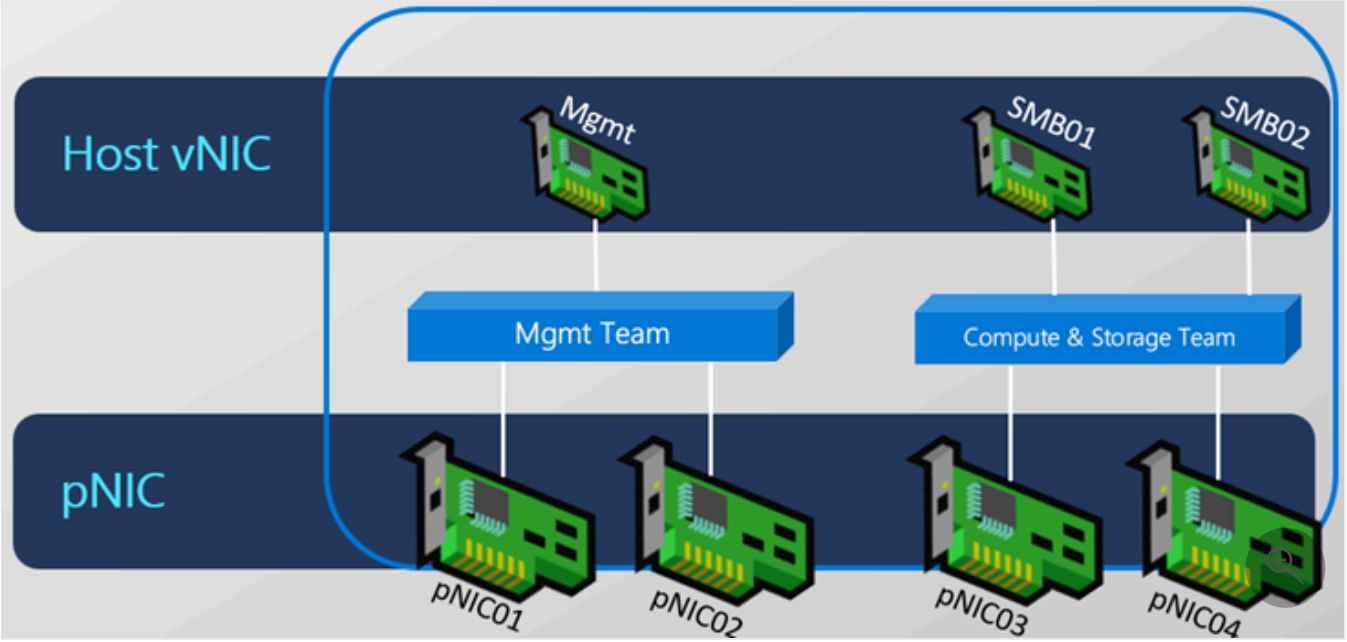


PowerShell

```
Add-NetIntent -Name ConvergedIntent -Management -Compute -Storage -AdapterName
pNIC01, pNIC02
```

Intention de calcul et de stockage convergée ; intention de gestion distincte

Deux intentions sont gérées sur des nœuds de cluster. Le management utilise pNIC01 et pNIC02 ; informatique et stockage se trouvent sur des adaptateurs différents.

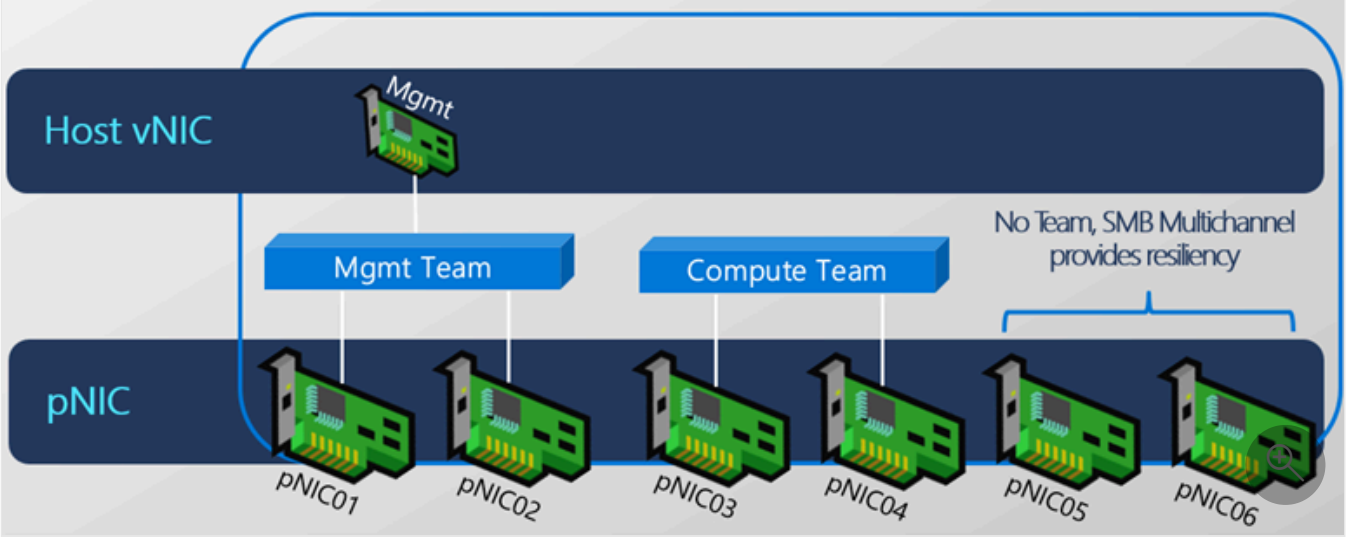


PowerShell

```
Add-NetIntent -Name Mgmt -Management -AdapterName pNIC01, pNIC02
Add-NetIntent -Name Compute_Storage -Compute -Storage -AdapterName pNIC03, pNIC04
```

Intention entièrement désagrégée

Pour cet objectif, les réseaux de calcul, de stockage et de gestion sont tous gérés sur différents adaptateurs à travers tous les nœuds du cluster.



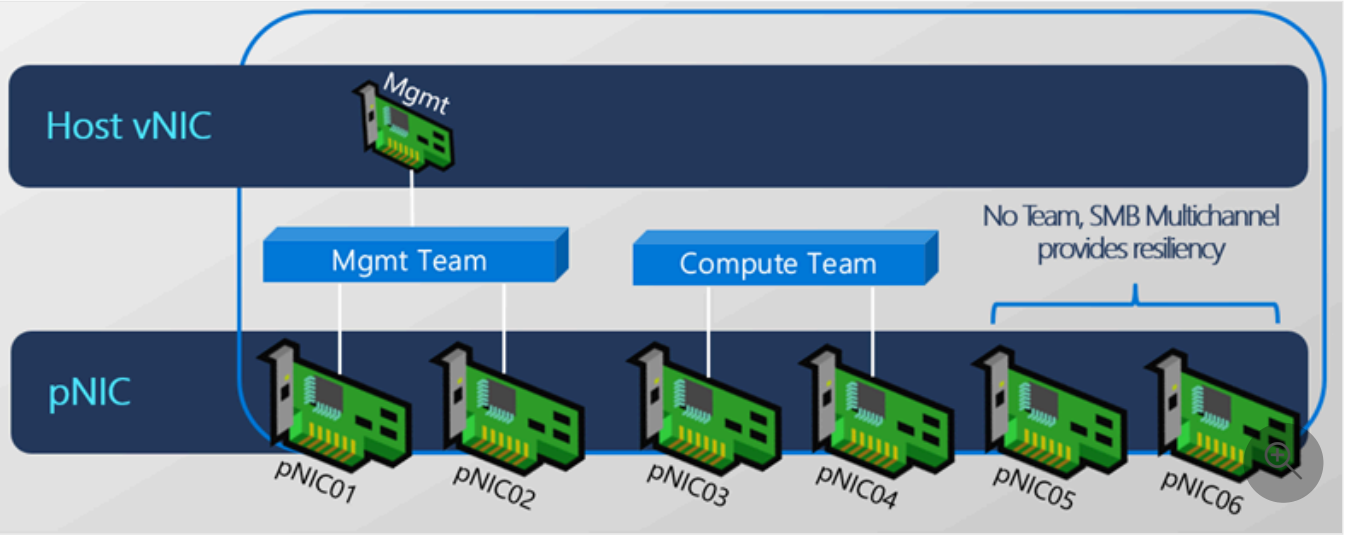
PowerShell

```
Add-NetIntent -Name Mgmt -Management -AdapterName pNIC01, pNIC02
Add-NetIntent -Name Compute -Compute -AdapterName pNIC03, pNIC04
```

```
Add-NetIntent -Name Storage -Storage -AdapterName pNIC05, pNIC06
```

Intention de stockage uniquement

Pour cette intention, seul le stockage est géré. Network ATC ne gère pas les cartes de gestion et de calcul.

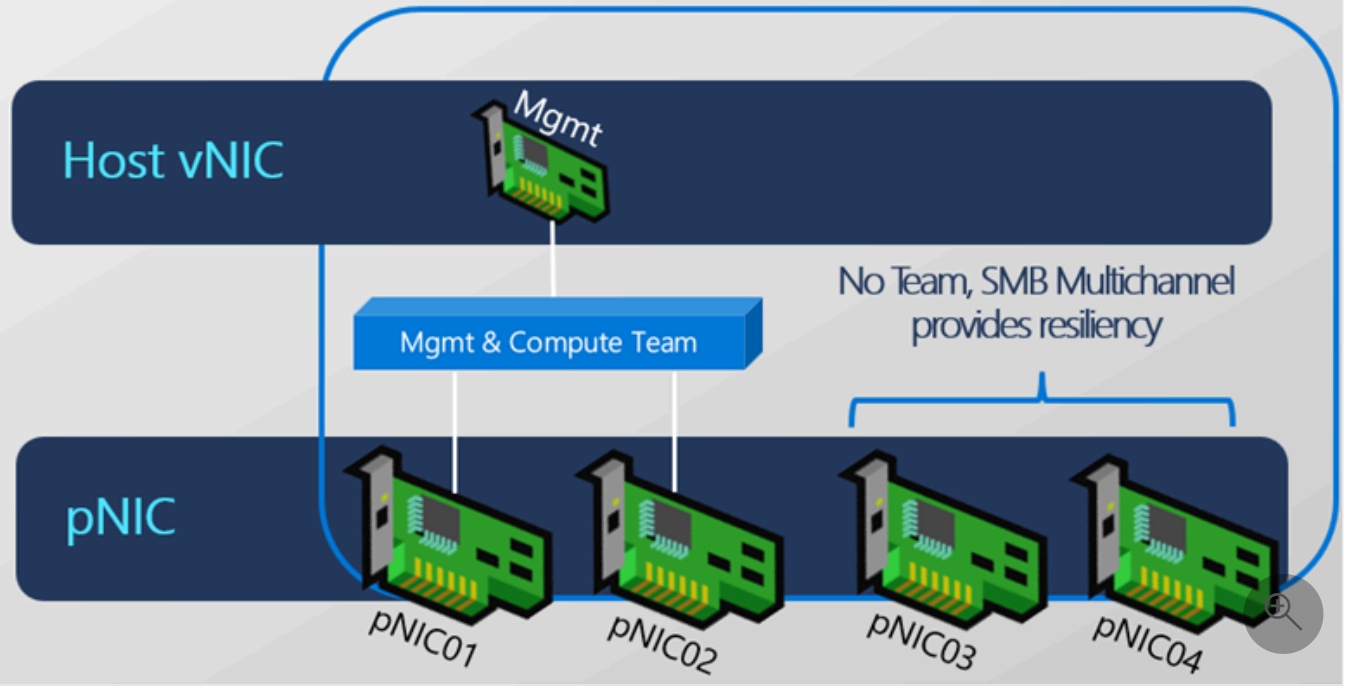


PowerShell

```
Add-NetIntent -Name Storage -Storage -AdapterName pNIC05, pNIC06
```

Intention de calcul et de gestion

Pour cette intention, les réseaux de calcul et de gestion sont gérés, mais pas le stockage.

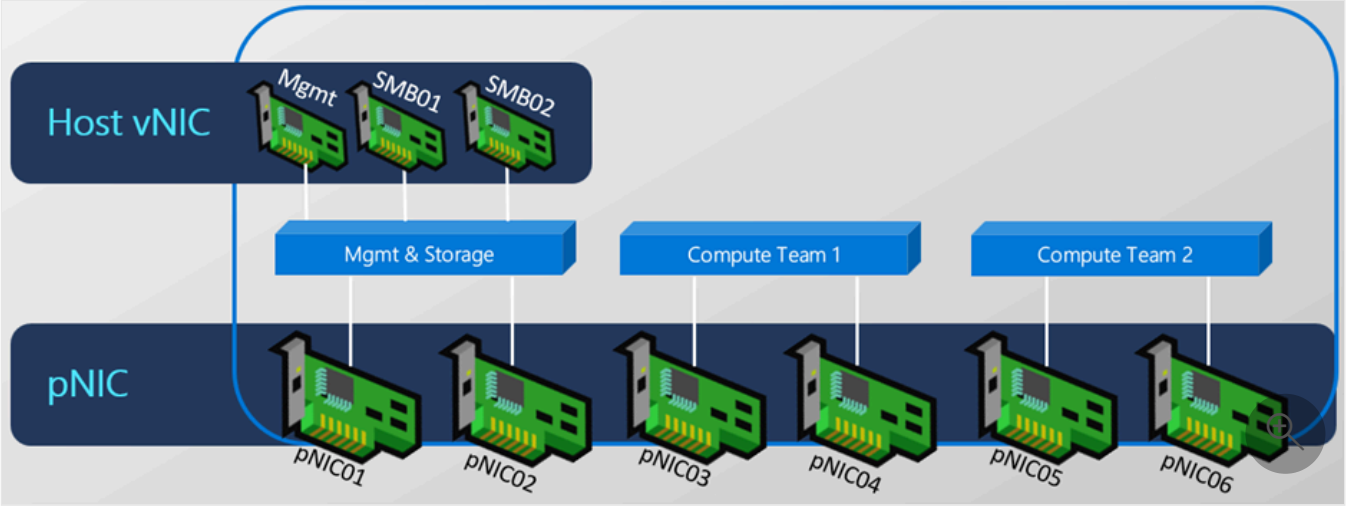


PowerShell

```
Add-NetIntent -Name Management_Compute -Management -Compute -AdapterName pNIC01,
pNIC02
```

Intentions de calcul multiple (commutateur)

À cette fin, plusieurs commutateurs de calcul sont gérés.



PowerShell

```
Add-NetIntent -Name Compute1 -Compute -AdapterName pNIC03, pNIC04
Add-NetIntent -Name Compute2 -Compute -AdapterName pNIC05, pNIC06
```

Valeurs par défaut de Network ATC

Network ATC utilise un ensemble de valeurs par défaut pour simplifier le déploiement et la gestion de la mise en réseau hôte. Ces valeurs par défaut sont appliquées lorsque vous créez des intentions ou modifiez des paramètres réseau. Comprendre ces valeurs par défaut peut vous aider à gérer efficacement la configuration de votre réseau.

Valeurs par défaut

Cette section décrit d'autres valeurs par défaut configurées par Network ATC.

Réseaux locaux virtuels par défaut

Network ATC utilise les réseaux locaux virtuels suivants par défaut pour les adaptateurs avec le type d'intention *de stockage* . Si les cartes sont connectées à un commutateur *physique* , ces

réseaux locaux virtuels doivent être autorisés sur le réseau physique. Si les adaptateurs sont sans commutateur, aucune autre configuration n'est requise.

Développer le tableau

Intention de l'adaptateur	Valeur par défaut
Management	Le réseau local virtuel configuré pour les adaptateurs de gestion n'est pas modifié
Adaptateur de stockage 1	711
Adaptateur de stockage 2	712
Adaptateur de stockage 3	713
Adaptateur de stockage 4	714
Adaptateur de stockage 5	715
Adaptateur de stockage 6	716
Adaptateur de stockage 7	717
Adaptateur de stockage 8	718
Utilisation future	719

Prenez la commande suivante :

PowerShell

```
Add-NetIntent -Name MyIntent -Storage -AdapterName pNIC01, pNIC02, pNIC03, pNIC04
```

La carte réseau physique (ou carte réseau virtuelle si nécessaire) est configurée pour utiliser respectivement les réseaux locaux virtuels 711, 712, 713 et 714.

> **Note**
>
> Network ATC vous permet de changer les VLAN utilisés avec le paramètre `StorageVlans` sur `Add-NetIntent`.

Adressage IP automatique du stockage

Network ATC configure automatiquement les adresses IP valides pour les cartes avec le type d'intention *de stockage* . Network ATC effectue cette configuration de manière uniforme sur tous les nœuds de votre cluster et vérifie que l'adresse choisie n'est pas déjà utilisée sur le réseau.

L'adresse IP par défaut pour chaque adaptateur sur chaque nœud de l'intention de stockage est configurée comme suit :

Développer le tableau

Adapter	Adresse IP et sous-réseau	VLAN
pNIC1	10.71.1.X	711
pNIC2	10.71.2.X	712
pNIC3	10.71.3.X	713

Pour remplacer l'adressage IP automatique du stockage, créez un remplacement de stockage et utilisez-le lorsque vous créez une intention :

PowerShell

```
$StorageOverride = New-NetIntentStorageOverrides
$StorageOverride.EnableAutomaticIPGeneration = $false
```

PowerShell

```
Add-NetIntent -Name MyIntent -Storage -Compute -AdapterName 'pNIC01', 'pNIC02' -
StorageOverrides $StorageOverride
```

Paramètres réseau du cluster

Network ATC configure un ensemble de fonctionnalités réseau de cluster par défaut. Les valeurs par défaut sont répertoriées comme suit :

Développer le tableau

Property	Default
`EnableNetworkNaming`	`$true`
`EnableLiveMigrationNetworkSelection`	`$true`
`EnableVirtualMachineMigrationPerformance`	`$true`

Property	Default
`VirtualMachineMigrationPerformanceOption`	La valeur par défaut est calculée : SMB, TCP ou Compression
`MaximumVirtualMachineMigrations`	1
`MaximumSMBMigrationBandwidthInGbps`	La valeur par défaut est calculée en fonction de la configuration

Configuration par défaut de Data Center Bridging (DCB)

Network ATC établit les priorités et réservations de bande passante suivantes. Cette configuration doit également être configurée sur le réseau physique.

Développer le tableau

Policy	Use	Priorité par défaut	Réservation de bande passante par défaut
Cluster	Réservation de pulsations de cluster	7	2% si un ou plusieurs adaptateurs sont <= 10 Gbits/s ; 1% si un ou plusieurs adaptateurs sont > de 10 Gbits/s
SMB_Direct	Trafic de stockage RDMA	3	50%
Default	Tous les autres types de trafic	0	Remainder

> **Note**
>
> Network ATC vous permet de remplacer les paramètres par défaut comme la réservation de bande passante par défaut. Pour obtenir des exemples, consultez Mettre à jour ou remplacer des paramètres réseau.

Messages d'erreur courants

Avec les nouveaux journaux d'événements, il existe certaines méthodes de résolution des problèmes simplistes pour identifier les échecs de déploiement d'intentions. Cette section décrit certaines des corrections courantes lorsqu'un problème est rencontré. Les erreurs suivantes proviennent de la sortie de l'applet `Get-NetIntentStatus` de commande.

Erreur : AdapterBindingConflict

```
Error                    : AdapterBindingConflict
Progress                 : 1 of 1
ConfigurationStatus      : Failed
ProvisioningStatus       : Completed
```

Scénario 1 : un adaptateur est lié à un commutateur virtuel existant qui est en conflit avec le nouveau commutateur virtuel déployé par Network ATC.

Solution: Supprimez le commutateur virtuel en conflit, puis Set-NetIntentRetryState

Scénario 2 : un adaptateur est lié au composant, mais pas nécessairement à un commutateur virtuel.

Solution: Désactivez le composant vms_pp (dissociez l'adaptateur à partir du commutateur virtuel), puis exécutez Set-NetIntentRetryState.

Erreur : ConflictingTrafficClass

```
Error                    : ConflictingTrafficClass
Progress                 : 1 of 1
ConfigurationStatus      : Failed
ProvisioningStatus       : Completed
```

Ce problème se produit parce qu'une classe de trafic est déjà configurée. Network ATC tente de déployer des classes de trafic qui entrent en conflit avec cette classe de trafic préconfigurée. Par exemple, vous avez peut-être déployé une classe de trafic appelée SMB lorsque Network ATC tente de déployer une classe de trafic similaire avec un autre nom.

Solution:

Effacer la configuration DCB existante sur le système, puis exécuter Set-NetIntentRetryState

PowerShell

```powershell
Get-NetQosTrafficClass | Remove-NetQosTrafficClass
Get-NetQosPolicy | Remove-NetQosPolicy -Confirm:$false
Get-NetQosFlowControl | Disable-NetQosFlowControl
```

Erreur : RDMANotOperational

```
Error                  : RdmaNotOperational
Progress               : 1 of 1
ConfigurationStatus    : Failed
ProvisioningStatus     : Completed
```

Ce message peut s'afficher :

1. Si la carte réseau utilise un pilote de boîte de réception. Les pilotes de boîte de réception ne sont pas pris en charge et doivent être mis à jour.

   Solution: Mettez à niveau le pilote pour l'adaptateur.

2. Si SR-IOV est désactivé dans le BIOS.

   Solution: Activer SR-IOV pour l'adaptateur dans le BIOS système

3. Si RDMA est désactivé dans le BIOS

   Solution: Activer RDMA pour l'adaptateur dans le BIOS système

Erreur : InvalidIsolationID

```
Error                  : InvalidIsolationId
Progress               : 1 of 1
ConfigurationStatus    : Failed
ProvisioningStatus     : Completed
```

Ce message se produit lorsque vous utilisez RoCE RDMA et remplacez le réseau local virtuel par défaut par une valeur non valide. Cela signifie que la valeur que vous avez choisie ne peut pas être utilisée avec ce protocole. Par exemple, RoCE RDMA nécessite un réseau local virtuel différent de zéro afin que les marquages PFC (Priority Flow Control) puissent être ajoutés au frame. Une valeur de réseau local virtuel comprise entre 1 et 4094 doit être utilisée. Network ATC ne remplace pas la valeur que vous avez spécifiée sans intervention de l'administrateur pour plusieurs raisons. Pour résoudre ce problème :

1. Choisissez iWARP comme protocole RDMA (NetworkDirect)

   Solution: Si la carte est prise en charge, Network ATC choisit automatiquement iWARP comme protocole RDMA qui peut utiliser un ID de réseau local virtuel de 0. Supprimez la

surcharge qui applique RoCE comme protocole choisi.

2. Utiliser les réseaux locaux virtuels par défaut

   Solution: Nous vous recommandons vivement d'utiliser les réseaux locaux virtuels par défaut d'ATC réseau

3. Utiliser un réseau local virtuel valide

   Lorsque vous spécifiez un réseau local virtuel, utilisez le paramètre -StorageVLANs et spécifiez des valeurs séparées par des virgules comprises entre 1 et 4094.

Étapes suivantes

- Gérer votre déploiement Network ATC. Consultez Gérer Network ATC.
- En savoir plus sur les clusters étendus.

Last updated on 27/11/2025

Gérer l'ATC réseau

Article • 22/05/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> S'applique à : Windows Server 2025 ; Azure Local 2311.2 et versions ultérieures

Cet article explique comment gérer Network ATC après son déploiement. Network ATC simplifie le déploiement et la gestion de la configuration réseau pour les clusters Windows Server et Azure Local. Utilisez Windows PowerShell pour gérer Network ATC.

Ajouter un nœud de serveur

Vous pouvez ajouter des nœuds à un cluster. Chaque nœud du cluster reçoit la même intention, ce qui améliore la fiabilité du cluster. Le nouveau nœud de serveur doit satisfaire à toutes les exigences décrites dans la section Configuration requise et meilleures pratiques de la mise en réseau de Mise en réseau des hôtes avec Network ATC.

Dans cette tâche, vous ajoutez des nœuds supplémentaires au cluster et observez comment une configuration réseau cohérente est appliquée sur tous les nœuds du cluster.

1. Utilisez l'applet `Add-ClusterNode` de commande pour ajouter les nœuds supplémentaires (non configurés) au cluster. À ce stade, vous avez uniquement besoin d'un accès de gestion au cluster. Pour tous les nœuds du cluster, les cartes réseau physiques doivent être nommées de la même façon.

   PowerShell

   ```
   Add-ClusterNode -Cluster CLUSTER01
   Get-ClusterNode
   ```

2. Vérifiez l'état sur tous les nœuds de cluster. Vous devez utiliser le paramètre dans la `-ClusterName` version 21H2. Network ATC détecte automatiquement le nom du cluster à partir de la version 22H2 et ultérieure.

   PowerShell

   ```
   Get-NetIntentStatus
   ```

   Notes

Si une carte réseau présente sur les autres serveurs est manquante sur l'un des serveurs que vous ajoutez au cluster, `Get-NetIntentStatus` signale l'erreur `PhysicalAdapterNotFound`.

3. Vérifiez l'état d'approvisionnement de tous les nœuds à l'aide de `Get-NetIntentStatus`. L'applet de commande affiche la configuration des deux nœuds. Cela peut prendre un certain temps pour provisionner le nœud d'origine.

   PowerShell

   ```
   Get-NetIntentStatus
   ```

   Vous pouvez également ajouter simultanément plusieurs nœuds au cluster.

Modifier des VLANS par défaut pour le stockage ou les systèmes d'administration

Vous pouvez utiliser des VLANS par défaut spécifiés par Network ATC ou utiliser des valeurs spécifiques à votre environnement. Pour ce faire, utilisez le paramètre -ManagementVLAN et -StorageVLANs sur Add-NetIntent.

PowerShell

```
Add-NetIntent -Name MyIntent -StorageVLANs 101, 102 -ManagementVLAN 10
```

Ajouter ou supprimer des cartes réseau d'une intention

Cette tâche vous aide à mettre à jour les cartes réseau affectées à une intention. Si vous changez des cartes physiques dans votre cluster, vous pouvez utiliser `Update-NetIntentAdapter` pour mettre à jour les intentions appropriées.

Dans cet exemple, nous avons installé deux nouveaux adaptateurs, pNIC03 et pNIC04, et nous voulons qu'ils soient utilisés dans notre intention nommée « Cluster_Compute ».

1. Sur l'un des nœuds de cluster, exécutez `Get-NetAdapter` pour vérifier que les deux cartes sont présentes et sont dans l'état « Opérationnel » sur chaque nœud de cluster.

   PowerShell

```
Get-NetAdapter -Name pNIC03, pNIC04 -CimSession (Get-ClusterNode).Name |
Select Name, PSComputerName
```

2. Exécutez la commande suivante pour mettre à jour l'intention avec les cartes réseau anciennes et nouvelles.

PowerShell

```
Update-NetIntentAdapter -Name Cluster_Compute -AdapterName
pNIC01,pNIC02,pNIC03,pNIC04
```

3. Vérifiez que les cartes réseau ont été correctement ajoutées à l'intention.

PowerShell

```
    Get-NetIntent -Name Cluster_Compute
```

Remplacements globaux et paramètres réseau de cluster

Network ATC se compose principalement de deux types de remplacements globaux : configurations de proxy et fonctionnalités réseau de cluster.

Fonctionnalités réseau de cluster

Dans cette section, nous allons sur l'ensemble des nouvelles fonctionnalités de réseau de cluster. Les nouvelles fonctionnalités de réseau de cluster permettent et optimisent le nommage du réseau de cluster, la gestion des réseaux de cluster en contrôlant les options de performances, les limites de bande passante et la gestion des migrations dynamiques.

Nommage du réseau de cluster

Description : par défaut, le clustering de basculement nomme toujours des sous-réseaux uniques comme suit : « Cluster Network 1 », « Cluster Network 2 », et ainsi de suite. Cela n'est pas connecté à l'utilisation réelle du réseau, car il n'existe aucun moyen pour le clustering de savoir comment vous avez prévu d'utiliser les réseaux – jusqu'à présent !

Une fois que vous avez défini votre configuration via Network ATC, nous comprenons maintenant comment les sous-réseaux vont être utilisés, et nous pouvons nommer les réseaux de cluster de manière plus appropriée. Par exemple, nous savons quel sous-réseau est utilisé

pour la gestion, le réseau de stockage 1, le réseau de stockage 2 (et ainsi de suite, le cas échéant). Par conséquent, nous pouvons nommer les réseaux de manière plus contextuelle.

Dans la capture d'écran suivante, vous pouvez voir que l'intention de stockage a été appliquée à cet ensemble d'adaptateurs. Il existe un autre réseau de cluster inconnu indiqué par l'administrateur.

```
PS C:\> Get-ClusterNetwork

Name                              State Metric            Role
----                              ----- ------            ----
storage_compute(Storage_VLAN711)     Up  20640         Cluster
storage_compute(Storage_VLAN712)     Up  20641         Cluster
Unused:Cluster Network 2             Up  70384 ClusterAndClient
```

Sélection du réseau de migration dynamique

Cette valeur active ou désactive la logique de sélection du réseau de cluster de migration dynamique basée sur l'intention. Par défaut, cette option est activée ($true) et entraîne la sélection des réseaux de cluster en fonction des informations d'intention envoyées. Si la sélection du réseau de migration dynamique est désactivée, l'utilisateur peut définir un réseau de migration dynamique et le comportement par défaut rétablit ce que vous attendez en l'absence d'ATC réseau.

Activer la migration des machines virtuelles : sélection des performances

Cette valeur active ou désactive la sélection basée sur l'intention des transports de migration dynamique des machines virtuelles. Par défaut, cela est activé et aboutit au système pour déterminer automatiquement le meilleur transport de migration dynamique, par exemple : SMB, Compression, TCP.

Si cette option est désactivée :

- La sélection de transport de migration dynamique utilise le transport spécifié dans La valeur de remplacement VirtualMachineMigrationPerformanceOption.
- Si la valeur de remplacement VirtualMachineMigrationPerformanceOption n'est pas spécifiée, Network ATC rétablit le comportement lorsque Network ATC était absent.
- Si la valeur est null, mais VirtualMachineMigrationPerformanceOption est configurée, configurez cette option pour $false et utilisez l'option spécifiée dans le remplacement VirtualMachineMigrationPerformanceOption.

Option de performances de migration des machines virtuelles

Network ATC configure le transport de migration dynamique vers TCPIP, Compression ou SMB. Si la valeur est Null, le système calcule la meilleure option en fonction de la configuration et des fonctionnalités du système.

Nombre maximal de migrations de machines virtuelles simultanées

Network ATC définit le nombre par défaut de migrations simultanées de machines virtuelles vers un. La plage de valeurs possibles autorisées pour cette propriété est une à 10.

Bande passante de migration SMB maximale

Cette valeur applique une limite de bande passante spécifique (en Gbits/s) sur le trafic de migration dynamique transporté par SMB pour empêcher la consommation de la classe de trafic SMB. Cette valeur est utilisable uniquement si le transport de migration dynamique est SMB. La valeur par défaut est calculée.

Personnaliser les paramètres réseau du cluster

Les fonctionnalités réseau de cluster fonctionnent via leurs valeurs par défaut définies. Étant donné que la désactivation des fonctionnalités réseau de cluster ne vous place pas dans un scénario non pris en charge, Network ATC a une option pour un globaloverride. Vous pouvez utiliser le remplacement global pour ajuster les propriétés et rendre les propriétés de fonctionnalités réseau de cluster personnalisées en fonction de vos besoins.

Pour ajouter un GlobalOverride avec Network ATC :

PowerShell

```
$clusterOverride = New-NetIntentGlobalClusterOverrides
```

La variable « clusterOverride » a les propriétés suivantes :

```
PS C:\Users\wolfpack> $clusterOverride


EnableNetworkNaming                                :
EnableLiveMigrationNetworkSelection                : True
EnableVirtualMachineMigrationPerformanceSelection  :
VirtualMachineMigrationPerformanceOption           :
MaximumVirtualMachineMigrations                    :
MaximumSMBMigrationBandwidthInGbps                 :
InstanceId                                         : 49d9a1fa-53ad-4bac-8dd3-8916f34b[illegible]fb
ObjectVersion                                      : 1.0.0.10
```

Une fois que vous avez défini une propriété pour le remplacement, vous pouvez l'ajouter en tant que GlobalOverride pour votre cluster avec la commande suivante :

```
PowerShell
Set-NetIntent -GlobalClusterOverrides $clusterOverride
```

Pour vérifier un déploiement réussi de votre clusterOverride, exécutez :

```
PowerShell
Get-NetIntentStatus -Globaloverrides
```

Pour supprimer GlobalClusterOverride, exécutez les opérations suivantes :

```
PowerShell
Remove-NetIntent -GlobalOverrides $clusterOverride
```

Configurations de proxy

Le proxy est différent des remplacements ATC existants, car il n'est pas lié à une intention spécifique. En fait, nous prenons en charge la configuration du proxy lorsqu'il n'existe aucune intention. Nous prenons en charge ce scénario le mieux en implémentant de nouveaux paramètres de remplacement globaux sur Add/Set/Get-NetIntent, comme pour les fonctionnalités réseau de cluster.

La `New-NetIntentGlobalProxyOverrides` commande est utilisée pour créer un objet de remplacement similaire aux remplacements QoS, RSS et SwitchConfig existants. La commande aura deux jeux de paramètres :

Jeu de paramètres par défaut

ProxyServer : Le paramètre ProxyServer prend des chaînes en tant qu'entrées, qui représentent l'URL du serveur proxy à utiliser pour le trafic https. ProxyServer est un paramètre obligatoire lors de la configuration du proxy.

ProxyBypass : Le paramètre ProxyBypass prend la liste des sites qui doivent être visités en contournant le proxy. Pour contourner tous les hôtes de nom court, utilisez `local`.

AutoDetect : AutoDetect est un paramètre true ou false qui détermine si la découverte automatique du proxy web (WPAD) doit être activée.

Jeu de paramètres AutoDetect

AutoConfigUrl : Le paramètre AutoConfigUrl prend une chaîne avec l'URL du serveur proxy à utiliser pour le trafic http et/ou https comme entrée. Pour les deux classes de trafic, utilisez un point-virgule pour séparer. Il s'agit d'un paramètre obligatoire.

AutoDetect : similaire au paramètre AutoDetect ci-dessus, il s'agit d'un paramètre true ou false qui détermine si la découverte automatique du proxy web (WPAD) doit être activée.

Configuration du proxy

Vous pouvez définir vos configurations de proxy de la manière suivante :

PowerShell

```
$ProxyOverride = New-NetIntentGlobalProxyOverrides -ProxyServer
https://itg.contoso.com:3128 -ProxyBypass *.foo.com
```

À l'aide du `AutoConfigURL` commutateur, vous pouvez définir votre configuration de proxy de la manière suivante :

PowerShell

```
$ProxyOverride = New-NetIntentGlobalProxyOverrides -AutoConfigUrl
https://itg.contoso.com
```

Vous pouvez ajouter un GlobalProxyOverride pour votre cluster comme suit :

PowerShell

```
Set-NetIntent -GlobalProxyOverride $ProxyOverride
```

Pour supprimer un GlobalProxyOverride pour votre cluster comme suit :

PowerShell

```
Remove-NetIntent -GlobalOverride $ProxyOverride
```

Enfin, pour accéder à n'importe quel remplacement global, proxy ou cluster, vous pouvez exécuter les commandes suivantes :

PowerShell

```
$Obj1 = Get-NetIntent -GlobalOverride
$Obj1
```

Plus précisément, vous pouvez accéder aux remplacements globaux de proxy et de cluster respectivement, en appelant leurs paramètres respectifs pour `$Obj1`:

PowerShell

```
$Obj1.ProxyOverride
$Obj1.ClusterOverride
```

Mettre à jour ou remplacer les paramètres réseau

Cette tâche vous aide à remplacer la configuration par défaut qui a déjà été déployée. Cet exemple modifie la réservation de bande passante par défaut pour SMB Direct.

> **Important**
>
> Nous vous recommandons d'utiliser les paramètres par défaut, basés sur les bonnes pratiques de Microsoft.

1. Obtenez la liste des applets de commande de remplacement possibles. Nous utilisons des caractères génériques pour afficher les options disponibles :

   PowerShell

   ```
   Get-Command -Noun NetIntent*Over* -Module NetworkATC
   ```

2. Créez un objet de remplacement pour la configuration de la qualité de service (QoS) DCB :

   PowerShell

   ```
   $QosOverride = New-NetIntentQosPolicyOverrides
   $QosOverride
   ```

3. Modifiez le pourcentage de bande passante pour SMB Direct :

   PowerShell

   ```
   $QosOverride.BandwidthPercentage_SMB = 25
   ```

```
$QosOverride
```

> ⓘ **Notes**
>
> Les valeurs sont affichées uniquement pour les propriétés que vous remplacez.

4. Envoyez la demande d'intention en spécifiant le remplacement :

```PowerShell
Set-NetIntent -Name Cluster_ComputeStorage -QosPolicyOverrides $QosOverride
```

5. Attendez la fin de l'état d'approvisionnement :

```PowerShell
Get-NetIntentStatus -Name Cluster_ComputeStorage | Format-Table IntentName,
Host, ProvisioningStatus, ConfigurationStatus
```

6. Vérifiez que le remplacement a été correctement défini sur tous les nœuds du cluster. Dans l'exemple, la classe de trafic SMB_Direct a été remplacée par un pourcentage de bande passante de 25 % :

```PowerShell
Get-NetQosTrafficClass -Cimsession (Get-ClusterNode).Name | Select
PSComputerName, Name, Priority, Bandwidth
```

Tester Network ATC dans les machines virtuelles

L'exécution d'Azure Local dans des machines virtuelles est utile pour les environnements de test. Pour ce faire, ajoutez une propriété d'adaptateur remplacée à votre intention qui désactive la propriété d'adaptateur **NetworkDirect** :

```PowerShell
$AdapterOverride = New-NetIntentAdapterPropertyOverrides
$AdapterOverride.NetworkDirect = 0
Add-NetIntent -Name MyIntent -AdapterName vmNIC01, vmNIC02 -Management -Compute -
Storage -AdapterPropertyOverrides $AdapterOverride
```

> ⓘ **Notes**
>
> Vérifiez que vous disposez de plusieurs processeurs virtuels sur chaque machine virtuelle.

Supprimer une intention

Parfois, vous pouvez avoir besoin de supprimer toutes les intentions et de recommencer, pour tester une configuration différente, par exemple. Même si vous pouvez supprimer les intentions avec la cmdlet Remove-NetIntent, cela ne nettoie pas les commutateurs virtuels et les configurations DCB/NetQoS créés pour les intentions. Network ATC s'efforce de ne rien détruire sur votre système, ce qui est généralement une bonne chose, mais cela signifie que vous devez effectuer des étapes manuelles pour recommencer.

Pour supprimer toutes les intentions réseau ainsi que les commutateurs virtuels et les configurations NetQoS créés par Network ATC pour ces intentions, exécutez le script suivant dans une session PowerShell exécutée localement sur l'un des serveurs du cluster (peu importe lequel).

PowerShell

```
$clusname = Get-Cluster
$clusternodes = Get-ClusterNode
$intents = Get-NetIntent -ClusterName $clusname

foreach ($intent in $intents)
{
    Remove-NetIntent -Name $intent.IntentName -ClusterName $clusname
}

foreach ($intent in $intents)
{
    foreach ($clusternode in $clusternodes)
    {
        Remove-VMSwitch -Name "*$($intent.IntentName)*" -ComputerName $clusternode
-ErrorAction SilentlyContinue -Force
    }
}

foreach ($clusternode in $clusternodes)
{
    New-CimSession -ComputerName $clusternode -Name $clusternode
    $CimSession = Get-CimSession
    Get-NetQosTrafficClass -CimSession $CimSession | Remove-NetQosTrafficClass -
CimSession $CimSession
    Get-NetQosPolicy -CimSession $CimSession | Remove-NetQosPolicy -Confirm:$false
-CimSession $CimSession
    Get-NetQosFlowControl -CimSession $CimSession | Disable-NetQosFlowControl -
```

```
CimSession $CimSession
    Get-CimSession | Remove-CimSession
}
```

Pour supprimer la configuration d'un déploiement par nœud, copiez et collez les commandes suivantes sur chaque nœud pour supprimer toutes les intentions existantes et leur commutateur virtuel correspondant :

PowerShell

```
$intents = Get-NetIntent
foreach ($intent in $intents)
{
    Remove-NetIntent -Name $intent.IntentName
    Remove-VMSwitch -Name "*$($intent.IntentName)*" -ErrorAction SilentlyContinue
-Force
}

Get-NetQosTrafficClass | Remove-NetQosTrafficClass
Get-NetQosPolicy | Remove-NetQosPolicy -Confirm:$false
Get-NetQosFlowControl | Disable-NetQosFlowControl
```

Tâches post-déploiement

Les tâches à effectuer à la suite d'un déploiement AtC réseau dépendent de la version d'Azure Stack HCI utilisée. Pour les clusters Azure Stack HCI 21H2 :

- **Ajouter des adresses IP aux adaptateurs de stockage :** utilisez DHCP sur les réseaux locaux virtuels de stockage ou définissez des adresses IP statiques à l'aide de l'applet de commande NetIPAdress. Vous ne pouvez pas utiliser les adresses d'adressage IP privé automatique (APIPA) fournies aux cartes qui ne peuvent pas obtenir d'adresse d'un serveur DHCP.

- **Définir les limites de bande passante SMB :** si la migration dynamique utilise SMB Direct (RDMA), configurez une limite de bande passante pour vous assurer que la migration dynamique ne consomme pas toutes les bandes passantes utilisées par espaces de stockage direct et le clustering de basculement.

- **Configuration du cluster étendu :** pour ajouter Stretch S2D à votre système managé Network ATC, vous devez ajouter manuellement la configuration appropriée (y compris les cartes réseau virtuelles, etc.) une fois que Network ATC a implémenté l'intention spécifiée.

L'adressage IP automatique pour les cartes de stockage, les limites de bande passante SMB et les configurations Stretch peuvent désormais être déployées avec Network ATC dans Azure

Local. Pour plus d'informations, consultez :

- Adressage IP de stockage automatique : **adressage** IP de stockage automatique avec ATC réseau
- **Paramètres réseau du cluster et configuration** SMB : adressage IP de stockage automatique avec ATC réseau
- **Configuration** du cluster Stretch : configurer Stretch Clustering avec Network ATC

Valider la correction automatique

Network ATC s'assure que la configuration déployée reste identique sur tous les nœuds du cluster. Dans cette section facultative, nous modifions notre configuration (sans remplacement) en émulant une modification accidentelle de la configuration et observons comment la fiabilité du système est améliorée en corrigeant la propriété mal configurée.

1. Vérifiez la valeur MTU (JumboPacket) existante de la carte :

   PowerShell

   ```
   Get-NetAdapterAdvancedProperty -Name pNIC01, pNIC02, vSMB* -RegistryKeyword
   *JumboPacket -Cimsession (Get-ClusterNode).Name
   ```

2. Modifiez une des unités MTU de la carte physique sans spécifier de remplacement. Cela émule une modification accidentelle ou une « dérive de configuration », qui doit être corrigée.

   PowerShell

   ```
   Set-NetAdapterAdvancedProperty -Name pNIC01 -RegistryKeyword *JumboPacket -
   RegistryValue 4088
   ```

3. Vérifiez que la valeur MTU (JumboPacket) existante de la carte a été modifiée :

   PowerShell

   ```
   Get-NetAdapterAdvancedProperty -Name pNIC01, pNIC02, vSMB* -RegistryKeyword
   *JumboPacket -Cimsession (Get-ClusterNode).Name
   ```

4. Testez à nouveau la configuration. Cette étape sert uniquement à accélérer la résolution du problème. Network ATC corrigera automatiquement cette configuration.

   PowerShell

```
Set-NetIntentRetryState -ClusterName CLUSTER01 -Name Cluster_ComputeStorage -
NodeName Node01
```

5. Vérifiez que la vérification de cohérence est terminée :

PowerShell

```
Get-NetIntentStatus -ClusterName CLUSTER01 -Name Cluster_ComputeStorage
```

6. Vérifiez que l'unité MTU (JumboPacket) de la carte est revenue à la valeur attendue :

PowerShell

```
Get-NetAdapterAdvancedProperty -Name pNIC01, pNIC02, vSMB* -RegistryKeyword
*JumboPacket -Cimsession (Get-ClusterNode).Name
```

Pour obtenir plus d'exemples de validation, consultez la démonstration Network ATC.

Étapes suivantes

- En savoir plus sur Network ATC.
- En savoir plus sur les clusters étendus.

Qu’est-ce que network HUD pour Windows Server ?

S’applique à: ✅ Windows Server 2025

> ⓘ **Important**
>
> L’HUD réseau pour Windows Server est actuellement en préversion. Ces informations concernent un produit en version préliminaire qui peut être sensiblement modifié avant sa commercialisation. Microsoft n’offre aucune garantie, exprimée ou implicite, en ce qui concerne les informations fournies ici.

Network HUD est un outil de diagnostic de mise en réseau hôte et opérationnel qui analyse et corrige les problèmes de mise en réseau de l’hôte. Network HID s'exécute en continu, corrélant les liens des commutateurs physiques, les paramètres des adaptateurs hôtes, et les rôles de cluster qui les utilisent. À l’aide de données d’intention réseau, Network HUD sélectionne les tests pertinents et déclenche des alertes précoces lorsque des problèmes émergents menacent les performances ou la stabilité de la charge de travail.

La mise en réseau de l’hôte peut être compliquée à dépanner, car vous devez collecter des informations à partir des commutateurs d’infrastructure physique, des hôtes de cluster, des paramètres des adaptateurs réseau et des charges de travail des invités. Cette séparation masque les causes racines, ralentit la correction et augmente le risque de dégradation des performances ou de la stabilité. L’HUD réseau vous aide à :

- Identifiez la configuration incorrecte sur le réseau physique. Par exemple, la priorité VLAN ou la priorité PFC manquante.
- Détectez les problèmes matériels opérationnels, tels que le flapping, les adaptateurs instables ou la sursouscription PCIe.
- Optimisez et validez la symétrie de la configuration de l’hôte et la préparation du pilote.
- Améliorer automatiquement certaines conditions, telles que la suppression d'adaptateurs instables du service, lorsque cela peut être fait en toute sécurité.

Disponibilité et exigences

Pour que le HUD réseau soit disponible pour vous, vous devez être éligible à la gestion de Windows Server activée par Azure Arc. Pour en savoir plus sur la disponibilité de l’avantage du HUD réseau, consultez Gestion de Windows Server activée par Azure Arc.

Lorsque vos machines sont éligibles à Windows Server Management activée par Azure Arc, votre environnement doit répondre aux exigences suivantes :

- Vous utilisez le cluster de basculement Windows Server.
- Les nœuds de cluster doivent exécuter Windows Server 2025 Datacenter.
- Network ATC est déployé avec des intentions de mise en réseau hôte. Pour en savoir plus sur le déploiement de Network ATC, voir Déployer la mise en réseau de l'hôte avec Network ATC.
- Le cluster doit avoir activé les espaces de stockage direct (S2D) (requis pour le service d'intégrité du cluster). Pour en savoir plus sur le déploiement d'espaces de stockage direct, consultez Déployer des espaces de stockage direct sur Windows Server.
- Chaque nœud de cluster doit être connecté à Azure Arc.

Terminologie

Le tableau suivant définit certains des termes clés utilisés dans ce document :

Agrandir le tableau

Terme	Definition
HUD réseau : HUD réseau	Windows Server Management, activé par Azure Arc, fournit une fonctionnalité qui analyse et, dans la mesure du possible, corrige les problèmes de réseau de l'hôte.
HUD réseau : contenu	Packages logiques de détection téléchargés séparément et mis à jour au fil du temps ; peuvent s'exécuter déconnectés.
HUD réseau : détection de contenu	Unités de détection individuelles qui surveillent le comportement indiquant qu'un problème se produit ou risque de se produire.
Network ATC : Intent	Définition de la façon dont vous envisagez d'utiliser un ou plusieurs adaptateurs physiques. Par exemple, un jeu de gestion/de calcul/stockage convergé. Chaque adaptateur physique ne peut appartenir qu'à une seule intention.
AtC réseau : Type d'intention	Rôle attribué dans une intention. Types pris en charge : Gestion, Calcul, Stockage, Stretch (similaire au stockage, mais sans RDMA).

Fonctionnement de Network HUD

Network HUD est conscient des clusters et interprète continuellement les signaux bruts d'hôte et d'infrastructure dans le contexte des intentions déclarées de Network ATC et des états de cluster. Au lieu de traiter des adaptateurs, des commutateurs et des rôles comme des composants isolés, il les met en corrélation sur le cluster afin de comprendre l'instabilité

émergente dans un contexte opérationnel. Par exemple, il détecte un port oscillant dans le cadre des fonctionnalités de stockage, de calcul ou de gestion. Chaque détection combine plusieurs flux de télémétrie pour réduire le bruit et ne faire remonter que les anomalies de santé actionnables.

Pour mettre en évidence des anomalies de santé actionnables, Network HUD collecte et normalise les événements à partir de :

- Métadonnées d'intention ATC réseau qui précisent ce que chaque adaptateur doit transporter, en déterminant les tests pertinents et en supprimant les sondes inutiles.
- LLDP échange avec des commutateurs en haut de rack pour mapper les ports physiques, l'annonce VLAN et l'aptitude du contrôle de flux prioritaire pour le trafic RDMA.
- Les journaux d'événements signalant la réinitialisation de l'adaptateur, les transitions d'état de liaison ou les anomalies de charge du pilote qui précèdent souvent la dégradation des performances.
- Compteurs de performances et métriques d'adaptateur en temps réel pour la bande passante, les indicateurs de congestion et la stabilité.
- Insights au niveau des paquets (à l'aide de `pktmon`) et des propriétés matérielles de bas niveau lorsque la précision est requise. Par exemple, la validation du risque de sursubscription.

Ces entrées sont combinées dans des détections sensibles aux intentions qui publient des erreurs de santé via le pipeline de santé du cluster existant, ce qui fait que Windows Admin Center et PowerShell reflètent les problèmes réseau. L'HUD réseau s'exécute localement sur chaque nœud pour une faible latence et une robustesse.

Scénarios de détection de santé

Network HUD détecte de manière proactive les conditions de mise en réseau de l'hôte qui précèdent généralement l'instabilité ou la dégradation des performances. Les scénarios suivants traduisent des signaux de détection bruts en erreurs d'intégrité actionnables que vous pouvez corriger avant que des configurations incorrectes ou des problèmes matériels affectent les performances ou la stabilité de la charge de travail.

Agrandir le tableau

Détection	Objectif
Échec des requêtes d'ATC réseau	Détecte les intentions qui ne provisionnent pas complètement (cartes virtuelles manquantes, QoS, paramètres de stockage) pour empêcher la dérive silencieuse et les lignes de base non fiables.

Détection	Objectif
Types d'intention de réseau ATC manquants	Garantit que les rôles de trafic requis (gestion, calcul, stockage) existent afin que les diagnostics spécifiques aux rôles s’exécutent ; absence réduit la couverture et masque le trafic non managé.
Surcharge de bande passante PCIe	Comparez les taux de liaison agrégés des cartes réseau à la capacité de la voie du slot/PCIe ; le surabonnement peut entraîner un bridage et des performances incohérentes sous charge.
Adaptateurs instables (flapping)	Signale les fréquentes réinitialisations ou pertes de lien qui provoquent des basculements, augmentent la latence et dégradent le débit avant que l'impact sur la charge de travail ne s'aggrave.
Pilotes de production de boîte de réception (non pris en charge)	Identifie les cartes réseau qui utilisent uniquement des pilotes de boîte de réception de base ne disposant pas de déchargement et d’optimisations avancés, augmentant ainsi le risque pour la fiabilité et les performances.
Conducteurs vieillissants ou obsolètes	Évalue l'âge du paquet de pilotes et identifie tôt les besoins de maintenance. Avertit lorsqu’un pilote a plus de deux ans pour planifier une mise à jour. L'interface de contrôle du réseau élève les avertissements à une faute lorsqu'un conducteur dépasse trois ans d'utilisation.
Incohérence de version du pilote	Détecte les versions incompatibles entre les adaptateurs identiques, empêchant le comportement asymétrique et les performances imprévisibles.
État opérationnel LLDP	Indique l'absence de paquets LLDP ou un échec d'analyse, ce qui réduit la détection des liaisons de commutateur physique et dégrade d'autres tests de validation du réseau.
Réseaux locaux virtuels mal configurés ou incohérents	Compare les VLANs publiés par rapport aux VLANs attendus entre les membres de l'intent du même hôte, le même intent sur tous les hôtes, et contre la disponibilité requise de la charge de travail (VLAN des cartes réseau de machine virtuelle). Les écarts risquent une perte de connectivité de machine virtuelle ou un échec d’isolation du stockage. Cohérence du VLAN sur trois étendues discrètes pour intercepter la mauvaise configuration localisée avant qu'elle ne devienne un problème de cluster : étendue de l'intent du même hôte : les ports de commutateur pertinents doivent annoncer le même ensemble de VLAN attribué à chaque adaptateur dans le même intent ATC réseau sur un seul hôte. Étendue de l’intention du cluster : tous les ports de commutation doivent annoncer un ensemble de VLAN cohérent aux adaptateurs dans la même intention d’ATC réseau sur chaque hôte du cluster. Étendue de disponibilité de la charge de travail : les VLAN requis pour toutes les charges de travail de calcul (les cartes réseau des machines virtuelles) doivent être annoncés à chaque adaptateur participant à la même intention de Network ATC à chaque hôte.
Contrôle de flux de priorité	Pour les adaptateurs d'intention de stockage, Network HUD compare les priorités annoncées par LLDP depuis le commutateur physique avec la PFC configurée par

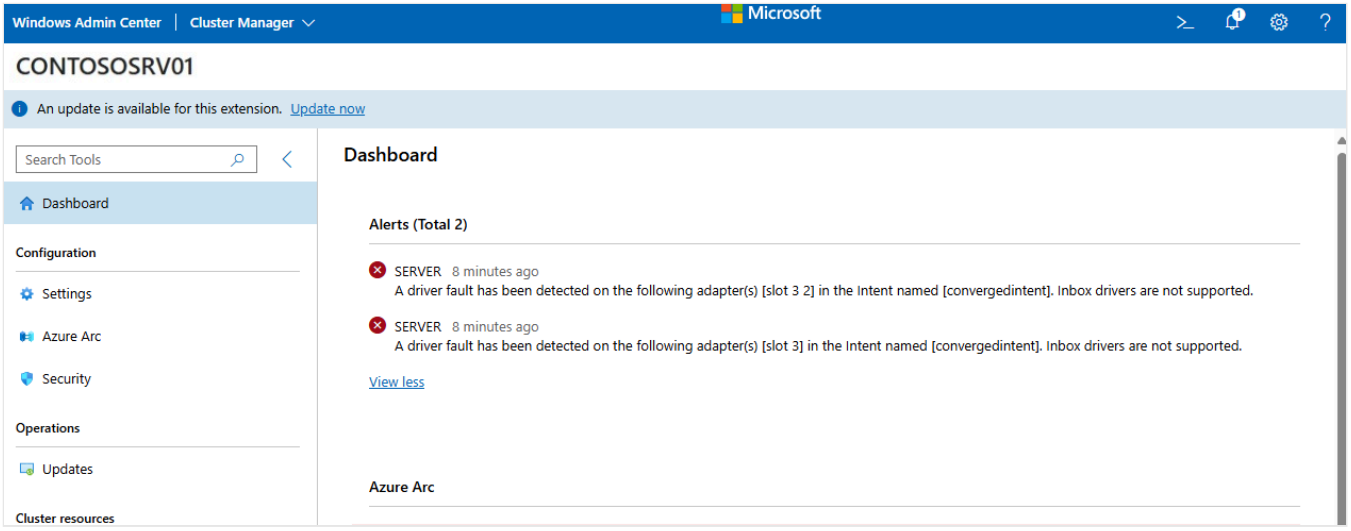
Détection	Objectif
incohérent (PFC)	l'hôte. Les indicateurs manquants ou incompatibles peuvent entraîner une congestion, des conditions de pause prolongées, une latence élevée ou des échecs de stockage (S2D). Alignement des priorités PFC pour le trafic de stockage via RDMA avec la configuration des intentions de l'hôte. Pour les adaptateurs d'intention de stockage, la validation PFC inclut la comparaison des priorités publiées par LLDP à partir du commutateur avec les priorités activées par Network ATC sur l'hôte. Les indicateurs réseau HUD signalent les configurations incohérentes pour assurer que la congestion, les conditions de pause prolongées, la latence élevée ou les échecs de stockage (S2D) n'ont pas lieu.

Les administrateurs peuvent interroger des erreurs à l'aide de PowerShell, par exemple :

PowerShell

```
Get-HealthFault | Where-Object Reason -like '*HUD*'
```

Les administrateurs peuvent également afficher les pannes HUD réseau dans les vues de santé du cluster dans le Windows Admin Center. La capture d'écran suivante montre un exemple d'erreur HUD réseau dans Windows Admin Center :



Étapes suivantes

- Installer l'HUD réseau pour Windows Server
- Gestion de Windows Server activée par Azure Arc.
- Déployez la mise en réseau de l'hôte avec Network ATC.
- Déployer des espaces de stockage direct sur Windows Server.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Last updated on 17/11/2025

Installer l'HUD réseau pour Windows Server

S'applique à: ✅ Windows Server 2025

> **ⓘ Important**
>
> L'HUD réseau pour Windows Server est actuellement en préversion. Ces informations concernent un produit de version préliminaire susceptible d'être sensiblement modifié avant sa publication. Microsoft n'offre aucune garantie, exprimée ou implicite, en ce qui concerne les informations fournies ici.

Network HUD est un outil de diagnostic du réseau hôte, conscient des clusters et dirigé par l'intention, qui analyse en permanence les adaptateurs, les connexions et les signaux de commutateurs pour détecter précocement les anomalies de santé exploitables. Cet article explique comment activer Network HUD sur un déploiement en cluster de Windows Server 2025 Datacenter connecté à Azure Arc et comment afficher les fautes d'intégrité à l'aide de Windows Admin Center ou de PowerShell.

Prerequisites

Avant d'installer Network HUD, vérifiez que vous disposez des conditions préalables suivantes :

- Configuration requise pour le clustering de basculement Windows Server :
  - Vous avez au moins un nœud dans le cluster.
  - Les nœuds de cluster doivent exécuter Windows Server 2025 Datacenter.
  - Network ATC est déployé avec des intentions de mise en réseau hôte. Pour en savoir plus sur le déploiement de Network ATC, voir Déployer la mise en réseau de l'hôte avec Network ATC.
  - Le cluster doit avoir activé les espaces de stockage direct (S2D). Pour en savoir plus sur le déploiement d'espaces de stockage direct, consultez Déployer des espaces de stockage direct sur Windows Server.
  - Chaque nœud de cluster a l'application `DataCenterBridging LLDP Tools` installée à partir de la fonctionnalité Outils d'administration de serveur distant.

- Configuration requise pour Azure Arc :
  - Chaque nœud de cluster doit être connecté à Azure Arc.
  - Vous devez être éligible à Windows Server Management activé par Azure Arc. Pour en savoir plus sur la disponibilité de l'avantage HUD réseau, consultez Gestion de Windows Server activée par Azure Arc.

- L’HUD réseau est disponible uniquement sur les machines des régions suivantes :
  - USA Est 2 EUAP
  - EUAP USA Centre
  - Central US
  - Est des États-Unis 2
  - East US
  - Canada Central
  - Ouest des États-Unis 2
  - Europe Nord
  - Europe Ouest
  - Japon Est
  - Asie du Sud-Est
  - Australia East

- L’HUD réseau pour Windows Server a les mêmes exigences de commutateur réseau que Celles d’Azure Local. Lorsque vous utilisez network HUD sur Windows Server, vérifiez que vous utilisez des commutateurs physiques validés pour Azure Local et que les exigences de commutateur réseau sont remplies. Pour plus d’informations, consultez les sections ***Commutateurs réseau pour Azure Local*** et ***Exigences relatives aux commutateurs réseau*** dans Exigences du réseau physique pour Azure Local. Les autres sections de l'article sur les exigences réseau physique pour Azure Local ne s'appliquent pas à HUD réseau Windows. Serveur

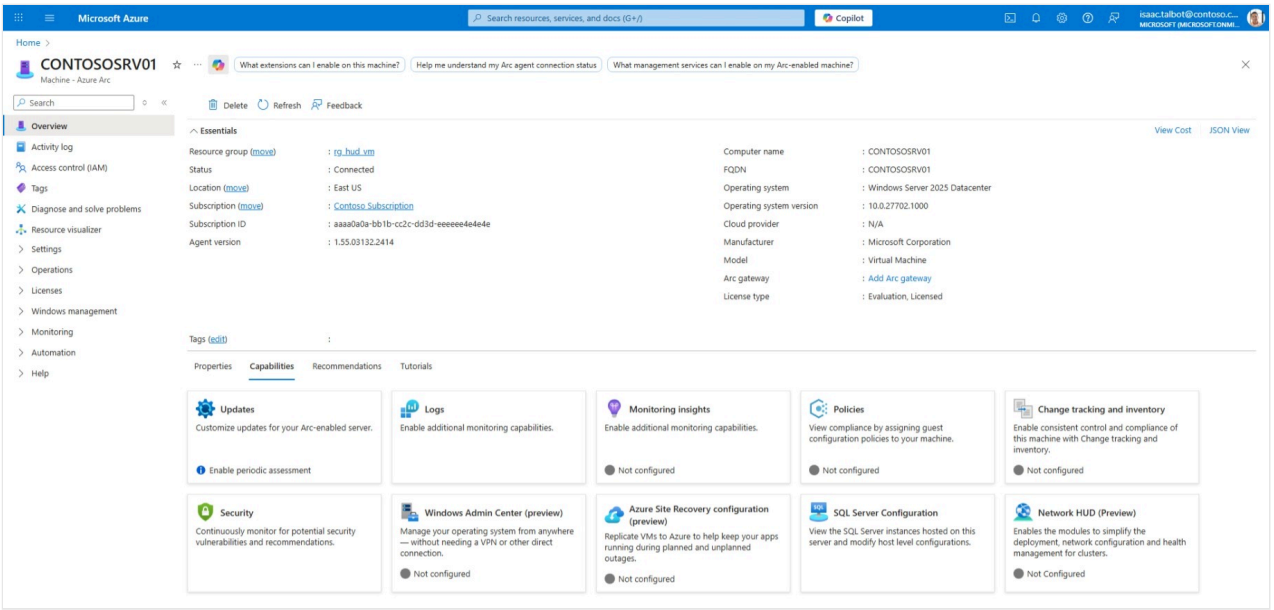
Activer l’extension HUD réseau dans le portail Azure

Pour utiliser le portail Azure pour activer l’extension HUD réseau, procédez comme suit :

1. Accédez au portail Azure, puis recherchez et sélectionnez **Machines - Azure Arc**.

2. Sélectionnez l’ordinateur sur lequel vous souhaitez activer l’extension HUD réseau.

3. Sélectionnez la vignette **Network HUD** .



4. Lorsque vous êtes prêt, sélectionnez **Activer**.

5. Une fois l'extension activée, un message de confirmation s'affiche et la vignette s'affiche comme **activée**.

Afficher les défauts de santé

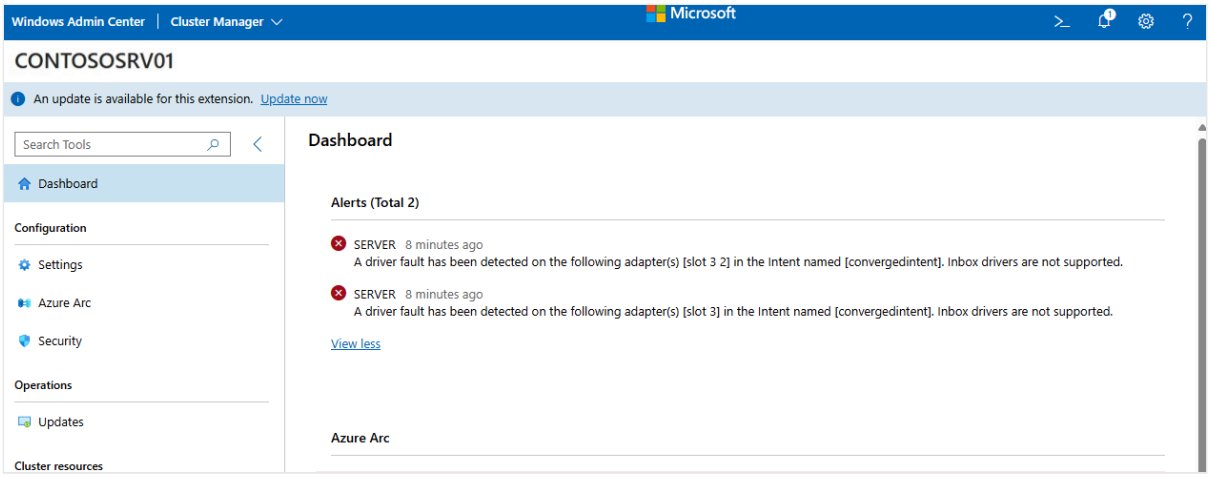
Pour vérifier l'installation et afficher les défaillances de santé, sélectionnez votre méthode préférée.

Centre d'administration Windows

Pour vérifier l'installation et afficher les erreurs de diagnostic avec Windows Admin Center, procédez comme suit :

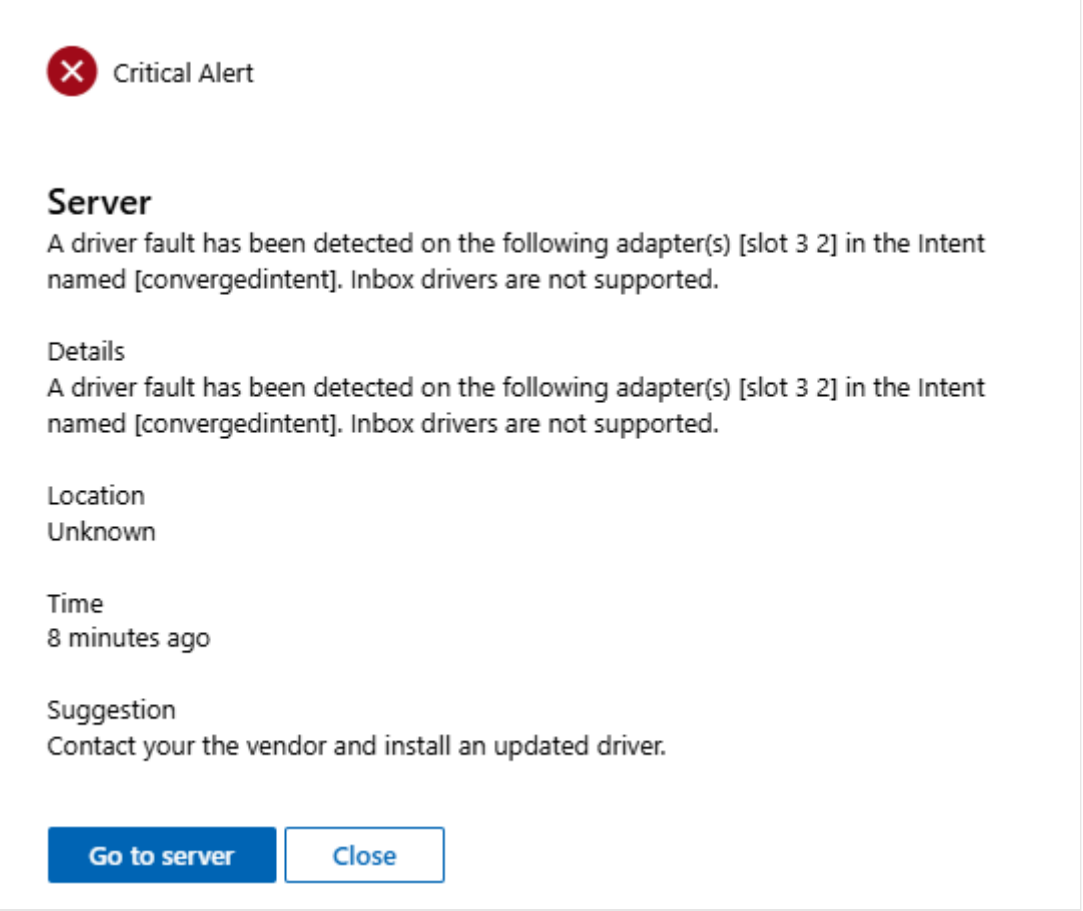
1. Ouvrez Windows Admin Center et connectez-vous à votre cluster Windows Server 2025 Datacenter.

2. Dans l'affichage Cluster, affichez les alertes à partir du tableau de bord ou sélectionnez l'icône de cloche de notification en haut à droite.



3. Recherchez les alertes liées à l'HUD réseau. Ces alertes fournissent des informations sur les problèmes de mise en réseau hôte détectés.

4. Sélectionnez une alerte pour afficher plus de détails et les actions recommandées pour la correction.



Les alertes se résolvent automatiquement lorsque le problème sous-jacent est résolu.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Last updated on 17/11/2025

Mise en réseau définie par logiciel (SDN)

Découvrez les fonctionnalités, la technologie et le déploiement du SDN (Software Defined Networking).

À propos de la mise en réseau définie par logiciel

VUE D'ENSEMBLE

Vue d'ensemble de la mise en réseau définie par logiciel (SDN)

Sécurité pour SDN

NOUVEAUTÉS

Nouveautés du SDN pour Windows Server 2019

CONCEPT

Composants clés de l'architecture SDN

VIDEO

Mécanique Microsoft SDN

Get started

DÉMARRAGE

Planifier une infrastructure SDN

Déployer une infrastructure SDN

Gérer une infrastructure SDN

VUE D'ENSEMBLE

Résoudre les problèmes et diagnostiquer une infrastructure SDN

Ressources d'apprentissage SDN

ENTRAINEMENT

Résoudre les problèmes de configuration des paramètres de bande passante VPN de la passerelle SDN RAS dans VMM

Feuille de données de mise en réseau définie par logiciel Microsoft

SDN Technologies

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Les rubriques de cette section fournissent une vue d'ensemble ainsi que des informations techniques sur les technologies SDN (Software-Defined Networking) incluses dans Windows Server.

Contrôleur de réseau

Le Contrôleur de réseau fournit un point d'automatisation centralisé et programmable pour la gestion, la configuration, le monitoring ainsi que la résolution des problèmes de l'infrastructure réseau virtuelle et physique de votre centre de données. Avec le Contrôleur de réseau, vous pouvez automatiser la configuration de l'infrastructure réseau au lieu d'effectuer une configuration manuelle des périphériques et des services réseau.

Le Contrôleur de réseau est un serveur hautement disponible et scalable. Il fournit deux interfaces de programmation d'applications (API) :

1. **API Southbound** : permet au contrôleur de réseau de communiquer avec le réseau.
2. **API Northbound** : vous permet de communiquer avec le contrôleur de réseau.

Vous pouvez utiliser Windows PowerShell, l'API REST (Representational State Transfer) ou une application de gestion pour gérer l'infrastructure réseau physique et virtuelle suivante :

- Ordinateurs virtuels Hyper-V et commutateurs virtuels
- Commutateurs de réseau physique
- Routeurs de réseau physique
- Logiciel de pare-feu
- Passerelles VPN, notamment les passerelles multilocataires RAS (service d'accès à distance)
- Équilibreurs de charge

Virtualisation de réseau Hyper-V

La fonctionnalité Virtualisation de réseau Hyper-V (HNV) vous aide à isoler vos applications et vos charges de travail du réseau physique en utilisant des réseaux virtuels. Les réseaux virtuels fournissent l'isolation mutualisée nécessaire moyennant une exécution sur une structure réseau physique partagée, ce qui augmente l'utilisation des ressources. Pour pouvoir reporter vos

investissements existants, vous pouvez configurer des réseaux virtuels sur le matériel réseau existant. De plus, les réseaux virtuels sont compatibles avec les réseaux locaux virtuels (VLAN).

Commutateur virtuel Hyper-V

Le commutateur virtuel Hyper-V est un commutateur réseau Ethernet logiciel de couche 2, disponible dans le Gestionnaire Hyper-V, une fois que vous avez installé le rôle serveur Hyper-V. Le commutateur offre des fonctionnalités gérées par programme et extensibles pour connecter des machines virtuelles aux réseaux virtuels et au réseau physique à la fois. De plus, le commutateur virtuel Hyper-V permet l'application de stratégies pour les niveaux de sécurité, d'isolation et de service.

Vous pouvez également déployer le commutateur virtuel Hyper-V avec la fonctionnalité SET (Switch Embedded Teaming) et la technologie RDMA (accès direct à la mémoire à distance). Pour plus d'informations, consultez la section RDMA (accès direct à la mémoire à distance) et SET (Switch Embedded Teaming) dans cette rubrique.

Service DNS interne (iDNS) pour SDN

Les machines virtuelles hébergées et les applications nécessitent DNS pour communiquer au sein de leurs réseaux et avec des ressources externes sur Internet. Avec iDNS, vous pouvez fournir aux locataires des services de résolution de noms DNS pour des ressources isolées, des ressources d'espace de noms local et des ressources Internet.

Virtualisation des fonctions réseau

Les appliances matérielles, par exemple les équilibreurs de charge, les pare-feu, les routeurs et les commutateurs, deviennent de plus en plus des appliances virtuelles. Microsoft dispose de réseaux, de commutateurs, de passerelles, de NAT, d'équilibreurs de charge et de pare-feu virtualisés. Cette « virtualisation des fonctions réseau » est une évolution naturelle de la virtualisation des serveurs et des réseaux. Les appliances virtuelles se développent rapidement et créent un tout nouveau marché. Elles ne cessent d'éveiller l'intérêt et de gagner en puissance dans les plateformes de virtualisation et les services cloud.

Les technologies de virtualisation des fonctions réseau suivantes sont disponibles.

- **Équilibreur de charge logicielle (SLB) et Traduction d'adresses réseau (NAT)**. Améliorez le débit en prenant en charge le retour direct du serveur, où le trafic réseau de retour peut contourner le multiplexeur d'équilibrage de charge. Pour plus d'informations, consultez Équilibrage de charge logiciel /(SLB/) pour SDN.

- **Pare-feu du centre de données**. Fournissez des listes ACL (listes de contrôle d'accès) précises, qui vous permettent d'appliquer des stratégies de pare-feu au niveau de l'interface des machines virtuelles ou au niveau des sous-réseaux. Pour plus d'informations, consultez Vue d'ensemble du pare-feu du centre de données.
- **Passerelle du serveur d'accès à distance pour SDN**. Routez le trafic réseau entre le réseau physique et les ressources réseau des machines virtuelles, quel que soit l'emplacement. Vous pouvez router le trafic réseau à la même localisation physique ou à plusieurs localisations différentes. Pour plus d'informations, consultez Passerelle RAS pour SDN.

RDMA (Remote Direct Memory Access) et SET (Switch Embedded Teaming)

Dans Windows Server 2016, vous pouvez activer la technologie RDMA sur les cartes réseau liées à un commutateur virtuel Hyper-V avec ou sans fonctionnalité SET (Switch Embedded Teaming). Cela vous permet d'utiliser moins de cartes réseau quand vous souhaitez utiliser RDMA et SET en même temps.

SET est une autre solution pour l'association de cartes réseau, que vous pouvez utiliser au sein des environnements qui incluent Hyper-V et la pile SDN (Software-Defined Networking) dans Windows Server 2016. SET intègre certaines des fonctionnalités d'association de cartes réseau dans le commutateur virtuel Hyper-V.

SET vous permet de regrouper entre une et huit cartes réseau Ethernet physiques sous forme d'une ou de plusieurs cartes réseau virtuelles logicielles. Ces cartes réseau virtuelles fournissent des performances élevées et une tolérance de panne importante en cas de défaillance de la carte réseau. Les cartes réseau membres de SET doivent toutes être installées sur le même hôte Hyper-V physique pour pouvoir faire l'objet d'une association.

De plus, vous pouvez utiliser des commandes Windows PowerShell pour activer la fonctionnalité DCB (Data Center Bridging), créer un commutateur virtuel Hyper-V avec une carte vNIC (carte d'interface réseau virtuelle) RDMA, et créer un commutateur virtuel Hyper-V avec des cartes vNIC tirant parti de SET et RDMA. Pour plus d'informations, consultez Accès direct à la mémoire à distance (Remote Direct Memory Access, RDMA) et association commutée/intégrée (Switched-Embedded Teaming, SET).

Protocole (BGP)

Le protocole BGP (Border Gateway Protocol) est un protocole de routage dynamique qui apprend automatiquement les routes entre les sites qui utilisent des connexions VPN de site à site. Ainsi, BGP réduit la configuration manuelle des routeurs. Quand vous configurez la

passerelle RAS, BGP vous permet de gérer le routage du trafic réseau entre les réseaux de machines virtuelles de vos locataires et les sites distants.

Équilibrage de charge logicielle (SLB) pour SDN

Les fournisseurs de services cloud et les entreprises qui déploient une architecture SDN peuvent utiliser l'équilibrage de charge logiciel pour distribuer de manière égale le trafic réseau des locataires et des clients de locataires entre les ressources de réseau virtuel. La fonctionnalité d'équilibrage de charge de Windows Server vous permet d'activer plusieurs serveurs pour héberger la même charge de travail, ce qui garantit évolutivité et haute disponibilité.

Conteneurs Windows Server

Les conteneurs Windows Server constituent une méthode de virtualisation de système d'exploitation légère, qui permet de séparer les applications ou les services d'autres services s'exécutant sur le même hôte de conteneur. Chaque conteneur a son propre système d'exploitation, ses propres processus, son propre système de fichiers, son propre Registre et ses propres adresses IP, que vous pouvez connecter à des réseaux virtuels.

System Center

Déployez et gérez l'infrastructure SDN avec VMM (Virtual Machine Management) et Operations Manager. Avec VMM, vous provisionnez et gérez les ressources nécessaires pour créer et déployer des machines virtuelles et services dans des clouds privés. Avec Operations Manager, vous supervisez les services, les appareils et les opérations au sein de votre entreprise pour identifier les problèmes qui nécessitent une action immédiate.

Virtualisation de réseau Hyper-V

14/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

La virtualisation de réseau Hyper-V (HNV), introduite dans Windows Server 2012, virtualise les réseaux clients sur une infrastructure réseau physique partagée. Les modifications à apporter à l’infrastructure réseau physique étant minimes, HNV confère aux fournisseurs de services l’agilité nécessaire pour déployer et migrer des charges de travail de locataire dans l’ensemble des trois clouds : le cloud du fournisseur de services, le cloud privé ou le cloud public Microsoft Azure.

Pour plus d'informations, voir les rubriques suivantes :

- Vue d’ensemble de la virtualisation de réseau Hyper-V dans Windows Server 2016
- Nouveautés de la Virtualisation de réseau Hyper-V dans Windows Server 2016

- Saviez-vous que Microsoft Azure offre des fonctionnalités similaires dans le cloud ? Découvrez plus en détail les solutions de virtualisation Microsoft Azure.
- Créer une solution de virtualisation hybride dans Microsoft Azure :
  - Connecter un réseau local à Azure via un VPN de site à site et étendre Active Directory sur un contrôleur de domaine de machine virtuelle IaaS dans Azure |

Vue d’ensemble de la Virtualisation de réseau Hyper-V dans Windows Server

Article • 17/04/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI versions 21H2 et 20H2

Dans Windows Server et Virtual Machine Manager, Microsoft fournit une solution de virtualisation de réseau de bout en bout. Cinq principaux composants constituent la solution de virtualisation de réseau de Microsoft :

- **Windows Azure Pack pour Windows Server** fournit un portail côté locataire pour créer des réseaux virtuels et un portail d’administration pour gérer les réseaux virtuels.
- **Virtual Machine Manager** (VMM) fournit une gestion centralisée de l’infrastructure réseau.
- Le **Contrôleur de réseau Microsoft** offre une fonction d’automatisation programmable et centralisée pour gérer, configurer, analyser et dépanner l’infrastructure réseau virtuelle et physique dans votre centre de données.
- La **virtualisation de réseau Hyper-V** fournit l’infrastructure nécessaire pour virtualiser le trafic réseau.
- Les **passerelles de virtualisation de réseau Hyper-V** établissent les connexions entre les réseaux virtuels et physiques.

Cette rubrique présente les principes et explique les principaux avantages et fonctionnalités clés de la Virtualisation de réseau Hyper-V (une partie de la solution de virtualisation de réseau globale) dans Windows Server 2016. Elle explique comment la virtualisation de réseau profite à la fois aux nuages privés qui recherchent une consolidation des charges de travail des entreprises et aux fournisseurs de services de nuages publics IaaS (Infrastructure as a Service).

Pour plus d’informations techniques sur la virtualisation de réseau dans Windows Server 2016, consultez Détails techniques de la Virtualisation de réseau Hyper-V dans Windows Server 2016.

Vous voulez dire

- Vue d'ensemble de la Virtualisation de réseau Hyper-V (Windows Server 2012 R2)
- Vue d'ensemble d'Hyper-V
- Vue d'ensemble du commutateur virtuel Hyper-V

Description de la fonctionnalité

La Virtualisation de réseau Hyper-V fournit des « réseaux virtuels » (ou réseau d'ordinateurs virtuels) aux ordinateurs virtuels de la même manière que la virtualisation de serveur (hyperviseur) fournit des « ordinateurs virtuels » au système d'exploitation. La virtualisation de réseau dissocie les réseaux virtuels de l'infrastructure réseau physique et élimine les contraintes liées aux réseaux VLAN et à l'affectation d'adresses IP hiérarchiques lors de l'approvisionnement d'ordinateurs virtuels. Du fait de cette souplesse, les clients n'ont pas de difficultés à adopter les nuages IaaS et les hébergeurs et administrateurs de centre de données gèrent leur infrastructure avec efficacité, tout en préservant l'isolation mutualisée nécessaire, les exigences de sécurité et en prenant en charge le chevauchement des adresses IP d'ordinateurs virtuels.

Les clients veulent étendre leurs centres de données dans le nuage en toute transparence. Aujourd'hui, bâtir des architectures de nuage hybride transparentes s'avère délicat du point de vue technique. L'une des plus grandes difficultés auxquelles les clients sont confrontés est la réutilisation de leurs topologies réseau existantes (sous-réseaux, adresses IP, services réseau, etc.) dans le cloud et le lien à établir entre leurs ressources locales et leurs ressources du cloud. La virtualisation de réseau Hyper-V repose sur le concept d'un réseau d'ordinateurs virtuels indépendant du réseau physique sous-jacent. Avec ce concept de réseau d'ordinateurs virtuels, qui est constitué d'un ou de plusieurs sous-réseaux virtuels, l'emplacement exact dans le réseau physique des ordinateurs virtuels associés à un réseau virtuel est dissocié de la topologie réseau virtuelle. De ce fait, les clients peuvent facilement transférer leurs sous-réseaux virtuels dans le nuage tout en conservant leurs adresses IP et topologie existantes dans le nuage, au point que les services existants continuent de fonctionner sans connaître l'emplacement physique des sous-réseaux. Autrement dit, la virtualisation de réseau Hyper-V permet de créer un cloud hybride transparent.

Abstraction faite du nuage hybride, nombreuses sont les organisations qui consolident leurs centres de données et créent des nuages privés pour exploiter en interne les avantages offerts par l'architecture en nuage sur le plan de l'efficacité et de l'extensibilité. La Virtualisation de réseau Hyper-V offre une souplesse et une efficacité plus abouties pour les clouds privés en dissociant la topologie réseau d'une unité commerciale (en la rendant virtuelle) de la topologie réseau physique réelle. Ainsi, les

unités commerciales peuvent facilement partager un nuage privé interne tout en étant isolées les unes des autres et conserver les topologies réseau existantes. L'équipe chargée des opérations d'un centre de données est libre de déployer et transférer dynamiquement des charges de travail n'importe où dans le centre de données sans aucune interruption de serveurs, ce qui procure une efficacité opérationnelle supérieure qui profite globalement au centre de données.

Pour les propriétaires de charges de travail, le principal avantage est qu'ils peuvent désormais transférer leurs « topologies » de charge de travail dans le cloud sans modifier leurs adresses IP ni réécrire leurs applications. Par exemple, l'application LOB tierce type est constituée d'un niveau frontal, d'un niveau logique métier et d'un niveau base de données. Par le biais d'une stratégie, la virtualisation de réseau Hyper-V permet au client d'intégrer tout ou partie des trois niveaux dans le nuage, tout en conservant la topologie de routage et les adresses IP des services (c.-à.-d., les adresses IP d'ordinateurs virtuels), sans qu'il soit nécessaire de modifier les applications.

Pour les propriétaires d'infrastructure, la souplesse accrue sur le plan de la sélection élective des ordinateurs virtuels permet d'envisager le déplacement des charges de travail n'importe où dans les centres de données sans avoir à modifier les ordinateurs virtuels ou reconfigurer les réseaux. Par exemple, la virtualisation de réseau Hyper-V autorise une migration dynamique entre sous-réseaux, ce qui permet à un ordinateur virtuel de migrer dynamiquement n'importe où dans le centre de données sans aucune interruption de service. Auparavant, la migration dynamique se cantonnait au même sous-réseau, ce qui limitait les possibilités quant à l'emplacement des ordinateurs virtuels. La migration dynamique entre sous-réseaux permet aux administrateurs de consolider les charges de travail en fonction des besoins en ressources dynamiques, de l'efficacité énergétique, et elle peut également s'accommoder de la maintenance de l'infrastructure sans perturber le temps d'activité des charges de travail client.

Cas pratiques

Devant le succès des centres de données virtualisés, les organisations informatiques et les fournisseurs d'hébergement (fournisseurs offrant des services de colocalisation ou de location de serveurs physiques) ont commencé à offrir des infrastructures virtualisées plus souples qui facilitent l'offre d'instances de serveur à la demande à leurs clients. Ce nouveau type de service est appelé « infrastructure en tant que service » ou « Infrastructure as a Service » (IaaS) en anglais. Windows Server 2016 intègre toutes les fonctionnalités de plateforme nécessaires pour permettre aux clients d'entreprise de créer des clouds privés et d'opérer une transition vers un modèle opérationnel d'informatique en que service. Windows Server 2016 permet également aux hébergeurs de créer des clouds publics et d'offrir des solutions IaaS à leurs clients. Lorsqu'elle est

associée à Virtual Machine Manager et Windows Azure Pack pour la gestion de la stratégie de la Virtualisation de réseau Hyper-V, la solution de cloud proposée ici par Microsoft s'avère très efficace.

La Virtualisation de réseau Hyper-V de Windows Server 2016 assure une virtualisation de réseau basée sur des stratégies et contrôlée par logiciel qui réduit les frais de gestion auxquels sont confrontées les entreprises qui développent des clouds IaaS dédiés. De plus, elle offre aux hébergeurs de cloud une souplesse et une scalabilité accrues pour gérer les ordinateurs virtuels en vue d'une utilisation plus efficace des ressources.

Dans un scénario IaaS mettant en scène des ordinateurs virtuels issus de différentes divisions d'organisation (nuage dédié) ou de différents clients (nuage hébergé), une isolation sécurisée s'avère nécessaire. La solution d'aujourd'hui, à savoir les réseaux locaux virtuels (VLAN), peut présenter des inconvénients de taille dans ce scénario.

VLAN

Actuellement, le VLAN est le mécanisme le plus utilisé par les organisations pour prendre en charge la réutilisation d'espaces d'adressage et l'isolation des locataires. Un VLAN utilise le balisage explicite (ID VLAN) dans les en-têtes de trame Ethernet et a recours à des commutateurs Ethernet pour mettre en œuvre l'isolation et limiter le trafic à destination des nœuds de réseau ayant le même ID VLAN. Les principaux inconvénients des VLAN sont les suivants :

- Risque accru d'interruptions involontaires en raison de la reconfiguration fastidieuse des commutateurs de production chaque fois que des ordinateurs virtuels ou des limites d'isolation sont déplacés dans le centre de données dynamique.

- Extensibilité limitée, car les commutateurs classiques prennent seulement en charge 1 000 ID VLAN sur un maximum de 4 094.

- Limitation à un seul sous-réseau IP, ce qui restreint le nombre de nœuds au sein d'un même VLAN et limite la sélection élective d'ordinateurs virtuels en fonction des emplacements physiques. Même si les VLAN peuvent être étendus à plusieurs sites, l'ensemble du VLAN doit se trouver sur le même sous-réseau.

Affectation d'adresses IP

En plus des inconvénients inhérents aux VLAN, l'attribution d'adresses IP d'ordinateurs virtuels pose certains problèmes, à savoir :

- Les emplacements physiques dans l'infrastructure réseau de centre de données déterminent les adresses IP des ordinateurs virtuels. Par conséquent, une transition

vers le nuage passe généralement par une modification des adresses IP des charges de travail de services.

- Les stratégies sont liées aux adresses IP, notamment les règles de pare-feu, les services d'annuaire et de découverte des ressources, etc. La modification des adresses IP nécessite la mise à jour de toutes les stratégies associées.
- Le déploiement d'ordinateurs virtuels et l'isolation du trafic sont dépendants de la topologie.

Lorsque les administrateurs réseau d'un centre de données conçoivent le plan de la topologie physique du centre de données, ils doivent prendre des décisions quant à l'emplacement physique et au routage des sous-réseaux. Ces décisions dépendent de la technologie IP et Ethernet qui détermine les adresses IP possibles pour les ordinateurs virtuels s'exécutant sur un serveur donné ou sur une lame connectée à un rack spécifique du centre de données. Lorsqu'un ordinateur virtuel est approvisionné et placé dans un centre de données, il doit adhérer à ces choix et aux restrictions relatives aux adresses IP. Par conséquent, les administrateurs de centre de données attribuent généralement de nouvelles adresses IP aux ordinateurs virtuels.

Le problème de cette exigence vient du fait que, en plus d'être une adresse, une adresse IP est associée à des informations sémantiques. Ainsi, un sous-réseau peut contenir certains services ou se trouver à un emplacement physique distinct. Les règles de pare-feu, les stratégies de contrôle d'accès et les associations de sécurité IPsec sont généralement associés à des adresses IP. La modification d'adresses IP contraint les propriétaires d'ordinateurs virtuels d'ajuster toutes leurs stratégies qui étaient basées sur les adresses IP d'origine. Cette renumérotation est si contraignante que bon nombre d'entreprises choisissent de ne déployer dans le nuage que les nouveaux services, sans toucher aux applications existantes.

La virtualisation de réseau Hyper-V dissocie les réseaux virtuels des ordinateurs virtuels client de l'infrastructure réseau physique. Les ordinateurs virtuels client peuvent ainsi conserver leurs adresses IP d'origine et les administrateurs de centre de données peuvent approvisionner les ordinateurs virtuels client n'importe où dans le centre de données sans reconfigurer les adresses IP physiques ou les ID VLAN. La section suivante propose un récapitulatif des principales fonctionnalités.

Fonctionnalités importantes

Les fonctionnalités, avantages et autres caractéristiques clés de la Virtualisation de réseau Hyper-V de Windows Server 2016 vous sont présentés dans la liste suivante :

- **Flexibilité de la sélection élective des charges de travail – Isolation réseau et réutilisation d'adresses IP sans VLAN**

  La Virtualisation de réseau Hyper-V dissocie les réseaux virtuels du client de l'infrastructure réseau physique des hébergeurs, ce qui confère une totale liberté quant à la sélection élective des charges de travail à l'intérieur des centres de données. La sélection élective des charges de travail des ordinateurs virtuels n'est plus limitée par l'attribution d'adresses IP ou les conditions d'isolation VLAN du réseau physique, car elle est mise en œuvre dans les hôtes Hyper-V selon les stratégies de virtualisation mutualisée définies par logiciel.

  Les ordinateurs virtuels de différents clients dont les adresses IP se chevauchent peuvent désormais être déployés sur un même serveur hôte sans avoir à passer par une configuration VLAN fastidieuse ou violer la hiérarchie d'adresses IP. La migration des charges de travail client vers des fournisseurs d'hébergement IaaS partagé peut s'en trouver simplifiée, ce qui permet aux clients de déplacer ces charges de travail sans modification (les adresse IP des ordinateurs virtuels restent inchangées). Pour le fournisseur d'hébergement, la prise en charge de nombreux clients désireux d'étendre leur espace d'adressage réseau existant au centre de données IaaS partagé est un exercice complexe de configuration et de gestion de VLAN isolés pour chaque client pour assurer la coexistence d'espaces d'adressage susceptibles de de se chevaucher. Avec la virtualisation de réseau Hyper-V, la prise en charge d'adresses qui se chevauchent est facilitée et la reconfiguration réseau se trouve allégée pour le fournisseur d'hébergement.

  De plus, la maintenance et les mises à niveau de l'infrastructure physique peuvent être effectuées sans entraîner d'arrêts au niveau des charges de travail client. Avec la virtualisation de réseau Hyper-V, les ordinateurs virtuels présents sur un hôte, un rack, un sous-réseau, un VLAN ou un cluster entier peuvent être migrés sans qu'il soit nécessaire de recourir à une modification des adresses IP physiques ni à une reconfiguration majeure.

- **Facilité de déplacement des charges de travail sur un nuage IaaS partagé**

  Avec la virtualisation de réseau Hyper-V, les adresses IP et les configurations d'ordinateur virtuel restent inchangées. Cela permet aux organisations informatiques de déplacer plus facilement les charges de travail de leurs centres de données vers un fournisseur d'hébergement IaaS partagé moyennant une reconfiguration minime de la charge de travail ou de leurs outils et stratégies d'infrastructure. S'il existe une connectivité entre deux centres de données, les administrateurs informatiques peuvent continuer d'utiliser leurs outils sans les reconfigurer.

- **Migration dynamique entre sous-réseaux**

  La migration dynamique de charges de travail d'ordinateurs virtuels se limitait traditionnellement à un même sous-réseau IP ou VLAN, car l'interconnexion de sous-réseaux exigeait la modification de l'adresse IP du système d'exploitation invité de l'ordinateur virtuel. Ce changement d'adresse avait pour effet de couper la communication existante et d'interrompre les services exécutés sur l'ordinateur virtuel. Avec la Virtualisation de réseau Hyper-V, les charges de travail peuvent être migrées dynamiquement depuis des serveurs exécutant Windows Server 2016 dans un sous-réseau, vers des serveurs exécutant Windows Server 2016 dans un autre sous-réseau, et ce, sans modifier les adresses IP des charges de travail. La virtualisation de réseau Hyper-V vérifie que le déplacement des ordinateurs virtuels lié à la migration dynamique a fait l'objet d'une mise à jour et d'une synchronisation entre les hôtes, qui ont une communication permanente avec les ordinateurs virtuels migrés.

- **Gestion simplifiée du fait de la dissociation de l'administration des serveurs et du réseau**

  La sélection élective des charges de travail serveur est simplifiée, car la migration et la sélection élective des charges de travail sont indépendantes de la configuration des réseaux physiques sous-jacents. Les administrateurs de serveurs peuvent se consacrer pleinement à la gestion des services et des serveurs, tandis que les administrateurs réseau peuvent se concentrer sur la gestion globale du trafic et de l'infrastructure réseau. Cela permet aux administrateurs de serveurs de centre de données de déployer et migrer des ordinateurs virtuels sans modifier les adresses IP des ordinateurs virtuels. La virtualisation de réseau Hyper-V permettant une sélection élective des ordinateurs virtuels quelle que soit la topologie du réseau, les administrateurs réseau sont moins impliqués dans les sélections électives qui pourraient modifier les limites d'isolation, ce qui allège leur charge de travail.

- **Simplification du réseau et amélioration de l'utilisation de ressources serveur/réseau**

  La rigidité des VLAN et le fait que la sélection élective des ordinateurs virtuels dépende d'une infrastructure réseau physique se traduisent par un surapprovisionnement et une sous-utilisation. En rompant cette dépendance, la sélection élective des charges de travail d'ordinateurs virtuels gagne en souplesse, ce qui peut simplifier la gestion du réseau et améliorer l'utilisation des ressources serveur et réseau. Notez que la virtualisation de réseau Hyper-V prend en charge les VLAN dans le contexte du centre de données physique. Par exemple, il peut

être décidé que pour un centre de données, l'ensemble du trafic de la virtualisation de réseau Hyper-V soit affecté à un VLAN spécifique.

- **Compatibilité avec l'infrastructure existante et les nouvelles technologies**

  La Virtualisation de réseau Hyper-V peut être déployée dans le centre de données d'aujourd'hui, ce qui ne l'empêche pas d'être compatible avec les technologies émergentes de « réseau plat » de centres de données.

  Par exemple, HNV dans Windows Server 2016 prend en charge le format d'encapsulation VXLAN et le protocole OVSDB (Open vSwitch Database Management Protocol) en tant qu'interface SBI (SouthBound Interface).

- **Interopérabilité et préparation pour l'écosystème**

  La virtualisation de réseau Hyper-V prend en charge diverses configurations pour permettre la communication avec les ressources existantes : connectivité intersite, réseau de zone stockage (SAN), accès non virtualisé aux ressources, etc. Microsoft s'est engagé à collaborer avec les partenaires de l'écosystème pour prendre en charge et améliorer l'expérience de la virtualisation de réseau Hyper-V en termes de performances, d'extensibilité et de gestion.

- **Configuration basée sur des stratégies**

  Les stratégies de virtualisation de réseau dans Windows Server 2016 sont configurées via le Contrôleur de réseau Microsoft. Le contrôleur de réseau dispose d'une API RESTful NorthBound et de l'interface Windows PowerShell pour configurer la stratégie. Pour plus d'informations sur le Contrôleur de réseau Microsoft, consultez Contrôleur de réseau.

Configuration logicielle requise

La Virtualisation de réseau Hyper-V à l'aide du Contrôleur de réseau Microsoft nécessite Windows Server 2016 et le rôle Hyper-V.

Voir aussi

Pour en savoir plus sur la Virtualisation de réseau Hyper-V dans Windows Server 2016, suivez les liens suivants :

Type de contenu	Références

Type de contenu	Références
Ressources de la communauté	- Blog des architectures de cloud privé - Posez des questions :cloudnetfb@microsoft.com
RFC	– VXLAN – RFC 7348
Technologies connexes	- Contrôleur de réseau - Vue d'ensemble de la Virtualisation de réseau Hyper-V (Windows Server 2012 R2)

Détails techniques sur la virtualisation de réseau Hyper-V dans Windows Server

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

La virtualisation de serveur permet à plusieurs instances de serveur de s'exécuter simultanément sur un seul hôte physique. Pourtant, les instances de serveur sont isolées les unes par rapport aux autres. En substance, chaque ordinateur virtuel fonctionne comme s'il s'agissait du seul serveur à s'exécuter sur l'ordinateur physique.

La virtualisation de réseau offre des possibilités similaires, le principe étant que plusieurs réseau virtuels (avec éventuellement des chevauchements d'adresses IP) s'exécutent sur une même infrastructure de réseau physique et chaque réseau virtuel fonctionne comme s'il s'agissait du seul réseau virtuel à s'exécuter sur l'infrastructure réseau partagée. La figure 1 illustre cette relation.

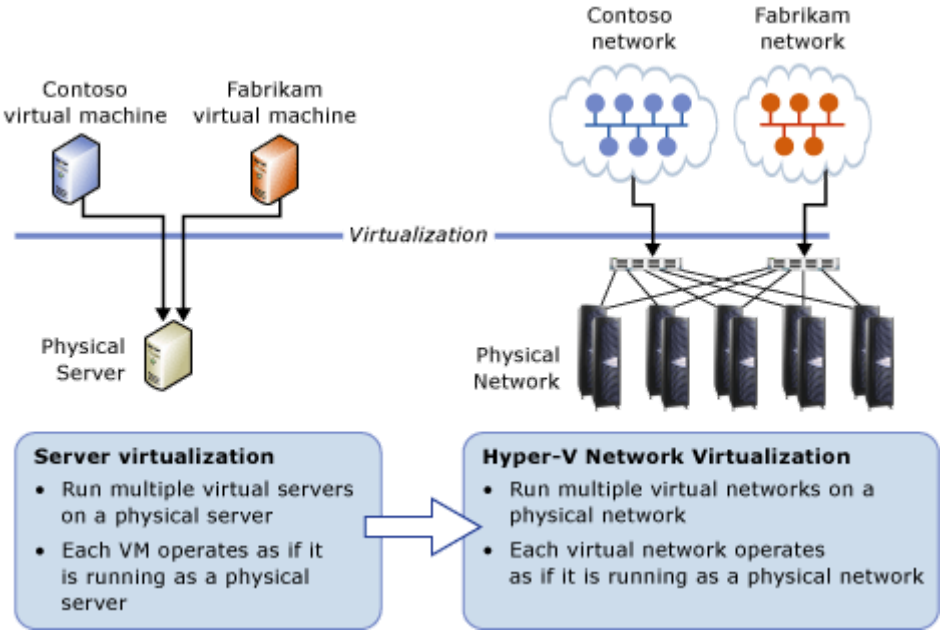


Figure 1: virtualisation de serveur comparée à la virtualisation de réseau

Principes de la virtualisation de réseau Hyper-V

Dans la virtualisation de réseau Hyper-V (HNV), un client ou un locataire est défini comme le « propriétaire » d'un ensemble de sous-réseaux IP déployés dans une entreprise ou un centre de données. Un client peut être une société ou une entreprise avec plusieurs services ou unités commerciales dans un centre de données privé qui nécessitent une isolation réseau, ou un locataire dans un centre de données public hébergé par un fournisseur de services. Chaque

client peut avoir un ou plusieurs réseaux virtuels dans le centre de données, et chaque réseau virtuel se compose d'un ou plusieurs sous-réseaux virtuels.

Il existe deux implémentations HNV qui seront disponibles dans Windows Server 2016 : HNVv1 et HNVv2.

- **HNVv1**

  HNVv1 est compatible avec Windows Server 2012 R2 et System Center 2012 R2 Virtual Machine Manager (VMM). La configuration de HNVv1 s'appuie sur la gestion WMI et les applets de commande Windows PowerShell (facilitées par System Center VMM) pour définir les paramètres d'isolation et les mappages et routage de l'adresse client (CA) - réseau virtuel - vers les adresses physiques (PA). Aucune fonctionnalité supplémentaire n'a été ajoutée à HNVv1 dans Windows Server 2016 et aucune nouvelle fonctionnalité n'est planifiée.
  - SET Teaming et HNV V1 ne sont pas compatibles par plateforme.

  o Pour utiliser des passerelles NVGRE HA, les utilisateurs doivent utiliser l'équipe LBFO ou Aucune équipe. Or

  o Utilisez les passerelles déployées par le contrôleur de réseau avec le commutateur SET associé.

- **HNVv2**

  Un nombre important de nouvelles fonctionnalités sont incluses dans HNVv2, qui est implémenté à l'aide de l'extension de transfert VFP (Azure Virtual Filtering Platform) dans le commutateur Hyper-V. HNVv2 est entièrement intégré à Microsoft Azure Stack, qui inclut le nouveau Contrôleur de réseau dans la pile SDN (Software Defined Networking). La stratégie de réseau virtuel est définie par le biais du contrôleur de réseau Microsoft à l'aide d'une API RESTful NorthBound (NB) et acheminée vers un agent hôte via plusieurs interfaces SouthBound (SBI), y compris OVSDB. L'agent hôte programme la stratégie dans l'extension VFP du commutateur Hyper-V où elle est appliquée.

  > **Important**
  >
  > Cette rubrique traite de HNVv2.

Réseau virtuel

- Chaque réseau virtuel se compose d'un ou plusieurs sous-réseaux virtuels. Un réseau virtuel forme une limite d'isolation où les machines virtuelles au sein d'un réseau virtuel

ne peuvent communiquer qu'entre elles. Traditionnellement, cette isolation était appliquée à l'aide de réseaux locaux virtuels avec une plage d'adresses IP séparée et une balise 802.1q ou un ID de réseau local virtuel. Toutefois, avec HNV, l'isolation est appliquée à l'aide de l'encapsulation NVGRE ou VXLAN pour créer des réseaux de superposition avec la possibilité de chevaucher des sous-réseaux IP entre des clients ou des locataires.

- Chaque réseau virtuel a un ID de domaine de routage (RDID) unique sur l'hôte. Ce RDID correspond approximativement à un ID de ressource pour identifier la ressource REST de réseau virtuel dans le contrôleur de réseau. La ressource REST de réseau virtuel est référencée à l'aide d'un espace de noms URI (Uniform Resource Identifier) avec l'ID de ressource ajouté.

Sous-réseaux virtuels

- Un sous-réseau virtuel implémente la sémantique de sous-réseau IP de couche 3 pour les ordinateurs virtuels qui font partie d'un même sous-réseau virtuel. Le sous-réseau virtuel forme un domaine de diffusion (similaire à un VLAN) et l'isolation est appliquée à l'aide du champ TNI (ID réseau de locataire NVGRE) ou VNI (VXLAN Network Identifier).

- Chaque sous-réseau virtuel appartient à un seul réseau virtuel (RDID) et un ID de sous-réseau virtuel (VSID) unique est attribué à l'aide de la clé TNI ou VNI dans l'en-tête de paquet encapsulé. Le VSID doit être unique au sein du centre de données et est compris dans une plage allant de 4096 à 2^24-2.

L'un des principaux avantages du réseau virtuel et du domaine de routage est qu'il permet aux clients d'apporter leurs propres topologies de réseau (par exemple, des sous-réseaux IP) dans le cloud. La figure 2 montre un exemple dans lequel Contoso Corp possède deux réseaux distincts : le réseau Recherche et développement (« R&D Net ») et le réseau commercial (« Sales Net »). Comme ces réseaux ont des ID de domaine de routage différents, ils ne peuvent pas interagir ensemble. Autrement dit, le réseau R&D Net Contoso est isolé du réseau Sales Net Contoso, alors même que les deux appartiennent à Contoso Corp. Le réseau R&D Net Contoso contient trois sous-réseaux virtuels. Notez que les RDID et VSID sont uniques au sein d'un centre de données.

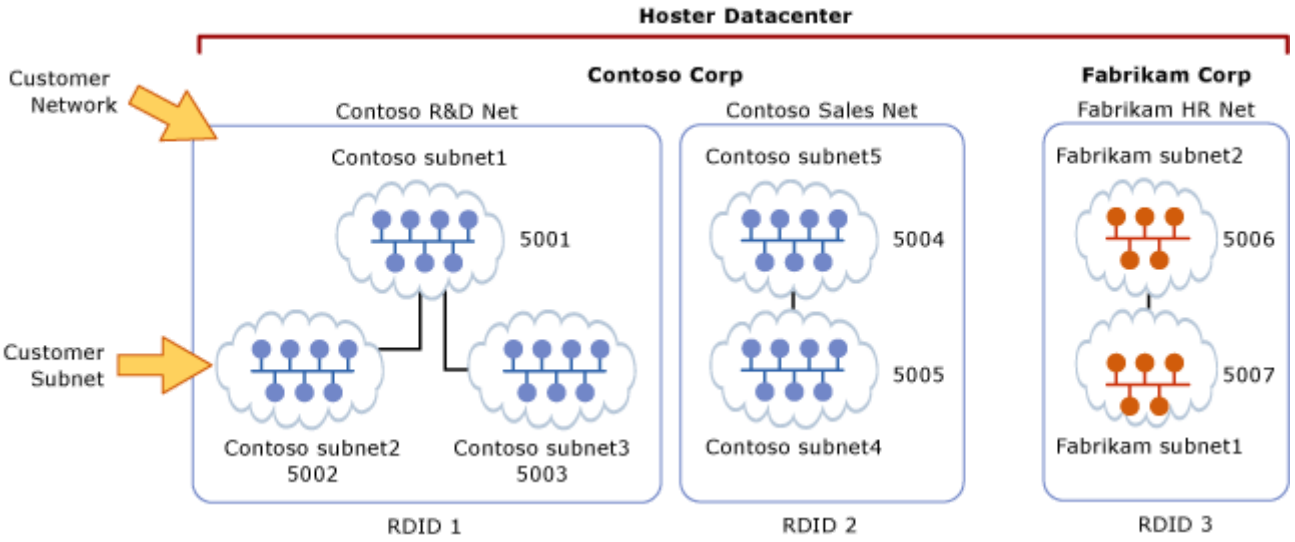


Figure 2 : réseaux client et sous-réseaux virtuels

Transfert de couche 2

Dans la figure 2, les paquets des machines virtuelles dans VSID 5001 peuvent être transférés aux machines virtuelles qui se trouvent également dans VSID 5001 via le commutateur Hyper-V. Les paquets entrants d'une machine virtuelle dans VSID 5001 sont envoyés à un VPort spécifique sur le commutateur Hyper-V. Les règles d'entrée (par exemple, encaps) et les mappages (par exemple, l'en-tête d'encapsulation) sont appliqués par le commutateur Hyper-V pour ces paquets. Les paquets sont ensuite transférés vers un autre VPort sur le commutateur Hyper-V (si la machine virtuelle de destination est attachée au même hôte) ou vers un commutateur Hyper-V différent sur un autre hôte (si la machine virtuelle de destination se trouve sur un autre hôte).

Routage de couche 3

De même, les paquets des machines virtuelles dans VSID 5001 peuvent être acheminés vers des machines virtuelles dans VSID 5002 ou VSID 5003 par le routeur distribué HNV qui est présent dans le commutateur virtuel de chaque hôte Hyper-V. Lors de la remise du paquet au commutateur Hyper-V, HNV met à jour le VSID du paquet entrant par rapport au VSID de l'ordinateur virtuel de destination. Cela ne se produit que si les deux VSID se trouvent dans le même RDID. Par conséquent, les cartes réseau virtuelles associés à RDID1 ne peuvent pas envoyer de paquets aux cartes réseau virtuelles associées à RDID2 sans traverser une passerelle.

> ⓘ **Notes**
>
> Dans la description du flux de paquet ci-dessus, le terme « ordinateur virtuel » signifie en réalité carte réseau virtuelle de l'ordinateur virtuel. Il est fréquent qu'un ordinateur virtuel

n'ait qu'une seule carte réseau virtuelle. Dans ce cas, les mots « ordinateur virtuel » et « carte réseau virtuelle » peuvent signifier la même chose sur le plan conceptuel.

Chaque sous-réseau virtuel définit un sous-réseau IP de couche 3 et une limite de domaine de diffusion de couche 2 similaire à un VLAN. Lorsqu'une machine virtuelle diffuse un paquet, HNV utilise la réplication de monodiffusion (UR) pour effectuer une copie du paquet d'origine et remplacer l'adresse IP et le MAC de destination par les adresses de chaque machine virtuelle qui se trouvent dans le même VSID.

> **Notes**
>
> Lorsque Windows Server 2016 est fourni, les multidiffusions de diffusion et de sous-réseau sont implémentées à l'aide de la réplication en monodiffusion. Le routage multidiffusion entre sous-réseaux et IGMP ne sont pas pris en charge.

En plus d'être un domaine de diffusion, le VSID assure une isolation. Une carte réseau virtuelle dans HNV est connectée à un port de commutateur Hyper-V dont les règles de liste de contrôle d'accès sont appliquées directement au port (ressource REST virtualNetworkInterface) ou au sous-réseau virtuel (VSID) dont elle fait partie.

Une règle ACL doit être appliquée au port du commutateur Hyper-V. Cette liste de contrôle d'accès peut être ALLOW ALL, DENY ALL ou être plus spécifique pour autoriser uniquement certains types de trafic en fonction de la correspondance à 5 tuples (Adresse IP source, Adresse IP de destination, port source, port de destination, protocole).

> **Notes**
>
> Les extensions de commutateur Hyper-V ne fonctionnent pas avec HNVv2 dans la nouvelle pile SDN (Software Defined Networking). HNVv2 est implémenté à l'aide de l'extension de commutateur VFP (Azure Virtual Filtering Platform) qui ne peut pas être utilisée conjointement avec une autre extension de commutateur tierce.

Passage et routage dans la virtualisation de réseau Hyper-V

HNVv2 implémente la commutation de couche 2 (L2) et la sémantique de routage de couche 3 correctes (L3) pour fonctionner comme un commutateur physique ou un routeur fonctionne. Lorsqu'une machine virtuelle connectée à un réseau virtuel HNV tente d'établir une connexion avec une autre machine virtuelle dans le même sous-réseau virtuel (VSID), elle doit d'abord

connaître l'adresse MAC de l'autorité de certification de la machine virtuelle distante. S'il existe une entrée ARP pour l'adresse IP de la machine virtuelle de destination dans la table ARP de la machine virtuelle source, l'adresse MAC de cette entrée est utilisée. Si aucune entrée n'existe, la machine virtuelle source envoie une diffusion ARP avec une demande de retour de l'adresse MAC correspondant à l'adresse IP de la machine virtuelle de destination. Le commutateur Hyper-V intercepte cette requête et l'envoie à l'agent hôte. L'agent hôte recherche dans sa base de données locale une adresse MAC correspondante pour l'adresse IP de la machine virtuelle de destination demandée.

> ⓘ **Notes**
>
> L'agent hôte, agissant en tant que serveur OVSDB, utilise une variante du schéma VTEP pour stocker les mappages CA-PA, table MAC, etc.

Si une adresse MAC est disponible, l'agent hôte injecte une réponse ARP et la renvoie à la machine virtuelle. Une fois que la pile réseau de la machine virtuelle contient toutes les informations d'en-tête L2 requises, la trame est envoyée au port Hyper-V correspondant sur le commutateur virtuel. En interne, le commutateur Hyper-V teste cette trame par rapport aux règles de correspondance de N-tuple affectées au V-Port et applique certaines transformations au frame en fonction de ces règles. Plus important encore, un ensemble de transformations d'encapsulation est appliqué pour construire l'en-tête d'encapsulation à l'aide de NVGRE ou VXLAN, en fonction de la stratégie définie sur le contrôleur de réseau. En fonction de la stratégie programmée par l'agent hôte, un mappage AC-AF est utilisé pour déterminer l'adresse IP de l'hôte Hyper-V où réside la machine virtuelle de destination. Le commutateur Hyper-V garantit que les règles d'acheminement et les balises de réseau local virtuel correctes sont appliquées au paquet externe afin qu'il atteigne l'adresse AF distante.

Si une machine virtuelle connectée à un réseau virtuel HNV souhaite créer une connexion avec une machine virtuelle dans un autre sous-réseau virtuel (VSID), le paquet doit être routé en conséquence. HNV suppose une topologie en étoile où il n'y a qu'une seule adresse IP dans l'espace d'autorité de certification utilisée comme tronçon suivant pour atteindre tous les préfixes IP (c'est-à-dire un itinéraire/passerelle par défaut). Actuellement, cela applique une limitation à un itinéraire par défaut unique, et les itinéraires autres que les routes par défaut ne sont pas pris en charge.

Routage entre des sous-réseaux virtuels

Dans un réseau physique, un sous-réseau IP est un domaine de couche 2 (L2) où les ordinateurs (virtuels et physiques) peuvent communiquer directement entre eux. Le domaine L2 est un domaine de diffusion où les entrées ARP (carte d'adresses IP:MAC) sont apprises via les requêtes ARP qui sont diffusées sur toutes les interfaces et les réponses ARP sont renvoyées

à l'hôte demandeur. L'ordinateur utilise les informations MAC apprises à partir de la réponse ARP pour construire complètement la trame L2, y compris les en-têtes Ethernet. Toutefois, si une adresse IP se trouve dans un autre sous-réseau L3, la requête ARP ne franchit pas cette limite L3. Au lieu de cela, une interface de routeur L3 (tronçon suivant ou passerelle par défaut) avec une adresse IP dans le sous-réseau source doit répondre à ces requêtes ARP avec sa propre adresse MAC.

Dans la mise en réseau Windows standard, un administrateur peut créer des itinéraires statiques et les affecter à une interface réseau. En outre, une « passerelle par défaut » est généralement configurée pour être l'adresse IP du tronçon suivant sur une interface où les paquets destinés à l'itinéraire par défaut (0.0.0.0/0) sont envoyés. Les paquets sont envoyés à cette passerelle par défaut si aucun itinéraire spécifique n'existe. Il s'agit en général du routeur pour votre réseau physique. HNV utilise un routeur intégré qui fait partie de chaque hôte et a une interface dans chaque VSID pour créer un routeur distribué pour les réseaux virtuels.

Étant donné que HNV suppose une topologie en étoile, le routeur distribué HNV agit comme une passerelle par défaut unique pour tout le trafic qui transite entre les sous-réseaux virtuels qui font partie du même réseau VSID. L'adresse utilisée comme passerelle par défaut est l'adresse IP la plus basse dans le VSID et est affectée au routeur distribué HNV. Ce routeur distribué représente un moyen très efficace de router correctement tout le trafic à l'intérieur d'un réseau VSID, car chaque hôte peut acheminer directement le trafic vers l'hôte approprié sans intermédiaire. Cela est particulièrement vrai lorsque deux ordinateurs virtuels du même réseau d'ordinateurs virtuels, mais de différents sous-réseaux virtuels, se trouvent sur le même hôte physique. Comme vous le verrez plus loin dans cette section, le paquet ne doit jamais quitter l'hôte physique.

Routage entre les sous-réseaux PA

Contrairement à HNVv1 qui a alloué une adresse IP PA pour chaque sous-réseau virtuel (VSID), HNVv2 utilise désormais une adresse IP PA par Switch-Embedded membre de l'équipe de cartes réseau SET (Teaming). Le déploiement par défaut suppose une équipe à deux cartes réseau et affecte deux adresses IP PA par hôte. Un seul hôte a des adresses IP PA attribuées à partir du même sous-réseau logique fournisseur (PA) sur le même VLAN. Deux machines virtuelles locataires dans le même sous-réseau virtuel peuvent en effet se trouver sur deux hôtes différents qui sont connectés à deux sous-réseaux logiques de fournisseur différents. HNV construit les en-têtes IP externes pour le paquet encapsulé en fonction du mappage CA-PA. Toutefois, il s'appuie sur la pile TCP/IP hôte vers ARP pour la passerelle PA par défaut, puis génère les en-têtes Ethernet externes en fonction de la réponse ARP. En règle générale, cette réponse ARP provient de l'interface SVI sur le commutateur physique ou le routeur L3 où l'hôte est connecté. HNV s'appuie donc sur le routeur L3 pour acheminer les paquets encapsulés entre les sous-réseaux logiques/VLAN du fournisseur.

Routage hors d'un réseau virtuel

La plupart des déploiements clients nécessitent une communication entre l'environnement HNV et les ressources qui ne font pas partie de ce même environnement. Les passerelles de virtualisation de réseau sont nécessaires pour permettre la communication entre les deux environnements. Les infrastructures nécessitant une passerelle HNV comprennent le Cloud privé et le Cloud hybride. Fondamentalement, les passerelles HNV sont requises pour le routage de couche 3 entre des réseaux internes et externes (physiques) (y compris NAT) ou entre différents sites et/ou clouds (privés ou publics) qui utilisent un tunnel IPSec VPN ou GRE.

Les passerelles peuvent présenter différents facteurs de forme physique. Elles peuvent être basées sur Windows Server 2016, incorporées dans un commutateur Top of Rack (TOR) agissant comme une passerelle VXLAN, accessibles via une adresse IP virtuelle (VIP) annoncée par un équilibreur de charge, placées dans d'autres appliances réseau existantes, ou peuvent être une nouvelle appliance réseau autonome.

Pour plus d'informations sur les options de passerelle RAS Windows, consultez la passerelle RAS.

Encapsulation de paquets

Dans HNV, chaque carte réseau virtuelle est associée à deux adresses IP :

- **Adresse client** (CA) Adresse IP attribuée par le client, en fonction de son infrastructure intranet. Cette adresse permet au client d'échanger du trafic réseau avec l'ordinateur virtuel comme s'il n'avait pas été transféré sur un cloud public ou privé. L'adresse client est visible de l'ordinateur virtuel et accessible au client.

- **Adresse du fournisseur** (PA) Adresse IP attribuée par le fournisseur d'hébergement ou les administrateurs du centre de données en fonction de leur infrastructure réseau physique. L'adresse fournisseur figure dans les paquets du réseau qui sont échangés avec le serveur exécutant Hyper-V qui héberge l'ordinateur virtuel. Cette adresse est visible sur le réseau physique, mais pas sur l'ordinateur virtuel.

Les adresses client préservent la topologie réseau du client, qui est virtualisée et dissociée des adresses et de la topologie du réseau physique sous-jacent, conformément à l'implémentation des adresses fournisseur. Le diagramme suivant illustre la relation conceptuelle entre les adresses client des ordinateurs virtuels et les adresses fournisseur d'une infrastructure réseau à la suite d'une virtualisation de réseau.

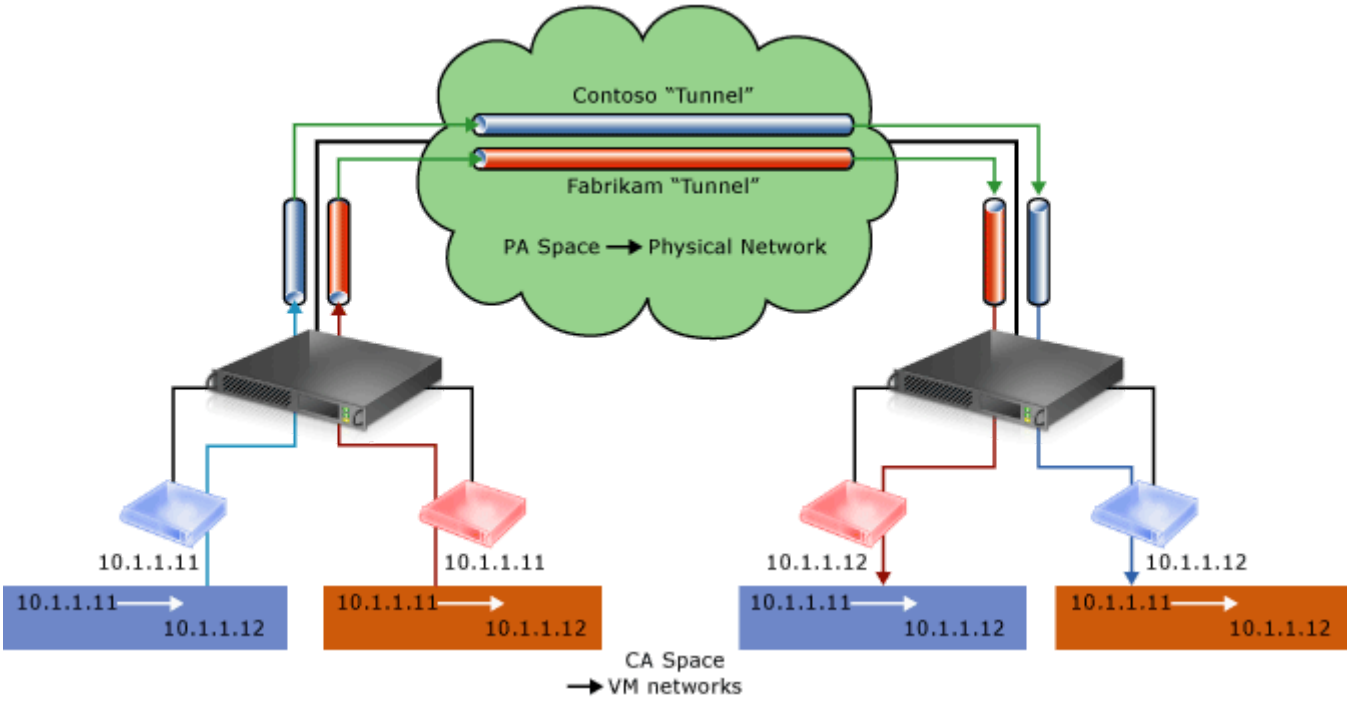


Figure 6 : diagramme conceptuel d'une virtualisation de réseau sur une infrastructure physique

Dans le diagramme, les ordinateurs virtuels client envoient des paquets de données dans l'espace d'adressage client, qui transitent par l'infrastructure réseau physique en empruntant leurs propres réseaux virtuels ou « tunnels ». Dans l'exemple ci-dessus, les tunnels peuvent être considérés comme des « enveloppes » pour les paquets de données Contoso et Fabrikam disposant d'étiquettes d'expédition (adresses fournisseur) vertes, qui doivent être remises par l'hôte source de gauche à l'hôte de destination de droite. La question essentielle est de savoir comment les hôtes déterminent les « adresses d'expédition » (fournisseur) correspondant aux adresses client Contoso et Fabrikam, comment l'« enveloppe » englobe les paquets et comment les hôtes de destination peuvent déballer les paquets et les remettre correctement aux ordinateurs virtuels de destination Contoso et Fabrikam.

Cette analogie simple a mis en évidence les principaux aspects de la virtualisation de réseau :

- Chaque adresse client d'ordinateur virtuel est mappée à une adresse fournisseur d'hôte physique. Plusieurs adresses client peuvent être associées à la même adresse fournisseur.
- Les ordinateurs virtuels envoient des paquets de données dans les espaces d'adressage client, qui sont mis dans une « enveloppe » avec une paire d'adresses fournisseur source et de destination en fonction du mappage.
- Les mappages entre adresses client et fournisseur doivent permettre aux hôtes de distinguer les paquets à destination des différents ordinateurs virtuels client.

Par conséquent, la virtualisation d'un réseau consiste à virtualiser les adresses réseau utilisées par les ordinateurs virtuels. Le contrôleur de réseau est responsable du mappage d'adresses et

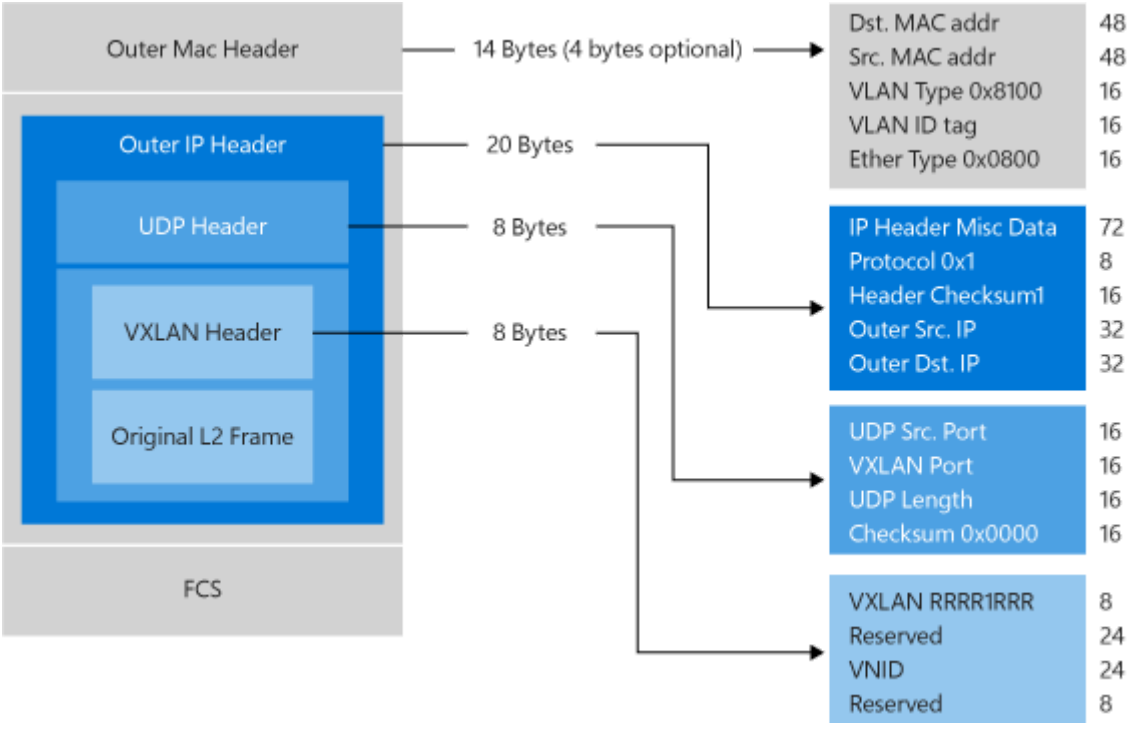
l'agent hôte gère la base de données de mappage à l'aide du schéma MS_VTEP. La section suivante décrit les mécanismes réels de la virtualisation d'adresses.

La virtualisation de réseau via la virtualisation d'adresses

HNV implémente des réseaux de locataires de superposition à l'aide de l'encapsulation de routage générique de virtualisation de réseau (NVGRE) ou du réseau local virtuel eXtensible (VXLAN). VXLAN est la valeur par défaut.

Réseau local virtuel eXtensible (VXLAN)

Le protocole VXtensible Local Area Network (VXLAN) (VXLAN) (Virtual eXtensible Local Area Network) (RFC 7348) a été largement adopté sur la place du marché, avec le support des fournisseurs comme Cisco, Brocade, Arista, Dell, HP et d'autres. Le protocole VXLAN utilise UDP comme transport. Le port de destination UDP attribué par IANA pour VXLAN est 4789 et le port source UDP doit être un hachage d'informations du paquet interne à utiliser pour la propagation ECMP. Après l'en-tête UDP, un en-tête VXLAN est ajouté au paquet qui comprend un champ réservé de 4 octets suivi d'un champ de 3 octets pour l'identificateur réseau VXLAN (VNI) - VSID - suivi d'un autre champ réservé de 1 octet. Après l'en-tête VXLAN, l'image d'autorité de certification L2 d'origine (sans le cadre Ethernet de l'autorité de certification FCS) est ajoutée.



Encapsulation de routage générique (NVGRE)

Ce mécanisme de virtualisation de réseau utilise l'encapsulation générique de routage (NVGRE) dans l'en-tête de tunnel. Avec NVGRE, le paquet de l'ordinateur virtuel est encapsulé dans un autre paquet. L'en-tête de ce nouveau paquet contient les adresses IP fournisseur sources et de destination appropriées, outre l'ID de sous-réseau virtuel, qui est stocké dans le champ de clé de l'en-tête GRE, comme le montre la figure 7.

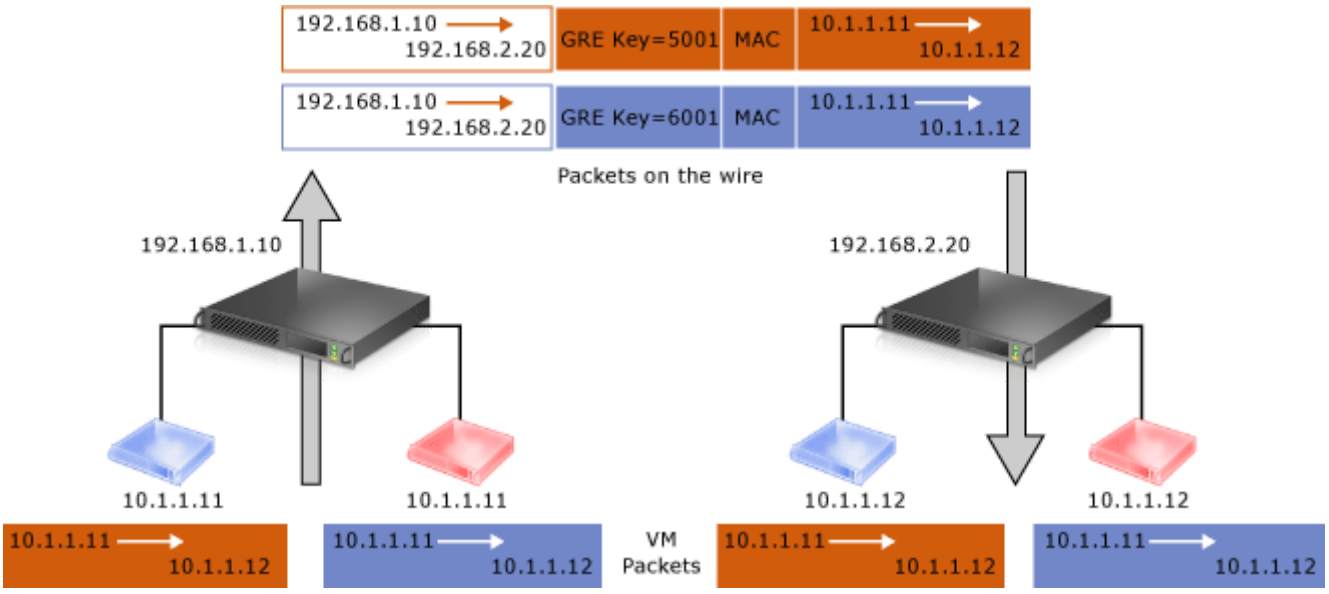


Figure 7 : virtualisation de réseau - encapsulation NVGRE

L'ID de sous-réseau virtuel permet aux hôtes d'identifier l'ordinateur virtuel client pour un paquet donné, même si les adresses fournisseur et client des paquets peuvent se chevaucher. De ce fait, tous les ordinateurs virtuels d'un même hôte peuvent partager une adresse fournisseur unique, comme l'illustre la figure 7.

La partage de l'adresse fournisseur a des conséquences importantes sur l'extensibilité réseau. Le nombre d'adresses IP et MAC que l'infrastructure réseau doit mémoriser s'en trouve considérablement réduit. Par exemple, si chaque hôte final compte en moyenne 30 ordinateurs virtuels, le nombre d'adresses IP et MAC que doit mémoriser l'infrastructure réseau est réduit selon un facteur de 30. Les ID de sous-réseau virtuel incorporés dans les paquets permettent en outre une corrélation facile entre les paquets et les clients effectifs.

Le schéma de partage AF pour Windows Server 2012 R2 est d'un AF par VSID et par hôte. Par Windows Server 2016 le schéma est d'un AF par membre de l'équipe de carte réseau.

Avec Windows Server 2016 et versions ultérieures, HNV prend entièrement en charge NVGRE et VXLAN en mode natif. Celle-ci ne nécessite AUCUNE mise à niveau ni acquisition de nouveau matériel réseau, tel qu'une carte réseau, un commutateur ou un routeur. Cela est dû au fait que les paquets transitant par le câble sont un paquet IP normal dans l'espace d'adressage fournisseur, qui est compatible avec l'infrastructure réseau d'aujourd'hui. Toutefois, pour obtenir les meilleures performances, utilisez des cartes réseau prises en charge avec les derniers pilotes qui prennent en charge les déchargements de tâches.

Exemple de déploiement mutualisé

Le diagramme suivant montre un exemple de déploiement où deux clients optent pour un centre de données cloud et où la relation entre les adresses client et fournisseur est définie par les stratégies HNV.

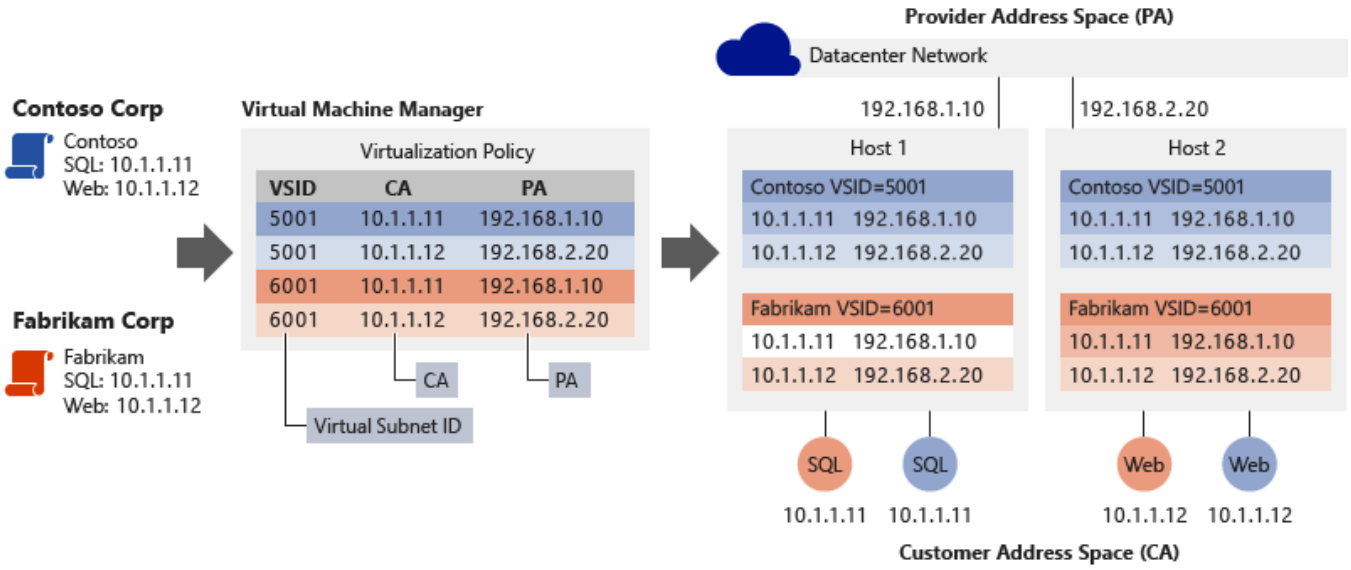


Figure 8 : exemple de déploiement mutualisé

Examinez l'exemple illustré dans la figure 8. Avant d'utiliser le service IaaS partagé du fournisseur d'hébergement :

- Contoso Corp a exécuté un serveur SQL Server (nommé **SQL**) à l'adresse IP 10.1.1.11 et un serveur web (nommé **Web**) à l'adresse IP 10.1.1.12, qui utilise son serveur SQL Server pour les transactions de base de données.
- Fabrikam Corp a exécuté un serveur SQL, également nommé **SQL** et affecté l'adresse IP 10.1.1.11 et un serveur web, également nommé **Web** et également à l'adresse IP 10.1.1.12, qui utilise son serveur SQL Server pour les transactions de base de données.

Nous partons du principe que le fournisseur de services d'hébergement a déjà créé le réseau logique du fournisseur (AF) via le contrôleur de réseau pour qu'il corresponde à sa topologie de réseau physique. Le contrôleur de réseau alloue deux adresses IP AF à partir du préfixe IP du sous-réseau logique où les hôtes sont connectés. Le contrôleur réseau indique également la balise VLAN appropriée pour appliquer les adresses IP.

À l'aide du contrôleur de réseau, Contoso Corp et Fabrikam Corp, créez ensuite leur réseau virtuel et leurs sous-réseaux qui sont soutenus par le réseau logique du fournisseur (AF) spécifié par le fournisseur de services d'hébergement. Contoso Corp et Fabrikam Corp déplacent leurs serveurs SQL et serveurs web respectifs vers le même service IaaS partagé du fournisseur d'hébergement où, par coïncidence, ils exécutent les machines virtuelles **SQL** sur

Hyper-V Hôte 1 et les machines virtuelles **Web** (IIS7) sur Hyper-V Hôte 2. Tous les ordinateurs virtuels conservent leurs adresses IP (client) intranet d'origine.

Le contrôleur de réseau attribue aux deux sociétés l'ID de sous-réseau virtuel (VSID) suivant, comme indiqué ci-dessous. L'agent hôte sur chacun des hôtes Hyper-V reçoit les adresses IP AF allouées du contrôleur de réseau et crée deux cartes réseau virtuelles hôtes pa dans un compartiment réseau non par défaut. Une interface réseau est affectée à chacune de ces cartes réseau virtuelles hôtes où l'adresse IP AF est affectée, comme indiqué ci-dessous :

- Machines virtuelles de Contoso Corp VSID et PAs : **VSID** est 5001, **SQL PA** est 192.168.1.10, **le pa web** est 192.168.2.20
- Machines virtuelles de Fabrikam Corp VSID et PAs : **VSID** est 6001, **SQL PA** est 192.168.1.10, **Web PA** est 192.168.2.20

Le contrôleur de réseau connecte toutes les stratégies réseau (y compris le mappage AC-AF) à l'agent hôte SDN qui maintient la stratégie dans un magasin persistant (dans les tables de base de données OVSDB).

Lorsque l'ordinateur virtuel Web de Contoso Corp (10.1.1.12) sur l'hôte Hyper-V 2 crée une connexion TCP sur son serveur SQL Server à l'adresse 10.1.1.11, voici ce qui se produit :

- ARP de machine virtuelle pour l'adresse MAC de destination 10.1.1.11
- L'extension VFP dans le vSwitch intercepte ce paquet et l'envoie à l'agent hôte SDN
- L'agent hôte SDN recherche dans son magasin de stratégies l'adresse MAC pour 10.1.1.11
- Si un MAC est trouvé, l'agent hôte injecte une réponse ARP à la machine virtuelle
- Si un MAC est introuvable, aucune réponse n'est envoyée et l'entrée ARP dans la machine virtuelle pour 10.1.1.11 est marquée comme inaccessible.
- La machine virtuelle construit maintenant un paquet TCP avec les en-têtes Ethernet et IP de l'autorité de certification appropriés et l'envoie au commutateur virtuel
- L'extension de transfert VFP dans le vSwitch traite ce paquet via les couches VFP (décrites ci-dessous) affectées au port vSwitch source sur lequel le paquet a été reçu et crée une entrée de flux dans la table de flux unifiée VFP
- Le moteur VFP effectue la correspondance de règles ou la recherche de table de flux pour chaque couche (par exemple, la couche réseau virtuelle) en fonction des en-têtes IP et Ethernet.
- La règle correspondante dans la couche de réseau virtuel fait référence à un espace de mappage AC-AF et effectue l'encapsulation.

- Le type d’encapsulation (VXLAN ou NVGRE) est spécifié dans la couche de réseau virtuel avec le VSID.
- Dans le cas de l’encapsulation VXLAN, un en-tête UDP externe est construit avec le VSID de 5001 dans l’en-tête VXLAN. Un en-tête d’adresse IP externe est construit avec l’adresse PA source et de destination affectée respectivement à l’hôte Hyper-V 2 (192.168.2.20) et à l’hôte Hyper-V 1 (192.168.1.10) en fonction du magasin de stratégies de l’agent hôte SDN.
- Ce paquet est ensuite acheminé vers la couche de routage AF dans VFP.
- La couche de routage AF dans VFP référence le compartiment réseau utilisé pour le trafic d’espace AF et un ID de VLAN, et utilise la pile TCP/IP de l’hôte pour transférer correctement le paquet AF à l’hôte Hyper-V 1.
- À la réception du paquet encapsulé, l’hôte Hyper-V 1 reçoit le paquet dans le compartiment réseau AF et le transfère au commutateur virtuel.
- Le VFP traite le paquet via ses couches VFP et crée une entrée de flux dans la table de flux unifiée VFP.
- Le moteur VFP correspond aux règles d’entrée dans la couche réseau virtuelle et supprime les en-têtes Ethernet, IP et VXLAN du paquet encapsulé externe.
- Le moteur VFP transfère ensuite le paquet au port vSwitch auquel la machine virtuelle de destination est connectée.

Un processus similaire pour le trafic entre les machines virtuelles Web Fabrikam **Corp etSQL** utilise les paramètres de stratégie HNV pour Fabrikam Corp. Par conséquent, avec HNV, Fabrikam Corp et les machines virtuelles Contoso Corp interagissent comme s’ils se trouvaient sur leurs intranets d’origine. Ils ne peuvent jamais interagir entre eux, même s’ils utilisent les mêmes adresses IP.

Les adresses distinctes (client et fournisseur), les paramètres de stratégie des hôtes Hyper-V et la traduction d’adresses entre adresses client et fournisseur pour le trafic entrant et sortant des ordinateurs virtuels ont pour effet d’isoler ces ensembles de serveurs en utilisant soit la Clé NVGRE ou VLXAN VNID. De plus, les mappages et la transformation de la virtualisation dissocient l’architecture de réseau virtuel de l’infrastructure de réseau physique. Bien que Contoso **SQL** et **Web** et Fabrikam **SQL** et **Web** résident dans leurs propres sous-réseaux IP d’autorité de certification (10.1.1/24), leur déploiement physique se produit sur deux hôtes dans des sous-réseaux PA différents, 192.168.1/24 et 192.168.2/24, respectivement. Cela implique que l’approvisionnement et la migration dynamique des ordinateurs virtuels entre sous-réseaux devient possible avec HNV.

Architecture de la virtualisation de réseau Hyper-V

Dans Windows Server 2016, HNVv2 est implémenté à l'aide de la plateforme de filtrage virtuel Azure (VFP), qui est une extension de filtrage NDIS dans le commutateur Hyper-V. Le concept clé de VFP est celui d'un moteur de flux Match-Action avec une API interne exposée à l'agent hôte SDN pour la programmation de la stratégie réseau. L'agent hôte SDN reçoit lui-même la stratégie réseau du contrôleur de réseau sur les canaux de communication OVSDB et WCF SouthBound. Non seulement la stratégie de réseau virtuel (par exemple le mappage AC-AF) est programmée à l'aide de VFP, mais une stratégie supplémentaire telle que les listes de contrôle d'accès, la qualité de service, etc.

La hiérarchie d'objets pour l'extension de transfert vSwitch et VFP est la suivante :

- vSwitch
  - Gestion des cartes réseau externes
  - Déchargements matériels de carte réseau
  - Règles de transfert globales
  - Port
    - Couche de transfert de sortie pour l'épinglage à cheveux
    - Listes d'espaces pour les mappages et les pools NAT
    - Table de flux unifiée
    - Couche VFP
      - Table de flux
      - Group
      - Rule
        - Les règles peuvent référencer des espaces

Dans le VFP, une couche est créée par type de stratégie (par exemple, Réseau virtuel) et est un ensemble générique de tables de règles/flux. Il n'a pas de fonctionnalités intrinsèques tant que des règles spécifiques n'ont pas été affectées à cette couche pour implémenter ces fonctionnalités. Chaque couche se voit attribuer une priorité et les couches sont affectées à un port par priorité croissante. Les règles sont organisées en groupes principalement en fonction de la direction et de la famille d'adresses IP. Une priorité est également attribuée aux groupes et, au maximum, une règle d'un groupe peut correspondre à un flux donné.

La logique de transfert pour le commutateur virtuel avec l’extension VFP est la suivante :

- Traitement d’entrée (entrée du point de vue du paquet entrant dans un port)
- Forwarding
- Traitement de sortie (sortie du point de vue du paquet sortant d’un port)

Le VFP prend en charge le transfert MAC interne pour les types d’encapsulation NVGRE et VXLAN, ainsi que le transfert basé sur un réseau local virtuel MAC externe.

L’extension VFP a un chemin d’accès lent et un chemin d’accès rapide pour la traversée de paquets. Le premier paquet d’un flux doit parcourir tous les groupes de règles de chaque couche et effectuer une recherche de règle, ce qui est une opération coûteuse. Toutefois, une fois qu’un flux est inscrit dans la table de flux unifiée avec une liste d’actions (en fonction des règles correspondantes), tous les paquets suivants sont traités en fonction des entrées de la table de flux unifiée.

La stratégie HNV est programmée par l’agent hôte. Chaque carte réseau d’ordinateur virtuel est configurée avec une adresse IPv4. Il s’agit des adresses client dont se serviront les ordinateurs virtuels pour communiquer entre eux et qui sont transportées dans les paquets IP en provenance des ordinateurs virtuels. HNV encapsule la trame d’autorité de certification dans une trame pa basée sur les stratégies de virtualisation de réseau stockées dans la base de données de l’agent hôte.

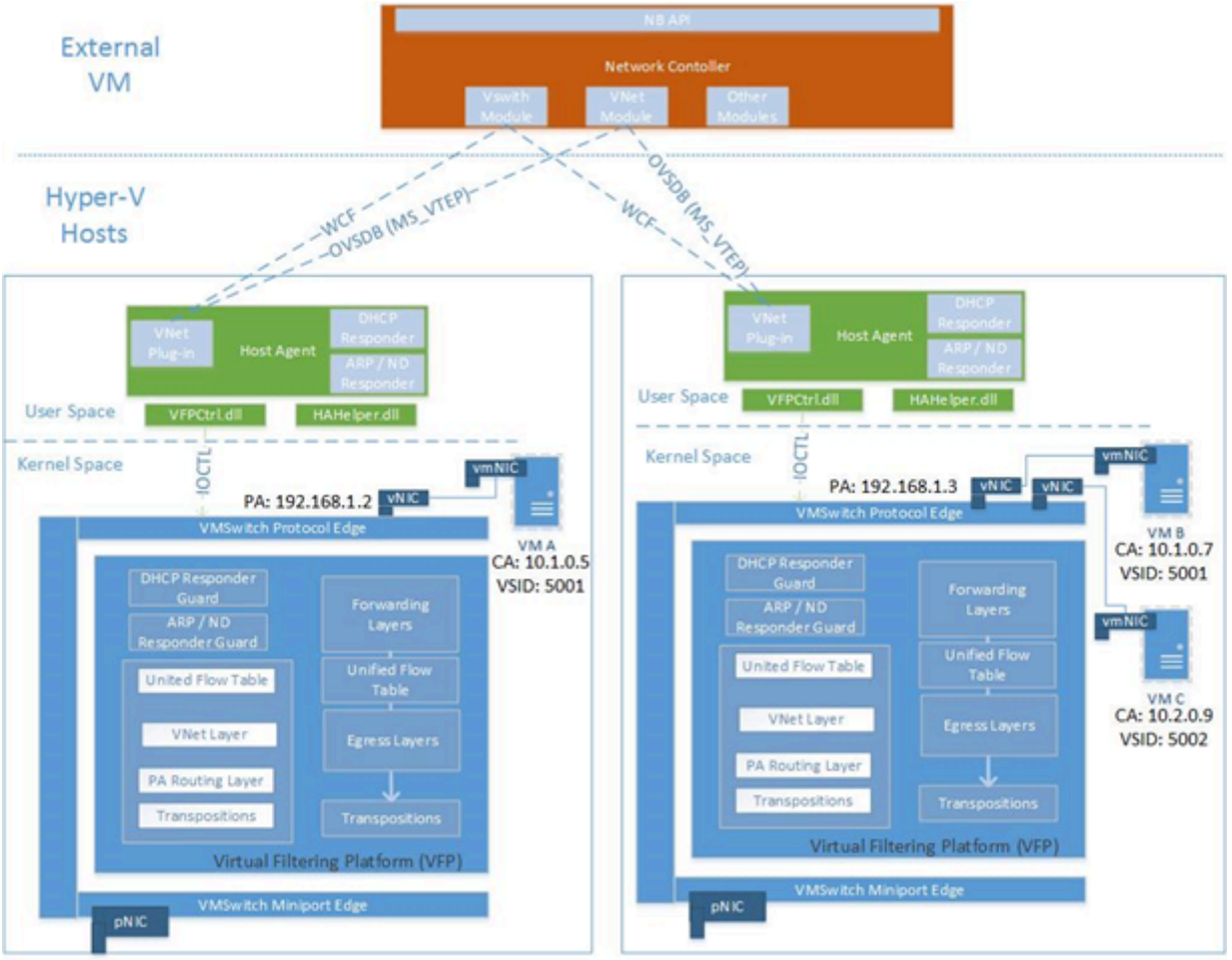


Figure 9 : architecture HNV

Summary

Les centres de données en nuage peuvent apporter de nombreux avantages, notamment une extensibilité améliorée et une meilleure utilisation des ressources. Pour profiter de ces avantages potentiels, il est nécessite de faire appel à une technologie à même de résoudre fondamentalement les problèmes de l'extensibilité mutualisée dans un environnement dynamique. La virtualisation HNV a été conçue pour traiter ces problèmes et également pour améliorer l'efficacité des opérations du centre de données en dissociant la topologie du réseau virtuel de la topologie du réseau physique. S'appuyant sur une norme existante, HNV s'exécute dans le centre de données d'aujourd'hui et fonctionne avec votre infrastructure VXLAN existante. Avec HNV, les clients peuvent désormais consolider leurs centres de données dans un cloud privé ou les étendre en toute transparence dans l'environnement d'un fournisseur de serveurs d'hébergement avec un cloud hybride.

Voir aussi

Pour en savoir plus sur HNVv2, voir les liens suivants :

Agrandir le tableau

Type de contenu	References
Ressources de la communauté	- Blog des architectures de cloud privé - Posez des questions :cloudnetfb@microsoft.com
RFC	- Document RFC préliminaire sur NVGRE - VXLAN - RFC 7348
Technologies associées	- Pour plus d'informations techniques sur la virtualisation de réseau Hyper-V dans Windows Server 2012 R2, consultez détails techniques de la virtualisation de réseau Hyper-V - Contrôleur de réseau

Service DNS interne pour SDN

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Si vous travaillez pour un fournisseur de services cloud (CSP) ou une entreprise qui prévoit de déployer la mise en réseau à définition logicielle (SDN) dans Windows Server, vous pouvez fournir des services DNS à vos charges de travail de locataires hébergées à l'aide du DNS interne (iDNS), qui est intégré à SDN.

Les machines virtuelles hébergées et les applications nécessitent que DNS communique au sein de leurs propres réseaux et avec des ressources externes sur Internet. Avec iDNS, vous pouvez fournir aux locataires des services de résolution de noms DNS pour leur espace de noms local et isolé et pour les ressources Internet.

Étant donné que le service iDNS n'est pas accessible à partir des réseaux virtuels du locataire, autre que par le biais du proxy iDNS, le serveur n'est pas vulnérable aux activités malveillantes sur les réseaux de locataires.

Fonctionnalités clés

Voici les principales fonctionnalités de iDNS.

- Fournit des services de résolution de noms DNS partagés pour les charges de travail des locataires
- Service DNS faisant autorité pour la résolution de noms et l'enregistrement DNS dans l'espace de noms du locataire
- Service DNS récursif pour la résolution de noms Internet à partir de machines virtuelles de locataire.
- Si vous le souhaitez, vous pouvez configurer l'hébergement simultané des noms d'infrastructure et de locataire
- Une solution DNS économique : les locataires n'ont pas besoin de déployer leur propre infrastructure DNS
- Haute disponibilité avec l'intégration d'Active Directory, ce qui est requis.

En plus de ces fonctionnalités, si vous souhaitez conserver vos serveurs DNS intégrés AD ouverts sur Internet, vous pouvez déployer des serveurs iDNS derrière un autre programme de résolution récursif dans le réseau de périmètre.

Comme iDNS est un serveur centralisé pour toutes les requêtes DNS, un fournisseur de services de configuration ou d'entreprise peut également implémenter des pare-feu DNS de locataire,

appliquer des filtres, détecter les activités malveillantes et auditer les transactions à un emplacement central

Infrastructure iDNS

L'infrastructure iDNS comprend les serveurs iDNS et le proxy iDNS.

Serveurs iDNS

iDNS inclut un ensemble de serveurs DNS qui hébergent des données spécifiques au locataire, telles que les enregistrements de ressources DNS de machine virtuelle.

Les serveurs iDNS sont les serveurs faisant autorité pour leurs zones DNS internes. Ils servent également de programme de résolution pour les noms publics quand des machines virtuelles de locataire tentent de se connecter à des ressources externes.

Tous les noms d'hôte des machines virtuelles sur des réseaux virtuels sont stockés en tant qu'enregistrements de ressources DNS dans la même zone. Par exemple, si vous déployez iDNS pour une zone nommée contoso.local, les enregistrements de ressources DNS pour les machines virtuelles sur ce réseau sont stockés dans la zone contoso.local.

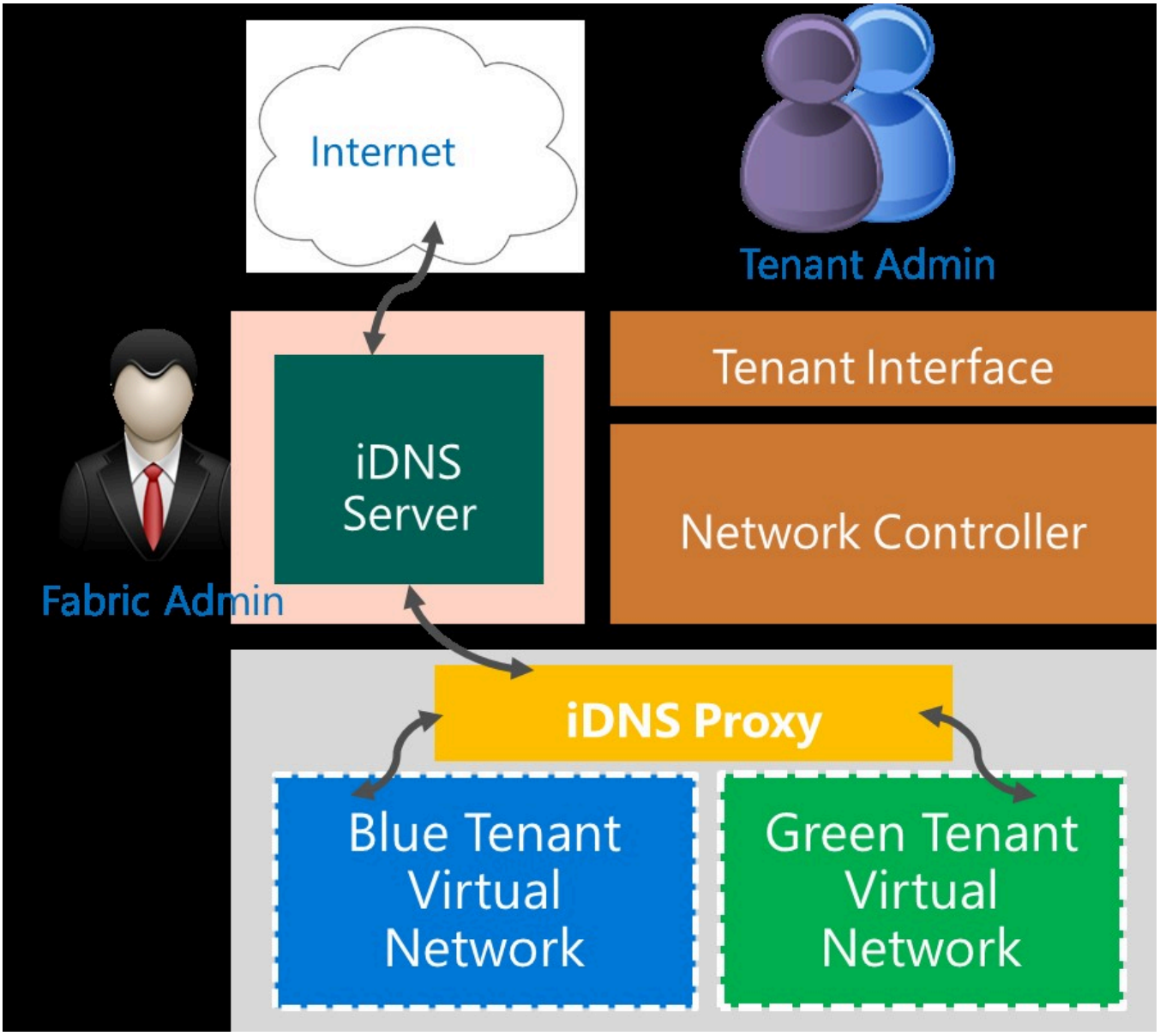
Les noms de domaine complets (FQDN) des machines virtuelles de locataire comprennent le nom d'ordinateur et la chaîne de suffixe DNS du réseau virtuel, au format GUID. Par exemple, si vous avez une machine virtuelle de locataire nommée TENANT1 qui se trouve sur le réseau virtuel contoso, local, le nom de domaine complet de la machine virtuelle est TENANT1. *vn-guid.contoso.local*, où *vn-guid* est la chaîne de suffixe DNS pour le réseau virtuel.

> **Notes**
>
> Si vous êtes un administrateur d'infrastructure, vous pouvez utiliser votre infrastructure de fournisseur de solutions Cloud ou DNS d'entreprise en tant que serveurs iDNS au lieu de déployer de nouveaux serveurs DNS spécifiquement destinés à être utilisés en tant que serveurs iDNS. Que vous déployiez de nouveaux serveurs pour iDNS ou que vous utilisiez votre infrastructure existante, iDNS s'appuie sur Active Directory pour fournir une haute disponibilité. Vos serveurs iDNS doivent donc être intégrés à Active Directory.

Proxy iDNS

Le proxy iDNS est un service Windows qui s'exécute sur chaque hôte et qui transfère le trafic DNS réseau virtuel locataire vers le serveur iDNS.

L'illustration suivante illustre les chemins d'accès au trafic DNS des réseaux virtuels de locataire via le proxy iDNS vers le serveur iDNS et Internet.



Comment déployer iDNS

Lorsque vous déployez SDN dans Windows Server 2016 à l'aide de scripts, iDNS est automatiquement inclus dans votre déploiement.

Pour plus d'informations, consultez les rubriques ci-dessous.

- Déployer une infrastructure SDN (Software Defined Networking) avec des scripts

Présentation des étapes de déploiement iDNS

Vous pouvez utiliser cette section pour comprendre comment iDNS est installé et configuré lorsque vous déployez SDN à l'aide de scripts.

Voici un résumé des étapes nécessaires au déploiement d'iDNS.

> ⓘ **Notes**
>
> Si vous avez déployé SDN à l'aide de scripts, vous n'avez pas besoin d'effectuer l'une de ces étapes. Les étapes sont fournies à des fins d'information et de résolution des problèmes uniquement.

Étape 1 : Déployer DNS

Vous pouvez déployer un serveur DNS à l'aide de l'exemple de commande Windows PowerShell suivant.

PowerShell

```
Install-WindowsFeature DNS -IncludeManagementTools
```

Étape 2 : Configurer les informations iDNS dans le contrôleur de réseau

Ce segment de script est un appel REST effectué par l'administrateur au contrôleur de réseau, l'informant de la configuration de la zone iDNS, telle que l'adresse IP du serveur iDNS et la zone utilisée pour héberger les noms iDNS.

```
Url: https://<url>/networking/v1/iDnsServer/configuration
Method: PUT
{
      "properties": {
        "connections": [
          {
            "managementAddresses": [
              "10.0.0.9"
            ],
            "credential": {
              "resourceRef": "/credentials/iDnsServer-Credentials"
            },
            "credentialType": "usernamePassword"
          }
        ],
        "zone": "contoso.local"
      }
    }
```

> ⓘ **Notes**
>
> Il s'agit d'un extrait de la section **Configuration ConfigureIDns** dans SDNExpress.ps1. Pour plus d'informations, consultez Deploy a Software Defined Network infrastructure using scripts (Déployer une infrastructure SDN à l'aide de scripts).

Étape 3 : Configurer le service proxy iDNS

Le service proxy iDNS s'exécute sur chacun des hôtes Hyper-V, fournissant le pont entre les réseaux virtuels des locataires et le réseau physique où se trouvent les serveurs iDNS. Les clés de registre suivantes doivent être créées sur chaque hôte Hyper-V.

Port DNS : Port fixe 53

- Clé de registre = HKLM\SYSTEM\CurrentControlSet\Services\NcHostAgent\Parameters\Plugins\Vnet\InfraServices\DnsProxyService"
- ValueName = « Port »
- ValueData = 53
- ValueType = « Dword »

Port du proxy DNS : port fixe 53

- Clé de registre = HKLM\SYSTEM\CurrentControlSet\Services\NcHostAgent\Parameters\Plugins\Vnet\InfraServices\DnsProxyService"
- ValueName = « ProxyPort »
- ValueData = 53
- ValueType = « Dword »

ADRESSE IP DNS : Adresse IP fixe configurée sur l'interface réseau, dans le cas où le locataire choisit d'utiliser le service iDNS

- Clé de registre = HKLM\SYSTEM\CurrentControlSet\Services\NcHostAgent\Parameters\Plugins\Vnet\InfraServices\DnsProxyService"
- ValueName = « IP »
- ValueData = « 169.254.169.254 »
- ValueType = « String »

Adresse MAC: Adresse de contrôle d'accès multimédia du serveur DNS

- Clé de registre = HKLM\SYSTEM\CurrentControlSet\Services\NcHostAgent\Parameters\Plugins\Vnet\InfraServices\DnsProxyService
- ValueName = « MAC »
- ValueData = "aa-bb-cc-aa-bb-cc»
- ValueType = « String »

Adresse du serveur IDNS : liste de serveurs iDNS séparés par des virgules.

- Clé de registre = HKLM\SYSTEM\CurrentControlSet\Services\DNSProxy\Parameters
- ValueName = « Expéditeurs »
- ValueData = « 10.0.0.9 »
- ValueType = « String »

> **Notes**
>
> Il s'agit d'un extrait de la section **Configuration ConfigureIDnsProxy** dans SDNExpress.ps1. Pour plus d'informations, consultez Deploy a Software Defined Network infrastructure using scripts (Déployer une infrastructure SDN à l'aide de scripts).

Étape 4 : Redémarrer le service agent hôte du contrôleur de réseau

Vous pouvez utiliser la commande Windows PowerShell suivante pour redémarrer le service agent hôte du contrôleur de réseau.

PowerShell

```
Restart-Service nchostagent -Force
```

Pour plus d'informations, consultez Restart-Service.

Activer les règles de pare-feu pour le service proxy DNS

Vous pouvez utiliser la commande Windows PowerShell suivante pour créer une règle de pare-feu qui autorise des exceptions pour que le proxy communique avec la machine virtuelle et le serveur iDNS.

PowerShell

```
Enable-NetFirewallRule -DisplayGroup 'DNS Proxy Firewall'
```

Pour plus d'informations, consultez Enable-NetFirewallRule.

Valider le service iDNS

Pour valider le service iDNS, vous devez déployer un exemple de charge de travail de locataire.

Pour plus d'informations, consultez Créer une machine virtuelle et établir la connexion à un réseau virtuel locataire ou un réseau local virtuel.

Si vous souhaitez que la machine virtuelle de locataire utilise le service iDNS, vous devez laisser la configuration du serveur DNS des interfaces réseau de machine virtuelle vide et autoriser les interfaces à utiliser DHCP.

Une fois la machine virtuelle avec une telle interface réseau lancée, elle reçoit automatiquement une configuration qui lui permet d'utiliser iDNS, et la machine virtuelle commence immédiatement à effectuer la résolution de noms à l'aide du service iDNS.

Si vous configurez la machine virtuelle cliente pour utiliser le service iDNS en laissant les informations du serveur DNS d'interface réseau et du serveur DNS secondaire vides, le contrôleur de réseau fournit à la machine virtuelle une adresse IP et effectue une inscription de nom DNS pour le compte de la machine virtuelle auprès du serveur iDNS.

Le contrôleur de réseau informe également le proxy iDNS sur la machine virtuelle et les détails requis pour effectuer la résolution de noms pour la machine virtuelle.

Lorsque la machine virtuelle lance une requête DNS, le proxy agit en tant que redirecteur de la requête du réseau virtuel vers le service iDNS.

Le proxy DNS garantit également que les requêtes de machine virtuelle de locataire sont isolées. Si le serveur iDNS fait autorité pour la requête, le serveur iDNS répond avec une réponse faisant autorité. Si le serveur iDNS ne fait pas autorité pour la requête, il effectue une récursivité DNS pour résoudre les noms Internet.

> ⓘ **Notes**
>
> Ces informations sont incluses dans la section **Configuration AttachToVirtualNetwork** dans SDNExpressTenant.ps1. Pour plus d'informations, consultez Deploy a Software Defined Network infrastructure using scripts (Déployer une infrastructure SDN à l'aide de scripts).

Qu’est-ce que le contrôleur de réseau ?

> S’applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Le contrôleur de réseau est la pierre angulaire de la gestion SDN (Software Defined Networking). Il s’agit d’un rôle serveur hautement évolutif qui fournit un point d’automatisation centralisé et programmable pour gérer, configurer, surveiller et dépanner l’infrastructure de réseau virtuel.

À l’aide du contrôleur de réseau, vous pouvez automatiser la configuration et la gestion de l’infrastructure réseau au lieu d’effectuer une configuration manuelle des appareils et services réseau.

Fonctionnement du contrôleur de réseau

Le contrôleur de réseau fournit une interface de programmation d’applications (API) qui lui permet de communiquer avec les appareils, services et composants réseau (API Southbound) et de les gérer ainsi qu’une deuxième API qui permet aux applications de gestion d’indiquer au contrôleur de réseau les paramètres réseau et les services dont elles ont besoin (API Northbound).

Avec l’API Southbound, le contrôleur de réseau peut gérer les appareils réseau et les services réseau et rassembler toutes les informations dont vous avez besoin sur le réseau. Le contrôleur de réseau supervise en permanence l’état des appareils et services réseau et s’assure que toute dérive de la configuration par rapport à l’état souhaité est corrigée.

L'API Northbound du contrôleur de réseau est implémentée comme une interface REST. Elle offre la possibilité de gérer le réseau de votre centre de données à partir d’applications de gestion. Pour la gestion, les utilisateurs peuvent recourir à l’API REST, directement ou par le biais de Windows PowerShell, ou des applications de gestion dotées d’une interface graphique utilisateur, comme Windows Admin Center ou System Center Virtual Machine Manager.

Pour en savoir plus sur ces applets de commande PowerShell, consultez la référence NetworkController.

Fonctionnalités du contrôleur de réseau

Le contrôleur de réseau vous permet de gérer les fonctionnalités SDN telles que les réseaux virtuels, les pare-feu, l'équilibreur de charge logiciel et la passerelle RAS. Voici quelques-unes de ses nombreuses fonctionnalités.

Gestion de réseau virtuel

Cette fonctionnalité du contrôleur de réseau vous permet de déployer et de configurer la virtualisation de réseau Hyper-V, de configurer des cartes réseau virtuelles sur des machines virtuelles individuelles et de stocker et distribuer des stratégies de réseau virtuel. Avec cette fonctionnalité, vous pouvez créer des réseaux virtuels et des sous-réseaux, attacher des machines virtuelles à ces réseaux et activer la communication entre les machines virtuelles du même réseau virtuel.

Le contrôleur de réseau prend en charge les réseaux virtuels basés sur un réseau local virtuel (VLAN), l'encapsulation de routage générique de virtualisation réseau (NVGRE) et le réseau VXLAN (Virtual Extensible Local Area Network).

Gestion de pare-feu

Cette fonctionnalité du contrôleur de réseau vous permet de configurer et de gérer les règles de pare-feu d'autorisation et de refus du contrôle d'accès pour vos machines virtuelles de charge de travail pour à la fois le trafic réseau interne (est/ouest) et externe (nord/sud) dans votre centre de données. Les règles de pare-feu sont intégrées dans le port vSwitch des VM de charge, de sorte qu'elles sont distribuées sur vos charges de travail dans le centre de données et accompagnent vos charges de travail.

À l'aide de l'API Northbound, vous pouvez définir les règles de pare-feu pour le trafic entrant et sortant à partir des machines virtuelles de charge de travail. Vous pouvez également configurer chaque règle de pare-feu pour consigner le trafic qui a été autorisé ou refusé par la règle.

Gestion de l'équilibreur de charge logiciel

Software Load Balancer vous permet d'activer plusieurs machines pour héberger la même charge de travail, ce qui offre une haute disponibilité et une scalabilité. À l'aide de l'équilibreur de charge logiciel, vous pouvez configurer et gérer l'équilibrage de charge, la traduction d'adresses réseau (NAT) de trafic entrant et l'accès sortant en direction d'Internet pour les charges de travail connectées aux réseaux virtuels et aux réseaux VLAN traditionnels.

Gestion de la passerelle

La passerelle RAS (Remote Access Service) vous permet de déployer, de configurer et de gérer des machines virtuelles qui sont membres d'un pool de passerelles, en fournissant une connectivité réseau externe aux charges de travail de vos clients. Avec les passerelles, les types de connectivité suivants sont pris en charge entre vos réseaux virtuels et distants :

- Connectivité avec la passerelle de réseau privé virtuel (VPN) de site à site à l'aide d'IPsec
- Connectivité de la passerelle VPN de site à site à l'aide de l'encapsulation GRE (Generic Routing Encapsulation)
- Fonctionnalité de transfert de couche 3

Les connexions de passerelle prennent en charge le protocole BGP (Border Gateway Protocol) pour la gestion dynamique des routes.

Chaînage d'appliances virtuelles

Cette fonctionnalité du contrôleur de réseau vous permet de joindre des appliances de réseau virtuel à vos réseaux virtuels. Ces appliances peuvent être utilisées pour de nombreux services réseau, tels que la protection avec pare-feu avancée, l'équilibrage de charge, la détection et la prévention des intrusions. Vous pouvez ajouter des appliances virtuelles qui exécutent des fonctions de routage et de mise en miroir des ports définies par l'utilisateur. Avec le routage défini par l'utilisateur, l'appliance virtuelle est utilisée en tant que routeur entre les sous-réseaux virtuels du réseau virtuel. Avec la mise en miroir de ports, tout le trafic réseau entrant ou sortant du port surveillé est dupliqué et envoyé à une appliance virtuelle pour analyse.

Pour en découvrir plus sur les routes définies par l'utilisateur, consultez Utiliser des équipements virtuels réseau sur un réseau virtuel.

Considérations relatives au déploiement du contrôleur de réseau

- Ne déployez pas le rôle serveur du contrôleur de réseau sur les hôtes physiques. Le contrôleur de réseau doit être déployé sur ses propres machines virtuelles dédiées.

- Vous pouvez déployer le contrôleur de réseau dans des environnements de domaine et non-domaine. Dans les environnements de domaine, le contrôleur de réseau authentifie les utilisateurs et les appareils réseau à l'aide de Kerberos ; dans les environnements non-domaines, vous devez déployer des certificats pour l'authentification.

- Il est essentiel que les déploiements du contrôleur de réseau offrent une haute disponibilité et la possibilité d'effectuer aisément un scale-up ou un scale-down en fonction des besoins

de votre centre de données. Utilisez au moins trois machines virtuelles afin de fournir une haute disponibilité pour l'application de contrôleur de réseau.

- Pour obtenir une disponibilité et une scalabilité élevées, le contrôleur de réseau s'appuie sur Service Fabric. Service Fabric fournit une plateforme de systèmes distribués pour la création d'applications scalables, fiables et faciles à gérer. Découvrez-en plus sur le contrôleur de réseau en tant qu'application Service Fabric.

Étapes suivantes

Pour consulter des informations connexes, reportez-vous également à :

- Planifier le déploiement du contrôleur de réseau
- Déployer le contrôleur de réseau à l'aide de Windows PowerShell
- SDN dans Azure Local et Windows Server

Dernière mise à jour : 15/09/2026

Network Controller avec le clustering de basculement

28/07/2025S'applique à: ✅ Windows Server 2025, ✅ Azure Local 2311.2 and later

À partir de Windows Server 2025, l'infrastructure réseau définie par logiciel utilise une empreinte plus petite pour le contrôleur de réseau (NC), un des composants essentiels de l'infrastructure. NC peut désormais être déployé directement sur l'hôte en tant que service Failover Clustering. L'infrastructure basée sur Service Fabric continue d'être prise en charge. Cet article fournit un aperçu de la haute disponibilité du contrôleur réseau en utilisant Failover Clustering, son fonctionnement avec le Load Balancer logiciel et les passerelles, et comment il diffère du contrôleur réseau sur Service Fabric.

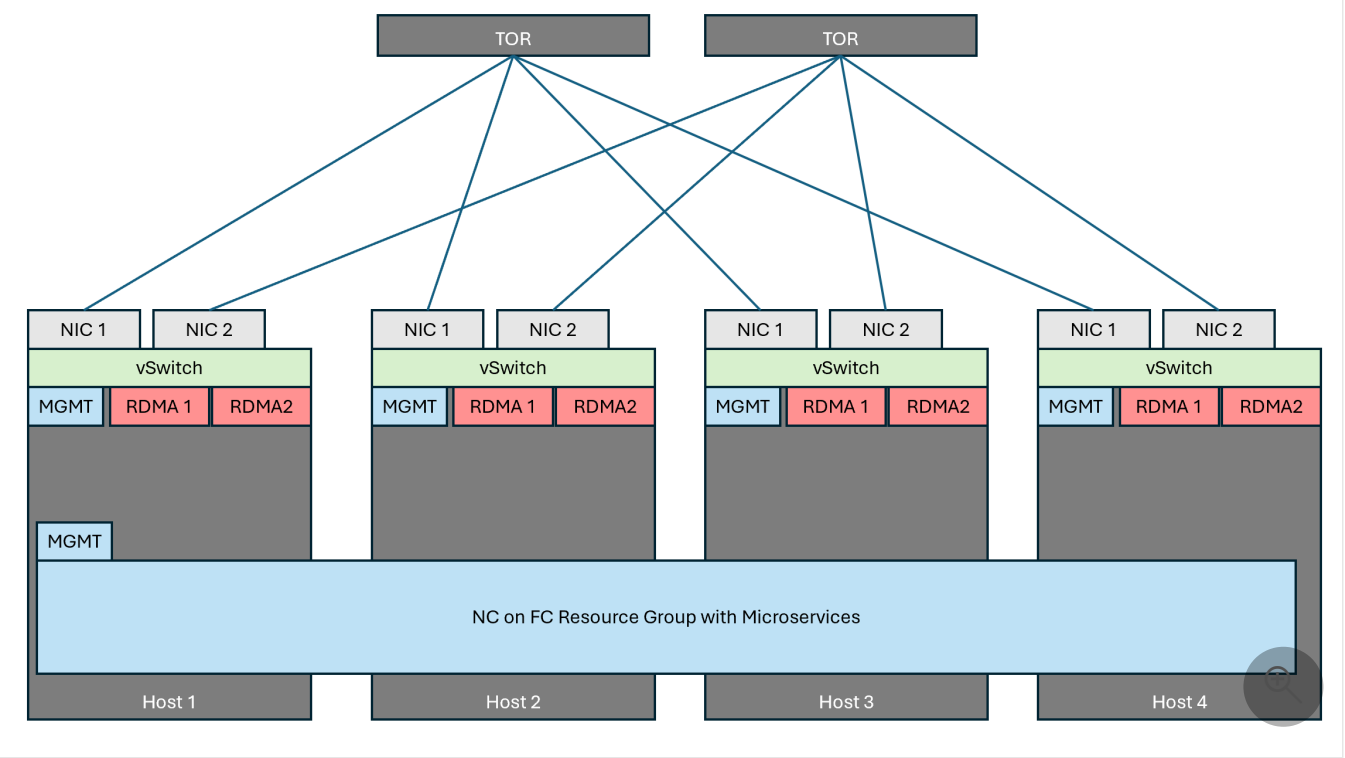
Contrôleur de réseau en tant que rôle

Le contrôleur de réseau est un composant clé de l'écosystème SDN. Il vous permet de déployer et de gérer vos configurations réseau client, notamment la mise en réseau virtuelle, la mise en réseau logique et la sécurité réseau. Dans les versions précédentes de Windows Server et d'Azure Local, le contrôleur de réseau devait être hébergé à l'intérieur d'une machine virtuelle. Le déploiement de ressources basées sur des machines virtuelles est long et gourmand en ressources. Les machines virtuelles ont pris davantage de processeur et de mémoire, ressources qui peuvent être dépensées sur vos charges de travail d'application principales. Depuis Windows Server 2025 et Azure Local 2311.2, le service de contrôleur réseau (NC) est nativement intégré à la machine hôte à l'aide du clustering de basculement, ce qui permet de libérer des ressources pour les autres charges de travail. L'illustration suivante fournit un aperçu des principales différences entre NC sur Service Fabric et NC sur Failover Clustering.

Architecture

Avec le contrôleur réseau sur Failover Clustering, tous les microservices du contrôleur réseau sont désormais contenus dans un groupe de ressources de cluster de basculement. Les microservices SDN utilisent une base de données unique et une partition unique, plutôt que trois bases de données dupliquées sur 3 machines virtuelles lors de l'utilisation de Service Fabric. Avec chaque microservice SDN en tant que groupe de ressources Failover Clustering, il y a une réduction significative de l'utilisation du CPU et du stockage.

Le contrôleur réseau et tous ses services sont configurés comme un groupe de ressources de cluster de basculement réparti sur les serveurs de votre cluster de Réseau Défini par Logiciel. Par exemple, votre topologie réseau inclut quatre serveurs regroupés avec un seul commutateur Top-of-Rack (ToR), et le composant contrôleur réseau en tant que *Failover Clustering Generic Resource* est réparti sur tous les serveurs. Au lieu des trois VM des versions précédentes, chaque microservice du contrôleur réseau est hautement disponible en tant que groupe de ressources de cluster de basculement. Le diagramme suivant montre un déploiement sur 4 nœuds avec le contrôleur réseau sur Failover Clustering.



Le groupe de ressources a les mêmes exigences d'approvisionnement que les machines virtuelles NC. Le microservice d'API nécessite une adresse IP flottante dans votre réseau de gestion et l'inscription DNS est toujours prise en charge.

High Availability

Avec le contrôleur réseau sur Failover Clustering, la propriété des ressources est associée à un nœud spécifique au sein du cluster de basculement. Lorsqu'un serveur tombe en panne, les groupes de ressources sont transférés vers un autre nœud au sein du cluster. La réplication des données est effectuée via l'infrastructure sous-jacente de Failover Clustering, qui est Storage Replica. Pour en savoir plus sur Failover Clustering et Storage Replica, veuillez consulter les ressources suivantes :

- Clustering de basculement dans Windows Server et Azure Local
- Vue d'ensemble de Storage Replica

Équilibrage de charge logicielle et passerelles

Cette transition de Service Fabric à Failover Clustering affecte uniquement nos services de contrôle réseau. D'autres rôles de virtualisation de fonction réseau, tels que l'équilibreur de charge logiciel et la passerelle, sont toujours hébergés sur des machines virtuelles. Le contrôleur réseau sur Failover Clustering n'affecte pas le comportement ou le fonctionnement des autres rôles de virtualisation des fonctions réseau. Pour plus d'informations sur l'équilibrage de charge logicielle et les passerelles, consultez les liens suivants :

- Qu’est-ce que l’équilibreur de charge logiciel (SLB) pour SDN ?
- Qu’est-ce que la passerelle RAS (Remote Access Service) pour la mise en réseau définie par logiciel ?

Next steps

Pour commencer à déployer le contrôleur réseau avec Failover Clustering dans votre environnement Réseau Défini par Logiciel, veuillez consulter Déployer un contrôleur réseau avec le cluster de basculement.

Pour en savoir plus sur les exigences et les options de configuration, consultez Planifier un déploiement SDN.

Contrôleur de réseau avec Service Fabric

Article • 28/12/2024 • S'applique à: ✅ Windows Server 2025, ✅ Azure Stack HCI, versions 24H2

Vous pouvez utiliser cette rubrique pour en savoir plus sur la haute disponibilité et la scalabilité du contrôleur de réseau pour la mise en réseau définie par logiciel (SDN) à l'aide de Service Fabric.

Lorsque vous déployez SDN dans votre centre de données, vous pouvez utiliser le contrôleur de réseau pour déployer, surveiller et gérer de nombreux éléments réseau, notamment les passerelles RAS, les équilibreurs de charge logicielles, les stratégies de mise en réseau virtuelle pour la communication des locataires, les stratégies de pare-feu du centre de données, la qualité de service (QoS) pour les stratégies SDN, les stratégies de mise en réseau hybride, etc.

Étant donné que le contrôleur de réseau est la pierre angulaire de la gestion SDN, il est essentiel pour les déploiements de contrôleur de réseau de fournir une haute disponibilité et la possibilité pour vous de monter ou de réduire facilement les nœuds de contrôleur de réseau avec vos besoins en matière de centre de données.

Bien que vous puissiez déployer le Contrôleur de réseau en tant que cluster d'une seule machine à des fins de haute disponibilité et de basculement, vous devez déployer le Contrôleur de réseau au sein d'un cluster de plusieurs machines comportant au moins trois machines.

> ⓘ **Notes**
>
> Vous pouvez déployer le contrôleur de réseau sur des ordinateurs serveur ou sur des machines virtuelles exécutant Windows Server 2016 Datacenter edition. Si vous déployez un contrôleur de réseau sur des machines virtuelles, les machines virtuelles doivent s'exécuter sur des hôtes Hyper-V qui exécutent également l'édition Datacenter. Le contrôleur de réseau n'est pas disponible sur Windows Server 2016 Standard Edition.

Contrôleur de réseau en tant qu'application Service Fabric

Pour obtenir une haute disponibilité et une scalabilité, le contrôleur de réseau s'appuie sur Service Fabric. Service Fabric fournit une plateforme de systèmes distribués pour créer des applications évolutives, fiables et faciles à gérer.

En tant que plateforme, Service Fabric fournit des fonctionnalités requises pour la création d'un système distribué évolutif. Il fournit un hébergement de service sur plusieurs instances de système d'exploitation, la synchronisation des informations d'état entre les instances, l'élection d'un leader, la détection des défaillances, l'équilibrage de charge, etc.

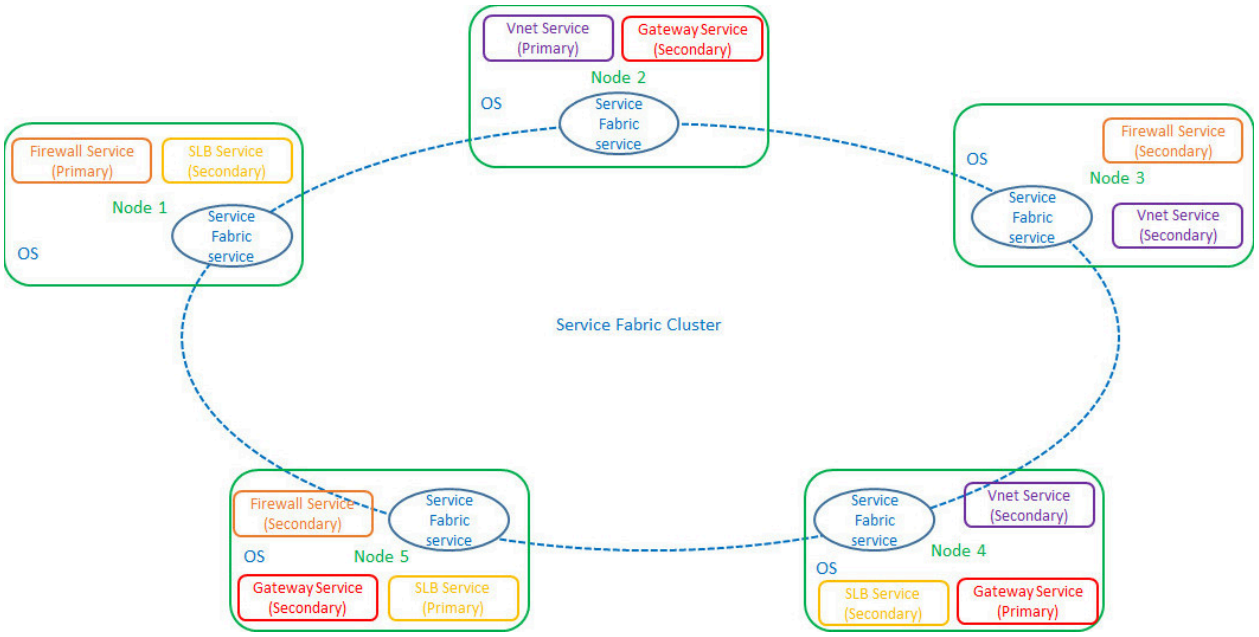
> ⓘ **Notes**
>
> Pour plus d'informations sur Service Fabric dans Azure, consultez **Vue d'ensemble d'Azure Service Fabric**.

Lorsque vous déployez le contrôleur de réseau sur plusieurs machines, le contrôleur de réseau s'exécute en tant qu'application Service Fabric unique sur un cluster Service Fabric. Vous pouvez former un cluster Service Fabric en connectant un ensemble d'instances de système d'exploitation.

L'application Contrôleur de réseau est composée de plusieurs services Service Fabric avec état. Chaque service est responsable d'une fonction réseau, telle que la gestion du réseau physique, la gestion du réseau virtuel, la gestion du pare-feu ou la gestion des passerelles.

Chaque service Service Fabric a une réplique principale et deux répliques secondaires. Le réplica de service principal traite les demandes, tandis que les deux réplicas de service secondaires fournissent une haute disponibilité dans les cas où le réplica principal est désactivé ou indisponible pour une raison quelconque.

L'illustration suivante illustre un cluster Service Fabric de contrôleur de réseau avec cinq machines. Quatre services sont distribués sur les cinq machines : service de pare-feu, service de passerelle, service d'équilibrage de charge logicielle (SLB) et service de réseau virtuel (Vnet). Chacun des quatre services comprend une réplique de service principal et deux répliques de service secondaire.



Avantages de l'utilisation de Service Fabric

Voici les principaux avantages de l'utilisation de Service Fabric pour les clusters Network Controller.

Haute disponibilité et scalabilité

Étant donné que le contrôleur de réseau est le cœur d'un réseau de centre de données, il doit être résilient à l'échec et être suffisamment évolutif pour permettre des modifications agiles dans les réseaux de centres de données au fil du temps. Les fonctionnalités suivantes fournissent ces capacités :

- **Bascule rapide**. Service Fabric permet une bascule rapide à des vitesses très élevées. Plusieurs réplicas de service secondaires chauds sont toujours disponibles. Si une instance de système d'exploitation devient indisponible en raison d'une défaillance matérielle, l'un des réplicas secondaires est immédiatement promu vers le réplica principal.
- **Agilité de mise à l'échelle**. Vous pouvez facilement et rapidement mettre à l'échelle ces services fiables à partir de quelques instances jusqu'à des milliers d'instances, puis revenir à quelques instances, en fonction de vos besoins en ressources.

Stockage persistant

L'application du contrôleur de réseau a de grandes exigences de stockage pour sa configuration et son état. L'application doit également être utilisable entre les pannes

planifiées et non planifiées. À cet effet, Service Fabric fournit un magasin Key-Value (KVS) qui est un magasin répliqué, transactionnel et persistant.

Modularité

Le contrôleur de réseau est conçu avec une architecture modulaire, avec chacun des services réseau, tels que le service de réseaux virtuels et le service de pare-feu, intégré en tant que services individuels.

Cette architecture d'application offre les avantages suivants.

1. La modularité du contrôleur de réseau permet un développement indépendant de chacun des services pris en charge, au fur et à mesure que les besoins évoluent. Par exemple, le service d'équilibrage de charge logiciel peut être mis à jour sans affecter les autres services ou le fonctionnement normal du contrôleur de réseau.
2. La modularité du contrôleur de réseau permet l'ajout de nouveaux services, au fur et à mesure que le réseau évolue. De nouveaux services peuvent être ajoutés au contrôleur de réseau sans impact sur les services existants.

> **Notes**
>
> Dans Windows Server 2016, l'ajout de services tiers au contrôleur de réseau n'est pas pris en charge.

La modularité Service Fabric utilise des schémas de modèle de service pour optimiser la facilité de développement, de déploiement et de maintenance d'une application.

Options de déploiement du contrôleur de réseau

Pour déployer le contrôleur de réseau à l'aide de System Center Virtual Machine Manager (VMM), consultez Configurer un contrôleur de réseau SDN dans l'infrastructure VMM.

Pour déployer un contrôleur de réseau à l'aide de scripts, consultez Déployer une infrastructure réseau définie par logiciel à l'aide de scripts.

Pour déployer un contrôleur de réseau à l'aide de Windows PowerShell, consultez Déployer un contrôleur de réseau à l'aide de Windows PowerShell

Pour plus d'informations sur le contrôleur de réseau, consultez contrôleur de réseau.

Commentaires

Cette page a-t-elle été utile ? Yes No

Installer le rôle serveur Contrôleur de réseau en utilisant le Gestionnaire de serveur

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cette rubrique fournit des instructions sur l'installation du rôle serveur pour le contrôleur de réseau à l'aide du Gestionnaire de serveur.

> ⓘ **Important**
>
> Ne déployez pas le rôle serveur du contrôleur de réseau sur les hôtes physiques. Pour déployer le contrôleur de réseau, vous devez installer le rôle serveur du contrôleur de réseau sur une machine virtuelle Hyper-V installée sur un hôte Hyper-V. Une fois que vous avez installé le contrôleur de réseau sur des machines virtuelles sur trois hôtes Hyper-V différents, vous devez activer les hôtes Hyper-V pour le SDN (Software Defined Networking) en ajoutant les hôtes au contrôleur de réseau à l'aide de la commande Windows PowerShell **New-NetworkControllerServer**. En procédant ainsi, vous activez le Load Balancer logiciel SDN pour qu'il fonctionne. Pour plus d'informations, consultez New-NetworkControllerServer.

Après avoir installé le contrôleur de réseau, vous devez utiliser les commandes Windows PowerShell pour une configuration supplémentaire du contrôleur de réseau. Pour plus d'informations, consultez Déployer le Contrôleur de réseau à l'aide de Windows PowerShell.

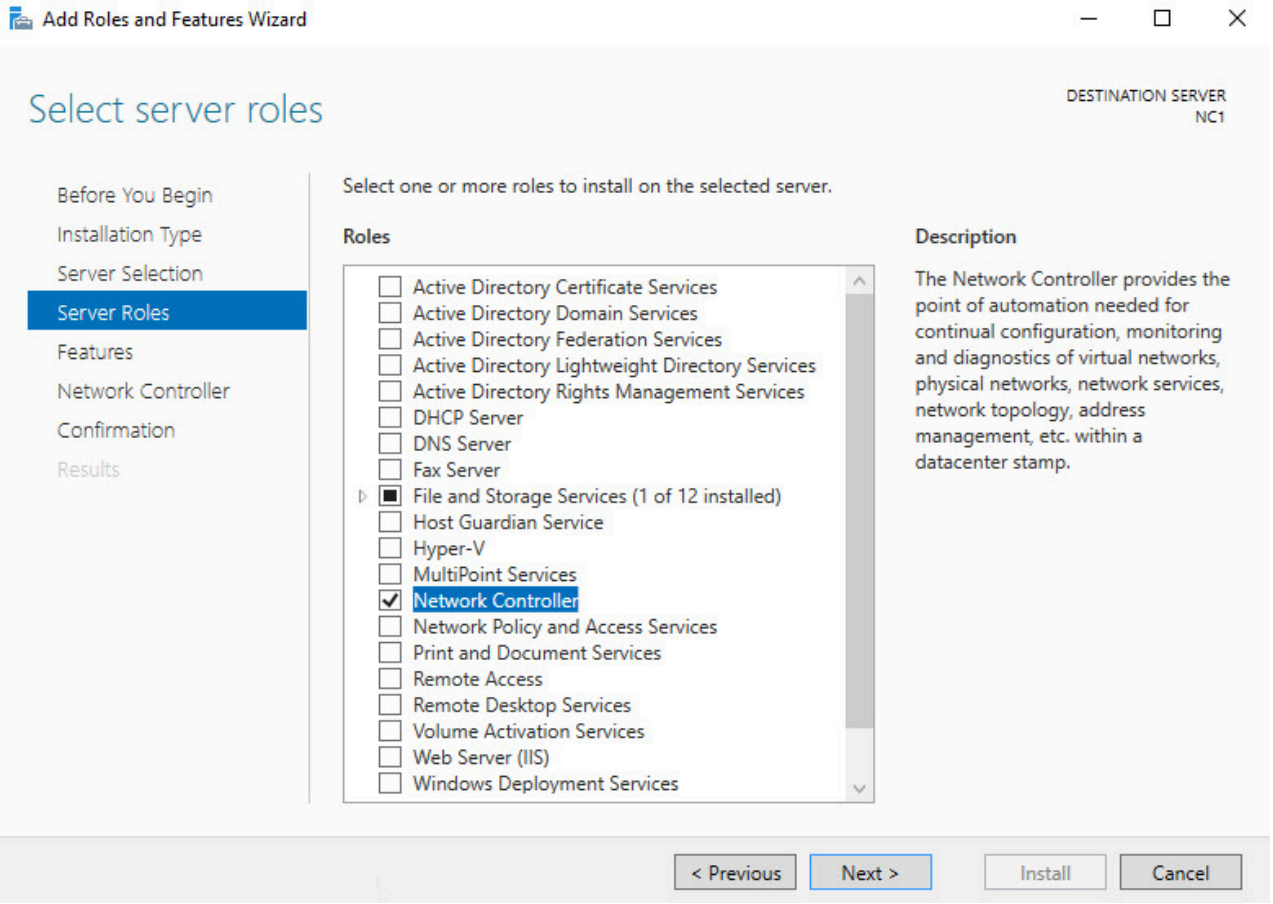
Pour installer le contrôleur de réseau

1. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre. Cliquez sur **Suivant**.

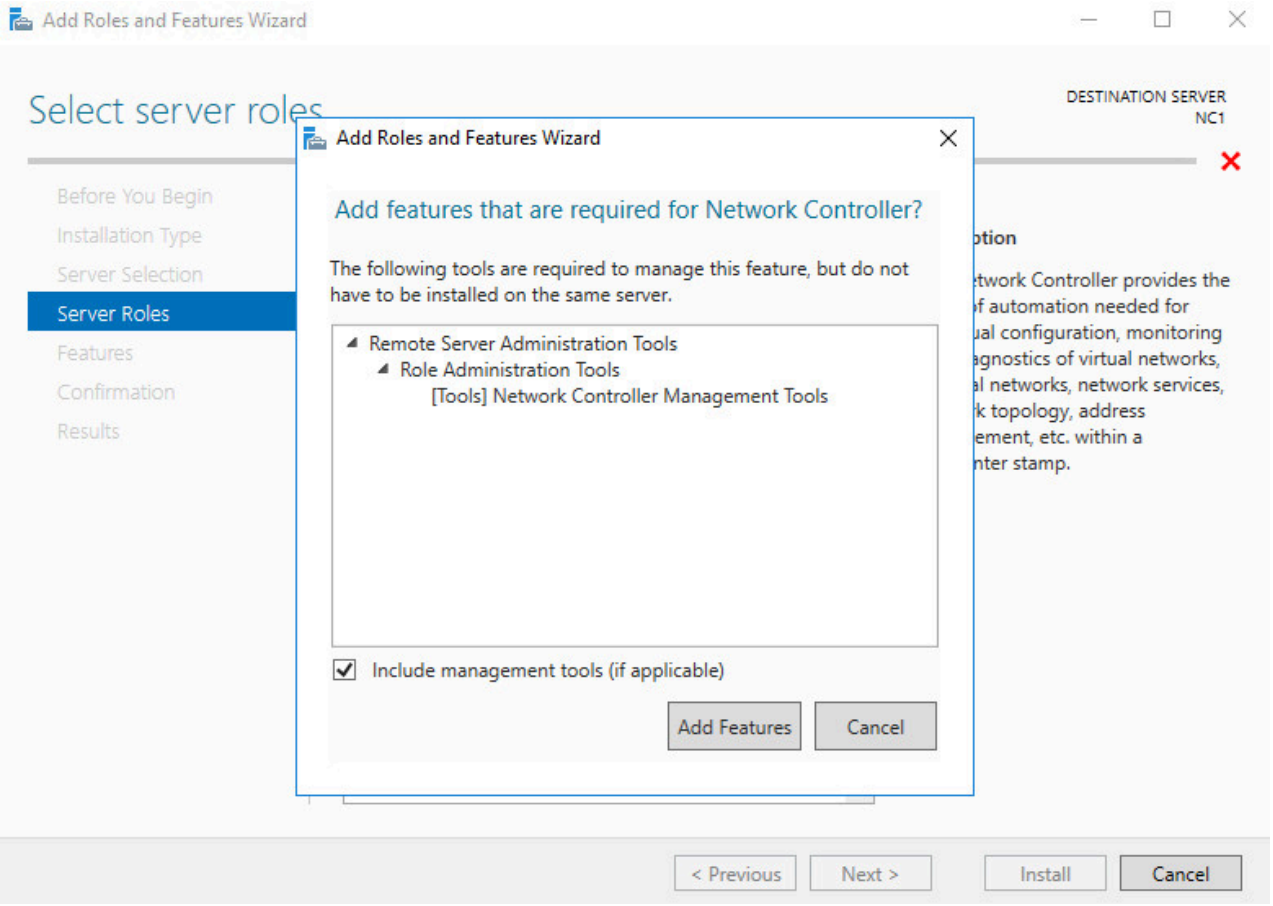
2. Dans **Sélectionner le type d'installation**, conservez le paramètre par défaut, puis cliquez sur **Suivant**.

3. Dans **Sélectionner le serveur de destination**, choisissez le serveur sur lequel vous souhaitez installer le contrôleur de réseau, puis cliquez sur **Suivant**.

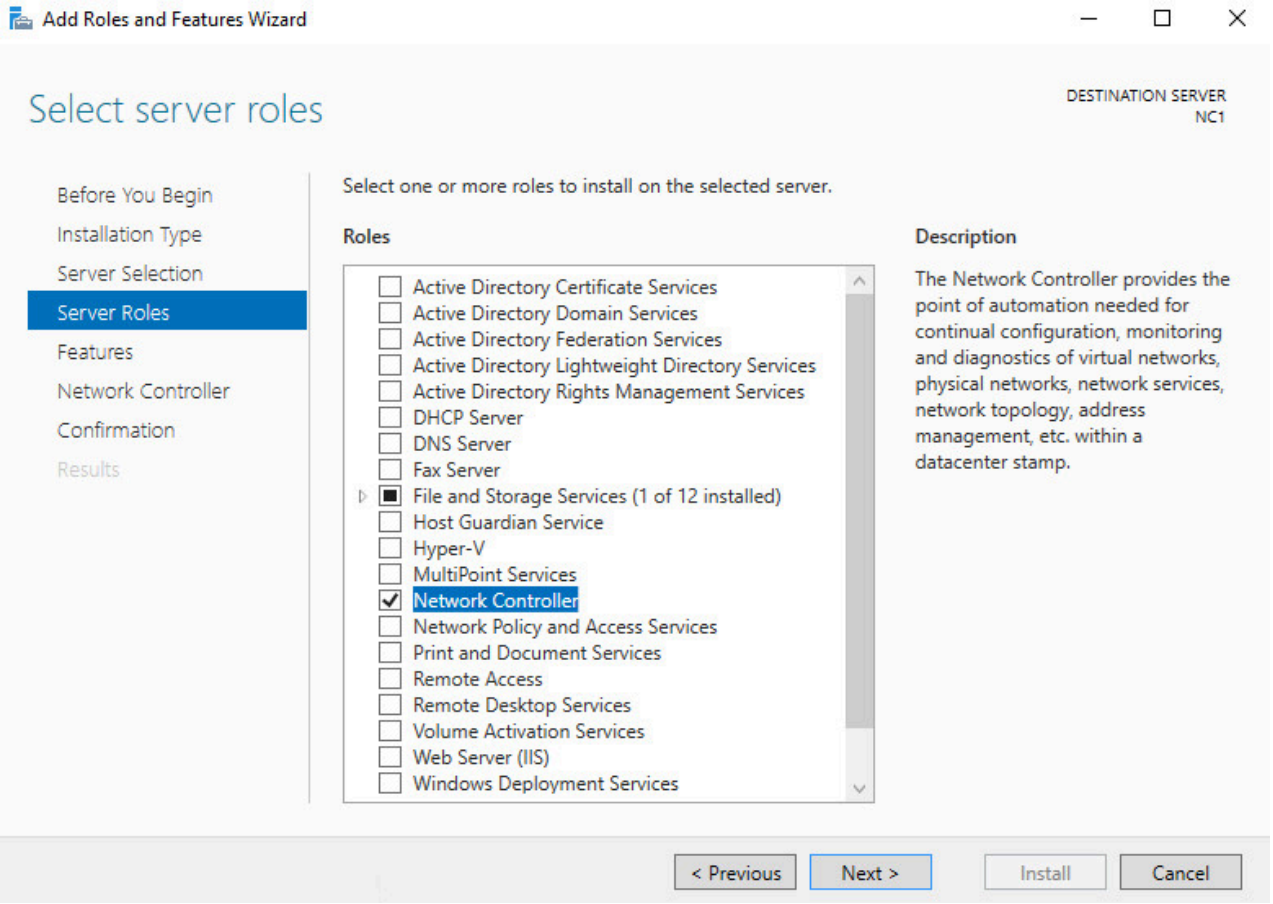
4. Dans **Sélectionner des rôles de serveur**, dans **Rôles**, cliquez sur **Contrôleur de réseau**.



5. La boîte de dialogue **Ajouter des fonctionnalités requises pour le contrôleur de réseau** s'ouvre. Cliquez sur **Ajouter des fonctionnalités**.



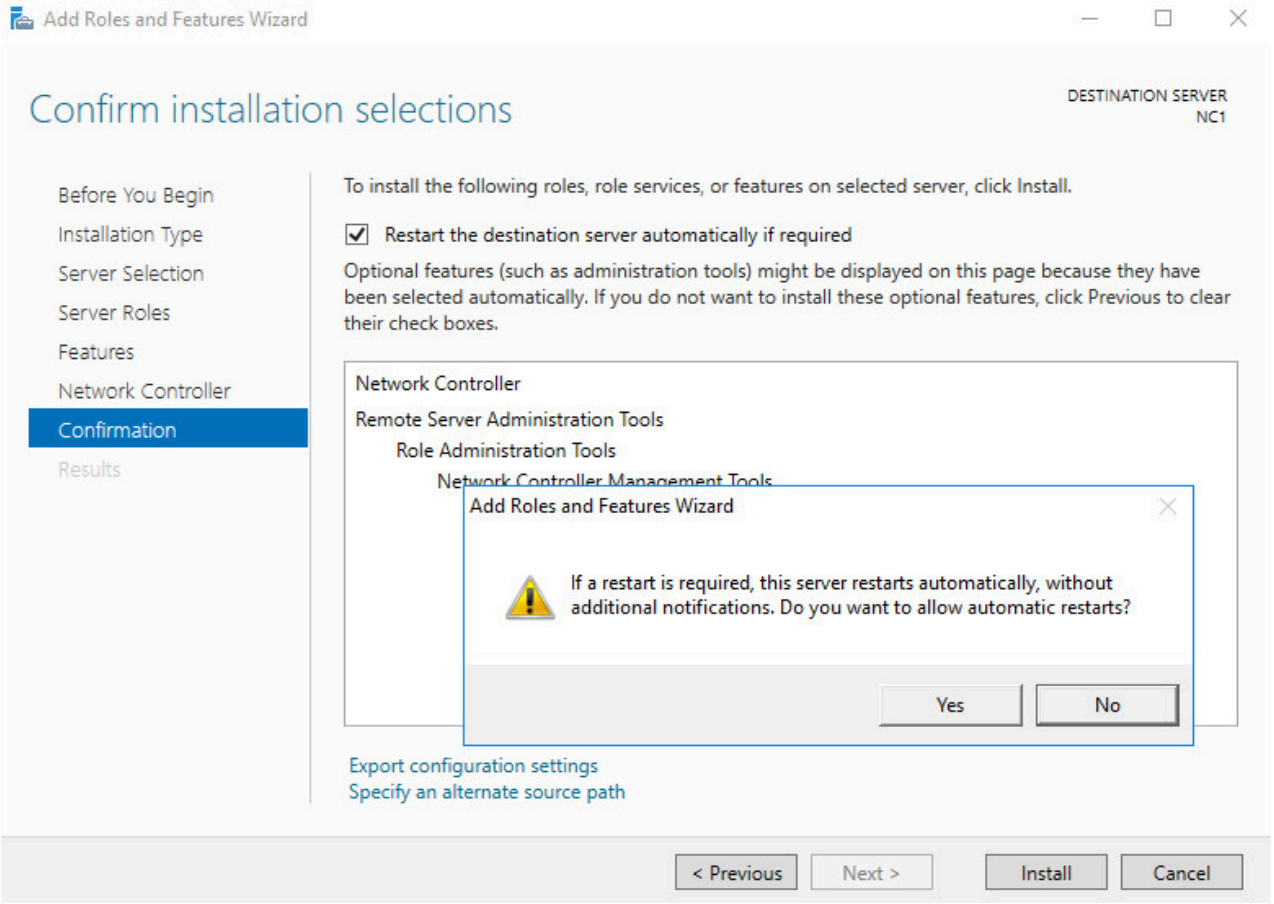
6. Dans **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.



7. Dans **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

8. Dans **le contrôleur de réseau** , cliquez sur **Suivant**.

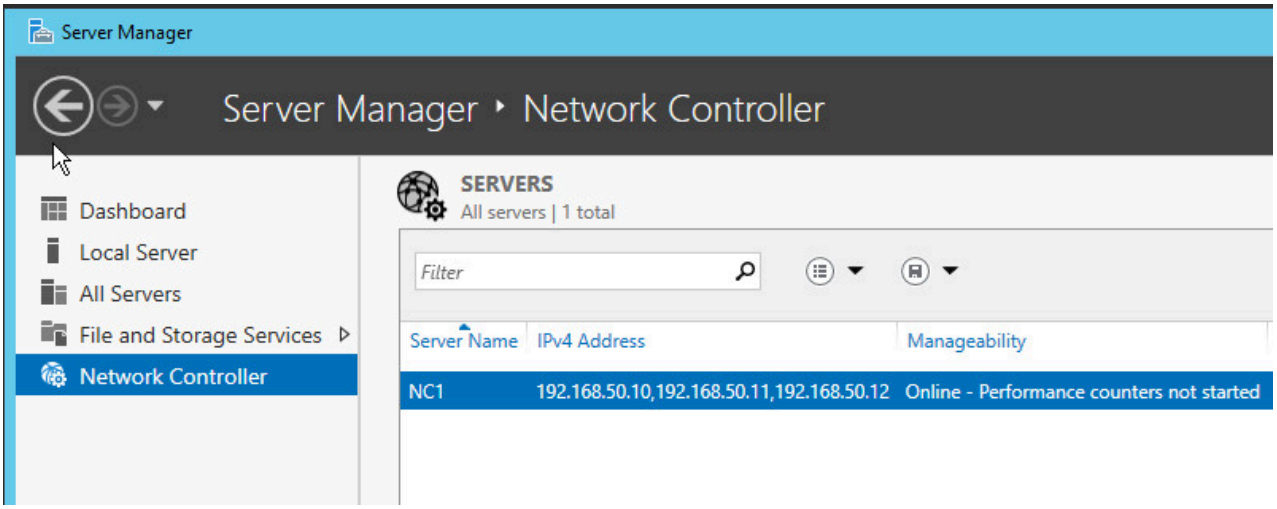
9. Dans **Confirmer les sélections d'installation**, passez en revue vos choix. L'installation du contrôleur de réseau nécessite que vous redémarriez l'ordinateur après l'exécution de l'assistant. Pour cette raison, cliquez sur **Redémarrer automatiquement le serveur de destination, si nécessaire**. La boîte de dialogue **Assistant d'ajout de rôles et de fonctionnalités** s'ouvre. Cliquez sur **Oui**.



10. Dans **Confirmer les sélections pour l'installation**, cliquez sur **Installer**.

11. Le rôle serveur pour le contrôleur de réseau s'installe sur le serveur de destination, puis le serveur redémarre.

12. Une fois l'ordinateur redémarré, connectez-vous à l'ordinateur et vérifiez l'installation du contrôleur de réseau en affichant le Gestionnaire de serveur.



Voir aussi

Contrôleur de réseau

Etapes de post-déploiement pour contrôleur de réseau

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Lorsque vous installez le contrôleur de réseau, vous pouvez choisir des déploiements Kerberos ou non Kerberos.

Pour les déploiements non Kerberos, vous devez configurer des certificats.

Configurer des certificats pour les déploiements non Kerberos

Si les ordinateurs ou machines virtuelles pour le contrôleur de réseau et le client de gestion ne sont pas joints à un domaine, vous devez configurer l'authentification basée sur les certificats en effectuant les étapes suivantes.

- Créez un certificat sur le contrôleur de réseau pour l'authentification de l'ordinateur. Le nom d'objet du certificat doit être le même que le nom DNS du Contrôleur de réseau ou machine virtuelle.
- Créez un certificat sur le client de gestion. Ce certificat doit être approuvé par le contrôleur de réseau.
- Inscrivez un certificat sur l'ordinateur ou la machine virtuelle du contrôleur de réseau. Le certificat doit répondre aux critères suivants.
  - L'objectif d'authentification du serveur et l'objectif d'authentification du client doivent être configurés dans les extensions Utilisation améliorée de la clé (EKU) ou Stratégies d'application. L'identificateur d'objet pour l'authentification du serveur est 1.3.6.1.5.5.7.3.1. L'identificateur d'objet pour l'authentification du client est 1.3.6.1.5.5.7.3.2.
  - Le nom de l'objet du certificat doit être résolu en :
    - Adresse IP de l'ordinateur ou de la machine virtuelle du contrôleur de réseau, si le contrôleur de réseau est déployé sur un seul ordinateur ou machine virtuelle.
    - Adresse IP REST, si le contrôleur de réseau est déployé sur plusieurs ordinateurs, plusieurs machines virtuelles ou les deux.

- Ce certificat doit être approuvé par tous les clients REST. Le certificat doit également être approuvé par le multiplexeur MUX (Software Load Balancing) et les ordinateurs hôtes en direction sud qui sont gérés par le contrôleur de réseau.
- Le certificat peut être inscrit par une autorité de certification ou peut être un certificat auto-signé. Les certificats auto-signés ne sont pas recommandés pour les déploiements de production, mais sont acceptables pour les environnements de laboratoire de test.
- Le même certificat doit être provisionné sur tous les nœuds du contrôleur de réseau. Après avoir créé le certificat sur un nœud, vous pouvez exporter le certificat (avec une clé privée) et l'importer sur les autres nœuds.

Pour plus d'informations, consultez Contrôleur de réseau.

Virtualisation de fonction réseau

08/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour en savoir plus sur la virtualisation des fonctions réseau, qui vous permet de déployer des appliances réseau virtuelles telles que le pare-feu datacenter, la passerelle RAS multilocataire et l'équilibrage de charge logicielle (SLB) multiplexeur (MUX).

> ⓘ **Notes**
>
> Outre cette rubrique, la documentation de virtualisation de fonction de réseau suivante est également disponible.
>
> - Présentation du pare-feu de centre de données
> - Passerelle du serveur d'accès à distance pour SDN
> - Équilibrage de la charge logicielle pour SDN

Dans les centres de données d'aujourd'hui avec définition logicielle, les fonctions réseau effectuées par les appliances matérielles (équilibreurs de charge, pare-feu, routeurs, commutateurs, etc.) sont de plus en plus virtualisées, de façon à jouer le rôle d'appliance virtuelle. Cette « virtualisation des fonctions réseau » est une évolution naturelle de la virtualisation des serveurs et des réseaux. Les appliances virtuelles se développent rapidement et créent un tout nouveau marché. Elles ne cessent d'éveiller l'intérêt et de gagner en puissance dans les plateformes de virtualisation et les services cloud.

Microsoft a inclus une passerelle autonome en tant qu'appliance virtuelle à partir de Windows Server 2012 R2 . Pour plus d'informations, voir Passerelle Windows Server. Maintenant, avec Windows Server 2016 Microsoft continue de se développer et d'investir dans le marché de la virtualisation des fonctions réseau.

Avantages de l'appliance virtuelle

Une appliance virtuelle est dynamique et facile à modifier, car il s'agit d'une machine virtuelle prédéfinie et personnalisée. Il peut s'agir d'une ou plusieurs machines virtuelles empaquetées, mises à jour et gérées en tant qu'unité. Avec la mise en réseau à définition logicielle (SDN), vous bénéficiez de l'agilité et de la flexibilité nécessaires dans l'infrastructure cloud d'aujourd'hui. Par exemple:

- La SDN présente le réseau sous la forme d'une ressource dynamique et groupée.
- La SDN facilite l'isolation des locataires.
- La SDN optimise la mise à l'échelle et les performances.
- Les appliances virtuelles permettent une expansion de la capacité transparente et la mobilité des charges de travail.
- Les appliances virtuelles réduisent la complexité opérationnelle.
- Les appliances virtuelles permettent aux clients d'acquérir, de déployer et de gérer facilement des solutions préintégrées.
    - Les clients peuvent facilement déplacer l'appliance virtuelle n'importe où dans le cloud.
    - Les clients peuvent mettre à l'échelle des appliances virtuelles de manière dynamique en fonction de la demande.

Pour plus d'informations sur Microsoft SDN, consultez SDN (Software Defined Networking).

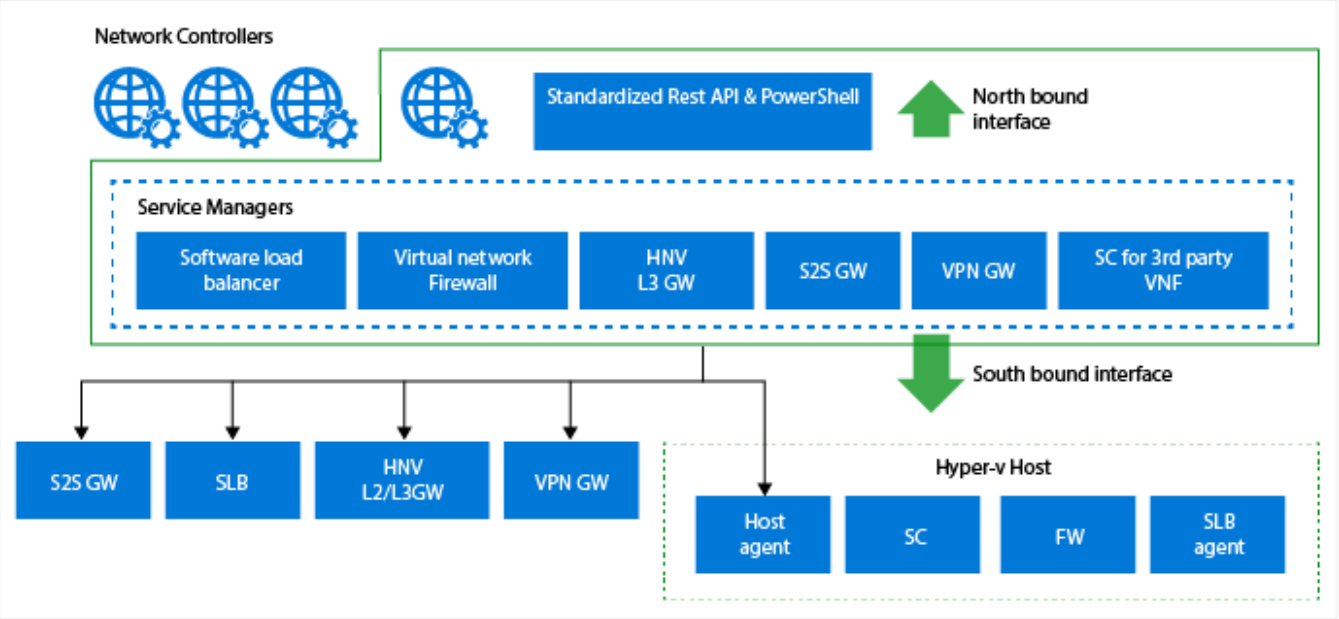
Quelles fonctions réseau sont virtualisées ?

La place de marché pour les fonctions réseau virtualisées se développe rapidement. Les fonctions réseau suivantes sont en cours de virtualisation :

- **Security**
    - Firewall
    - Antivirus
    - DDoS (Déni de service distribué)
    - IPS/IDS (Système de prévention des intrusions/Système de détection d'intrusion)
- **Optimiseurs d'application/WAN**
- **Edge**
    - Passerelle de site à site
    - Passerelles L3
    - Routers
    - Switches

- NAT
- Équilibreurs de charge (pas nécessairement en périphérie)
- Serveur proxy HTTP

Pourquoi Microsoft est une excellente plateforme pour les appliances virtuelles



La plateforme Microsoft a été conçue pour être une excellente plateforme pour créer et déployer des appliances virtuelles. Voici pourquoi :

- Microsoft fournit des fonctions réseau virtualisées clés avec Windows Server 2016.
- Vous pouvez déployer une appliance virtuelle à partir du fournisseur de votre choix.
- Vous pouvez déployer, configurer et gérer vos appliances virtuelles avec le contrôleur de réseau Microsoft fourni avec Windows Server 2016. Pour plus d'informations sur le contrôleur de réseau, consultez Contrôleur de réseau.
- Hyper-V peut héberger les principaux systèmes d'exploitation invités dont vous avez besoin.

Virtualisation des fonctions réseau dans Windows Server 2016

Fonctions d'appliances virtuelles fournies par Microsoft

Les appliances virtuelles suivantes sont fournies avec Windows Server 2016 :

Équilibreur de charge logiciel

Équilibreur de charge de couche 4 fonctionnant à l'échelle du centre de données. Il s'agit d'une version similaire de l'équilibreur de charge d'Azure qui a été déployé à grande échelle dans l'environnement Azure. Pour plus d'informations sur Microsoft Software Load Balancer, consultez Équilibrage de charge logiciel (SLB) pour SDN. Pour plus d'informations sur les services d'équilibrage de charge Microsoft Azure, consultez Microsoft Azure Load Balancing Services.

Gateway. La passerelle RAS fournit toutes les combinaisons des fonctions de passerelle suivantes.

- **Passerelle de site à site**

  La passerelle RAS fournit un protocole de type Border Gateway Protocol (BGP), multilocataire qui permet à vos locataires d'accéder à leurs ressources et de les gérer sur des connexions VPN site à site à partir de sites distants, et qui autorise le flux de trafic réseau entre les ressources virtuelles dans le cloud et les réseaux physiques du locataire. Pour plus d'informations sur la passerelle RAS, consultez Haute disponibilité de la passerelle RAS et Passerelle RAS.

- **Passerelle de transfert**

  La passerelle RAS achemine le trafic entre les réseaux virtuels et le réseau physique du fournisseur d'hébergement. Par exemple, si les locataires créent un ou plusieurs réseaux virtuels et ont besoin d'accéder aux ressources partagées sur le réseau physique du fournisseur d'hébergement, la passerelle de transfert peut acheminer le trafic entre le réseau virtuel et le réseau physique pour fournir aux utilisateurs travaillant sur le réseau virtuel les services dont ils ont besoin. Pour plus d'informations, consultez Haute disponibilité de la passerelle RAS et Passerelle RAS.

- **Passerelles de tunnel GRE**

  Les tunnels GRE activent la connectivité entre les réseaux virtuels clients et les réseaux externes. Dans la mesure où le protocole GRE est léger et que sa prise en charge est disponible sur la plupart des périphériques réseau, il constitue un choix idéal pour le tunneling, dans lequel le chiffrement de données n'est pas nécessaire. La prise en charge GRE dans les tunnels de site à site (S2S) résout le problème de transfert entre les réseaux virtuels clients et les réseaux externes clients à l'aide d'une passerelle mutualisée. Pour plus d'informations, sur les tunnels GRE, voir Tunneling GRE dans Windows Server 2016.

Plan de contrôle de routage avec BGP

Le contrôle de routage HNV (Hyper-V Network Virtualization) est l'entité logique centralisée dans le plan de contrôle, qui transporte toutes les routes du plan d'adresse client et apprend dynamiquement, puis met à jour les routeurs de passerelle RAS distribués dans le réseau virtuel. Pour plus d'informations, consultez Haute disponibilité de la passerelle RAS et Passerelle RAS.

Pare-feu multilocataire distribué

Le pare-feu protège la couche réseau des réseaux virtuels. Les stratégies sont appliquées au niveau du port SDN-vSwitch de chaque machine virtuelle locataire. Il protège tous les flux de trafic : est-ouest et nord-sud. Les stratégies sont envoyées via le portail des locataires, tandis que le contrôleur de réseau les distribue à tous les hôtes applicables. Pour plus d'informations sur le pare-feu multilocataire distribué, consultez Vue d'ensemble du pare-feu du centre de données.

Qu'est-ce que le pare-feu de centre de données ?

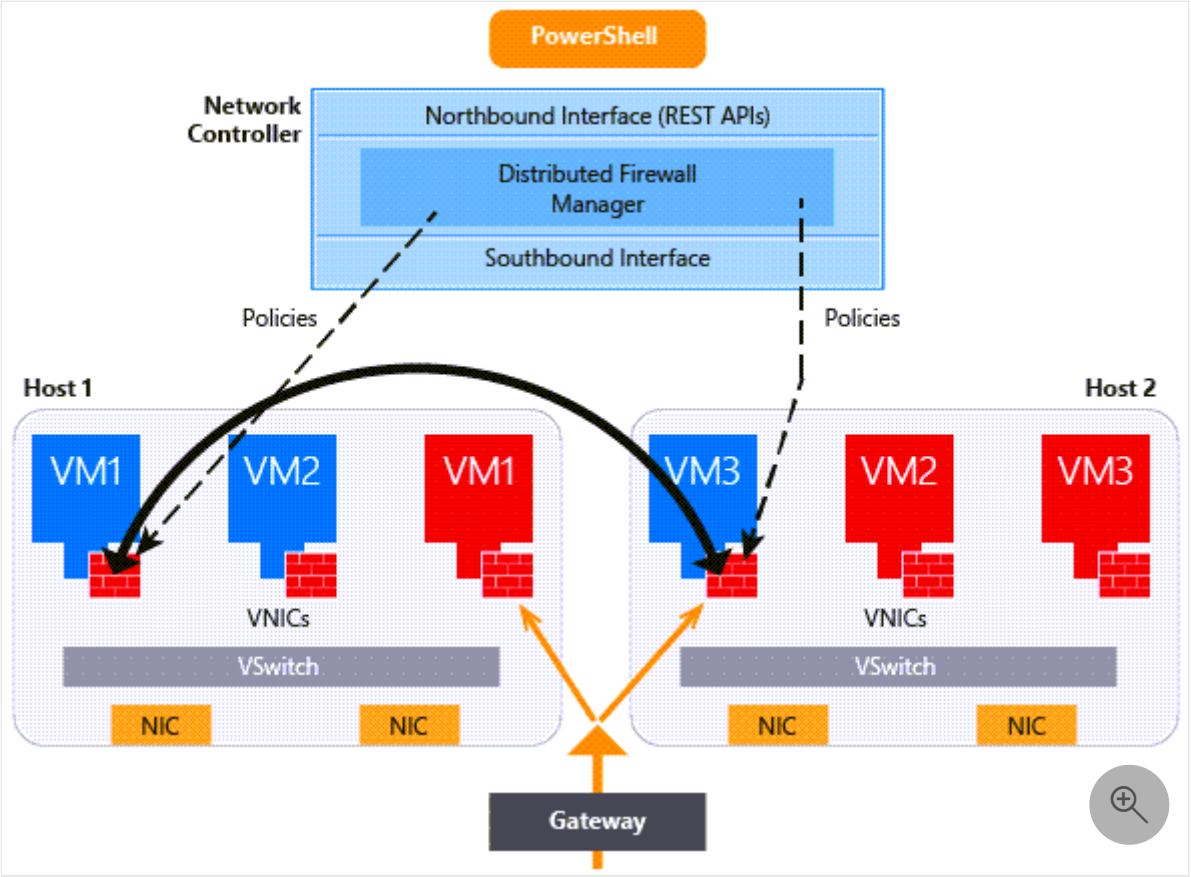
> S’applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Le pare-feu Datacenter est un pare-feu de couche réseau à 5 tuples (protocole, numéro de port source et de destination, adresses IP source et de destination), avec état et mise en réseau SDN (Software Defined Networking) multilocataire. Le Pare-feu Datacenter protège les flux de trafic Est-Ouest et Nord-Sud sur la couche réseau des réseaux virtuels et des réseaux VLAN traditionnels.

Comment fonctionne le pare-feu de centre de données

Vous activez et configurez le Pare-feu du centre de données en créant des groupes de sécurité réseau (NSG) qui sont appliqués à un sous-réseau ou à une interface réseau. Les stratégies de pare-feu sont appliquées au port vSwitch de chaque machine virtuelle client. Les stratégies sont envoyées via le portail des locataires, tandis que le contrôleur de réseau les distribue à tous les hôtes applicables.

Les administrateurs de locataires peuvent installer et configurer des stratégies de pare-feu pour protéger leurs réseaux contre le trafic indésirable provenant des réseaux Internet et intranet.



L'administrateur de fournisseur de services ou l'administrateur de locataire peut gérer les stratégies du Pare-feu Datacenter via le contrôleur de réseau et les API orientées Nord. Vous pouvez également configurer et gérer les stratégies du Pare-feu Datacenter avec Windows Admin Center.

Avantages pour les fournisseurs de services cloud

Le Pare-feu de centres de données offre les avantages suivants pour les fournisseurs de services cloud :

- Une solution de pare-feu logicielle hautement scalable, gérable et diagnosticable qui peut être offerte aux locataires
- La liberté de déplacer les machines virtuelles locataires vers différents hôtes de calcul sans rompre les stratégies de pare-feu de locataire
  - Déployé en tant que pare-feu de l'agent hôte du port vSwitch
  - Les machines virtuelles locataires obtiennent les stratégies affectées au pare-feu de leur agent hôte vSwitch
  - Les règles de pare-feu sont configurées dans chaque port vSwitch, indépendamment de l'hôte exécutant la machine virtuelle

- Offre une protection aux machines virtuelles locataires, indépendamment du système d'exploitation invité du locataire

Avantages pour les locataires

Le Pare-feu Datacenter offre les avantages suivants pour les locataires :

- Possibilité de définir des règles de pare-feu pour protéger les charges de travail orientées Internet et les charges de travail internes sur les réseaux
- Possibilité de définir des règles de pare-feu pour protéger le trafic entre les machines virtuelles sur le même sous-réseau de couche 2 (L2) et entre les machines virtuelles sur différents sous-réseaux L2
- Possibilité de définir des règles de pare-feu pour protéger et isoler le trafic réseau entre les réseaux locaux de locataire et leurs réseaux virtuels au niveau du fournisseur de services
- Possibilité d'appliquer des stratégies de pare-feu à des réseaux VLAN traditionnels et à des réseaux virtuels basés sur des superpositions

Étapes suivantes

Pour consulter des informations connexes, reportez-vous également à :

- Configurer des groupes de sécurité réseau avec Windows Admin Center
- Configurer des groupes de sécurité réseau avec PowerShell
- SDN dans Azure Local et Windows Server

Dernière mise à jour : 15/09/2026

Qu’est-ce que la passerelle RAS (Remote Access Service) pour la mise en réseau définie par logiciel ?

> S’applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Cet article fournit une vue d’ensemble de la passerelle RAS (Remote Access Service) for Software Defined Networking (SDN) dans Azure Local et Windows Server.

La passerelle RAS est un routeur logiciel prenant en charge le protocole BGP (Border Gateway Protocol) conçu pour les fournisseurs de services Cloud (CSP) et les entreprises qui hébergent des réseaux virtuels multilocataires à l’aide de la virtualisation de réseau Hyper-V (HNV). Vous pouvez utiliser la passerelle RAS pour router le trafic réseau entre un réseau virtuel et un autre réseau, qu’il soit local ou distant.

La passerelle RAS nécessite un contrôleur de réseau, qui effectue le déploiement de pools de passerelles, configure les connexions de locataire sur chaque passerelle et bascule les flux de trafic réseau vers une passerelle de secours en cas d’échec d’une passerelle.

> **Remarque**
>
> Une architecture multilocataire désigne la possibilité pour une infrastructure cloud de prendre en charge les charges de travail des machines virtuelles de plusieurs locataires. Les charges, bien qu’isolées les unes des autres, sont exécutées dans la même infrastructure. Les multiples charges de travail d’un locataire seul peuvent être interconnectées et être gérées à distance mais ces systèmes n’offrent aucune interconnexion avec les charges de travail d’autres locataires et ces derniers ne peuvent pas eux-mêmes les gérer à distance.

Fonctionnalités

La passerelle RAS offre de nombreuses fonctionnalités pour le réseau privé virtuel (VPN), le tunneling, le transfert et le routage dynamique.

VPN IPSec de site à site

Cette fonctionnalité de la passerelle RAS vous permet de connecter deux réseaux à des localisations physiques différentes sur Internet à l'aide d'une connexion de réseau privé virtuel (VPN) de site à site (S2S). Il s'agit d'une connexion chiffrée utilisant le protocole VPN IKEv2.

Pour les fournisseurs de solutions cloud qui hébergent de nombreux locataires dans leur centre de données, la passerelle RAS fournit une solution de passerelle multilocataire qui permet aux locataires d'accéder à leurs ressources et de les gérer via des connexions VPN de site à site à partir de sites distants. La passerelle RAS permet le flux du trafic réseau entre les ressources virtuelles de votre centre de données et leur réseau physique.

Tunnels GRE de site à site

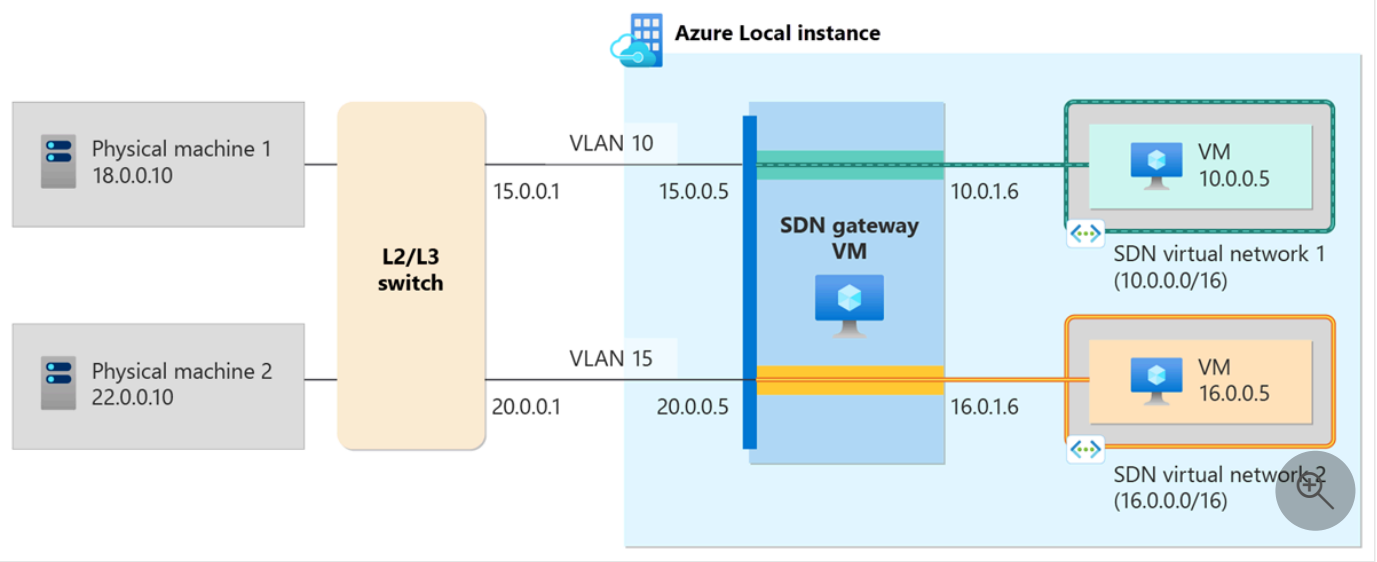
Les tunnels GRE (Generic Routing Encapsulation) permettent la connectivité entre les réseaux virtuels locataires et les réseaux externes. Étant donné que le protocole GRE est léger et que la prise en charge de GRE est disponible sur la plupart des appareils réseau, il s'agit d'un choix idéal pour le tunneling où le chiffrement des données n'est pas nécessaire.

La prise en charge de l'encapsulation GRE dans les tunnels S2S résout le problème de transfert entre les réseaux virtuels locataires et les réseaux externes locataires à l'aide d'une passerelle multilocataire.

Transfert de couche 3

Le transfert de couche 3 (L3) permet la connectivité entre l'infrastructure physique du centre de données et l'infrastructure virtualisée dans le cloud de virtualisation du réseau Hyper-V. En utilisant la connexion de transfert L3, les machines virtuelles réseau client peuvent se connecter à un réseau physique via la passerelle SDN, qui est déjà configurée dans l'environnement SDN. Dans ce cas, la passerelle SDN agit comme un routeur entre le réseau virtualisé et le réseau physique.

Le diagramme suivant montre un exemple de configuration du transfert L3 dans Azure Local configuré avec SDN :



- Il existe deux réseaux virtuels dans l'instance locale Azure : le réseau virtuel SDN 1 avec le préfixe d'adresse 10.0.0.0/16 et le réseau virtuel SDN 2 avec le préfixe d'adresse 16.0.0.0/16.
- Chaque réseau virtuel dispose d'une connexion L3 au réseau physique.
- Étant donné que les connexions L3 concernent différents réseaux virtuels, la passerelle SDN dispose d'un compartiment distinct pour chaque connexion afin de fournir des garanties d'isolation.
- Chaque compartiment de passerelle SDN a une interface dans l'espace réseau virtuel et une interface dans l'espace réseau physique.
- Chaque connexion L3 doit être mappée à un VLAN unique sur le réseau physique. Ce réseau local virtuel doit être différent du VLAN du fournisseur HNV, qui est utilisé comme réseau physique de transfert de données sous-jacent pour le trafic réseau virtualisé.
- Cet exemple utilise le routage statique.

Voici les détails de chaque connexion utilisée dans cet exemple :

Agrandir le tableau

Élément réseau	Connexion 1	Connexion 2
Préfixe de sous-réseau de passerelle	10.0.1.0/24	16.0.1.0/24
Adresse IP L3	15.0.0.5/24	20.0.0.5/24
Adresse IP de l'homologue L3	15.0.0.1	20.0.0.1
Itinéraires sur la connexion	18.0.0.0/24	22.0.0.0/24

Considérations relatives au routage lors de l'utilisation du transfert L3

Pour le routage statique, vous devez configurer un itinéraire sur le réseau physique pour atteindre le réseau virtuel. Par exemple, un itinéraire avec le préfixe d'adresse 10.0.0.0/16 avec le tronçon suivant comme adresse IP L3 de la connexion (15.0.0.5).

Pour le routage dynamique avec BGP, vous devez toujours configurer une route statique /32, car la connexion BGP se trouve entre l'interface interne du compartiment de passerelle et l'adresse IP homologue L3. Pour la connexion 1, le peering est compris entre 10.0.1.6 et 15.0.0.1. Par conséquent, pour cette connexion, vous avez besoin d'un itinéraire statique sur le commutateur physique avec le préfixe de destination 10.0.1.6/32 avec le tronçon suivant comme 15.0.0.5.

Si vous envisagez de déployer des connexions de passerelle L3 avec le routage BGP, veillez à configurer les paramètres BGP du commutateur Top of Rack (ToR) avec les éléments suivants :

- update-source : spécifie l'adresse source des mises à jour BGP, qui est L3 VLAN. Par exemple, VLAN 250.
- ebgp multihop : cela spécifie que d'autres tronçons sont requis, car le voisin BGP est à plus d'un tronçon.

> ⓘ **Remarque**
>
> Lorsque vous utilisez BGP avec une adresse IP homologue L3 dans un sous-réseau différent du routeur BGP, vous devez configurer un itinéraire statique /32 dans la connexion L3. Par exemple, si l'homologue L3 est 15.0.0.1 et que l'homologue BGP est 25.0.0.1, ajoutez un itinéraire avec la destination 25.0.0.1/32 et le tronçon suivant 15.0.0.5 (IP L3).

Routage dynamique avec BGP

Le protocole BGP réduit la nécessité d'une configuration manuelle des itinéraires sur les routeurs, car il s'agit d'un protocole de routage dynamique et apprend automatiquement les itinéraires entre les sites connectés à l'aide de connexions VPN de site à site. Si votre organisation dispose de plusieurs sites connectés à l'aide de routeurs compatibles BGP, tels que la passerelle RAS, BGP permet aux routeurs de calculer et d'utiliser automatiquement des itinéraires valides entre eux en cas d'interruption ou de défaillance du réseau.

Le réflecteur de route BGP inclus dans la passerelle RAS fournit une alternative à la topologie à maillage complet BGP qui est nécessaire pour la synchronisation des routes entre les routeurs. Pour plus d'informations, consultez Qu'est-ce que le réflecteur de route ?.

Fonctionnement de la passerelle RAS

La passerelle RAS route le trafic réseau entre le réseau physique et les ressources du réseau machines virtuelles, quelle que soit la localisation. Vous pouvez router le trafic réseau à la même localisation physique ou à plusieurs localisations différentes.

Vous pouvez déployer la passerelle RAS dans des pools à haute disponibilité qui utilisent plusieurs fonctionnalités à la fois. Les pools de passerelles contiennent plusieurs instances de la passerelle RAS pour offrir la haute disponibilité et le basculement.

Vous pouvez facilement agrandir ou réduire un pool de passerelles en ajoutant ou en supprimant des machines virtuelles dans le pool. La suppression ou l'ajout de passerelles n'interrompt pas les services fournis par un pool. Vous pouvez également ajouter et supprimer des pools de passerelles complets. Pour plus d'informations, consultez Haute disponibilité de la passerelle RAS.

Chaque pool de passerelles fournit une redondance M+N. Cela signifie que « M » machines virtuelles de passerelle actives sont secondées par « N » machines virtuelles de passerelle de secours. La redondance M+N offre une plus grande flexibilité pour déterminer le niveau de fiabilité dont vous avez besoin quand vous déployez la passerelle RAS.

Vous pouvez affecter une adresse IP publique unique à tous les pools ou à une partie des pools. Cela réduit considérablement le nombre d'adresses IP publiques que vous devez utiliser, car il est possible que tous les locataires se connectent au cloud sur une seule adresse IP.

Étapes suivantes

Pour consulter des informations connexes, reportez-vous également à :

- Architecture de déploiement de la passerelle RAS
- Vue d'ensemble du contrôleur de réseau
- Planifier le déploiement du contrôleur de réseau
- SDN dans Azure Local et Windows Server

Dernière mise à jour : 15/09/2026

Architecture de déploiement de la passerelle du serveur d'accès à distance

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI versions 21H2 et 20H2

Vous pouvez utiliser cette rubrique pour en savoir plus sur le déploiement du fournisseur de services cloud (CSP) de la passerelle RAS, notamment les pools de passerelle RAS, les réflecteurs de routage et le déploiement de plusieurs passerelles pour des locataires individuels.

Les sections suivantes fournissent une brève vue d'ensemble de certaines des nouvelles fonctionnalités de la passerelle RAS afin que vous puissiez comprendre comment utiliser ces fonctionnalités dans la conception de votre déploiement de passerelle.

En outre, un exemple de déploiement est fourni, y compris des informations sur le processus d'ajout de nouveaux locataires, la synchronisation des itinéraires et le routage du plan de données, le basculement de passerelle et de réflecteur de routage, et bien plus encore.

Cette rubrique contient les sections suivantes.

- Utilisation de nouvelles fonctionnalités de la passerelle RAS pour concevoir votre déploiement
- Exemple de déploiement
- Ajout de nouveaux locataires et d'espace d'adresse client (CA) Appairage EBGP
- Synchronisation de routage et routage du plan de données
- Comment le contrôleur de réseau répond au basculement de la passerelle RAS et du réflecteur de routage
- Avantages de l'utilisation de nouvelles fonctionnalités de passerelle RAS

Utilisation de nouvelles fonctionnalités de la passerelle RAS pour concevoir votre déploiement

La passerelle RAS inclut plusieurs nouvelles fonctionnalités qui modifient et améliorent la façon dont vous déployez votre infrastructure de passerelle dans votre centre de données.

Réflecteur de routage BGP

La fonction BGP (Border Gateway Protocol) Réflecteur de routage est maintenant incluse dans RAS Gateway, et fournit une alternative à la topologie BGP maillage complet qui est normalement requise pour la synchronisation des routes entre les routeurs. Avec la synchronisation à maillage complet, tous les routeurs BGP doivent se connecter à tous les autres routeurs de la topologie de routage. Toutefois, quand vous utilisez le réflecteur de route, celui-ci est le seul routeur qui se connecte à tous les autres routeurs, appelés clients du réflecteur de route BGP, ce qui simplifie la synchronisation des routes et réduit le trafic réseau. Le réflecteur de route apprend toutes les routes, calcule les meilleures routes et les redistribue à ses clients BGP.

Pour plus d'informations, consultez Nouveautés de la passerelle RAS.

Pools de passerelles

Dans Windows Server 2016, vous pouvez créer de nombreux pools de passerelle de différents types. Les pools de passerelle contiennent de nombreuses instances de passerelle RAS et routent le trafic réseau entre les réseaux physiques et virtuels.

Pour plus d'informations, consultez Nouveautés de la passerelle RAS et la Haute disponibilité de la passerelle RAS.

Scalabilité du pool de passerelle

Vous pouvez facilement effectuer un scale-up ou un scale-down d'un pool de passerelles en ajoutant ou en supprimant des machines virtuelles de passerelle dans le pool. La suppression ou l'ajout de passerelles n'interrompt pas les services fournis par un pool. Vous pouvez également ajouter et supprimer des pools de passerelles complets.

Pour plus d'informations, consultez Nouveautés de la passerelle RAS et la Haute disponibilité de la passerelle RAS.

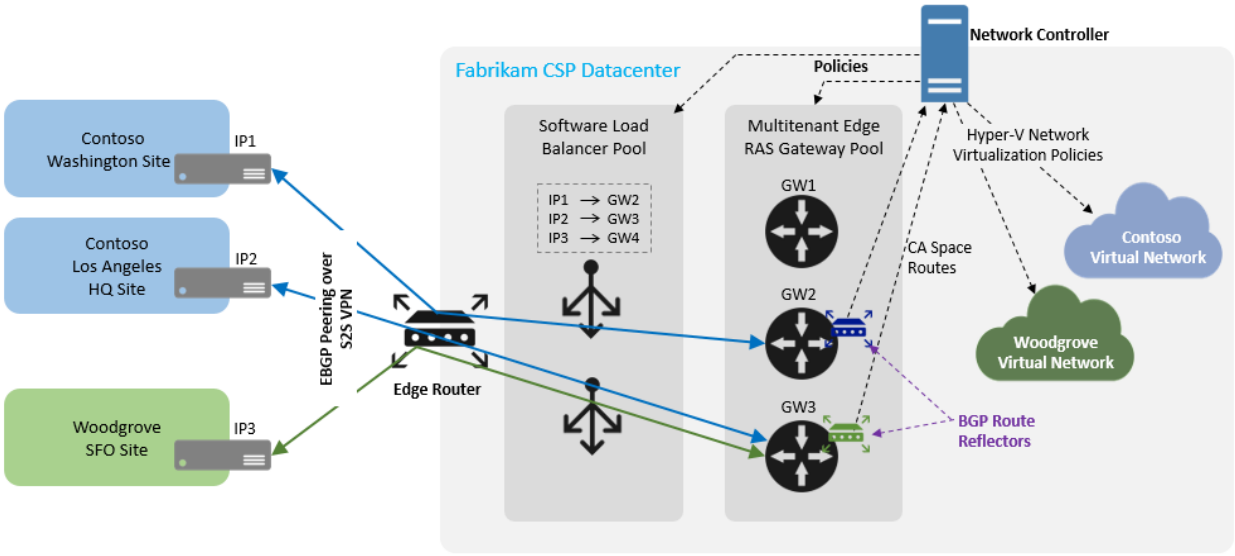
Redondance du pool de passerelles M+N

Chaque pool de passerelles est redondant M+N. Cela signifie qu'un nombre « M » de machines virtuelles de passerelle actives sont secondées par un nombre « N » de machines virtuelles de passerelle de secours. La redondance M+N offre une plus grande flexibilité pour déterminer le niveau de fiabilité dont vous avez besoin quand vous déployez la passerelle RAS.

Pour plus d'informations, consultez Nouveautés de la passerelle RAS et la Haute disponibilité de la passerelle RAS.

Exemple de déploiement

L'illustration suivante fournit un exemple de peering eBGP sur des connexions VPN de site à site configurées entre deux locataires, Contoso et Woodgrove, et le centre de données CSP Fabrikam.



Dans cet exemple, Contoso a besoin d'une bande passante de passerelle supplémentaire, ce qui conduit à la décision de conception de l'infrastructure de passerelle de mettre fin au site Contoso Los Angeles sur GW3 au lieu de GW2. Pour cette raison, les connexions VPN Contoso à partir de différents sites se terminent dans le centre de données CSP sur deux passerelles différentes.

Ces deux passerelles, GW2 et GW3, étaient les premières passerelles RAS configurées par le contrôleur de réseau lorsque le fournisseur de solutions cloud a ajouté les locataires Contoso et Woodgrove à son infrastructure. Pour cette raison, ces deux passerelles sont configurées en tant que réflecteurs de routage pour ces clients (ou locataires) correspondants. GW2 est le réflecteur de routage Contoso et GW3 est le réflecteur de route Woodgrove, en plus d'être le point d'arrêt de la passerelle RAS CSP pour la connexion VPN avec le site QG de Contoso Los Angeles.

> **Notes**
>
> Une passerelle RAS peut acheminer le trafic réseau virtuel et physique pour jusqu'à cent locataires différents, en fonction des besoins en bande passante de chaque locataire.

En tant que réflecteurs de routage, GW2 envoie des itinéraires d'espace d'autorité de certification Contoso au contrôleur de réseau, et GW3 envoie des itinéraires d'espace d'autorité de certification Woodgrove au contrôleur de réseau.

Le contrôleur de réseau envoie les stratégies de virtualisation de réseau Hyper-V aux réseaux virtuels Contoso et Woodgrove, ainsi que les stratégies RAS aux passerelles RAS et les stratégies d'équilibrage de charge aux multiplexeurs (MUX) configurés en tant que pool d'équilibrage de charge logiciel.

Ajout de nouveaux locataires et d'espace d'adresse client (CA) Appairage eBGP

Lorsque vous signez un nouveau client et ajoutez le client en tant que nouveau locataire dans votre centre de données, vous pouvez utiliser le processus suivant, dont une grande partie est effectuée automatiquement par les routeurs eBGP du contrôleur de réseau et de la passerelle RAS.

1. Approvisionnez un nouveau réseau virtuel et des charges de travail en fonction des besoins de votre locataire.

2. Si nécessaire, configurez la connectivité à distance entre le site d'entreprise du locataire distant et son réseau virtuel au niveau de votre centre de données. Lorsque vous déployez une connexion VPN de site à site pour le locataire, le contrôleur de réseau sélectionne automatiquement une machine virtuelle de passerelle RAS disponible dans le pool de passerelles disponible et configure la connexion.

3. Lors de la configuration de la machine virtuelle de passerelle RAS pour le nouveau locataire, le contrôleur de réseau configure également la passerelle RAS en tant que routeur BGP et la désigne comme réflecteur de routage pour le locataire. Cela est vrai même dans les cas où la passerelle RAS sert de passerelle ou de réflecteur de passerelle et de routage pour d'autres locataires.

4. Selon que le routage de l'espace d'autorité de certification est configuré pour utiliser des réseaux configurés de manière statique ou un routage BGP dynamique,

le contrôleur de réseau configure les itinéraires statiques correspondants, les voisins BGP ou les deux sur la machine virtuelle de passerelle RAS et le réflecteur de routage.

> ⓘ **Notes**
>
> - Une fois que le contrôleur de réseau a configuré une passerelle RAS et un réflecteur de routage pour le locataire, chaque fois que le même locataire a besoin d'une nouvelle connexion VPN de site à site, le contrôleur de réseau vérifie la capacité disponible sur cette machine virtuelle de passerelle RAS. Si la passerelle d'origine peut traiter la capacité requise, la nouvelle connexion réseau est également configurée sur la même machine virtuelle de passerelle RAS. Si la machine virtuelle de passerelle RAS ne peut pas gérer une capacité supplémentaire, le contrôleur de réseau sélectionne une nouvelle machine virtuelle de passerelle RAS disponible et configure la nouvelle connexion sur celle-ci. Cette nouvelle machine virtuelle de passerelle RAS associée au locataire devient le client Réflecteur de route du client d'origine RAS Gateway Réflecteur de routage.
>
> - Étant donné que les pools de passerelle RAS sont derrière les équilibreurs de charge logiciels (SLB), les adresses VPN de site à site des locataires utilisent chacune une seule adresse IP publique, appelée adresse IP virtuelle (VIP), qui est traduite par les SLB en une adresse IP interne au centre de données, appelée adresse IP dynamique (DIP), pour une passerelle RAS qui achemine le trafic pour le locataire Entreprise. Ce mappage d'adresses IP publiques à privées par SLB garantit que les tunnels VPN de site à site sont correctement établis entre les sites d'entreprise et les passerelles CSP RAS et les réflecteurs de routage.
>
> Pour plus d'informations sur l'équilibrage de charge SLB, les adresses IP virtuelles et les adresses IP virtuelles, consultez **L'équilibrage de charge logicielle (SLB) pour SDN**.

5. Une fois que le tunnel VPN de site à site entre le site d'entreprise et la passerelle RAS du centre de données CSP est établi pour le nouveau locataire, les itinéraires statiques associés aux tunnels sont automatiquement provisionnés sur les côtés Entreprise et CSP du tunnel.

6. Avec le routage BGP de l'espace d'autorité de certification, le peering eBGP entre les sites d'entreprise et le réflecteur de routage de passerelle RAS CSP est également établi.

Routage de la synchronisation et du plan de données

Une fois le peering eBGP établi entre les sites d'entreprise et le réflecteur de routage de passerelle CSP RAS, le réflecteur de route apprend toutes les routes d'entreprise à l'aide du routage BGP dynamique. Le réflecteur de routage synchronise ces itinéraires entre tous les clients du réflecteur de routage afin qu'ils soient tous configurés avec le même ensemble d'itinéraires.

Le réflecteur de routage met également à jour ces itinéraires consolidés, à l'aide de la synchronisation des itinéraires, vers le contrôleur de réseau. Le contrôleur de réseau traduit ensuite les itinéraires en stratégies de virtualisation de réseau Hyper-V et configure le réseau fabric pour s'assurer que le routage des chemins de données de bout en bout est approvisionné. Ce processus rend le réseau virtuel du locataire accessible à partir des sites d'entreprise du locataire.

Pour le routage du plan de données, les paquets qui atteignent les machines virtuelles de passerelle RAS sont directement acheminés vers le réseau virtuel du locataire, car les itinéraires requis sont désormais disponibles avec toutes les machines virtuelles de passerelle RAS participantes.

De même, une fois les stratégies de virtualisation de réseau Hyper-V en place, le réseau virtuel locataire achemine les paquets directement vers les machines virtuelles de passerelle RAS (sans avoir besoin de connaître le réflecteur de routage), puis vers les sites d'entreprise via les tunnels VPN de site à site.

Par ailleurs : Le retour du trafic du réseau virtuel du locataire vers le site d'entreprise du locataire distant contourne les SLB, un processus appelé Retour direct du serveur (DSR).

Comment le contrôleur de réseau répond à la passerelle RAS et au basculement du réflecteur de routage

Voici deux scénarios de basculement possibles : l'un pour les clients de réflecteurs de routage de passerelle RAS et l'autre pour les réflecteurs de routage de passerelle RAS, y

compris des informations sur la façon dont le contrôleur de réseau gère le basculement pour les machines virtuelles dans l'une ou l'autre configuration.

Échec de machine virtuelle d'un client de réflecteur de routage BGP de passerelle RAS

Le contrôleur de réseau effectue les actions suivantes lorsqu'un client de réflecteur de routage de passerelle RAS échoue.

> ⓘ **Notes**
>
> Lorsqu'une passerelle RAS n'est pas un réflecteur de routage pour l'infrastructure BGP d'un locataire, il s'agit d'un client réflecteur de routage dans l'infrastructure BGP du locataire.

- Le contrôleur de réseau sélectionne une machine virtuelle de passerelle RAS de secours disponible et approvisionne la nouvelle machine virtuelle de passerelle RAS avec la configuration de la machine virtuelle de passerelle RAS ayant échoué.
- Le contrôleur de réseau met à jour la configuration SLB correspondante pour s'assurer que les tunnels VPN de site à site des sites locataires vers la passerelle RAS ayant échoué sont correctement établis avec la nouvelle passerelle RAS.
- Le contrôleur de réseau configure le client BGP Réflecteur de routage sur la nouvelle passerelle.
- Le contrôleur de réseau configure le nouveau client de réflecteur de routage BGP de passerelle RAS comme actif. La passerelle RAS démarre immédiatement le peering avec le réflecteur de routage du locataire pour partager des informations de routage et activer le peering eBGP pour le site d'entreprise correspondant.

Échec de machine virtuelle pour un réflecteur de routage BGP de passerelle RAS

Le contrôleur de réseau effectue les actions suivantes lorsqu'un réflecteur de routage BGP de passerelle RAS échoue.

- Le contrôleur de réseau sélectionne une machine virtuelle de passerelle RAS de secours disponible et approvisionne la nouvelle machine virtuelle de passerelle RAS avec la configuration de la machine virtuelle de passerelle RAS ayant échoué.

- Le contrôleur de réseau configure le réflecteur de routage sur la nouvelle machine virtuelle de passerelle RAS et affecte à la nouvelle machine virtuelle la même adresse IP que celle utilisée par la machine virtuelle défaillante, fournissant ainsi l'intégrité de la route malgré l'échec de la machine virtuelle.
- Le contrôleur de réseau met à jour la configuration SLB correspondante pour s'assurer que les tunnels VPN de site à site des sites locataires vers la passerelle RAS ayant échoué sont correctement établis avec la nouvelle passerelle RAS.
- Le contrôleur de réseau configure la nouvelle machine virtuelle de réflecteur de routage BGP de passerelle RAS en tant que machine virtuelle active.
- Le réflecteur de routage devient immédiatement actif. Le tunnel VPN de site à site vers l'entreprise est établi, et le réflecteur de routage utilise le peering eBGP et échange des itinéraires avec les routeurs de site d'entreprise.
- Après la sélection de l'itinéraire BGP, le réflecteur de routage BGP de la passerelle RAS met à jour les clients de réflecteur de routage du locataire dans le centre de données et synchronise les itinéraires avec le contrôleur de réseau, ce qui rend le chemin des données de bout en bout disponible pour le trafic client.

Avantages de l'utilisation de nouvelles fonctionnalités de passerelle RAS

Voici quelques-uns des avantages de l'utilisation de ces nouvelles fonctionnalités de passerelle RAS lors de la conception de votre déploiement de passerelle RAS.

Extensibilité de la passerelle RAS

Étant donné que vous pouvez ajouter autant de machines virtuelles de passerelle RAS que nécessaire aux pools de passerelle RAS, vous pouvez facilement mettre à l'échelle votre déploiement de passerelle RAS pour optimiser les performances et la capacité. Lorsque vous ajoutez des machines virtuelles à un pool, vous pouvez configurer ces passerelles RAS avec des connexions VPN de site à site de tout type (IKEv2, L3, GRE), éliminant ainsi les goulots d'étranglement de la capacité sans temps d'arrêt.

Gestion simplifiée de la passerelle de site d'entreprise

Lorsque votre locataire a plusieurs sites d'entreprise, le locataire peut configurer tous les sites avec une adresse IP VPN de site à site distante et une seule adresse IP de voisin distante : l'adresse IP de votre centre de données CSP RAS Gateway BGP Réflecteur de routage pour ce locataire. Cela simplifie la gestion de la passerelle pour vos locataires.

Correction rapide de l’échec de passerelle

Pour garantir une réponse de basculement rapide, vous pouvez configurer le temps du paramètre BGP Keepalive entre les itinéraires de périphérie et le routeur de contrôle sur un intervalle de temps court, par exemple inférieur ou égal à dix secondes. Avec ce court intervalle de maintien en vie, si un routeur de périphérie BGP de passerelle RAS échoue, l’échec est rapidement détecté et le contrôleur de réseau suit les étapes fournies dans les sections précédentes. Cet avantage peut réduire la nécessité d’un protocole de détection des défaillances distinct, tel que le protocole BFD (Bidirectional Forwarding Detection).

Haute disponibilité de la passerelle du serveur d'accès à distance

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI versions 21H2 et 20H2

Vous pouvez utiliser cette rubrique pour en savoir plus sur les configurations de haute disponibilité pour la passerelle mutualisée RAS pour la mise en réseau à définition logicielle (SDN).

Cette rubrique contient les sections suivantes.

- Vue d'ensemble de la passerelle RAS
- Vue d'ensemble des pools de passerelles
- Vue d'ensemble du déploiement de la passerelle RAS
- Intégration de la passerelle RAS au contrôleur de réseau

Vue d'ensemble de la passerelle RAS

Si votre organisation est un fournisseur de services cloud (CSP) ou une entreprise avec plusieurs locataires, vous pouvez déployer la passerelle RAS en mode multilocataire pour fournir le routage du trafic réseau à destination et en provenance de réseaux virtuels et physiques, y compris Internet.

Vous pouvez déployer la passerelle RAS en mode multilocataire en tant que passerelle de périphérie pour acheminer le trafic réseau client vers les ressources et réseaux virtuels du locataire.

Lorsque vous déployez plusieurs instances de machines virtuelles de passerelle RAS qui fournissent une haute disponibilité et un basculement, vous déployez un pool de passerelles. Dans Windows Server 2012 R2, toutes les machines virtuelles de passerelle formaient un pool unique, ce qui rendait une séparation logique du déploiement de la passerelle un peu difficile. Windows Server 2012 passerelle R2 offrait un déploiement de redondance 1:1 pour les machines virtuelles de passerelle, ce qui a entraîné une sous-utilisation de la capacité disponible pour les connexions VPN de site à site (S2S).

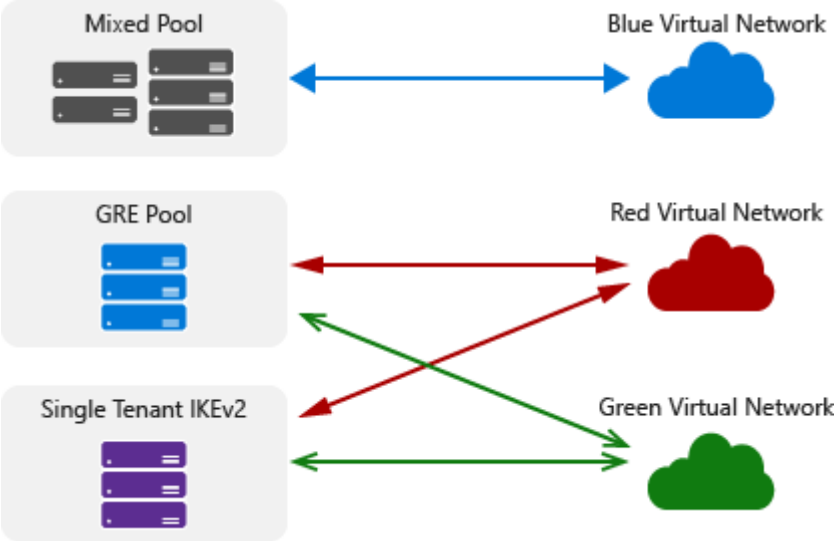
Ce problème est résolu dans Windows Server 2016, qui fournit plusieurs pools de passerelles, qui peuvent être de types différents pour la séparation logique. Le nouveau mode de redondance M+N permet une configuration de basculement plus efficace.

Pour plus d'informations sur la passerelle RAS, consultez Passerelle RAS.

Vue d'ensemble des pools de passerelles

Dans Windows Server 2016, vous pouvez déployer des passerelles dans un ou plusieurs pools.

L'illustration suivante montre différents types de pools de passerelles qui fournissent le routage du trafic entre les réseaux virtuels.



Chaque pool possède les propriétés suivantes.

- Chaque pool est redondant M+N. Cela signifie qu'un nombre « M » de machines virtuelles de passerelle actives sont secondées par un nombre « N » de machines virtuelles de passerelle de secours. La valeur de N (passerelles de secours) est toujours inférieure ou égale à M (passerelles actives).

- Un pool peut effectuer l'une des fonctions de passerelle individuelles - Internet Key Exchange version 2 (IKEv2) S2S, Couche 3 (L3) et GRE (Generic Routing Encapsulation) - ou le pool peut effectuer toutes ces fonctions.

- Vous pouvez affecter une adresse IP publique unique à tous les pools ou à une partie des pools. Cela réduit considérablement le nombre d'adresses IP publiques que vous devez utiliser, car vous pouvez ainsi obliger tous les locataires à se connecter au cloud sur une seule adresse IP. La section ci-dessous sur la haute disponibilité et l'équilibrage de charge décrit comment cela fonctionne.

- Vous pouvez facilement effectuer un scale-up ou un scale-down d'un pool de passerelles en ajoutant ou en supprimant des machines virtuelles de passerelle dans le pool. La suppression ou l'ajout de passerelles n'interrompt pas les services fournis par un pool. Vous pouvez également ajouter et supprimer des pools de passerelles complets.

- Les connexions d'un seul locataire peuvent se terminer sur plusieurs pools et plusieurs passerelles dans un pool. Toutefois, si un client a des connexions qui se terminent dans un pool de passerelles **Tous**, il ne peut pas s'abonner à d'autres pools de passerelles **Tous** ou de type individuel.

Les pools de passerelles offrent également la flexibilité nécessaire pour activer des scénarios supplémentaires :

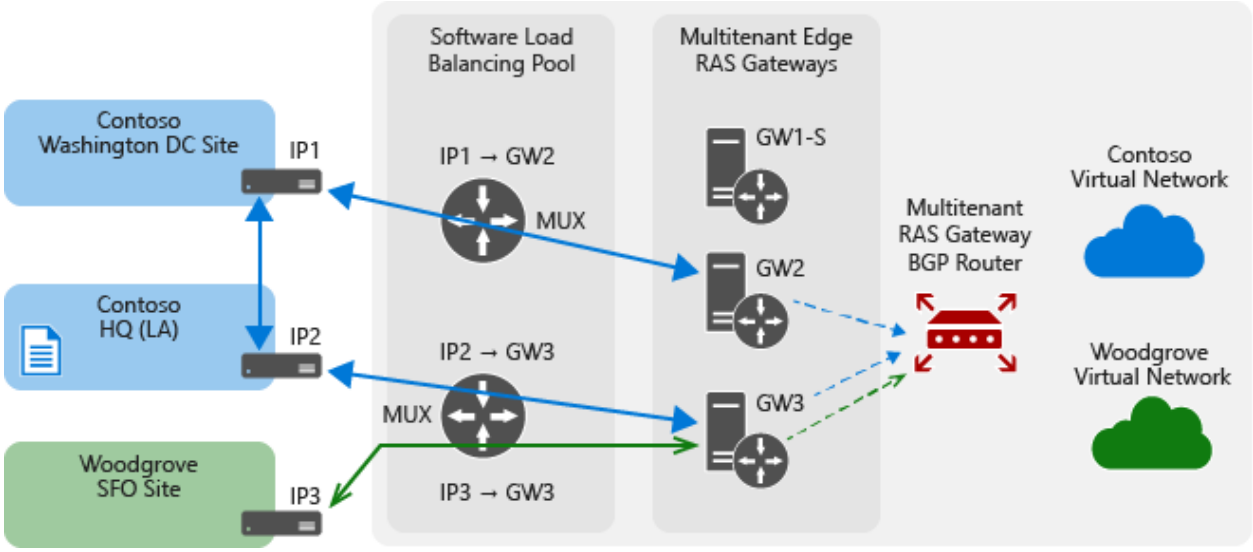
- Pools à locataire unique : vous pouvez créer un pool à utiliser par un locataire.

- Si vous vendez des services cloud par le biais de canaux partenaires (revendeurs), vous pouvez créer des ensembles distincts de pools pour chaque revendeur.

- Plusieurs pools peuvent fournir la même fonction de passerelle, mais des capacités différentes. Par exemple, vous pouvez créer un pool de passerelles qui prend en charge à la fois les connexions S2S IKEv2 à haut débit et à faible débit.

Vue d'ensemble du déploiement de la passerelle RAS

L'illustration suivante illustre un déploiement de fournisseur de services cloud (CSP) classique de la passerelle RAS.



Avec ce type de déploiement, les pools de passerelles sont déployés derrière un software Load Balancer (SLB), ce qui permet au fournisseur de services cloud d'attribuer une seule adresse IP publique pour l'ensemble du déploiement. Plusieurs connexions de passerelle d'un locataire peuvent se terminer sur plusieurs pools de passerelles, ainsi que sur plusieurs passerelles au sein d'un pool. Cela est illustré par les connexions IKEv2 S2S dans le diagramme ci-dessus, mais la même chose s'applique également à d'autres fonctions de passerelle, telles que les passerelles L3 et GRE.

Dans l'illustration, l'appareil MT BGP est une passerelle multilocataire RAS avec BGP. Le protocole BGP multilocataire est utilisé pour le routage dynamique. Le routage d'un locataire est centralisé : un point unique, appelé réflecteur de routage (RR), gère le peering BGP pour tous les sites de locataire. Le RR lui-même est distribué sur toutes les passerelles d'un pool. Il en résulte une configuration où les connexions d'un locataire (chemin de données) se terminent sur plusieurs passerelles, mais la RR du locataire (point d'homologation BGP - chemin de contrôle) se trouve sur une seule des passerelles.

Le routeur BGP est séparé dans le diagramme pour représenter ce concept de routage centralisé. L'implémentation BGP de la passerelle fournit également le routage de transit, ce qui permet au cloud d'agir en tant que point de transit pour le routage entre deux sites clients. Ces fonctionnalités BGP s'appliquent à toutes les fonctions de passerelle.

Intégration de la passerelle RAS avec le contrôleur de réseau

La passerelle RAS est entièrement intégrée au contrôleur de réseau dans Windows Server 2016. Lorsque la passerelle RAS et le contrôleur de réseau sont déployés, le contrôleur de réseau effectue les fonctions suivantes.

- Déploiement des pools de passerelles
- Configuration des connexions de locataire sur chaque passerelle
- Basculement des flux de trafic réseau vers une passerelle de secours en cas de défaillance de la passerelle

Les sections suivantes fournissent des informations détaillées sur la passerelle RAS et le contrôleur de réseau.

- Provisionnement et équilibrage de charge des connexions de passerelle (IKEv2, L3 et GRE)

- Haute disponibilité pour IKEv2 S2S
- Haute disponibilité pour GRE
- Haute disponibilité pour les passerelles de transfert L3

Provisionnement et équilibrage de charge des connexions de passerelle (IKEv2, L3 et GRE)

Lorsqu'un locataire demande une connexion de passerelle, la demande est envoyée au contrôleur de réseau. Le contrôleur de réseau est configuré avec des informations sur tous les pools de passerelles, y compris la capacité de chaque pool et de chaque passerelle dans chaque pool. Le contrôleur de réseau sélectionne le pool et la passerelle appropriés pour la connexion. Cette sélection est basée sur la bande passante requise pour la connexion. Le contrôleur de réseau utilise un algorithme « best fit » pour sélectionner efficacement les connexions dans un pool. Le point d'homologation BGP pour la connexion est également désigné à ce stade s'il s'agit de la première connexion du locataire.

Une fois que le contrôleur de réseau a sélectionné une passerelle RAS pour la connexion, le contrôleur de réseau provisionne la configuration nécessaire pour la connexion sur la passerelle. Si la connexion est une connexion IKEv2 S2S, le contrôleur de réseau provisionne également une règle NAT (Network Address Translation) sur le pool SLB ; cette règle NAT sur le pool SLB dirige les demandes de connexion du locataire vers la passerelle désignée. Les locataires sont différenciés par l'adresse IP source, qui est censée être unique.

> ⓘ **Notes**
>
> Les connexions L3 et GRE contournent l'équilibrage de charge SLB et se connectent directement à la passerelle RAS désignée. Ces connexions nécessitent que le routeur de point de terminaison distant (ou tout autre appareil tiers) soit correctement configuré pour se connecter à la passerelle RAS.

Si le routage BGP est activé pour la connexion, l'homologation BGP est lancée par la passerelle RAS et les itinéraires sont échangés entre les passerelles locales et cloud. Les itinéraires appris par le protocole BGP (ou configurés de manière statique si le protocole BGP n'est pas utilisé) sont envoyés au contrôleur de réseau. Le contrôleur de réseau transmet ensuite les itinéraires aux hôtes Hyper-V sur lesquels les machines virtuelles clientes sont installées. À ce stade, le trafic client peut être routé vers le site local approprié. Le contrôleur de réseau crée également des stratégies de virtualisation de

réseau Hyper-V associées qui spécifient des emplacements de passerelle et les répartit vers les hôtes Hyper-V.

Haute disponibilité pour IKEv2 S2S

Une passerelle RAS dans un pool se compose à la fois de connexions et d'homologation BGP de différents locataires. Chaque pool a des passerelles actives « M » et des passerelles de secours « N ».

Le contrôleur de réseau gère la défaillance des passerelles de la manière suivante.

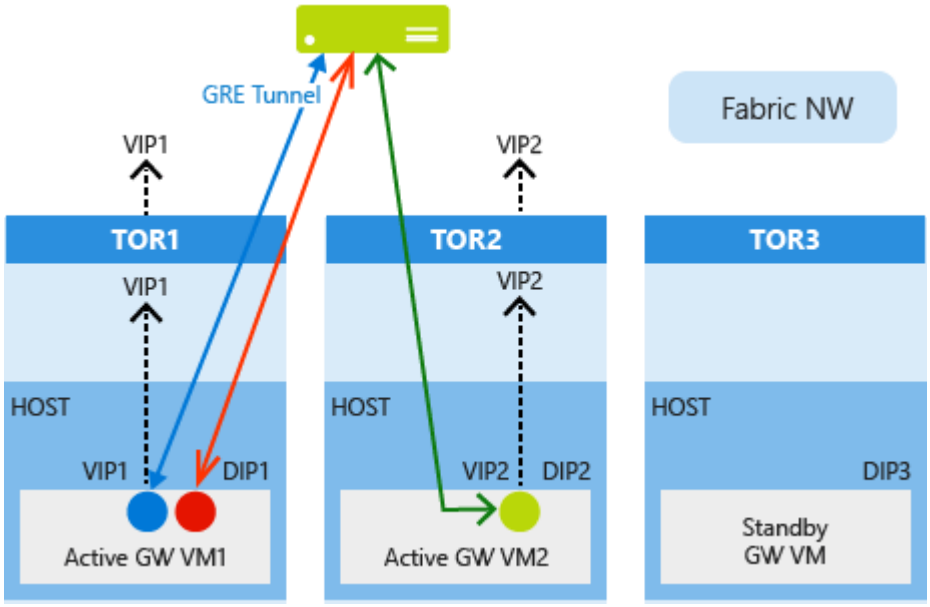
- Le contrôleur de réseau effectue constamment un test ping sur les passerelles dans tous les pools et peut détecter une passerelle qui a échoué ou en cours d'échec. Le contrôleur de réseau peut détecter les types suivants d'échecs de passerelle RAS.
  - Échec de la machine virtuelle de la passerelle RAS
  - Défaillance de l'hôte Hyper-V sur lequel la passerelle RAS s'exécute
  - Échec du service de passerelle RAS

  Le contrôleur de réseau stocke la configuration de toutes les passerelles actives déployées. La configuration se compose de paramètres de connexion et de paramètres de routage.
- En cas d'échec d'une passerelle, cela a un impact sur les connexions de locataire sur la passerelle, ainsi que sur les connexions de locataire qui se trouvent sur d'autres passerelles, mais dont la RR réside sur la passerelle ayant échoué. Le temps d'arrêt des dernières connexions est inférieur à la première. Lorsque le contrôleur de réseau détecte une passerelle défaillante, il effectue les tâches suivantes.
  - Supprime les routes des connexions impactées des hôtes de calcul.
  - Supprime les stratégies de virtualisation de réseau Hyper-V sur ces hôtes.
  - Sélectionne une passerelle de secours, la convertit en passerelle active et configure la passerelle.
  - Modifie les mappages NAT sur le pool SLB pour pointer les connexions vers la nouvelle passerelle.
- Simultanément, à mesure que la configuration se produit sur la nouvelle passerelle active, les connexions S2S IKEv2 et l'homologation BGP sont rétablis. Les connexions et l'homologation BGP peuvent être lancés par la passerelle cloud ou la

passerelle locale. Les passerelles actualisent leurs itinéraires et les envoient au contrôleur de réseau. Une fois que le contrôleur de réseau a appris les nouveaux itinéraires découverts par les passerelles, le contrôleur de réseau envoie les itinéraires et les stratégies de virtualisation de réseau Hyper-V associées aux hôtes Hyper-V où résident les machines virtuelles des locataires affectés par une défaillance. Cette activité du contrôleur de réseau est similaire à la situation d'une nouvelle configuration de connexion, mais elle se produit à une plus grande échelle.

Haute disponibilité pour GRE

Le processus de réponse de basculement de la passerelle RAS par le contrôleur de réseau , y compris la détection des défaillances, la copie de la configuration de la connexion et du routage vers la passerelle de secours, le basculement du routage BGP/statique des connexions impactées (y compris le retrait et le réacheminement des routes sur les hôtes de calcul et la ré-homologation BGP) et la reconfiguration des stratégies de virtualisation de réseau Hyper-V sur les hôtes de calcul, est le même pour les passerelles et connexions GRE. Toutefois, le rétablissement des connexions GRE se produit différemment, et la solution de haute disponibilité pour GRE présente certaines exigences supplémentaires.



Au moment du déploiement de la passerelle, une adresse IP dynamique (DIP) est attribuée à chaque machine virtuelle de passerelle RAS. En outre, chaque machine virtuelle de passerelle se voit également attribuer une adresse IP virtuelle (VIP) pour la haute disponibilité GRE. Les adresses IP virtuelles sont affectées uniquement aux passerelles dans les pools qui peuvent accepter des connexions GRE, et non aux pools non GRE. Les adresses IP virtuelles affectées sont publiées sur les commutateurs TOR (top of rack) à l'aide de BGP, qui publie ensuite les adresses IP virtuelles dans le réseau

physique cloud. Cela rend les passerelles accessibles à partir des routeurs distants ou des appareils tiers où réside l'autre extrémité de la connexion GRE. Cette homologation BGP est différente de l'homologation BGP au niveau du locataire pour l'échange d'itinéraires de locataire.

Au moment de l'approvisionnement de la connexion GRE, le contrôleur de réseau sélectionne une passerelle, configure un point de terminaison GRE sur la passerelle sélectionnée et retourne l'adresse IP virtuelle de la passerelle affectée. Cette adresse IP virtuelle est ensuite configurée comme adresse de tunnel GRE de destination sur le routeur distant.

En cas de défaillance d'une passerelle, le contrôleur de réseau copie l'adresse IP virtuelle de la passerelle ayant échoué et d'autres données de configuration vers la passerelle de secours. Lorsque la passerelle de secours devient active, elle publie l'adresse IP virtuelle sur son commutateur TOR et plus loin dans le réseau physique. Les routeurs distants continuent de connecter les tunnels GRE à la même adresse IP virtuelle et l'infrastructure de routage garantit que les paquets sont acheminés vers la nouvelle passerelle active.

Haute disponibilité pour les passerelles de transfert L3

Une Virtualisation de réseau Hyper-V L3 agit comme un pont entre l'infrastructure physique du centre de données et l'infrastructure virtualisée dans le cloud de virtualisation de réseau Hyper-V. Sur une passerelle de transfert L3 multilocataire, chaque locataire utilise son propre réseau logique balisé VLAN pour la connectivité avec le réseau physique du locataire.

Lorsqu'un nouveau locataire crée une passerelle L3, la passerelle du contrôleur de réseau Service Manager sélectionne une machine virtuelle de passerelle disponible et configure une nouvelle interface de locataire avec une adresse IP d'espace d'adresse client (CA) hautement disponible (à partir du réseau logique étiqueté VLAN du locataire). L'adresse IP est utilisée comme adresse IP homologue sur la passerelle distante (réseau physique) et est le tronçon suivant pour atteindre le réseau de virtualisation de réseau Hyper-V du locataire.

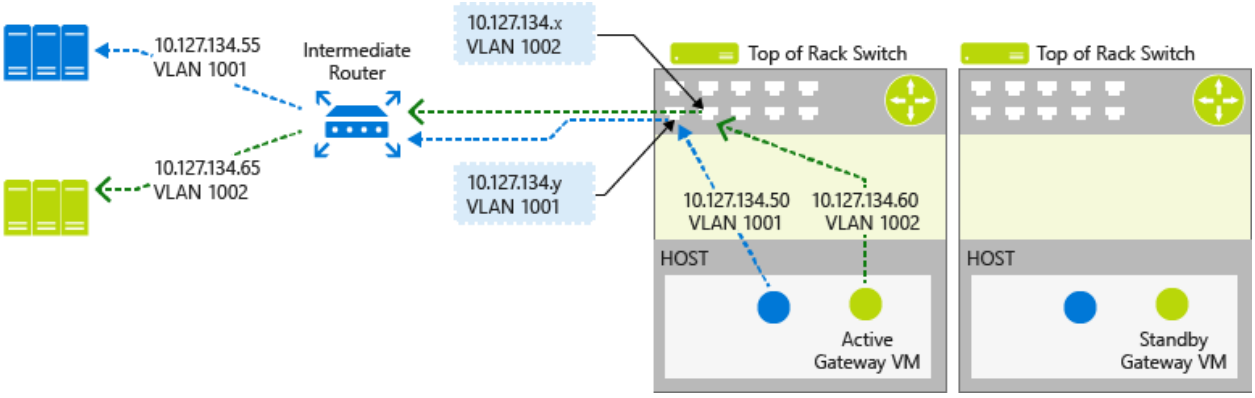
Contrairement aux connexions réseau IPsec ou GRE, le commutateur TOR n'apprend pas dynamiquement le réseau VLAN du locataire. Le routage du réseau balisé VLAN du locataire doit être configuré sur le commutateur TOR et tous les commutateurs et routeurs intermédiaires entre l'infrastructure physique et la passerelle pour garantir une connectivité de bout en bout. Voici un exemple de configuration Réseau virtuel CSP, comme illustré dans l'illustration ci-dessous.

Réseau	Subnet	ID du réseau local virtuel	Passerelle par défaut
Réseau logique Contoso L3	10.127.134.0/24	1001	10.127.134.1
Réseau logique Woodgrove L3	10.127.134.0/24	1002	10.127.134.1

Voici des exemples de configurations de passerelle de locataire, comme illustré dans l'illustration ci-dessous.

Nom du locataire	Adresse IP de la passerelle L3	ID du réseau local virtuel	Adresse IP du pair
Contoso	10.127.134.50	1001	10.127.134.55
Woodgrove	10.127.134.60	1002	10.127.134.65

Voici l'illustration de ces configurations dans un centre de données CSP.



Les défaillances de passerelle, la détection des défaillances et le processus de basculement de passerelle dans le contexte d'une passerelle de transfert L3 sont similaires aux processus pour les passerelles RAS IKEv2 et GRE. Les différences concernent la façon dont les adresses IP externes sont gérées.

Lorsque l'état de la machine virtuelle de la passerelle devient défectueux, le contrôleur de réseau sélectionne l'une des passerelles de secours dans le pool et approvisionne à nouveau les connexions réseau et le routage sur la passerelle de secours. Lors du déplacement des connexions, l'adresse IP de l'espace d'autorité de certification hautement disponible de la passerelle de transfert L3 est également déplacée vers la nouvelle machine virtuelle de passerelle avec l'adresse IP BGP de l'espace d'autorité de certification du locataire.

Étant donné que l'adresse IP de peering L3 est déplacée vers la nouvelle machine virtuelle de passerelle pendant le basculement, l'infrastructure physique distante est à nouveau en mesure de se connecter à cette adresse IP et, par la suite, d'atteindre la

charge de travail Virtualisation de réseau Hyper-V. Pour le routage dynamique BGP, à mesure que l'adresse IP BGP de l'espace d'autorité de certification est déplacée vers la nouvelle machine virtuelle de passerelle, le routeur BGP distant peut rétablir le peering et apprendre à nouveau tous les itinéraires de virtualisation de réseau Hyper-V.

Notes

Vous devez configurer séparément les commutateurs TOR et tous les routeurs intermédiaires afin d'utiliser le réseau logique balisé VLAN pour la communication du locataire. En outre, le basculement L3 est limité aux racks configurés de cette façon. Pour cette raison, le pool de passerelles L3 doit être configuré avec soin et la configuration manuelle doit être effectuée séparément.

Qu’est-ce que l’équilibreur de charge logiciel (SLB) pour le SDN ?

> S’applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Les fournisseurs de services cloud (CSP) et les entreprises qui déploient un SDN (Software-Defined Networking) peuvent utiliser un équilibreur de charge logiciel (SLB) pour distribuer uniformément le trafic réseau des locataires et clients de locataires entre des ressources de réseau virtuel. L’équilibrage de charge logicielle (SLB) permet à plusieurs serveurs d’héberger une même charge de travail, ce qui assure une disponibilité et une scalabilité de haut niveau.

Un équilibreur de charge logiciel peut fournir une périphérie unifiée mutualisée en s’intégrant avec des technologies SDN telles qu’une passerelle de serveur d’accès à distance, un pare-feu de centre de données et un réflecteur d’itinéraire.

> **Remarque**
>
> L’architecture mutualisée pour les réseaux locaux virtuels n’est pas prise en charge par le contrôleur de réseau. En revanche, vous pouvez utiliser des VLAN avec un SLB pour des charges de travail gérées par le fournisseur de services, telles que l’infrastructure d’un centre de données et des serveurs web haute densité.

À l’aide d’un équilibreur de charge logiciel, vous pouvez effectuer un scale-out de vos capacités d’équilibrage de charge en utilisant des machines virtuelles SLB sur les serveurs de calcul Hyper-V que vous utilisez pour vos autres charges de travail de machine virtuelle. Ainsi, un équilibreur de charge logiciel prend en charge la création et la suppression rapides de points de terminaison d’équilibrage de charge, comme l’exigent les opérations de CSP. En outre, Software Load Balancer prend en charge des dizaines de gigaoctets par système, fournit un modèle d’approvisionnement simple et est facile à effectuer un scale-out et à un scale-in.

Pour savoir comment gérer les stratégies d’équilibreur de charge logiciel à l’aide de Windows Admin Center, consultez Gérer l’équilibreur de charge logiciel pour SDN.

Qu’est-ce qu’inclut l’équilibreur de charge logiciel ?

L'équilibreur de charge logiciel comprend les fonctionnalités suivantes :

- Services d'équilibrage de charge de couche 4 (L4) pour le trafic TCP/UDP nord/sud et est/ouest
- Équilibrage de la charge du trafic réseau public et du trafic réseau interne
- Prise en charge des adresses IP dynamiques sur des réseaux locaux virtuels (VLAN) et sur des réseaux virtuels que vous créez à l'aide de la virtualisation de réseau Hyper-V
- Prise en charge des sondes d'intégrité
- Compatibilité avec la mise à l'échelle dans le cloud, notamment les capacités de scale-out et de scale-up pour les multiplexeurs et les agents hôtes.

Pour plus d'informations, consultez Fonctionnalités de l'équilibreur de charge logiciel dans cet article.

Fonctionnement d'un équilibreur de charge logiciel

Un équilibreur de charge logiciel mappe des adresses IP virtuelles à des adresses IP dynamiques qui font partie d'un ensemble de ressources de service cloud dans le centre de données.

Les adresses IP virtuelles sont des adresses IP uniques qui fournissent un accès public à un pool de machines virtuelles à charge équilibrée. Par exemple, les adresses IP virtuelles sont des adresses IP qui sont exposées sur Internet afin que les locataires et les clients des locataires puissent se connecter aux ressources de locataire dans le centre de données cloud.

Les adresses IP dynamiques sont les adresses IP des machines virtuelles membres d'un pool à charge équilibrée situé derrière l'adresse IP virtuelle. Les adresses IP dynamiques sont affectées dans l'infrastructure cloud aux ressources de locataire.

Les adresses IP virtuelles sont situées dans le multiplexeur (MUX) SLB. Le multiplexeur est constitué d'une ou de plusieurs machines virtuelles. Le contrôleur de réseau fournit chaque adresse IP virtuelle à chaque multiplexeur, et chaque multiplexeur utilise à son tour BGP (Border Gateway Protocol) pour publier chaque adresse IP virtuelle sur les routeurs du réseau physique en tant que route /32. Avec BGP, les routeurs de réseau physique peuvent :

- Découvrir qu'une adresse IP virtuelle est disponible sur chaque multiplexeur, même si les multiplexeurs se trouvent sur des sous-réseaux différents d'un réseau de couche 3

- Répartir la charge de chaque adresse IP virtuelle sur l'ensemble des multiplexeurs disponibles à l'aide du routage ECMP (Equal Cost Multi-Path)
- Détecter automatiquement la suppression ou la défaillance d'un multiplexeur et arrêter d'envoyer du trafic vers ce dernier
- Répartir la charge du multiplexeur défaillant ou supprimé entre les multiplexeurs sains

Lorsque le trafic public arrive à partir d'Internet, l'expérience utilisateur MUX SLB examine le trafic, qui contient l'adresse IP virtuelle comme destination, et mappe et réécrit le trafic afin qu'il arrive à un DIP individuel. Pour le trafic réseau entrant, cette transaction est effectuée au cours d'un processus en deux étapes qui est réparti entre les machines virtuelles de multiplexeur et l'hôte Hyper-V dans lequel se trouve l'adresse IP dynamique de destination :

1. Équilibrage de charge : le multiplexeur utilise l'adresse IP virtuelle pour sélectionner une adresse IP dynamique, encapsule le paquet et transfère le trafic vers l'hôte Hyper-V où se trouve l'adresse IP dynamique.
2. Traduction d'adresses réseau (NAT) : l'hôte Hyper-V supprime l'encapsulation du paquet, convertit l'adresse IP virtuelle en adresse IP dynamique, remappe les ports et transfère le paquet à la machine virtuelle détenant l'adresse IP dynamique.

Le multiplexeur sait comment mapper les adresses IP virtuelles en adresses IP dynamiques correctes grâce aux stratégies d'équilibrage de charge que vous définissez à l'aide du contrôleur de réseau. Ces règles incluent le protocole, le port front-end, le port back-end et l'algorithme de distribution (5, 3 ou 2 tuples).

La NAT étant exécutée par l'hôte Hyper-V, quand les machines virtuelles de locataire répondent et envoient le trafic réseau sortant vers Internet ou des localisations de locataire distantes, le trafic contourne le multiplexeur et passe directement au routeur de périphérie à partir de l'hôte Hyper-V. Ce processus de contournement du multiplexeur est appelé « retour direct du serveur » (DSR).

Une fois établi le flux de trafic réseau initial, le trafic réseau entrant contourne complètement le multiplexeur SLB.

Dans l'illustration suivante, un ordinateur client exécute une requête DNS pour l'adresse IP d'un site SharePoint d'entreprise, en l'occurrence, une société fictive nommée Contoso. Le processus suivant se produit :

1. Le serveur DNS retourne l'adresse IP virtuelle 107.105.47.60 au client.

2. Le client envoie une requête HTTP à l'adresse IP virtuelle.

3. Le réseau physique dispose de plusieurs chemins pour atteindre l'adresse IP virtuelle située sur n'importe quel multiplexeur. Chaque routeur franchi utilise ECMP pour choisir le segment suivant du chemin jusqu'à ce que la demande atteigne un multiplexeur.

4. Le multiplexeur qui reçoit la demande vérifie les stratégies configurées et constate qu'il y a deux adresses IP dynamiques disponibles, 10.10.10.5 et 10.10.20.5, sur un réseau virtuel pour communiquer la demande à l'adresse IP virtuelle107.105.47.60

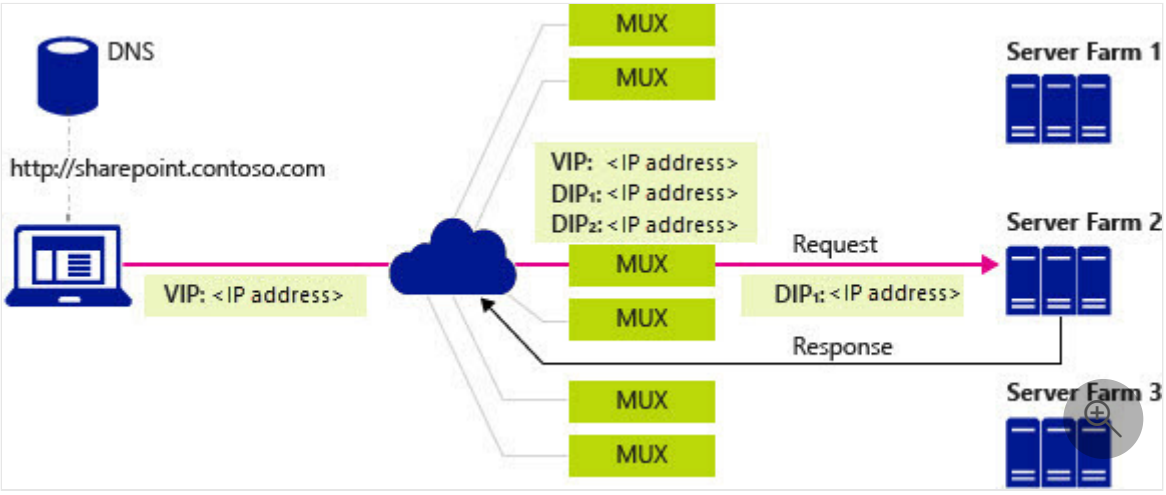
5. Le multiplexeur sélectionne l'adresse IP dynamique 10.10.10.5 et encapsule les paquets à l'aide de la technologie VXLAN afin qu'il puisse les envoyer à l'hôte contenant l'adresse IP dynamique par le biais de l'adresse réseau physique de l'hôte.

6. L'hôte reçoit le paquet encapsulé et l'inspecte. Il supprime l'encapsulation et réécrit le paquet afin que la destination soit à présent l'adresse IP dynamique 10.10.10.5 à la place de l'adresse IP virtuelle, puis envoie le trafic à la machine virtuelle détenant l'adresse IP dynamique.

7. La demande atteint le site SharePoint de Contoso dans la batterie de serveurs 2. Le serveur génère une réponse et l'envoie au client, en utilisant sa propre adresse IP comme source.

8. L'hôte intercepte le paquet sortant dans le commutateur virtuel, qui se souvient que le client, maintenant la destination, a fait la demande d'origine à l'adresse IP virtuelle. L'hôte réécrit la source du paquet pour être l'adresse IP virtuelle afin que le client ne voit pas l'adresse DIP.

9. L'hôte transfère le paquet directement à la passerelle par défaut du réseau physique qui utilise sa table de routage standard pour transférer le paquet au client, qui reçoit finalement la réponse.



Équilibrage de charge du trafic interne du centre de données

Lors de l'équilibrage de charge du trafic réseau interne au centre de données, par exemple entre des ressources de locataire qui s'exécutent sur des serveurs différents et qui sont membres du même réseau virtuel, le commutateur virtuel Hyper-V auquel les machines virtuelles sont connectées exécute la NAT.

Avec l'équilibrage de charge du trafic interne, la première demande est envoyée au multiplexeur et traitée par celui-ci, qui sélectionne l'adresse IP dynamique appropriée, vers laquelle il route le trafic. À partir de là, le flux de trafic établi contourne le multiplexeur et passe directement d'une machine virtuelle à l'autre.

Sondes d'intégrité

Software Load Balancer inclut les sondes d'intégrité suivantes pour valider l'intégrité de l'infrastructure réseau :

- Sonde TCP vers le port
- Sonde HTTP vers le port et l'URL

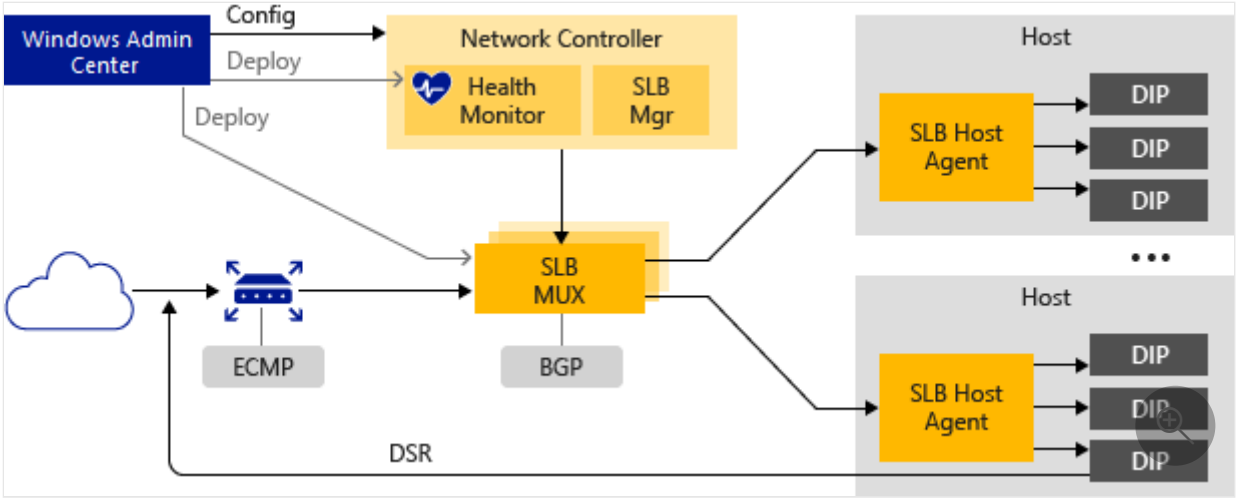
Contrairement à une appliance d'équilibrage de charge classique dans laquelle la sonde va de l'appliance à l'adresse IP dynamique, la sonde SLB part de l'hôte où se trouve l'adresse IP dynamique et va directement de l'agent hôte SLB à l'adresse IP dynamique, répartissant davantage le travail entre les hôtes.

Infrastructure de l'équilibreur de charge logiciel

Avant de pouvoir configurer l'équilibreur de charge logiciel, vous devez déployer un contrôleur de réseau et une ou plusieurs machines virtuelles de multiplexeur SLB.

En outre, vous devez configurer les hôtes locaux Azure avec le commutateur virtuel Hyper-V compatible SDN et vous assurer que l'agent hôte SLB est en cours d'exécution. Les routeurs qui desservent les hôtes doivent prendre en charge le routage ECMP et le protocole BGP (Border Gateway Protocol) et doivent être configurés pour accepter les demandes de peering BGP provenant des multiplexeurs SLB.

La figure suivante fournit une vue d'ensemble de l'infrastructure SLB.



Les sections suivantes fournissent des informations supplémentaires sur ces éléments de l'infrastructure de l'équilibreur de charge logiciel.

Contrôleur réseau

Le contrôleur de réseau héberge le gestionnaire SLB et effectue les actions suivantes pour l'équilibreur de charge logiciel :

- Il traite les commandes SLB qui arrivent via l'API Northbound en provenance de Windows Admin Center, de System Center, de Windows PowerShell ou d'une autre application de gestion de réseau.
- Calcule la stratégie de distribution vers des hôtes locaux Azure et des muX SLB.
- Il indique l'état d'intégrité de l'infrastructure de l'équilibreur de charge logiciel.

Vous pouvez utiliser Windows Admin Center ou Windows PowerShell pour installer et configurer le contrôleur de réseau ou une autre infrastructure SLB.

Multiplexeur SLB

Le multiplexeur SLB traite le trafic réseau entrant et mappe les adresses IP virtuelles aux adresses IP dynamiques, puis transfère le trafic à l'adresse IP dynamique appropriée. Chaque multiplexeur utilise également le protocole BGP pour publier les routes d'adresses IP virtuelles sur les routeurs de périphérie. BGP Keep Alive avertit les MUX lorsqu'un MUX échoue, ce qui permet aux MUX actifs de redistribuer la charge en cas d'échec d'un MUX. Elle constitue l'essentiel de l'équilibrage de charge assuré par les équilibreurs de charge.

Agent hôte SLB

Quand vous déployez l'équilibreur de charge logiciel, vous devez utiliser Windows Admin Center, System Center, Windows PowerShell ou une autre application de gestion pour déployer l'agent hôte SLB sur chaque serveur hôte.

L'agent hôte SLB écoute les mises à jour de stratégie SLB à partir du contrôleur de réseau. L'agent hôte programme aussi les règles d'équilibrage de charge logiciel dans les commutateurs virtuels Hyper-V compatible SDN qui sont configurés sur l'ordinateur local.

Commutateur virtuel Hyper-V compatible SDN

Pour qu'un commutateur virtuel soit compatible avec l'équilibreur de charge logiciel, l'extension VFP (Virtual Filtering Platform) doit être activée sur le commutateur virtuel. Cette opération est effectuée automatiquement par les scripts PowerShell de déploiement SDN, l'Assistant Déploiement de Windows Admin Center et le déploiement de System Center Virtual Machine Manager (SCVMM).

Pour plus d'informations sur l'activation de l'extension VFP sur des commutateurs virtuels, consultez les commandes Windows PowerShell Get-VMSystemSwitchExtension et Enable-VMSwitchExtension.

Le commutateur virtuel Hyper-V compatible SDN effectue les actions suivantes pour l'équilibreur de charge logiciel :

- Il traite le chemin de données pour l'équilibreur de charge logiciel.
- Il reçoit le trafic réseau entrant provenant du multiplexeur.
- Il contourne le multiplexeur pour le trafic réseau sortant, qu'il envoie au routeur en utilisant le processus DSR.

Routeur BGP

Le routeur BGP effectue les actions suivantes pour l'équilibreur de charge logiciel :

- Il route le trafic entrant vers le multiplexeur en utilisant la technologie ECMP.
- Pour le trafic réseau sortant, il utilise la route fournie par l'hôte.
- Il écoute les mises à jour des routes pour les adresses IP virtuelles à partir du multiplexeur SLB.
- Il supprime les multiplexeurs SLB de la rotation SLB si Keep Alive échoue.

Fonctionnalités de l’équilibreur de charge logiciel

Les sections suivantes décrivent certaines des fonctionnalités de l’équilibreur de charge logiciel.

Fonctionnalité de base

- L’équilibreur de charge logiciel fournit des services d’équilibrage de charge de couche 4 (L4) pour le trafic TCP/UDP nord/sud et est/ouest.
- Vous pouvez utiliser l’équilibreur de charge logiciel sur un réseau basé sur la virtualisation de réseau Hyper-V.
- Vous pouvez utiliser SLB avec un réseau local virtuel pour les machines virtuelles DIP connectées à un commutateur virtuel Hyper-V activé par SDN.
- Une instance SLB peut gérer plusieurs locataires.
- L’équilibreur de charge logiciel et les adresses IP dynamiques prennent en charge un chemin de retour scalable et à faible latence, tel qu’implémenté par le processus DSR.
- Fonctions SLB lorsque vous utilisez également Switch Embedded Teaming (SET) ou une virtualisation d’entrée/sortie racine unique (SR-IOV).
- L’équilibreur de charge logiciel prend en charge les protocoles Internet versions 6 (IPv6) et 4 (IPv4).
- Pour les scénarios de passerelle de site à site, l’équilibreur de charge logiciel fournit des fonctionnalités NAT afin de permettre à toutes les connexions de site à site d’utiliser une seule adresse IP publique.

Scalabilité et performances

- Compatibilité avec la mise à l’échelle dans le cloud, notamment les capacités de scale-out et de scale-up pour les multiplexeurs et les agents hôtes.
- Un module actif du contrôleur de réseau hébergeant le gestionnaire SLB peut prendre en charge huit instances de multiplexeur.

Haute disponibilité

- Vous pouvez déployer l’équilibreur de charge logiciel sur plus de deux nœuds dans une configuration actif/actif.

- Vous pouvez ajouter et supprimer des multiplexeurs dans le pool de multiplexeurs sans affecter le service SLB. La disponibilité de l'équilibreur de charge logiciel est ainsi assurée quand un correctif est appliqué à des multiplexeurs individuels.
- Les instances de multiplexeur individuelles ont une durée de bon fonctionnement de 99 %.
- Les données de supervision de l'intégrité sont disponibles pour les entités de gestion.

Étapes suivantes

Pour consulter des informations connexes, reportez-vous également à :

- Gérer l'équilibreur de charge logiciel pour SDN
- SDN dans Azure Local et Windows Server

Dernière mise à jour : 15/09/2026

Qu’est-ce que SDN Multisite ?

> S'applique à Windows Server 2025

Cet article fournit une vue d’ensemble de SDN Multisite, y compris ses avantages et ses limitations actuelles. Vous pouvez l’utiliser comme guide pour vous aider à concevoir votre topologie réseau et votre plan de récupération d’urgence.

SDN Multisite vous permet d’étendre les fonctionnalités du SDN traditionnel déployé à différents emplacements physiques. SDN Multisite permet une connectivité native de couche 2 et de couche 3 entre différents emplacements physiques pour les charges de travail virtualisées. Dans cet article, toutes les références aux sites signifient des emplacements physiques.

Pour plus d’informations sur la gestion de SDN Multisite, consultez Gérer SDN Multisite pour Azure Local.

Avantages

Voici les avantages de l’utilisation de SDN Multisite :

- **Système de gestion des stratégies unifié.** Avec les réseaux virtuels partagés et les configurations de stratégie, vous pouvez gérer et configurer vos réseaux multisite à partir de n’importe quel site.
- **Migration transparente de la charge de travail.** Migrez en toute transparence les charges de travail entre les sites physiques sans avoir à reconfigurer les adresses IP ou les groupes de sécurité réseau (NSG).
- **Accessibilité automatique aux nouvelles machines virtuelles.** Obtenez une accessibilité automatique aux machines virtuelles nouvellement créées sur des réseaux virtuels, ainsi qu'une gestion automatisée de tous leurs groupes de sécurité réseau associés, sur vos emplacements physiques.

Limites

La fonctionnalité multisite SDN présente actuellement quelques limitations :

- La prise en charge n'est possible qu'entre deux sites.
- Les sites doivent être connectés via un réseau privé, car la prise en charge du chiffrement pour les sites connectés via Internet n’est pas fournie.

- L’équilibrage de charge interne n’est pas pris en charge entre sites.
- Le déploiement et la gestion multisite avec un SDN natif, également appelé contrôleur de réseau sur le cluster de basculement, n'est pris en charge que via PowerShell.

Peering multisite

Le multisite nécessite un peering entre les différents sites, qui s'effectue comme un appairage de réseaux virtuels. Une connexion est automatiquement lancée sur les deux sites via Windows Admin Center. Lorsqu’une connexion est établie, le peering est réussi. Pour obtenir des instructions sur l’établissement d’un peering, consultez Établir un peering.

Les sections suivantes décrivent les rôles de chaque site dans un environnement multisite et la façon dont les ressources sont gérées et synchronisées entre les sites.

Rôles de site principal et secondaire

Dans un environnement SDN multisite, un site est désigné comme principal et l’autre comme secondaire. Le site principal gère la synchronisation des ressources. Pendant le peering multisite, le site principal est automatiquement sélectionné, que vous pouvez modifier ultérieurement à l’aide de Windows Admin Center.

Gestion des ressources

- Si le site principal est inaccessible, les ressources globales et les ressources nécessitant une validation globale ou des allocations d’adresses client globales ne peuvent pas être mises à jour via le site secondaire. Toutefois, d’autres ressources locales peuvent être mises à jour via le site secondaire.

  Voici quelques exemples de ressources nécessitant une validation globale :
  - Pools MAC.
  - Pool réseau/IP logique.

  Voici quelques exemples d’allocations d’autorité de certification globales :
  - Équilibrage de charge interne pour le sous-réseau virtuel. Actuellement, cela n’est pas pris en charge par le biais de Multisite.
  - Connexions de passerelle pour le sous-réseau virtuel.

- Si le site secondaire est inaccessible, les ressources peuvent être mises à jour via le site principal. Toutefois, le site secondaire peut avoir des ressources obsolètes jusqu’à ce que la connectivité soit restaurée. Une fois la connectivité restaurée, la synchronisation reprend.

- Si le site principal tombe en panne, vous pouvez désigner votre site secondaire comme nouveau site principal pour effectuer des mises à jour de vos groupes de sécurité réseau et réseaux virtuels. Toutefois, toute synchronisation de données en attente à partir de l'ancien site principal est perdue. Pour résoudre ce problème, appliquez ces mêmes modifications sur le nouveau site principal une fois que l'ancien site principal est de nouveau en ligne. Toutefois, il peut également entraîner des conflits d'allocation d'autorité de certification globaux.

Synchronisation des ressources

Lorsque vous activez SDN Multisite, toutes les ressources de chaque site ne sont pas synchronisées sur tous les sites. Voici les listes de ressources qui sont synchronisées et qui restent non synchronisées.

- **Ressources synchronisées**

  Ces ressources sont synchronisées sur tous les sites suite à l'établissement du peering. Vous pouvez mettre à jour ces ressources à partir de n'importe quel site, qu'elle soit primaire ou secondaire. Toutefois, le site principal est chargé de s'assurer que ces ressources sont appliquées et synchronisées entre les sites. Les instructions et les instructions relatives à la gestion de ces ressources restent les mêmes que dans un environnement SDN à site unique.
  - Réseaux virtuels. Pour obtenir des instructions sur la gestion des réseaux virtuels, consultez Gérer les réseaux virtuels de locataire. Notez que les réseaux logiques ne sont pas synchronisés entre les sites. Toutefois, si vos réseaux virtuels référencent un réseau logique, le réseau logique portant le même nom doit exister sur les deux sites.
  - Groupes de sécurité réseau (NSG) . Pour obtenir des instructions sur la configuration du groupe de sécurité réseau avec Windows Admin Center et PowerShell, consultez Configurer des groupes de sécurité réseau avec Windows Admin Center et configurer des groupes de sécurité réseau avec PowerShell.
  - Routage défini par l'utilisateur. Pour obtenir des instructions sur l'utilisation du routage défini par l'utilisateur, consultez Utiliser des appliances virtuelles réseau sur un réseau virtuel.

- **Ressources non synchronisées**

  Ces ressources ne sont pas synchronisées après l'établissement du peering :
  - Stratégies d'équilibrage de charge.
  - Adresses IP virtuelles.
  - Stratégies de passerelle.

- Réseaux logiques. Bien que les réseaux logiques ne soient pas synchronisés entre les sites, il est vérifié que les pools IP ne se chevauchent pas, et un tel chevauchement n'est pas autorisé.

Ces stratégies sont créées sur le site local et, si vous souhaitez les mêmes stratégies sur l'autre site, vous devez les créer manuellement. Si vos machines virtuelles principales pour les stratégies d'équilibrage de charge se trouvent sur un site unique, la connectivité via SLB fonctionne correctement sans aucune configuration supplémentaire. Toutefois, si vous attendez que les machines virtuelles de back-end passent d'un site à l'autre, par défaut, la connectivité fonctionne uniquement s'il existe des machines virtuelles de back-end derrière une adresse IP virtuelle sur le site local. Si toutes les machines virtuelles de back-end se déplacent vers un autre site, la connectivité via cette adresse IP virtuelle échoue.

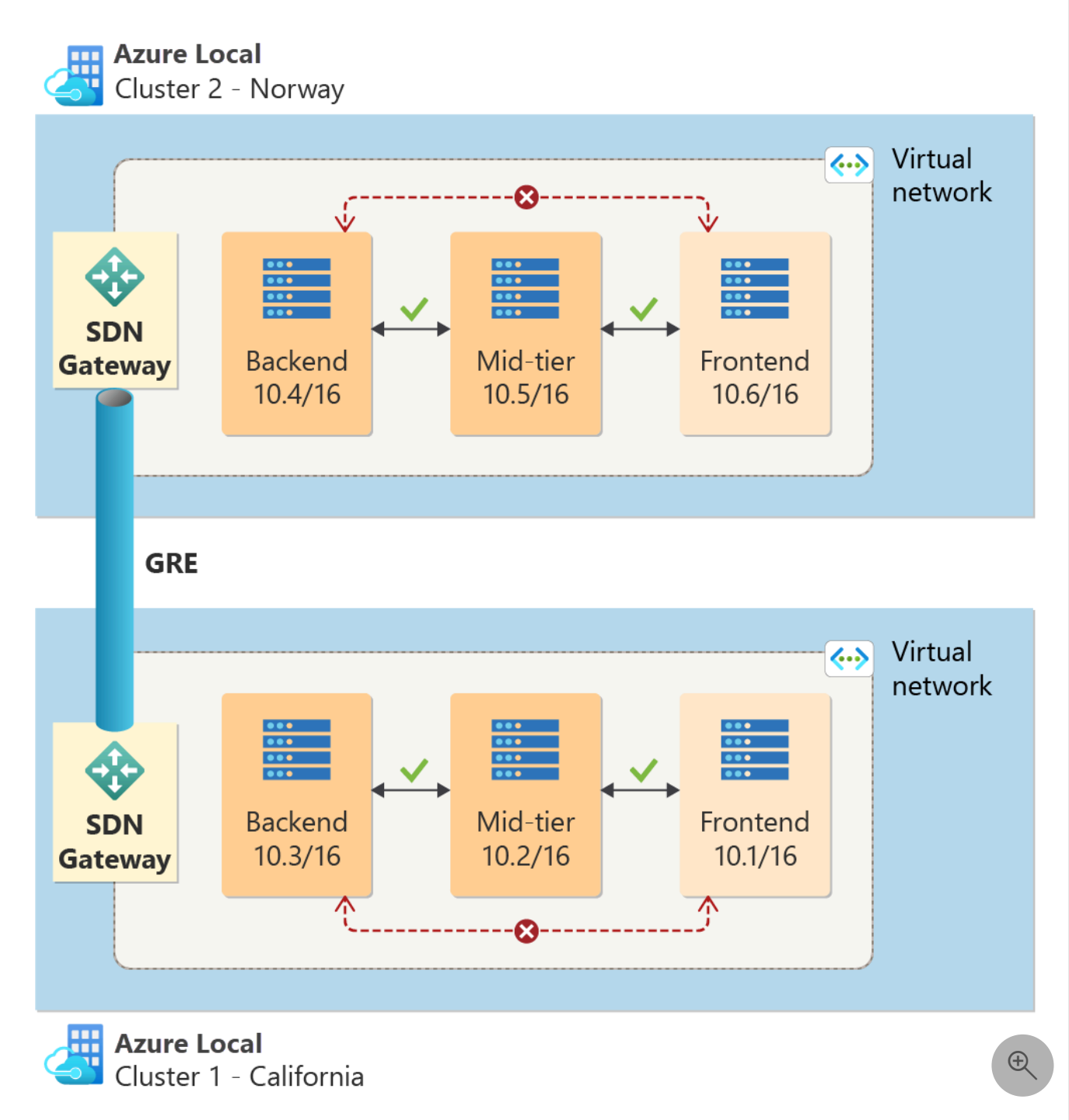
Flux de trafic est-ouest et partage de sous-réseau

Multisite permet aux machines virtuelles sur différents sites avec le SDN déployé de communiquer sur le même sous-réseau sans avoir à configurer les connexions de passerelle SDN. Cela simplifie la topologie réseau et réduit le besoin de machines virtuelles et de sous-réseaux supplémentaires. Le chemin des données entre les machines virtuelles sur différents sites s'appuie sur l'infrastructure physique sous-jacente.

Les scénarios suivants comparent la façon dont la communication de machine virtuelle est établie entre deux sites physiques dans une configuration SDN traditionnelle et dans une configuration multisite SDN.

Communication de machine virtuelle à machine virtuelle sans SDN multisite

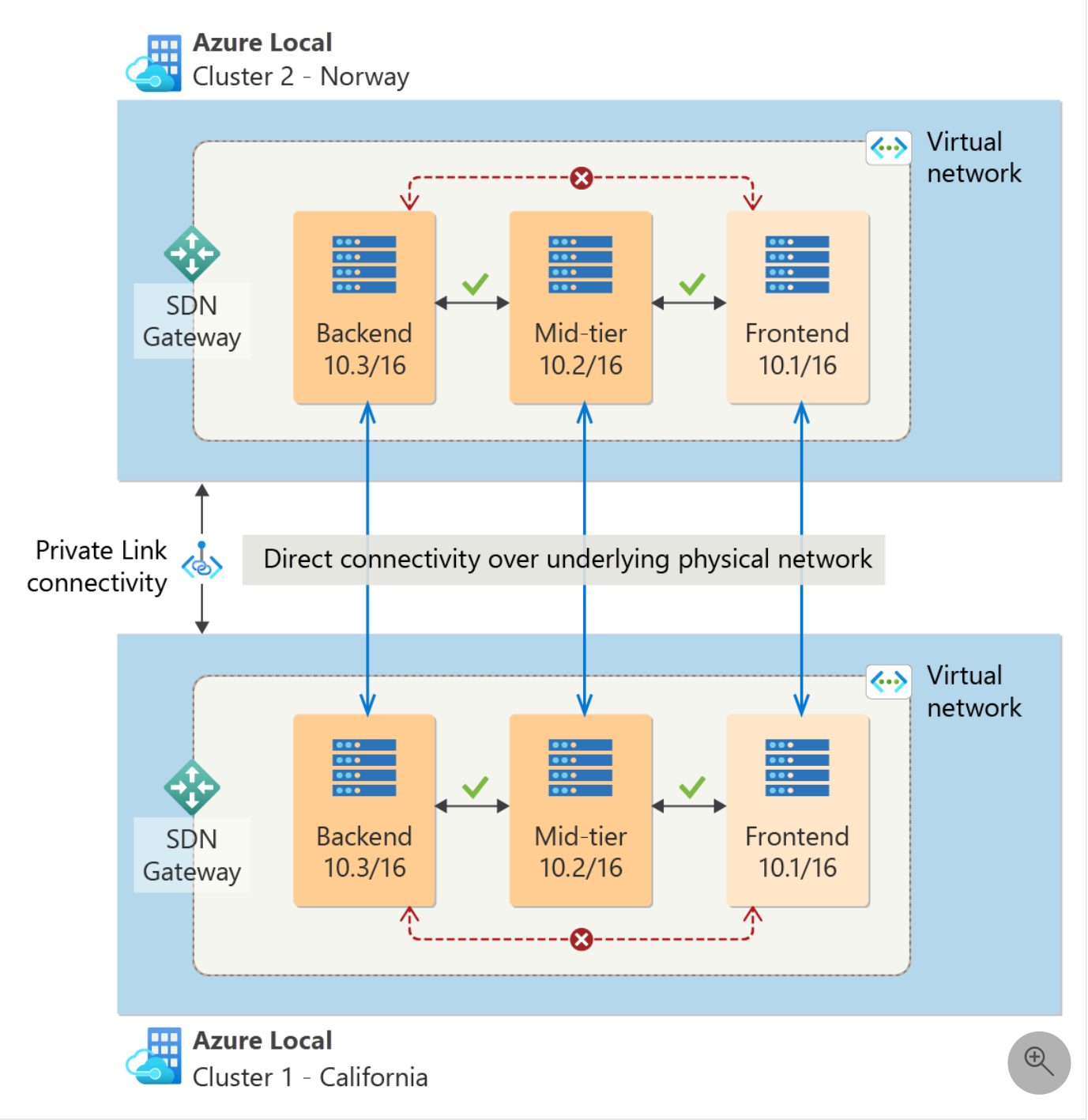
Dans une configuration traditionnelle avec SDN déployé sur deux sites physiques, vous devez établir une connexion de passerelle L3 ou GRE pour la communication intersite. Vous devez également fournir davantage de sous-réseaux pour vos applications. Par exemple, si chaque site héberge des applications frontales, vous allouez des plages de sous-réseaux distinctes comme 10.1/16 et 10.6/16. En outre, lorsque vous configurez une connexion de passerelle, vous devez également allouer davantage de machines virtuelles pour vos machines virtuelles de passerelle et les gérer par la suite.



Communication de machine virtuelle à machine virtuelle avec SDN Multisite

Avec SDN Multisite sur deux emplacements physiques, vous pouvez disposer d'une connectivité de couche 2 native pour la communication intersite. Cela vous permet d'avoir une plage de sous-réseaux unique pour vos applications qui s'étendent sur les deux emplacements, ce qui élimine la nécessité de configurer la connexion de passerelle SDN. Par exemple, comme illustré dans le diagramme suivant, les applications frontales sur les deux emplacements peuvent utiliser le même sous-réseau, tel que 10.1/16, au lieu de conserver deux éléments distincts. Avec cette configuration, le flux de données d'une machine virtuelle à une autre s'appuie uniquement sur

votre infrastructure physique sous-jacente, ce qui évite de devoir parcourir une autre machine virtuelle de passerelle SDN.



Équilibreurs de charge logiciels et leurs limitations

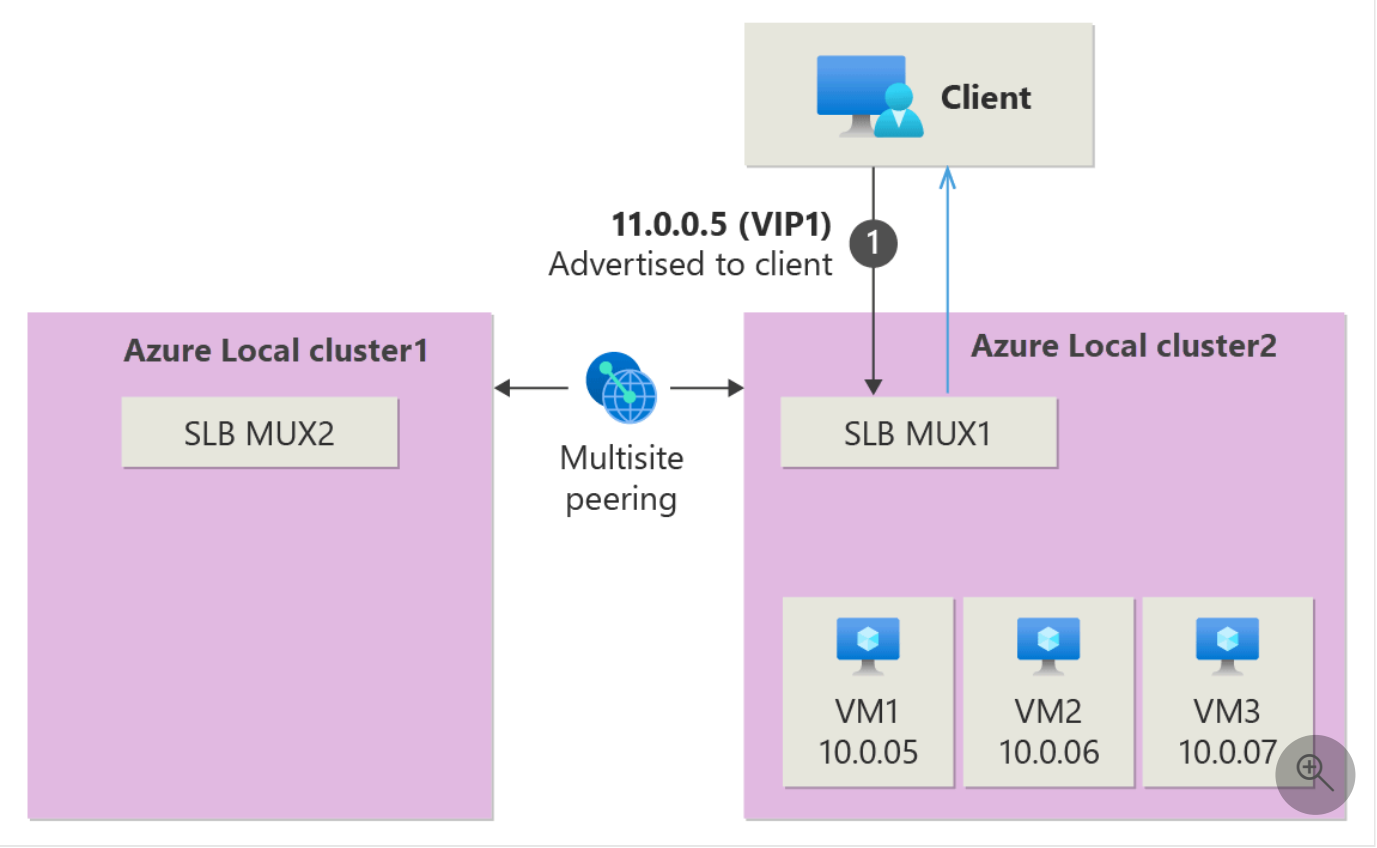
Actuellement, les équilibreurs de charge logiciel sont des ressources locales pour chacun de vos sites physiques. Cela signifie que les stratégies et configurations d'équilibrage de charge ne sont pas synchronisées entre les sites via Multisite. Gardez cela à l'esprit lors de la migration de machines virtuelles d'un emplacement vers un autre dans une configuration multisite SDN.

Équilibrage de charge dans SDN Multisite : exemple de scénario

Les sections suivantes expliquent l'équilibrage de charge dans Multisite via un exemple de scénario, illustrant à la fois sans et avec la migration de machines virtuelles de charge de travail. Supposons que vous ayez deux instances locales Azure avec SDN Multisite activé, chacune avec son propre infrastructure SDN déployée et configurée. Dans ce scénario, un client souhaite accéder à la machine virtuelle VM1 avec l'adresse IP 10.0.0.5 et l'adresse IP virtuelle 11.0.0.5.

Équilibrage de charge dans SDN Multisite sans migrer des machines virtuelles de charge de travail

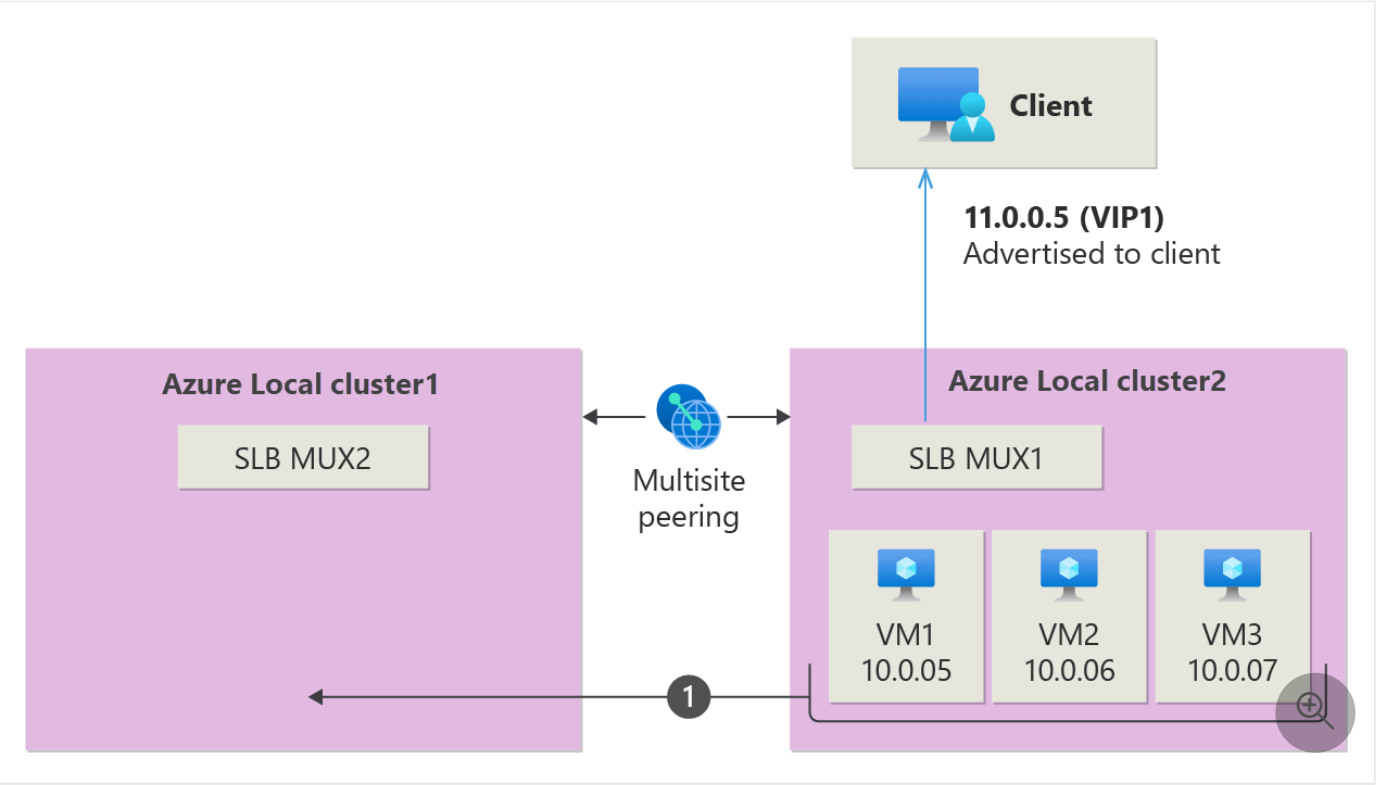
Dans SDN Multisite, s'il n'y a pas de migration de machine virtuelle entre les emplacements, les paquets de données sont transférés comme d'habitude, comme d'habitude, à l'instar de la configuration SDN traditionnelle. L'animation suivante illustre le chemin des données de la machine cliente vers VM1 via SLB MUX1 dans le cluster 2.



Équilibrage de charge dans SDN Multisite avec migration de machines virtuelles de charge de travail

Si vous décidez de migrer une machine virtuelle ou toutes les machines virtuelles derrière l'adresse IP virtuelle vers l'autre site, vous pouvez rencontrer des situations où la machine virtuelle que vous essayez d'atteindre devient inaccessible sur l'adresse IP virtuelle, en fonction de son emplacement. Cela se produit, car les ressources d'équilibreur de charge sont locales pour chaque instance locale Azure. À mesure que les machines virtuelles de charge de travail se

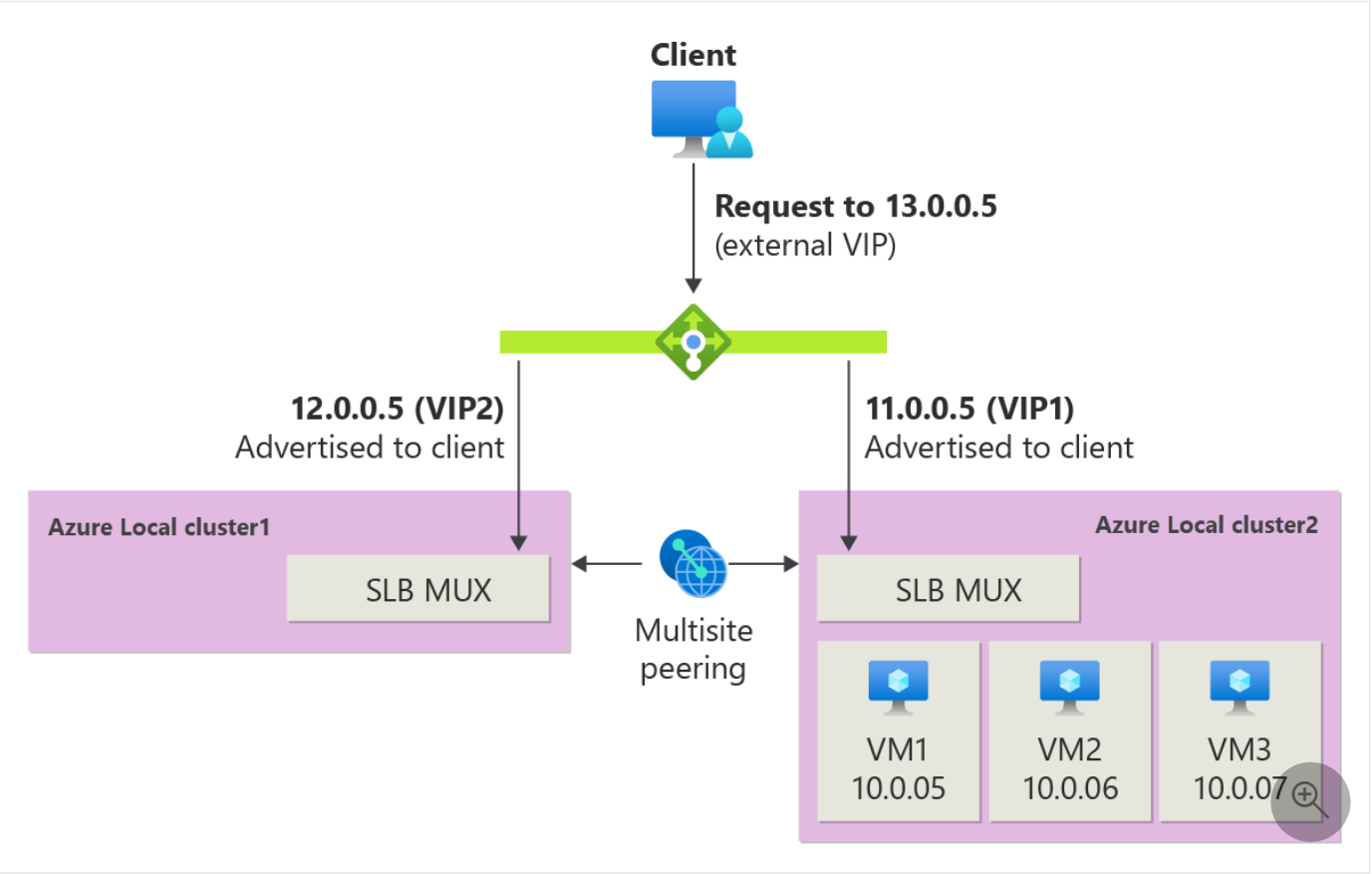
déplacent, les configurations sur les MUX ne sont pas globales, ce qui laisse l'autre site sans connaissance des migrations. L'animation suivante illustre la migration des machines virtuelles du cluster 2 vers le cluster 1 et la façon dont le chemin du paquet de données échoue après la migration.



Pour contourner cette limitation, vous pouvez utiliser l'équilibreur de charge externe qui vérifie la disponibilité des machines virtuelles principales sur chaque site et achemine le trafic en conséquence. Consultez Utiliser l'équilibreur de charge externe dans Multisite avec la migration des machines virtuelles de charge de travail.

Utiliser l'équilibreur de charge externe dans Multisite avec la migration de machines virtuelles de charge de travail

Vous pouvez activer un équilibreur de charge externe pour vérifier s'il existe des machines virtuelles principales derrière un équilibreur de charge sur l'un de vos sites. S'il n'existe aucune machine virtuelle de back-end derrière un équilibreur de charge, l'adresse IP virtuelle pour le multiplexeur n'est pas annoncée jusqu'à l'équilibreur de charge externe et toute sonde d'intégrité envoyée échoue. Cet équilibreur de charge externe garantit la connectivité aux charges de travail, même lorsque les machines virtuelles passent d'un site à un autre.



Toutefois, si le déploiement d'un équilibreur de charge externe n'est pas réalisable, utilisez la solution d'équilibrage de charge logicielle, comme décrit dans l'équilibrage de charge dans SDN Multisite sans migrer les machines virtuelles de charge de travail tant que vous n'avez pas de machines virtuelles de charge de travail migrées.

Passerelles et leurs limitations

SDN multisite ne synchronise pas les ressources locales, telles que les connexions de passerelle entre les sites. Chaque site possède ses propres machines virtuelles de passerelle et connexions de passerelle. Lorsqu'une machine virtuelle de charge de travail est créée ou migrée vers un site, elle reçoit une configuration de passerelle locale, notamment les itinéraires de passerelle. Si vous créez une connexion de passerelle pour un réseau virtuel particulier sur un site, les machines virtuelles de ce site perdent la connectivité de passerelle lors de la migration vers l'autre site. Pour que les machines virtuelles conservent la connectivité de passerelle lors de la migration, vous devez configurer une connexion de passerelle distincte pour le même réseau virtuel sur l'autre site.

Étapes suivantes

Gérer SDN Multisite pour Azure Local

Dernière mise à jour : 15/09/2026

Vue d'ensemble de la mise en réseau de conteneurs

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Dans cette rubrique, nous vous proposons une vue d'ensemble de la pile réseau pour les conteneurs Windows et nous incluons des liens vers des conseils supplémentaires sur la création, la configuration et la gestion des réseaux de conteneurs.

Les conteneurs Windows Server constituent une méthode de virtualisation de système d'exploitation légère et utilisée pour séparer des applications ou des services d'autres services exécutés sur le même hôte de conteneur. Les conteneurs Windows fonctionnent de façon similaire aux machines virtuelles. Lorsque cette option est activée, chaque conteneur a une vue distincte du système d'exploitation, des processus, du système de fichiers, du registre et des adresses IP, que vous pouvez connecter aux réseaux virtuels.

Un conteneur Windows partage un noyau avec l'hôte de conteneur et tous les conteneurs exécutés sur l'hôte. En raison de l'espace de noyau partagé, ces conteneurs requièrent la même version et configuration de noyau. Les conteneurs assurent l'isolation d'applications grâce à la technologie d'isolation des processus et des espaces de noms.

> ⓘ **Important**
>
> Les conteneurs Windows ne créent pas de frontière de sécurité contre le code hostile et ne doivent pas être utilisés pour isoler du code non fiable.

Avec les conteneurs Windows, vous pouvez déployer un hôte Hyper-V, dans lequel vous créez une ou plusieurs machines virtuelles sur les hôtes de machine virtuelle. À l'intérieur des hôtes de machine virtuelle, les conteneurs sont créés et l'accès réseau se fait par le biais d'un commutateur virtuel exécuté à l'intérieur de la machine virtuelle. Vous pouvez utiliser des images réutilisables stockées dans un référentiel pour déployer le système d'exploitation et les services dans des conteneurs. Chaque conteneur possède une carte réseau virtuelle qui est connectée à un commutateur virtuel sur lequel le trafic entrant et sortant est transféré. Vous pouvez attacher des points de terminaison de conteneur à un réseau hôte local (comme NAT), au réseau physique ou au réseau virtuel de superposition créé via la pile SDN.

Pour appliquer l'isolation entre les conteneurs sur le même hôte, vous créez un compartiment réseau pour chaque conteneur Windows Server et Hyper-V. Les conteneurs Windows Server utilisent une carte réseau virtuelle hôte pour s'attacher au commutateur virtuel. Les conteneurs Hyper-V utilisent une carte réseau de machine virtuelle synthétique (non exposée à la machine virtuelle d'utilitaire) pour s'attacher au commutateur virtuel.

Rubriques connexes

- Mise en réseau de conteneurs Windows : découvrez comment créer et gérer des réseaux de conteneurs pour les déploiements sans superposition/SDN.
- Connecter les points de terminaison de conteneur à un réseau virtuel locataire : découvrez comment créer et gérer des réseaux de conteneurs pour superposer des réseaux virtuels avec SDN.

Commentaires

Cette page a-t-elle été utile ? Yes No

Déployer une infrastructure SDN (Software Defined Networking)

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Déployez l'infrastructure SDN (Software Defined Networking) de Microsoft.

Ces déploiements incluent toutes les technologies dont vous avez besoin pour une infrastructure entièrement fonctionnelle, y compris la virtualisation de réseau Hyper-V (HNV), les contrôleurs réseau, les équilibreurs de charge logiciels (SLB/MUX) et les passerelles.

Configurer l'infrastructure SDN dans la matrice VMM

- Configurer une infrastructure SDN (Software-Defined Networking) dans l'infrastructure VMM

  Utilisez cette méthode si vous souhaitez incorporer System Center Virtual Machine Manager (VMM) pour gérer votre infrastructure SDN.

Déployer l'infrastructure SDN en utilisant des scripts

- Déployer une infrastructure SDN (Software Defined Networking) avec des scripts

  Utilisez cette méthode si vous ne souhaitez pas utiliser VMM pour gérer votre infrastructure SDN, ou si vous disposez d'une autre méthode de gestion.

Déployer des technologies SDN individuelles au lieu d'une infrastructure entière

Si vous souhaitez déployer des technologies SDN individuelles au lieu d'une infrastructure entière, consultez Déployer des technologies réseau définies par logiciel à l'aide de Windows PowerShell.

Rubriques connexes

- Mise en réseau SDN (Software Defined Networking)
- SDN Technologies
- Plan SDN
- Gérer SDN
- Sécurité pour SDN
- Résoudre les problèmes de SDN

Déployer une infrastructure SDN (Software Defined Networking) avec des scripts

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans cette rubrique, vous déployez une infrastructure de mise en réseau SDN (Software Defined Network) Microsoft à l'aide de scripts. L'infrastructure comprend un contrôleur de réseau à haute disponibilité (HA), un équilibreur de charge logiciel HA (SLB)/MUX, des réseaux virtuels et des listes de contrôle d'accès (ACL) associées. De plus, un autre script déploie une charge de travail locataire pour que vous puissiez valider votre infrastructure SDN.

Si vous souhaitez que les charges de travail de vos locataires communiquent en dehors de leurs réseaux virtuels, vous pouvez configurer des règles NAT SLB, des tunnels de passerelle site à site ou un transfert de couche 3 pour assurer le routage entre les charges de travail virtuelles et physiques.

Vous pouvez également déployer une infrastructure SDN à l'aide de VMM (Virtual Machine Manager). Pour plus d'informations, consultez Configurer une infrastructure SDN (Software Defined Network) dans l'infrastructure VMM.

Predeployment

> ⓘ **Important**
>
> Avant de commencer le déploiement, vous devez planifier et configurer vos ordinateurs hôtes et l'infrastructure réseau physique. Pour plus d'informations, consultez **Planifier une mise en réseau SDN (Software Defined Networking)**.

Tous les hôtes Hyper-V doivent avoir installé Windows Server 2019 ou 2016.

Étapes du déploiement

Commencez par configurer le commutateur virtuel Hyper-V (serveurs physiques) de l'hôte Hyper-V et l'attribution de l'adresse IP. Vous pouvez utiliser n'importe quel type de stockage compatible avec Hyper-V, partagé ou local.

Installer la mise en réseau de l'hôte

1. Installez les derniers pilotes réseau disponibles pour votre matériel de carte réseau.

2. Installez le rôle Hyper-V sur tous les hôtes. Pour plus d'informations, voir Installer le rôle Hyper-V sur Windows Server.

   PowerShell

   ```
   Install-WindowsFeature -Name Hyper-V -ComputerName <computer_name> -
   IncludeManagementTools -Restart
   ```

3. Créez le commutateur virtuel Hyper-V.

   Utilisez le même nom de commutateur pour tous les hôtes, par exemple **sdnSwitch**. Configurez au moins une carte réseau ou, si vous utilisez SET, configurez au moins deux cartes réseau. La diffusion entrante maximale se produit lors de l'utilisation de deux cartes réseau.

   PowerShell

   ```
   New-VMSwitch "<switch name>" -NetAdapterName "<NetAdapter1>" [, "
   <NetAdapter2>" -EnableEmbeddedTeaming $True] -AllowManagementOS $True
   ```

   > **Conseil**
   >
   > Vous pouvez ignorer les étapes 4 et 5 si vous avez des cartes réseau de gestion distinctes.

4. Reportez-vous à la rubrique de planification (Planifier une infrastructure SDN (Software Defined Network)) et collaborez avec votre administrateur réseau pour obtenir l'ID de réseau local virtuel du réseau local virtuel de gestion. Attachez la carte réseau virtuelle de gestion du commutateur virtuel créé au réseau local virtuel de gestion. Cette étape peut être omise si votre environnement n'utilise pas de balises VLAN.

   PowerShell

   ```
   Set-VMNetworkAdapterIsolation -ManagementOS -IsolationMode Vlan -
   DefaultIsolationID <Management VLAN> -AllowUntaggedTraffic $True
   ```

5. Reportez-vous à la rubrique de planification (Planifier une infrastructure SDN (Software Defined Network)) et collaborez avec votre administrateur réseau pour utiliser des affectations d'adresses IP statiques ou DHCP afin d'affecter une adresse IP à la carte réseau virtuelle de gestion du commutateur virtuel créé. L'exemple suivant montre

comment créer une adresse IP statique et l'affecter à la carte réseau virtuelle de gestion du commutateur virtuel :

```
PowerShell

New-NetIPAddress -InterfaceAlias "vEthernet (<switch name>)" -IPAddress <IP>
-DefaultGateway <Gateway IP> -AddressFamily IPv4 -PrefixLength <Length of
Subnet Mask - for example: 24>
```

6. [Facultatif] Déployez un ordinateur virtuel pour héberger les services de domaine Active Directory (Installer les services de domaine Active Directory (niveau 100) et un serveur DNS.

   a. Connectez l'ordinateur virtuel Active Directory/le serveur DNS au réseau local virtuel de gestion :

```
PowerShell

Set-VMNetworkAdapterIsolation -VMName "<VM Name>" -Access -VlanId <Management
VLAN> -AllowUntaggedTraffic $True
```

   b. Installez les services de domaine Active Directory (AD DS) et DNS.

> ⓘ **Notes**
>
> Le contrôleur de réseau prend en charge les certificats Kerberos et X.509 pour l'authentification. Ce guide utilise les deux mécanismes d'authentification à des fins différentes (bien qu'un seul soit obligatoire).

7. Créez un réplica de jeu de configuration pour tous les hôtes Hyper-V au domaine. Vérifiez que l'entrée du serveur DNS pour la carte réseau dont l'adresse IP est affectée au réseau de gestion pointe vers un serveur DNS qui peut résoudre le nom de domaine.

```
PowerShell

Set-DnsClientServerAddress -InterfaceAlias "vEthernet (<switch name>)" -
ServerAddresses <DNS Server IP>
```

   a. Cliquez avec le bouton droit sur **Démarrer**, sélectionnez **Système**, puis **Sélectionnez Modifier les paramètres**. **Modifier les paramètres**. b. Sélectionnez **Modifier**. c. Sélectionnez **Domaine** et spécifiez le nom de domaine. d. Sélectionnez **OK**. e. Tapez le nom d'utilisateur et le mot de passe lorsque vous y êtes invité. f. Redémarrez le serveur.

Validation

Suivez les étapes suivantes pour vérifier que la mise en réseau des hôtes est correcte.

1. Vérifiez que le commutateur de l'ordinateur virtuel a été créé correctement :

   PowerShell

   ```
   Get-VMSwitch "<switch name>"
   ```

2. Vérifiez que la carte réseau virtuelle de gestion sur le commutateur de l'ordinateur virtuel est connectée au réseau local virtuel de gestion :

   > **Notes**
   >
   > Pertinent uniquement si les trafics de gestion et de locataire partagent la même carte réseau.

   PowerShell

   ```
   Get-VMNetworkAdapterIsolation -ManagementOS
   ```

3. Validez tous les hôtes Hyper-V et toutes les ressources de gestion externe, par exemple, les serveurs DNS. Assurez-vous qu'ils sont accessibles par ping à l'aide de leur adresse IP de gestion et/ou de leur nom de domaine complet (FQDN).

   PowerShell

   ```
   ping <Hyper-V Host IP>
   ping <Hyper-V Host FQDN>
   ```

4. Exécutez la commande suivante sur l'hôte de déploiement et spécifiez le FQDN de chaque hôte Hyper-V pour vous assurer que les informations d'identification Kerberos utilisées permettent d'accéder à tous les serveurs.

   PowerShell

   ```
   winrm id -r:<Hyper-V Host FQDN>
   ```

Exécuter les scripts SDN Express

1. Accédez au référentiel GitHub Microsoft SDN pour obtenir les fichiers d'installation.

2. Téléchargez les fichiers d'installation depuis le référentiel sur l'ordinateur de déploiement désigné. Cliquez sur **Cloner ou Télécharger**, puis cliquez sur **Télécharger le fichier ZIP**.

> ⓘ **Notes**
>
> L'ordinateur de déploiement désigné doit exécuter Windows Server 2016 ou une version ultérieure.

3. Développez le fichier zip et copiez le dossier **SDNExpress** dans le dossier de l'ordinateur de `C:\` déploiement.

4. Partagez le `C:\SDNExpress` dossier en tant que « **SDNExpress** » avec l'autorisation pour **tout le monde** de **lire/écrire**.

5. Accédez au dossier `C:\SDNExpress`.

   Les dossiers suivants apparaissent :

Agrandir le tableau

Nom du dossier	Description
AgentConf	Contient de nouvelles copies des schémas OVSDB utilisés par l'agent hôte SDN sur chaque hôte Windows Server 2016 Hyper-V pour programmer la stratégie réseau.
Certs	Emplacement partagé temporaire du fichier de certificat NC.
Images	Vide, placez votre image vhdx Windows Server 2016 ici
Tools	Utilitaires pour la résolution des problèmes et le débogage. Copié sur les ordinateurs hôtes et les ordinateurs virtuels. Nous vous recommandons de placer Network Monitor ou Wireshark ici afin qu'il soit disponible si nécessaire.
Scripts	Scripts de déploiement. - **SDNExpress.ps1** Déploie et configure la structure, y compris les machines virtuelles du contrôleur de réseau, les machines virtuelles SLB Mux, le(s) pool(s) de passerelles et la(les) machine(s) virtuelle(s) de passerelle HNV correspondant au(x) pool(s). - **FabricConfig.psd1** Modèle de fichier de configuration pour le script SDNExpress. Vous adapterez cette fonction à votre environnement. - **SDNExpressTenant.ps1** Déploie un exemple de charge de travail locataire sur un réseau virtuel avec une adresse IP virtuelle équilibrée en charge. Approvisionne également une ou plusieurs connexions réseau (VPN IPSec S2S, GRE, L3) sur les passerelles de périphérie du fournisseur de services qui sont connectées à

Nom du dossier	Description
	la charge de travail locataire créée précédemment. Les passerelles IPSec et GRE sont disponibles pour la connectivité via l'adresse IP virtuelle correspondante, et la passerelle de transfert L3 sur le pool d'adresses correspondant. Ce script peut également être utilisé pour supprimer la configuration correspondante avec une option Annuler. - **TenantConfig.psd1** Fichier de configuration de modèle pour la charge de travail locataire et la configuration de la passerelle S2S. - **SDNExpressUndo.ps1** Nettoie l'environnement d'infrastructure et le réinitialise à un état de départ. - **SDNExpressEnterpriseExample.ps1** Fournit un ou plusieurs environnements de sites d'entreprise avec une passerelle d'accès à distance et (éventuellement) une machine virtuelle d'entreprise correspondante par site. Les passerelles d'entreprise IPSec ou GRE se connectent à l'adresse IP virtuelle correspondante de la passerelle du fournisseur de services pour établir les tunnels S2S. La passerelle de transfert L3 se connecte à l'adresse IP de pair correspondante. Ce script peut également être utilisé pour supprimer la configuration correspondante avec une option Annuler. - **EnterpriseConfig.psd1** Fichier de configuration de modèle pour la passerelle de site à site d'entreprise et la configuration de l'ordinateur virtuel client.
TenantApps	Fichiers utilisés pour déployer des exemples de charges de travail locataire.

6. Vérifiez que le fichier VHDX Windows Server 2016 se trouve dans le dossier **Images** .

7. Personnalisez le fichier SDNExpress\scripts\FabricConfig.psd1 en changeant les étiquettes << **Remplacer** >> par des spécifiques en fonction de l'infrastructure de votre laboratoire, notamment les noms d'hôte, les noms de domaine, les noms d'utilisateur et les mots de passe, ainsi que les informations réseau pour les réseaux listés dans la rubrique Réseau de planification.

8. Créez un enregistrement Hôte A dans DNS pour NetworkControllerRestName (FQDN) et NetworkControllerRestIP.

9. Exécutez le script en tant qu'utilisateur disposant d'informations d'identification d'administrateur de domaine :

PowerShell

```
SDNExpress\scripts\SDNExpress.ps1 -ConfigurationDataFile FabricConfig.psd1 -
Verbose
```

10. Pour annuler toutes les opérations, exécutez la commande suivante :

PowerShell

```
 SDNExpress\scripts\SDNExpressUndo.ps1 -ConfigurationDataFile FabricConfig.psd1 -
Verbose
```

Validation

En supposant que le script SDN Express s'est exécuté jusqu'à l'achèvement sans signaler d'erreurs, vous pouvez effectuer l'étape suivante pour vous assurer que les ressources d'infrastructure ont été déployées correctement et sont disponibles pour le déploiement du locataire.

Utilisez les outils de diagnostic pour vous assurer qu'il n'existe aucune erreur sur les ressources de l'infrastructure dans le contrôleur de réseau.

PowerShell

```
Debug-NetworkControllerConfigurationState -NetworkController <FQDN of Network
Controller Rest Name>
```

Déployer un exemple de charge de travail locataire avec l'équilibreur de charge logiciel

Maintenant que les ressources d'infrastructure ont été déployées, vous pouvez valider votre déploiement SDN de bout en bout en déployant un exemple de charge de travail locataire. Cette charge de travail locataire se compose de deux sous-réseaux virtuels (niveau Web et niveau base de données) protégés par des règles de liste de contrôle d'accès (ACL) à l'aide du pare-feu distribué SDN. Le sous-réseau virtuel du niveau Web est accessible via le SLB/MUX à l'aide d'une adresse IP virtuelle (VIP). Le script déploie automatiquement deux ordinateurs virtuels de niveau Web et un ordinateur virtuel de niveau base de données et les connecte aux sous-réseaux virtuels.

1. Personnalisez le fichier SDNExpress\scripts\TenantConfig.psd1 en changeant les étiquettes << **Remplacer** >> par des valeurs spécifiques (par exemple, nom de l'image VHD, nom REST du contrôleur de réseau, nom du commutateur virtuel, etc. comme cela est défini précédemment dans le fichier FabricConfig.psd1)

2. Exécutez le script. Par exemple:

   PowerShell

```
SDNExpress\scripts\SDNExpressTenant.ps1 -ConfigurationDataFile
TenantConfig.psd1 -Verbose
```

3. Pour annuler la configuration, exécutez le même script avec le paramètre **d'annulation** . Par exemple:

```PowerShell
SDNExpress\scripts\SDNExpressTenant.ps1 -Undo -ConfigurationDataFile
TenantConfig.psd1 -Verbose
```

Validation

Pour vérifier que le déploiement du locataire a réussi, procédez comme suit :

1. Connectez-vous à la machine virtuelle de niveau base de données et essayez d'envoyer un ping à l'adresse IP de l'une des machines virtuelles de niveau Web (assurez-vous que le pare-feu Windows est désactivé dans les machines virtuelles de niveau Web).

2. Vérifiez que les ressources locataire du contrôleur de réseau ne présentent pas d'erreurs. Exécutez ce qui suit à partir de n'importe quel hôte Hyper-V ayant une connectivité de couche 3 au contrôleur de réseau :

```PowerShell
Debug-NetworkControllerConfigurationState -NetworkController <FQDN of Network
Controller REST Name>
```

3. Pour vérifier que l'équilibreur de charge s'exécute correctement, exécutez la commande suivante à partir de n'importe quel hôte Hyper-V :

```PowerShell
wget <VIP IP address>/unique.htm -disablekeepalive -usebasicparsing
```

où `<VIP IP address>` est l'adresse IP virtuelle du niveau Web que vous avez configurée dans le fichier TenantConfig.psd1.

> **Conseil**
>
> Recherchez la variable `VIPIP` dans TenantConfig.psd1.

Exécutez cette opération plusieurs fois pour voir le commutateur de l’équilibreur de charge entre les DIP disponibles. Vous pouvez également observer ce comportement à l’aide d’un navigateur Web. Accédez à `<VIP IP address>/unique.htm`. Fermez le navigateur, ouvrez une nouvelle instance et parcourez à nouveau. Vous verrez la page bleue et la page verte s'alterner, sauf lorsque le navigateur met la page en cache avant que le cache ne s'épuise.

Déployer le Network Controller avec le clustering de basculement

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Depuis Windows Server 2025 et Azure Local 2311.2, le contrôleur réseau (NC) peut désormais être déployé directement en tant que service de clustering de basculement. Dans cet article, vous apprenez les prérequis nécessaires, l'installation du module PowerShell SDN Express, et comment déployer le Network Controller avec le clustering de basculement. Pour en savoir plus sur son fonctionnement avec le Software Load Balancer et les Gateways, et comment il diffère du Network Controller sur Service Fabric, veuillez consulter Network Controller avec le clustering de basculement.

Prerequisites

Avant de pouvoir déployer le Network Controller avec le clustering de basculement, vous devez remplir les prérequis suivants.

- Vous disposez d'un cluster de basculement avec au moins deux nœuds exécutant Windows Server 2025 ou version ultérieure.
- (Optionnel) Si vous avez l'intention de déployer le Software Load Balancer et les services Gateway en tant que machines virtuelles en utilisant le Failover Cluster, créez un VHDX amorçable avec l'image Windows Server 2025 à utiliser plus tard dans cet article. Pour en savoir plus sur la création d'un VHDX amorçable, suivez les étapes 1 et 2 dans Démarrer sur un disque dur virtuel : Ajouter un VHDX ou un VHD au menu de démarrage.
- Vous disposez d'un stockage partagé disponible pour le cluster de basculement. Nous vous recommandons d'utiliser l'espace de stockage de cluster ou S2D. Pour en savoir plus sur les architectures de stockage disponibles, consultez les architectures de stockage physique pour Hyper-V.
- Tous les nœuds de cluster doivent avoir Hyper-V activé.
- Tous les nœuds de cluster doivent avoir le rôle serveur du contrôleur de réseau installé. Cela doit inclure les outils d'administration de serveur distant (RSAT).

> ⓘ **Important**

> Vous devez redémarrer chaque nœud après avoir installé le rôle serveur du contrôleur de réseau avant de pouvoir poursuivre le déploiement.

- Tous les nœuds de cluster doivent être joints à Active Directory.
- Un commutateur virtuel doit être créé sur chaque nœud de cluster.
- Le réseau physique doit être configuré pour les sous-réseaux et les réseaux locaux virtuels que vous envisagez d'utiliser et doit être cohérent sur tous les nœuds de cluster.
- Si vous prévoyez d'utiliser Windows Admin Center pour déployer le Network Controller avec le clustering de basculement, vous devez disposer de Windows Admin Center version 2410 ou une version ultérieure. Vous devez également installer l'extension SDN Windows Admin Center et la mettre à jour vers la version 3.6.0 ou ultérieure.
- (Facultatif) Si vous envisagez de déployer l'équilibreur de charge logiciel et les services de passerelle en tant que machines virtuelles à l'aide du cluster de basculement, vous devez disposer d'un emplacement pour stocker les fichiers VHDX et de configuration. L'emplacement doit être accessible à partir du nœud sur lequel le script SDN Express est exécuté.

Deployment

Pour déployer le Network Controller avec le clustering de basculement, sélectionnez votre méthode de déploiement préférée.

Windows Admin Center

Pour déployer le Network Controller avec le clustering de basculement en utilisant Windows Admin Center, suivez ces étapes :

1. Connectez-vous à Windows Admin Center en tant qu'administrateur.
2. Dans Windows Admin Center, sous **Toutes les connexions** , sélectionnez le cluster que vous souhaitez gérer, puis sélectionnez **Se connecter**.
3. Dans la vue **Gestionnaire de cluster** , dans le volet **Outils** de gauche, sélectionnez **Infrastructure SDN**.
4. Sélectionnez **Prise en main** pour commencer le processus de déploiement.
5. Sous l'onglet **Type d'infrastructure** , sélectionnez **SDN natif**, puis sélectionnez **Suivant : Paramètres du cluster**.

6. Sous l'onglet **Paramètres du cluster** , fournissez les informations suivantes, puis sélectionnez **Suivant : Déployer** :

Agrandir le tableau

Nom du paramètre	Value
Host	
Nom REST du contrôleur de réseau	Nom DNS utilisé par les clients de gestion (par exemple, Windows Admin Center) pour communiquer avec NC
Adresse IP/sous-réseau REST du Network Controller	Adresse IP statique pour votre API REST, qui est allouée à partir de votre réseau de gestion. Il peut être utilisé pour la résolution DNS ou les déploiements BASÉS sur l'adresse IP REST. L'adresse IP doit utiliser la notation CIDR IP comme moyen de représenter l'adresse IP et son préfixe réseau. Par exemple, l'adresse IP `10.10.10.10` avec un masque de sous-réseau de `255.255.255.0` serait en écriture en tant que `10.10.10.10/25`.
ID de réseau local virtuel	ID de réseau local virtuel pour le réseau de gestion
Credentials	
Username	Nom d'utilisateur administrateur. Le nom d'utilisateur doit être au format suivant : `domainname\username`. Par exemple, si le domaine est `contoso.com`, entrez le nom d'utilisateur en tant que `contoso\<username>`. N'utilisez pas de formats tels que `contoso.com\<username>` ou `username@contoso.com`
Password	Mot de passe du compte d'administrateur
Advanced	
Chemin d'accès à la base de	Chemin d'accès au fichier de la base de données FCNC. Ce chemin d'accès de fichier peut être n'importe quel partage SMB, mais nous vous recommandons d'utiliser CSV ou S2D.
Démarrage du pool d'adresses MAC	Adresse de début du pool MAC pour les VMs de charge de travail client
Fin du pool d'adresses MAC	Adresse de fin du pool MAC pour les machines virtuelles de charge de travail client

7. Une fois que vous avez entré les détails de configuration, vous accédez à la page de déploiement. Passez en revue la progression du déploiement, une fois terminé, sélectionnez **Terminer**.

Vous pouvez maintenant commencer à déployer et à gérer vos réseaux de locataires.

Contenu connexe

- Network Controller avec le clustering de basculement

Gérer SDN

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser les rubriques de cette section pour gérer la mise en réseau à définition logicielle, y compris les charges de travail de locataire et les réseaux virtuels.

> ⓘ **Notes**
>
> Pour obtenir une documentation supplémentaire sur la mise en réseau définie par logiciel, vous pouvez utiliser les sections de bibliothèque suivantes.
>
> - SDN Technologies
> - Plan SDN
> - Déployer SDN
> - Sécurité pour SDN
> - Résoudre les problèmes de SDN

Cette section contient les rubriques suivantes :

- Gérer les réseaux virtuels locataires
- Gérer les charges de travail locataires
- Mettre à jour, sauvegarder et restaurer l'infrastructure réseau définie par logiciel

Configurer des groupes de sécurité réseau avec des balises dans Windows Admin Center

> S'applique à Windows Server 2025

Cet article explique comment configurer des groupes de sécurité réseau avec des balises de sécurité réseau dans Windows Admin Center.

En utilisant des balises de sécurité réseau, vous pouvez créer des balises personnalisées définies par l'utilisateur, attacher ces balises à vos interfaces réseau de machine virtuelle et appliquer des stratégies d'accès réseau (à l'aide de groupes de sécurité réseau) en fonction de ces balises.

Prerequisites

Pour utiliser des groupes de sécurité réseau avec des balises, vous devez remplir les conditions préalables suivantes :

- Vous disposez de Windows Server 2025 ou une version ultérieure. Pour plus d'informations, reportez-vous à Bien démarrer avec Windows Server.
- Vous disposez d'un contrôleur de réseau installé. Pour plus d'informations, découvrez comment déployer une infrastructure SDN à l'aide de SDN Express.
- Vous disposez d'un réseau logique ou d'un réseau virtuel. Pour plus d'informations, découvrez comment créer un réseau logique ou créer un réseau virtuel.
- Vous avez une machine virtuelle à laquelle appliquer un groupe de sécurité réseau. Pour plus d'informations, découvrez comment gérer des machines virtuelles avec Windows Admin Center.
- Vous disposez d'autorisations d'administrateur ou équivalentes pour les nœuds de cluster et le contrôleur réseau.

Simplifier la sécurité avec les balises de sécurité réseau

Les groupes de sécurité réseau vous permettent de configurer des stratégies d'accès basées sur des constructions réseau telles que des préfixes réseau et des sous-réseaux. Par exemple, si vous souhaitez restreindre la communication entre vos machines virtuelles de serveur web et les machines virtuelles de base de données, vous devez identifier les sous-réseaux réseau correspondants et créer une stratégie pour refuser la communication entre ces sous-réseaux. Toutefois, cette approche présente certaines limitations :

- Vos stratégies de sécurité sont liées aux constructions réseau, ce qui signifie que vous devez savoir quelles applications résident sur des segments de réseau spécifiques. La compréhension de votre infrastructure réseau et de votre architecture devient cruciale.
- Lors de la génération de stratégies pour les applications, vous pourriez souhaiter les réutiliser dans différents scénarios. Par exemple, si votre application web de production n'est accessible que sur le port 80 à partir d'Internet et qu'elle n'est pas accessible par d'autres applications en production ou dans d'autres environnements, vous disposeriez d'une stratégie similaire pour toute nouvelle application. Toutefois, avec la segmentation du réseau, vous devez recréer des stratégies en raison d'éléments réseau uniques pour chaque application.
- Si vous désactivez une ancienne application et déployez-en une nouvelle au sein du même segment réseau, vous devez ajuster les stratégies.

En utilisant des balises de sécurité réseau, vous n'avez plus besoin de suivre les segments réseau où vos applications sont hébergées. Les balises de sécurité réseau simplifient la gestion des stratégies et évitent les complexités associées aux constructions réseau. Examinons l'exemple avec des machines virtuelles de serveur web et de base de données : étiqueter les machines virtuelles correspondantes avec des balises de sécurité réseau **web** et **de base de données** , puis créer une règle pour restreindre la communication entre les balises **web** et **de base de données** .

Créer des groupes de sécurité réseau basés sur des balises de sécurité réseau

Pour créer des groupes de sécurité réseau basés sur des balises de sécurité réseau, procédez comme suit :

1. Créez une ou plusieurs balises de sécurité réseau.
2. Attribuez une balise de sécurité réseau à une machine virtuelle.
3. Créez un groupe de sécurité réseau.

4. Créez une règle de sécurité réseau pour le groupe de sécurité réseau.

5. Appliquez le groupe de sécurité réseau à une machine virtuelle, un sous-réseau de réseau, une balise de sécurité réseau.

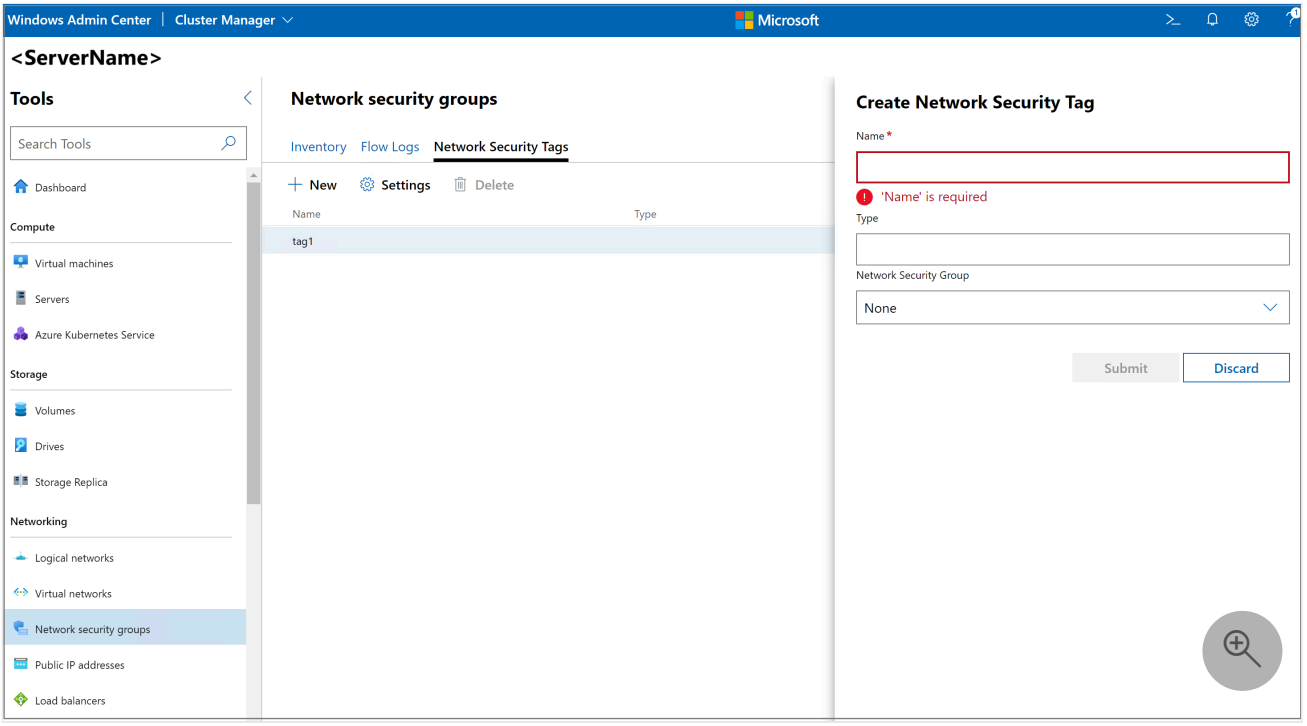
Créer des balises de sécurité réseau

1. Dans l'écran d'accueil Windows Admin Center, sous **Toutes les connexions**, sélectionnez le cluster dans lequel vous souhaitez créer le groupe de sécurité réseau.

2. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Groupes de sécurité réseau**.

3. Sous **Groupes de sécurité réseau**, sélectionnez l'onglet **Balises de sécurité réseau** , puis **Sélectionnez Nouveau**.

4. Dans le volet **Créer une balise de sécurité réseau**, saisissez un nom pour la balise de sécurité réseau dans le champ **Nom**.



5. (Facultatif) Dans le champ **Type**, saisissez un type pour la balise. Ce champ est utile si vous souhaitez classer les balises pour faciliter la gestion. Par exemple, vous pouvez avoir des balises différentes avec le même type « Application », comme SQL, Web, IOT, Sensor, etc.

6. Sélectionnez **Envoyer**.

Attribuer une balise de sécurité réseau à une machine virtuelle

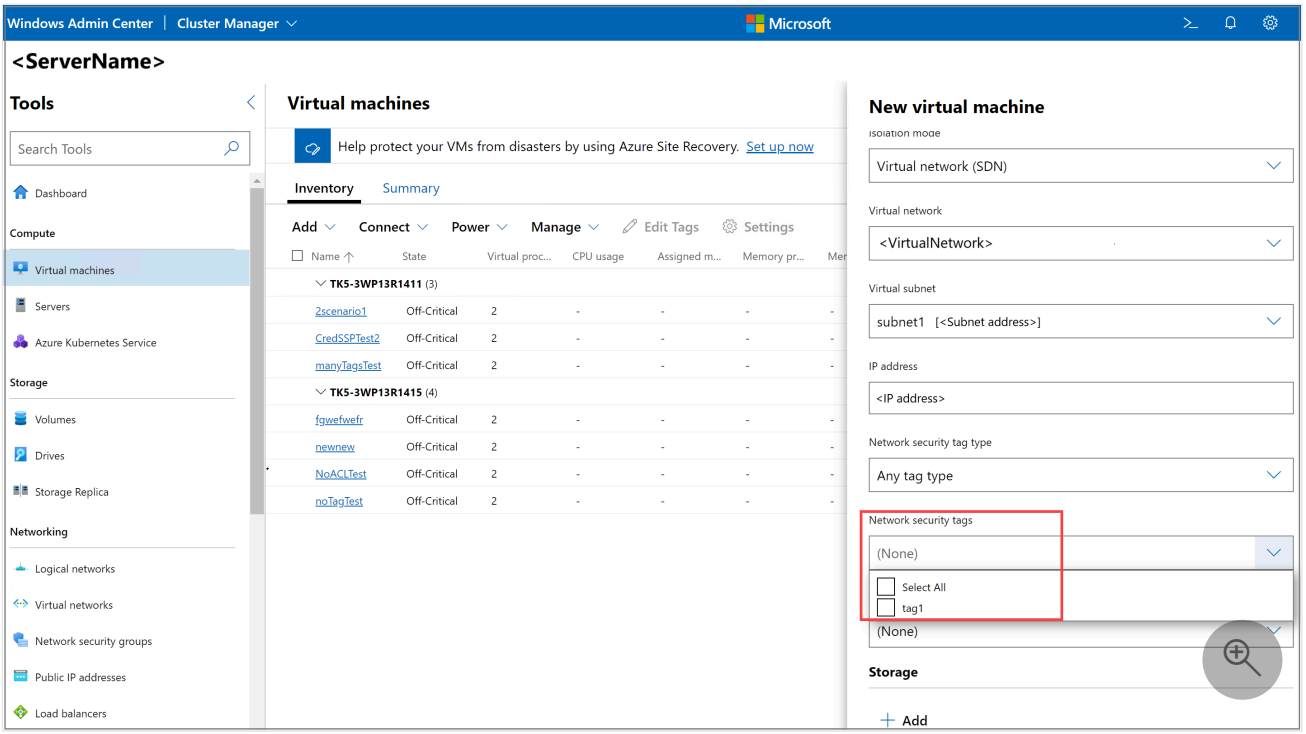
Vous pouvez attribuer une balise de sécurité réseau à une machine virtuelle lors de la création d'une nouvelle machine virtuelle ou ultérieurement lors de la modification des propriétés d'une machine virtuelle existante.

Attribuer une balise de sécurité réseau lors de la création de la machine virtuelle

Pour apprendre pas-à-pas à créer une nouvelle machine virtuelle, consultez Créer une nouvelle machine virtuelle.

Pour attribuer une balise de sécurité réseau lors de la création d'une nouvelle machine virtuelle :

1. Dans l'écran d'accueil Windows Admin Center, sous **Toutes les connexions**, sélectionnez le serveur ou le cluster dans lequel vous souhaitez créer la machine virtuelle.
2. Sous **Outils**, faites défiler la liste et sélectionnez **Machines virtuelles**.
3. Dans **Machines virtuelles**, sélectionnez l'onglet **Inventaire**, puis **Ajouter**, puis sélectionnez **Nouveau**.
4. Sous **Nouvelle machine virtuelle**, entrez un nom pour votre machine virtuelle.
5. Entrez d'autres propriétés pour la machine virtuelle.
6. Dans **Réseau**, sélectionnez la balise de sécurité réseau précédemment créée dans Créer une balise de sécurité réseau.



7. Sélectionnez **Créer**.

Attribuer une balise de sécurité réseau à une machine virtuelle existante

Affectez une balise de sécurité réseau à une machine virtuelle existante en modifiant ses paramètres. Pour obtenir des instructions détaillées, consultez Modifier les paramètres de machine virtuelle.

1. Sous **Outils**, faites défiler jusqu'à la zone **Mise en réseau**, puis sélectionnez **Machines virtuelles**.

2. Sélectionnez l'onglet **Inventaire**, sélectionnez une VM, puis cliquez sur **Paramètres**.

3. Sur la page **Paramètres**, cliquez sur **Réseaux**.

4. Sous la section **Étiquette de sécurité réseau** , sélectionnez **Ajouter une balise de sécurité réseau**, puis sélectionnez la balise de sécurité réseau que vous avez créée précédemment dans Créer une balise de sécurité réseau.

5. Sélectionnez **Enregistrer les paramètres réseau**.

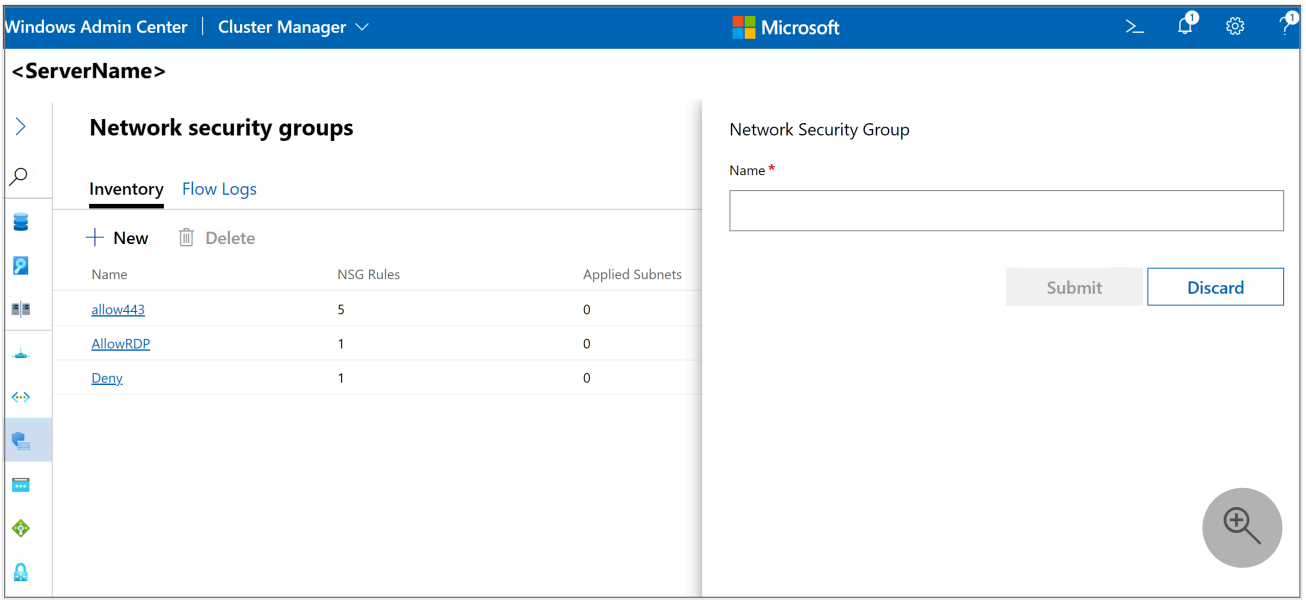
Créer un groupe de sécurité réseau

1. Dans l'écran d'accueil Windows Admin Center, sous **Toutes les connexions**, sélectionnez le cluster dans lequel vous souhaitez créer le groupe de sécurité réseau.

2. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Groupes de sécurité réseau**.

3. Dans **Groupes de sécurité réseau**, sélectionnez l'onglet **Inventaire**, puis sélectionnez **Nouveau**.

4. Dans le volet **Groupes de sécurité réseau**, saisissez un nom pour le groupe de sécurité réseau, puis sélectionnez **Envoyer**.



5. Dans **Groupes de sécurité réseau**, vérifiez que l'**État d'approvisionnement** du nouveau groupe de sécurité réseau affiche **Réussi**.

Créer une règle de groupe de sécurité réseau

Une fois le groupe de sécurité réseau créé, vous pouvez créer des règles pour ce groupe. Si vous souhaitez appliquer des règles de groupe de sécurité réseau au trafic entrant et sortant, vous devez créer deux règles.

1. Dans l'écran d'accueil Windows Admin Center, sous **Toutes les connexions**, sélectionnez le cluster dans lequel vous souhaitez créer le groupe de sécurité réseau.

2. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Groupes de sécurité réseau**.

3. Dans **Groupes de sécurité réseau**, sélectionnez l'onglet **Inventaire**, puis sélectionnez le groupe de sécurité réseau précédemment créé dans Créer un groupe de sécurité réseau.

4. Dans **Règle de sécurité réseau**, sélectionnez **Nouveau**.

5. Dans le volet **Règle de sécurité réseau**, fournissez les informations suivantes :

Agrandir le tableau

Champ	Descriptif
Name	Nom de la règle.
Priorité	Priorité de la règle. Les valeurs possibles vont de **101** à **65000**. Une valeur inférieure représente une priorité plus élevée.
Types	Type de la règle. Ce type de règle peut être **entrant** ou **sortant**.
Protocol	Protocole correspondant à un paquet entrant ou sortant. Les valeurs acceptables sont **All**, **TCP** et **UDP**.
Source	Sélectionnez **Balise de sécurité réseau**. **Remarque :** vous pouvez sélectionner un préfixe d'adresse ou une balise de sécurité réseau, mais pas les deux.
Type de balise de sécurité source	(Facultatif) Sélectionnez un type pour la balise.
Balise de sécurité source	Sélectionnez une balise de sécurité réseau précédemment créée dans Créer une balise de sécurité réseau.
Plage de ports source	Spécifiez la plage de ports source pour qu'elle corresponde à un paquet entrant ou sortant. Vous pouvez saisir `*` pour spécifier tous les ports sources.
Destination	Sélectionnez **Balise de sécurité réseau**. **Remarque :** vous pouvez sélectionner un préfixe d'adresse ou une balise de sécurité réseau, mais pas les deux. La source et la destination peuvent être différentes.
Type de balise de sécurité de destination	(Facultatif) Sélectionnez un type pour la balise.
Balise de sécurité de destination	Sélectionnez une balise de sécurité réseau précédemment créée dans Créer une balise de sécurité réseau.
Plage de ports de destination	Définissez la plage des ports de destination pour qu'elle corresponde à un paquet entrant ou sortant. Vous pouvez saisir `*` pour spécifier tous les ports de destination.
Actions	Si les conditions précédentes sont mises en correspondance, spécifiez l'autorisation ou le blocage du paquet. Les valeurs possibles sont **Autoriser** et **Refuser**.

Champ	Descriptif
Journalisation	Choisissez d'activer ou de désactiver la journalisation de la règle. Si la journalisation est activée, tout le trafic correspondant à cette règle est consigné sur les ordinateurs hôtes.

6. Sélectionnez **Envoyer**.

Appliquer le groupe de sécurité réseau

Vous pouvez appliquer un groupe de sécurité réseau à :

- Sous-réseau de réseau virtuel
- Sous-réseau de réseau logique
- Interface de réseau spécifique
- Balise de sécurité réseau

Appliquer un groupe de sécurité réseau à une balise de sécurité réseau

Quand vous appliquez un groupe de sécurité réseau à une balise de sécurité réseau, les règles du groupe de sécurité réseau s'appliquent à toutes les interfaces réseau de machines virtuelles associées à cette balise de sécurité réseau.

Pour appliquer un groupe de sécurité réseau à une balise de sécurité réseau via Windows Admin Center, procédez comme suit :

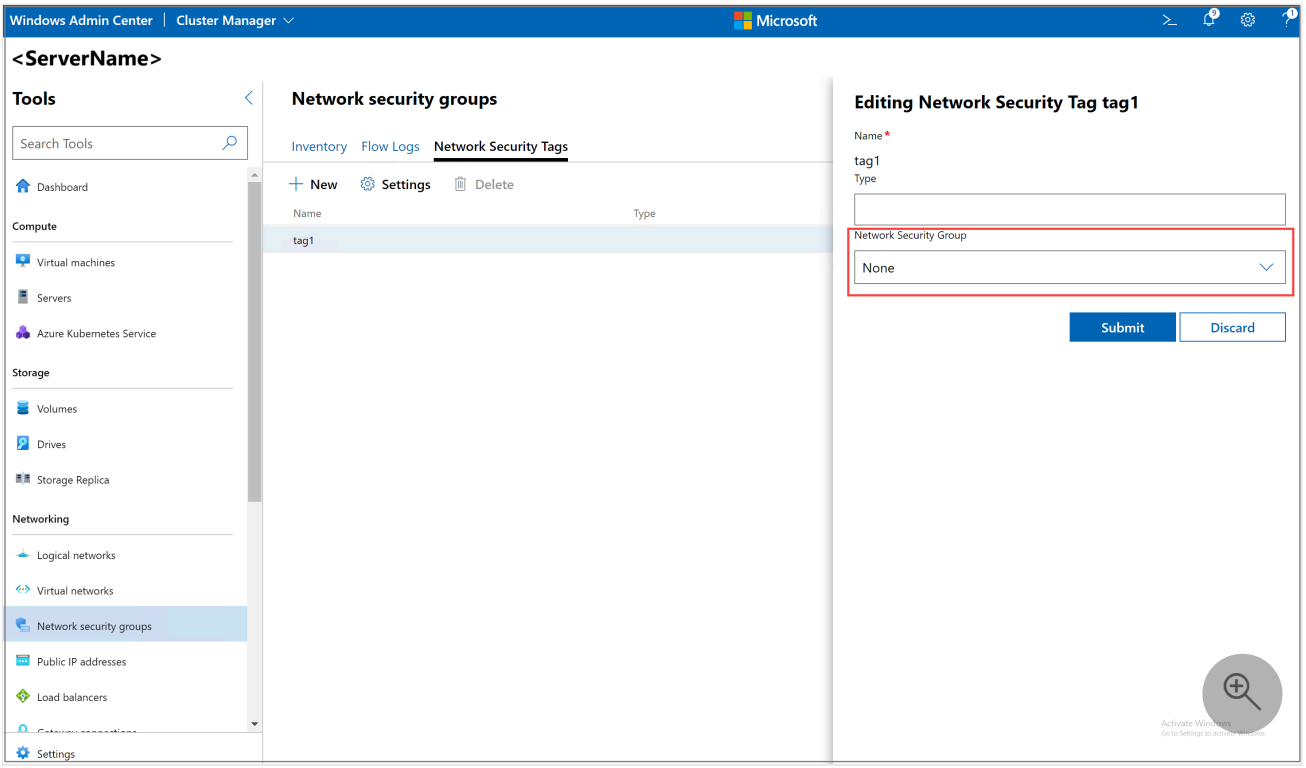
1. Dans l'écran d'accueil Windows Admin Center, sous **Toutes les connexions**, sélectionnez le cluster dans lequel vous souhaitez appliquer le groupe de sécurité réseau.

2. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Groupes de sécurité réseau**.

3. Sous **Groupes de sécurité réseau**, sélectionnez l'onglet **Balises de sécurité réseau** .

4. Sélectionnez la balise de sécurité réseau que vous souhaitez modifier, puis sélectionnez **Paramètres**.

5. Dans le volet **Modifier la balise de sécurité réseau** de la balise sélectionnée, sélectionnez le groupe de sécurité réseau que vous souhaitez appliquer à la balise de sécurité réseau.



6. Sélectionnez **Envoyer**.

Étapes suivantes

Pour plus d'informations, consultez :

- Qu'est-ce que le Pare-feu de centre de données ?
- Configurer des groupes de sécurité réseau avec Windows Admin Center
- Configurer des groupes de sécurité réseau avec PowerShell

Dernière mise à jour : 15/09/2026

Utiliser des stratégies d'accès réseau par défaut sur des machines virtuelles sur Azure Local

> S'applique à Windows Server 2025

Cet article explique comment activer les stratégies d'accès réseau par défaut et les affecter aux machines virtuelles.

Utilisez des stratégies réseau par défaut pour protéger les machines virtuelles contre les attaques non autorisées externes. Ces stratégies bloquent tous les accès entrants aux machines virtuelles (à l'exception des ports de gestion spécifiés que vous souhaitez activer) tout en autorisant tous les accès sortants. Utilisez ces stratégies pour vous assurer que vos machines virtuelles de charge de travail ont accès aux ressources requises uniquement, ce qui rend difficile la propagation des menaces ultérieurement.

> **Remarque**
>
> Dans cette version, vous pouvez activer et affecter des stratégies réseau par défaut via Windows Admin Center.

Prérequis

Remplissez les conditions préalables suivantes pour utiliser des stratégies d'accès réseau :

- Vous disposez de Windows Server 2025 ou version ultérieure. Pour plus d'informations, consultez Prise en main de Windows Server.
- Le contrôleur de réseau est installé. Le contrôleur de réseau applique les stratégies réseau par défaut. Pour plus d'informations, consultez comment installer le contrôleur de réseau.
- Vous disposez d'un réseau logique ou d'un réseau virtuel à utiliser. Pour plus d'informations, consultez comment créer un réseau logique ou créer un réseau virtuel.
- Vous avez une machine virtuelle à laquelle appliquer des stratégies. Pour plus d'informations, consultez comment gérer des machines virtuelles avec Windows Admin

Center.

- Vous disposez d'autorisations d'administrateur ou équivalentes aux nœuds système et au contrôleur de réseau.

Affecter des stratégies réseau par défaut à une machine virtuelle

Vous pouvez attacher des stratégies par défaut à une machine virtuelle de deux façons :

- Lors de la création de la machine virtuelle. Vous devez attacher la machine virtuelle à un réseau logique (réseau VLAN traditionnel) ou à un réseau virtuel SDN.
- Après la création de la machine virtuelle.

Créer et attacher des réseaux

Selon le type de réseau auquel vous souhaitez attacher votre machine virtuelle, les étapes peuvent différer.

- **Attachez des machines virtuelles à un réseau** physique : créez un ou plusieurs réseaux logiques pour représenter ces réseaux physiques. Un réseau logique n'est qu'une représentation d'un ou plusieurs réseaux physiques disponibles pour Azure Local. Pour plus d'informations, consultez comment créer un réseau logique.

- **Attachez des machines virtuelles à un réseau** virtuel SDN : créez un réseau virtuel avant de créer la machine virtuelle. Pour plus d'informations, consultez comment créer un réseau virtuel.

Attacher une machine virtuelle à un réseau logique

Après avoir créé un réseau logique dans Windows Admin Center, vous pouvez créer une machine virtuelle dans Windows Admin Center et l'attacher au réseau logique. Dans le cadre de la création de la machine virtuelle, sélectionnez le **mode** d'isolation en tant que **réseau** logique, sélectionnez le sous-réseau **logique approprié** sous le réseau logique et fournissez une adresse IP pour la machine virtuelle.

> ⓘ **Remarque**
>
> Vous devez créer un réseau logique représentant le réseau local virtuel, créer un sous-réseau de réseau logique avec le réseau local virtuel, puis attacher la machine virtuelle au sous-

réseau de réseau logique.

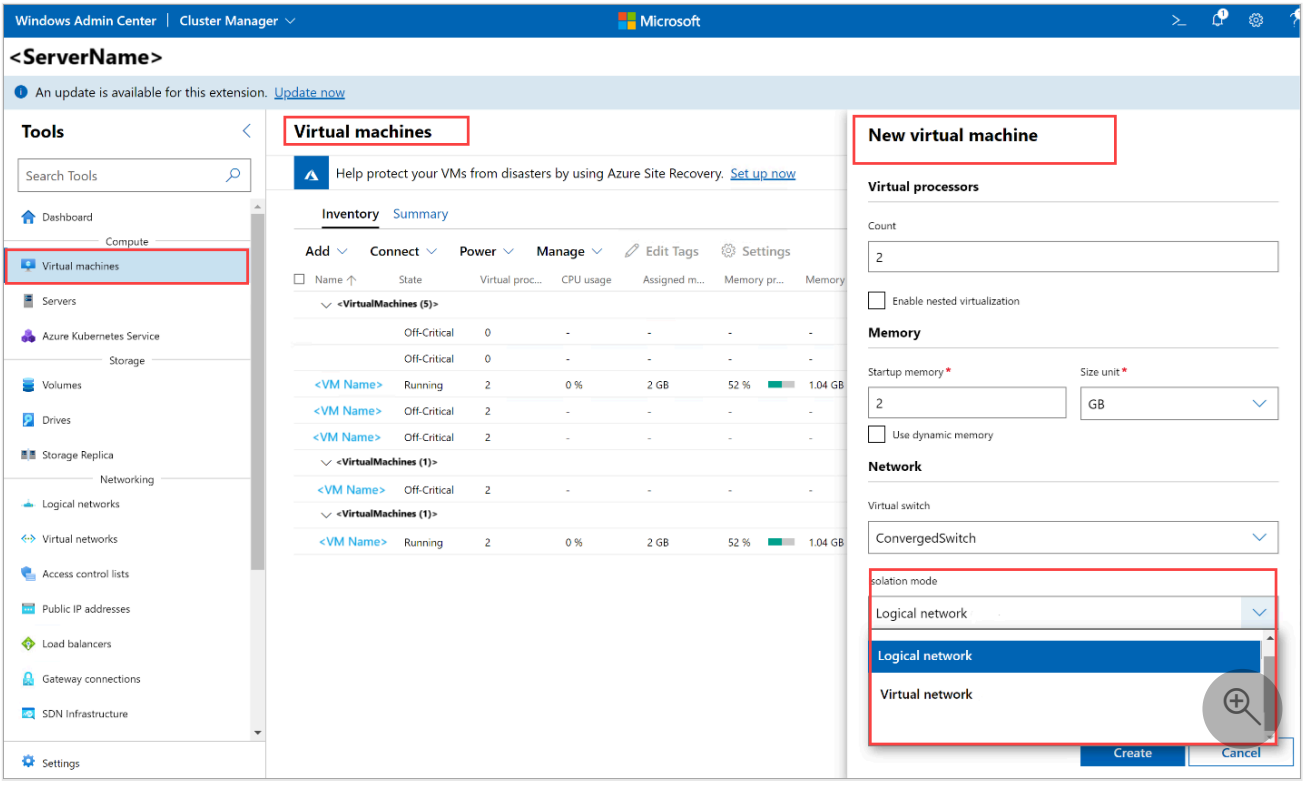
Voici un exemple qui explique comment attacher votre machine virtuelle directement à un réseau local virtuel lorsque le contrôleur de réseau est installé. Dans cet exemple, vous allez montrer comment connecter votre machine virtuelle à VLAN 5 :

1. Créez un réseau logique avec n'importe quel nom. Vérifiez que la virtualisation du réseau est désactivée.

2. Ajoutez un sous-réseau logique avec n'importe quel nom. Indiquez l'ID de réseau local virtuel (5) lors de la création du sous-réseau.

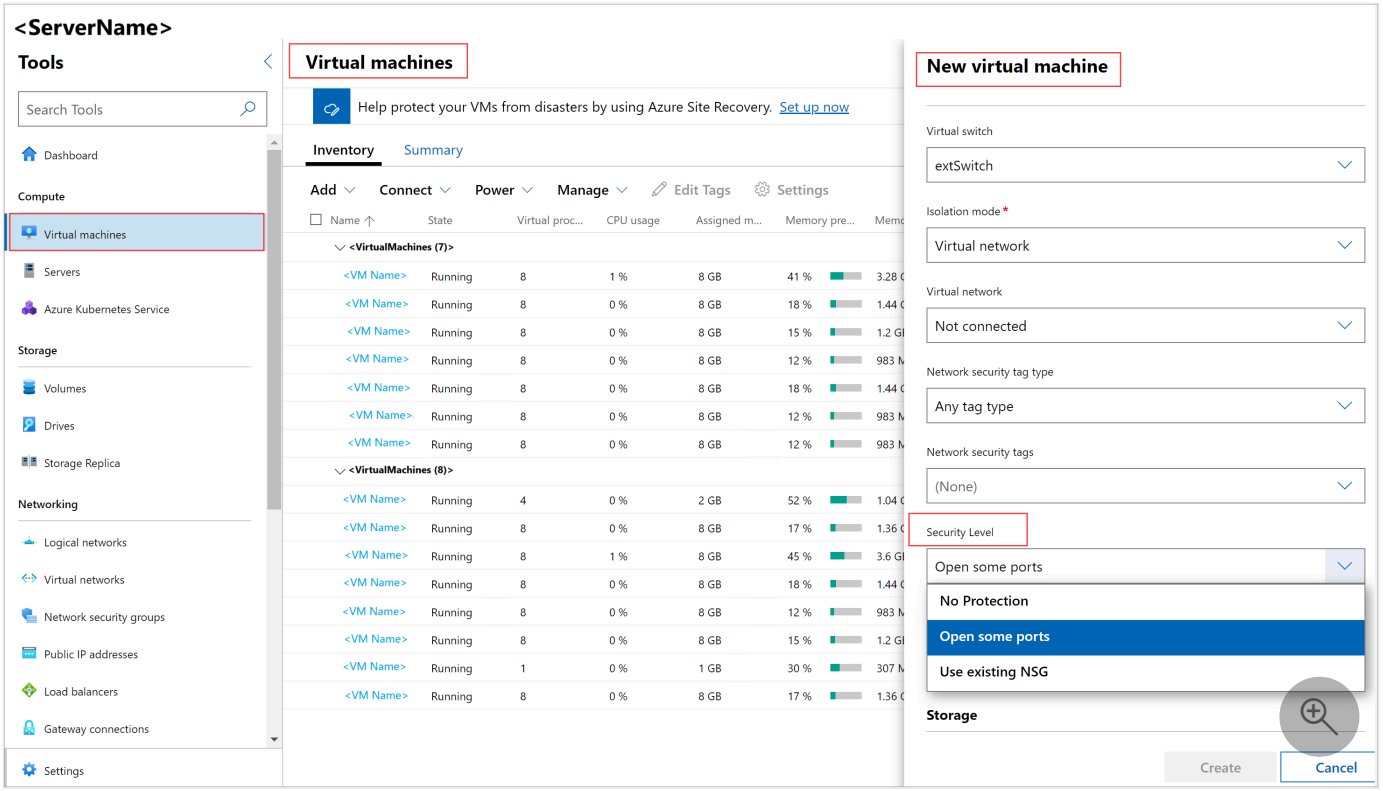
3. Appliquez les modifications.

4. Lors de la création d'une machine virtuelle, attachez-la au réseau logique et au sous-réseau de réseau logique que vous avez créés précédemment. Pour plus d'informations, consultez comment créer un réseau logique.



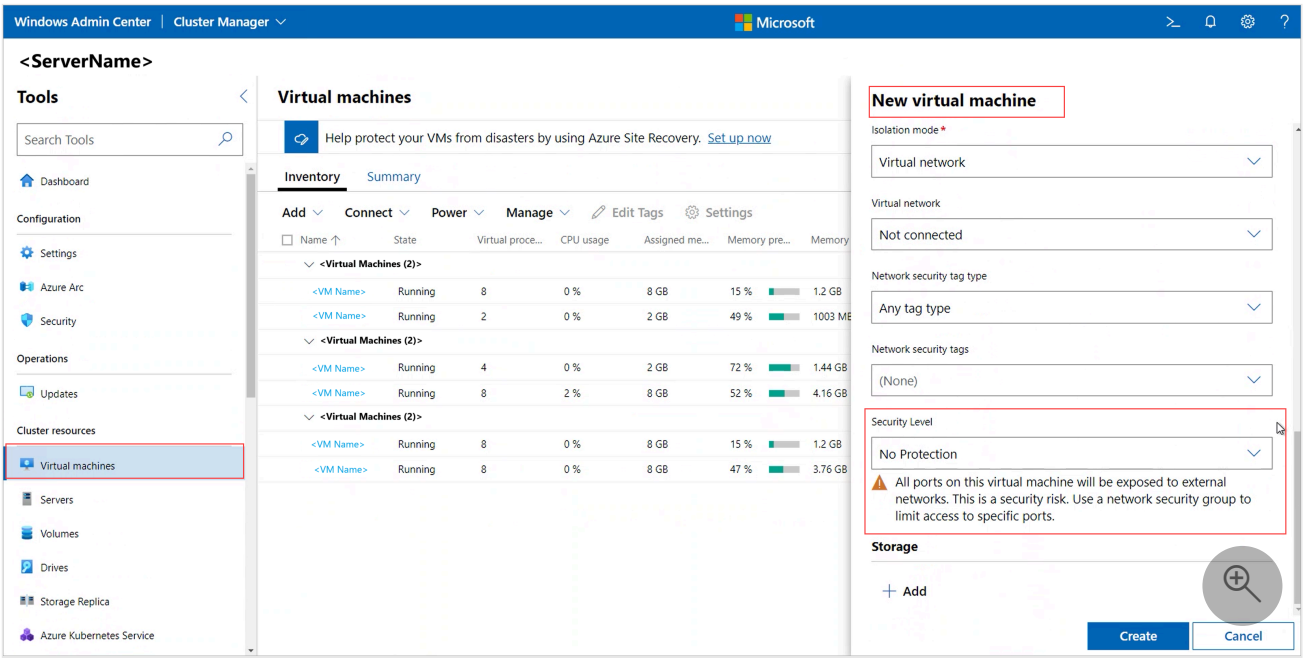
Appliquer des stratégies réseau par défaut

Lorsque vous créez une machine virtuelle via Windows Admin Center, vous voyez un **paramètre de niveau** de sécurité.



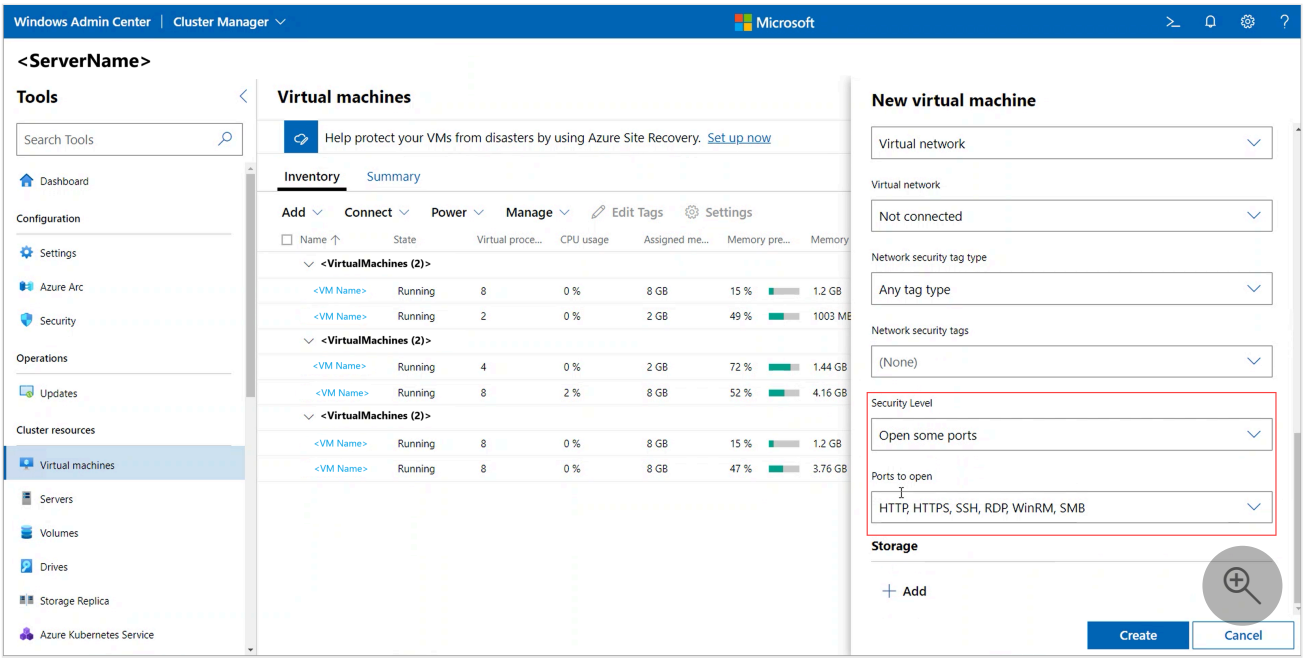
Trois options s'offrent à vous :

- **Aucune protection** : choisissez cette option si vous ne souhaitez pas appliquer de stratégies d'accès réseau à votre machine virtuelle. Lorsque vous sélectionnez cette option, tous les ports de votre machine virtuelle sont exposés à des réseaux externes, ce qui pose un risque de sécurité. N'utilisez pas cette option.

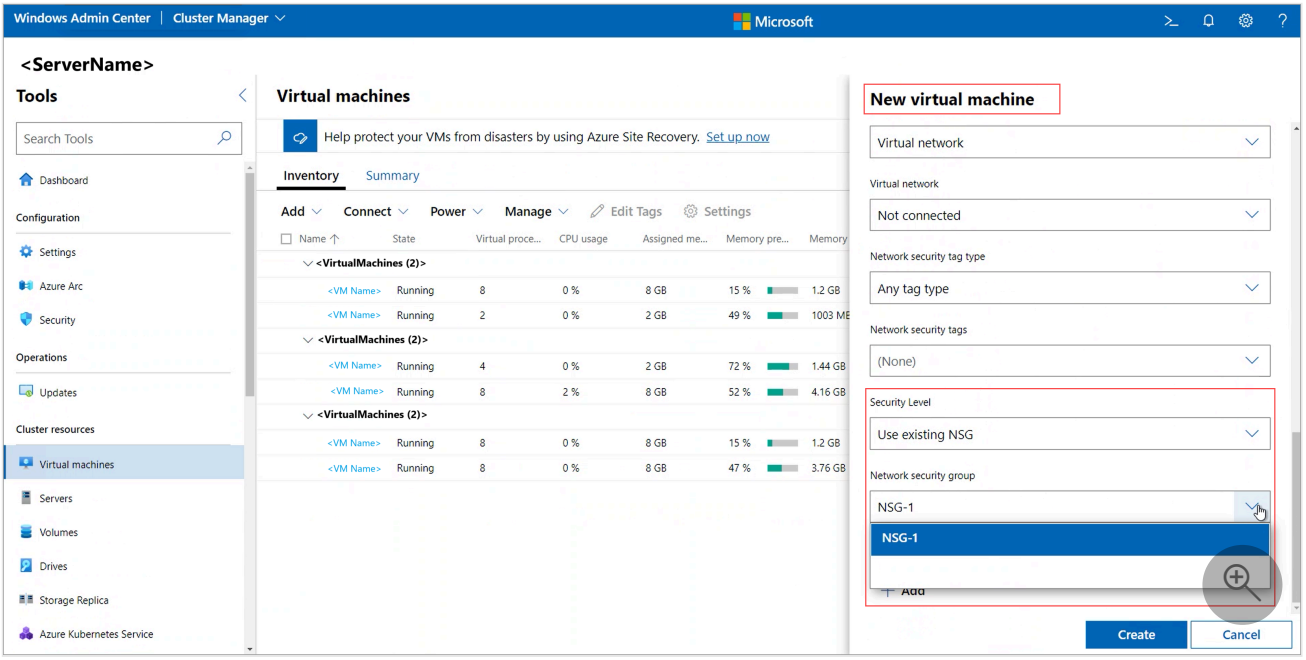


- **Ouvrez certains ports** : choisissez cette option pour utiliser les stratégies par défaut. Les stratégies par défaut bloquent tout accès entrant et autorisent tous les accès sortants. Vous

pouvez éventuellement activer l'accès entrant à un ou plusieurs ports bien définis, tels que HTTP, HTTPS, SSH ou RDP, en fonction de vos besoins.



- **Utiliser un NSG existant** - Choisissez cette option pour appliquer des stratégies personnalisées. Vous spécifiez un groupe de sécurité réseau (NSG) que vous avez déjà créé.



Machines virtuelles créées en dehors de Windows Admin Center

Vous pouvez rencontrer des problèmes lorsque vous créez des machines virtuelles en dehors de Windows Admin Center et activez les stratégies d'accès réseau par défaut. Par exemple, vous

pouvez activer les stratégies d'accès réseau par défaut et créer des machines virtuelles à l'aide de l'interface utilisateur Hyper-V ou de l'applet de commande PowerShell New-VM.

- Les machines virtuelles peuvent ne pas avoir de connectivité réseau. Étant donné que la machine virtuelle est gérée par une extension de commutateur Hyper-V appelée VFP (Virtual Filtering Platform), le port Hyper-V connecté à la machine virtuelle est bloqué par défaut.

  Pour débloquer le port, exécutez les commandes suivantes à partir d'une session PowerShell sur un hôte Hyper-V où se trouve la machine virtuelle :

  1. Exécutez PowerShell en tant qu'administrateur.

  2. Téléchargez et installez le module SdnDiagnostics . Exécutez la commande suivante :

     Azure PowerShell

     ```
     Install-Module -Name SdnDiagnostics
     ```

     Sinon, si elle est déjà installée, utilisez la commande suivante :

     Azure PowerShell

     ```
     Update-Module -Name SdnDiagnostics
     ```

     Acceptez toutes les invites à installer à partir de PowerShell Gallery .

  3. Vérifiez si le port VFP est appliqué à la machine virtuelle

     Azure PowerShell

     ```
     Get-SdnVMNetworkAdapterPortProfile -VMName <VMName>
     ```

     Vérifiez que les informations de profil de port VFP sont retournées pour l'adaptateur. Si ce n'est pas le cas, associez un profil de port.

  4. Spécifiez les ports à débloquer sur la machine virtuelle.

     Azure PowerShell

     ```
     Set-SdnVMNetworkAdapterPortProfile -VMName <VMName> -MacAddress <MACAddress>
     -ProfileId ([guid]::Empty) -ProfileData 2
     ```

- La machine virtuelle n’a pas de stratégies réseau par défaut appliquées. Étant donné que vous avez créé cette machine virtuelle en dehors de Windows Admin Center, les stratégies par défaut de la machine virtuelle ne sont pas appliquées et les **paramètres réseau** de la machine virtuelle ne s'affichent pas correctement. Pour corriger ce problème, procédez comme suit :

  Dans Windows Admin Center, créez un réseau logique. Créez un sous-réseau sous le réseau logique et ne fournissez pas d’ID de réseau local virtuel ou de préfixe de sous-réseau. Ensuite, attachez une machine virtuelle au réseau logique en procédant comme suit :

  1. Sous **Outils**, faites défiler vers le bas jusqu’à la **zone Réseau** , puis sélectionnez **Machines virtuelles**

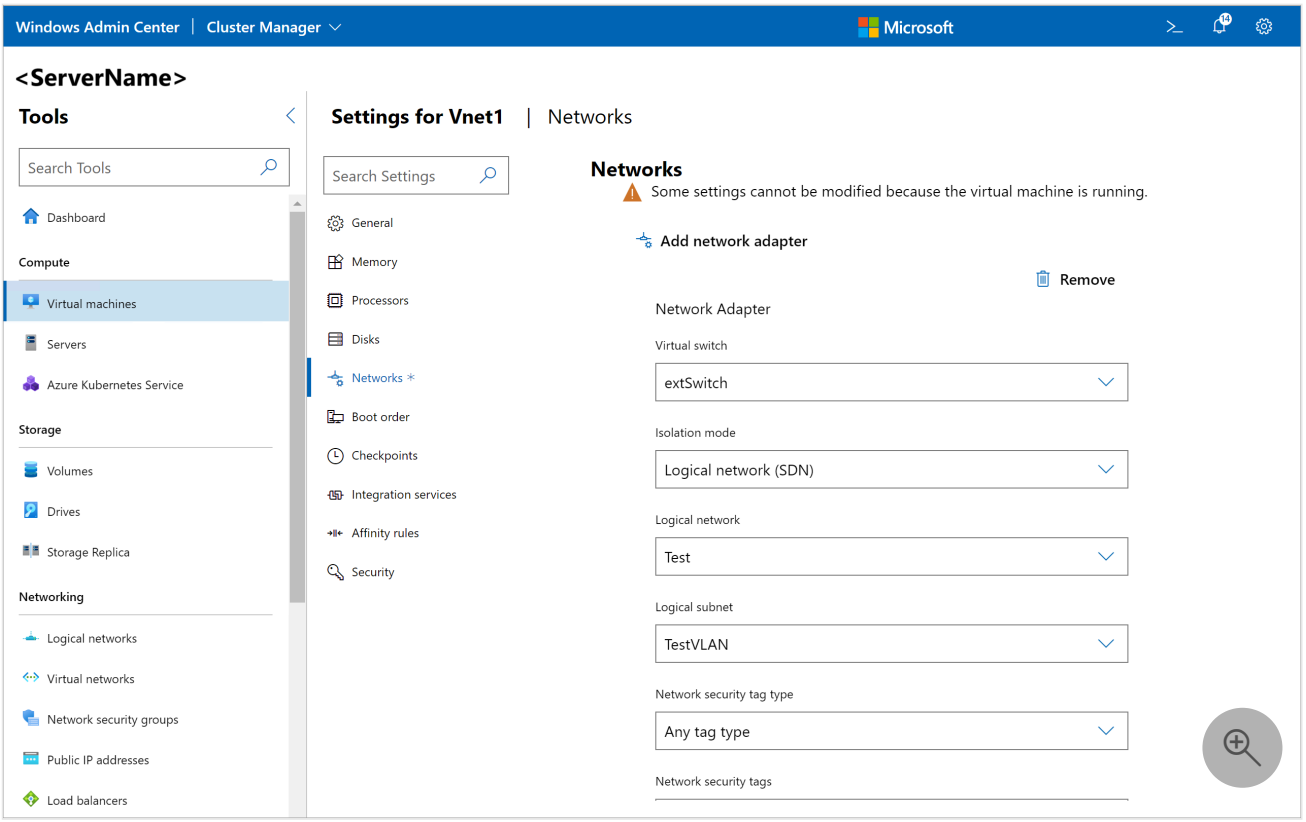
  2. Sélectionnez l’onglet **Inventaire** , sélectionnez la machine virtuelle, puis sélectionnez **Paramètres**.

  3. Sur la page **Paramètres**, cliquez sur **Réseaux**.

  4. Pour le mode d’isolation, sélectionnez **Réseau** logique.

  5. Sélectionnez le réseau logique et **le sous-réseau** logique que vous avez créés précédemment.

     a. Pour **le niveau** de sécurité, vous avez deux options :
        i. **Aucune protection : choisissez cette option** si vous ne souhaitez pas de stratégies d’accès réseau pour vos machines virtuelles.
        ii. **Utilisez un groupe de sécurité réseau (NSG) existant** : choisissez-le si vous souhaitez appliquer des stratégies d'accès réseau pour vos machines virtuelles. Vous pouvez créer un groupe de sécurité réseau et l’attacher à la machine virtuelle ou attacher n’importe quel groupe de sécurité réseau existant à la machine virtuelle.



Étapes suivantes

Pour en savoir plus :

- Configurer des groupes de sécurité réseau avec des balises

Dernière mise à jour : 15/09/2026

Gérer les réseaux virtuels locataires

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Vous pouvez utiliser les rubriques de cette section pour gérer les réseaux virtuels de virtualisation de réseau Hyper-V locataire après avoir déployé la mise en réseau définie par logiciel à l'aide de la rubrique Déployer une infrastructure de réseau défini par logiciel à l'aide de scripts.

Cette section contient les rubriques suivantes :

- Présentation de l'utilisation des réseaux virtuels et réseaux locaux virtuels (VLAN)
- Utiliser des listes de contrôle d'accès (ACL) pour gérer le flux de trafic réseau du centre de données
- Créer, supprimer ou mettre à jour des réseaux virtuels locataires
- Ajouter une passerelle virtuelle à un réseau virtuel locataire
- Connecter les points de terminaison de conteneur à un réseau virtuel locataire

---

Commentaires

Cette page a-t-elle été utile ? Yes No

Présentation de l'utilisation des réseaux virtuels et réseaux locaux virtuels

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Dans cette rubrique, vous allez découvrir les réseaux virtuels de virtualisation de réseau Hyper-V et leur différence entre les réseaux locaux virtuels (VLAN). Avec la virtualisation de réseau Hyper-V, vous créez des réseaux virtuels de superposition, également appelés réseaux virtuels.

La mise en réseau définie par logiciel (SDN) dans Windows Server 2016 est basée sur la stratégie de programmation pour la superposition de réseaux virtuels au sein d'un commutateur virtuel Hyper-V. Vous pouvez créer des réseaux virtuels de superposition, également appelés réseaux virtuels, avec virtualisation de réseau Hyper-V.

Lorsque vous déployez la virtualisation de réseau Hyper-V, les réseaux superposés sont créés en encapsulant la trame Ethernet de couche 2 de la machine virtuelle locataire d'origine avec un en-tête de superposition - ou de tunnel (par exemple, VXLAN ou NVGRE) et des en-têtes IP de couche 3 et Ethernet de couche 2 du réseau sous-jacent (ou physique). Les réseaux virtuels de superposition sont identifiés par un identificateur de Réseau virtuel (VNI) 24 bits pour maintenir l'isolation du trafic client et permettre le chevauchement des adresses IP. Le VNI se compose d'un ID de sous-réseau virtuel (VSID), d'un ID de commutateur logique et d'un ID de tunnel.

En outre, chaque locataire se voit attribuer un domaine de routage (similaire au routage et au transfert virtuels - VRF) afin que plusieurs préfixes de sous-réseaux virtuels (chacun représenté par un VNI) puissent être routés directement les uns vers les autres. Le routage interlocataire (ou domaine de routage croisé) n'est pas pris en charge sans passer par une passerelle.

Le réseau physique sur lequel le trafic encapsulé de chaque locataire est tunnelisé est représenté par un réseau logique appelé réseau logique du fournisseur. Ce réseau logique de fournisseur se compose d'un ou plusieurs sous-réseaux, chacun représenté par un préfixe IP et, éventuellement, une balise VLAN 802.1q.

Vous pouvez créer des réseaux logiques et des sous-réseaux supplémentaires à des fins d'infrastructure pour transporter le trafic de gestion, le trafic de stockage, le trafic de migration dynamique, etc.

Microsoft SDN ne prend pas en charge l'isolation des réseaux de locataires à l'aide de VLAN. L'isolation des locataires s'effectue uniquement à l'aide de la superposition de réseaux virtuels et de l'encapsulation de réseaux virtuels Hyper-V.

Commentaires

Cette page a-t-elle été utile ? Yes No

Configurer des groupes de sécurité réseau sur votre instance Azure Local avec PowerShell

> S'applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Cet article fournit des instructions pour configurer des groupes de sécurité réseau (NSG) pour gérer le flux de trafic de données à l'aide du pare-feu datacenter pour la mise en réseau SDN (Software Defined Networking) dans Azure Local à l'aide de Windows PowerShell. Vous activez et configurez le Pare-feu du centre de données en créant des groupes de sécurité réseau qui sont appliqués à un sous-réseau ou à une interface réseau.

Les exemples de scripts de cet article utilisent des commandes Windows PowerShell exportées à partir du module **NetworkController** . Vous pouvez également utiliser Windows Admin Center pour configurer et gérer des groupes de sécurité réseau.

Configurer le Pare-feu Datacenter de manière à autoriser tout le trafic

Une fois que vous avez déployé la mise en réseau SDN, vous devez tester la connectivité réseau de base dans votre nouvel environnement. Pour ce faire, créez une règle pour le Pare-feu Datacenter qui autorise tout le trafic réseau, sans restriction.

Utilisez les entrées du tableau suivant pour créer un ensemble de règles qui autorisent tout le trafic réseau entrant et sortant.

Agrandir le tableau

IP Source	IP de destination	Protocole	Port source	Port de destination	Sens	Action	Priorité
*	*	Tous	*	*	Trafic entrant	Autoriser	100
*	*	Tous	*	*	Règle de trafic sortant	Autoriser	110

Dans cet exemple, vous créez un groupe de sécurité réseau avec deux règles :

1. AllowAll_Inbound : permet à tout le trafic réseau de passer dans l'interface réseau où ce groupe de sécurité réseau est configuré.
2. **AllowAllOutbound** : autorise tout le trafic à passer hors de l'interface réseau. Ce groupe de sécurité réseau, identifié par l'ID de ressource « AllowAll-1 » est maintenant prêt à être utilisé dans les sous-réseaux virtuels et les interfaces réseau.

Vous pouvez exécuter cette commande à partir de n'importe quel ordinateur qui a accès au point de terminaison REST du contrôleur de réseau. Tout d'abord, ouvrez une session PowerShell. Dans cet exemple, utilisez l'applet de commande **Enter-PSSession** et remplacez `<computer-name>` par le nom de l'ordinateur disposant du point de terminaison REST du contrôleur de réseau.

PowerShell

```
Enter-PSSession <computer-name>
```

Ensuite, exécutez le script suivant pour créer le groupe de sécurité réseau :

PowerShell

```
$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "100"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"
$aclrule1 = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule1.Properties = $ruleproperties
$aclrule1.ResourceId = "AllowAll_Inbound"
$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "110"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"
$aclrule2 = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule2.Properties = $ruleproperties
$aclrule2.ResourceId = "AllowAll_Outbound"
$acllistproperties = new-object
```

```
Microsoft.Windows.NetworkController.AccessControlListProperties
$acllistproperties.AclRules = @($aclrule1, $aclrule2)
New-NetworkControllerAccessControlList -ResourceId "AllowAll" -Properties
$acllistproperties -ConnectionUri <NC REST FQDN>
```

> **Remarque**
>
> La référence de commande Windows PowerShell pour le contrôleur de réseau se trouve dans les applets de commande du contrôleur de réseau.

Utiliser des groupes de sécurité réseau pour limiter le trafic sur un sous-réseau

Dans cet exemple, vous créez un groupe de sécurité réseau qui empêche les machines virtuelles de communiquer entre elles dans le sous-réseau 192.168.0.0/24. Ce type de groupe de sécurité réseau est utile pour limiter la capacité d'un attaquant à se propager ultérieurement au sein du sous-réseau, tout en permettant aux machines virtuelles de recevoir des demandes provenant de l'extérieur du sous-réseau et de communiquer avec d'autres services sur d'autres sous-réseaux.

Agrandir le tableau

IP Source	IP de destination	Protocole	Port source	Port de destination	Sens	Action	Priorité
192.168.0.1	*	Tous	*	*	Trafic entrant	Autoriser	100
*	192.168.0.1	Tous	*	*	Règle de trafic sortant	Autoriser	101
192.168.0.0/24	*	Tous	*	*	Trafic entrant	Bloquer	102
*	192.168.0.0/24	Tous	*	*	Règle de trafic sortant	Bloquer	1:03
*	*	Tous	*	*	Trafic entrant	Autoriser	104
*	*	Tous	*	*	Règle de trafic sortant	Autoriser	105

Le groupe de sécurité réseau créé par l'exemple de script ci-dessous, identifié par l'ID de ressource **Subnet-192-168-0-0**, peut désormais être appliqué à un sous-réseau de réseau virtuel qui utilise l'adresse de sous-réseau « 192.168.0.0/24 ». Toute interface réseau attachée à ce sous-réseau de réseau virtuel obtient automatiquement les règles de groupe de sécurité réseau ci-dessus appliquées.

Voici un exemple de script pour créer ce groupe de sécurité réseau à l'aide de l'API REST du contrôleur de réseau :

PowerShell

```
import-module networkcontroller
$ncURI = "https://mync.contoso.local"
$aclrules = @()

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "192.168.0.1"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "100"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowRouter_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "192.168.0.1"
$ruleproperties.Priority = "101"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowRouter_Outbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
```

```
$ruleproperties.Action = "Deny"
$ruleproperties.SourceAddressPrefix = "192.168.0.0/24"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "102"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "DenySubnet_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Deny"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "192.168.0.0/24"
$ruleproperties.Priority = "103"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "DenySubnet_Outbound"

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "104"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowAll_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "105"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
```

```
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowAll_Outbound"
$aclrules += $aclrule

$acllistproperties = new-object
Microsoft.Windows.NetworkController.AccessControlListProperties
$acllistproperties.AclRules = $aclrules

New-NetworkControllerAccessControlList -ResourceId "Subnet-192-168-0-0" -Properties
$acllistproperties -ConnectionUri $ncURI
```

Ajouter un groupe de sécurité réseau à une interface réseau

Une fois que vous avez créé un groupe de sécurité réseau et que vous l'avez affecté à un sous-réseau virtuel, vous pouvez remplacer ce groupe de sécurité réseau par défaut sur le sous-réseau virtuel par un groupe de sécurité réseau spécifique pour une interface réseau individuelle. À compter de Windows Server 2019 Datacenter, vous pouvez appliquer des groupes de sécurité réseau spécifiques directement aux interfaces réseau attachées aux réseaux logiques SDN, en plus des réseaux virtuels SDN. Si vous avez défini des groupes de sécurité réseau sur le sous-réseau virtuel connecté à l'interface réseau, les deux groupes de sécurité réseau sont appliqués et les groupes de sécurité réseau d'interface réseau sont hiérarchisés au-dessus des groupes de sécurité réseau de sous-réseau virtuel.

Dans cet exemple, nous montrons comment ajouter un groupe de sécurité réseau à un réseau virtuel.

> **Conseil**
>
> Il est également possible d'ajouter un groupe de sécurité réseau en même temps que vous créez l'interface réseau.

1. Obtenez ou créez l'interface réseau à laquelle vous ajouterez le groupe de sécurité réseau.

   PowerShell

   ```
   $nic = get-networkcontrollernetworkinterface -ConnectionUri $uri -ResourceId
   "MyVM_Ethernet1"
   ```

2. Obtenez ou créez le groupe de sécurité réseau que vous allez ajouter à l'interface réseau.

   PowerShell

```
$acl = get-networkcontrolleraccesscontrollist -ConnectionUri $uri -ResourceId
"AllowAllACL"
```

3. Affectez le groupe de sécurité réseau à la propriété AccessControlList de l'interface réseau.

PowerShell

```
 $nic.properties.ipconfigurations[0].properties.AccessControlList = $acl
```

4. Ajoutez l'interface réseau dans le Contrôleur de réseau.

PowerShell

```
new-networkcontrollernetworkinterface -ConnectionUri $uri -Properties
$nic.properties -ResourceId $nic.resourceid
```

Supprimer un groupe de sécurité réseau d'une interface réseau

Dans cet exemple, nous vous montrons comment supprimer un groupe de sécurité réseau d'une interface réseau. La suppression d'un groupe de sécurité réseau applique l'ensemble de règles par défaut à l'interface réseau. L'ensemble de règles par défaut autorise tout le trafic sortant, mais bloque tout le trafic entrant. Si vous souhaitez autoriser tout le trafic entrant, vous devez suivre l'exemple précédent pour ajouter un groupe de sécurité réseau qui autorise tous les trafics entrants et sortants.

1. Obtenez l'interface réseau à partir de laquelle vous allez supprimer le groupe de sécurité réseau.

PowerShell

```
$nic = get-networkcontrollernetworkinterface -ConnectionUri $uri -ResourceId
"MyVM_Ethernet1"
```

2. Attribuez $null à la propriété AccessControlList d'ipConfiguration.

PowerShell

```
$nic.properties.ipconfigurations[0].properties.AccessControlList = $null
```

3. Ajoutez l'objet d'interface réseau dans le Contrôleur de réseau.

PowerShell

```
new-networkcontrollernetworkinterface -ConnectionUri $uri -Properties
$nic.properties -ResourceId $nic.resourceid
```

Audit du pare-feu

La fonctionnalité d'audit du pare-feu du pare-feu du centre de données enregistre tout flux traité par les règles de pare-feu SDN. Tous les groupes de sécurité réseau activés pour la journalisation sont enregistrés. Les fichiers journaux doivent se trouver dans une syntaxe cohérente avec les journaux de flux Azure Network Watcher. Ces journaux peuvent être utilisés à des fins de diagnostic ou archivés en vue d'une analyse ultérieure.

Voici un exemple de script pour activer l'audit du pare-feu sur les machines hôtes. Mettez à jour les variables au début et exécutez-la sur une instance locale Azure avec le contrôleur de réseau déployé :

PowerShell

```
$logpath = "C:\test\log1"
$servers = @("sa18n22-2", "sa18n22-3", "sa18n22-4")
$uri = "https://sa18n22sdn.sa18.nttest.microsoft.com"

# Create log directories on the hosts
invoke-command -Computername $servers  {
    param(
        $Path
    )
    mkdir $path    -force
} -argumentlist $LogPath

# Set firewall auditing settings on Network Controller
$AuditProperties = new-object
Microsoft.Windows.NetworkController.AuditingSettingsProperties
$AuditProperties.OutputDirectory = $logpath
set-networkcontrolleauditingsettingsconfiguration -connectionuri $uri -properties
$AuditProperties -force  | out-null

# Enable logging on each server
$servers = get-networkcontrollerserver -connectionuri $uri
foreach ($s in $servers) {
    $s.properties.AuditingEnabled = @("Firewall")
    new-networkcontrollerserver -connectionuri $uri -resourceid $s.resourceid -
properties $s.properties -force | out-null
}
```

Une fois activé, un nouveau fichier apparaît dans le répertoire spécifié de chaque hôte environ une fois par heure. Vous devez régulièrement traiter ces fichiers et les supprimer des hôtes. La longueur du fichier actuel est nulle et il est verrouillé jusqu'à ce qu'il soit vidé à l'heure suivante :

syntax

```
PS C:\test\log1> dir

    Directory: C:\test\log1

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/19/2018   6:28 AM          17055 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL122803093.json
-a----        7/19/2018   7:28 AM           7880 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL132803173.json
-a----        7/19/2018   8:28 AM           7867 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL142803264.json
-a----        7/19/2018   9:28 AM          10949 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL152803360.json
-a----        7/19/2018   9:28 AM              0 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL162803464.json
```

Ces fichiers contiennent une séquence d'événements de flux, par exemple :

syntax


```
{
    "records": [
        {
            "properties":{
                "Version":"1.0",
                "flows":[
                    {
                        "flows":[
                            {
                                "flowTuples":
["1531963580,192.122.0.22,192.122.255.255,138,138,U,I,A"],
                                "portId":"9",
                                "portName":"7290436D-0422-498A-8EB8-C6CF5115DACE"
                            }
                        ],
                        "rule":"Allow_Inbound"
                    }
                ]
            },
            "operationName":"NetworkSecurityGroupFlowEvents",
            "resourceId":"a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1",
            "time":"20180719:L012620622",
            "category":"NetworkSecurityGroupFlowEvent",
```

```
            "systemId":"d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a"
            },
```

Notez que la journalisation a lieu uniquement pour les règles dont la **journalisation** est **activée**, par exemple :

syntax

```
{
    "Tags":  null,
    "ResourceRef":  "/accessControlLists/AllowAll",
    "InstanceId":  "4a63e1a5-3264-4986-9a59-4e77a8b107fa",
    "Etag":  "W/\"1535a780-0fc8-4bba-a15a-093ecac9b88b\"",
    "ResourceMetadata":  null,
    "ResourceId":  "AllowAll",
    "Properties":  {
                        "ConfigurationState":  null,
                        "ProvisioningState":  "Succeeded",
                        "AclRules":  [
                                        {
                                            "ResourceMetadata":  null,
                                            "ResourceRef":
"/accessControlLists/AllowAll/aclRules/AllowAll_Inbound",
                                            "InstanceId":  "ba8710a8-0f01-422b-9038-
d1f2390645d7",
                                            "Etag":  "W/\"1535a780-0fc8-4bba-a15a-
093ecac9b88b\"",
                                            "ResourceId":  "AllowAll_Inbound",
                                            "Properties":  {
                                                                "Protocol":  "All",
                                                                "SourcePortRange":  "0-
65535",
                                                                "DestinationPortRange":
"0-65535",
                                                                "Action":  "Allow",
                                                                "SourceAddressPrefix":
"*",
                                                                "DestinationAddressPrefix":  "*",
                                                                "Priority":  "101",
                                                                "Description":  null,
                                                                "Type":  "Inbound",
                                                                "Logging":  "Enabled",
                                                                "ProvisioningState":
"Succeeded"
                                                            }
                                        },
                                        {
                                            "ResourceMetadata":  null,
                                            "ResourceRef":
"/accessControlLists/AllowAll/aclRules/AllowAll_Outbound",
                                            "InstanceId":  "068264c6-2186-4dbc-bbe7-
f504c6f47fa8",
```

```
                                                "Etag":  "W/\"1535a780-0fc8-4bba-a15a-
093ecac9b88b\"",
                                                "ResourceId":  "AllowAll_Outbound",
                                                "Properties":  {
                                                                    "Protocol":  "All",
                                                                    "SourcePortRange":  "0-
65535",
                                                                    "DestinationPortRange":
"0-65535",
                                                                    "Action":  "Allow",
                                                                    "SourceAddressPrefix":
"*",
                                                                    "DestinationAddressPrefix":  "*",
                                                                    "Priority":  "110",
                                                                    "Description":  null,
                                                                    "Type":  "Outbound",
                                                                    "Logging":  "Enabled",
                                                                    "ProvisioningState":
"Succeeded"
                                                                }
                                            }
                                        ],
                        "IpConfigurations":  [
                                                ],
                        "Subnets":  [
                                            {
                                                "ResourceMetadata":  null,
                                                "ResourceRef":
"/virtualNetworks/10_0_1_0/subnets/Subnet1",
                                                "InstanceId":  "00000000-0000-0000-0000-
000000000000",
                                                "Etag":  null,
                                                "ResourceId":  null,
                                                "Properties":  null
                                            }
                                        ]
                    }
}
```


Étapes suivantes

Pour plus d'informations, consultez :

- Vue d'ensemble du pare-feu du centre de données.
- Vue d'ensemble du contrôleur de réseau.
- SDN dans Azure Local et Windows Server.

Dernière mise à jour : 15/09/2026

Créer, supprimer ou mettre à jour des réseaux virtuels locataires

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans cette rubrique, vous allez découvrir comment créer, supprimer et mettre à jour des réseaux virtuels basés sur la fonctionnalité Virtualisation de réseau Hyper-V après avoir déployé une solution SDN (Software-Defined Networking). La fonctionnalité Virtualisation de réseau Hyper-V vous permet d'isoler les réseaux de locataires pour que chacun d'entre eux constitue une entité distincte. Les entités ne peuvent pas être connectées entre elles, sauf si vous configurez des charges de travail d'accès public.

Créer un réseau virtuel

La création d'un réseau virtuel pour un locataire permet de placer celui-ci au sein d'un domaine de routage unique sur l'hôte Hyper-V. Sous chaque réseau virtuel, il existe au moins un sous-réseau virtuel. Les sous-réseaux virtuels sont définis par un préfixe IP et référencent une liste ACL définie au préalable.

Les étapes de création d'un réseau virtuel sont les suivantes :

1. Identifiez les préfixes d'adresses IP à partir desquels vous souhaitez créer les sous-réseaux virtuels.
2. Identifiez le réseau du fournisseur logique sur lequel le trafic du locataire est tunnelisé.
3. Créez au moins un sous-réseau virtuel pour chaque préfixe IP identifié à l'étape 1.
4. (Facultatif) Ajoutez les listes ACL créées aux sous-réseaux virtuels, ou ajoutez une connectivité de passerelle pour les locataires.

Le tableau suivant comprend des exemples d'ID de sous-réseau et de préfixes pour deux locataires fictifs. Le locataire Fabrikam a deux sous-réseaux virtuels, tandis que le locataire Contoso a trois sous-réseaux virtuels.

Agrandir le tableau

Nom du locataire	ID de sous-réseau virtuel	Préfixe de sous-réseau virtuel
Fabrikam	5001	24.30.1.0/24
Fabrikam	5002	24.30.2.0/20

Nom du locataire	ID de sous-réseau virtuel	Préfixe de sous-réseau virtuel
Contoso	6001	24.30.1.0/24
Contoso	6002	24.30.2.0/24
Contoso	6003	24.30.3.0/24

L'exemple de script suivant utilise des commandes Windows PowerShell exportées à partir du module **NetworkController** pour créer le réseau virtuel de Contoso et un sous-réseau :

Powershell

```
import-module networkcontroller
$URI = "https://ncrest.contoso.local"

#Find the HNV Provider Logical Network

$logicalnetworks = Get-NetworkControllerLogicalNetwork -ConnectionUri $uri
foreach ($ln in $logicalnetworks) {
   if ($ln.Properties.NetworkVirtualizationEnabled -eq "True") {
      $HNVProviderLogicalNetwork = $ln
   }
}

#Find the Access Control List to user per virtual subnet

$acllist = Get-NetworkControllerAccessControlList -ConnectionUri $uri -ResourceId
"AllowAll"

#Create the Virtual Subnet

$vsubnet = new-object Microsoft.Windows.NetworkController.VirtualSubnet
$vsubnet.ResourceId = "Contoso_WebTier"
$vsubnet.Properties = new-object
Microsoft.Windows.NetworkController.VirtualSubnetProperties
$vsubnet.Properties.AccessControlList = $acllist
$vsubnet.Properties.AddressPrefix = "24.30.1.0/24"

#Create the Virtual Network

$vnetproperties = new-object
Microsoft.Windows.NetworkController.VirtualNetworkProperties
$vnetproperties.AddressSpace = new-object
Microsoft.Windows.NetworkController.AddressSpace
$vnetproperties.AddressSpace.AddressPrefixes = @("24.30.1.0/24")
$vnetproperties.LogicalNetwork = $HNVProviderLogicalNetwork
$vnetproperties.Subnets = @($vsubnet)
New-NetworkControllerVirtualNetwork -ResourceId "Contoso_VNet1" -ConnectionUri
$uri -Properties $vnetproperties
```

Modifier un réseau virtuel existant

Vous pouvez utiliser Windows PowerShell pour mettre à jour un sous-réseau ou un réseau virtuel existant.

Quand vous exécutez l'exemple de script suivant, les ressources mises à jour sont simplement placées sur le Contrôleur de réseau avec le même ID de ressource. Si votre locataire Contoso souhaite ajouter un nouveau sous-réseau virtuel (24.30.2.0/24) à son réseau virtuel, vous ou l'administrateur Contoso pouvez utiliser le script suivant.

PowerShell

```
$acllist = Get-NetworkControllerAccessControlList -ConnectionUri $uri -ResourceId
"AllowAll"

$vnet = Get-NetworkControllerVirtualNetwork -ResourceId "Contoso_VNet1" -
ConnectionUri $uri

$vnet.properties.AddressSpace.AddressPrefixes += "24.30.2.0/24"

$vsubnet = new-object Microsoft.Windows.NetworkController.VirtualSubnet
$vsubnet.ResourceId = "Contoso_DBTier"
$vsubnet.Properties = new-object
Microsoft.Windows.NetworkController.VirtualSubnetProperties
$vsubnet.Properties.AccessControlList = $acllist
$vsubnet.Properties.AddressPrefix = "24.30.2.0/24"

$vnet.properties.Subnets += $vsubnet

New-NetworkControllerVirtualNetwork -ResourceId "Contoso_VNet1" -ConnectionUri
$uri -properties $vnet.properties
```

Supprimer un réseau virtuel

Vous pouvez utiliser Windows PowerShell pour supprimer un réseau virtuel.

L'exemple Windows PowerShell suivant permet de supprimer un réseau virtuel de locataire en émettant une requête de suppression HTTP vers l'URI de l'ID de ressource.

PowerShell

```
Remove-NetworkControllerVirtualNetwork -ResourceId "Contoso_Vnet1" -ConnectionUri
$uri
```

Ajouter une passerelle virtuelle à un réseau virtuel locataire

29/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Découvrez comment utiliser les applets de commande et les scripts Windows PowerShell pour fournir une connectivité de site à site aux réseaux virtuels de votre locataire. Dans cette rubrique, vous allez utiliser le Contrôleur de réseau pour ajouter des passerelles virtuelles de locataire à des instances de passerelle RAS membres de pools de passerelles. La passerelle RAS prend en charge jusqu'à 100 locataires, en fonction de la bande passante utilisée par chaque locataire. Le Contrôleur de réseau détermine automatiquement la meilleure passerelle RAS à utiliser quand vous déployez une nouvelle passerelle virtuelle pour vos locataires.

Chaque passerelle virtuelle correspond à un locataire particulier et se compose d'une ou de plusieurs connexions réseau (tunnels VPN de site à site) et, éventuellement, de connexions BGP (Border Gateway Protocol). Quand vous fournissez une connectivité de site à site, vos clients peuvent connecter leur réseau virtuel locataire à un réseau externe, par exemple un réseau d'entreprise locataire, un réseau de fournisseur de services ou Internet.

Quand vous déployez une passerelle virtuelle de locataire, vous disposez des options de configuration suivantes :

Agrandir le tableau

Options de connexion réseau	Options de configuration de BGP
• Réseau privé virtuel (VPN) de site à site IPsec • Encapsulation de routage générique (GRE) • Transfert de couche 3	• Configuration du routeur BGP • Configuration du pair BGP • Configuration des stratégies de routage BGP

Les exemples de scripts et de commandes Windows PowerShell de cette rubrique montrent comment déployer une passerelle virtuelle de locataire sur une passerelle RAS avec chacune de ces options.

> **Important**
>
> Avant d'exécuter l'un des exemples de commandes et de scripts Windows PowerShell fournis, vous devez changer toutes les valeurs des variables pour qu'elles soient

appropriées à votre déploiement.

1. Vérifiez que l'objet de pool de passerelles existe dans le Contrôleur de réseau.

PowerShell

```
$uri = "https://ncrest.contoso.com"

# Retrieve the Gateway Pool configuration
$gwPool = Get-NetworkControllerGatewayPool -ConnectionUri $uri

# Display in JSON format
$gwPool | ConvertTo-Json -Depth 2
```

2. Vérifiez que le sous-réseau utilisé pour le routage des paquets hors du réseau virtuel du locataire existe dans le Contrôleur de réseau. Récupérez également le sous-réseau virtuel utilisé pour le routage entre la passerelle de locataire et le réseau virtuel.

PowerShell

```
$uri = "https://ncrest.contoso.com"

# Retrieve the Tenant Virtual Network configuration
$Vnet = Get-NetworkControllerVirtualNetwork -ConnectionUri $uri  -ResourceId
"Contoso_Vnet1"

# Display in JSON format
$Vnet | ConvertTo-Json -Depth 4

# Retrieve the Tenant Virtual Subnet configuration
$RoutingSubnet = Get-NetworkControllerVirtualSubnet -ConnectionUri $uri  -
ResourceId "Contoso_WebTier" -VirtualNetworkID $vnet.ResourceId

# Display in JSON format
$RoutingSubnet | ConvertTo-Json -Depth 4
```

3. Créez un objet pour la passerelle virtuelle de locataire, puis mettez à jour la référence du pool de passerelles. Spécifiez également le sous-réseau virtuel utilisé pour le routage entre la passerelle et le réseau virtuel. Une fois que vous avez spécifié le sous-réseau virtuel, mettez à jour le reste des propriétés de l'objet de passerelle virtuelle, puis ajoutez la nouvelle passerelle virtuelle pour le locataire.

PowerShell

```
# Create a new object for Tenant Virtual Gateway
$VirtualGWProperties = New-Object
```

```
Microsoft.Windows.NetworkController.VirtualGatewayProperties

# Update Gateway Pool reference
$VirtualGWProperties.GatewayPools = @()
$VirtualGWProperties.GatewayPools += $gwPool

# Specify the Virtual Subnet that is to be used for routing between the
gateway and Virtual Network
$VirtualGWProperties.GatewaySubnets = @()
$VirtualGWProperties.GatewaySubnets += $RoutingSubnet

# Update the rest of the Virtual Gateway object properties
$VirtualGWProperties.RoutingType = "Dynamic"
$VirtualGWProperties.NetworkConnections = @()
$VirtualGWProperties.BgpRouters = @()

# Add the new Virtual Gateway for tenant
$virtualGW = New-NetworkControllerVirtualGateway -ConnectionUri $uri  -
ResourceId "Contoso_VirtualGW" -Properties $VirtualGWProperties -Force
```

4. Créez une connexion VPN de site à site avec la redirection IPsec, GRE ou L3 (Couche 3).

> **Conseil**
>
> Vous pouvez éventuellement regrouper toutes les étapes précédentes et configurer une passerelle virtuelle de locataire avec les trois options de connexion. Pour plus d'informations, consultez Configurer une passerelle avec les trois types de connexion (IPsec, GRE, L3) et BGP.

> **Notes**
>
> `PerfectForwardSecrecy` doit correspondre aux sites locaux et distants.

Connexion réseau VPN de site à site IPsec

PowerShell

```
# Create a new object for Tenant Network Connection
$nwConnectionProperties = New-Object
Microsoft.Windows.NetworkController.NetworkConnectionProperties

# Update the common object properties
$nwConnectionProperties.ConnectionType = "IPSec"
$nwConnectionProperties.OutboundKiloBitsPerSecond = 10000
$nwConnectionProperties.InboundKiloBitsPerSecond = 10000

# Update specific properties depending on the Connection Type
```

```
$nwConnectionProperties.IpSecConfiguration = New-Object
Microsoft.Windows.NetworkController.IpSecConfiguration
$nwConnectionProperties.IpSecConfiguration.AuthenticationMethod = "PSK"
$nwConnectionProperties.IpSecConfiguration.SharedSecret = "P@ssw0rd"

$nwConnectionProperties.IpSecConfiguration.QuickMode = New-Object
Microsoft.Windows.NetworkController.QuickMode
$nwConnectionProperties.IpSecConfiguration.QuickMode.PerfectForwardSecrecy =
"PFS2048"
$nwConnectionProperties.IpSecConfiguration.QuickMode.AuthenticationTransforma
tionConstant = "SHA256128"
$nwConnectionProperties.IpSecConfiguration.QuickMode.CipherTransformationCons
tant = "DES3"
$nwConnectionProperties.IpSecConfiguration.QuickMode.SALifeTimeSeconds = 1233
$nwConnectionProperties.IpSecConfiguration.QuickMode.IdleDisconnectSeconds =
500
$nwConnectionProperties.IpSecConfiguration.QuickMode.SALifeTimeKiloBytes =
1048576

$nwConnectionProperties.IpSecConfiguration.MainMode = New-Object
Microsoft.Windows.NetworkController.MainMode
$nwConnectionProperties.IpSecConfiguration.MainMode.DiffieHellmanGroup =
"Group2"
$nwConnectionProperties.IpSecConfiguration.MainMode.IntegrityAlgorithm =
"SHA256"
$nwConnectionProperties.IpSecConfiguration.MainMode.EncryptionAlgorithm =
"AES256"
$nwConnectionProperties.IpSecConfiguration.MainMode.SALifeTimeSeconds = 1234
$nwConnectionProperties.IpSecConfiguration.MainMode.SALifeTimeKiloBytes =
1048576

# L3 specific configuration (leave blank for IPSec)
$nwConnectionProperties.IPAddresses = @()
$nwConnectionProperties.PeerIPAddresses = @()

# Update the IPv4 Routes that are reachable over the site-to-site VPN Tunnel
$nwConnectionProperties.Routes = @()
$ipv4Route = New-Object Microsoft.Windows.NetworkController.RouteInfo
$ipv4Route.DestinationPrefix = "14.1.10.1/32"
$ipv4Route.metric = 10
$nwConnectionProperties.Routes += $ipv4Route

# Tunnel Destination (Remote Endpoint) Address
$nwConnectionProperties.DestinationIPAddress = "10.127.134.121"

# Add the new Network Connection for the tenant
New-NetworkControllerVirtualGatewayNetworkConnection -ConnectionUri $uri -
VirtualGatewayId $virtualGW.ResourceId -ResourceId "Contoso_IPSecGW" -
Properties $nwConnectionProperties -Force
```

Connexion réseau VPN de site à site GRE

PowerShell

```
# Create a new object for the Tenant Network Connection
$nwConnectionProperties = New-Object
Microsoft.Windows.NetworkController.NetworkConnectionProperties

# Update the common object properties
$nwConnectionProperties.ConnectionType = "GRE"
$nwConnectionProperties.OutboundKiloBitsPerSecond = 10000
$nwConnectionProperties.InboundKiloBitsPerSecond = 10000

# Update specific properties depending on the Connection Type
$nwConnectionProperties.GreConfiguration = New-Object
Microsoft.Windows.NetworkController.GreConfiguration
$nwConnectionProperties.GreConfiguration.GreKey = 1234

# Update the IPv4 Routes that are reachable over the site-to-site VPN Tunnel
$nwConnectionProperties.Routes = @()
$ipv4Route = New-Object Microsoft.Windows.NetworkController.RouteInfo
$ipv4Route.DestinationPrefix = "14.2.20.1/32"
$ipv4Route.metric = 10
$nwConnectionProperties.Routes += $ipv4Route

# Tunnel Destination (Remote Endpoint) Address
$nwConnectionProperties.DestinationIPAddress = "10.127.134.122"

# L3 specific configuration (leave blank for GRE)
$nwConnectionProperties.L3Configuration = New-Object
Microsoft.Windows.NetworkController.L3Configuration
$nwConnectionProperties.IPAddresses = @()
$nwConnectionProperties.PeerIPAddresses = @()

# Add the new Network Connection for the tenant
New-NetworkControllerVirtualGatewayNetworkConnection -ConnectionUri $uri -
VirtualGatewayId $virtualGW.ResourceId -ResourceId "Contoso_GreGW" -
Properties $nwConnectionProperties -Force
```

Connexion réseau de redirection L3

Pour qu'une connexion réseau de redirection L3 fonctionne correctement, vous devez configurer un réseau logique correspondant.

a. Configurez un réseau logique pour la connexion réseau de redirection L3.

PowerShell

```
# Create a new object for the Logical Network to be used for L3 Forwarding
$lnProperties = New-Object
Microsoft.Windows.NetworkController.LogicalNetworkProperties

$lnProperties.NetworkVirtualizationEnabled = $false
```

```
$lnProperties.Subnets = @()

# Create a new object for the Logical Subnet to be used for L3 Forwarding
and update properties
$logicalsubnet = New-Object
Microsoft.Windows.NetworkController.LogicalSubnet
$logicalsubnet.ResourceId = "Contoso_L3_Subnet"
$logicalsubnet.Properties = New-Object
Microsoft.Windows.NetworkController.LogicalSubnetProperties
$logicalsubnet.Properties.VlanID = 1001
$logicalsubnet.Properties.AddressPrefix = "10.127.134.0/25"
$logicalsubnet.Properties.DefaultGateways = "10.127.134.1"

$lnProperties.Subnets += $logicalsubnet

# Add the new Logical Network to Network Controller
$vlanNetwork = New-NetworkControllerLogicalNetwork -ConnectionUri $uri -
ResourceId "Contoso_L3_Network" -Properties $lnProperties -Force
```

b. Créez un objet JSON de connexion réseau, puis ajoutez-le au Contrôleur de réseau.

PowerShell

```
# Create a new object for the Tenant Network Connection
$nwConnectionProperties = New-Object
Microsoft.Windows.NetworkController.NetworkConnectionProperties

# Update the common object properties
$nwConnectionProperties.ConnectionType = "L3"
$nwConnectionProperties.OutboundKiloBitsPerSecond = 10000
$nwConnectionProperties.InboundKiloBitsPerSecond = 10000

# GRE specific configuration (leave blank for L3)
$nwConnectionProperties.GreConfiguration = New-Object
Microsoft.Windows.NetworkController.GreConfiguration

# Update specific properties depending on the Connection Type
$nwConnectionProperties.L3Configuration = New-Object
Microsoft.Windows.NetworkController.L3Configuration
$nwConnectionProperties.L3Configuration.VlanSubnet =
$vlanNetwork.properties.Subnets[0]

$nwConnectionProperties.IPAddresses = @()
$localIPAddress = New-Object
Microsoft.Windows.NetworkController.CidrIPAddress
$localIPAddress.IPAddress = "10.127.134.55"
$localIPAddress.PrefixLength = 25
$nwConnectionProperties.IPAddresses += $localIPAddress

$nwConnectionProperties.PeerIPAddresses = @("10.127.134.65")

# Update the IPv4 Routes that are reachable over the site-to-site VPN
```

```
Tunnel
$nwConnectionProperties.Routes = @()
$ipv4Route = New-Object Microsoft.Windows.NetworkController.RouteInfo
$ipv4Route.DestinationPrefix = "14.2.20.1/32"
$ipv4Route.metric = 10
$nwConnectionProperties.Routes += $ipv4Route

# Add the new Network Connection for the tenant
New-NetworkControllerVirtualGatewayNetworkConnection -ConnectionUri $uri -
VirtualGatewayId $virtualGW.ResourceId -ResourceId "Contoso_L3GW" -
Properties $nwConnectionProperties -Force
```

5. Configurez la passerelle en tant que routeur BGP, puis ajoutez-la au Contrôleur de réseau.

   a. Ajoutez un routeur BGP pour le locataire.

PowerShell

```
# Create a new object for the Tenant BGP Router
$bgpRouterproperties = New-Object
Microsoft.Windows.NetworkController.VGwBgpRouterProperties

# Update the BGP Router properties
$bgpRouterproperties.ExtAsNumber = "0.64512"

# Add the new BGP Router for the tenant
$bgpRouter = New-NetworkControllerVirtualGatewayBgpRouter -ConnectionUri
$uri -VirtualGatewayId $virtualGW.ResourceId -ResourceId
"Contoso_BgpRouter1" -Properties $bgpRouterProperties -Force
```

   b. Ajoutez un pair BGP pour ce locataire, qui correspond à la connexion réseau VPN de site à site ajoutée ci-dessus.

PowerShell

```
# Create a new object for Tenant BGP Peer
$bgpPeerProperties = New-Object
Microsoft.Windows.NetworkController.VGwBgpPeerProperties

# Update the BGP Peer properties
$bgpPeerProperties.PeerIpAddress = "14.1.10.1"
$bgpPeerProperties.AsNumber = 64521
$bgpPeerProperties.ExtAsNumber = "0.64521"

# Add the new BGP Peer for tenant
New-NetworkControllerVirtualGatewayBgpPeer -ConnectionUri $uri -
VirtualGatewayId $virtualGW.ResourceId -BgpRouterName $bgpRouter.ResourceId
```

```
-ResourceId "Contoso_IPSec_Peer" -Properties $bgpPeerProperties -Force
```

(Étape facultative) Configurer une passerelle avec les trois types de connexion (IPsec, GRE, L3) et BGP

Vous pouvez éventuellement regrouper toutes les étapes précédentes et configurer une passerelle virtuelle de locataire avec les trois options de connexion :

> **Notes**
>
> `PerfectForwardSecrecy` doit correspondre aux sites locaux et distants.

PowerShell

```
# Create a new Virtual Gateway Properties type object
$VirtualGWProperties = New-Object
Microsoft.Windows.NetworkController.VirtualGatewayProperties

# Update GatewayPool reference
$VirtualGWProperties.GatewayPools = @()
$VirtualGWProperties.GatewayPools += $gwPool

# Specify the Virtual Subnet that is to be used for routing between GW and VNET
$VirtualGWProperties.GatewaySubnets = @()
$VirtualGWProperties.GatewaySubnets += $RoutingSubnet

# Update some basic properties
$VirtualGWProperties.RoutingType = "Dynamic"

# Update Network Connection object(s)
$VirtualGWProperties.NetworkConnections = @()

# IPSec Connection configuration
$ipSecConnection = New-Object
Microsoft.Windows.NetworkController.NetworkConnection
$ipSecConnection.ResourceId = "Contoso_IPSecGW"
$ipSecConnection.Properties = New-Object
Microsoft.Windows.NetworkController.NetworkConnectionProperties
$ipSecConnection.Properties.ConnectionType = "IPSec"
$ipSecConnection.Properties.OutboundKiloBitsPerSecond = 10000
$ipSecConnection.Properties.InboundKiloBitsPerSecond = 10000

$ipSecConnection.Properties.IpSecConfiguration = New-Object
Microsoft.Windows.NetworkController.IpSecConfiguration

$ipSecConnection.Properties.IpSecConfiguration.AuthenticationMethod = "PSK"
$ipSecConnection.Properties.IpSecConfiguration.SharedSecret = "P@ssw0rd"
```

```
$ipSecConnection.Properties.IpSecConfiguration.QuickMode = New-Object
Microsoft.Windows.NetworkController.QuickMode

$ipSecConnection.Properties.IpSecConfiguration.QuickMode.PerfectForwardSecrecy =
"PFS2048"
$ipSecConnection.Properties.IpSecConfiguration.QuickMode.AuthenticationTransformat
ionConstant = "SHA256128"
$ipSecConnection.Properties.IpSecConfiguration.QuickMode.CipherTransformationConst
ant = "DES3"
$ipSecConnection.Properties.IpSecConfiguration.QuickMode.SALifeTimeSeconds = 1233
$ipSecConnection.Properties.IpSecConfiguration.QuickMode.IdleDisconnectSeconds =
500
$ipSecConnection.Properties.IpSecConfiguration.QuickMode.SALifeTimeKiloBytes =
1048576

$ipSecConnection.Properties.IpSecConfiguration.MainMode = New-Object
Microsoft.Windows.NetworkController.MainMode

$ipSecConnection.Properties.IpSecConfiguration.MainMode.DiffieHellmanGroup =
"Group2"
$ipSecConnection.Properties.IpSecConfiguration.MainMode.IntegrityAlgorithm =
"SHA256"
$ipSecConnection.Properties.IpSecConfiguration.MainMode.EncryptionAlgorithm =
"AES256"
$ipSecConnection.Properties.IpSecConfiguration.MainMode.SALifeTimeSeconds = 1234
$ipSecConnection.Properties.IpSecConfiguration.MainMode.SALifeTimeKiloBytes =
1048576

$ipSecConnection.Properties.IPAddresses = @()
$ipSecConnection.Properties.PeerIPAddresses = @()

$ipSecConnection.Properties.Routes = @()

$ipv4Route = New-Object Microsoft.Windows.NetworkController.RouteInfo
$ipv4Route.DestinationPrefix = "14.1.10.1/32"
$ipv4Route.metric = 10
$ipSecConnection.Properties.Routes += $ipv4Route

$ipSecConnection.Properties.DestinationIPAddress = "10.127.134.121"

# GRE Connection configuration
$greConnection = New-Object Microsoft.Windows.NetworkController.NetworkConnection
$greConnection.ResourceId = "Contoso_GreGW"

$greConnection.Properties = New-Object
Microsoft.Windows.NetworkController.NetworkConnectionProperties
$greConnection.Properties.ConnectionType = "GRE"
$greConnection.Properties.OutboundKiloBitsPerSecond = 10000
$greConnection.Properties.InboundKiloBitsPerSecond = 10000

$greConnection.Properties.GreConfiguration = New-Object
Microsoft.Windows.NetworkController.GreConfiguration
$greConnection.Properties.GreConfiguration.GreKey = 1234
```

```
$greConnection.Properties.IPAddresses = @()
$greConnection.Properties.PeerIPAddresses = @()

$greConnection.Properties.Routes = @()

$ipv4Route = New-Object Microsoft.Windows.NetworkController.RouteInfo
$ipv4Route.DestinationPrefix = "14.2.20.1/32"
$ipv4Route.metric = 10
$greConnection.Properties.Routes += $ipv4Route

$greConnection.Properties.DestinationIPAddress = "10.127.134.122"

$greConnection.Properties.L3Configuration = New-Object
Microsoft.Windows.NetworkController.L3Configuration

# L3 Forwarding connection configuration
$l3Connection = New-Object Microsoft.Windows.NetworkController.NetworkConnection
$l3Connection.ResourceId = "Contoso_L3GW"

$l3Connection.Properties = New-Object
Microsoft.Windows.NetworkController.NetworkConnectionProperties
$l3Connection.Properties.ConnectionType = "L3"
$l3Connection.Properties.OutboundKiloBitsPerSecond = 10000
$l3Connection.Properties.InboundKiloBitsPerSecond = 10000

$l3Connection.Properties.GreConfiguration = New-Object
Microsoft.Windows.NetworkController.GreConfiguration
$l3Connection.Properties.L3Configuration = New-Object
Microsoft.Windows.NetworkController.L3Configuration
$l3Connection.Properties.L3Configuration.VlanSubnet =
$vlanNetwork.properties.Subnets[0]

$l3Connection.Properties.IPAddresses = @()
$localIPAddress = New-Object Microsoft.Windows.NetworkController.CidrIPAddress
$localIPAddress.IPAddress = "10.127.134.55"
$localIPAddress.PrefixLength = 25
$l3Connection.Properties.IPAddresses += $localIPAddress

$l3Connection.Properties.PeerIPAddresses = @("10.127.134.65")

$l3Connection.Properties.Routes = @()
$ipv4Route = New-Object Microsoft.Windows.NetworkController.RouteInfo
$ipv4Route.DestinationPrefix = "14.2.20.1/32"
$ipv4Route.metric = 10
$l3Connection.Properties.Routes += $ipv4Route

# Update BGP Router Object
$VirtualGWProperties.BgpRouters = @()

$bgpRouter = New-Object Microsoft.Windows.NetworkController.VGwBgpRouter
$bgpRouter.ResourceId = "Contoso_BgpRouter1"
$bgpRouter.Properties = New-Object
Microsoft.Windows.NetworkController.VGwBgpRouterProperties

$bgpRouter.Properties.ExtAsNumber = "0.64512"
```

```
$bgpRouter.Properties.BgpPeers = @()

# Create BGP Peer Object(s)
# BGP Peer for IPSec Connection
$bgpPeer_IPSec = New-Object Microsoft.Windows.NetworkController.VGwBgpPeer
$bgpPeer_IPSec.ResourceId = "Contoso_IPSec_Peer"

$bgpPeer_IPSec.Properties = New-Object
Microsoft.Windows.NetworkController.VGwBgpPeerProperties
$bgpPeer_IPSec.Properties.PeerIpAddress = "14.1.10.1"
$bgpPeer_IPSec.Properties.AsNumber = 64521
$bgpPeer_IPSec.Properties.ExtAsNumber = "0.64521"

$bgpRouter.Properties.BgpPeers += $bgpPeer_IPSec

# BGP Peer for GRE Connection
$bgpPeer_Gre = New-Object Microsoft.Windows.NetworkController.VGwBgpPeer
$bgpPeer_Gre.ResourceId = "Contoso_Gre_Peer"

$bgpPeer_Gre.Properties = New-Object
Microsoft.Windows.NetworkController.VGwBgpPeerProperties
$bgpPeer_Gre.Properties.PeerIpAddress = "14.2.20.1"
$bgpPeer_Gre.Properties.AsNumber = 64522
$bgpPeer_Gre.Properties.ExtAsNumber = "0.64522"

$bgpRouter.Properties.BgpPeers += $bgpPeer_Gre

# BGP Peer for L3 Connection
$bgpPeer_L3 = New-Object Microsoft.Windows.NetworkController.VGwBgpPeer
$bgpPeer_L3.ResourceId = "Contoso_L3_Peer"

$bgpPeer_L3.Properties = New-Object
Microsoft.Windows.NetworkController.VGwBgpPeerProperties
$bgpPeer_L3.Properties.PeerIpAddress = "14.3.30.1"
$bgpPeer_L3.Properties.AsNumber = 64523
$bgpPeer_L3.Properties.ExtAsNumber = "0.64523"

$bgpRouter.Properties.BgpPeers += $bgpPeer_L3

$VirtualGWProperties.BgpRouters += $bgpRouter

# Finally Add the new Virtual Gateway for tenant
New-NetworkControllerVirtualGateway -ConnectionUri $uri  -ResourceId
"Contoso_VirtualGW" -Properties $VirtualGWProperties -Force
```

Modifier une passerelle pour un réseau virtuel

Récupérer la configuration du composant et la stocker dans une variable

```
PowerShell
```

```
$nwConnection = Get-NetworkControllerVirtualGatewayNetworkConnection -
ConnectionUri $uri -VirtualGatewayId "Contoso_VirtualGW" -ResourceId
"Contoso_IPSecGW"
```

Naviguer dans la structure de la variable pour atteindre la propriété nécessaire, et lui affecter la valeur mise à jour

PowerShell

```
$nwConnection.properties.IpSecConfiguration.SharedSecret = "C0mplexP@ssW0rd"
```

Ajouter la configuration modifiée pour remplacer l'ancienne configuration sur le contrôleur de réseau

PowerShell

```
New-NetworkControllerVirtualGatewayNetworkConnection -ConnectionUri $uri -
VirtualGatewayId "Contoso_VirtualGW" -ResourceId $nwConnection.ResourceId -
Properties $nwConnection.Properties -Force
```

Supprimer une passerelle d'un réseau virtuel

Vous pouvez utiliser les commandes Windows PowerShell suivantes pour supprimer des fonctionnalités de passerelle spécifiques ou l'ensemble de la passerelle.

Supprimer une connexion réseau

PowerShell

```
Remove-NetworkControllerVirtualGatewayNetworkConnection -ConnectionUri $uri -
VirtualGatewayId "Contoso_VirtualGW" -ResourceId "Contoso_IPSecGW" -Force
```

Supprimer un homologue BGP

PowerShell

```
Remove-NetworkControllerVirtualGatewayBgpPeer -ConnectionUri $uri -
VirtualGatewayId "Contoso_VirtualGW" -BgpRouterName "Contoso_BgpRouter1" -
ResourceId "Contoso_IPSec_Peer" -Force
```

Supprimer un routeur BGP

PowerShell

```
Remove-NetworkControllerVirtualGatewayBgpRouter -ConnectionUri $uri -
VirtualGatewayId "Contoso_VirtualGW" -ResourceId "Contoso_BgpRouter1" -Force
```

Supprimer une passerelle

PowerShell

```
Remove-NetworkControllerVirtualGateway -ConnectionUri $uri -ResourceId
"Contoso_VirtualGW" -Force
```

Connecter les points de terminaison de conteneur à un réseau virtuel locataire

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans cette rubrique, nous vous montrons comment connecter des points de terminaison de conteneur à un réseau virtuel client existant créé via SDN. Vous utilisez le pilote réseau *l2bridge* (et éventuellement *l2tunnel*) disponible avec le plug-in Windows libnetwork pour Docker afin de créer un réseau de conteneurs sur la machine virtuelle cliente.

Dans la rubrique Pilotes réseau de conteneur, nous avons abordé les multiples pilotes réseau disponibles via Docker sur Windows. Pour SDN, utilisez les pilotes *l2bridge* et *l2tunnel* . Pour les deux pilotes, chaque point de terminaison de conteneur se trouve dans le même sous-réseau virtuel que la machine virtuelle hôte de conteneur (locataire).

Le service de mise en réseau hôte (HNS), via le plug-in de cloud privé, affecte dynamiquement les adresses IP pour les points de terminaison de conteneur. Les points de terminaison de conteneur ont des adresses IP uniques, mais partagent la même adresse MAC de la machine virtuelle hôte de conteneur (locataire) en raison de la traduction d'adresses de couche 2.

La stratégie réseau (ACL, encapsulation et QoS) pour ces points de terminaison de conteneur est appliquée dans l'hôte Physique Hyper-V tel que reçu par le contrôleur de réseau et défini dans les systèmes de gestion de couche supérieure.

Les différences entre les pilotes *l2bridge* et *l2tunnel* sont les suivantes :

Agrandir le tableau

l2bridge	l2tunnel
Points de terminaison de conteneur qui résident sur : • La même machine virtuelle hôte de conteneur et le même sous-réseau ont tout le trafic réseau ponté dans le commutateur virtuel Hyper-V. • Le trafic des machines virtuelles hôtes de conteneur ou sur des sous-réseaux différents est transféré à l'hôte Physique Hyper-V. La stratégie réseau n'est pas appliquée, car le trafic réseau entre les conteneurs sur le même hôte et dans le même sous-réseau ne circule pas vers l'hôte physique. La stratégie réseau s'applique uniquement au trafic réseau de conteneurs entre hôtes ou entre sous-réseaux.	*Tout* le trafic réseau entre deux points de terminaison de conteneur est transféré vers l'hôte physique Hyper-V quel que soit l'hôte ou le sous-réseau. La stratégie réseau s'applique au trafic réseau entre sous-réseaux et entre hôtes.

> ⓘ **Notes**
>
> Ces modes de mise en réseau ne fonctionnent pas pour connecter des points de terminaison de conteneur Windows à un réseau virtuel de locataire dans le cloud public Azure.

Prerequisites

- Une infrastructure SDN déployée avec le contrôleur de réseau.
- Un réseau virtuel locataire a été créé.
- Une machine virtuelle de locataire déployée avec la fonctionnalité conteneur Windows activée, Docker installé et la fonctionnalité Hyper-V activée. La fonctionnalité Hyper-V est nécessaire pour installer plusieurs fichiers binaires pour les réseaux l2bridge et l2tunnel.

  PowerShell

  ```
  # To install HyperV feature without checks for nested virtualization
  dism /Online /Enable-Feature /FeatureName:Microsoft-Hyper-V /All
  ```

> ⓘ **Notes**
>
> La virtualisation imbriquée et l'exposition des extensions de virtualisation ne sont pas requises, sauf si vous utilisez des conteneurs Hyper-V.

Workflow

1. Ajoutez plusieurs configurations IP à une ressource de carte réseau de machine virtuelle existante via le contrôleur de réseau (hôte Hyper-V)2. Activez le proxy réseau sur l'hôte pour allouer des adresses IP d'autorité de certification pour les points de terminaison de conteneur (hôte Hyper-V)3. Installez le plug-in de cloud privé pour affecter des adresses IP d'autorité de certification aux points de terminaison de conteneur (machine virtuelle hôte de conteneur)4. Créer un réseau *l2bridge* ou *l2tunnel* à l'aide de docker (machine virtuelle hôte de conteneur)

> **Notes**
>
> Plusieurs configurations IP ne sont pas prises en charge sur les ressources de carte réseau de machine virtuelle créées via System Center Virtual Machine Manager. Pour ces types de déploiements, il est recommandé de créer la ressource de carte réseau de machine virtuelle hors bande à l'aide de PowerShell du contrôleur de réseau.

1. Ajouter plusieurs configurations IP

Dans cette étape, nous partons du principe que la carte réseau de la machine virtuelle du locataire a une configuration IP avec l'adresse IP 192.168.1.9 et qu'elle est attachée à un ID de ressource de réseau virtuel « VNet1 » et à la ressource de sous-réseau de machine virtuelle « Subnet1 » dans le sous-réseau IP 192.168.1.0/24. Nous ajoutons 10 adresses IP pour les conteneurs de 192.168.1.101 à 192.168.1.110.

PowerShell

```
Import-Module NetworkController

# Specify Network Controller REST IP or FQDN
$uri = "<NC REST IP or FQDN>"
$vnetResourceId = "VNet1"
$vsubnetResourceId = "Subnet1"

$vmnic= Get-NetworkControllerNetworkInterface -ConnectionUri $uri | where
{$_.properties.IpConfigurations.Properties.PrivateIPAddress -eq "192.168.1.9" }
$vmsubnet = Get-NetworkControllerVirtualSubnet -VirtualNetworkId $vnetResourceId -
ResourceId $vsubnetResourceId -ConnectionUri $uri

# For this demo, we will assume an ACL has already been defined; any ACL can be
applied here
$allowallacl = Get-NetworkControllerAccessControlList -ConnectionUri $uri -
ResourceId "AllowAll"


foreach ($i in 1..10)
```

```
{
    $newipconfig = new-object
Microsoft.Windows.NetworkController.NetworkInterfaceIpConfiguration
    $props = new-object
Microsoft.Windows.NetworkController.NetworkInterfaceIpConfigurationProperties

    $resourceid = "IP_192_168_1_1"
    if ($i -eq 10)
    {
        $resourceid += "10"
        $ipstr = "192.168.1.110"
    }
    else
    {
        $resourceid += "0$i"
        $ipstr = "192.168.1.10$i"
    }

    $newipconfig.ResourceId = $resourceid
    $props.PrivateIPAddress = $ipstr

    $props.PrivateIPAllocationMethod = "Static"
    $props.Subnet = new-object Microsoft.Windows.NetworkController.Subnet
    $props.Subnet.ResourceRef = $vmsubnet.ResourceRef
    $props.AccessControlList = new-object
Microsoft.Windows.NetworkController.AccessControlList
    $props.AccessControlList.ResourceRef = $allowallacl.ResourceRef

    $newipconfig.Properties = $props
    $vmnic.Properties.IpConfigurations += $newipconfig
}

New-NetworkControllerNetworkInterface -ResourceId $vmnic.ResourceId -Properties
$vmnic.Properties -ConnectionUri $uri
```

2. Activer le proxy réseau

Au cours de cette étape, vous allez autoriser le proxy réseau à allouer plusieurs adresses IP à la machine virtuelle hôte du conteneur.

Pour activer le proxy réseau, exécutez le script ConfigureMCNP.ps1 sur **l'hôteHyper-V** hébergeant la machine virtuelle hôte de conteneur (locataire).

PowerShell

```
PS C:\> ConfigureMCNP.ps1
```

3. Installer le plug-in de cloud privé

Dans cette étape, vous installez un plug-in pour permettre au service HNS de communiquer avec le proxy réseau sur l'hôte Hyper-V.

Pour installer le plug-in, exécutez le script InstallPrivateCloudPlugin.ps1 à l'intérieur de la **machine virtuelle hôte de conteneur (locataire)**.

PowerShell

```
PS C:\> InstallPrivateCloudPlugin.ps1
```

4. Créer un réseau de conteneurs *l2bridge*

Dans cette étape, vous utilisez la `docker network create` commande sur la **machine virtuelle hôte de conteneur (locataire)** pour créer un réseau l2bridge.

PowerShell

```
# Create the container network
C:\> docker network create -d l2bridge --subnet="192.168.1.0/24" --
gateway="192.168.1.1" MyContainerOverlayNetwork

# Attach a container to the MyContainerOverlayNetwork
C:\> docker run -it --network=MyContainerOverlayNetwork <image> <cmd>
```

> **Notes**
>
> L'attribution d'adresses IP statiques n'est pas prise en charge avec les réseaux de conteneurs *l2bridge* ou *l2tunnel* lorsqu'elles sont utilisées avec la pile SDN Microsoft.

Plus d'informations

Pour plus d'informations sur le déploiement d'une infrastructure SDN, consultez Déployer une infrastructure réseau à définition logicielle.

Configurer le chiffrement pour un sous-réseau virtuel

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Le chiffrement des réseaux virtuels permet de chiffrer le trafic de réseau virtuel entre des machines virtuelles qui communiquent entre elles au sein des sous-réseaux marqués comme « Chiffrement activé ». Il utilise aussi le protocole DTLS (Datagram Transport Layer Security) sur le sous-réseau virtuel pour chiffrer les paquets. DTLS protège contre les écoutes clandestines, l'altération et la falsification par toute personne ayant accès au réseau physique.

Le chiffrement de réseau virtuel nécessite :

- Certificats de chiffrement installés sur chacun des hôtes Hyper-V avec SDN.
- Objet d'informations d'identification dans le contrôleur de réseau référençant l'empreinte numérique de ce certificat.
- La configuration sur chacun des réseaux virtuels contient des sous-réseaux qui nécessitent un chiffrement.

Une fois que vous avez activé le chiffrement sur un sous-réseau, tout le trafic réseau au sein de ce sous-réseau est chiffré automatiquement, en plus de tout chiffrement au niveau de l'application qui peut également avoir lieu. Le trafic qui traverse les sous-réseaux, même s'il est marqué comme chiffré, est envoyé automatiquement non chiffré. Tout trafic qui franchit la délimitation du réseau virtuel est également envoyé non chiffré.

> **Notes**
>
> Lors de la communication avec une autre machine virtuelle sur le même sous-réseau, qu'elle soit actuellement connectée ou connectée ultérieurement, le trafic est chiffré automatiquement.

> **Conseil**
>
> Si vous devez restreindre les applications pour qu'elles communiquent uniquement sur le sous-réseau chiffré, vous pouvez utiliser des listes de contrôle d'accès (ACL) pour autoriser uniquement la communication au sein du sous-réseau actuel. Pour plus d'informations, consultez **Utiliser des listes de contrôle d'accès (ACL) pour gérer le flux de trafic réseau du centre de données**.

Étape 1 : Créer le certificat de chiffrement

Un certificat de chiffrement doit être installé sur chaque hôte. Vous pouvez utiliser le même certificat pour tous les clients ou en générer un unique pour chaque client.

1. Générer le certificat

```
$subjectName = "EncryptedVirtualNetworks"
$cryptographicProviderName = "Microsoft Base Cryptographic Provider v1.0";
[int] $privateKeyLength = 1024;
$sslServerOidString = "1.3.6.1.5.5.7.3.1";
$sslClientOidString = "1.3.6.1.5.5.7.3.2";
[int] $validityPeriodInYear = 5;

$name = new-object -com "X509Enrollment.CX500DistinguishedName.1"
$name.Encode("CN=" + $SubjectName, 0)

#Generate Key
$key = new-object -com "X509Enrollment.CX509PrivateKey.1"
$key.ProviderName = $cryptographicProviderName
$key.KeySpec = 1 #X509KeySpec.XCN_AT_KEYEXCHANGE
$key.Length = $privateKeyLength
$key.MachineContext = 1
$key.ExportPolicy = 0x2
#X509PrivateKeyExportFlags.XCN_NCRYPT_ALLOW_EXPORT_FLAG
$key.Create()

#Configure Eku
$serverauthoid = new-object -com "X509Enrollment.CObjectId.1"
$serverauthoid.InitializeFromValue($sslServerOidString)
$clientauthoid = new-object -com "X509Enrollment.CObjectId.1"
$clientauthoid.InitializeFromValue($sslClientOidString)
$ekuoids = new-object -com "X509Enrollment.CObjectIds.1"
$ekuoids.add($serverauthoid)
$ekuoids.add($clientauthoid)
$ekuext = new-object -com "X509Enrollment.CX509ExtensionEnhancedKeyUsage.1"
$ekuext.InitializeEncode($ekuoids)

# Set the hash algorithm to sha512 instead of the default sha1
$hashAlgorithmObject = New-Object -ComObject X509Enrollment.CObjectId
$hashAlgorithmObject.InitializeFromAlgorithmName(
$ObjectIdGroupId.XCN_CRYPT_HASH_ALG_OID_GROUP_ID,
$ObjectIdPublicKeyFlags.XCN_CRYPT_OID_INFO_PUBKEY_ANY,
$AlgorithmFlags.AlgorithmFlagsNone, "SHA512")


#Request Certificate
$cert = new-object -com "X509Enrollment.CX509CertificateRequestCertificate.1"

$cert.InitializeFromPrivateKey(2, $key, "")
$cert.Subject = $name
```

```
$cert.Issuer = $cert.Subject
$cert.NotBefore = (get-date).ToUniversalTime()
$cert.NotAfter = $cert.NotBefore.AddYears($validityPeriodInYear);
$cert.X509Extensions.Add($ekuext)
$cert.HashAlgorithm = $hashAlgorithmObject
$cert.Encode()

$enrollment = new-object -com "X509Enrollment.CX509Enrollment.1"
$enrollment.InitializeFromRequest($cert)
$certdata = $enrollment.CreateRequest(0)
$enrollment.InstallResponse(2, $certdata, 0, "")
```

Après l'exécution du script, un nouveau certificat s'affiche dans mon magasin :

```
PS D:\> dir cert:\\localmachine\my
PSParentPath: Microsoft.PowerShell.Security\Certificate::localmachine\my

Thumbprint                                Subject
----------                                -------
84857CBBE7A1C851A80AE22391EB2C39BF820CE7  CN=MyNetwork
5EFF2CE51EACA82408572A56AE1A9BCC7E0843C6  CN=EncryptedVirtualNetworks
```

2. Exportez le certificat vers un fichier.

   Vous avez besoin de deux copies du certificat, l'une avec la clé privée et l'autre sans.

```
$subjectName = "EncryptedVirtualNetworks"
$cert = Get-ChildItem cert:\localmachine\my | ? {$_.Subject -eq
"CN=$subjectName"}
[System.io.file]::WriteAllBytes("c:\$subjectName.pfx", $cert.Export("PFX",
"secret"))
Export-Certificate -Type CERT -FilePath "c:\$subjectName.cer" -cert $cert
```

3. Installer les certificats sur chacun de vos hôtes Hyper-v

```
PS C:\> dir c:\$subjectname.*

Directory: C:\

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        9/22/2017   4:54 PM            543 EncryptedVirtualNetworks.cer
-a----        9/22/2017   4:54 PM           1706 EncryptedVirtualNetworks.pfx
```

4. Installation sur un hôte Hyper-V

```
$server = "Server01"

$subjectname = "EncryptedVirtualNetworks"
copy c:\$SubjectName.* \\$server\c$
invoke-command -computername $server -ArgumentList $subjectname,"secret" {
    param (
        [string] $SubjectName,
        [string] $Secret
    )
    $certFullPath = "c:\$SubjectName.cer"

    # create a representation of the certificate file
    $certificate = new-object
System.Security.Cryptography.X509Certificates.X509Certificate2
    $certificate.import($certFullPath)

    # import into the store
    $store = new-object
System.Security.Cryptography.X509Certificates.X509Store("Root",
"LocalMachine")
    $store.open("MaxAllowed")
    $store.add($certificate)
    $store.close()

    $certFullPath = "c:\$SubjectName.pfx"
    $certificate = new-object
System.Security.Cryptography.X509Certificates.X509Certificate2
    $certificate.import($certFullPath, $Secret,
"MachineKeySet,PersistKeySet")

    # import into the store
    $store = new-object
System.Security.Cryptography.X509Certificates.X509Store("My", "LocalMachine")
    $store.open("MaxAllowed")
    $store.add($certificate)
    $store.close()

    # Important: Remove the certificate files when finished
    remove-item C:\$SubjectName.cer
    remove-item C:\$SubjectName.pfx
}
```

5. Répétez cette opération pour chaque serveur de votre environnement.

   Après la répétition pour chaque serveur, vous devez avoir un certificat installé à la racine et dans mon magasin de chaque hôte Hyper-V.

6. Vérifiez l’installation du certificat.

Vérifiez les certificats en vérifiant le contenu des magasins de certificats My et Root :

```
PS C:\> enter-pssession Server1

[Server1]: PS C:\> get-childitem
cert://localmachine/my,cert://localmachine/root | ? {$_.Subject -eq
"CN=EncryptedVirtualNetworks"}

PSParentPath: Microsoft.PowerShell.Security\Certificate::localmachine\my

Thumbprint                                Subject
----------                                -------
5EFF2CE51EACA82408572A56AE1A9BCC7E0843C6  CN=EncryptedVirtualNetworks

PSParentPath: Microsoft.PowerShell.Security\Certificate::localmachine\root

Thumbprint                                Subject
----------                                -------
5EFF2CE51EACA82408572A56AE1A9BCC7E0843C6  CN=EncryptedVirtualNetworks
```

7. Notez l’empreinte numérique.

   Vous devez noter l’empreinte numérique, car vous en avez besoin pour créer l’objet d’informations d’identification de certificat dans le contrôleur de réseau.

Étape 2 : Créer les informations d’identification du certificat

Après avoir installé le certificat sur chacun des hôtes Hyper-V connectés au contrôleur de réseau, vous devez maintenant configurer le contrôleur de réseau pour l’utiliser. Pour ce faire, vous devez créer un objet d’informations d’identification contenant l’empreinte numérique du certificat de l’ordinateur sur lequel les modules PowerShell du contrôleur de réseau sont installés.

```
///Replace with the thumbprint from your certificate
$thumbprint = "5EFF2CE51EACA82408572A56AE1A9BCC7E0843C6"

$uri = "https://nc.contoso.com"

///Replace with your Network Controller URI
Import-module networkcontroller

$credproperties = new-object
Microsoft.Windows.NetworkController.CredentialProperties
```

```
$credproperties.Type = "X509Certificate"
$credproperties.Value = $thumbprint
New-networkcontrollercredential -connectionuri $uri -resourceid
"EncryptedNetworkCertificate" -properties $credproperties -force
```

Conseil

Vous pouvez réutiliser ces informations d'identification pour chaque réseau virtuel chiffré, ou vous pouvez déployer et utiliser un certificat unique pour chaque client.

Étape 3 : Configuration d'un réseau virtuel pour le chiffrement

Cette étape suppose que vous avez déjà créé un nom de réseau virtuel « Mon réseau » et qu'il contient au moins un sous-réseau virtuel. Pour plus d'informations sur la création de réseaux virtuels, consultez Créer, supprimer ou mettre à jour des réseaux virtuels de client.

Notes

Lors de la communication avec une autre machine virtuelle sur le même sous-réseau, qu'elle soit actuellement connectée ou connectée ultérieurement, le trafic est chiffré automatiquement.

1. Récupérez les objets Réseau virtuel et Informations d'identification à partir du contrôleur de réseau :

```
$vnet = Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceId
"MyNetwork"
$certcred = Get-NetworkControllerCredential -ConnectionUri $uri -ResourceId
"EncryptedNetworkCertificate"
```

2. Ajoutez une référence aux informations d'identification du certificat et activez le chiffrement sur des sous-réseaux individuels :

```
$vnet.properties.EncryptionCredential = $certcred

# Replace the Subnets index with the value corresponding to the subnet you
want encrypted.
```

```
# Repeat for each subnet where encryption is needed
$vnet.properties.Subnets[0].properties.EncryptionEnabled = $true
```

3. Placez l’objet Réseau virtuel mis à jour dans le contrôleur de réseau :

```

New-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceId
$vnet.ResourceId -Properties $vnet.Properties -force
```

*Félicitations!** Vous avez terminé une fois que vous avez effectué ces étapes.

Contrôle de sortie dans un réseau virtuel

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Un aspect fondamental de la monétisation des réseaux cloud est la possibilité de facturer par utilisation de la bande passante réseau. Les données sortantes sont facturées en fonction de la quantité totale de données sortant des centres de données via Internet au cours d'un cycle de facturation donné.

Le contrôle de sortie pour le trafic réseau SDN dans Windows Server 2019 permet d'offrir des compteurs d'utilisation pour les transferts de données sortants. Le trafic réseau qui quitte chaque réseau virtuel mais reste dans le centre de données peut être suivi séparément afin d'être exclu des calculs de facturation. Les paquets liés aux adresses IP de destination qui ne sont pas inclus dans l'une des plages d'adresses non facturées sont suivis en tant que transferts de données sortants facturés.

Plages d'adresses non facturées de réseau virtuel (liste verte de plages d'adresses IP)

Vous trouverez des plages d'adresses non facturées sous la propriété **UnbilledAddressRanges** d'un réseau virtuel existant. Par défaut, aucune plage d'adresses n'est ajoutée.

PowerShell

```
import-module NetworkController
$uri = "https://sdn.contoso.com"

(Get-NetworkControllerVirtualNetwork -ConnectionURI $URI -ResourceId
"VNet1").properties
```

Votre sortie devrait ressembler à ceci :

```
 AddressSpace           : Microsoft.Windows.NetworkController.AddressSpace
 DhcpOptions            :
 UnbilledAddressRanges  :
 ConfigurationState     :
 ProvisioningState      : Succeeded
 Subnets                : {21e71701-9f59-4ee5-b798-2a9d8c2762f0, 5f4758ef-9f96-
40ca-a389-35c414e996cc,
                       29fe67b8-6f7b-486c-973b-8b9b987ec8b3}
 VirtualNetworkPeerings :
```

```
EncryptionCredential    :
LogicalNetwork          : Microsoft.Windows.NetworkController.LogicalNetwork
```

Exemple : Gérer les plages d'adresses non facturées d'un réseau virtuel

Vous pouvez gérer l'ensemble des préfixes de sous-réseau IP à exclure du contrôle de sortie facturé en définissant la propriété **UnbilledAddressRange** d'un réseau virtuel. Tout trafic envoyé par les interfaces réseau sur le réseau virtuel avec une adresse IP de destination correspondant à l'un des préfixes ne sera pas inclus dans la propriété BilledEgressBytes.

1. Mettez à jour la propriété **UnbilledAddressRanges** pour contenir les sous-réseaux qui ne seront pas facturés pour l'accès.

   PowerShell

   ```
   $vnet = Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceID
   "VNet1"
   $vnet.Properties.UnbilledAddressRanges = "10.10.2.0/24,10.10.3.0/24"
   ```

   > **Conseil**
   >
   > Si vous ajoutez plusieurs sous-réseaux IP, utilisez une virgule entre chacun des sous-réseaux IP. N'incluez aucun espace avant ou après la virgule.

2. Mettez à jour la ressource de réseau virtuel avec la propriété **UnbilledAddressRanges** modifiée.

   PowerShell

   ```
   New-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceId "VNet1" -
   Properties $unbilled.Properties -PassInnerException
   ```

   Votre sortie devrait ressembler à ceci :

   ```
      Confirm
      Performing the operation 'New-NetworkControllerVirtualNetwork' on entities
   of type
      'Microsoft.Windows.NetworkController.VirtualNetwork' via
      'https://sdn.contoso.com/networking/v3/virtualNetworks/VNet1'. Are you
   sure you want to continue?
   ```

```
    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y


    Tags              :
    ResourceRef       : /virtualNetworks/VNet1
    InstanceId        : 29654b0b-9091-4bed-ab01-e172225dc02d
    Etag              : W/"6970d0a3-3444-41d7-bbe4-36327968d853"
    ResourceMetadata  :
    ResourceId        : VNet1
    Properties        :
Microsoft.Windows.NetworkController.VirtualNetworkProperties
```

3. Vérifiez le réseau virtuel pour voir **lesranges UnbilledAddressRanges configurés**.

PowerShell

```
(Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceID
"VNet1").properties
```

La sortie devrait maintenant ressembler à ceci :

```
AddressSpace           : Microsoft.Windows.NetworkController.AddressSpace
DhcpOptions            :
UnbilledAddressRanges  : 10.10.2.0/24,192.168.2.0/24
ConfigurationState     :
ProvisioningState      : Succeeded
Subnets                : {21e71701-9f59-4ee5-b798-2a9d8c2762f0, 5f4758ef-
9f96-40ca-a389-35c414e996cc,
                     29fe67b8-6f7b-486c-973b-8b9b987ec8b3}
VirtualNetworkPeerings :
EncryptionCredential   :
LogicalNetwork         : Microsoft.Windows.NetworkController.LogicalNetwork
```

Vérifier l'utilisation de sortie non facturée d'un réseau virtuel

Après avoir configuré la propriété **UnbilledAddressRanges** , vous pouvez vérifier l'utilisation de sortie facturée et non facturée de chaque sous-réseau au sein d'un réseau virtuel. Le trafic de sortie est mis à jour toutes les quatre minutes avec le nombre total d'octets des plages facturées et non facturées.

Les propriétés suivantes sont disponibles pour chaque sous-réseau virtuel :

- **UnbilledEgressBytes** indique le nombre d'octets non facturés envoyés par les interfaces réseau connectées à ce sous-réseau virtuel. Les octets non facturés sont des octets envoyés aux plages d'adresses qui font partie de la propriété **UnbilledAddressRanges** du réseau virtuel parent.
- **BilledEgressBytes** indique le nombre d'octets facturés envoyés par les interfaces réseau connectées à ce sous-réseau virtuel. Les octets facturés sont des octets envoyés aux plages d'adresses qui ne font pas partie de la propriété **UnbilledAddressRanges** du réseau virtuel parent.

Utilisez l'exemple suivant pour interroger l'utilisation de la sortie :

PowerShell

```
(Get-NetworkControllerVirtualNetwork -ConnectionURI $URI -ResourceId
"VNet1").properties.subnets.properties | ft
AddressPrefix,BilledEgressBytes,UnbilledEgressBytes
```

Votre sortie devrait ressembler à ceci :

```
AddressPrefix BilledEgressBytes UnbilledEgressBytes
------------- ----------------- -------------------
10.0.255.8/29          16827067                   0
10.0.2.0/24           781733019                   0
10.0.4.0/24                   0                   0
```

Gérer les charges de travail locataires

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Cette rubrique contient des liens vers la documentation qui vous permet de gérer les charges de travail de locataire en ajoutant des machines virtuelles de locataire, à l'aide d'appliances virtuelles réseau, de la configuration de l'équilibrage de charge logicielle, etc.

Cette section comprend les rubriques suivantes.

- Créer une machine virtuelle et établir la connexion à un réseau virtuel locataire ou un réseau local virtuel
- Configurer la qualité de service (QoS) pour une carte réseau de machine virtuelle locataire
- Configurer des listes de contrôle d'accès (ACL) du pare-feu de centre de données
- Configurer l'équilibreur de charge logicielle pour l'équilibrage de charge et la traduction d'adresses réseau (NAT)
- Utiliser des équipements virtuels réseau sur un réseau virtuel
- Clustering invité dans un réseau virtuel

Commentaires

Cette page a-t-elle été utile ? Yes No

Créer une machine virtuelle et établir la connexion à un réseau virtuel locataire ou un réseau local virtuel

Article • 30/04/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans cette rubrique, vous créez une machine virtuelle locataire et vous la connectez à un réseau virtuel que vous avez créé avec la virtualisation de réseau Hyper-V ou à un réseau local virtuel (VLAN). Vous pouvez utiliser les applets de commande Windows PowerShell du contrôleur de réseau pour vous connecter à un réseau virtuel ou NetworkControllerRESTWrappers pour vous connecter à un VLAN.

Utilisez les processus décrits dans cette rubrique pour déployer des appliances virtuelles. En quelques étapes supplémentaires, vous pouvez configurer des appliances pour traiter ou inspecter les paquets de données qui circulent vers ou depuis d'autres machines virtuelles sur le Réseau virtuel.

Les sections de cette rubrique incluent des exemples de commandes Windows PowerShell qui contiennent des exemples de valeurs pour de nombreux paramètres. Veillez à remplacer les exemples de valeurs dans ces commandes par des valeurs appropriées à votre déploiement avant d'exécuter ces commandes.

Prérequis

1. Adaptateurs réseau de machine virtuelle créés avec des adresses MAC statiques pendant la durée de vie de la machine virtuelle.

   Si l'adresse MAC change pendant la durée de vie de la machine virtuelle, le contrôleur de réseau ne peut pas configurer la stratégie nécessaire pour l'adaptateur réseau. Le fait de ne pas configurer la stratégie pour le réseau empêche l'adaptateur réseau de traiter le trafic réseau, et toutes les communications avec le réseau échouent.

2. Si la machine virtuelle nécessite un accès réseau au démarrage, ne démarrez la machine virtuelle qu'après avoir défini l'ID d'interface sur le port de l'adaptateur réseau de machine virtuelle. Si vous démarrez la machine virtuelle avant de définir l'ID d'interface et que l'interface réseau n'existe pas, la machine virtuelle ne peut pas communiquer sur le réseau dans le contrôleur de réseau et toutes les stratégies sont appliquées.

3. Si vous avez besoin d'ACL personnalisées pour cette interface réseau, créez la liste de contrôle d'accès maintenant à l'aide d'instructions de la rubrique Utiliser les listes de

contrôle d'accès (ACL) pour gérer le flux de trafic réseau du centre de données

Vérifiez que vous avez déjà créé un Réseau virtuel avant d'utiliser cet exemple de commande. Pour plus d'informations, consultez Créer, supprimer ou mettre à jour des réseaux virtuels de locataire.

Créez une machine virtuelle et connectez-vous à un Réseau virtuel à l'aide des applets de commande du contrôleur de réseau Windows PowerShell

1. Créez une machine virtuelle avec un adaptateur réseau de machine virtuelle qui a une adresse MAC statique.

   PowerShell

   ```
   New-VM -Generation 2 -Name "MyVM" -Path "C:\VMs\MyVM" -MemoryStartupBytes 4GB
   -VHDPath "C:\VMs\MyVM\Virtual Hard Disks\WindowsServer2016.vhdx" -SwitchName
   "SDNvSwitch"

   Set-VM -Name "MyVM" -ProcessorCount 4

   Set-VMNetworkAdapter -VMName "MyVM" -StaticMacAddress "00-11-22-33-44-55"
   ```

2. Obtenez le réseau virtuel qui contient le sous-réseau auquel vous souhaitez connecter l'adaptateur réseau.

   Powershell

   ```
   $vnet = Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceId
   "Contoso_WebTier"
   ```

3. Créez un objet interface réseau dans le contrôleur de réseau.

   > **Conseil**
   >
   > Dans cette étape, vous utilisez la liste de contrôle d'accès personnalisée.

   PowerShell

   ```
   $vmnicproperties = New-Object
   Microsoft.Windows.NetworkController.NetworkInterfaceProperties
   ```

```
$vmnicproperties.PrivateMacAddress = "001122334455"
$vmnicproperties.PrivateMacAllocationMethod = "Static"
$vmnicproperties.IsPrimary = $true

$vmnicproperties.DnsSettings = New-Object
Microsoft.Windows.NetworkController.NetworkInterfaceDnsSettings
$vmnicproperties.DnsSettings.DnsServers = @("24.30.1.11", "24.30.1.12")

$ipconfiguration = New-Object
Microsoft.Windows.NetworkController.NetworkInterfaceIpConfiguration
$ipconfiguration.resourceid = "MyVM_IP1"
$ipconfiguration.properties = New-Object
Microsoft.Windows.NetworkController.NetworkInterfaceIpConfigurationProperties
$ipconfiguration.properties.PrivateIPAddress = "24.30.1.101"
$ipconfiguration.properties.PrivateIPAllocationMethod = "Static"

$ipconfiguration.properties.Subnet = New-Object
Microsoft.Windows.NetworkController.Subnet
$ipconfiguration.properties.subnet.ResourceRef =
$vnet.Properties.Subnets[0].ResourceRef

$vmnicproperties.IpConfigurations = @($ipconfiguration)
New-NetworkControllerNetworkInterface –ResourceID "MyVM_Ethernet1" –
Properties $vmnicproperties –ConnectionUri $uri
```

4. Obtenez l'InstanceId de l'interface réseau à partir du contrôleur de réseau.

PowerShell

```
 $nic = Get-NetworkControllerNetworkInterface -ConnectionUri $uri -ResourceId
"MyVM_Ethernet1"
```

5. Définissez l'ID d'interface sur le port de l'adaptateur réseau de machine virtuelle Hyper-V.

> ⓘ **Notes**
>
> Vous devez exécuter ces commandes sur l'hôte Hyper-V sur lequel la machine virtuelle est installée.

PowerShell

```
#Do not change the hardcoded IDs in this section, because they are fixed
values and must not change.

$FeatureId = "9940cd46-8b06-43bb-b9d5-93d50381fd56"

$vmNics = Get-VMNetworkAdapter -VMName "MyVM"

$CurrentFeature = Get-VMSwitchExtensionPortFeature -FeatureId $FeatureId -
```

```
VMNetworkAdapter $vmNics

if ($CurrentFeature -eq $null) {
    $Feature = Get-VMSystemSwitchExtensionPortFeature -FeatureId $FeatureId

    $Feature.SettingData.ProfileId = "{$($nic.InstanceId)}"
    $Feature.SettingData.NetCfgInstanceId = "{56785678-a0e5-4a26-bc9b-
c0cba27311a3}"
    $Feature.SettingData.CdnLabelString = "TestCdn"
    $Feature.SettingData.CdnLabelId = 1111
    $Feature.SettingData.ProfileName = "Testprofile"
    $Feature.SettingData.VendorId = "{1FA41B39-B444-4E43-B35A-E1F7985FD548}"
    $Feature.SettingData.VendorName = "NetworkController"
    $Feature.SettingData.ProfileData = 1

    Add-VMSwitchExtensionPortFeature -VMSwitchExtensionFeature  $Feature -
VMNetworkAdapter $vmNics
} else {
    $CurrentFeature.SettingData.ProfileId = "{$($nic.InstanceId)}"
    $CurrentFeature.SettingData.ProfileData = 1

    Set-VMSwitchExtensionPortFeature -VMSwitchExtensionFeature
$CurrentFeature  -VMNetworkAdapter $vmNics
}
```

6. Démarrez la machine virtuelle.

PowerShell

```
Get-VM -Name "MyVM" | Start-VM
```

Vous avez correctement créé une machine virtuelle, connecté la machine virtuelle à un locataire Réseau virtuel et démarré la machine virtuelle afin qu'elle puisse traiter les charges de travail des locataires.

Créez une machine virtuelle et connectez-vous à un VLAN à l'aide de NetworkControllerRESTWrappers

1. Créez la machine virtuelle et affectez une adresse MAC statique à la machine virtuelle.

PowerShell

```
New-VM -Generation 2 -Name "MyVM" -Path "C:\VMs\MyVM" -MemoryStartupBytes 4GB
-VHDPath "C:\VMs\MyVM\Virtual Hard Disks\WindowsServer2016.vhdx" -SwitchName
"SDNvSwitch"
```

```
Set-VM -Name "MyVM" -ProcessorCount 4

Set-VMNetworkAdapter -VMName "MyVM" -StaticMacAddress "00-11-22-33-44-55"
```

2. Définissez l'ID de réseau local virtuel sur l'adaptateur réseau de machine virtuelle.

PowerShell

```
Set-VMNetworkAdapterIsolation –VMName "MyVM" -AllowUntaggedTraffic $true -
IsolationMode VLAN -DefaultIsolationId 123
```

3. Obtenez le sous-réseau de réseau logique et créez l'interface réseau.

PowerShell

```
 $logicalnet = Get-NetworkControllerLogicalNetwork -ConnectionUri $uri -
ResourceId "00000000-2222-1111-9999-000000000002"

 $vmnicproperties = New-Object
Microsoft.Windows.NetworkController.NetworkInterfaceProperties
 $vmnicproperties.PrivateMacAddress = "00-1D-C8-B7-01-02"
 $vmnicproperties.PrivateMacAllocationMethod = "Static"
 $vmnicproperties.IsPrimary = $true

 $vmnicproperties.DnsSettings = New-Object
Microsoft.Windows.NetworkController.NetworkInterfaceDnsSettings
 $vmnicproperties.DnsSettings.DnsServers =
$logicalnet.Properties.Subnets[0].DNSServers

 $ipconfiguration = New-Object
Microsoft.Windows.NetworkController.NetworkInterfaceIpConfiguration
 $ipconfiguration.resourceid = "MyVM_Ip1"
 $ipconfiguration.properties = New-Object
Microsoft.Windows.NetworkController.NetworkInterfaceIpConfigurationProperties
 $ipconfiguration.properties.PrivateIPAddress = "10.127.132.177"
 $ipconfiguration.properties.PrivateIPAllocationMethod = "Static"

 $ipconfiguration.properties.Subnet = New-Object
Microsoft.Windows.NetworkController.Subnet
 $ipconfiguration.properties.subnet.ResourceRef =
$logicalnet.Properties.Subnets[0].ResourceRef

 $vmnicproperties.IpConfigurations = @($ipconfiguration)
 $vnic = New-NetworkControllerNetworkInterface –ResourceID "MyVM_Ethernet1" –
Properties $vmnicproperties –ConnectionUri $uri

 $vnic.InstanceId
```

4. Définissez l'InstanceId sur le port Hyper-V.

PowerShell

```
#The hardcoded Ids in this section are fixed values and must not change.
$FeatureId = "9940cd46-8b06-43bb-b9d5-93d50381fd56"

$vmNics = Get-VMNetworkAdapter -VMName "MyVM"

$CurrentFeature = Get-VMSwitchExtensionPortFeature -FeatureId $FeatureId -
VMNetworkAdapter $vmNics

if ($CurrentFeature -eq $null) {
    $Feature = Get-VMSystemSwitchExtensionFeature -FeatureId $FeatureId

    $Feature.SettingData.ProfileId = "{$InstanceId}"
    $Feature.SettingData.NetCfgInstanceId = "{56785678-a0e5-4a26-bc9b-
c0cba27311a3}"
    $Feature.SettingData.CdnLabelString = "TestCdn"
    $Feature.SettingData.CdnLabelId = 1111
    $Feature.SettingData.ProfileName = "Testprofile"
    $Feature.SettingData.VendorId = "{1FA41B39-B444-4E43-B35A-E1F7985FD548}"
    $Feature.SettingData.VendorName = "NetworkController"
    $Feature.SettingData.ProfileData = 1

    Add-VMSwitchExtensionFeature -VMSwitchExtensionFeature  $Feature -
VMNetworkAdapter $vmNics
} else {
    $CurrentFeature.SettingData.ProfileId = "{$InstanceId}"
    $CurrentFeature.SettingData.ProfileData = 1

    Set-VMSwitchExtensionPortFeature -VMSwitchExtensionFeature
$CurrentFeature  -VMNetworkAdapter $vmNics
}
```

5. Démarrez la machine virtuelle.

PowerShell

```
Get-VM -Name "MyVM" | Start-VM
```

Vous avez correctement créé une machine virtuelle, connecté la machine virtuelle à un VLAN et démarré la machine virtuelle afin qu'elle puisse traiter les charges de travail des locataires.

Configurer la qualité de service (QoS) pour une carte réseau de machine virtuelle

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez configurer la qualité de service (QoS) de la mise en réseau SDN (Software Defined Networking) pour une carte réseau de machine virtuelle afin de limiter la bande passante sur une interface virtuelle pour éviter qu'une machine virtuelle à trafic élevé ne fasse face à d'autres trafics réseau de machines virtuelles. Vous pouvez également configurer la qualité de service (QoS) SDN pour réserver une quantité spécifique de bande passante pour une machine virtuelle afin de garantir que la machine virtuelle peut envoyer du trafic, indépendamment du reste du trafic sur le réseau. Cela peut être appliqué aux machines virtuelles attachées à des réseaux locaux virtuels traditionnels, ainsi qu'aux machines virtuelles attachées à des réseaux de superposition SDN.

Vous pouvez également configurer ***le déchargement QoS*** pour appliquer des règles QoS à la carte réseau physique plutôt qu'au commutateur virtuel, ce qui réduit l'utilisation du processeur et améliore l'application. Le déchargement de la qualité de service (QoS) est une fonctionnalité facultative des cartes réseau certifiées Windows Server 2022 qui ont obtenu la qualification supplémentaire (AQ) Premium du centre de données à définition logicielle Windows Server (SDDC). Pour plus d'informations, consultez la section Sélectionner une carte réseau.

Limites de bande passante QoS SDN

La qualité de service (QoS) SDN permet de configurer la bande passante maximale autorisée côté envoi ou côté réception pour les machines virtuelles. Cette fonction est prise en charge pour les machines virtuelles connectées à un réseau local virtuel traditionnel, ainsi que pour les machines virtuelles connectées à un réseau virtuel SDN. Une fois définie, votre machine virtuelle ne sera pas en mesure d'envoyer ou de recevoir du trafic au-delà des limites maximales configurées. Pour une machine virtuelle, vous pouvez choisir de configurer une limite d'envoi, une limite de réception ou les deux.

Les paramètres qui peuvent être configurés via la qualité de service (QoS) SDN sont les suivants :

- **OutboundReservedValue** : si `outboundReservedMode` le mode est « absolu », la valeur indique la bande passante, en Mbits/s, garantie au port virtuel pour la transmission

(sortie). Si le mode `outboundReservedMode` est « poids », la valeur indique la partie pondérée de la bande passante garantie.

- **OutboundMaximumMbps** : indique la bande passante maximale autorisée côté envoi, en Mbits/s, pour le port virtuel (sortie).
- **InboundMaximumMbps** : indique la bande passante maximale autorisée côté réception pour le port virtuel (entrée) en Mbits/s.

Stratégies QoS SDN

Une fois le contrôleur de réseau pour SDN configuré, vous pouvez déployer vos stratégies de qualité de service (QoS). Aujourd'hui, vous pouvez le faire à l'aide des applets de commande PowerShell du contrôleur de réseau .

Pour tous les exemples de scripts utilisés ci-dessous, `-ConnectionUri` est l'URI REST du contrôleur de réseau. Par exemple : `https://nc.contoso.com`.

Étape 1 : Configurer les paramètres QoS globaux

Exécutez la commande PowerShell suivante sur un ordinateur du contrôleur de réseau ou un client de gestion du contrôleur de réseau. Cela permet aux paramètres globaux de configurer des stratégies QoS via le contrôleur de réseau :

PowerShell

```
$vswitchConfig=
[Microsoft.Windows.NetworkController.VirtualSwitchManagerProperties]::new()
$qos=[Microsoft.Windows.NetworkController.VirtualSwitchQosSettings]::new()
$qos.EnableSoftwareReservations=$true
$vswitchConfig.QosSettings =$qos
Set-NetworkControllerVirtualSwitchConfiguration -ConnectionUri $uri -Properties
$vswitchConfig
```

Étape 2 : Configurer les stratégies QoS

Tout d'abord, vous devez identifier l'interface réseau de la machine virtuelle de charge de travail dans laquelle vous souhaitez appliquer la stratégie :

PowerShell

```
$NwInterface=Get-NetworkControllerNetworkInterface -ConnectionUri $uri -ResourceId
Vnet-VM2_Net_Adapter_0
```

Ensuite, configurez le débit maximal entrant et sortant autorisé sur l'interface réseau :

PowerShell

```
$NwInterface.Properties.PortSettings.QosSettings=
[Microsoft.Windows.NetworkController.VirtualNetworkInterfaceQosSettings]::new()
$NwInterface.Properties.PortSettings.QosSettings.InboundMaximumMbps ="1000"
New-NetworkControllerNetworkInterface -ConnectionUri $uri -ResourceId
$NwInterface.ResourceId -Properties $NwInterface.Properties
```

Déchargement QoS (facultatif)

Vous pouvez configurer la carte réseau physique pour utiliser le déchargement QoS. Si votre carte réseau prend en charge le déchargement QoS, vérifiez qu'il est activé à l'aide de l'une des deux méthodes suivantes :

- Network ATC (recommandé)
- Activation manuelle à l'aide des propriétés de la carte réseau

Utiliser Network ATC

Le déchargement QoS est automatiquement activé sur toutes les cartes réseau avec le type d'intention `Compute`. Pour plus d'informations, consultez la section Simplifier la mise en réseau hôte avec Network ATC.

> **Notes**
>
> Cette option est disponible uniquement pour les abonnés locaux Azure.

Utiliser l'activation manuelle

L'activation manuelle se fait via les applets de commande intégrées utilisées pour gérer les propriétés de la carte réseau physique.

> **Important**
>
> Vous devez vous assurer que `QosOffload` est activé sur chaque carte réseau physique de l'équipe et sur chaque hôte. Sans cela, la règle QoS est appliquée via le commutateur virtuel, ce qui réduit l'efficacité.

Utilisez les applets de commande suivantes pour vérifier si vos cartes réseau prennent en charge `QosOffload` et modifient les propriétés de la carte réseau :

PowerShell

```
Get-NetAdapterAdvancedProperty -Name <physical NIC Name> -RegistryKeyword
*QosOffload
Enable QosOffload for your adapters:
Set-NetAdapterAdvancedProperty -Name  <physical NIC Name> -RegistryKeyword
*QosOffload -RegistryValue 1
```

Configurer la qualité de service (QoS) du matériel

Vous pouvez configurer la qualité de service (QoS) du matériel à l'aide des paramètres et des stratégies.

Étape 1 – Configurer les paramètres QoS globaux

Effectuez les étapes ci-dessous sur un ordinateur du contrôleur de réseau ou un client de gestion du contrôleur de réseau. Cela permet au paramètre global de configurer des stratégies QoS via le contrôleur de réseau.

PowerShell

```
$vswitchConfig=
[Microsoft.Windows.NetworkController.VirtualSwitchManagerProperties]::new()
$qos=[Microsoft.Windows.NetworkController.VirtualSwitchQosSettings]::new()
$qos.EnableHardwareLimits=$true
$vswitchConfig.QosSettings =$qos
Set-NetworkControllerVirtualSwitchConfiguration -ConnectionUri $uri -Properties
$vswitchConfig
```

Étape 2 – Configurer les stratégies QoS

Tout d'abord, identifiez l'interface réseau de la machine virtuelle de charge de travail dans laquelle vous souhaitez appliquer la stratégie :

PowerShell

```
$NwInterface=Get-NetworkControllerNetworkInterface -ConnectionUri $uri -ResourceId
Vnet-VM2_Net_Adapter_0
```

Ensuite, configurez le débit maximal sortant autorisé sur l'interface réseau. L'exemple suivant crée une règle QoS qui limite le trafic sortant d'une interface de machine virtuelle à 1 Gbit/s.

> **Important**
>
> Qos Offload prend uniquement en charge **OutboundMaximumMbps**. Vous ne pouvez pas utiliser **OutboundReservedValue** ou **InboundMaximumMbps** avec Qos Offload.

PowerShell

```
$NwInterface.Properties.PortSettings.QosSettings=
[Microsoft.Windows.NetworkController.VirtualNetworkInterfaceQosSettings]::new()
$NwInterface.Properties.PortSettings.QosSettings. EnableHardwareLimits=$true
$NwInterface.Properties.PortSettings.QosSettings.OutboundMaximumMbps ="1000"
New-NetworkControllerNetworkInterface -ConnectionUri $uri -ResourceId
$NwInterface.ResourceId -Properties $NwInterface.Properties
```

> **Notes**
>
> Lors d'une migration dynamique, une machine virtuelle peut être déplacée vers un hôte qui ne prend pas en charge le déchargement QoS. Dans ce scénario, la migration dynamique réussit, mais la qualité de service (QoS) revient à QoS SDN.

Configurer des groupes de sécurité réseau sur votre instance Azure Local avec PowerShell

> S'applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Cet article fournit des instructions pour configurer des groupes de sécurité réseau (NSG) pour gérer le flux de trafic de données à l'aide du pare-feu datacenter pour la mise en réseau SDN (Software Defined Networking) dans Azure Local à l'aide de Windows PowerShell. Vous activez et configurez le Pare-feu du centre de données en créant des groupes de sécurité réseau qui sont appliqués à un sous-réseau ou à une interface réseau.

Les exemples de scripts de cet article utilisent des commandes Windows PowerShell exportées à partir du module **NetworkController** . Vous pouvez également utiliser Windows Admin Center pour configurer et gérer des groupes de sécurité réseau.

Configurer le Pare-feu Datacenter de manière à autoriser tout le trafic

Une fois que vous avez déployé la mise en réseau SDN, vous devez tester la connectivité réseau de base dans votre nouvel environnement. Pour ce faire, créez une règle pour le Pare-feu Datacenter qui autorise tout le trafic réseau, sans restriction.

Utilisez les entrées du tableau suivant pour créer un ensemble de règles qui autorisent tout le trafic réseau entrant et sortant.

Agrandir le tableau

IP Source	IP de destination	Protocole	Port source	Port de destination	Sens	Action	Priorité
*	*	Tous	*	*	Trafic entrant	Autoriser	100
*	*	Tous	*	*	Règle de trafic sortant	Autoriser	110

Dans cet exemple, vous créez un groupe de sécurité réseau avec deux règles :

1. AllowAll_Inbound : permet à tout le trafic réseau de passer dans l'interface réseau où ce groupe de sécurité réseau est configuré.
2. **AllowAllOutbound** : autorise tout le trafic à passer hors de l'interface réseau. Ce groupe de sécurité réseau, identifié par l'ID de ressource « AllowAll-1 » est maintenant prêt à être utilisé dans les sous-réseaux virtuels et les interfaces réseau.

Vous pouvez exécuter cette commande à partir de n'importe quel ordinateur qui a accès au point de terminaison REST du contrôleur de réseau. Tout d'abord, ouvrez une session PowerShell. Dans cet exemple, utilisez l'applet de commande **Enter-PSSession** et remplacez `<computer-name>` par le nom de l'ordinateur disposant du point de terminaison REST du contrôleur de réseau.

PowerShell

```
Enter-PSSession <computer-name>
```

Ensuite, exécutez le script suivant pour créer le groupe de sécurité réseau :

PowerShell

```
$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "100"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"
$aclrule1 = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule1.Properties = $ruleproperties
$aclrule1.ResourceId = "AllowAll_Inbound"
$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "110"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"
$aclrule2 = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule2.Properties = $ruleproperties
$aclrule2.ResourceId = "AllowAll_Outbound"
$acllistproperties = new-object
```

```
Microsoft.Windows.NetworkController.AccessControlListProperties
$acllistproperties.AclRules = @($aclrule1, $aclrule2)
New-NetworkControllerAccessControlList -ResourceId "AllowAll" -Properties
$acllistproperties -ConnectionUri <NC REST FQDN>
```

> **Remarque**
>
> La référence de commande Windows PowerShell pour le contrôleur de réseau se trouve dans les applets de commande du contrôleur de réseau.

Utiliser des groupes de sécurité réseau pour limiter le trafic sur un sous-réseau

Dans cet exemple, vous créez un groupe de sécurité réseau qui empêche les machines virtuelles de communiquer entre elles dans le sous-réseau 192.168.0.0/24. Ce type de groupe de sécurité réseau est utile pour limiter la capacité d'un attaquant à se propager ultérieurement au sein du sous-réseau, tout en permettant aux machines virtuelles de recevoir des demandes provenant de l'extérieur du sous-réseau et de communiquer avec d'autres services sur d'autres sous-réseaux.

Agrandir le tableau

IP Source	IP de destination	Protocole	Port source	Port de destination	Sens	Action	Priorité
192.168.0.1	*	Tous	*	*	Trafic entrant	Autoriser	100
*	192.168.0.1	Tous	*	*	Règle de trafic sortant	Autoriser	101
192.168.0.0/24	*	Tous	*	*	Trafic entrant	Bloquer	102
*	192.168.0.0/24	Tous	*	*	Règle de trafic sortant	Bloquer	1:03
*	*	Tous	*	*	Trafic entrant	Autoriser	104
*	*	Tous	*	*	Règle de trafic sortant	Autoriser	105

Le groupe de sécurité réseau créé par l'exemple de script ci-dessous, identifié par l'ID de ressource **Subnet-192-168-0-0**, peut désormais être appliqué à un sous-réseau de réseau virtuel qui utilise l'adresse de sous-réseau « 192.168.0.0/24 ». Toute interface réseau attachée à ce sous-réseau de réseau virtuel obtient automatiquement les règles de groupe de sécurité réseau ci-dessus appliquées.

Voici un exemple de script pour créer ce groupe de sécurité réseau à l'aide de l'API REST du contrôleur de réseau :

PowerShell

```
import-module networkcontroller
$ncURI = "https://mync.contoso.local"
$aclrules = @()

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "192.168.0.1"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "100"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowRouter_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "192.168.0.1"
$ruleproperties.Priority = "101"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowRouter_Outbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
```

```
$ruleproperties.Action = "Deny"
$ruleproperties.SourceAddressPrefix = "192.168.0.0/24"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "102"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "DenySubnet_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Deny"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "192.168.0.0/24"
$ruleproperties.Priority = "103"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "DenySubnet_Outbound"

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "104"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowAll_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "105"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
```

```
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowAll_Outbound"
$aclrules += $aclrule

$acllistproperties = new-object
Microsoft.Windows.NetworkController.AccessControlListProperties
$acllistproperties.AclRules = $aclrules

New-NetworkControllerAccessControlList -ResourceId "Subnet-192-168-0-0" -Properties
$acllistproperties -ConnectionUri $ncURI
```

Ajouter un groupe de sécurité réseau à une interface réseau

Une fois que vous avez créé un groupe de sécurité réseau et que vous l'avez affecté à un sous-réseau virtuel, vous pouvez remplacer ce groupe de sécurité réseau par défaut sur le sous-réseau virtuel par un groupe de sécurité réseau spécifique pour une interface réseau individuelle. À compter de Windows Server 2019 Datacenter, vous pouvez appliquer des groupes de sécurité réseau spécifiques directement aux interfaces réseau attachées aux réseaux logiques SDN, en plus des réseaux virtuels SDN. Si vous avez défini des groupes de sécurité réseau sur le sous-réseau virtuel connecté à l'interface réseau, les deux groupes de sécurité réseau sont appliqués et les groupes de sécurité réseau d'interface réseau sont hiérarchisés au-dessus des groupes de sécurité réseau de sous-réseau virtuel.

Dans cet exemple, nous montrons comment ajouter un groupe de sécurité réseau à un réseau virtuel.

> **Conseil**
>
> Il est également possible d'ajouter un groupe de sécurité réseau en même temps que vous créez l'interface réseau.

1. Obtenez ou créez l'interface réseau à laquelle vous ajouterez le groupe de sécurité réseau.

   PowerShell

   ```
   $nic = get-networkcontrollernetworkinterface -ConnectionUri $uri -ResourceId
   "MyVM_Ethernet1"
   ```

2. Obtenez ou créez le groupe de sécurité réseau que vous allez ajouter à l'interface réseau.

   PowerShell

```
$acl = get-networkcontrolleraccesscontrollist -ConnectionUri $uri -ResourceId
"AllowAllACL"
```

3. Affectez le groupe de sécurité réseau à la propriété AccessControlList de l'interface réseau.

PowerShell

```
 $nic.properties.ipconfigurations[0].properties.AccessControlList = $acl
```

4. Ajoutez l'interface réseau dans le Contrôleur de réseau.

PowerShell

```
new-networkcontrollernetworkinterface -ConnectionUri $uri -Properties
$nic.properties -ResourceId $nic.resourceid
```

Supprimer un groupe de sécurité réseau d'une interface réseau

Dans cet exemple, nous vous montrons comment supprimer un groupe de sécurité réseau d'une interface réseau. La suppression d'un groupe de sécurité réseau applique l'ensemble de règles par défaut à l'interface réseau. L'ensemble de règles par défaut autorise tout le trafic sortant, mais bloque tout le trafic entrant. Si vous souhaitez autoriser tout le trafic entrant, vous devez suivre l'exemple précédent pour ajouter un groupe de sécurité réseau qui autorise tous les trafics entrants et sortants.

1. Obtenez l'interface réseau à partir de laquelle vous allez supprimer le groupe de sécurité réseau.

PowerShell

```
$nic = get-networkcontrollernetworkinterface -ConnectionUri $uri -ResourceId
"MyVM_Ethernet1"
```

2. Attribuez $null à la propriété AccessControlList d'ipConfiguration.

PowerShell

```
$nic.properties.ipconfigurations[0].properties.AccessControlList = $null
```

3. Ajoutez l'objet d'interface réseau dans le Contrôleur de réseau.

PowerShell

```
new-networkcontrollernetworkinterface -ConnectionUri $uri -Properties
$nic.properties -ResourceId $nic.resourceid
```

Audit du pare-feu

La fonctionnalité d'audit du pare-feu du pare-feu du centre de données enregistre tout flux traité par les règles de pare-feu SDN. Tous les groupes de sécurité réseau activés pour la journalisation sont enregistrés. Les fichiers journaux doivent se trouver dans une syntaxe cohérente avec les journaux de flux Azure Network Watcher. Ces journaux peuvent être utilisés à des fins de diagnostic ou archivés en vue d'une analyse ultérieure.

Voici un exemple de script pour activer l'audit du pare-feu sur les machines hôtes. Mettez à jour les variables au début et exécutez-la sur une instance locale Azure avec le contrôleur de réseau déployé :

PowerShell

```
$logpath = "C:\test\log1"
$servers = @("sa18n22-2", "sa18n22-3", "sa18n22-4")
$uri = "https://sa18n22sdn.sa18.nttest.microsoft.com"

# Create log directories on the hosts
invoke-command -Computername $servers  {
    param(
        $Path
    )
    mkdir $path    -force
} -argumentlist $LogPath

# Set firewall auditing settings on Network Controller
$AuditProperties = new-object
Microsoft.Windows.NetworkController.AuditingSettingsProperties
$AuditProperties.OutputDirectory = $logpath
set-networkcontrolleauditingsettingsconfiguration -connectionuri $uri -properties
$AuditProperties -force  | out-null

# Enable logging on each server
$servers = get-networkcontrollerserver -connectionuri $uri
foreach ($s in $servers) {
    $s.properties.AuditingEnabled = @("Firewall")
    new-networkcontrollerserver -connectionuri $uri -resourceid $s.resourceid -
properties $s.properties -force | out-null
}
```

Une fois activé, un nouveau fichier apparaît dans le répertoire spécifié de chaque hôte environ une fois par heure. Vous devez régulièrement traiter ces fichiers et les supprimer des hôtes. La longueur du fichier actuel est nulle et il est verrouillé jusqu'à ce qu'il soit vidé à l'heure suivante :

syntax

```
PS C:\test\log1> dir

    Directory: C:\test\log1

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/19/2018   6:28 AM          17055 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL122803093.json
-a----        7/19/2018   7:28 AM           7880 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL132803173.json
-a----        7/19/2018   8:28 AM           7867 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL142803264.json
-a----        7/19/2018   9:28 AM          10949 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL152803360.json
-a----        7/19/2018   9:28 AM              0 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL162803464.json
```

Ces fichiers contiennent une séquence d'événements de flux, par exemple :

syntax


```
{
    "records": [
        {
            "properties":{
                "Version":"1.0",
                "flows":[
                    {
                        "flows":[
                            {
                                "flowTuples":
["1531963580,192.122.0.22,192.122.255.255,138,138,U,I,A"],
                                "portId":"9",
                                "portName":"7290436D-0422-498A-8EB8-C6CF5115DACE"
                            }
                        ],
                        "rule":"Allow_Inbound"
                    }
                ]
            },
            "operationName":"NetworkSecurityGroupFlowEvents",
            "resourceId":"a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1",
            "time":"20180719:L012620622",
            "category":"NetworkSecurityGroupFlowEvent",
```

```
            "systemId":"d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a"
            },
```

Notez que la journalisation a lieu uniquement pour les règles dont la **journalisation** est **activée**, par exemple :

syntax

```
{
    "Tags":  null,
    "ResourceRef":  "/accessControlLists/AllowAll",
    "InstanceId":  "4a63e1a5-3264-4986-9a59-4e77a8b107fa",
    "Etag":  "W/\"1535a780-0fc8-4bba-a15a-093ecac9b88b\"",
    "ResourceMetadata":  null,
    "ResourceId":  "AllowAll",
    "Properties":  {
                        "ConfigurationState":  null,
                        "ProvisioningState":  "Succeeded",
                        "AclRules":  [
                                        {
                                            "ResourceMetadata":  null,
                                            "ResourceRef":
"/accessControlLists/AllowAll/aclRules/AllowAll_Inbound",
                                            "InstanceId":  "ba8710a8-0f01-422b-9038-
d1f2390645d7",
                                            "Etag":  "W/\"1535a780-0fc8-4bba-a15a-
093ecac9b88b\"",
                                            "ResourceId":  "AllowAll_Inbound",
                                            "Properties":  {
                                                                "Protocol":  "All",
                                                                "SourcePortRange":  "0-
65535",
                                                                "DestinationPortRange":
"0-65535",
                                                                "Action":  "Allow",
                                                                "SourceAddressPrefix":
"*",
                                                                "DestinationAddressPrefix":  "*",
                                                                "Priority":  "101",
                                                                "Description":  null,
                                                                "Type":  "Inbound",
                                                                "Logging":  "Enabled",
                                                                "ProvisioningState":
"Succeeded"
                                                            }
                                        },
                                        {
                                            "ResourceMetadata":  null,
                                            "ResourceRef":
"/accessControlLists/AllowAll/aclRules/AllowAll_Outbound",
                                            "InstanceId":  "068264c6-2186-4dbc-bbe7-
f504c6f47fa8",
```

```
                                                "Etag":  "W/\"1535a780-0fc8-4bba-a15a-
093ecac9b88b\"",
                                                "ResourceId":  "AllowAll_Outbound",
                                                "Properties":  {
                                                                    "Protocol":  "All",
                                                                    "SourcePortRange":  "0-
65535",
                                                                    "DestinationPortRange":
"0-65535",
                                                                    "Action":  "Allow",
                                                                    "SourceAddressPrefix":
"*",
                                                                    "DestinationAddressPrefix":  "*",
                                                                    "Priority":  "110",
                                                                    "Description":  null,
                                                                    "Type":  "Outbound",
                                                                    "Logging":  "Enabled",
                                                                    "ProvisioningState":
"Succeeded"
                                                                }
                                            }
                                        ],
                        "IpConfigurations":  [
                                                ],
                        "Subnets":  [
                                            {
                                                "ResourceMetadata":  null,
                                                "ResourceRef":
"/virtualNetworks/10_0_1_0/subnets/Subnet1",
                                                "InstanceId":  "00000000-0000-0000-0000-
000000000000",
                                                "Etag":  null,
                                                "ResourceId":  null,
                                                "Properties":  null
                                            }
                                        ]
                    }
}
```


Étapes suivantes

Pour plus d'informations, consultez :

- Vue d'ensemble du pare-feu du centre de données.
- Vue d'ensemble du contrôleur de réseau.
- SDN dans Azure Local et Windows Server.

Dernière mise à jour : 15/09/2026

Configurer l’équilibreur de charge logicielle pour l’équilibrage de charge et la traduction d’adresses réseau (NAT)

Article • 09/03/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI versions 21H2 et 20H2

Vous pouvez utiliser cette rubrique afin de découvrir comment utiliser l’équilibreur de charge logiciel SDN (Software-Defined Networking) pour fournir une fonctionnalité NAT (traduction d’adresses réseau) sortante, une fonctionnalité NAT entrante ou un équilibrage de charge entre plusieurs instances d’une application.

Vue d’ensemble d’un équilibreur de charge logicielle

L’équilibreur de charge logicielle SDN offre une haute disponibilité et des performances réseau optimales à vos applications. Il s’agit d’un équilibreur de charge de Couche 4 (TCP, UDP) qui distribue le trafic entrant entre les instances de service saines au sein des services cloud, ou les machines virtuelles définies dans un ensemble d’équilibreurs de charge.

Configurez l’équilibreur de charge logiciel pour effectuer les opérations suivantes :

- Équilibrer la charge du trafic entrant externe vers un réseau virtuel et vers des machines virtuelles, également appelé équilibrage de charge d’adresses IP virtuelles publiques.
- Équilibrer la charge du trafic entrant entre les machines virtuelles d’un réseau virtuel, entre les machines virtuelles des services cloud ou entre les ordinateurs locaux et les machines virtuelles d’un réseau virtuel entre différents locaux.
- Rediriger le trafic réseau des machines virtuelles du réseau virtuel vers des destinations externes à l’aide de la fonctionnalité de traduction d’adresses réseau (NAT). Porte également le nom de NAT sortant.
- Rediriger le trafic externe vers une machine virtuelle spécifique. Porte également le nom de NAT entrant.

Exemple : Créer une adresse IP virtuelle publique pour l'équilibrage de charge d'un pool de deux machines virtuelles dans un réseau virtuel

Dans cet exemple, vous créez un objet d'équilibreur de charge avec une adresse IP virtuelle publique et deux machines virtuelles membres d'un pool pour traiter les requêtes adressées à l'adresse IP virtuelle. Cet exemple de code ajoute également une sonde d'intégrité HTTP pour détecter si l'un des membres du pool cesse de répondre.

1. Préparez l'objet d'équilibreur de charge.

   PowerShell

   ```
   import-module NetworkController

   $URI = "https://sdn.contoso.com"

   $LBResourceId = "LB2"

   $LoadBalancerProperties = new-object
   Microsoft.Windows.NetworkController.LoadBalancerProperties
   ```

2. Affectez une adresse IP de front-end, communément appelée adresse IP virtuelle.

   L'adresse IP virtuelle doit correspondre à une adresse IP inutilisée dans l'un des pools d'adresses IP de réseau logique fournis au gestionnaire de l'équilibreur de charge.

   PowerShell

   ```
   $VIPIP = "10.127.134.5"
   $VIPLogicalNetwork = get-networkcontrollerlogicalnetwork -
   ConnectionUri $uri -resourceid "PublicVIP" -PassInnerException

   $FrontEndIPConfig = new-object
   Microsoft.Windows.NetworkController.LoadBalancerFrontendIpConfiguration
   $FrontEndIPConfig.ResourceId = "FE1"
   $FrontEndIPConfig.ResourceRef =
   "/loadBalancers/$LBResourceId/frontendIPConfigurations/$($FrontEndIPCon
   fig.ResourceId)"

   $FrontEndIPConfig.Properties = new-object
   Microsoft.Windows.NetworkController.LoadBalancerFrontendIpConfiguration
   Properties
   $FrontEndIPConfig.Properties.Subnet = new-object
   Microsoft.Windows.NetworkController.Subnet
   ```

```
 $FrontEndIPConfig.Properties.Subnet.ResourceRef =
$VIPLogicalNetwork.Properties.Subnets[0].ResourceRef
 $FrontEndIPConfig.Properties.PrivateIPAddress = $VIPIP
 $FrontEndIPConfig.Properties.PrivateIPAllocationMethod = "Static"

 $LoadBalancerProperties.FrontEndIPConfigurations += $FrontEndIPConfig
```

3. Allouez un pool d'adresses de back-end, qui contient les adresses IP dynamiques composant les membres de l'ensemble de machines virtuelles à charge équilibrée.

PowerShell

```
 $BackEndAddressPool = new-object
Microsoft.Windows.NetworkController.LoadBalancerBackendAddressPool
 $BackEndAddressPool.ResourceId = "BE1"
 $BackEndAddressPool.ResourceRef =
"/loadBalancers/$LBResourceId/backendAddressPools/$($BackEndAddressPool
.ResourceId)"

 $BackEndAddressPool.Properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerBackendAddressPoolProp
rties

 $LoadBalancerProperties.backendAddressPools += $BackEndAddressPool
```

4. Définissez une sonde d'intégrité que l'équilibreur de charge va utiliser pour déterminer l'état d'intégrité des membres du pool de back-ends.

   Dans cet exemple, vous définissez une sonde HTTP qui interroge le RequestPath de « /health.htm ». La requête s'exécute toutes les 5 secondes, comme le spécifie la propriété IntervalInSeconds.

   La sonde d'intégrité doit recevoir un code de réponse HTTP 200 pour 11 requêtes consécutives afin que la sonde considère l'IP de back-end comme saine. Si l'adresse IP de back-end n'est pas saine, elle ne reçoit pas de trafic de l'équilibreur de charge.

   > **ⓘ Important**
   >
   > Ne bloquez pas le trafic à destination ou en provenance de la première adresse IP du sous-réseau pour les listes ACL (listes de contrôle d'accès) que vous appliquez à l'IP de back-end, car il s'agit du point d'origine des sondes.

   Utilisez l'exemple suivant pour définir une sonde d'intégrité.

PowerShell

```
 $Probe = new-object
Microsoft.Windows.NetworkController.LoadBalancerProbe
 $Probe.ResourceId = "Probe1"
 $Probe.ResourceRef =
"/loadBalancers/$LBResourceId/Probes/$($Probe.ResourceId)"

 $Probe.properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerProbeProperties
 $Probe.properties.Protocol = "HTTP"
 $Probe.properties.Port = "80"
 $Probe.properties.RequestPath = "/health.htm"
 $Probe.properties.IntervalInSeconds = 5
 $Probe.properties.NumberOfProbes = 11

 $LoadBalancerProperties.Probes += $Probe
```

5. Définissez une règle d'équilibrage de charge pour envoyer le trafic qui arrive à l'IP de front-end vers l'IP de back-end. Dans cet exemple, le pool de back-ends reçoit le trafic TCP sur le port 80.

   Utilisez l'exemple suivant pour définir une règle d'équilibrage de charge :

   PowerShell

```
$Rule = new-object
Microsoft.Windows.NetworkController.LoadBalancingRule
$Rule.ResourceId = "webserver1"

$Rule.Properties = new-object
Microsoft.Windows.NetworkController.LoadBalancingRuleProperties
$Rule.Properties.FrontEndIPConfigurations += $FrontEndIPConfig
$Rule.Properties.backendaddresspool = $BackEndAddressPool
$Rule.Properties.protocol = "TCP"
$Rule.Properties.FrontEndPort = 80
$Rule.Properties.BackEndPort = 80
$Rule.Properties.IdleTimeoutInMinutes = 4
$Rule.Properties.Probe = $Probe

$LoadBalancerProperties.loadbalancingRules += $Rule
```

6. Ajoutez la configuration de l'équilibreur de charge au Contrôleur de réseau.

   Utilisez l'exemple suivant pour ajouter la configuration de l'équilibreur de charge au Contrôleur de réseau :

   PowerShell

```
 $LoadBalancerResource = New-NetworkControllerLoadBalancer -
ConnectionUri $URI -ResourceId $LBResourceId -Properties
```

```
$LoadBalancerProperties -Force -PassInnerException
```

7. Suivez l'exemple ci-après pour ajouter les interfaces réseau à ce pool de back-ends.

Exemple : Utiliser l'équilibreur de charge logiciel pour la fonctionnalité NAT sortante

Dans cet exemple, vous configurez l'équilibreur de charge logiciel avec un pool de back-ends pour fournir une fonctionnalité NAT sortante à une machine virtuelle située dans l'espace d'adressage privé d'un réseau virtuel afin qu'elle puisse établir des connexions sortantes vers Internet.

1. Créez les propriétés de l'équilibreur de charge, l'IP de front-end et le pool de back-ends.

PowerShell

```
import-module NetworkController
$URI = "https://sdn.contoso.com"

$LBResourceId = "OutboundNATMMembers"
$VIPIP = "10.127.134.6"

$VIPLogicalNetwork = get-networkcontrollerlogicalnetwork -
ConnectionUri $uri -resourceid "PublicVIP" -PassInnerException

$LoadBalancerProperties = new-object
Microsoft.Windows.NetworkController.LoadBalancerProperties

$FrontEndIPConfig = new-object
Microsoft.Windows.NetworkController.LoadBalancerFrontendIpConfiguration
$FrontEndIPConfig.ResourceId = "FE1"
$FrontEndIPConfig.ResourceRef =
"/loadBalancers/$LBResourceId/frontendIPConfigurations/$($FrontEndIPCon
fig.ResourceId)"

$FrontEndIPConfig.Properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerFrontendIpConfiguration
Properties
$FrontEndIPConfig.Properties.Subnet = new-object
Microsoft.Windows.NetworkController.Subnet
$FrontEndIPConfig.Properties.Subnet.ResourceRef =
$VIPLogicalNetwork.Properties.Subnets[0].ResourceRef
$FrontEndIPConfig.Properties.PrivateIPAddress = $VIPIP
$FrontEndIPConfig.Properties.PrivateIPAllocationMethod = "Static"

$LoadBalancerProperties.FrontEndIPConfigurations += $FrontEndIPConfig
```

```
 $BackEndAddressPool = new-object
Microsoft.Windows.NetworkController.LoadBalancerBackendAddressPool
 $BackEndAddressPool.ResourceId = "BE1"
 $BackEndAddressPool.ResourceRef =
"/loadBalancers/$LBResourceId/backendAddressPools/$($BackEndAddressPool
.ResourceId)"
 $BackEndAddressPool.Properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerBackendAddressPoolProperties

 $LoadBalancerProperties.backendAddressPools += $BackEndAddressPool
```

2. Définissez la règle NAT sortante.

PowerShell

```
 $OutboundNAT = new-object
Microsoft.Windows.NetworkController.LoadBalancerOutboundNatRule
 $OutboundNAT.ResourceId = "onat1"

 $OutboundNAT.properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerOutboundNatRuleProperties
 $OutboundNAT.properties.frontendipconfigurations += $FrontEndIPConfig
 $OutboundNAT.properties.backendaddresspool = $BackEndAddressPool
 $OutboundNAT.properties.protocol = "ALL"

 $LoadBalancerProperties.OutboundNatRules += $OutboundNAT
```

3. Ajoutez l'objet d'équilibreur de charge au Contrôleur de réseau.

PowerShell

```
 $LoadBalancerResource = New-NetworkControllerLoadBalancer -
ConnectionUri $URI -ResourceId $LBResourceId -Properties
$LoadBalancerProperties -Force -PassInnerException
```

4. Suivez l'exemple ci-après pour ajouter les interfaces réseau auxquelles vous souhaitez fournir l'accès à Internet.

Exemple : Ajouter des interfaces réseau au pool de back-ends

Dans cet exemple, vous ajoutez des interfaces réseau au pool de back-ends. Vous devez répéter cette étape pour chaque interface réseau pouvant traiter les requêtes adressées à l'adresse IP virtuelle.

Vous pouvez également répéter ce processus sur une seule interface réseau pour l'ajouter à plusieurs objets d'équilibreur de charge. Par exemple, vous avez un objet d'équilibreur de charge pour une adresse IP virtuelle de serveur web, et un objet d'équilibreur de charge distinct pour fournir la fonctionnalité NAT sortante.

1. Récupérez l'objet d'équilibreur de charge contenant le pool de back-ends pour ajouter une interface réseau.

   PowerShell

   ```
   $lbresourceid = "LB2"
   $lb = get-networkcontrollerloadbalancer -connectionuri $uri -resourceID
   $LBResourceId -PassInnerException
   ```

2. Récupérez l'interface réseau, puis ajoutez le pool d'adresses de back-end au tableau loadbalancerbackendaddresspools.

   PowerShell

   ```
   $nic = get-networkcontrollernetworkinterface  -connectionuri $uri -
   resourceid 6daca142-7d94-0000-1111-c38c0141be06 -PassInnerException
   $nic.properties.IpConfigurations[0].properties.LoadBalancerBackendAddre
   ssPools += $lb.properties.backendaddresspools[0]
   ```

3. Placez l'interface réseau pour appliquer le changement.

   PowerShell

   ```
   new-networkcontrollernetworkinterface  -connectionuri $uri -resourceid
   6daca142-7d94-0000-1111-c38c0141be06 -properties $nic.properties -force
   -PassInnerException
   ```

Exemple : Utiliser l'équilibreur de charge logiciel pour la redirection du trafic

Si vous devez mapper une adresse IP virtuelle à une seule interface réseau sur un réseau virtuel sans définir de ports individuels, vous pouvez créer une règle de redirection L3. Cette règle redirige tout le trafic à destination et en provenance de la machine virtuelle via l'adresse IP virtuelle affectée contenue dans un objet PublicIPAddress.

Si vous avez défini l'adresse IP virtuelle et l'adresse IP dynamique dans le même sous-réseau, cela équivaut à effectuer une redirection L3 sans NAT.

> **Notes**
>
> Ce processus ne vous oblige pas à créer un objet d'équilibreur de charge. L'affectation de PublicIPAddress à l'interface réseau suffit à l'équilibreur de charge logiciel pour effectuer sa configuration.

1. Créez un objet d'adresse IP publique pour contenir l'adresse IP virtuelle.

PowerShell

```
$publicIPProperties = new-object
Microsoft.Windows.NetworkController.PublicIpAddressProperties
$publicIPProperties.ipaddress = "10.127.134.7"
$publicIPProperties.PublicIPAllocationMethod = "static"
$publicIPProperties.IdleTimeoutInMinutes = 4
$publicIP = New-NetworkControllerPublicIpAddress -ResourceId "MyPIP" -
Properties $publicIPProperties -ConnectionUri $uri -Force -
PassInnerException
```

2. Affectez PublicIPAddress à une interface réseau.

PowerShell

```
$nic = get-networkcontrollernetworkinterface  -connectionuri $uri -
resourceid 6daca142-7d94-0000-1111-c38c0141be06
$nic.properties.IpConfigurations[0].Properties.PublicIPAddress =
$publicIP
New-NetworkControllerNetworkInterface -ConnectionUri $uri -ResourceId
$nic.ResourceId -Properties $nic.properties -PassInnerException
```

Exemple : Utiliser l'équilibreur de charge logiciel pour la redirection du trafic avec une adresse IP virtuelle allouée de manière dynamique

Cet exemple répète la même action que l'exemple précédent. Toutefois, il alloue automatiquement l'adresse IP virtuelle à partir du pool d'adresses IP virtuelles disponibles dans l'équilibreur de charge au lieu de spécifier une adresse IP particulière.

1. Créez un objet d'adresse IP publique pour contenir l'adresse IP virtuelle.

PowerShell

```
$publicIPProperties = new-object
Microsoft.Windows.NetworkController.PublicIpAddressProperties
$publicIPProperties.PublicIPAllocationMethod = "dynamic"
$publicIPProperties.IdleTimeoutInMinutes = 4
$publicIP = New-NetworkControllerPublicIpAddress -ResourceId "MyPIP" -
Properties $publicIPProperties -ConnectionUri $uri -Force -
PassInnerException
```

2. Interrogez la ressource PublicIPAddress pour déterminer l'adresse IP affectée.

PowerShell

```
 (Get-NetworkControllerPublicIpAddress -ConnectionUri $uri -ResourceId
"MyPIP").properties
```

La propriété IpAddress contient l'adresse affectée. Le résultat ressemble à ce qui suit :

```
Counters                  : {}
ConfigurationState        :
IpAddress                 : 10.127.134.2
PublicIPAddressVersion    : IPv4
PublicIPAllocationMethod  : Dynamic
IdleTimeoutInMinutes      : 4
DnsSettings               :
ProvisioningState         : Succeeded
IpConfiguration           :
PreviousIpConfiguration   :
```

3. Affectez PublicIPAddress à une interface réseau.

PowerShell

```
$nic = get-networkcontrollernetworkinterface  -connectionuri $uri -
resourceid 6daca142-7d94-0000-1111-c38c0141be06
$nic.properties.IpConfigurations[0].Properties.PublicIPAddress =
$publicIP
New-NetworkControllerNetworkInterface -ConnectionUri $uri -ResourceId
$nic.ResourceId -Properties $nic.properties -PassInnerException
```

Exemple : Supprimer une adresse IP publique utilisée pour la redirection du

trafic, et la retourner au pool d’adresses IP virtuelles

Cet exemple supprime la ressource PublicIPAddress créée par les exemples précédents. Une fois la ressource PublicIPAddress supprimée, la référence à PublicIPAddress est automatiquement supprimée de l’interface réseau, le trafic cesse d’être redirigé, et l’adresse IP est retournée au pool d’adresses IP virtuelles publiques pour être réutilisée.

4. Supprimer l’adresse IP publique

PowerShell

```
Remove-NetworkControllerPublicIPAddress -ConnectionURI $uri -ResourceId
"MyPIP"
```

Utiliser des équipements virtuels réseau sur un réseau virtuel

Article • 11/04/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI versions 21H2 et 20H2

Dans cette rubrique, vous allez apprendre à déployer des appliances virtuelles réseau sur des réseaux virtuels de locataire. Vous pouvez ajouter des appliances virtuelles réseau à des réseaux qui exécutent des fonctions de routage et de mise en miroir des ports définies par l'utilisateur.

Types d'appliances virtuelles réseau

Vous pouvez utiliser l'un des deux types d'appliances virtuelles :

1. **Routage défini par l'utilisateur** : remplace les routeurs distribués sur le réseau virtuel par les fonctionnalités de routage de l'appliance virtuelle. Avec le routage défini par l'utilisateur, l'appliance virtuelle est utilisée en tant que routeur entre les sous-réseaux virtuels du réseau virtuel.

2. **Mise en miroir des ports** : tout le trafic réseau entrant ou sortant au niveau du port supervisé est dupliqué et envoyé à une appliance virtuelle à des fins d'analyse.

Déployer une appliance virtuelle réseau

Pour déployer une appliance virtuelle réseau, vous devez d'abord créer une machine virtuelle qui contient l'appliance, puis connecter la machine virtuelle aux sous-réseaux de réseau virtuel appropriés. Pour plus d'informations, consultez Créer une machine virtuelle de locataire et établir la connexion à un réseau virtuel locataire ou un réseau local virtuel.

Certaines appliances nécessitent plusieurs cartes réseau virtuelles. En règle générale, une carte réseau dédiée à la gestion de l'appliance, tandis que les autres cartes traitent le trafic. Si votre appliance nécessite plusieurs cartes réseau, vous devez créer chaque interface réseau dans le contrôleur de réseau. Vous devez également affecter un ID d'interface sur chaque hôte pour chacun des adaptateurs supplémentaires qui se trouvent sur des sous-réseaux virtuels différents.

Une fois que vous avez déployé l'appliance virtuelle réseau, vous pouvez utiliser l'appliance pour le routage défini, la mise en miroir de ports, ou les deux.

Exemple : routage défini par l'utilisateur

Pour la plupart des environnements, vous avez uniquement besoin des itinéraires système déjà définis par le routeur distribué du réseau virtuel. Toutefois, vous pouvez créer une table d'itinéraires et ajouter un ou plusieurs itinéraires dans des cas spécifiques, par exemple :

- Forcer le tunneling vers Internet via votre réseau local.
- Utiliser des appliances virtuelles dans votre environnement.

Pour ces scénarios, vous devez créer une table de routage et ajouter des itinéraires définis par l'utilisateur à la table. Vous pouvez avoir plusieurs tables d'itinéraires et celles-ci peuvent être associées à un ou plusieurs sous-réseaux. Vous ne pouvez associer chaque sous-réseau qu'à une seule table de routage. L'ensemble des machines virtuelles d'un sous-réseau utilisent la table d'itinéraires associée à ce sous-réseau.

Les sous-réseaux s'appuient sur des itinéraires système jusqu'à ce qu'une table de routage leur soit associée. Une fois que l'association existe, le routage se base sur la correspondance de préfixe la plus longue parmi les itinéraires définis par l'utilisateur et les itinéraires du système. S'il existe plusieurs itinéraires avec la même correspondance LPM, l'itinéraire défini par l'utilisateur est sélectionné en premier, avant l'itinéraire système.

Procédure :

1. Créez les propriétés de la table de routage, qui contient tous les itinéraires définis par l'utilisateur.

   Les routes système s'appliquent toujours selon les règles définies ci-dessus.

   PowerShell

   ```
   $routetableproperties = new-object
   Microsoft.Windows.NetworkController.RouteTableProperties
   ```

2. Ajoutez un itinéraire aux propriétés de la table de routage.

   Tout itinéraire destiné au sous-réseau 12.0.0.0/8 est routé vers l'appliance virtuelle à l'adresse 192.168.1.10. L'appliance doit avoir une carte réseau virtuelle attachée au réseau virtuel avec cette adresse IP affectée à une interface réseau.

PowerShell

```
$route = new-object Microsoft.Windows.NetworkController.Route
$route.ResourceID = "0_0_0_0_0"
$route.properties = new-object
Microsoft.Windows.NetworkController.RouteProperties
$route.properties.AddressPrefix = "0.0.0.0/0"
$route.properties.nextHopType = "VirtualAppliance"
$route.properties.nextHopIpAddress = "192.168.1.10"
$routetableproperties.routes += $route
```

Conseil

Si vous souhaitez ajouter d'autres itinéraires, répétez cette étape pour chaque itinéraire que vous souhaitez définir.

3. Ajoutez la table de routage au contrôleur de réseau.

PowerShell

```
$routetable = New-NetworkControllerRouteTable -ConnectionUri $uri -
ResourceId "Route1" -Properties $routetableproperties
```

4. Appliquez la table de routage au sous-réseau virtuel.

   Lorsque vous appliquez la table de routage au sous-réseau virtuel, le premier sous-réseau virtuel du réseau Tenant1_Vnet1 utilise la table de routage. Vous pouvez affecter la table de routage à autant de sous-réseaux du réseau virtuel que vous le souhaitez.

PowerShell

```
$vnet = Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -
ResourceId "Tenant1_VNet1"
$vnet.properties.subnets[0].properties.RouteTable = $routetable
new-networkcontrollervirtualnetwork -connectionuri $uri -properties
$vnet.properties -resourceId $vnet.resourceid
```

Dès que vous appliquez la table de routage au réseau virtuel, le trafic est transféré à l'appliance virtuelle. Vous devez configurer la table de routage dans l'appliance virtuelle pour transférer le trafic, d'une manière adaptée à votre environnement.

Exemple : Mise en miroir de ports

Dans cet exemple, vous configurez le trafic pour MyVM_Ethernet1 pour mettre en miroir Appliance_Ethernet1. Nous partons du principe que vous avez déployé deux machines virtuelles, l'une en tant qu'appliance et l'autre en tant que machine virtuelle à surveiller avec la mise en miroir.

L'appliance doit avoir une deuxième interface réseau pour la gestion. Une fois que vous avez activé la mise en miroir en tant que destination sur Appliciance_Ethernet1, elle ne reçoit plus le trafic destiné à l'interface IP qui y est configurée.

Procédure :

1. Obtenez le réseau virtuel sur lequel se trouvent vos machines virtuelles.

   PowerShell

   ```
   $vnet = Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -
   ResourceId "Tenant1_VNet1"
   ```

2. Obtenez les interfaces réseau du contrôleur de réseau pour la source et la destination de mise en miroir.

   PowerShell

   ```
   $dstNic = get-networkcontrollernetworkinterface -ConnectionUri $uri -
   ResourceId "Appliance_Ethernet1"
   $srcNic = get-networkcontrollernetworkinterface -ConnectionUri $uri -
   ResourceId "MyVM_Ethernet1"
   ```

3. Créez un objet serviceinsertionproperties pour contenir les règles de mise en miroir de ports et l'élément qui représente l'interface de destination.

   PowerShell

   ```
   $portmirror =
   [Microsoft.Windows.NetworkController.ServiceInsertionProperties]::new()
   $portMirror.Priority = 1
   ```

4. Créez un objet serviceinsertionrules pour contenir les règles qui doivent être mises en correspondance pour que le trafic soit envoyé à l'appliance.

   Les règles définies ci-dessous correspondent à l'ensemble du trafic, à la fois entrant et sortant, qui représente un miroir traditionnel. Vous pouvez ajuster ces règles si vous souhaitez mettre en miroir un port spécifique, ou une source/des destinations spécifiques.

PowerShell

```
$portmirror.ServiceInsertionRules =
[Microsoft.Windows.NetworkController.ServiceInsertionRule[]]::new(1)

$portmirror.ServiceInsertionRules[0] =
[Microsoft.Windows.NetworkController.ServiceInsertionRule]::new()
$portmirror.ServiceInsertionRules[0].ResourceId = "Rule1"
$portmirror.ServiceInsertionRules[0].Properties =
[Microsoft.Windows.NetworkController.ServiceInsertionRuleProperties]::n
ew()

$portmirror.ServiceInsertionRules[0].Properties.Description = "Port
Mirror Rule"
$portmirror.ServiceInsertionRules[0].Properties.Protocol = "All"
$portmirror.ServiceInsertionRules[0].Properties.SourcePortRangeStart =
"0"
$portmirror.ServiceInsertionRules[0].Properties.SourcePortRangeEnd =
"65535"
$portmirror.ServiceInsertionRules[0].Properties.DestinationPortRangeSta
rt = "0"
$portmirror.ServiceInsertionRules[0].Properties.DestinationPortRangeEnd
= "65535"
$portmirror.ServiceInsertionRules[0].Properties.SourceSubnets = "*"
$portmirror.ServiceInsertionRules[0].Properties.DestinationSubnets =
"*"
```

5. Créez un objet serviceinsertionelements pour contenir l'interface réseau de l'appliance mise en miroir.

PowerShell

```
$portmirror.ServiceInsertionElements =
[Microsoft.Windows.NetworkController.ServiceInsertionElement[]]::new(1)

$portmirror.ServiceInsertionElements[0] =
[Microsoft.Windows.NetworkController.ServiceInsertionElement]::new()
$portmirror.ServiceInsertionElements[0].ResourceId = "Element1"
$portmirror.ServiceInsertionElements[0].Properties =
[Microsoft.Windows.NetworkController.ServiceInsertionElementProperties]
::new()

$portmirror.ServiceInsertionElements[0].Properties.Description = "Port
Mirror Element"
$portmirror.ServiceInsertionElements[0].Properties.NetworkInterface =
$dstNic
$portmirror.ServiceInsertionElements[0].Properties.Order = 1
```

6. Ajoutez l'objet d'insertion de service au Contrôleur de réseau.

Lorsque vous émettez cette commande, tout le trafic vers l'interface réseau de l'appliance spécifiée à l'étape précédente s'arrête.

PowerShell

```
$portMirror = New-NetworkControllerServiceInsertion -ConnectionUri $uri
-Properties $portmirror -ResourceId "MirrorAll"
```

7. Mettez à jour l'interface réseau de la source à mettre en miroir.

PowerShell

```
$srcNic.Properties.IpConfigurations[0].Properties.ServiceInsertion =
$portMirror
$srcNic = New-NetworkControllerNetworkInterface -ConnectionUri $uri  -
Properties $srcNic.Properties -ResourceId $srcNic.ResourceId
```

Une fois ces étapes terminées, l'interface Appliance_Ethernet1 reflète le trafic de l'interface MyVM_Ethernet1.

Clustering invité dans un réseau virtuel

Article • 11/04/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI versions 21H2 et 20H2

Les machines virtuelles connectées à un réseau virtuel sont uniquement autorisées à utiliser les adresses IP que le contrôleur de réseau a affectées pour communiquer sur le réseau. Les technologies de clustering qui nécessitent une adresse IP flottante, comme le clustering de basculement Microsoft, nécessitent des étapes supplémentaires pour fonctionner correctement.

La méthode permettant d'atteindre l'adresse IP flottante consiste à utiliser une adresse IP virtuelle (VIP) Software Load Balancer (SLB). L'équilibreur de charge logiciel doit être configuré avec une sonde d'intégrité sur un port sur cette adresse IP afin que SLB dirige le trafic vers l'ordinateur qui possède actuellement cette adresse IP.

Exemple : Configuration de l'équilibreur de charge

Cet exemple part du principe que vous avez déjà créé les machines virtuelles qui deviendront des nœuds de cluster et que vous les avez attachées à un Réseau virtuel. Pour obtenir des conseils, consultez Créer une machine virtuelle et établir la connexion à un réseau virtuel locataire ou un réseau local virtuel.

Dans cet exemple, vous allez créer une adresse IP virtuelle (192.168.2.100) pour représenter l'adresse IP flottante du cluster et configurer une sonde d'intégrité pour surveiller le port TCP 59999 afin de déterminer le nœud actif.

1. Sélectionnez l'adresse IP virtuelle.

   Préparez-vous en affectant une adresse IP VIP, qui peut être n'importe quelle adresse inutilisée ou réservée dans le même sous-réseau que les nœuds de cluster. L'adresse IP virtuelle doit correspondre à l'adresse flottante du cluster.

   PowerShell

   ```
   $VIP = "192.168.2.100"
   $subnet = "Subnet2"
   $VirtualNetwork = "MyNetwork"
   $ResourceId = "MyNetwork_InternalVIP"
   ```

2. Créez l'objet de propriétés de l'équilibreur de charge.

PowerShell

```
$LoadBalancerProperties = new-object
Microsoft.Windows.NetworkController.LoadBalancerProperties
```

3. Créez une adresse IP frontale.

PowerShell

```
$LoadBalancerProperties.frontendipconfigurations += $FrontEnd = new-
object
Microsoft.Windows.NetworkController.LoadBalancerFrontendIpConfiguration
$FrontEnd.properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerFrontendIpConfiguration
Properties
$FrontEnd.resourceId = "Frontend1"
$FrontEnd.resourceRef =
"/loadBalancers/$ResourceId/frontendIPConfigurations/$($FrontEnd.resour
ceId)"
$FrontEnd.properties.subnet = new-object
Microsoft.Windows.NetworkController.Subnet
$FrontEnd.properties.subnet.ResourceRef =
"/VirtualNetworks/MyNetwork/Subnets/Subnet2"
$FrontEnd.properties.privateIPAddress = $VIP
$FrontEnd.properties.privateIPAllocationMethod = "Static"
```

4. Créez un pool de back-ends pour contenir les nœuds de cluster.

PowerShell

```
$BackEnd = new-object
Microsoft.Windows.NetworkController.LoadBalancerBackendAddressPool
$BackEnd.properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerBackendAddressPoolPrope
rties
$BackEnd.resourceId = "Backend1"
$BackEnd.resourceRef =
"/loadBalancers/$ResourceId/backendAddressPools/$($BackEnd.resourceId)"
$LoadBalancerProperties.backendAddressPools += $BackEnd
```

5. Ajoutez une sonde pour détecter le nœud de cluster sur lequel l'adresse flottante est actuellement active.

ⓘ **Notes**

La sonde interroge l'adresse permanente de la machine virtuelle au niveau du port défini ci-dessous. Le port doit répondre uniquement sur le nœud actif.

PowerShell

```
$LoadBalancerProperties.probes += $lbprobe = new-object
Microsoft.Windows.NetworkController.LoadBalancerProbe
$lbprobe.properties = new-object
Microsoft.Windows.NetworkController.LoadBalancerProbeProperties

$lbprobe.ResourceId = "Probe1"
$lbprobe.resourceRef =
"/loadBalancers/$ResourceId/Probes/$($lbprobe.resourceId)"
$lbprobe.properties.protocol = "TCP"
$lbprobe.properties.port = "59999"
$lbprobe.properties.IntervalInSeconds = 5
$lbprobe.properties.NumberOfProbes = 11
```

6. Ajoutez les règles d'équilibrage de charge pour le port TCP 1433.

   Vous pouvez modifier le protocole et le port en fonction des besoins. Vous pouvez également répéter cette étape plusieurs fois pour d'autres ports et protocoles sur cette VIP. Il est important qu'EnableFloatingIP soit défini sur $true, car cela indique à l'équilibreur de charge d'envoyer le paquet au nœud avec l'adresse IP virtuelle d'origine en place.

PowerShell

```
$LoadBalancerProperties.loadbalancingRules += $lbrule = new-object
Microsoft.Windows.NetworkController.LoadBalancingRule
$lbrule.properties = new-object
Microsoft.Windows.NetworkController.LoadBalancingRuleProperties
$lbrule.ResourceId = "Rules1"

$lbrule.properties.frontendipconfigurations += $FrontEnd
$lbrule.properties.backendaddresspool = $BackEnd
$lbrule.properties.protocol = "TCP"
$lbrule.properties.frontendPort = $lbrule.properties.backendPort = 1433
$lbrule.properties.IdleTimeoutInMinutes = 4
$lbrule.properties.EnableFloatingIP = $true
$lbrule.properties.Probe = $lbprobe
```

7. Créez l'équilibreur de charge dans le contrôleur de réseau.

PowerShell

```
$lb = New-NetworkControllerLoadBalancer -ConnectionUri $URI -ResourceId
$ResourceId -Properties $LoadBalancerProperties -Force
```

8. Ajoutez les nœuds de cluster au pool de back-ends.

   Vous pouvez ajouter autant de nœuds au pool que nécessaire pour le cluster.

   PowerShell

   ```
   # Cluster Node 1

   $nic = get-networkcontrollernetworkinterface  -connectionuri $uri -
   resourceid "ClusterNode1_Network-Adapter"
   $nic.properties.IpConfigurations[0].properties.LoadBalancerBackendAddre
   ssPools += $lb.properties.backendaddresspools[0]
   $nic = new-networkcontrollernetworkinterface  -connectionuri $uri -
   resourceid $nic.resourceid -properties $nic.properties -force

    # Cluster Node 2

   $nic = get-networkcontrollernetworkinterface  -connectionuri $uri -
   resourceid "ClusterNode2_Network-Adapter"
   $nic.properties.IpConfigurations[0].properties.LoadBalancerBackendAddre
   ssPools += $lb.properties.backendaddresspools[0]
   $nic = new-networkcontrollernetworkinterface  -connectionuri $uri -
   resourceid $nic.resourceid -properties $nic.properties -force
   ```

   Une fois que vous avez créé l'équilibreur de charge et ajouté les interfaces réseau au pool de back-ends, vous êtes prêt à configurer le cluster.

9. (Facultatif) Si vous utilisez un cluster de basculement Microsoft, passez à l'exemple suivant.

Exemple 2 : Configuration d'un cluster de basculement Microsoft

Vous pouvez utiliser les étapes suivantes pour configurer un cluster de basculement.

1. Installez et configurez les propriétés d'un cluster de basculement.

   PowerShell

   ```
   add-windowsfeature failover-clustering -IncludeManagementTools
   Import-module failoverclusters

   $ClusterName = "MyCluster"

   $ClusterNetworkName = "Cluster Network 1"
   $IPResourceName =
   $ILBIP = "192.168.2.100"
   ```

```
$nodes = @("DB1", "DB2")
```

2. Créez le cluster sur un nœud.

PowerShell

```
New-Cluster -Name $ClusterName -NoStorage -Node $nodes[0]
```

3. Arrêtez la ressource de cluster.

PowerShell

```
Stop-ClusterResource "Cluster Name"
```

4. Définissez l'adresse IP du cluster et le port de sonde.

   L'adresse IP doit correspondre à l'adresse IP frontale utilisée dans l'exemple précédent, et le port de sonde doit correspondre au port de sonde dans l'exemple précédent.

PowerShell

```
Get-ClusterResource "Cluster IP Address" | Set-ClusterParameter -
Multiple
@{"Address"="$ILBIP";"ProbePort"="59999";"SubnetMask"="255.255.255.255"
;"Network"="$ClusterNetworkName";"EnableDhcp"=0}
```

5. Démarrez les ressources du cluster.

PowerShell

```
 Start-ClusterResource "Cluster IP Address"  -Wait 60
 Start-ClusterResource "Cluster Name"  -Wait 60
```

6. Ajoutez les nœuds restants.

PowerShell

```
Add-ClusterNode $nodes[1]
```

Votre cluster est actif. Le trafic vers l'adresse IP virtuelle sur le port spécifié est dirigé vers le nœud actif.

Gérer SDN Multisite pour Azure Local et Windows Server

> S'applique à Windows Server 2025

Cet article explique comment déployer et gérer la solution multisite SDN (Software Defined Networking) pour Windows Server à l'aide de Windows Admin Center.

Pour obtenir une vue d'ensemble des capacités et limitations actuelles de SDN Multisite, consultez Vue d'ensemble de SDN Multisite.

Prérequis

Avant de pouvoir activer SDN Multisite, vérifiez que les conditions préalables suivantes sont remplies :

- Vous devez avoir accès aux clusters Windows Server 2025 ou ultérieur déployés sur deux sites physiques distincts.
- Il doit y avoir une connectivité réseau physique sous-jacente entre les sites. En outre, le nom du réseau du fournisseur doit être le même sur les deux sites.
- SDN doit être installé sur les deux sites séparément, à l'aide de scripts Windows Admin Center ou SDN Express. Des sites distincts sont nécessaires pour que les composants SDN, tels que les machines virtuelles du contrôleur de réseau, les machines virtuelles multiplexeur d'équilibreur de charge logicielle et les machines virtuelles de passerelle SDN soient uniques à chaque site.
- Votre configuration de pare-feu doit autoriser le port TCP 49001 pour la communication entre clusters.
- Windows Admin Center version 2311 ou ultérieure doit être installé sur votre PC ou serveur d'administration. Consultez Installer Windows Admin Center.
- L'un des deux sites ne doit pas avoir de réseaux virtuels, de groupes de sécurité réseau et d'itinéraires définis par l'utilisateur configurés.
- Le pool MAC SDN ne doit pas chevaucher les deux sites.

- Les pools IP pour les réseaux logiques, y compris l'adresse du fournisseur de virtualisation de réseau Hyper-V (HNV PA), l'adresse IP virtuelle publique, l'adresse IP virtuelle privée, l'encapsulation de routage générique (GRE) et L3 ne doivent pas chevaucher les deux sites.

Activer SDN Multisite

Voici un flux de travail de haut niveau pour activer SDN Multisite :

- Remplissez les conditions préalables. Consultez les conditions préalables.
- Établissez un peering. Consultez Établir un peering.
- Vérifiez l'état du peering. Consultez Vérifier l'état du peering.

Établir un peering

Procédez comme suit pour établir un peering sur plusieurs sites à l'aide de Windows Admin Center :

1. Dans Windows Admin Center, connectez-vous à votre cluster dans le site principal pour commencer le peering entre les sites. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Contrôleurs réseau**.

2. Dans la page **Contrôleurs de réseau** , sélectionnez **Nouveau** pour ajouter un site secondaire.

3. Dans le volet **Connecter des clusters** , fournissez les informations de connexion nécessaires :

   a. Entrez le **nom** du site secondaire. Par exemple, **site secondaire**.

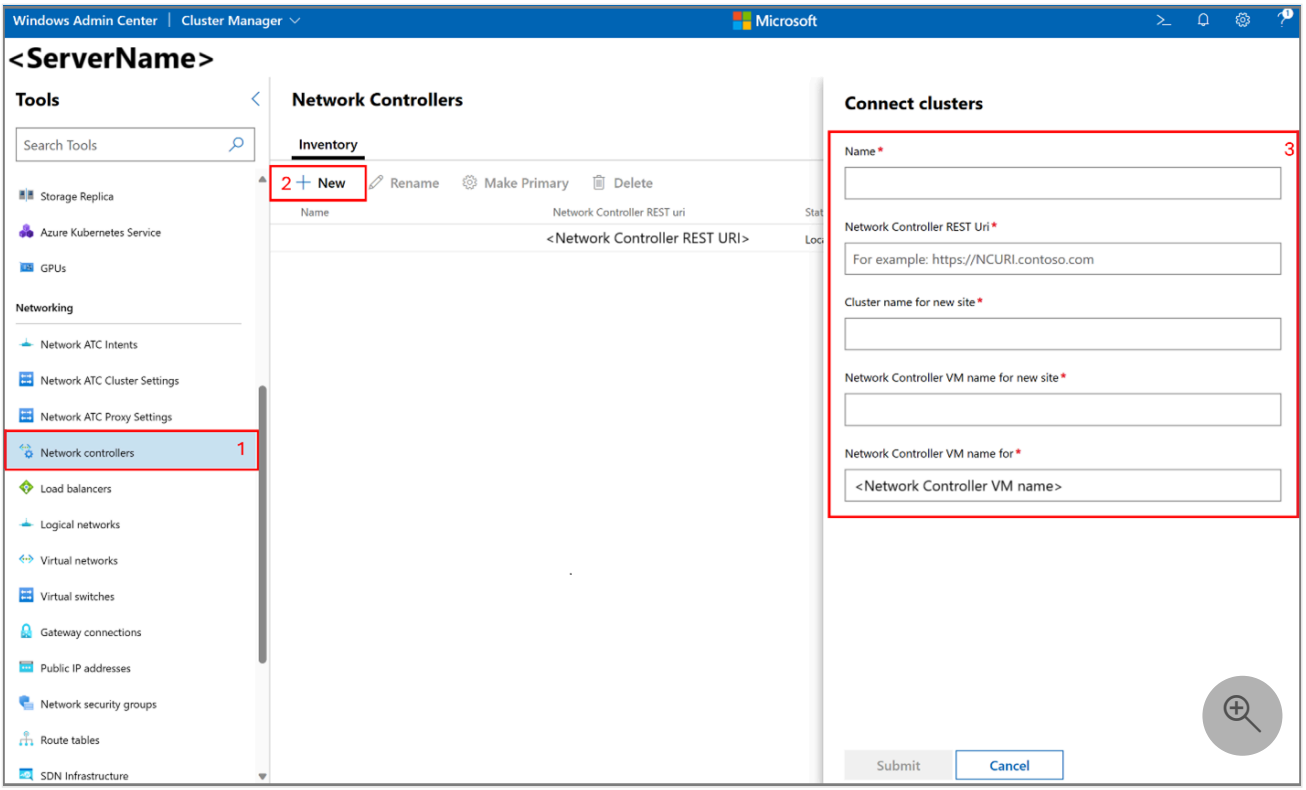
   b. Entrez l'URI REST du contrôleur de réseau du site secondaire.

   c. Entrez le **nom du cluster pour le nouveau site** ou le site secondaire.

   d. Entrez le nom de la **machine virtuelle du contrôleur de réseau pour le nouveau site** ou le site secondaire. Le nom peut être n'importe quel nom de machine virtuelle du contrôleur de réseau du site secondaire.

   e. Entrez le nom de la **machine virtuelle du contrôleur de réseau pour** votre emplacement principal. Le nom peut être n'importe quel nom de machine virtuelle du contrôleur de réseau de votre emplacement principal.

4. Sélectionnez **Envoyer**.



Une fois le peering lancé, les ressources telles que les réseaux virtuels ou les configurations de stratégie qui étaient une fois locales sur le site principal deviennent des ressources globales synchronisées entre les sites.

Vérifier l'état du peering

Après avoir activé SDN Multisite, passez en revue la configuration actuelle pour déterminer quel site est désigné comme principal et celui qui est le serveur secondaire.

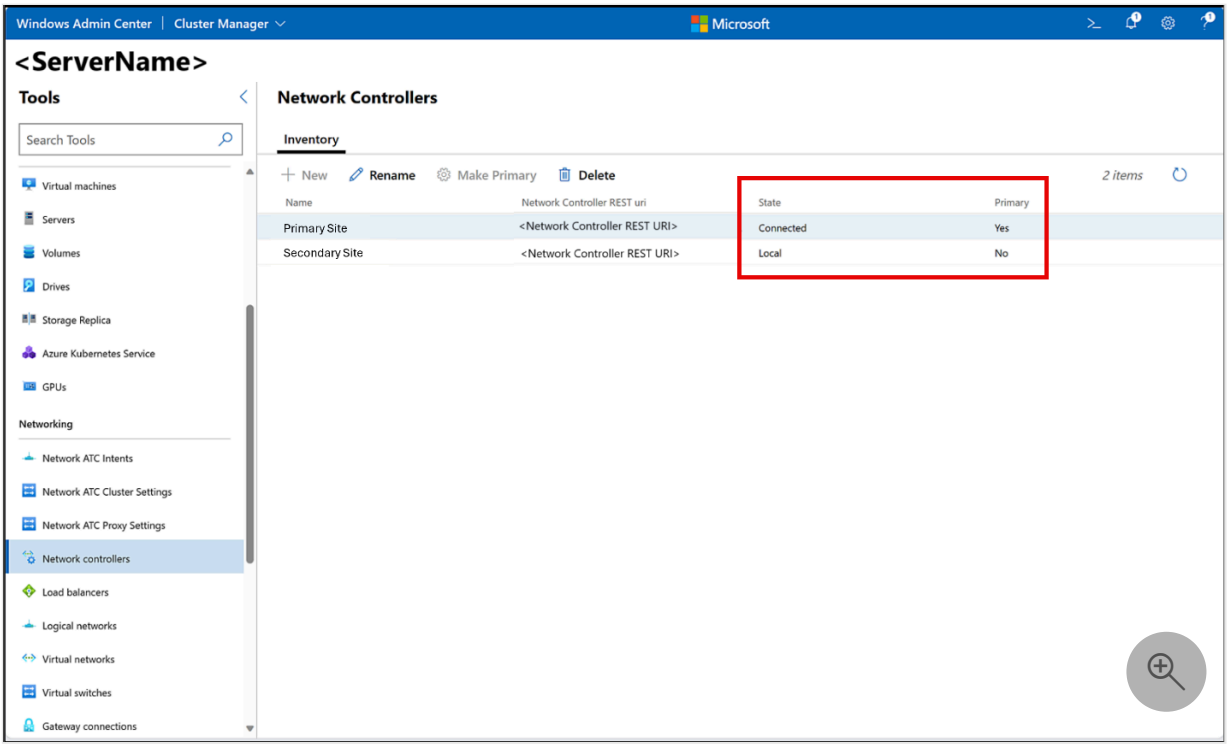
Suivez ces étapes pour passer en revue l'état du peering multisite SDN :

1. Dans Windows Admin Center, connectez-vous à votre cluster sur n'importe quel site. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Contrôleurs réseau**.

2. Dans la page **Contrôleurs réseau** , sous l'onglet **Inventaire** , passez en revue l'état des deux colonnes suivantes :

   - **État** : cette colonne peut avoir l'une des valeurs suivantes :
     - `Local` indique le site via lequel vous accédez à SDN Multisite.
     - `Initiated`, `Connected` ou `Failed` indique l'état du peering.

   - **Principal** : cette colonne peut avoir l'une des valeurs suivantes :
     - `Yes` indique que le site est un site principal.
     - `No` indique que le site est un site secondaire.



Gérer SDN Multisite

Cette section décrit les tâches que vous pouvez effectuer pour gérer votre solution multisite SDN à l'aide de Windows Admin Center.

Modifier le site principal

Vous ne pouvez avoir qu'un seul site principal à la fois. Si votre scénario nécessite plusieurs sites principaux, contactez sdn_feedback@microsoft.com.

Dans certains scénarios, vous devrez peut-être modifier votre site principal. Par exemple, si votre site principal tombe en panne et devient inaccessible, mais qu'il existe des stratégies globales et des ressources à modifier et à synchroniser. Dans ce cas, vous pouvez modifier le site principal pour empêcher la perte de données et garantir la continuité des informations. Toutefois, s'il existe des modifications en attente dans votre ancien site principal, il existe un risque potentiel de perte de données lors de la transition vers les nouveaux sites principaux.

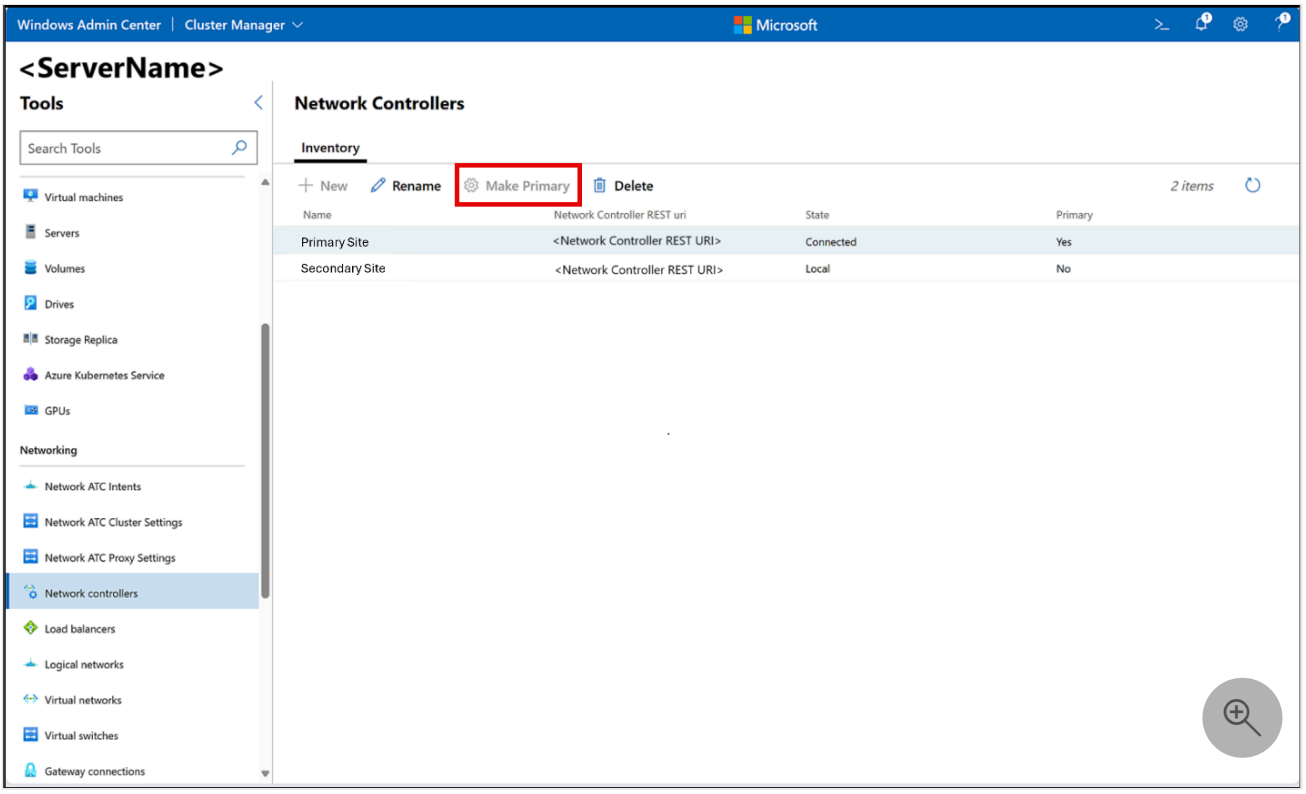
Procédez comme suit pour modifier le site principal :

1. Vérifiez que SDN Multisite est activé. Consultez Vérifier l'état du peering.

2. Connectez-vous à votre cluster sur n'importe quel site. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Contrôleurs réseau**.

3. Dans la page **Contrôleurs de réseau** , sous l'onglet **Inventaire** , sélectionnez la ligne du site secondaire que vous souhaitez convertir en serveur principal.

4. Sélectionnez **Rendre principal** pour modifier le site secondaire en site principal.



Renommer des sites

Il peut arriver que vous deviez renommer vos sites pour améliorer la pertinence ou respecter la convention d'affectation de noms suivie dans votre organisation.

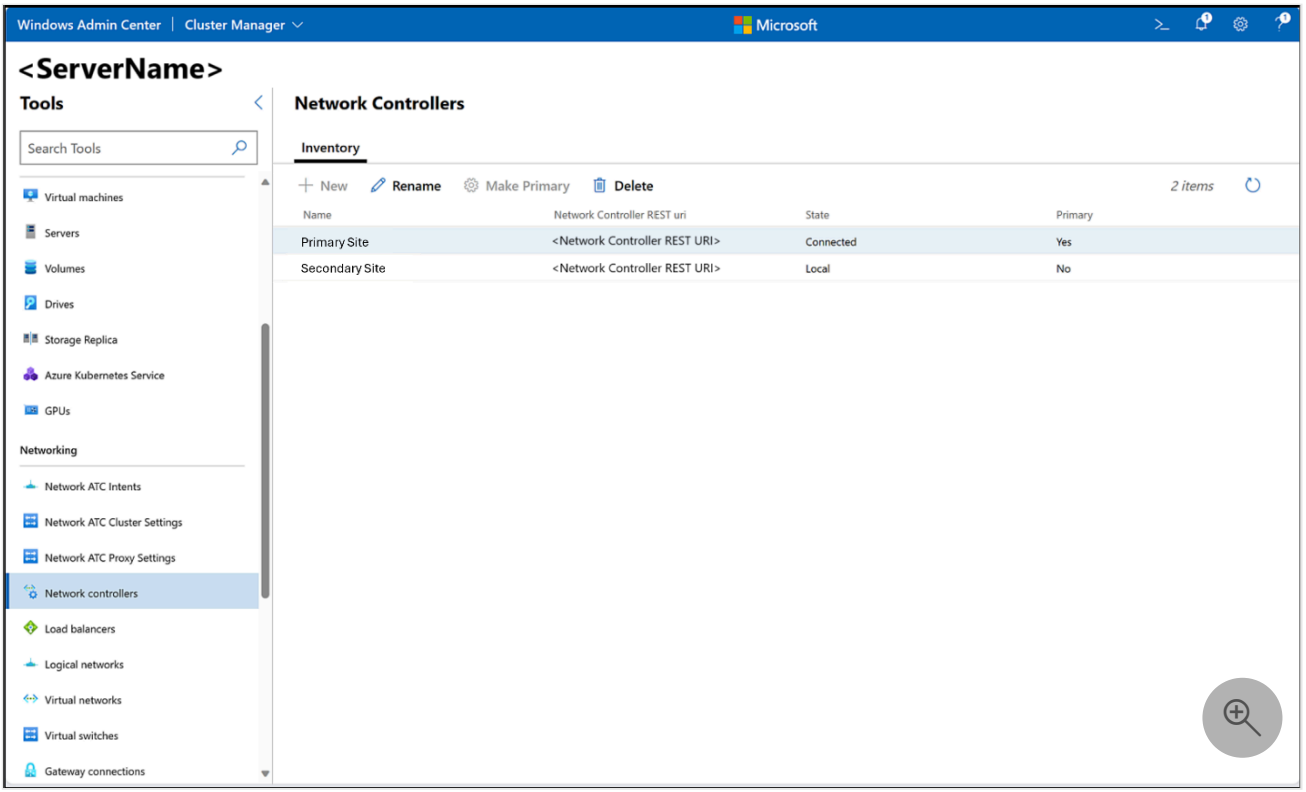
Pour renommer des sites, procédez comme suit :

1. Vérifiez que SDN Multisite est activé. Consultez Vérifier l'état du peering.

2. Connectez-vous à votre cluster sur n'importe quel site. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Contrôleurs réseau**.

3. Dans la page **Contrôleurs de réseau** , sous l'onglet **Inventaire** , sélectionnez le site à renommer.

4. Sélectionnez **Renommer** pour modifier le nom du site.



Supprimer SDN Multisite

Dans certains cas, vous devrez peut-être supprimer le peering pour arrêter la synchronisation des ressources entre les sites. Par exemple, pour isoler les ressources en raison d'une préoccupation de sécurité ou d'un changement dans la stratégie d'infrastructure de votre organisation.

Lorsque vous supprimez le peering, la synchronisation des ressources est abandonnée et chaque site conserve sa propre copie des ressources. Par exemple, vous disposez d'un réseau virtuel avec deux machines virtuelles, une sur chaque site. Lorsque le peering est supprimé, chaque site a toujours la même ressource de réseau virtuel et la machine virtuelle de site local fonctionne toujours avec les mêmes paramètres réseau. Mais elle ne peut pas communiquer avec la machine virtuelle sur le site distant.

Pour supprimer le peering, procédez comme suit :

1. Dans Windows Admin Center, connectez-vous à votre cluster sur n'importe quel site. Sous **Outils**, faites défiler jusqu'à la section **Mise en réseau** , puis sélectionnez **Contrôleurs réseau**.

2. Dans la page **Contrôleurs réseau** , sélectionnez **Supprimer**.

3. Dans la fenêtre de confirmation, sélectionnez **Oui**.

   Après avoir supprimé le peering, il faut un moment pour que vos sites se mettent à jour. S'il n'est pas mis à jour, actualisez votre navigateur.

Rétablir le peering après la suppression de SDN Multisite

Si vous envisagez de rétablir votre connexion multisite après sa suppression, votre site secondaire doit être configuré en tant que nouvel environnement SDN. Cela signifie qu'il ne peut pas y avoir de réseaux virtuels ou de groupes de sécurité réseau préexistants. Toutefois, votre emplacement secondaire a un cache local des ressources globales une fois à partir de SDN Multisite. Même lorsque vous supprimez SDN Multisite, votre emplacement secondaire a toujours une copie de ces ressources. Sans SDN Multisite, ces ressources ne sont plus synchronisées.

Pour le redéploiement après la suppression de SDN Multisite, vérifiez que les éléments suivants sont supprimés :

- Réseaux virtuels. Voir Supprimer un réseau virtuel
- Groupes de sécurité réseau. Voir Supprimer un groupe de sécurité réseau

Étapes suivantes

- Lisez le blog sur SDN Multisite
- Mise en réseau définie par logiciel (SDN) dans Azure Local et Windows Server

---

Dernière mise à jour : 15/09/2026

Mettez à niveau, sauvegardez et restaurez l'infrastructure SDN

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans cette rubrique, vous allez apprendre à mettre à niveau, sauvegarder et restaurer une infrastructure SDN.

Mettez à niveau l'infrastructure SDN

L'infrastructure SDN peut être mise à jour de Windows Server 2016 vers Windows Server 2019. Pour l'ordre de mise à jour, suivez la même séquence d'étapes que celle mentionnée dans la section « Mettre à niveau l'infrastructure SDN ». Avant la mise à jour, il est recommandé d'effectuer une sauvegarde de la base de données du contrôleur de réseau.

Pour les machines de Contrôleur de réseau, utilisez l'applet de commande Get-NetworkControllerNode pour vérifier l'état du nœud une fois la mise à jour terminée. Assurez-vous que le nœud revient à l'état « Up » avant de mettre à niveau les autres nœuds. Une fois que vous avez mis à niveau tous les nœuds du Contrôleur de réseau, le Contrôleur de réseau met à niveau les micro-services en cours d'exécution dans le cluster du Contrôleur de réseau en l'espace d'une heure. Vous pouvez déclencher une mise à jour immédiate à l'aide de l'applet de commande update-networkcontroller.

Installez les mêmes mises à niveau Windows sur tous les composants du système d'exploitation du système SDN (Software Defined Networking), notamment :

- Hôtes Hyper-V activés par SDN
- Machines virtuelles du Contrôleur de réseau
- Machines virtuelles de l'équilibreur de charge logiciel Mux
- Machines virtuelles de la passerelle RAS

> **ⓘ Important**
>
> Si vous utilisez System Center Virtual Manager, vous devez le mettre à niveau avec les derniers correctifs cumulatifs.

Quand vous mettez à niveau chaque composant, vous pouvez utiliser n'importe laquelle des méthodes standard pour installer les mises à jour de Windows. Toutefois, pour garantir un

temps d'arrêt minimal pour les charges de travail et l'intégrité de la base de données du contrôleur de réseau, procédez comme suit :

1. Mettez à jour les consoles de gestion.

   Installez les mises à jour sur chacun des ordinateurs sur lesquels vous utilisez le module PowerShell du contrôleur de réseau. Y compris partout où vous avez installé le rôle RSAT-NetworkController installé par lui-même. À l'exception des machines virtuelles du contrôleur de réseau elles-mêmes ; vous les mettez à jour à l'étape suivante.

2. Sur la première machine virtuelle du contrôleur de réseau, installez toutes les mises à jour et redémarrez.

3. Avant de passer à la machine virtuelle du contrôleur de réseau suivante, utilisez l'applet de commande `get-networkcontrollernode` pour vérifier l'état du nœud que vous avez mis à jour et redémarré.

4. Pendant le cycle de redémarrage, attendez que le nœud du contrôleur de réseau s'éteigne, puis se rallume.

   Après le redémarrage de la machine virtuelle, il peut prendre plusieurs minutes avant de revenir à l'état ***Up*** . Pour obtenir un exemple de sortie, consultez

5. Installez les mises à jour sur chaque machine virtuelle SLB Mux, une à la fois, pour garantir la disponibilité continue de l'infrastructure de l'équilibreur de charge.

6. Mettez à jour Hyper-V des hôtes et des passerelles RAS, en commençant par les hôtes qui contiennent les passerelles RAS en mode **veille** .

   Les machines virtuelles de passerelle RAS ne peuvent pas être migrées en direct sans perdre les connexions de locataire. Pendant le cycle de mise à jour, vous devez veiller à minimiser le nombre de fois où les connexions des locataires basculent vers une nouvelle passerelle RAS. En coordonnant la mise à jour des hôtes et des passerelles RAS, chaque locataire bascule une fois, au maximum.

   a. Évacuez l'hôte de machines virtuelles capables de migrer en direct.

   Les machines virtuelles de la passerelle RAS doivent rester sur l'hôte.

   b. Installez les mises à jour sur chaque machine virtuelle de la passerelle sur cet hôte.

   c. Si la mise à jour nécessite le redémarrage de la machine virtuelle de passerelle, redémarrez la machine virtuelle.

   d. Installez les mises à jour sur l'hôte contenant la machine virtuelle de la passerelle qui vient d'être mise à jour.

e. Redémarrez l'hôte si nécessaire par les mises à jour.

f. Répétez cette opération pour chaque hôte supplémentaire contenant une passerelle de secours.

Si aucune passerelle de secours n'est en attente, suivez ces mêmes étapes pour tous les hôtes restants.

Exemple : utilisez l'applet de commande get-networkcontrollernode

Dans cet exemple, vous voyez la sortie de l'applet de commande `get-networkcontrollernode` exécutée à partir de l'une des machines virtuelles du contrôleur de réseau.

L'état des nœuds que vous voyez dans l'exemple de sortie est le suivant :

- NCNode1.contoso.com = Down
- NCNode2.contoso.com = Up
- NCNode3.contoso.com = Up

> **Important**
>
> Vous devez attendre plusieurs minutes jusqu'à ce que l'état du nœud passe à ***Haut*** avant de mettre à jour les nœuds supplémentaires, un à la fois.

Une fois que vous avez mis à jour tous les nœuds du contrôleur de réseau, le contrôleur de réseau met à jour les micro-services en cours d'exécution dans le cluster du contrôleur de réseau dans l'heure.

> **Conseil**
>
> Vous pouvez déclencher une mise à jour immédiate à l'aide de l'applet de commande `update-networkcontroller`.

PowerShell

```
PS C:\> get-networkcontrollernode
Name            : NCNode1.contoso.com
Server          : NCNode1.Contoso.com
FaultDomain     : fd:/NCNode1.Contoso.com
RestInterface   : Ethernet
NodeCertificate :
Status          : Down
```

```
Name            : NCNode2.Contoso.com
Server          : NCNode2.contoso.com
FaultDomain     : fd:/ NCNode2.Contoso.com
RestInterface   : Ethernet
NodeCertificate :
Status          : Up

Name            : NCNode3.Contoso.com
Server          : NCNode3.Contoso.com
FaultDomain     : fd:/ NCNode3.Contoso.com
RestInterface   : Ethernet
NodeCertificate :
Status          : Up
```

Exemple : utilisez l'applet de commande update-networkcontroller

Dans cet exemple, vous voyez la sortie de l'applet de commande `update-networkcontroller` pour forcer la mise à jour du Contrôleur de réseau.

> **Important**
>
> Exécutez cette applet de commande lorsque vous n'avez plus de mises à jour à installer.

PowerShell

```
PS C:\> update-networkcontroller
NetworkControllerClusterVersion NetworkControllerVersion
------------------------------- ------------------------
10.1.1                          10.1.15
```

Sauvegardez l'infrastructure SDN

Les sauvegardes régulières de la base de données du contrôleur de réseau garantissent la continuité de l'activité en cas de sinistre ou de perte de données. La sauvegarde des machines virtuelles du contrôleur de réseau n'est pas suffisante, car elle ne garantit pas que la session continue sur les plusieurs nœuds du contrôleur de réseau.

Requirements:

- Un partage SMB et des informations d'identification avec des autorisations de lecture/écriture sur le système de partage et de fichiers.

- Vous pouvez éventuellement utiliser un compte de service administré de groupe (GMSA) si le contrôleur de réseau a également été installé à l'aide d'un GMSA.

Procedure:

1. Utilisez la méthode de sauvegarde de machine virtuelle de votre choix ou utilisez Hyper-V pour exporter une copie de chaque machine virtuelle du contrôleur de réseau.

   La sauvegarde de la machine virtuelle du contrôleur de réseau garantit que les certificats nécessaires au déchiffrement de la base de données sont présents.

2. Si vous utilisez System Center Virtual Machine Manager (SCVMM), arrêtez SCVMM et sauvegardez-le via SQL Server.

   L'objectif ici est de s'assurer qu'aucune mise à jour n'est apportée à SCVMM pendant cette période, ce qui peut créer une incohérence entre la sauvegarde du contrôleur de réseau et SCVMM.

   > ⓘ **Important**
   >
   > Ne redémarrez pas le service SCVMM tant que la sauvegarde du contrôleur de réseau n'est pas terminée.

3. Sauvegardez la base de données du contrôleur de réseau avec l'applet de commande `new-networkcontrollerbackup`.

4. Vérifiez l'achèvement et le succès de la sauvegarde avec l'applet de commande `get-networkcontrollerbackup`.

5. Si vous utilisez SCVMM, démarrez le service SCVMM.

Exemple : sauvegarde de la base de données du contrôleur de réseau

PowerShell

```
$URI = "https://NC.contoso.com"
$Credential = Get-Credential

# Get or Create Credential object for File share user

$ShareUserResourceId = "BackupUser"

$ShareCredential = Get-NetworkControllerCredential -ConnectionURI $URI -Credential
$Credential | Where {$_.ResourceId -eq $ShareUserResourceId }
```

```
If ($ShareCredential -eq $null) {
    $CredentialProperties = New-Object
Microsoft.Windows.NetworkController.CredentialProperties
    $CredentialProperties.Type = "usernamePassword"
    $CredentialProperties.UserName = "contoso\user01"
    $CredentialProperties.Value = "<Password>"

    $ShareCredential = New-NetworkControllerCredential -ConnectionURI $URI -
Credential $Credential -Properties $CredentialProperties -ResourceId
$ShareUserResourceId -Force
}

# Create backup

$BackupTime = (get-date).ToString("s").Replace(":", "_")

$BackupProperties = New-Object
Microsoft.Windows.NetworkController.NetworkControllerBackupProperties
$BackupProperties.BackupPath = "\\fileshare\backups\NetworkController\$BackupTime"
$BackupProperties.Credential = $ShareCredential

$Backup = New-NetworkControllerBackup -ConnectionURI $URI -Credential $Credential
-Properties $BackupProperties -ResourceId $BackupTime -Force
```

Exemple : vérification de l'état d'une opération de sauvegarde du contrôleur de réseau

PowerShell

```
PS C:\ > Get-NetworkControllerBackup -ConnectionUri $URI -Credential $Credential -
ResourceId $Backup.ResourceId
| ConvertTo-JSON -Depth 10
{
    "Tags":  null,
    "ResourceRef":  "/networkControllerBackup/2017-04-25T16_53_13",
    "InstanceId":  "c3ea75ae-2892-4e10-b26c-a2243b755dc8",
    "Etag":  "W/\"0dafea6c-39db-401b-bda5-d2885ded470e\"",
    "ResourceMetadata":  null,
    "ResourceId":  "2017-04-25T16_53_13",
    "Properties":  {
                     "BackupPath":  "\\\\fileshare\backups\NetworkController\\2017-
04-25T16_53_13",
                     "ErrorMessage":  "",
                     "FailedResourcesList":  [

                                             ],
                     "SuccessfulResourcesList":  [

"/networking/v1/credentials/11ebfc10-438c-4a96-a1ee-8a048ce675be",

"/networking/v1/credentials/41229069-85d4-4352-be85-034d0c5f4658",
```

"/networking/v1/credentials/b2a82c93-2583-4a1f-91f8-232b801e11bb",

"/networking/v1/credentials/BackupUser",

"/networking/v1/credentials/fd5b1b96-b302-4395-b6cd-ed9703435dd1",

"/networking/v1/virtualNetworkManager/configuration",

"/networking/v1/virtualSwitchManager/configuration",

"/networking/v1/accessControlLists/f8b97a4c-4419-481d-b757-a58483512640",

"/networking/v1/logicalnetworks/24fa1af9-88d6-4cdc-aba0-66e38c1a7bb8",

"/networking/v1/logicalnetworks/48610528-f40b-4718-938e-99c2be76f1e0",

"/networking/v1/logicalnetworks/89035b49-1ee3-438a-8d7a-f93cbae40619",

"/networking/v1/logicalnetworks/a9c8eaa0-519c-4988-acd6-11723e9efae5",

"/networking/v1/logicalnetworks/d4ea002c-c926-4c57-a178-461d5768c31f",

"/networking/v1/macPools/11111111-1111-1111-1111-111111111111",

"/networking/v1/loadBalancerManager/config",

"/networking/v1/publicIPAddresses/2c502b2d-b39a-4be1-a85a-55ef6a3a9a1d",

"/networking/v1/GatewayPools/Default",

"/networking/v1/servers/4c4c4544-0058-5810-8056-b4c04f395931",

"/networking/v1/servers/4c4c4544-0058-5810-8057-b4c04f395931",

"/networking/v1/servers/4c4c4544-0058-5910-8056-b4c04f395931",

"/networking/v1/networkInterfaces/058430d3-af43-4328-a440-56540f41da50",

"/networking/v1/networkInterfaces/08756090-6d55-4dec-98d5-80c4c5a47db8",

"/networking/v1/networkInterfaces/2175d74a-aacd-44e2-80d3-03f39ea3bc5d",

"/networking/v1/networkInterfaces/2400c2c3-2291-4b0b-929c-9bb8da55851a",

"/networking/v1/networkInterfaces/4c695570-6faa-4e4d-a552-0b36ed3e0962",

"/networking/v1/networkInterfaces/7e317638-2914-42a8-a2dd-3a6d966028d6",

"/networking/v1/networkInterfaces/834e3937-f43b-4d3c-88be-d79b04e63bce",

"/networking/v1/networkInterfaces/9d668fe6-b1c6-48fc-b8b1-b3f98f47d508",

"/networking/v1/networkInterfaces/ac4650ac-c3ef-4366-96e7-d9488fb661ba",

```
"/networking/v1/networkInterfaces/b9f23e35-d79e-495f-a1c9-fa626b85ae13",

"/networking/v1/networkInterfaces/fdd929f1-f64f-4463-949a-77b67fe6d048",

"/networking/v1/virtualServers/15a891ee-7509-4e1d-878d-de0cb4fa35fd",

"/networking/v1/virtualServers/57416993-b410-44fd-9675-727cd4e98930",

"/networking/v1/virtualServers/5f8aebdc-ee5b-488f-ac44-dd6b57bd316a",

"/networking/v1/virtualServers/6c812217-5931-43dc-92a8-1da3238da893",

"/networking/v1/virtualServers/d78b7fa3-812d-4011-9997-aeb5ded2b431",

"/networking/v1/virtualServers/d90820a5-635b-4016-9d6f-bf3f1e18971d",

"/networking/v1/loadBalancerMuxes/5f8aebdc-ee5b-488f-ac44-dd6b57bd316a_suffix",

"/networking/v1/loadBalancerMuxes/d78b7fa3-812d-4011-9997-aeb5ded2b431_suffix",

"/networking/v1/loadBalancerMuxes/d90820a5-635b-4016-9d6f-bf3f1e18971d_suffix",

"/networking/v1/Gateways/15a891ee-7509-4e1d-878d-de0cb4fa35fd_suffix",

"/networking/v1/Gateways/57416993-b410-44fd-9675-727cd4e98930_suffix",

"/networking/v1/Gateways/6c812217-5931-43dc-92a8-1da3238da893_suffix",

"/networking/v1/virtualNetworks/b3dbafb9-2655-433d-b47d-a0e0bbac867a",

"/networking/v1/virtualNetworks/d705968e-2dc2-48f2-a263-76c7892fb143",

"/networking/v1/loadBalancers/24fa1af9-88d6-4cdc-aba0-66e38c1a7bb8_10.127.132.2",

"/networking/v1/loadBalancers/24fa1af9-88d6-4cdc-aba0-66e38c1a7bb8_10.127.132.3",

"/networking/v1/loadBalancers/24fa1af9-88d6-4cdc-aba0-66e38c1a7bb8_10.127.132.4"
                                                    ],
                    "InProgressResourcesList":  [

                                                    ],
                    "ProvisioningState":  "Succeeded",
                    "Credential":  {
                                        "Tags":  null,
                                        "ResourceRef":  "/credentials/BackupUser",
                                        "InstanceId":  "00000000-0000-0000-0000-
000000000000",
                                        "Etag":  null,
                                        "ResourceMetadata":  null,
                                        "ResourceId":  null,
                                        "Properties":  null
                                    }
                }
}
```

Restaurez l'infrastructure SDN à partir d'une sauvegarde

Lorsque vous restaurez tous les composants nécessaires à partir d'une sauvegarde, l'environnement SDN redevient opérationnel.

> **ⓘ Important**
>
> Les étapes varient en fonction du nombre de composants restaurés.

1. Si nécessaire, redéployez les hôtes Hyper-V et le stockage nécessaire.
2. Si nécessaire, restaurez les machines virtuelles du contrôleur de réseau, les machines virtuelles de passerelle RAS et les machines virtuelles Mux à partir de la sauvegarde.
3. Arrêtez l'agent hôte NC et l'agent hôte SLB sur tous les hôtes Hyper-V :

   ```
   stop-service slbhostagent

   stop-service nchostagent
   ```

4. Arrêtez les machines virtuelles de la passerelle RAS.
5. Arrêtez les machines virtuelles SLB Mux.
6. Restaurez le contrôleur de réseau avec l'applet de commande `new-networkcontrollerrestore`.
7. Vérifiez la restauration **ProvisioningState** pour savoir quand la restauration s'est terminée correctement.
8. Si vous utilisez SCVMM, restaurez la base de données SCVMM à l'aide de la sauvegarde créée en même temps que la sauvegarde du contrôleur de réseau.
9. Si vous souhaitez restaurer des machines virtuelles de charge de travail à partir d'une sauvegarde, faites-le maintenant.
10. Vérifiez l'intégrité de votre système avec l'applet de commande debug-networkcontrollerconfigurationstate.

PowerShell

```
$cred = Get-Credential
Debug-NetworkControllerConfigurationState -NetworkController
"https://NC.contoso.com" -Credential $cred

Fetching ResourceType:     accessControlLists
Fetching ResourceType:     servers
Fetching ResourceType:     virtualNetworks
Fetching ResourceType:     networkInterfaces
Fetching ResourceType:     virtualGateways
Fetching ResourceType:     loadbalancerMuxes
Fetching ResourceType:     Gateways
```

Exemple : restauration d'une base de données du contrôleur de réseau

PowerShell

```
$URI = "https://NC.contoso.com"
$Credential = Get-Credential

$ShareUserResourceId = "BackupUser"
$ShareCredential = Get-NetworkControllerCredential -ConnectionURI $URI -Credential
$Credential | Where {$_.ResourceId -eq $ShareUserResourceId }

$RestoreProperties = New-Object
Microsoft.Windows.NetworkController.NetworkControllerRestoreProperties
$RestoreProperties.RestorePath = "\\fileshare\backups\NetworkController\2017-04-
25T16_53_13"
$RestoreProperties.Credential = $ShareCredential

$RestoreTime = (Get-Date).ToString("s").Replace(":", "_")
New-NetworkControllerRestore -ConnectionURI $URI -Credential $Credential -
Properties $RestoreProperties -ResourceId $RestoreTime -Force
```

Exemple : Vérification de l'état d'une restauration d'une base de données du contrôleur de réseau

PowerShell

```
PS C:\ > get-networkcontrollerrestore -connectionuri $uri -credential $cred -
ResourceId $restoreTime | convertto-json -depth 10
{
    "Tags":  null,
    "ResourceRef":  "/networkControllerRestore/2017-04-26T15_04_44",
    "InstanceId":  "22edecc8-a613-48ce-a74f-0418789f04f6",
    "Etag":  "W/\"f14f6b84-80a7-4b73-93b5-59a9c4b5d98e\"",
    "ResourceMetadata":  null,
```

```
    "ResourceId":  "2017-04-26T15_04_44",
    "Properties":  {
                     "RestorePath":  "\\\\sa18fs\\sa18n22\\NetworkController\\2017-
04-25T16_53_13",
                     "ErrorMessage":  null,
                     "FailedResourcesList":  null,
                     "SuccessfulResourcesList":  null,
                     "ProvisioningState":  "Succeeded",
                     "Credential":  null
                 }
}
```


Pour plus d'informations sur les messages d'état de configuration qui peuvent apparaître, consultez Résoudre les problèmes de la pile de mise en réseau SDN (Software Defined Networking) dans Windows Server 2016.

Sécuriser le contrôleur de réseau

> S'applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Cet article explique comment configurer la sécurité pour toutes les communications entre le contrôleur de réseau et d'autres logiciels et appareils.

Les chemins de communication que vous pouvez sécuriser incluent la communication Nord sur le plan de gestion, la communication entre les machines virtuelles du contrôleur de réseau dans un cluster, et la communication Sud sur le plan de données.

1. **Communication orientée vers le nord**. Le contrôleur de réseau communique sur le plan d'administration avec un logiciel de gestion compatible SDN comme Windows PowerShell et System Center Virtual Machine Manager (SCVMM). Ces outils de gestion vous permettent de définir la stratégie réseau et de créer un état d'objectif pour le réseau, par rapport auquel vous pouvez comparer la configuration réseau réelle pour mettre la configuration en parité avec l'état d'objectif.

2. **Communication du cluster du contrôleur de réseau**. Lorsque vous configurez trois machines virtuelles ou plus en tant que nœuds de cluster de contrôleur de réseau, ces nœuds communiquent entre eux. Cette communication peut être liée à la synchronisation et à la réplication des données entre les nœuds ou une communication spécifique entre les services de contrôleur de réseau.

3. **Communication vers les composants de niveau inférieur**. Le contrôleur de réseau communique sur le plan de données avec l'infrastructure SDN et d'autres appareils tels que les équilibreurs de charge logicielles, les passerelles et les machines hôtes. Vous pouvez utiliser le contrôleur de réseau pour configurer et gérer ces dispositifs de niveau inférieur afin qu'ils conservent l'état cible du réseau que vous avez défini.

Communication vers les composants de niveau supérieur

Le contrôleur de réseau prend en charge l'authentification, l'autorisation et le chiffrement pour la communication vers les composants de niveau supérieur. Les sections suivantes fournissent des informations sur la configuration de ces paramètres de sécurité.

Authentification

Lorsque vous configurez l'authentification pour la communication Northbound du contrôleur de réseau, vous autorisez les nœuds de cluster du contrôleur de réseau et les clients de gestion à vérifier l'identité de l'appareil avec lequel ils communiquent.

Le contrôleur de réseau prend en charge les trois modes d'authentification suivants entre les clients de gestion et les nœuds de contrôleur de réseau.

> ⓘ **Remarque**
>
> Si vous déployez un contrôleur de réseau avec System Center Virtual Machine Manager, seul **le mode Kerberos** est pris en charge.

1. **Kerberos**. Utilisez l'authentification Kerberos lors de la liaison du client de gestion et de tous les nœuds de cluster du contrôleur réseau à un domaine Active Directory. Le domaine Active Directory doit avoir des comptes de domaine utilisés pour l'authentification.

2. **X509**. Utilisez X509 pour l'authentification basée sur des certificats pour les clients de gestion non joints à un domaine Active Directory. Vous devez inscrire des certificats à tous les nœuds de cluster de contrôleur de réseau et clients de gestion. En outre, tous les nœuds et clients de gestion doivent approuver les certificats des autres.

3. **Aucun**. Utilisez Aucun à des fins de test dans un environnement de test. Par conséquent ce mode n'est pas recommandé pour une utilisation dans un environnement de production. Lorsque vous choisissez ce mode, aucune authentification n'est effectuée entre les nœuds et les clients de gestion.

Vous pouvez configurer le mode d'authentification pour la communication vers des composants de niveau supérieur à l'aide de la commande Windows PowerShell **Install-NetworkController** avec le paramètre *ClientAuthentication*.

Autorisation

Lorsque vous configurez l'autorisation pour la communication Northbound du contrôleur de réseau, vous autorisez les nœuds de cluster du contrôleur de réseau et les clients de gestion à vérifier que l'appareil avec lequel ils communiquent est approuvé et dispose de l'autorisation de participer à la communication.

Utilisez les méthodes d'autorisation suivantes pour chacun des modes d'authentification pris en charge par le contrôleur de réseau.

1. **Kerberos**. Lorsque vous utilisez la méthode d'authentification Kerberos, vous définissez les utilisateurs et les ordinateurs autorisés à communiquer avec le contrôleur de réseau en créant un groupe de sécurité dans Active Directory, puis en ajoutant les utilisateurs et ordinateurs autorisés au groupe. Vous pouvez configurer le contrôleur de réseau pour utiliser le groupe de sécurité pour l'autorisation à l'aide du paramètre *ClientSecurityGroup* de la commande **Install-NetworkController** Windows PowerShell. Après avoir installé le contrôleur de réseau, vous pouvez modifier le groupe de sécurité à l'aide de la commande **Set-NetworkController** avec le paramètre *-ClientSecurityGroup*. Si vous utilisez SCVMM, vous devez fournir le groupe de sécurité en tant que paramètre pendant le déploiement.

2. **X509**. Lorsque vous utilisez la méthode d'authentification X509, le contrôleur de réseau accepte uniquement les demandes des clients de gestion dont les empreintes de certificat sont connues du contrôleur de réseau. Vous pouvez configurer ces empreintes à l'aide du paramètre *ClientCertificateThumbprint* de la commande **Install-NetworkController** Windows PowerShell. Vous pouvez ajouter d'autres empreintes clientes à tout moment à l'aide de la commande **Set-NetworkController**.

3. **Aucun**. Lorsque vous choisissez ce mode, aucune authentification n'est effectuée entre les nœuds et les clients de gestion. Utilisez Aucun à des fins de test dans un environnement de test. Par conséquent ce mode n'est pas recommandé pour une utilisation dans un environnement de production.

Chiffrement

La communication vers des composants de niveau supérieur utilise SSL (Secure Sockets Layer) pour créer un canal chiffré entre les clients de gestion et les nœuds de contrôleur de réseau. Le chiffrement SSL pour la communication vers des composants de niveau supérieur inclut les exigences suivantes :

- Tous les nœuds du contrôleur de réseau doivent avoir un certificat identique qui inclut les objectifs d'authentification serveur et d'authentification client dans les extensions EKU (utilisation améliorée de la clé).

- L'URI utilisé par les clients de gestion pour communiquer avec le contrôleur de réseau doit être le nom de l'objet du certificat. Le nom de l'objet du certificat doit contenir le nom de domaine complet (FQDN) ou l'adresse IP du point de terminaison REST du contrôleur de réseau.

- Si les nœuds du contrôleur de réseau se trouvent sur différents sous-réseaux, le nom de l'objet de leurs certificats doit être identique à la valeur utilisée pour le paramètre *RestName* dans la commande **Install-NetworkController** Windows PowerShell.
- Tous les clients de gestion doivent approuver le certificat SSL.

Inscription et configuration du certificat SSL

Vous devez inscrire manuellement le certificat SSL sur les nœuds du contrôleur de réseau.

Une fois le certificat inscrit, vous pouvez configurer le contrôleur de réseau pour utiliser le certificat avec le paramètre **-ServerCertificate** de la commande **Install-NetworkController** Windows PowerShell. Si vous avez déjà installé le contrôleur de réseau, vous pouvez mettre à jour la configuration à tout moment à l'aide de la commande **Set-NetworkController**.

> ⓘ **Remarque**
>
> Si vous utilisez SCVMM, vous devez ajouter le certificat en tant que ressource de bibliothèque. Pour plus d'informations, consultez **Configurer un contrôleur de réseau SDN dans l'infrastructure VMM**.

Communication du cluster du contrôleur de réseau

Le contrôleur de réseau prend en charge l'authentification, l'autorisation et le chiffrement pour la communication entre les nœuds du contrôleur de réseau. La communication est sur Windows Communication Foundation (WCF) et TCP.

Vous pouvez configurer ce mode avec le paramètre **ClusterAuthentication** de la commande **Install-NetworkControllerCluster** Windows PowerShell.

Pour plus d'informations, consultez Install-NetworkControllerCluster.

Authentification

Lorsque vous configurez l'authentification pour la communication du cluster du contrôleur de réseau, vous autorisez les nœuds de cluster du contrôleur de réseau à vérifier l'identité des autres nœuds avec lesquels ils communiquent.

Le contrôleur de réseau prend en charge les trois modes d'authentification suivants entre les nœuds du contrôleur de réseau.

> **Remarque**
>
> Si vous déployez le contrôleur de réseau à l'aide de SCVMM, seul le mode **Kerberos** est pris en charge.

1. **Kerberos**. Vous pouvez utiliser l'authentification Kerberos lorsque tous les nœuds de cluster de contrôleur de réseau sont joints à un domaine Active Directory, avec des comptes de domaine utilisés pour l'authentification.

2. **X509**. X509 est une authentification basée sur des certificats. Vous pouvez utiliser l'authentification X509 lorsque les nœuds de cluster du contrôleur de réseau ne sont pas liés à un domaine Active Directory. Pour utiliser X509, vous devez inscrire des certificats à tous les nœuds de cluster du contrôleur de réseau, et tous les nœuds doivent approuver les certificats. En outre, le nom de l'objet du certificat inscrit sur chaque nœud doit être identique au nom DNS du nœud.

3. **Aucun**. Lorsque vous choisissez ce mode, aucune authentification n'est effectuée entre les nœuds du contrôleur de réseau. Ce mode est fourni uniquement à des fins de test et n'est pas recommandé pour une utilisation dans un environnement de production.

Autorisation

Lorsque vous configurez l'autorisation pour la communication du cluster de contrôleur de réseau, vous autorisez les nœuds de cluster du contrôleur de réseau à vérifier que les nœuds avec lesquels ils communiquent sont approuvés et ont l'autorisation de participer à la communication.

Pour chacun des modes d'authentification pris en charge par le contrôleur de réseau, les méthodes d'autorisation suivantes sont utilisées.

1. **Kerberos**. Les nœuds du contrôleur de réseau acceptent uniquement les demandes de communication à partir d'autres comptes de machine de contrôleur de réseau. Vous pouvez configurer ces comptes lorsque vous déployez le contrôleur de réseau à l'aide du paramètre **Name** de la commande New-NetworkControllerNodeObject Windows PowerShell.

2. **X509**. Les nœuds du contrôleur de réseau acceptent uniquement les demandes de communication à partir d'autres comptes de machine de contrôleur de réseau. Vous pouvez configurer ces comptes lorsque vous déployez le contrôleur de réseau à l'aide du paramètre **Name** de la commande New-NetworkControllerNodeObject Windows PowerShell.

3. **Aucun**. Lorsque vous choisissez ce mode, aucune autorisation n'est effectuée entre les nœuds du contrôleur de réseau. Ce mode est fourni uniquement à des fins de test et n'est pas recommandé pour une utilisation dans un environnement de production.

Chiffrement

La communication entre les nœuds du contrôleur de réseau est chiffrée à l'aide du chiffrement au niveau du transport WCF. Cette forme de chiffrement est utilisée lorsque les méthodes d'authentification et d'autorisation sont des certificats Kerberos ou X509. Pour plus d'informations, consultez les rubriques ci-dessous.

- Procédure : sécuriser un service avec des informations d'identification Windows
- Procédure : sécuriser un service avec un certificat X.509.

Communication vers le sud

Le contrôleur de réseau interagit avec différents types d'appareils pour la communication vers le Sud. Ces interactions utilisent différents protocoles. En raison de cela, il existe différentes exigences pour l'authentification, l'autorisation et le chiffrement en fonction du type d'appareil et de protocole utilisé par le contrôleur de réseau pour communiquer avec l'appareil.

Le tableau suivant fournit des informations sur l'interaction du contrôleur de réseau avec différents appareils connectés côté sud.

Agrandir le tableau

Dispositif/service orienté vers le sud	Protocole	Authentification utilisée
Équilibrage de la charge logicielle	WCF (MUX), TCP (hôte)	Certificats
Pare-feu	OVSDB	Certificats
Passerelle	WinRM	Kerberos, Certificats
Réseau virtuel	OVSDB, WCF	Certificats
Itinéraire défini par l'utilisateur	OVSDB	Certificats

Pour chacun de ces protocoles, le mécanisme de communication est décrit dans la section suivante.

Authentification

Pour la communication vers le sud, les protocoles et méthodes d'authentification suivants sont utilisés.

1. **WCF/TCP/OVSDB**. Pour ces protocoles, l'authentification est effectuée à l'aide de certificats X509. Le contrôleur de réseau et le multiplexeur (MUX)/hôte d'équilibrage de charge logiciel (SLB) homologue présentent leurs certificats l'un à l'autre en vue d'une authentification mutuelle. Chaque certificat doit être approuvé par l'homologue distant.

   Pour l'authentification dirigée vers le sud, vous pouvez utiliser le même certificat SSL configuré pour chiffrer la communication avec les clients dirigée vers le nord. Vous devez également configurer un certificat sur les appareils SLB MUX et hôtes. Le nom d'objet du certificat doit être le même que le nom DNS de l'appareil.

2. **WinRM**. Pour ce protocole, l'authentification est réalisée à l'aide de Kerberos (pour les machines reliées à un domaine) et à l'aide de certificats (pour les machines non reliées à un domaine).

Autorisation

Pour la communication descendante, les protocoles et méthodes d'autorisation suivants sont utilisés.

1. **WCF/TCP**. Pour ces protocoles, l'autorisation est basée sur le nom de l'objet de l'entité homologue. Le contrôleur de réseau stocke le nom DNS de l'appareil homologue et l'utilise pour l'autorisation. Ce nom DNS doit correspondre au nom de l'objet de l'appareil dans le certificat. De même, le certificat du contrôleur de réseau doit correspondre au nom DNS du contrôleur de réseau stocké sur l'appareil homologue.

2. **WinRM**. Si Kerberos est utilisé, le compte client WinRM doit être présent dans un groupe prédéfini dans Active Directory ou dans le groupe Administrateurs locaux sur le serveur. Si des certificats sont utilisés, le client présente un certificat au serveur que le serveur autorise à l'aide du nom/émetteur de l'objet, et le serveur utilise un compte d'utilisateur mappé pour effectuer l'authentification.

3. **OVSDB**. L'autorisation est basée sur le nom de l'objet de l'entité homologue. Le contrôleur de réseau stocke le nom DNS de l'appareil homologue et l'utilise pour l'autorisation. Ce nom DNS doit correspondre au nom de l'objet de l'appareil dans le certificat.

Chiffrement

Pour la communication vers les composants de niveau inférieur, les méthodes de chiffrement suivantes sont utilisées pour les protocoles.

1. **WCF/TCP/OVSDB**. Pour ces protocoles, le chiffrement est effectué à l'aide du certificat inscrit sur le client ou le serveur.

2. **WinRM**. Le trafic WinRM est chiffré par défaut à l'aide du fournisseur de support de sécurité Kerberos (SSP). Vous pouvez configurer un chiffrement supplémentaire, sous la forme de SSL, sur le serveur WinRM.

Dernière mise à jour : 15/09/2026

Gérer les certificats pour la mise en réseau définie par logiciel

> S’applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Cet article explique comment gérer des certificats pour les communications Northbound et Southbound du contrôleur de réseau lorsque vous déployez un SDN (Software Defined Networking) et quand vous utilisez System Center Virtual Machine Manager (SCVMM) comme client de gestion SDN.

> **Remarque**
>
> Pour obtenir des informations générales sur le contrôleur de réseau, consultez Contrôleur de réseau.

Si vous n’utilisez pas Kerberos pour sécuriser la communication du contrôleur de réseau, vous pouvez utiliser des certificats X.509 pour l’authentification, l’autorisation et le chiffrement.

SDN dans Windows Server 2019 et 2016 Datacenter prend en charge à la fois les certificats X.509 auto-signés et ceux signés par une autorité de certification (CA). Cette rubrique fournit des instructions pas à pas pour créer ces certificats et les appliquer afin de sécuriser les canaux de communication du contrôleur de réseau avec les clients de gestion (Northbound) et les communications avec les appareils réseau tels que le Load Balancer logiciel (SLB) (Southbound).

Lorsque vous utilisez l’authentification basée sur un certificat, vous devez inscrire un certificat sur des nœuds de contrôleur de réseau utilisés de la manière suivante.

1. Chiffrement de la communication nord avec SSL (Secure Sockets Layer) entre les nœuds du contrôleur de réseau et les clients de gestion, tels que System Center Virtual Machine Manager.
2. Authentification entre les nœuds du contrôleur de réseau et les appareils et services orientés vers le sud, tels que les hôtes Hyper-V et les équilibreurs de charge logiciel (SLB).

Création et inscription d’un certificat X.509

Vous pouvez créer et inscrire un certificat auto-signé ou un certificat émis par une autorité de certification.

> **Remarque**
>
> Lorsque vous utilisez SCVMM pour déployer le contrôleur de réseau, vous devez spécifier le certificat X.509 utilisé pour chiffrer les communications Northbound pendant la configuration du modèle de service du contrôleur de réseau.

La configuration du certificat doit inclure les valeurs suivantes.

- La valeur de la zone de texte **RestEndPoint** doit être le nom de domaine complet du contrôleur de réseau (FQDN) ou l'adresse IP.
- La valeur **RestEndPoint** doit correspondre au nom de l'objet (Nom commun, CN) du certificat X.509.

Création d'un certificat X.509 auto-signé

Vous pouvez créer un certificat X.509 auto-signé et l'exporter avec la clé privée (protégée par un mot de passe) en suivant ces étapes pour les déploiements à nœud unique et à plusieurs nœuds du contrôleur de réseau.

Lorsque vous créez des certificats auto-signés, vous pouvez utiliser les instructions suivantes.

- Vous pouvez utiliser l'adresse IP du point de terminaison REST du contrôleur de réseau pour le paramètre DnsName, mais cela n'est pas recommandé, car cela nécessite que les nœuds du contrôleur de réseau se trouvent tous dans un seul sous-réseau de gestion (par exemple, sur un seul rack)
- Pour les déploiements de contrôleur de réseau à plusieurs nœuds, le nom DNS que vous spécifiez deviendra le nom de domaine complet du cluster du contrôleur de réseau (les enregistrements DNS Host A sont créés automatiquement.)
- Pour les déploiements de contrôleur de réseau à nœud unique, le nom DNS peut être le nom d'hôte du contrôleur de réseau suivi du nom de domaine complet.

Nœud multiple

Vous pouvez utiliser la commande New-SelfSignedCertificate Windows PowerShell pour créer un certificat auto-signé.

Syntaxe

PowerShell

```
New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong
Cryptographic Provider" -FriendlyName "<YourNCComputerName>" -DnsName @("
<NCRESTName>")
```

Exemple d'utilisation

PowerShell

```
New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong
Cryptographic Provider" -FriendlyName "MultiNodeNC" -DnsName
@("NCCluster.Contoso.com")
```

Nœud unique

Vous pouvez utiliser la commande New-SelfSignedCertificate Windows PowerShell pour créer un certificat auto-signé.

Syntaxe

PowerShell

```
New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong
Cryptographic Provider" -FriendlyName "<YourNCComputerName>" -DnsName @("<NCFQDN>")
```

Exemple d'utilisation

PowerShell

```
New-SelfSignedCertificate -KeyUsageProperty All -Provider "Microsoft Strong
Cryptographic Provider" -FriendlyName "SingleNodeNC" -DnsName
@("SingleNodeNC.Contoso.com")
```

Création d'un certificat X.509 signé par l'autorité de certification

Pour créer un certificat à l'aide d'une autorité de certification, vous devez avoir déjà déployé une infrastructure à clé publique (PKI) avec les services de certificats Active Directory (AD CS).

> ⓘ **Remarque**

Vous pouvez utiliser des autorités de certification ou des outils tiers, tels que openssl, pour créer un certificat à utiliser avec le contrôleur de réseau, mais les instructions de cette rubrique sont spécifiques à AD CS. Pour savoir comment utiliser une autorité de certification ou un outil tiers, consultez la documentation relative au logiciel que vous utilisez.

La création d'un certificat avec une autorité de certification inclut les étapes suivantes.

1. Vous ou l'administrateur de domaine ou de sécurité de votre organisation configurez le modèle de certificat.
2. Vous ou l'administrateur de contrôleur de réseau de votre organisation ou l'administrateur SCVMM demande un nouveau certificat auprès de l'autorité de certification.

Configuration requise pour les certificats

Pendant que vous configurez un modèle de certificat à l'étape suivante, assurez-vous que le modèle que vous configurez inclut les éléments requis suivants.

1. Le nom du sujet du certificat doit être le nom de domaine complet de l'hôte Hyper-V.
2. Le certificat doit être placé dans le stockage personnel de l'ordinateur local (My – cert:\localmachine\my).
3. Le certificat doit avoir à la fois les politiques d'application pour l'authentification serveur (EKU : 1.3.6.1.5.5.7.3.1) et l'authentification client (EKU : 1.3.6.1.5.5.7.3.2).

Remarque

Si le magasin de certificats Personnel (My – cert:\localmachine\my) sur l'hôte Hyper-V comporte plusieurs certificats X.509 avec le nom d'objet (CN) comme nom de domaine complet (FQDN) de l'hôte, veillez à ce que le certificat utilisé par SDN possède une propriété personnalisée supplémentaire d'utilisation améliorée de la clé avec l'OID 1.3.6.1.4.1.311.95.1.1.1. Sinon, la communication entre le Contrôleur de réseau et l'hôte risquerait de ne pas fonctionner.

Pour configurer le modèle de certificat

Remarque

Avant d'effectuer cette procédure, vous devez passer en revue les exigences de certificat et les modèles de certificats disponibles dans la console Modèles de certificats. Vous pouvez

modifier un modèle existant ou créer un doublon d'un modèle existant, puis modifier votre copie du modèle. Il est recommandé de créer une copie d'un modèle existant.

1. Sur le serveur sur lequel AD CS est installé, dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**. La Console de gestion de l'autorité de certification Microsoft (Microsoft Management Console - MMC) s'ouvre.
2. Dans la console MMC, double-cliquez sur le nom de l'autorité de certification, faites un clic droit sur **Modèles de certificat**, puis cliquez sur **Gérer**.
3. La console Modèles de certificats s'ouvre. Tous les modèles de certificat sont affichés dans le volet d'informations.
4. Dans le volet d'informations, cliquez sur le modèle que vous souhaitez dupliquer.
5. Cliquez sur le menu **Action**, puis sur **Dupliquer le modèle**. La boîte de dialogue **Propriétés** du modèle s'ouvre.
6. Dans la boîte de dialogue **Propriétés** du modèle, sous l'onglet **Nom de l'objet**, cliquez sur **Fournir dans la requête**. (Ce paramètre est requis pour les certificats SSL du contrôleur de réseau.)
7. Dans la boîte de dialogue **Propriétés** du modèle, sous l'onglet **Gestion des requêtes**, vérifiez que l'option **Autoriser l'exportation de la clé privée** est sélectionnée. Vérifiez également que l'objectif **Signature et chiffrement** est sélectionné.
8. Dans la boîte de dialogue **Propriétés** du modèle, sous l'onglet **Extensions**, sélectionnez **Utilisation de la clé**, puis cliquez sur **Modifier**.
9. Dans **Signature**, vérifiez que **Signature numérique** est sélectionnée.
10. Dans la boîte de dialogue **Propriétés** du modèle, sous l'onglet **Extensions**, sélectionnez **Stratégies d'application**, puis cliquez sur **Modifier**.
11. Dans **Stratégies d'application**, vérifiez que les options **Authentification client** et **Authentification serveur** sont répertoriées.
12. Enregistrez la copie du modèle de certificat avec un nom unique, tel que le **Modèle de contrôleur de réseau**.

Pour demander un certificat à l'autorité de certification

Vous pouvez utiliser le composant logiciel enfichable Certificats pour demander des certificats. Vous pouvez demander n'importe quel type de certificat préconfiguré et mis à disposition par un administrateur de l'autorité de certification qui traite la demande de certificat.

Utilisateurs ou **Administrateurs** locaux est l'appartenance minimale au groupe requise pour effectuer cette procédure.

1. Ouvrez le composant logiciel enfichable Certificats d'un ordinateur.
2. Dans l'arborescence de la console, cliquez sur **Certificats (ordinateur local)**. Sélectionnez le magasin de certificats **Personnel**.
3. Dans le menu **Action**, pointez sur** Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat** pour démarrer l'Assistant d'inscription de certificats. Cliquez sur **Suivant**.
4. Sélectionnez la stratégie d'inscription de certificat **Configurée par votre administrateur**, puis cliquez sur **Suivant**.
5. Sélectionnez la **Stratégie d'inscription Active Directory** (basée sur le modèle d'autorité de certification que vous avez configuré dans la section précédente).
6. Développez la section **Détails** et configurez les éléments suivants.
7. L'**usage des clés** doit inclure la **signature numérique **et le** chiffrage de clés**.
8. Vérifiez que les **stratégies d'application** incluent **l'authentification serveur** (1.3.6.1.5.5.7.3.1) et **l'authentification client** (1.3.6.1.5.5.7.3.2).
9. Cliquez sur **Propriétés**.
10. Sous l'onglet **Objet**, dans **Nom de l'objet**, dans **Type**, sélectionnez **Nom commun**. Dans Valeur, spécifiez le **point de terminaison REST du contrôleur de réseau**.
11. Cliquez sur **Appliquer**, puis sur **OK**.
12. Cliquez sur **Inscrire**.

Dans la MMC Certificats, cliquez sur le magasin Personnel pour afficher le certificat que vous avez inscrit à partir de l'autorité de certification.

Exporter et copier le certificat dans la bibliothèque SCVMM

Une fois le certificat auto-signé ou signé par une autorité de certification créé, vous devez exporter le certificat avec la clé privée (au format .pfx) et sans la clé privée (au format Base-64 .cer) à partir du composant logiciel enfichable Certificats.

Vous devez ensuite copier les deux fichiers exportés dans les dossiers **ServerCertificate.cr** et **NCCertificate.cr** que vous avez spécifiés au moment où vous avez importé le modèle de service NC.

1. Ouvrez le composant logiciel enfichable Certificats (certlm.msc) et recherchez le certificat dans le magasin de certificats Personnel de l'ordinateur local.
2. Cliquez avec le bouton droit sur le certificat, cliquez sur **Toutes les tâches**, puis cliquez sur **Exporter**. L'assistant d'exportation de certificat s'ouvre. Cliquez sur **Suivant**.
3. Sélectionnez **Oui**, exportez l'option de la clé privée, puis cliquez sur **Suivant**.

4. Choisissez **Échange d'informations personnelles - PKCS #12 (.PFX)** et acceptez la valeur par défaut **Inclure tous les certificats dans le chemin d'accès de certification si possible**.
5. Affectez les utilisateurs/groupes et un mot de passe pour le certificat que vous exportez, cliquez sur **Suivant**.
6. Dans la page Fichier à exporter, accédez à l'emplacement où vous souhaitez placer le fichier exporté et donnez-lui un nom.
7. De même, exportez le certificat au format .CER. Remarque : Pour exporter au format. CER, décochez l'option Oui, exporter la clé privée.
8. Copiez le fichier .PFX dans le dossier ServerCertificate.cr.
9. Copiez le fichier .CER dans le dossier NCCertificate.cr.

Lorsque vous avez terminé, actualisez ces dossiers dans la bibliothèque SCVMM et vérifiez que vous avez copié ces certificats. Poursuivez la configuration et le déploiement du modèle de service de contrôleur de réseau.

Authentification des appareils et services orientés vers le sud

La communication du contrôleur de réseau avec les hôtes et les appareils SLB MUX utilise des certificats pour l'authentification. La communication avec les hôtes est sur le protocole OVSDB, tandis que la communication avec les appareils MUX SLB est sur le protocole WCF.

Communication de l'hôte Hyper-V avec le contrôleur de réseau

Pour la communication avec les hôtes Hyper-V via OVSDB, le contrôleur de réseau doit présenter un certificat aux machines hôtes. Par défaut, SCVMM récupère le certificat SSL configuré sur le contrôleur de réseau et l'utilise pour la communication sud avec les hôtes.

C'est la raison pour laquelle le certificat SSL doit être configuré pour l'EKU d'authentification du client. Ce certificat est configuré sur la ressource REST « Serveurs » (les hôtes Hyper-V sont représentés dans le contrôleur de réseau en tant que ressource serveur) et peuvent être affichés en exécutant la commande **Windows PowerShell Get-NetworkControllerServer**.

Voici un exemple partiel de la ressource REST du serveur.

```
"resourceId": "host31.fabrikam.com",
   "properties": {
     "connections": [
       {
```

```
            "managementAddresses": [
               "host31.fabrikam.com"
            ],
            "credential": {
              "resourceRef": "/credentials/a738762f-f727-43b5-9c50-cf82a70221fa"
            },
            "credentialType": "X509Certificate"
          }
        ],
```

Pour l'authentification mutuelle, l'hôte Hyper-V doit également disposer d'un certificat pour communiquer avec le contrôleur de réseau.

Vous pouvez inscrire le certificat auprès d'une autorité de certification. Si un certificat basé sur une autorité de certification est introuvable sur l'ordinateur hôte, SCVMM crée un certificat auto-signé et le provisionne sur l'ordinateur hôte.

Le contrôleur de réseau et les certificats hôtes Hyper-V doivent être approuvés les uns par les autres. Le certificat racine du certificat hôte Hyper-V doit être présent dans le magasin des autorités de certification racines de confiance du contrôleur de réseau de l'ordinateur local, et vice versa.

Quand vous utilisez des certificats auto-signés, SCVMM garantit que les certificats requis sont présents dans le magasin des autorités de certification racines de confiance de l'ordinateur local.

Si vous utilisez les certificats basés sur une autorité de certification des hôtes Hyper-V, vous devez vous assurer que le certificat racine de l'autorité de certification est présent sur le magasin des autorités de certification racines de confiance du contrôleur de réseau de l'ordinateur local.

Communication MUX de l'équilibreur de charge logiciel avec le contrôleur de réseau

Le logiciel Load Balancer multiplexeur (MUX) et le contrôleur de réseau communiquent via le protocole WCF, à l'aide de certificats pour l'authentification.

Par défaut, SCVMM récupère le certificat SSL configuré sur le contrôleur de réseau et l'utilise pour la communication sud avec les appareils MUX. Ce certificat est configuré sur la ressource REST « NetworkControllerLoadBalancerMux » et peut être affiché en exécutant l'applet de commande PowerShell **Get-NetworkControllerLoadBalancerMux**.

Exemple de ressource REST MUX (partielle) :

```
      "resourceId": "slbmux1.fabrikam.com",
      "properties": {
        "connections": [
          {
            "managementAddresses": [
               "slbmux1.fabrikam.com"
            ],
            "credential": {
              "resourceRef": "/credentials/a738762f-f727-43b5-9c50-cf82a70221fa"
            },
            "credentialType": "X509Certificate"
          }
        ],
```

Pour l'authentification mutuelle, vous devez également disposer d'un certificat sur les appareils SLB MUX. Ce certificat est automatiquement configuré par SCVMM lorsque vous déployez un équilibreur de charge logiciel à l'aide de SCVMM.

> **Important**
>
> Sur les nœuds hôte et SLB, il est essentiel que le magasin des autorités de certification racines de confiance n'inclut aucun certificat dans lequel la valeur « Émis à » n'est pas la même que celle de « Émis par ». Si cela se produit, la communication entre le contrôleur de réseau et l'appareil de liaison descendante échoue.

Le contrôleur de réseau et les certificats multiplexeurs SLB doivent être approuvés les uns par les autres (le certificat racine du certificat multiplexeur SLB doit être présent dans le magasin des autorités de certification racines de confiance de l'ordinateur du contrôleur de réseau et vice versa). Quand vous utilisez des certificats auto-signés, SCVMM garantit que les certificats requis sont présents dans le magasin des autorités de certification racines de confiance de l'ordinateur local.

Dernière mise à jour : 15/09/2026

Renouveler des certificats pour le contrôleur de réseau

> S'applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022 et Windows Server 2019

Cet article fournit des instructions sur le renouvellement ou la modification des certificats de contrôleur de réseau, automatiquement et manuellement. Si vous rencontrez des problèmes lors du renouvellement de vos certificats de contrôleur de réseau, contactez Support Microsoft.

Dans votre réseau SDN (Software Defined Networking) géré par l'infrastructure d'outils locaux, le contrôleur de réseau utilise l'authentification basée sur des certificats pour sécuriser les canaux de communication Northbound avec des clients de gestion et des communications southbound avec des appareils réseau, comme l'équilibreur de charge logiciel. Les certificats du contrôleur de réseau sont fournis avec une certaine période de validité, au-delà de laquelle ils deviennent non valides et ne peuvent plus être utilisés. Nous vous recommandons vivement de les renouveler avant leur expiration.

Pour obtenir une vue d'ensemble du contrôleur de réseau, consultez Qu'est-ce que le contrôleur de réseau ?

Quand renouveler ou modifier des certificats de contrôleur de réseau

Vous pouvez renouveler ou modifier des certificats de contrôleur de réseau quand :

- Les certificats arrivent à expiration. Vous pouvez en effet renouveler des certificats de contrôleur de réseau à tout moment avant leur expiration.

  > **Remarque**
  >
  > Si vous renouvelez des certificats existants avec la même clé, vous n'avez rien de plus à faire.

- Vous souhaitez remplacer un certificat auto-signé par un certificat signé par une autorité de certification.

> **Remarque**
>
> Lors d'un changement de certificat, veillez à utiliser le même nom d'objet que l'ancien certificat.

Types de certificats du contrôleur de réseau

Dans Azure Local, chaque machine virtuelle de contrôleur de réseau utilise deux types de certificats :

- Certificat REST. Certificat unique pour les communications vers les composants de niveau supérieur avec les clients REST (comme Windows Admin Center) et pour les communications vers les composants de niveau inférieur avec les hôtes Hyper-V et les équilibreurs de charge logiciels. Ce même certificat est présent sur toutes les machines virtuelles du contrôleur de réseau. Pour renouveler des certificats REST, consultez la section Renouveler des certificats REST.
- Certificat de nœud du contrôleur de réseau. Certificat sur chaque machine virtuelle du contrôleur de réseau pour l'authentification entre nœuds. Pour renouveler les certificats de nœud du contrôleur de réseau, consultez la section Renouveler des certificats de nœud.

> **Avertissement**
>
> Ne laissez pas ces certificats expirer. Renouvelez-les avant l'expiration pour éviter tout problème d'authentification. En outre, ne supprimez aucun certificat expiré existant avant de les renouveler. Pour connaître la date d'expiration d'un certificat, consultez **Afficher l'expiration** du certificat.

Afficher l'expiration du certificat

Utilisez la cmdlet suivante sur chaque machine virtuelle du contrôleur de réseau pour vérifier la date d'expiration d'un certificat :

PowerShell

```
Get-ChildItem Cert:\LocalMachine\My | where{$_.Subject -eq "CN=<Certificate-subject-name>"} | Select-Object NotAfter, Subject
```

- Pour obtenir l'expiration d'un certificat REST, remplacez « Certificate-subject-name » par RestIPAddress ou RestName du contrôleur de réseau. Vous pouvez obtenir cette valeur à partir de la cmdlet `Get-NetworkController`.
- Pour obtenir l'expiration d'un certificat de nœud, remplacez « Certificate-subject-name » par le nom de domaine complet (FQDN) de la machine virtuelle du contrôleur de réseau. Vous pouvez obtenir cette valeur à partir de la cmdlet `Get-NetworkController`.

Renouveler les certificats du contrôleur de réseau

Vous pouvez renouveler vos certificats de contrôleur de réseau automatiquement ou manuellement.

Renouvellement automatique

L'applet Start-SdnCertificateRotation de commande vous permet d'automatiser le renouvellement de vos certificats de contrôleur de réseau. Le renouvellement automatique du certificat permet de réduire les temps d'arrêt ou les pannes non planifiées causées par des problèmes d'expiration de certificat.

Voici les scénarios dans lesquels vous pouvez utiliser l'applet `Start-SdnCertificateRotation` de commande pour renouveler automatiquement les certificats du contrôleur de réseau :

- Certificats auto-signés. Utilisez l'applet `Start-SdnCertificateRotation` de commande pour générer des certificats auto-signés et renouveler ces certificats dans tous les nœuds du contrôleur de réseau.
- Apportez votre propre certificat. Vous apportez vos propres certificats, auto-signés ou signés par l'autorité de certification et utilisez l'applet de commande pour le `Start-SdnCertificateRotation` renouvellement des certificats. L'applet de commande installe les certificats sur tous les nœuds du contrôleur de réseau et les distribue à d'autres composants d'infrastructure SDN.
- Certificats préinstallés. Les certificats requis sont déjà installés sur les nœuds du contrôleur de réseau. Utilisez l'applet `Start-SdnCertificateRotation` de commande pour renouveler ces certificats à d'autres composants d'infrastructure SDN.

Pour plus d'informations sur la création et la gestion de certificats SDN, consultez Gérer les certificats pour la mise en réseau définie par logiciel.

Spécifications

Voici les conditions requises pour le renouvellement automatique du certificat :

- Vous devez exécuter l'applet `Start-SdnCertificateRotation` de commande sur l'un des nœuds du contrôleur de réseau. Pour obtenir des instructions d'installation, consultez le module Installer SdnDiagnostics.
- Vous devez disposer d'informations d'identification pour les deux types de comptes suivants pour autoriser la communication entre les nœuds du contrôleur de réseau :
  - `Credential` pour spécifier un compte d'utilisateur avec des privilèges d'administrateur local sur le contrôleur de réseau.
  - `NcRestCredential` pour spécifier un compte d'utilisateur ayant accès à l'API REST du contrôleur de réseau. C'est un membre du `ClientSecurityGroup` de Get-NetworkController. Ce compte est utilisé pour appeler l'API REST pour mettre à jour la ressource d'informations d'identification avec le nouveau certificat.

  Pour plus d'informations sur la configuration de l'autorisation pour la communication Northbound du contrôleur de réseau, consultez Autorisation pour la communication Northbound.

Renouveler automatiquement des certificats auto-signés

Vous pouvez utiliser l'applet `Start-SdnCertificateRotation` de commande pour générer de nouveaux certificats auto-signés et les renouveler automatiquement sur tous les nœuds du contrôleur de réseau. Par défaut, l'applet de commande génère des certificats avec une période de validité de trois ans, mais vous pouvez spécifier une période de validité différente.

Effectuez ces étapes sur l'un des nœuds du contrôleur de réseau pour générer des certificats auto-signés et les renouveler automatiquement :

1. Pour générer des certificats auto-signés, exécutez la cmdlet `Start-SdnCertificateRotation`. Vous pouvez utiliser le `-Force` paramètre avec l'applet de commande pour éviter toute invite de confirmation ou d'entrées manuelles pendant le processus de rotation.

   - Pour générer des certificats auto-signés avec la période de validité par défaut de trois ans, exécutez les commandes suivantes :

     PowerShell

```
Import-Module -Name SdnDiagnostics -Force
Start-SdnCertificateRotation -GenerateCertificate -CertPassword (Get-Credential).Password -Credential (Get-Credential)
```

- Pour générer des certificats auto-signés avec une période de validité spécifique, utilisez le `NotAfter` paramètre pour spécifier la période de validité.

  Par exemple, pour générer des certificats auto-signés avec une période de validité de cinq ans, exécutez les commandes suivantes :

  PowerShell

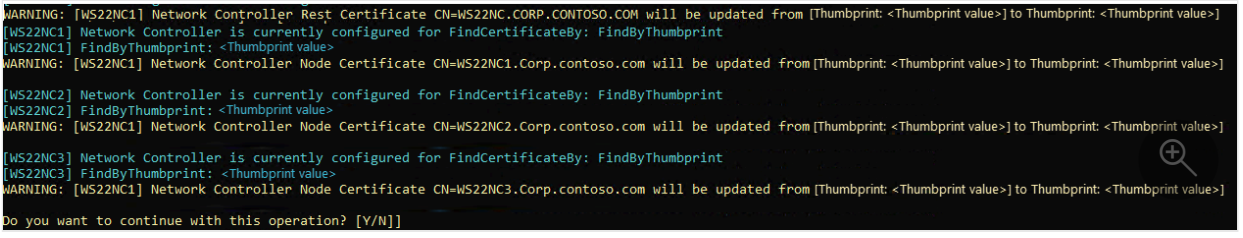
```
Import-Module -Name SdnDiagnostics -Force
Start-SdnCertificateRotation -GenerateCertificate -CertPassword (Get-Credential).Password -NotAfter (Get-Date).AddYears(5) -Credential (Get-Credential)
```

2. Entrez les informations d'identification. Vous obtenez deux invites pour fournir deux types d'informations d'identification :

   - Dans la première invite, entrez le mot de passe pour sécuriser le certificat généré. Le nom d'utilisateur peut être n'importe quoi et n'est pas utilisé.
   - Dans la deuxième invite, utilisez les informations d'identification qui disposent d'un accès administrateur à tous les nœuds du contrôleur de réseau.

3. Une fois les nouveaux certificats générés, vous recevez un avertissement pour confirmer si vous souhaitez poursuivre le processus de rotation des certificats. Le texte d'avertissement affiche la liste des certificats de contrôleur de réseau qui seront remplacés par les certificats nouvellement générés. Tapez `Y` pour confirmer.

   Voici un exemple de capture d'écran de l'avertissement :

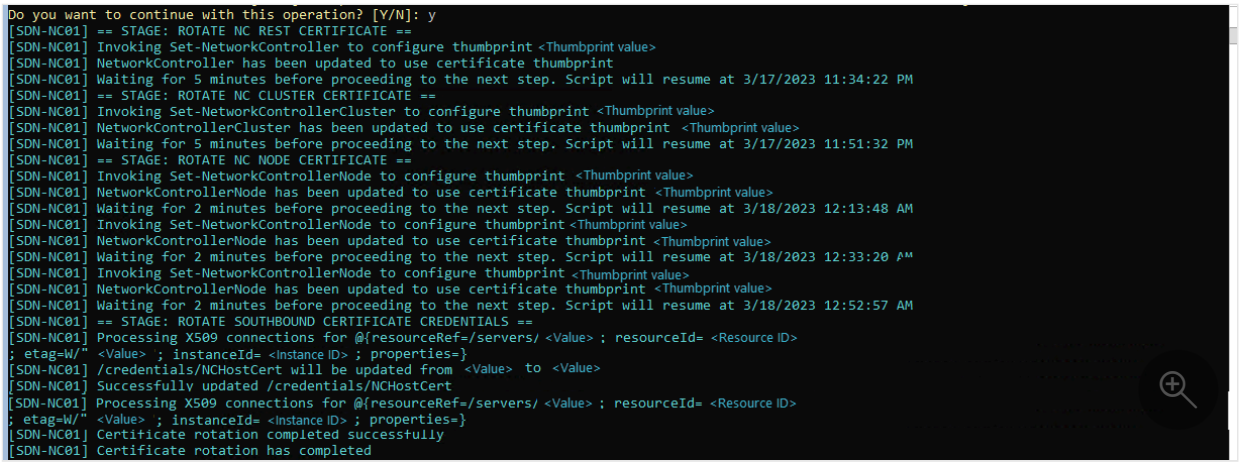


4. Après avoir confirmé la poursuite de la rotation des certificats, vous pouvez afficher l'état des opérations en cours dans la fenêtre de commande PowerShell.

> **Important**

> Ne fermez pas la fenêtre PowerShell tant que l'applet de commande n'est pas terminée. Selon votre environnement, tel que le nombre de nœuds de contrôleur de réseau dans le cluster, la fin peut prendre plusieurs minutes ou plus d'une heure.

Voici un exemple de capture d'écran de la fenêtre de commande PowerShell montrant l'état des opérations en cours :



Renouveler automatiquement vos propres certificats

En plus de générer des certificats de contrôleur de réseau auto-signés, vous pouvez également apporter vos propres certificats, auto-signés ou signés par l'autorité de certification, et utiliser l'applet `Start-SdnCertificateRotation` de commande pour renouveler ces certificats.

Effectuez ces étapes sur l'un des nœuds du contrôleur de réseau pour renouveler automatiquement vos propres certificats :

1. Préparez vos certificats au `.pfx` format et enregistrez dans un dossier sur l'un des nœuds du contrôleur de réseau à partir duquel vous exécutez l'applet `Start-SdnCertificateRotation` de commande. Vous pouvez utiliser le `-Force` paramètre avec l'applet de commande pour éviter toute invite de confirmation ou d'entrées manuelles pendant le processus de rotation.

2. Pour démarrer le renouvellement du certificat, exécutez les commandes suivantes :

PowerShell

```
Import-Module -Name SdnDiagnostics -Force
Start-SdnCertificateRotation -CertPath "<Path where you put your
```

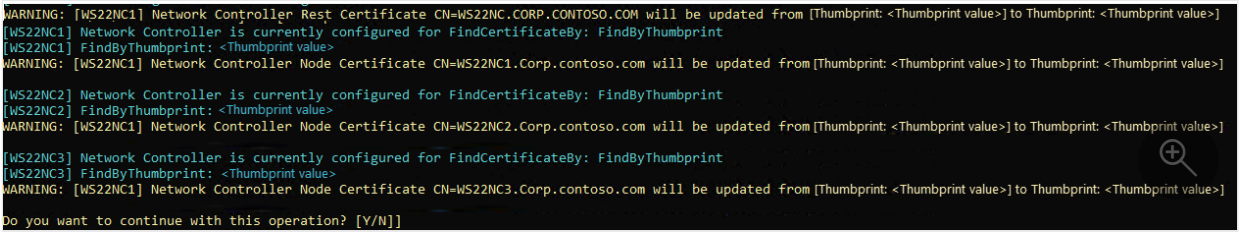
```
certificates>" -CertPassword (Get-Credential).Password -Credential (Get-Credential)
```

3. Entrez les informations d'identification. Vous obtenez deux invites pour fournir deux types d'informations d'identification :

   - Dans la première invite, entrez le mot de passe de votre certificat. Le nom d'utilisateur peut être n'importe quoi et n'est pas utilisé.
   - Dans la deuxième invite, utilisez les informations d'identification qui disposent d'un accès administrateur à tous les nœuds du contrôleur de réseau.

4. Vous recevez un avertissement pour confirmer si vous souhaitez poursuivre le processus de rotation des certificats. Le texte d'avertissement affiche la liste des certificats de contrôleur de réseau qui seront remplacés par les certificats nouvellement générés. Tapez `Y` pour confirmer.

   Voici un exemple de capture d'écran de l'avertissement :



5. Après avoir confirmé la poursuite de la rotation des certificats, vous pouvez afficher l'état des opérations en cours dans la fenêtre de commande PowerShell.

   > **ⓘ Important**
   >
   > Ne fermez pas la fenêtre PowerShell tant que l'applet de commande n'est pas terminée. Selon votre environnement, tel que le nombre de nœuds de contrôleur de réseau dans le cluster, la fin peut prendre plusieurs minutes ou plus d'une heure.

Renouveler automatiquement les certificats préinstallés

Dans ce scénario, vous disposez des certificats requis installés sur les nœuds du contrôleur de réseau. Utilisez l'applet `Start-SdnCertificateRotation` de commande pour renouveler ces certificats sur d'autres composants d'infrastructure SDN.

Effectuez ces étapes sur l'un des nœuds du contrôleur de réseau pour renouveler automatiquement les certificats préinstallés :

1. Installez les certificats du contrôleur de réseau sur tous les nœuds du contrôleur de réseau en fonction de votre méthode préférée. Vérifiez que les certificats sont approuvés par d'autres composants d'infrastructure SDN, notamment les serveurs SDN MUX et les hôtes SDN.

2. Créer une configuration de rotation de certificat :

   a. Pour générer la configuration de rotation de certificat par défaut, exécutez les commandes suivantes :

   PowerShell

   ```
   Import-Module -Name SdnDiagnostics -Force
   $certConfig = New-SdnCertificateRotationConfig
   $certConfig
   ```

   b. Passez en revue la configuration de rotation des certificats par défaut pour vérifier si les certificats détectés automatiquement sont ceux que vous souhaitez utiliser. Par défaut, il récupère le dernier certificat émis à utiliser.

   Voici un exemple de configuration de rotation de certificat :

   Output

   ```
   PS C:\Users\LabAdmin> $certConfig

   Name                    Value
   ----                    -----
   ws22ncl.corp.contoso.com    F4AAF14991DAF282D9056E147AE60C2C5FE80A49
   ws22nc3.corp.contoso.com    BC3E6B090E2AA80220B7BAED7F8F981A1E1DD115
   ClusterCredentialType       X509
   ws22nc2.corp.contoso.corn   75DC229A8E61AD855CC445C42482F9F919CC1077
   NcRestCert              029D7CA0067A60FB24827D8434566787114AC30C
   ```

   où :

   - **ws22nc*x.corp.contoso.com*** affiche l'empreinte numérique du certificat pour chaque nœud du contrôleur de réseau.
   - **ClusterCredentialType** affiche le type d'authentification du cluster du contrôleur de réseau. Si le type d'authentification n'est pas X509, le certificat de nœud n'est pas utilisé et n'est pas affiché dans la sortie.

- **NcRestCert** affiche l'empreinte numérique du certificat Rest du contrôleur de réseau.

c. (Facultatif) Si la génération `$certConfig` n'est pas correcte, vous pouvez la modifier en spécifiant l'empreinte numérique d'un nouveau certificat. Par exemple, pour modifier l'empreinte numérique du certificat Rest du contrôleur de réseau, exécutez la commande suivante :

PowerShell

```
$certConfig.NcRestCert = <new certificate thumbprint>
```

3. Démarrez la rotation des certificats. Vous pouvez utiliser le `-Force` paramètre avec l'applet de commande pour éviter toute invite de confirmation ou d'entrées manuelles pendant le processus de rotation.

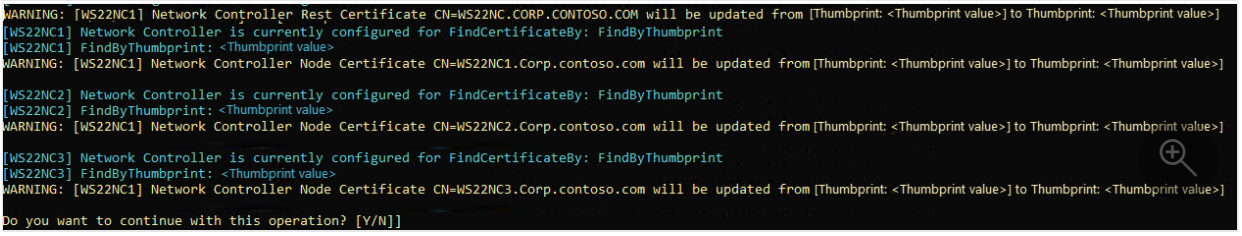
PowerShell

```
Import-Module -Name SdnDiagnostics -Force
Start-SdnCertificateRotation -CertRotateConfig $certConfig -Credential (Get-Credential)
```

4. Lorsque vous y êtes invité, entrez les informations d'identification qui disposent d'un accès administrateur à tous les nœuds du contrôleur de réseau.

5. Vous recevez un avertissement pour confirmer si vous souhaitez poursuivre la rotation automatique des certificats. L'avertissement affiche la liste des certificats de contrôleur de réseau qui seront remplacés par vos propres certificats. Tapez `Y` pour confirmer.

   Voici un exemple de capture d'écran de l'avertissement qui vous invite à confirmer la rotation des certificats :



6. Après avoir confirmé la poursuite de la rotation des certificats, vous pouvez afficher l'état des opérations en cours dans la fenêtre de commande PowerShell.

> **Important**

Ne fermez pas la fenêtre PowerShell tant que l'applet de commande n'est pas terminée. Selon votre environnement, tel que le nombre de nœuds de contrôleur de réseau dans le cluster, la fin peut prendre plusieurs minutes ou plus d'une heure.

Réimporter des certificats dans Windows Admin Center

Si vous avez renouvelé le certificat REST du contrôleur de réseau et que vous utilisez Windows Admin Center pour gérer SDN, vous devez supprimer l'instance locale Azure de Windows Admin Center et l'ajouter à nouveau. En procédant ainsi, vous vous assurez que Windows Admin Center importe le certificat renouvelé et l'utilise pour la gestion SDN.

Procédez comme suit pour réimporter le certificat renouvelé dans Windows Admin Center :

1. Dans Windows Admin Center, sélectionnez **Gestionnaire** de cluster dans le menu déroulant supérieur.
2. Sélectionnez le cluster à supprimer, puis sélectionnez **Supprimer**.
3. Sélectionnez **Ajouter**, entrez le nom du cluster, puis sélectionnez **Ajouter**.
4. Une fois le cluster chargé, sélectionnez **Infrastructure** SDN. Cela force Windows Admin Center à réimporter automatiquement le certificat renouvelé.

Étapes suivantes

- Mettez à jour l'infrastructure SDN pour Azure Local.

Dernière mise à jour : 15/09/2026

Kerberos avec un nom principal de service (SPN)

> S’applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019

Cet article explique comment utiliser l’authentification Kerberos avec le nom du principal de service (SPN).

Le contrôleur de réseau prend en charge plusieurs méthodes d’authentification pour la communication avec les clients de gestion. Vous pouvez utiliser l’authentification Kerberos, l’authentification basée sur les certificats X509. Vous avez également la possibilité d’utiliser aucune authentification pour les déploiements de test.

System Center Virtual Machine Manager utilise l’authentification Kerberos. Si vous utilisez l’authentification Kerberos, vous devez configurer un SPN pour le contrôleur de réseau dans Active Directory. Le SPN est un identificateur unique pour l’instance de service du contrôleur de réseau, qui est utilisé par l’authentification Kerberos pour associer une instance de service à un compte de connexion de service. Pour plus d'information, consultez Noms Principal de Service.

Configurer des noms de principal du service (SPN)

Le contrôleur de réseau configure automatiquement le SPN. Il vous suffit de fournir des autorisations pour que les machines du contrôleur de réseau inscrivent et modifient le SPN.

1. Sur l’ordinateur contrôleur de domaine, démarrez **Utilisateurs et ordinateurs Active Directory**.
2. Sélectionnez **Affichage** > **avancé**.
3. Sous **Ordinateurs**, recherchez l’un des comptes d’ordinateur du contrôleur de réseau, puis cliquez avec le bouton droit et sélectionnez **Propriétés**.
4. Sélectionnez l’onglet **Sécurité** et **sélectionnez Avancé**.
5. Dans la liste, si tous les comptes de l’ordinateur du contrôleur de réseau ou un groupe de sécurité dont tous les comptes d’ordinateur de contrôleur de réseau ne sont pas répertoriés, sélectionnez **Ajouter** pour l’ajouter.

6. Pour chaque compte d'ordinateur du contrôleur de réseau ou un seul groupe de sécurité contenant les comptes d'ordinateur du contrôleur de réseau :

   a. Sélectionnez le compte ou le groupe, puis sélectionnez **Modifier**.

   b. Sous Autorisations, sélectionnez **Valider Write servicePrincipalName**.

   c. Faites défiler vers le bas et, sous **Propriétés** , sélectionnez :

      - **Lire NomPrincipalDuService**
      - **Écrire le nom principal de service**

   d. Sélectionnez **OK** deux fois.

7. Répétez les étapes 3 à 6 pour chaque contrôleur de réseau.

8. Fermez **les utilisateurs et ordinateurs Active Directory**.

Impossible de fournir des autorisations pour l'inscription ou la modification du SPN.

Sur un nouveau déploiement de Windows Server 2019, si vous avez choisi Kerberos pour l'authentification du client REST et que vous n'autorisez pas les nœuds du contrôleur de réseau à inscrire ou modifier le SPN, les opérations REST sur le contrôleur de réseau échouent. Cela vous empêche de gérer efficacement votre infrastructure SDN.

Pour une mise à niveau de Windows Server 2016 vers Windows Server 2019 et que vous avez choisi Kerberos pour l'authentification du client REST, les opérations REST ne sont pas bloquées, ce qui garantit la transparence des déploiements de production existants.

Si spN n'est pas inscrit, l'authentification du client REST utilise NTLM, ce qui est moins sécurisé. Vous recevez également un événement critique dans le canal d'événements Admin du canal d'événements **NetworkController-Framework**, vous demandant de fournir des autorisations aux nœuds du contrôleur de réseau pour inscrire le SPN. Une fois que vous avez fourni l'autorisation, le contrôleur de réseau inscrit automatiquement le SPN et toutes les opérations clientes utilisent Kerberos.

> **Conseil**
>
> En règle générale, vous pouvez configurer le contrôleur de réseau pour qu'il utilise une adresse IP ou un nom DNS pour les opérations basées sur REST. Toutefois, lorsque vous

configurez Kerberos, vous ne pouvez pas utiliser d'adresse IP pour les requêtes REST sur le contrôleur de réseau. Par exemple, vous pouvez utiliser <https://networkcontroller.consotso.com>, mais vous ne pouvez pas utiliser <https://192.34.21.3>. Les noms de principal de service ne peuvent pas fonctionner si les adresses IP sont utilisées.

Si vous utilisiez l'adresse IP pour les opérations REST avec l'authentification Kerberos dans Windows Server 2016, la communication réelle aurait été effectuée sur l'authentification NTLM. Dans ce déploiement, une fois que vous effectuez une mise à niveau vers Windows Server 2019, vous continuez à utiliser l'authentification basée sur NTLM. Pour passer à l'authentification Kerberos, vous devez utiliser le nom DNS du contrôleur de réseau pour les opérations REST et fournir l'autorisation aux nœuds du contrôleur de réseau d'inscrire le SPN.

Étapes suivantes

- Sécurisez le contrôleur de réseau.

Dernière mise à jour : 15/09/2026

Configurer des groupes de sécurité réseau sur votre instance Azure Local avec PowerShell

> S'applique à : Azure Local 2311.2 et versions ultérieures ; Windows Server 2022, Windows Server 2019, Windows Server 2016

Cet article fournit des instructions pour configurer des groupes de sécurité réseau (NSG) pour gérer le flux de trafic de données à l'aide du pare-feu datacenter pour la mise en réseau SDN (Software Defined Networking) dans Azure Local à l'aide de Windows PowerShell. Vous activez et configurez le Pare-feu du centre de données en créant des groupes de sécurité réseau qui sont appliqués à un sous-réseau ou à une interface réseau.

Les exemples de scripts de cet article utilisent des commandes Windows PowerShell exportées à partir du module **NetworkController** . Vous pouvez également utiliser Windows Admin Center pour configurer et gérer des groupes de sécurité réseau.

Configurer le Pare-feu Datacenter de manière à autoriser tout le trafic

Une fois que vous avez déployé la mise en réseau SDN, vous devez tester la connectivité réseau de base dans votre nouvel environnement. Pour ce faire, créez une règle pour le Pare-feu Datacenter qui autorise tout le trafic réseau, sans restriction.

Utilisez les entrées du tableau suivant pour créer un ensemble de règles qui autorisent tout le trafic réseau entrant et sortant.

Agrandir le tableau

IP Source	IP de destination	Protocole	Port source	Port de destination	Sens	Action	Priorité
*	*	Tous	*	*	Trafic entrant	Autoriser	100
*	*	Tous	*	*	Règle de trafic sortant	Autoriser	110

Dans cet exemple, vous créez un groupe de sécurité réseau avec deux règles :

1. AllowAll_Inbound : permet à tout le trafic réseau de passer dans l'interface réseau où ce groupe de sécurité réseau est configuré.
2. **AllowAllOutbound** : autorise tout le trafic à passer hors de l'interface réseau. Ce groupe de sécurité réseau, identifié par l'ID de ressource « AllowAll-1 » est maintenant prêt à être utilisé dans les sous-réseaux virtuels et les interfaces réseau.

Vous pouvez exécuter cette commande à partir de n'importe quel ordinateur qui a accès au point de terminaison REST du contrôleur de réseau. Tout d'abord, ouvrez une session PowerShell. Dans cet exemple, utilisez l'applet de commande **Enter-PSSession** et remplacez `<computer-name>` par le nom de l'ordinateur disposant du point de terminaison REST du contrôleur de réseau.

PowerShell

```
Enter-PSSession <computer-name>
```

Ensuite, exécutez le script suivant pour créer le groupe de sécurité réseau :

PowerShell

```
$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "100"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"
$aclrule1 = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule1.Properties = $ruleproperties
$aclrule1.ResourceId = "AllowAll_Inbound"
$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "110"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"
$aclrule2 = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule2.Properties = $ruleproperties
$aclrule2.ResourceId = "AllowAll_Outbound"
$acllistproperties = new-object
```

```
Microsoft.Windows.NetworkController.AccessControlListProperties
$acllistproperties.AclRules = @($aclrule1, $aclrule2)
New-NetworkControllerAccessControlList -ResourceId "AllowAll" -Properties
$acllistproperties -ConnectionUri <NC REST FQDN>
```

> **Remarque**
>
> La référence de commande Windows PowerShell pour le contrôleur de réseau se trouve dans les applets de commande du contrôleur de réseau.

Utiliser des groupes de sécurité réseau pour limiter le trafic sur un sous-réseau

Dans cet exemple, vous créez un groupe de sécurité réseau qui empêche les machines virtuelles de communiquer entre elles dans le sous-réseau 192.168.0.0/24. Ce type de groupe de sécurité réseau est utile pour limiter la capacité d'un attaquant à se propager ultérieurement au sein du sous-réseau, tout en permettant aux machines virtuelles de recevoir des demandes provenant de l'extérieur du sous-réseau et de communiquer avec d'autres services sur d'autres sous-réseaux.

Agrandir le tableau

IP Source	IP de destination	Protocole	Port source	Port de destination	Sens	Action	Priorité
192.168.0.1	*	Tous	*	*	Trafic entrant	Autoriser	100
*	192.168.0.1	Tous	*	*	Règle de trafic sortant	Autoriser	101
192.168.0.0/24	*	Tous	*	*	Trafic entrant	Bloquer	102
*	192.168.0.0/24	Tous	*	*	Règle de trafic sortant	Bloquer	1:03
*	*	Tous	*	*	Trafic entrant	Autoriser	104
*	*	Tous	*	*	Règle de trafic sortant	Autoriser	105

Le groupe de sécurité réseau créé par l'exemple de script ci-dessous, identifié par l'ID de ressource **Subnet-192-168-0-0**, peut désormais être appliqué à un sous-réseau de réseau virtuel qui utilise l'adresse de sous-réseau « 192.168.0.0/24 ». Toute interface réseau attachée à ce sous-réseau de réseau virtuel obtient automatiquement les règles de groupe de sécurité réseau ci-dessus appliquées.

Voici un exemple de script pour créer ce groupe de sécurité réseau à l'aide de l'API REST du contrôleur de réseau :

PowerShell

```
import-module networkcontroller
$ncURI = "https://mync.contoso.local"
$aclrules = @()

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "192.168.0.1"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "100"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowRouter_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "192.168.0.1"
$ruleproperties.Priority = "101"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowRouter_Outbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
```

```
$ruleproperties.Action = "Deny"
$ruleproperties.SourceAddressPrefix = "192.168.0.0/24"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "102"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "DenySubnet_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Deny"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "192.168.0.0/24"
$ruleproperties.Priority = "103"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "DenySubnet_Outbound"

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "104"
$ruleproperties.Type = "Inbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowAll_Inbound"
$aclrules += $aclrule

$ruleproperties = new-object Microsoft.Windows.NetworkController.AclRuleProperties
$ruleproperties.Protocol = "All"
$ruleproperties.SourcePortRange = "0-65535"
$ruleproperties.DestinationPortRange = "0-65535"
$ruleproperties.Action = "Allow"
$ruleproperties.SourceAddressPrefix = "*"
$ruleproperties.DestinationAddressPrefix = "*"
$ruleproperties.Priority = "105"
$ruleproperties.Type = "Outbound"
$ruleproperties.Logging = "Enabled"

$aclrule = new-object Microsoft.Windows.NetworkController.AclRule
```

```
$aclrule.Properties = $ruleproperties
$aclrule.ResourceId = "AllowAll_Outbound"
$aclrules += $aclrule

$acllistproperties = new-object
Microsoft.Windows.NetworkController.AccessControlListProperties
$acllistproperties.AclRules = $aclrules

New-NetworkControllerAccessControlList -ResourceId "Subnet-192-168-0-0" -Properties
$acllistproperties -ConnectionUri $ncURI
```

Ajouter un groupe de sécurité réseau à une interface réseau

Une fois que vous avez créé un groupe de sécurité réseau et que vous l'avez affecté à un sous-réseau virtuel, vous pouvez remplacer ce groupe de sécurité réseau par défaut sur le sous-réseau virtuel par un groupe de sécurité réseau spécifique pour une interface réseau individuelle. À compter de Windows Server 2019 Datacenter, vous pouvez appliquer des groupes de sécurité réseau spécifiques directement aux interfaces réseau attachées aux réseaux logiques SDN, en plus des réseaux virtuels SDN. Si vous avez défini des groupes de sécurité réseau sur le sous-réseau virtuel connecté à l'interface réseau, les deux groupes de sécurité réseau sont appliqués et les groupes de sécurité réseau d'interface réseau sont hiérarchisés au-dessus des groupes de sécurité réseau de sous-réseau virtuel.

Dans cet exemple, nous montrons comment ajouter un groupe de sécurité réseau à un réseau virtuel.

> **Conseil**
>
> Il est également possible d'ajouter un groupe de sécurité réseau en même temps que vous créez l'interface réseau.

1. Obtenez ou créez l'interface réseau à laquelle vous ajouterez le groupe de sécurité réseau.

   PowerShell

   ```
   $nic = get-networkcontrollernetworkinterface -ConnectionUri $uri -ResourceId
   "MyVM_Ethernet1"
   ```

2. Obtenez ou créez le groupe de sécurité réseau que vous allez ajouter à l'interface réseau.

   PowerShell

```
$acl = get-networkcontrolleraccesscontrollist -ConnectionUri $uri -ResourceId
"AllowAllACL"
```

3. Affectez le groupe de sécurité réseau à la propriété AccessControlList de l'interface réseau.

PowerShell

```
 $nic.properties.ipconfigurations[0].properties.AccessControlList = $acl
```

4. Ajoutez l'interface réseau dans le Contrôleur de réseau.

PowerShell

```
new-networkcontrollernetworkinterface -ConnectionUri $uri -Properties
$nic.properties -ResourceId $nic.resourceid
```

Supprimer un groupe de sécurité réseau d'une interface réseau

Dans cet exemple, nous vous montrons comment supprimer un groupe de sécurité réseau d'une interface réseau. La suppression d'un groupe de sécurité réseau applique l'ensemble de règles par défaut à l'interface réseau. L'ensemble de règles par défaut autorise tout le trafic sortant, mais bloque tout le trafic entrant. Si vous souhaitez autoriser tout le trafic entrant, vous devez suivre l'exemple précédent pour ajouter un groupe de sécurité réseau qui autorise tous les trafics entrants et sortants.

1. Obtenez l'interface réseau à partir de laquelle vous allez supprimer le groupe de sécurité réseau.

PowerShell

```
$nic = get-networkcontrollernetworkinterface -ConnectionUri $uri -ResourceId
"MyVM_Ethernet1"
```

2. Attribuez $null à la propriété AccessControlList d'ipConfiguration.

PowerShell

```
$nic.properties.ipconfigurations[0].properties.AccessControlList = $null
```

3. Ajoutez l'objet d'interface réseau dans le Contrôleur de réseau.

PowerShell

```
new-networkcontrollernetworkinterface -ConnectionUri $uri -Properties
$nic.properties -ResourceId $nic.resourceid
```

Audit du pare-feu

La fonctionnalité d'audit du pare-feu du pare-feu du centre de données enregistre tout flux traité par les règles de pare-feu SDN. Tous les groupes de sécurité réseau activés pour la journalisation sont enregistrés. Les fichiers journaux doivent se trouver dans une syntaxe cohérente avec les journaux de flux Azure Network Watcher. Ces journaux peuvent être utilisés à des fins de diagnostic ou archivés en vue d'une analyse ultérieure.

Voici un exemple de script pour activer l'audit du pare-feu sur les machines hôtes. Mettez à jour les variables au début et exécutez-la sur une instance locale Azure avec le contrôleur de réseau déployé :

PowerShell

```
$logpath = "C:\test\log1"
$servers = @("sa18n22-2", "sa18n22-3", "sa18n22-4")
$uri = "https://sa18n22sdn.sa18.nttest.microsoft.com"

# Create log directories on the hosts
invoke-command -Computername $servers  {
    param(
        $Path
    )
    mkdir $path    -force
} -argumentlist $LogPath

# Set firewall auditing settings on Network Controller
$AuditProperties = new-object
Microsoft.Windows.NetworkController.AuditingSettingsProperties
$AuditProperties.OutputDirectory = $logpath
set-networkcontrolleauditingsettingsconfiguration -connectionuri $uri -properties
$AuditProperties -force  | out-null

# Enable logging on each server
$servers = get-networkcontrollerserver -connectionuri $uri
foreach ($s in $servers) {
    $s.properties.AuditingEnabled = @("Firewall")
    new-networkcontrollerserver -connectionuri $uri -resourceid $s.resourceid -
properties $s.properties -force | out-null
}
```

Une fois activé, un nouveau fichier apparaît dans le répertoire spécifié de chaque hôte environ une fois par heure. Vous devez régulièrement traiter ces fichiers et les supprimer des hôtes. La longueur du fichier actuel est nulle et il est verrouillé jusqu'à ce qu'il soit vidé à l'heure suivante :

syntax

```
PS C:\test\log1> dir

    Directory: C:\test\log1

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/19/2018   6:28 AM          17055 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL122803093.json
-a----        7/19/2018   7:28 AM           7880 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL132803173.json
-a----        7/19/2018   8:28 AM           7867 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL142803264.json
-a----        7/19/2018   9:28 AM          10949 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL152803360.json
-a----        7/19/2018   9:28 AM              0 SdnFirewallAuditing.d8b3b697-5355-
40e2-84d2-1bf2f0e0dc4a.20180719TL162803464.json
```

Ces fichiers contiennent une séquence d'événements de flux, par exemple :

syntax


```
{
    "records": [
        {
            "properties":{
                "Version":"1.0",
                "flows":[
                    {
                        "flows":[
                            {
                                "flowTuples":
["1531963580,192.122.0.22,192.122.255.255,138,138,U,I,A"],
                                "portId":"9",
                                "portName":"7290436D-0422-498A-8EB8-C6CF5115DACE"
                            }
                        ],
                        "rule":"Allow_Inbound"
                    }
                ]
            },
            "operationName":"NetworkSecurityGroupFlowEvents",
            "resourceId":"a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1",
            "time":"20180719:L012620622",
            "category":"NetworkSecurityGroupFlowEvent",
```

```
            "systemId":"d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a"
            },
```

Notez que la journalisation a lieu uniquement pour les règles dont la **journalisation** est **activée**, par exemple :

syntax

```
{
    "Tags":  null,
    "ResourceRef":  "/accessControlLists/AllowAll",
    "InstanceId":  "4a63e1a5-3264-4986-9a59-4e77a8b107fa",
    "Etag":  "W/\"1535a780-0fc8-4bba-a15a-093ecac9b88b\"",
    "ResourceMetadata":  null,
    "ResourceId":  "AllowAll",
    "Properties":  {
                        "ConfigurationState":  null,
                        "ProvisioningState":  "Succeeded",
                        "AclRules":  [
                                        {
                                            "ResourceMetadata":  null,
                                            "ResourceRef":
"/accessControlLists/AllowAll/aclRules/AllowAll_Inbound",
                                            "InstanceId":  "ba8710a8-0f01-422b-9038-
d1f2390645d7",
                                            "Etag":  "W/\"1535a780-0fc8-4bba-a15a-
093ecac9b88b\"",
                                            "ResourceId":  "AllowAll_Inbound",
                                            "Properties":  {
                                                                "Protocol":  "All",
                                                                "SourcePortRange":  "0-
65535",
                                                                "DestinationPortRange":
"0-65535",
                                                                "Action":  "Allow",
                                                                "SourceAddressPrefix":
"*",
                                                                "DestinationAddressPrefix":  "*",
                                                                "Priority":  "101",
                                                                "Description":  null,
                                                                "Type":  "Inbound",
                                                                "Logging":  "Enabled",
                                                                "ProvisioningState":
"Succeeded"
                                                            }
                                        },
                                        {
                                            "ResourceMetadata":  null,
                                            "ResourceRef":
"/accessControlLists/AllowAll/aclRules/AllowAll_Outbound",
                                            "InstanceId":  "068264c6-2186-4dbc-bbe7-
f504c6f47fa8",
```

```
                                                "Etag":  "W/\"1535a780-0fc8-4bba-a15a-
093ecac9b88b\"",
                                                "ResourceId":  "AllowAll_Outbound",
                                                "Properties":  {
                                                                    "Protocol":  "All",
                                                                    "SourcePortRange":  "0-
65535",
                                                                    "DestinationPortRange":
"0-65535",
                                                                    "Action":  "Allow",
                                                                    "SourceAddressPrefix":
"*",
                                                                    "DestinationAddressPrefix":  "*",
                                                                    "Priority":  "110",
                                                                    "Description":  null,
                                                                    "Type":  "Outbound",
                                                                    "Logging":  "Enabled",
                                                                    "ProvisioningState":
"Succeeded"
                                                                }
                                            }
                                        ],
                        "IpConfigurations":  [
                                                ],
                        "Subnets":  [
                                            {
                                                "ResourceMetadata":  null,
                                                "ResourceRef":
"/virtualNetworks/10_0_1_0/subnets/Subnet1",
                                                "InstanceId":  "00000000-0000-0000-0000-
000000000000",
                                                "Etag":  null,
                                                "ResourceId":  null,
                                                "Properties":  null
                                            }
                                        ]
                    }
}
```


Étapes suivantes

Pour plus d'informations, consultez :

- Vue d'ensemble du pare-feu du centre de données.
- Vue d'ensemble du contrôleur de réseau.
- SDN dans Azure Local et Windows Server.

Dernière mise à jour : 15/09/2026

Peering de réseau virtuel

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Le peering de réseaux virtuels vous permet de connecter deux réseaux virtuels de manière transparente. Une fois le peering établi, à des fins de connectivité, les réseaux virtuels apparaissent sous la forme d'un seul réseau.

Voici quelques-uns des avantages du peering de réseaux virtuels :

- Le trafic entre les machines virtuelles des réseaux virtuels appairés est routé via l'infrastructure principale uniquement via des adresses IP *privées* . La communication entre les réseaux virtuels ne nécessite pas l'accès à l'Internet public ou à des passerelles.
- Connexion à latence faible et haut débit entre les ressources de différents réseaux virtuels.
- Possibilité pour les ressources d'un réseau virtuel de communiquer avec celles d'un autre réseau virtuel.
- Aucun temps d'arrêt pour les ressources des réseaux virtuels au moment de la création du peering.

Exigences et contraintes

Le peering de réseaux virtuels présente quelques obligations et contraintes :

- Les réseaux virtuels appairés doivent :
  - Disposer d'espaces d'adressage IP qui ne se chevauchent pas
  - Être gérés par le même Contrôleur de réseau
- Une fois que vous avez appairé un réseau virtuel à un autre réseau virtuel, vous ne pouvez plus ajouter ou supprimer de plages d'adresses dans l'espace d'adressage.

> **Conseil**
>
> Si vous devez ajouter des plages d'adresses :
>
> 1. Supprimez le peering.
> 2. Ajoutez l'espace d'adressage.
> 3. Ajoutez à nouveau le peering.

- Dans la mesure où le peering de réseaux virtuels s'effectue entre deux réseaux virtuels, il n'existe aucune relation transitive dérivée entre les peerings. Par exemple, si vous appairez virtualNetworkA avec virtualNetworkB et virtualNetworkB avec virtualNetworkC, virtualNetworkA n'est pas appairé avec virtualNetworkC.

Connectivity

Une fois que vous avez appairé des réseaux virtuels, les ressources de l'un ou l'autre des réseaux virtuels peuvent se connecter directement aux ressources du réseau virtuel appairé.

- Le temps de réponse du réseau entre les machines virtuelles des réseaux virtuels appairés est identique à la latence au sein d'un seul réseau virtuel.
- Le débit réseau est basé sur la bande passante autorisée pour la machine virtuelle. Aucune restriction de bande passante supplémentaire n'est appliquée au sein du peering.
- Le trafic entre les machines virtuelles dans les réseaux virtuels appairés est routé directement via l'infrastructure de l'artère principale, et non via une passerelle ou l'Internet public.
- Les machines virtuelles d'un réseau virtuel peuvent accéder à l'équilibreur de charge interne du réseau virtuel appairé.

Vous pouvez appliquer des listes ACL (listes de contrôle d'accès) aux réseaux virtuels pour bloquer l'accès aux autres réseaux virtuels ou sous-réseaux, le cas échéant. Si vous ouvrez totalement la connectivité entre les réseaux virtuels appairés (option par défaut), vous pouvez appliquer des listes ACL à des sous-réseaux ou à des machines virtuelles spécifiques pour bloquer ou refuser un accès spécifique. Pour en savoir plus sur les listes ACL, consultez Utiliser des listes de contrôle d'accès (ACL) pour gérer le flux de trafic réseau du centre de données.

Chaînage de services

Vous pouvez configurer des routes définies par l'utilisateur, qui pointent vers les machines virtuelles dans les réseaux virtuels appairés en tant qu'adresses IP du tronçon suivant, pour activer le chaînage de services. Le chaînage de services vous permet de diriger le trafic d'un réseau virtuel vers une appliance virtuelle, au sein d'un réseau virtuel appairé, via les routes définies par l'utilisateur.

Vous pouvez déployer des réseaux hub-and-spoke, où le réseau virtuel hub peut héberger des composants d'infrastructure tels qu'une appliance virtuelle réseau. Tous les réseaux virtuels

Spoke sont homologués avec le réseau virtuel hub. Le trafic peut passer par les appliances virtuelles réseau du réseau virtuel hub.

L'appairage de réseaux virtuels permet de définir le tronçon suivant dans un itinéraire défini par l'utilisateur sur l'adresse IP d'une machine virtuelle du réseau virtuel appairé. Pour en découvrir plus sur les routes définies par l'utilisateur, consultez Utiliser des équipements virtuels réseau sur un réseau virtuel.

Passerelles et connectivité locale

Chaque réseau virtuel, qu'il soit appairé ou non à un autre réseau virtuel, peut toujours avoir sa propre passerelle pour se connecter à un réseau local. Quand vous appairez des réseaux virtuels, vous pouvez également configurer la passerelle du réseau virtuel appairé en tant que point de transit vers un réseau local. Dans ce cas, le réseau virtuel qui utilise une passerelle distante ne peut pas avoir sa propre passerelle. Un réseau virtuel ne peut avoir qu'une seule passerelle. Celle-ci peut être une passerelle locale ou distante (dans le réseau virtuel appairé).

Monitor

Quand vous appairez deux réseaux virtuels, vous devez configurer un peering pour chaque réseau virtuel du peering.

Vous pouvez effectuer le monitoring de l'état de la connexion du peering, qui peut correspondre à l'un des états suivants :

- **Initié:** Illustré lorsque vous créez le peering à partir du premier réseau virtuel vers le deuxième réseau virtuel.
- **Relié:** Illustré après avoir créé le peering à partir du deuxième réseau virtuel vers le premier réseau virtuel. L'état de peering du premier réseau virtuel passe de Initié à Connecté. Les deux pairs de réseau virtuel doivent être à l'état Connecté pour que le peering de réseaux virtuels réussisse.
- **Coupé:** Indiqué si un réseau virtuel se déconnecte d'un autre réseau virtuel.

[infographie des états]

Étapes suivantes

Configurer l'appairage de réseaux virtuels : dans cette procédure, vous utilisez Windows PowerShell pour rechercher le réseau logique du fournisseur HNV afin de créer deux

réseaux virtuels, chacun avec un seul sous-réseau. Vous configurez également le peering entre les deux réseaux virtuels.

Configurer le peering de réseaux virtuels

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans cette procédure, vous utilisez Windows PowerShell pour créer deux réseaux virtuels, chacun avec un seul sous-réseau. Vous configurez ensuite le peering entre les deux réseaux virtuels pour activer la connectivité entre eux.

- Étape 1. Créer le premier réseau virtuel
- Étape 2. Créer le deuxième réseau virtuel
- Étape 3. Configurer le peering du premier réseau virtuel vers le deuxième réseau virtuel
- Étape 4. Configurer le peering du deuxième réseau virtuel vers le premier réseau virtuel

> ⓘ **Important**
>
> N'oubliez pas de mettre à jour les propriétés de votre environnement.

Étape 1 : Créer le premier réseau virtuel

Au cours de cette étape, vous utilisez Windows PowerShell pour rechercher le réseau logique du fournisseur HNV afin de créer le premier réseau virtuel avec un seul sous-réseau. L'exemple de script suivant crée le réseau virtuel de Contoso avec un seul sous-réseau.

PowerShell

```
#Find the HNV Provider Logical Network

$logicalnetworks = Get-NetworkControllerLogicalNetwork -ConnectionUri $uri
foreach ($ln in $logicalnetworks) {
   if ($ln.Properties.NetworkVirtualizationEnabled -eq "True") {
      $HNVProviderLogicalNetwork = $ln
   }
}

#Create the Virtual Subnet

$vsubnet = new-object Microsoft.Windows.NetworkController.VirtualSubnet
$vsubnet.ResourceId = "Contoso"
$vsubnet.Properties = new-object
Microsoft.Windows.NetworkController.VirtualSubnetProperties
$vsubnet.Properties.AddressPrefix = "24.30.1.0/24"
```

```
$uri=”https://restserver”

#Create the Virtual Network

$vnetproperties = new-object
Microsoft.Windows.NetworkController.VirtualNetworkProperties
$vnetproperties.AddressSpace = new-object
Microsoft.Windows.NetworkController.AddressSpace
$vnetproperties.AddressSpace.AddressPrefixes = @("24.30.1.0/24")
$vnetproperties.LogicalNetwork = $HNVProviderLogicalNetwork
$vnetproperties.Subnets = @($vsubnet)
New-NetworkControllerVirtualNetwork -ResourceId "Contoso_VNet1" -ConnectionUri
$uri -Properties $vnetproperties
```

Étape 2 : Créer le deuxième réseau virtuel

Au cours de cette étape, vous créez un deuxième réseau virtuel avec un seul sous-réseau. L’exemple de script suivant crée le réseau virtuel de Woodgrove avec un seul sous-réseau.

PowerShell

```
#Create the Virtual Subnet

$vsubnet = new-object Microsoft.Windows.NetworkController.VirtualSubnet
$vsubnet.ResourceId = "Woodgrove"
$vsubnet.Properties = new-object
Microsoft.Windows.NetworkController.VirtualSubnetProperties
$vsubnet.Properties.AddressPrefix = "24.30.2.0/24"
$uri=”https://restserver”

#Create the Virtual Network

$vnetproperties = new-object
Microsoft.Windows.NetworkController.VirtualNetworkProperties
$vnetproperties.AddressSpace = new-object
Microsoft.Windows.NetworkController.AddressSpace
$vnetproperties.AddressSpace.AddressPrefixes = @("24.30.2.0/24")
$vnetproperties.LogicalNetwork = $HNVProviderLogicalNetwork
$vnetproperties.Subnets = @($vsubnet)
New-NetworkControllerVirtualNetwork -ResourceId "Woodgrove_VNet1" -ConnectionUri
$uri -Properties $vnetproperties
```

Étape 3 : Configurer l’appairage du premier réseau virtuel avec le deuxième réseau virtuel

Au cours de cette étape, vous allez configurer le peering entre le premier réseau virtuel et le deuxième réseau virtuel que vous avez créés au cours des deux étapes précédentes. L'exemple de script suivant établit le peering de réseaux virtuels de **Contoso_vnet1** à **Woodgrove_vnet1**.

PowerShell

```
$peeringProperties = New-Object
Microsoft.Windows.NetworkController.VirtualNetworkPeeringProperties
$vnet2 = Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceId
"Woodgrove_VNet1"
$peeringProperties.remoteVirtualNetwork = $vnet2

#Indicate whether communication between the two virtual networks
$peeringProperties.allowVirtualnetworkAccess = $true

#Indicates whether forwarded traffic is allowed across the vnets
$peeringProperties.allowForwardedTraffic = $true

#Indicates whether the peer virtual network can access this virtual networks
gateway
$peeringProperties.allowGatewayTransit = $false

#Indicates whether this virtual network uses peer virtual networks gateway
$peeringProperties.useRemoteGateways =$false

New-NetworkControllerVirtualNetworkPeering -ConnectionUri $uri -VirtualNetworkId
“Contoso_vnet1” -ResourceId “ContosotoWoodgrove” -Properties $peeringProperties
```

> ⓘ **Important**
>
> Après avoir créé ce peering, l'état du réseau virtuel indique **Initié**.

Étape 4 : Configurer l'appairage du second réseau virtuel avec le premier réseau virtuel

Au cours de cette étape, vous configurez le peering entre le deuxième réseau virtuel et le premier réseau virtuel que vous avez créés aux étapes 1 et 2 ci-dessus. L'exemple de script suivant établit le peering de réseaux virtuels de **Woodgrove_vnet1** à **Contoso_vnet1**.

PowerShell

```
$peeringProperties = New-Object
Microsoft.Windows.NetworkController.VirtualNetworkPeeringProperties
$vnet2=Get-NetworkControllerVirtualNetwork -ConnectionUri $uri -ResourceId
"Contoso_VNet1"
```

```
$peeringProperties.remoteVirtualNetwork = $vnet2

# Indicates whether communication between the two virtual networks is allowed
$peeringProperties.allowVirtualnetworkAccess = $true

# Indicates whether forwarded traffic will be allowed across the vnets
$peeringProperties.allowForwardedTraffic = $true

# Indicates whether the peer virtual network can access this virtual network's
gateway
$peeringProperties.allowGatewayTransit = $false

# Indicates whether this virtual network will use peer virtual network's gateway
$peeringProperties.useRemoteGateways =$false

New-NetworkControllerVirtualNetworkPeering -ConnectionUri $uri -VirtualNetworkId
“Woodgrove_vnet1” -ResourceId “WoodgrovetoContoso” -Properties $peeringProperties
```

Après avoir créé ce peering, l'état de peering des réseaux virtuels affiche **Connecté** pour les deux homologues. Désormais, les machines virtuelles d’un réseau virtuel peuvent communiquer avec les machines virtuelles du réseau virtuel appairé.

Performances de la passerelle SDN

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans Windows Server 2016, l'une des préoccupations du client était l'incapacité de la passerelle SDN à répondre aux exigences de débit des réseaux modernes. Le débit réseau des tunnels IPsec et GRE avait des limitations avec le débit de connexion unique pour la connectivité IPsec d'environ 300 Mbits/s et pour la connectivité GRE d'environ 2,5 Gbits/s.

À compter de Windows Server 2019, nous avons considérablement amélioré les performances de la passerelle réseau SDN, avec des chiffres atteignant respectivement 1,8 Go/s et 15 Go/s pour les connexions IPsec et GRE. Tout cela, avec des réductions significatives des cycles du processeur/par octet, offrant ainsi un débit ultra-hautes performances avec beaucoup moins d'utilisation du processeur.

Activer des hautes performances avec des passerelles

Pour **les connexions GRE**, une fois que vous avez déployé ou mis à niveau vers les versions de Windows Server 2019 sur les machines virtuelles de passerelle, vous remarquerez automatiquement une amélioration des performances. Aucune procédure manuelle n'est impliquée.

Pour **les connexions IPsec**, par défaut, lorsque vous créez la connexion pour vos réseaux virtuels, vous obtenez le chemin d'accès aux données windows Server 2016 et les numéros de performances. Pour activer le chemin des données Windows Server 2019, procédez comme suit :

1. Sur une machine virtuelle de passerelle SDN, accédez à **la console Services** (services.msc).
2. Recherchez le service nommé **Service de passerelle Azure** et définissez le type de démarrage sur **Automatique**.
3. Redémarrer la machine virtuelle de passerelle. Les connexions actives sur cette passerelle basculent vers une machine virtuelle de passerelle redondante.
4. Répétez les étapes précédentes sur le reste des machines virtuelles de passerelle.

Les exigences suivantes doivent être remplies pour que les connexions IPsec atteignent de hautes performances:

- Network Address Translation-Traversal (NAT-T) doit être activée sur votre passerelle locale. Lors de l'activation des connexions IPsec hautes performances, la passerelle SDN

configure une règle NAT. Vous devez donc également activer NAT-T sur votre passerelle locale.

- La passerelle locale doit autoriser les paquets UDP (User Datagram Protocol) sur les ports 500 et 4500 et les protocoles 50 et 51.

> **Conseil**
>
> Pour obtenir les meilleurs résultats en matière de performances, assurez-vous que le chiffrementTransformationConstant et authenticationTransformConstant dans les paramètres quickMode de la connexion IPsec utilise la suite de chiffrement **GCMAES256** .
>
> Pour des performances maximales, le matériel hôte de passerelle doit prendre en charge les jeux d'instructions de processeur AES-NI et PCLMULQQ. Ceux-ci sont disponibles sur n'importe quel Westmere (32nm) et versions ultérieures du processeur Intel, sauf sur les modèles où AES-NI a été désactivé. Vous pouvez consulter la documentation de votre fournisseur de matériel pour voir si le processeur prend en charge les jeux d'instructions de processeur AES-NI et PCLMULQDQ.

Voici un exemple REST de connexion IPsec avec des algorithmes de sécurité optimaux :

PowerShell

```
# NOTE: The virtual gateway must be created before creating the IPsec connection.
More details here.
# Create a new object for Tenant Network IPsec Connection
$nwConnectionProperties = New-Object
Microsoft.Windows.NetworkController.NetworkConnectionProperties

# Update the common object properties
$nwConnectionProperties.ConnectionType = "IPSec"
$nwConnectionProperties.OutboundKiloBitsPerSecond = 2000000
$nwConnectionProperties.InboundKiloBitsPerSecond = 2000000

# Update specific properties depending on the Connection Type
$nwConnectionProperties.IpSecConfiguration = New-Object
Microsoft.Windows.NetworkController.IpSecConfiguration
$nwConnectionProperties.IpSecConfiguration.AuthenticationMethod = "PSK"
$nwConnectionProperties.IpSecConfiguration.SharedSecret = "111_aaa"

$nwConnectionProperties.IpSecConfiguration.QuickMode = New-Object
Microsoft.Windows.NetworkController.QuickMode
$nwConnectionProperties.IpSecConfiguration.QuickMode.PerfectForwardSecrecy =
"PFS2048"
$nwConnectionProperties.IpSecConfiguration.QuickMode.AuthenticationTransformationC
onstant = "GCMAES256"
$nwConnectionProperties.IpSecConfiguration.QuickMode.CipherTransformationConstant
= "GCMAES256"
$nwConnectionProperties.IpSecConfiguration.QuickMode.SALifeTimeSeconds = 3600
```

```
$nwConnectionProperties.IpSecConfiguration.QuickMode.IdleDisconnectSeconds = 500
$nwConnectionProperties.IpSecConfiguration.QuickMode.SALifeTimeKiloBytes = 2000

$nwConnectionProperties.IpSecConfiguration.MainMode = New-Object
Microsoft.Windows.NetworkController.MainMode
$nwConnectionProperties.IpSecConfiguration.MainMode.DiffieHellmanGroup = "Group2"
$nwConnectionProperties.IpSecConfiguration.MainMode.IntegrityAlgorithm = "SHA256"
$nwConnectionProperties.IpSecConfiguration.MainMode.EncryptionAlgorithm = "AES256"
$nwConnectionProperties.IpSecConfiguration.MainMode.SALifeTimeSeconds = 28800
$nwConnectionProperties.IpSecConfiguration.MainMode.SALifeTimeKiloBytes = 2000

# L3 specific configuration (leave blank for IPSec)
$nwConnectionProperties.IPAddresses = @()
$nwConnectionProperties.PeerIPAddresses = @()

# Update the IPv4 Routes that are reachable over the site-to-site VPN Tunnel
$nwConnectionProperties.Routes = @()
$ipv4Route = New-Object Microsoft.Windows.NetworkController.RouteInfo
$ipv4Route.DestinationPrefix = "<<On premise subnet that must be reachable over
the VPN tunnel. Ex: 10.0.0.0/24>>"
$ipv4Route.metric = 10
$nwConnectionProperties.Routes += $ipv4Route

# Tunnel Destination (Remote Endpoint) Address
$nwConnectionProperties.DestinationIPAddress = "<<Public IP address of the On-
Premise VPN gateway. Ex: 192.168.3.4>>"

# Add the new Network Connection for the tenant. Note that the virtual gateway
must be created before creating the IPsec connection. $uri is the REST URI of your
deployment and must be in the form of “https://<REST URI>”
New-NetworkControllerVirtualGatewayNetworkConnection -ConnectionUri $uri -
VirtualGatewayId $virtualGW.ResourceId -ResourceId "Contoso_IPSecGW" -Properties
$nwConnectionProperties -Force
```

Résultats des tests

Nous avons effectué des tests de performances étendus pour les passerelles SDN dans nos laboratoires de test. Dans les tests, nous avons comparé les performances réseau de passerelle avec Windows Server 2019 dans les scénarios SDN et les scénarios non-SDN. Vous trouverez les résultats et les détails du programme d’installation des tests capturés dans l’article de blog ici .

Allocation de bande passante de la passerelle

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans Windows Server 2016, la bande passante du tunnel individuel pour IPsec, GRE et L3 était un ratio de la capacité totale de passerelle. Par conséquent, les clients fournissent la capacité de passerelle en fonction de la bande passante TCP standard qui attend cette sortie de la machine virtuelle de passerelle.

En outre, la bande passante maximale du tunnel IPsec sur la passerelle était limitée à (3/20)*Capacité de passerelle fournie par le client. Par exemple, si vous définissez la capacité de la passerelle sur 1 000 Mbits/s, la capacité du tunnel IPsec est de 150 Mbits/s. Les rapports équivalents pour les tunnels GRE et L3 sont 1/5 et 1/2, respectivement.

Bien que cela ait fonctionné pour la majorité des déploiements, le modèle de ratio fixe n'était pas approprié pour les environnements à haut débit. Même lorsque les taux de transfert de données étaient élevés (par exemple, plus de 40 Gbits/s), le débit maximal des tunnels de la passerelle SDN est plafonné en raison de facteurs internes.

Dans Windows Server 2019, pour un type de tunnel, le débit maximal est fixe. Même si votre hôte/machine virtuelle de passerelle prend en charge les cartes réseau avec un débit beaucoup plus élevé, le débit de tunnel maximal disponible est fixe. Un autre problème concerne les passerelles de surapprovisionnement arbitrairement, qui se produit lors de la fourniture d'un nombre très élevé pour la capacité de la passerelle.

Le débit maximal disponible pour différents types de tunnel est le suivant :

- IPsec = 5 Gbits/s
- GRE = 15 Gbits/s
- L3 = 5 Gbit/s

> ⓘ **Notes**
>
> Par défaut, l'allocation de bande passante IPsec utilise le comportement Windows Server 2016 décrit plus loin dans cet article. Pour obtenir un débit maximal (5 Gbits/s), procédez comme suit sur chaque machine virtuelle de passerelle :

1. Exécutez la commande suivante pour activer le service de passerelle :

```
PowerShell
Set-Service gatewayservice -StartupType Automatic -Status Running
```

2. Redémarrer la machine virtuelle de passerelle.

Calcul de la capacité de passerelle

Dans l'idéal, vous définissez la capacité de débit de passerelle sur le débit disponible pour la machine virtuelle de passerelle. Par exemple, si vous disposez d'une seule machine virtuelle de passerelle et que le débit de carte réseau hôte sous-jacente est de 25 Gbits/s, le débit de la passerelle peut également être défini sur 25 Gbits/s.

Si vous utilisez une passerelle uniquement pour les connexions IPsec, la capacité fixe maximale disponible est de 5 Gbits/s. Par exemple, si vous approvisionnez des connexions IPsec sur la passerelle, vous ne pouvez provisionner qu'une bande passante agrégée (entrante + sortante) sous la forme de 5 Gbits/s.

Si vous utilisez la passerelle pour la connectivité IPsec et GRE, vous pouvez approvisionner un débit IPsec maximal de 5 Gbits/s ou 15 Gbits/s de débit GRE maximum. Par exemple, si vous approvisionnez 2 Gbits/s de débit IPsec, vous avez 3 Gbits/s de débit IPsec à provisionner sur la passerelle ou 9 Gbits/s de débit GRE gauche.

Pour mettre cela en termes plus mathématiques :

- Capacité totale de la passerelle = 25 Gbits/s
- Capacité totale IPsec disponible = 5 Gbits/s (fixe)
- Capacité totale GRE disponible = 15 Gbits/s (fixe)
- Ratio de débit IPsec pour cette passerelle = 25/5 = 5 Gbits/s
- Taux de débit GRE pour cette passerelle = 25/15 = 5/3 Gbits/s

Par exemple, si vous allouez 2 Gbits/s de débit IPsec à un client :

Capacité disponible restante sur la passerelle = Capacité totale de la passerelle – Ratio de débit IPsec*Débit IPsec alloué (capacité utilisée)

25–5*2 = 15 Gbit/s

Débit IPsec restant que vous pouvez allouer sur la passerelle

5-2 = 3 Gbits/s

Débit GRE restant que vous pouvez allouer sur la passerelle = Capacité restante du ratio de débit de passerelle/GRE

15*3/5 = 9 Gbits/s

Le ratio de débit varie selon la capacité totale de la passerelle. Une chose à noter est que vous devez définir la capacité totale sur la bande passante TCP disponible pour la machine virtuelle de passerelle. Si vous avez plusieurs machines virtuelles hébergées sur la passerelle, vous devez ajuster la capacité totale de la passerelle en conséquence.

En outre, si la capacité de passerelle est inférieure à la capacité totale du tunnel disponible, la capacité totale du tunnel disponible est définie sur la capacité de passerelle. Par exemple, si vous définissez la capacité de passerelle sur 4 Gbits/s, la capacité totale disponible pour IPsec, L3 et GRE est définie sur 4 Gbits/s, ce qui laisse le ratio de débit pour chaque tunnel à 1 Gbit/s.

Comportement Windows Server 2016

L'algorithme de calcul de capacité de passerelle pour Windows Server 2016 reste inchangé. Dans Windows Server 2016, la bande passante maximale du tunnel IPsec était limitée à la capacité de passerelle (3/20)*sur une passerelle. Les rapports équivalents pour les tunnels GRE et L3 étaient 1/5 et 1/2, respectivement.

Si vous effectuez une mise à niveau de Windows Server 2016 vers Windows Server 2019 :

1. **Tunnels GRE et L3 :** la logique d'allocation Windows Server 2019 prend effet une fois que les nœuds du contrôleur de réseau sont mis à jour vers Windows Server 2019
2. **Tunnels IPSec :** La logique d'allocation de passerelle Windows Server 2016 continue de fonctionner jusqu'à ce que toutes les passerelles du pool de passerelles sont mises à niveau vers Windows Server 2019. Pour toutes les passerelles du pool de passerelles, vous devez définir le service de passerelle Azure sur **Automatique**.

> ⓘ **Notes**
>
> Il est possible qu'après la mise à niveau vers Windows Server 2019, une passerelle devienne surprovisionnée (car la logique d'allocation passe de Windows Server 2016 à Windows Server 2019). Dans ce cas, les connexions existantes sur la passerelle continuent d'exister. La ressource REST pour la passerelle lève un avertissement indiquant que la

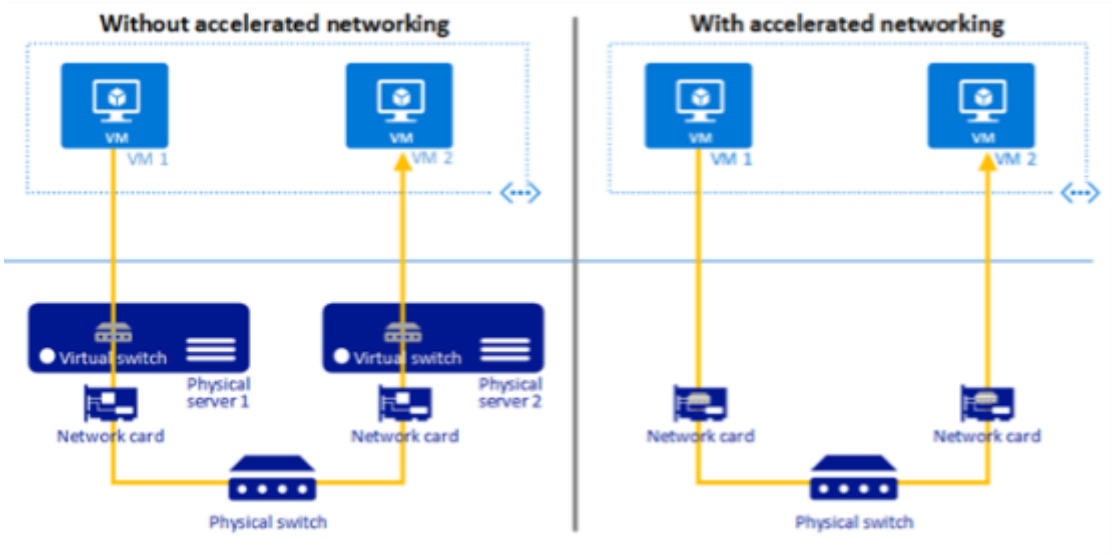
passerelle est surprovisionnée. Dans ce cas, vous devez déplacer certaines connexions vers une autre passerelle.

Mise en réseau accélérée

S'applique à: ✅ Windows Server 2025

Les performances réseau accélérées permettent la virtualisation d'entrée-sortie (E/S) en racine unique (SR-IOV) sur les types de machines virtuelles prises en charge, ce qui améliore considérablement les performances réseau. Les performances réseau accélérées permettent au trafic réseau de contourner la couche commutateur logicielle des piles de virtualisation Hyper-V. Étant donné que les performances réseau accélérées affectent la fonction virtuelle (VF) à une partition enfant, le trafic réseau circule directement entre la VF et la partition enfant. Par conséquent, la surcharge d'E/S dans la couche d'émulation logicielle diminue jusqu'à ce que les performances réseau deviennent presque équivalentes aux environnements physiques locaux. Les deux serveurs uniques qui ne sont pas cluster et Windows Server Standard edition ne prennent pas en charge la mise en réseau accélérée.

Le diagramme suivant illustre la façon dont deux machines virtuelles communiquent avec et sans performances réseau accélérées.



Le chemin de données haute performance des performances réseau accélérées permet la virtualisation d'E/S d'une racine unique (SR-IOV) sur les types de machines virtuelles prises en charge, ce qui améliore considérablement les performances réseau de la manière suivante :

- Une latence plus faible et un plus grand nombre de paquets par seconde (pps)
- Gigue réduite
- Utilisation réduite du processeur

Les performances réseau accélérées ajoutent également une couche de gestion supplémentaire avec les fonctionnalités suivantes :

- Vérifications préalables intégrées qui vous permettent de savoir si votre déploiement est compatible avec les performances réseau accélérées en vérifiant la prise en charge de la SR-IOV, la version du système d'exploitation, l'état d'hyperthreading, et ainsi de suite.
- La configuration de l'hôte garantit que la SR-IOV est activée sur les charges de travail de machine virtuelle d'hébergement vSwitch correctes, et vous permet également de configurer des nœuds de réserve pour les scénarios de basculement et d'éviter le surabonnement des ressources.
- Paramètres de performances de machine virtuelle simplifiés qui montrent les performances globales avec une échelle faibles, moyennes et élevées pour faciliter la configuration.

Ces fonctionnalités rendent la mise en réseau accélérée utile pour les environnements qui nécessitent un calcul haute performance (HPC). Il est idéal pour les tâches de calcul intensives et les applications en temps réel telles que les plateformes de négociation financière. En outre, il bénéficie aux déploiements qui utilisent la virtualisation de fonction réseau (NFV) pour contourner les limites du débit réseau.

Prerequisites

Votre déploiement doit répondre aux conditions préalables suivantes pour utiliser la mise en réseau accélérée :

- Vous devez configurer un cluster fonctionnel exécutant l'édition Windows Server 2025 Datacenter.
- Vous devez installer la fonctionnalité **Network ATC** . Pour plus d'informations, consultez Installer ou désinstaller des rôles, des services de rôle ou des fonctionnalités et configurer une intention de calcul valide avant d'activer la mise en réseau accélérée.

  Vous pouvez également exécuter la commande suivante pour installer cette fonctionnalité :

  PowerShell
  ```
  Install-WindowsFeature -Name NetworkATC
  ```

- Votre carte d'interface réseau doit prendre en charge SR-IOV et SR-IOV activées dans le BIOS. Vous devrez peut-être contacter votre fournisseur de matériel pour voir si votre machine prend en charge SR-IOV. Exécutez l'applet de commande suivante pour activer SR-IOV sur votre carte réseau :

PowerShell

```
Enable-NetAdapterSriov
```

- La virtualisation doit être activée dans le BIOS. Passez en revue le guide du fournisseur de matériel sur la définition de cette fonctionnalité.
- Vous devez utiliser un abonnement Windows Server paiement à l'utilisation ou des types de licence Software Assurance .

Configurer la mise en réseau accélérée

Pour configurer la mise en réseau accélérée sur votre appareil, vous pouvez le faire à l'aide d'une fenêtre PowerShell avec élévation de privilèges ou via windows Admin Center.

PowerShell

Exécutez l'applet de commande suivante pour vous assurer que votre système répond à toutes les conditions préalables requises :

PowerShell

```
Get-AccelNetManagementPreReq
```

Exécutez la commande suivante pour activer la mise en réseau accélérée sur un cluster :

PowerShell

```
Enable-AccelNetManagement -IntentName "MyIntent" -NodeReservePercentage
```

Le paramètre `-IntentName` est obligatoire. Si vous laissez la `NodeReservePercentage` valeur vide, le système a la valeur **par défaut 50%**. Cette valeur doit être un entier supérieur ou égal à **0** et inférieur ou égal à **99**.

Exécutez la commande suivante pour activer la mise en réseau accélérée sur une machine virtuelle définie sur des performances élevées :

PowerShell

```
Enable-AccelNetVM -VMName "MyVM" -Performance High
```

Pour activer les performances réseau accélérées pour plusieurs machines virtuelles à exécuter en faible performance, exécutez la commande suivante :

PowerShell

```
Get-VM -VMName "MyVM01, MyVM02" | Enable-AccelNetVM -Performance Low
```

Les paramètres `-VMName` et `-Performance` sont obligatoires. Vous pouvez définir la valeur de performances sur Faibles, Moyennes ou Élevées. Les options de performances ont des exigences minimales en matière de processeurs virtuels en fonction de l'état d'hyperthreading, comme indiqué dans le tableau suivant :

Développer le tableau

Configuration d'Hyperthreading	Paramètre de performances	Nombre minimal de processeurs virtuels requis
Disabled	Low	2
Disabled	Medium	2
Disabled	High	4
Enabled	Low	4
Enabled	Medium	4
Enabled	High	4

Exécutez l'applet de commande suivante pour désactiver la mise en réseau accélérée sur un cluster :

PowerShell

```
Disable-AccelNetManagement
```

Après avoir désactivé les performances réseau accélérées sur le cluster, l'HUD réseau ne contrôle plus l'intégrité de la fonctionnalité.

> **Note**
>
> La désactivation de la mise en réseau accélérée au niveau du cluster ne modifie pas les paramètres sur des machines virtuelles individuelles. L'HUD réseau arrête la surveillance de ces machines virtuelles, et la mise en réseau accélérée cesse de les gérer.

Exécutez la commande suivante pour désactiver la mise en réseau accélérée sur une machine virtuelle :

PowerShell

```
Disable-AccelNetVM -VMName "MyVM"
```

Pour désactiver les performances réseau accélérées pour plusieurs machines virtuelles, exécutez la commande suivante :

PowerShell

```
Get-VM -VMName "MyVM01, MyVM02" | Disable-AccelNetVM
```

Pour configurer la mise en réseau accélérée sur un cluster, accédez à votre nœud et exécutez la commande suivante avec les valeurs de la nouvelle intention et de la réserve de nœud :

PowerShell

```
Set-AccelNetManagement -IntentName "MyIntent" -NodeReservePercentage
```

Exécutez la commande suivante pour configurer votre machine virtuelle pour qu'elle s'exécute en performances moyennes :

PowerShell

```
Set-AccelNetManagement -VMName "MyVM" -Performance Medium
```

Pour en savoir plus sur les applets de commande PowerShell de mise en réseau accélérée, consultez le jeu de modules FailoverClusters .

Erreurs PowerShell connues

Vous pouvez rencontrer les messages d'erreur suivants lors de l'utilisation de cette fonctionnalité.

Développer le tableau

Erreur	Descriptif	Résolution
`Accel_net_not_supported`	`Node {0} does not support Accelerated Networking. Windows Server 2025 or later is required.`	Votre appareil doit exécuter la dernière version de Windows Server 2025.

Erreur	Descriptif	Résolution
`cannot_provision_performance`	`Cannot provision {0} on this system.`	Sélectionnez une autre option de performances ou mettez à jour vos cartes réseau.
`cluster_not_enough_resources`	`The cluster does not have enough SRIOV resources to enable VM {0}.`	Réduisez la valeur **NodeReservePercentage** , sélectionnez une autre option de performances ou augmentez le nombre de ressources SRIOV dans votre cluster.
`enable_accel_net_failed`	`Failed to enable Accelerated Networking on the cluster {0}.`	Vérifiez que vous utilisez une licence d'abonnement paiement à l'utilisation valide.
`Get_network_adapter_failed`	`Failed to get network adapters for VM {0}.`	Vérifiez que la machine virtuelle possède au moins une carte réseau.
`ht_enabled_min_processor_counter`	`The minimum required processor count for requested performance with hyperthreading enabled/disabled is {0}.`	Pour répondre aux exigences, ajoutez d'autres processeurs virtuels à votre machine virtuelle.
`Hyperthreading_check_failed`	`Hyperthreading validation: Failed. There is an inconsistency across the cluster. Either disable or enable hyperthreading on all nodes.`	Vérifiez que la configuration de l'hyperthreading est cohérente pour chaque nœud de votre cluster.
`Intent_not_found`	`Intent validation: Failed. Intent {0} not found.`	Vérifiez que le nom de l'intention que vous avez entré est correct, puis réessayez.
`Intent_type_check_failed`	`The selected intent {0} does not have Compute capabilities.`	Créez ou mettez à jour une intention avec l'état de calcul.
`Sriov_support_MissingAcs`	`Adapter {0} cannot be enabled for Accelerated Networking because it is in a PCIe slot that does not support Access Control Services (ACS).`	Essayez de déplacer l'appareil vers un autre emplacement PCIe ou contactez votre fournisseur de matériel.
`Sriov_support_MissingPfDriver`	`Adapter {0} cannot be enabled for Accelerated`	Vérifiez que les pilotes sont mis à jour.

Erreur	Descriptif	Résolution
	`Networking because the device driver does not support SR-IOV.`	
`Sriov_support_NoBusResources`	`Adapter {0} cannot be enabled for Accelerated Networking because there are not enough PCI Express bus numbers available.`	Ajustez la vitesse de bus PCI Express dans les paramètres DU BIOS ou ajoutez une carte d'extension qui prend en charge davantage d'emplacements PCI Express.
`Sriov_support_Unknown`	`Adapter {0} cannot be enabled for Accelerated Networking because it is not advertising SR-IOV Support.`	Assurez-vous que le matériel de l'ordinateur peut prendre en charge SR-IOV et que vous avez activé la virtualisation des E/S dans le BIOS.
`vm_not_enough_vcpus`	`VM {0} does not have enough vCPUs to enable Accelerated Networking with the specified performance.`	Augmentez le montant du processeur virtuel pour votre machine virtuelle.

Voir aussi

- Vue d'ensemble deHyper-V
- Qu'est-ce que les serveurs avec Azure Arc ?
- Mise en réseau haute performance (HPN)

Last updated on 17/11/2025

Protocole EAP (Extensible Authentication Protocol) pour l'accès réseau

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10

Le protocole EAP (Extensible Authentication Protocol) est un cadre d'authentification qui permet l'utilisation de différentes méthodes d'authentification pour les technologies d'accès réseau sécurisées. Parmi les exemples de ces technologies, citons l'accès sans fil à l'aide de la norme IEEE 802.1X, l'accès câblé avec la norme IEEE 802.1X et les connexions PPP (Point-to-Point Protocol) comme le réseau privé virtuel (VPN). Le protocole EAP n'est pas une méthode d'authentification spécifique comme MS-CHAP v2. Il s'agit davantage d'un cadre qui permet aux fournisseurs de mise en réseau de développer et d'installer de nouvelles méthodes d'authentification, connues sous le nom de « méthodes EAP » sur le client d'accès et sur le serveur d'authentification. L'infrastructure EAP est initialement définie par RFC 3748 et étendue par d'autres RFC et normes.

Méthodes d'authentification

Les méthodes d'authentification EAP utilisées dans les méthodes EAP tunnelées sont couramment appelées **méthodes internes** ou **types EAP**. Les méthodes configurées comme **méthodes internes** ont les mêmes paramètres de configuration que ceux utilisés comme méthode externe. Cet article contient des informations de configuration propres aux méthodes d'authentification suivantes dans le protocole EAP.

EAP-TLS : méthode EAP basée sur des normes, utilisant TLS avec des certificats pour l'authentification mutuelle. Apparaît comme **Carte à puce ou autre certificat (EAP-TLS)** dans Windows. EAP-TLS pouvez être déployé en tant que **méthode interne** pour une autre méthode EAP ou en tant que méthode EAP autonome.

> **Conseil**
>
> Comme elles reposent sur des certificats, les méthodes EAP qui utilisent EAP-TLS offrent généralement le niveau de sécurité le plus élevé. Par exemple, EAP-TLS est la seule méthode EAP autorisée pour le mode WPA3-Enterprise 192 bits.

EAP-MSCHAP v2 (EAP-Microsoft Challenge Handshake Authentication Protocol version 2) : méthode EAP définie par Microsoft qui encapsule le protocole d'authentification MSCHAP v2, utilisant le nom d'utilisateur et un mot de passe pour l'authentification. Apparaît

comme **Mot de passe sécurisé (EAP-MSCHAP v2)** dans Windows. EAP-MSCHAPv2 pouvez être utilisé comme méthode autonome pour VPN, mais uniquement comme **méthode interne** pour les connexions câblées/sans fil.

> ⚠ **Avertissement**
>
> Les connexions MSCHAPv2 peuvent faire l'objet d'attaques similaires à celles dont fait l'objet NTLMv1. Windows 11 Entreprise version 22H2 (build 22621) active **Windows Defender Credential Guard**, ce qui peut engendrer des problèmes avec les connexions MSCHAPv2.

PEAP (Protected EAP) : méthode EAP définie par Microsoft qui encapsule EAP dans un tunnel TLS. Le tunnel TLS sécurise la méthode EAP interne, qui pourrait autrement ne pas être protégée. Windows prend en charge EAP-TLS et EAP-MSCHAP v2 comme méthodes internes.

EAP-TTLS (EAP-Tunneled Transport Layer Security) : décrite par le document RFC 5281, cette méthode encapsule une session TLS qui effectue une authentification mutuelle à l'aide d'un autre mécanisme d'authentification interne. Cette méthode interne peut être un protocole EAP comme EAP-MSCHAP v2 ou un protocole non EAP comme le protocole PAP (Password Authentication Protocol). Dans Windows Server 2012, l'inclusion d'EAP-TTLS assure une prise en charge côté client uniquement (dans Windows 8). NPS ne prend pas en charge EAP-TTLS pour le moment. La prise en charge du client permet l'interopérabilité avec les serveurs RADIUS couramment déployés, compatibles avec EAP-TTLS.

EAP-SIM (EAP-Subscriber Identity Module), EAP-AKA (EAP-Authentication and Key Agreement) et EAP-AKA' (EAP-AKA Prime) : décrite par différents documents RFC, cette méthode active l'authentification à l'aide de cartes SIM et est implémentée quand un client achète un forfait de service haut débit sans fil auprès d'un opérateur de réseau mobile. Dans le cadre du plan, le client reçoit généralement un profil sans fil qui est préconfiguré pour l'authentification SIM.

TEAP (Tunnel EAP) : décrite par le document RFC 7170, cette méthode EAP tunnelisée établit un tunnel TLS sécurisé et y exécute d'autres méthodes EAP. Prend en charge le chaînage EAP, en authentifiant l'ordinateur et l'utilisateur au sein d'une seule session d'authentification. Dans Windows Server 2022, l'inclusion de TEAP assure une prise en charge de Windows 10 version 2004 (build 19041) côté client uniquement. NPS ne prend pas en charge TEAP pour le moment. La prise en charge du client permet l'interopérabilité avec les serveurs RADIUS couramment déployés, compatibles avec TEAP. Windows prend en charge EAP-TLS et EAP-MSCHAP v2 comme méthodes internes.

Le tableau suivant répertorie certaines méthodes EAP courantes et les numéros de type de méthode que l'IANA leur a attribués.

Agrandir le tableau

Méthode EAP	Numéro de type attribué à IANA	Prise en charge Windows en natif
MD5-Challenge (EAP-MD5)	4	❌
Mot de passe à usage unique (EAP-OTP)	5	❌
Carte de jeton générique (EAP-GTC)	6	❌
EAP-TLS	13	✅
EAP-SIM	18	✅
EAP-TTLS	21	✅
EAP-AKA	23	✅
PEAP	25	✅
EAP-MSCHAP v2	26	✅
Mot de passe protégé à usage unique (EAP-POTP)	32	❌
EAP-FAST	43	❌
Clé prépartagée (EAP-PSK)	47	❌
EAP-IKEv2	49	❌
EAP-AKA'	50	✅
EAP-EKE	53	❌
TEAP	55	✅
EAP-NOOB	56	❌

Configuration des propriétés EAP

Vous pouvez accéder aux propriétés EAP pour un accès câblé et sans fil authentifié 802.1X de différentes façons :

- En configurant les extensions Stratégies de réseau câblé (IEEE 802.3) et Stratégies de réseau sans fil (IEEE 802.11) dans la stratégie de groupe.
  - **Configuration de l'ordinateur**>**Manifeste**>**Paramètres**> Windows**Paramètres de sécurité**

- Utilisation de logiciels de gestion des appareils mobiles (GPM), comme Intune (wi-fi/câblé)
  - fournisseur de solutions cloudWi-Fi
  - WiredNetwork CSP
- En configurant manuellement les connexions câblées ou sans fil sur les ordinateurs clients.

Vous pouvez accéder aux propriétés EAP pour les connexions réseau privé virtuel (VPN) de différentes façons :

- Utilisation de logiciels de gestion des appareils mobiles (GPM), comme Intune
  - VPNv2 CSP
  - Options de profil VPN
- En configurant manuellement les connexions VPN sur les ordinateurs clients.
- En utilisant le Kit d'administration Gestionnaire des connexions (CMAK) pour configurer les connexions VPN.

Pour plus d'informations sur la configuration des propriétés EAP, consultez Configurer des profils et des paramètres EAP dans Windows.

Profils XML pour EAP

Les profils utilisés pour les différents types de connexions sont des fichiers XML contenant les options de configuration de cette connexion. Chaque type de connexion distinct suit un schéma spécifique :

- Profils Wi-Fi (WLAN)
- Profils de réseau câblé (Ethernet)
- Profils VPN

Toutefois, lorsqu'il est configuré pour utiliser EAP, chaque schéma de profil a un élément EapHostConfig enfant.

- Filaire/sans fil : `EapHostConfig` est un élément enfant de l'élément EAPConfig . **MSM** > **sécurité** (Câblé/Sans fil) >OneX> **EAPConfig**
- VPN : `EapHostConfig` est un élément enfant de **NativeProfile** > **Authentification** > **Eap** > **Configuration**

Cette syntaxe de configuration est définie dans la spécification Stratégie de groupe : extension de protocole sans fil/câblé.

> ⓘ **Notes**

Les différentes interfaces utilisateur graphiques ne présentent pas toujours toutes les options techniquement possibles. Par exemple, Windows Server 2019 (et les versions antérieures) ne permet pas de configurer TEAP dans l'interface utilisateur. Toutefois, il est souvent possible d'importer un profil XML existant, qui a déjà été configuré.

Le reste de cet article a pour but d'établir une corrélation entre les parties spécifiques à EAP de l'interface utilisateur Stratégie de groupe/Panneau de configuration et les options de configuration XML, et de fournir une description du paramètre.

Vous trouverez plus d'informations sur la configuration des profils XML dans les profils XML. Pour obtenir un exemple d'utilisation d'un profil XML contenant des paramètres EAP, consultez Provisionner un profil Wi-Fi via un site web.

Paramètres de sécurité

Le tableau suivant explique les paramètres de sécurité configurables pour un profil qui utilise 802.1X. Ces paramètres sont mappés à OneX.

Agrandir le tableau

Setting	XML element	Description
Sélectionner une méthode d'authentification réseau :	EAPConfig	Permet de sélectionner la méthode EAP à utiliser pour l'authentification. Consultez Paramètres de configuration de la méthode d'authentification et Paramètres de configuration de l'authentification cellulaire
Properties		Ouvre la boîte de dialogue Propriétés correspondant à la méthode EAP sélectionnée.
Mode d'authentification	authMode	Spécifie le type d'informations d'identification utilisées pour l'authentification. Les valeurs suivantes sont prises en charge : 1. Authentification de l'utilisateur ou de l'ordinateur 2. Authentification de l'ordinateur 3. Authentification de l'utilisateur 4. Authentification de l'invité Dans ce contexte, « Ordinateur » est désigné par « Machine » dans d'autres références. `machineOrUser` est la valeur par défaut dans Windows.

Setting	XML element	Description
Nbre max. d'échecs d'authentification	maxAuthFailures	Spécifie le nombre maximal d'échecs d'authentification autorisés pour un ensemble d'informations d'identification, avec `1` comme valeur par défaut.
Mettre en cache les informations de l'utilisateur pour les connexions ultérieures à ce réseau	cacheUserData	Spécifie si les informations d'identification de l'utilisateur doivent être mises en cache pour les connexions ultérieures au même réseau, avec `true` comme valeur par défaut.

Paramètres de sécurité avancés et IEEE 802.1X

Si la case **Appliquer les paramètres avancés 802.1X** est cochée, tous les paramètres suivants seront configurés. Si elle n'est pas cochée, les paramètres par défaut s'appliquent. Au format XML, tous les éléments sont facultatifs. Les valeurs par défaut sont utilisées si ces éléments ne sont pas spécifiés.

Agrandir le tableau

Setting	XML element	Description
Nbre max. de messages Eapol-Start	maxStart	Spécifie le nombre maximal de messages EAPOL-Start pouvant être envoyés à l'authentificateur (serveur RADIUS) avant que le demandeur (client Windows) suppose qu'aucun authentificateur n'est présent, avec `3` comme valeur par défaut.
Période de démarrage (s)	startPeriod	Spécifie le temps d'attente (en secondes) avant l'envoi d'un message EAPOL-Start pour démarrer le processus d'authentification 802.1X, avec `5` comme valeur par défaut.
Période de maintien (s)	heldPeriod	Spécifie le temps d'attente (en secondes) après l'échec d'une tentative d'authentification pour réessayer l'authentification, avec `1` comme valeur par défaut.
Période d'authentification (s)	authPeriod	Spécifie le temps d'attente (en secondes) d'une réponse de l'authentificateur (serveur RADIUS) avant de supposer qu'aucun authentificateur n'est présent, avec `18` comme valeur par défaut.
message Eapol-Start	supplicantMode	Spécifie la méthode de transmission utilisée pour les messages EAPOL-Start. Les valeurs suivantes sont prises en charge : 1. Ne pas transmettre (`inhibitTransmission`) 2. Transmettre (`includeLearning`) 3. Transmettre via IEEE 802.1X (`compliant`)

Setting	XML element	Description
		Dans ce contexte, « Ordinateur » est désigné par « Machine » dans d'autres références. `compliant` est la valeur par défaut dans Windows et est la seule option valide pour les profils sans fil.

Paramètres de sécurité avancés et authentification unique

Le tableau suivant explique les paramètres d'authentification unique (SSO), anciennement appelée PLAP (Pre-Logon Access Provider).

Agrandir le tableau

Setting	XML element	Description
Activer l'authentification unique pour ce réseau	singleSignOn	Spécifie si l'authentification unique est activée pour ce réseau, avec `false` comme valeur par défaut. N'utilisez pas `singleSignOn` dans un profil si le réseau n'en a pas besoin.
Immédiatement avant l'ouverture de session de l'utilisateur Immédiatement après l'ouverture de session de l'utilisateur	type	Spécifie si l'authentification unique doit être effectuée avant ou après l'ouverture de session de l'utilisateur.
Délai maximal pour la connectivité (secondes)	maxDelay	Spécifie le délai maximal (en secondes) avant l'échec de la tentative d'authentification unique, avec `10` comme valeur par défaut.
Autoriser l'affichage de boîtes de dialogue supplémentaires lors de l'authentification unique	allowAdditionalDialogs	Spécifie si l'affichage des boîtes de dialogue EAP doit être autorisé pendant l'authentification unique, avec `false` comme valeur par défaut.
Ce réseau utilise différents VLAN pour gérer l'authentification via des informations d'identification utilisateur et ordinateur	userBasedVirtualLan	Spécifie si le réseau local virtuel (VLAN) utilisé par l'appareil change en fonction des informations d'identification de l'utilisateur, avec `false` comme valeur par défaut.

Paramètres de configuration de la méthode d'authentification

> **Attention**
>
> Un serveur d'accès réseau configuré pour autoriser le même type de méthode d'authentification pour une méthode EAP tunnelisée (par exemple, PEAP) et une méthode EAP non tunnelisée (par exemple, EAP-MSCHAP v2) peut donner lieu à une faille de sécurité potentielle. Quand vous déployez une méthode EAP tunnelisée et EAP (qui n'offre pas de protection), n'utilisez pas le même type d'authentification. Par exemple, si vous déployez PEAP-TLS, ne déployez pas également EAP-TLS, car si vous avez besoin de la protection du tunnel, cela ne sert à rien d'autoriser l'exécution de la méthode en dehors du tunnel.

Le tableau suivant décrit les paramètres configurables pour chaque méthode d'authentification.

EAP-TLS

Les paramètres EAP-TLS de l'interface utilisateur sont mappés à EapTlsConnectionPropertiesV1, qui est étendu par EapTlsConnectionPropertiesV2 et EapTlsConnectionPropertiesV3.

Agrandir le tableau

Setting	XML element	Description
Utiliser ma carte à puce	CredentialsSource>Carte à puce	Spécifie que les clients effectuant des demandes d'authentification doivent présenter un certificat de carte à puce pour l'authentification réseau.
Utiliser un certificat sur cet ordinateur	CredentialsSource>CertificateStore	Spécifie que les clients doivent, pour s'authentifier, utiliser un certificat qui se trouve dans le magasin de certificats Utilisateur actuel ou Ordinateur local.
Utiliser la sélection de certificat simple (recommandé)	SimpleCertSelection	Spécifie si Windows sélectionnera automatiquement un certificat pour l'authentification sans interaction de l'utilisateur (dans la mesure du possible) ou si Windows affichera une liste déroulante permettant à l'utilisateur de sélectionner un certificat.
Advanced		Ouvre la boîte de dialogue Configurer la sélection des certificats.
Options de validation du		

Setting	XML element	Description
serveur		
Utiliser un nom d'utilisateur différent pour la connexion	DifferentUsername	Spécifie s'il faut utiliser un nom d'utilisateur pour l'authentification qui est différent d'un nom d'utilisateur du certificat.

Le tableau suivant répertorie les paramètres permettant de **configurer la sélection du certificat**. Ces paramètres définissent les critères qu'un client utilise pour sélectionner le certificat approprié pour l'authentification. Cette interface utilisateur est mappée à TLSExtensions>FilteringInfo.

Agrandir le tableau

Setting	XML element	Description
Émetteur de certificat	**CAHashList** `Enabled="true"`	Spécifie si le filtrage Émetteur de certificat est activé. Si **l'émetteur de certificat** et **l'utilisation de clé étendue (EKU)** sont activés, seuls les certificats qui répondent aux deux conditions sont considérés comme valides pour l'authentification du client auprès du serveur.
Autorités de certification racine	**IssuerHash**	Répertorie les noms de tous les émetteurs pour lesquels les certificats d'autorité de certification correspondants sont présents dans le magasin de certificats **Autorités de certification racines de confiance** ou **Autorités de certification intermédiaires** du compte d'ordinateur local. Cela inclut les éléments suivants : • Toutes les autorités de certification racines et toutes les autorités de certification intermédiaires. • Contient uniquement les émetteurs pour lesquels des certificats valides correspondants sont présents sur l'ordinateur (par exemple, des certificats qui n'ont pas expiré ou qui n'ont pas été révoqués). • La liste finale des certificats qui sont autorisés pour l'authentification contient

Setting	XML element	Description
		uniquement les certificats qui ont été émis par l'un des émetteurs sélectionnés dans cette liste. En XML, il s'agit de l'empreinte SHA-1 (hash) du certificat.
Utilisation améliorée de la clé		Vous permet de sélectionner **Tous les objectifs**, **l'authentification du client**, **AnyPurpose** ou toute combinaison de celles-ci. Spécifie que lorsqu'une combinaison est sélectionnée, tous les certificats remplissant au moins une des trois conditions sont considérés comme valides pour l'authentification du client auprès du serveur. Si le filtrage basé sur l'utilisation améliorée de la clé est activé, l'une des options doit être sélectionnée. Sinon, la case **Utilisation améliorée de la clé** sera décochée.
Tout objectif	**AllPurposeEnabled**	Lorsque cette option est sélectionnée, cet élément spécifie que les certificats ayant la référence EKU **à usage unique** sont considérés comme des certificats valides pour l'authentification du client auprès du serveur. L'identificateur d'objet (OID) à **tous les fins** est `0` ou vide.
Authentification du client	**ClientAuthEKUList** `Enabled="true"` (> **EKUMapInList** > **EKUName**)	Spécifie que les certificats ayant la référence EKU **d'authentification client** et la liste spécifiée des EKU sont considérés comme des certificats valides pour l'authentification du client auprès du serveur. L'identificateur d'objet (OID) pour **l'authentification du client** est `1.3.6.1.5.5.7.3.2`.
AnyPurpose	**AnyPurposeEKUList** `Enabled="true"` (> **EKUMapInList** > **EKUName**)	Spécifie que tous les certificats ayant une référence EKU **AnyPurpose** et la liste spécifiée des EKU sont considérés comme des certificats valides pour l'authentification du client auprès du serveur. L'identificateur d'objet (OID) pour **AnyPurpose** est `1.3.6.1.4.1.311.10.12.1`.

Setting	XML element	Description
Add	EKUMapping > EKUMap > EKUName/EKUOID	Ouvre la boîte de dialogue **Sélectionner des EKU** , qui vous permet d'ajouter des EKU standard, personnalisées ou spécifiques au fournisseur à la liste **Authentification client** ou **AnyPurpose** . La sélection de **l'option Ajouter** ou **modifier** dans la boîte de dialogue **Sélectionner des EKUs** ouvre la boîte de dialogue **Ajouter/Modifier la référence EKU** , qui fournit deux options : 1. **Entrer le nom de l'utilisation améliorée de la clé** : fournit un emplacement où saisir le nom de l'utilisation améliorée de la clé personnalisée. 2. **Entrer l'OID de l'utilisation améliorée de la clé** : fournit un emplacement où saisir l'OID de l'utilisation améliorée de la clé. Seuls les chiffres, les séparateurs et `.` sont autorisés. Les caractères génériques sont autorisés ; dans ce cas, tous les OID enfants dans la hiérarchie sont autorisés. Par exemple, l'entrée `1.3.6.1.4.1.311.*` autorise `1.3.6.1.4.1.311.42` et `1.3.6.1.4.1.311.42.2.1`.
Edit		Permet de modifier les utilisations améliorées de la clé personnalisées que vous avez ajoutées. Les utilisations améliorées de la clé prédéfinies par défaut ne peuvent pas être modifiées.
Remove		Supprime la référence EKU sélectionnée de la liste **Authentification client** ou **AnyPurpose** .

Validation du certificat de serveur

De nombreuses méthodes EAP incluent une option permettant au client de valider le certificat du serveur. Si le certificat du serveur n'est pas validé, le client ne pourra pas s'assurer qu'il communique avec le bon serveur. Cela expose le client à des risques de sécurité, notamment à la possibilité qu'il se connecte sans le savoir à un réseau non autorisé.

> **Notes**
>
> Windows nécessite que le certificat de serveur dispose de la référence EKU **d'authentification du serveur** . L'identificateur d'objet (OID) pour cette utilisation améliorée de la clé est `1.3.6.1.5.5.7.3.1`.

Le tableau suivant répertorie les options de validation du serveur applicables à chaque méthode EAP. Windows 11 a mis à jour la logique de validation du serveur afin d'en améliorer la cohérence. Pour plus d'informations, consultez Comportement de validation du certificat de serveur mis à jour dans Windows 11. En cas de conflit, les descriptions du tableau suivant spécifient le comportement dans les versions Windows 10 et antérieures.

Agrandir le tableau

Setting	XML element	Description
Vérifier l'identité du serveur en validant le certificat	EAP-TLS: PerformServerValidation PEAP: PerformServerValidation	Cet élément spécifie que le client vérifie que les certificats de serveur présentés à l'ordinateur client répondent aux critères suivants : • Signatures correctes • Signatures n'ayant pas expiré • Ont été émis par une autorité de certification racine de confiance (CA) **Si cette case est décochée, les ordinateurs clients ne peuvent pas vérifier l'identité de vos serveurs pendant le processus d'authentification. Si l'authentification des serveurs n'a pas lieu, les utilisateurs s'exposent à des risques de sécurité graves, avec notamment la possibilité que des utilisateurs se connectent sans le savoir à des réseaux non autorisés.**
Connexion à ces serveurs	EAP-TLS: ServerValidation>ServerNames PEAP: ServerValidation>ServerNames EAP-TTLS: **ServerValidation> ServerNames** TEAP:	Permet de spécifier le nom des serveurs RADIUS (Remote Authentication Dial-In User Service) qui assurent l'authentification et l'autorisation réseau. Vous devez taper le nom **exactement** tel qu'il apparaît dans le champ **objet** de chaque certificat de serveur RADIUS ou utiliser des expressions régulières (regex) pour spécifier le nom du serveur. La syntaxe complète de l'expression régulière peut être utilisée pour indiquer le nom du serveur, mais pour différencier une expression régulière d'une

Setting	XML element	Description
	ServerValidation> **ServerNames**	chaîne littérale, vous devez utiliser au moins un `*` dans la chaîne spécifiée. Par exemple, vous pouvez définir `nps.*\.example\.com` pour spécifier le serveur RADIUS `nps1.example.com` ou `nps2.example.com`. Vous pouvez également inclure un `;` pour séparer plusieurs serveurs. **Si aucun serveur RADIUS n'est spécifié, le client vérifie toujours que le certificat de serveur RADIUS a été émis par une autorité de certification racine approuvée.**
Autorités de certification racine approuvées	EAP-TLS: ServerValidation>TrustedRootCA PEAP: ServerValidation>TrustedRootCA EAP-TTLS: **ServerValidation**> **TrustedRootCAHashes** TEAP: **ServerValidation**> **TrustedRootCAHashes**	Répertorie les autorités de certification racines de confiance. La liste est créée à partir des autorités de certification racines approuvées installées dans les magasins de certificats de l'ordinateur et de l'utilisateur. Vous pouvez spécifier quels sont les certificats d'autorité de certification racine de confiance utilisés par les demandeurs pour déterminer s'ils font confiance à vos serveurs, par exemple votre serveur exécutant NPS ou votre serveur d'approvisionnement. Si aucune autorité de certification racine de confiance n'est sélectionnée, le client 802.1X vérifie si le certificat d'ordinateur du serveur RADIUS est émis par une autorité de certification racine de confiance installée. Si une ou plusieurs autorités de certification racines de confiance sont sélectionnées, le client 802.1X vérifie que le certificat d'ordinateur du serveur RADIUS a été émis par l'une des autorités sélectionnées. **Si aucune autorité de certification racine approuvée n'est sélectionnée, le client vérifie toujours que le certificat de serveur RADIUS a été émis par une autorité de certification racine approuvée.** Si vous disposez d'une infrastructure à clé publique (PKI) sur votre réseau et que vous utilisez votre autorité de certification pour émettre des certificats à vos serveurs RADIUS, votre certificat d'autorité de certification est automatiquement ajouté à la liste des autorités de certification racines de confiance. Vous pouvez également acheter un certificat d'autorité de certification auprès d'un fournisseur autre que Microsoft. Certaines autorités de certification racines de confiance non-Microsoft fournissent avec le certificat que vous avez acheté un logiciel qui installe automatiquement le certificat acheté dans le magasin

Setting	XML element	Description
		de certificats **Autorités de certification racines de confiance**. Dans ce cas, l'autorité de certification racine de confiance apparaît automatiquement dans la liste des autorités de certification racines de confiance. Ne spécifiez pas un certificat d'autorité de certification racine approuvée qui ne figure pas dans les magasins de certificats **Autorités de certification racines de confiance** pour **Utilisateur actuel** et **Ordinateur local**. Si vous désignez un certificat qui n'est pas installé sur les ordinateurs clients, l'authentification échoue. Au format XML, il s'agit de l'empreinte SHA-1 (hash) du certificat (ou SHA-256 pour TEAP).

Invite utilisateur de validation du serveur

Le tableau suivant décrit les options d'invite utilisateur liées à la validation du serveur, disponibles pour chaque méthode EAP. Lorsqu'un certificat de serveur n'est pas approuvé, ces options déterminent si :

- La connexion échoue immédiatement.
- L'utilisateur reçoit une invite lui permettant d'accepter ou de rejeter manuellement la connexion.

EAP-TLS

Agrandir le tableau

Setting	XML element
Ne pas demander à l'utilisateur d'autoriser de nouveaux serveurs ou des autorités de certification approuvées.	ServerValidation > DisableUserPromptForServerValidation

Permet d'éviter de demander à l'utilisateur d'approuver un certificat de serveur s'il est mal configuré et/ou n'est pas encore approuvé (si cette option est activée). Pour simplifier l'expérience utilisateur et empêcher les utilisateurs d'approuver par erreur un serveur déployé par un attaquant, il est recommandé de cocher cette case.

Paramètres de configuration de l'authentification cellulaire

La liste suivante répertorie les paramètres de configuration respectivement pour EAP-SIM, EPA-AKA et EPA-AKA'.

EAP-SIM

EAP-SIM est défini dans RFC 4186. EAP-SIM est utilisé pour l'authentification et la distribution de clés de session avec un module SIM de réseau mobile de 2e génération GSM.

Paramètres EAP-SIM dans l'interface utilisateur mappé à EapSimConnectionPropertiesV1.

Agrandir le tableau

Item	XML element	Description
Utiliser des clés de chiffrement fortes	**UseStrongCipherKeys**	Si cette option est sélectionnée, spécifie que le profil utilise un chiffrement renforcé.
Ne pas révéler l'identité réelle au serveur quand un pseudonyme est disponible	**DontRevealPermanentID**	Si cette option est activée, force l'échec de l'authentification du client si les demandes de serveur en matière d'identité permanente par le biais du client ont un pseudonyme. Les pseudonymes sont utilisés à des fins de protection de la confidentialité, de manière à ce que l'identité réelle ou permanente d'un utilisateur ne soit pas révélée lors de l'authentification.
	ProviderName	Disponible uniquement en XML, chaîne qui indique le nom du fournisseur autorisé pour l'authentification.
Activer l'utilisation des domaines	**Royaume**=`true`	Fournit un emplacement pour taper le nom de domaine. Si ce champ n'est pas renseigné et que l'option **Activer l'utilisation des domaines** est sélectionnée, le domaine est dérivé de l'identité IMSI (International Mobile Subscriber Identity) à l'aide du domaine 3gpp.org, comme décrit dans la norme 3GPP (3rd Generation Partnership Project) 23.003 V6.8.0.

Item	XML element	Description
Spécifier un domaine	**Realm**	Fournit un emplacement pour saisir un nom de domaine. Si l'option **Activer l'utilisation des domaines** est activée, cette chaîne est utilisée. Si ce champ est vide, le domaine dérivé est utilisé.

Mode WPA3-Enterprise 192 bits

Le mode WPA3-Enterprise 192 bits est un mode spécial pour WPA3-Enterprise qui applique certaines exigences de sécurité élevées sur la connexion sans fil pour fournir un minimum de 192 bits de sécurité. Ces exigences s'alignent sur la suite CNSA (Commercial National Security Algorithm), CNSSP 15, qui est un ensemble d'algorithmes cryptographique approuvés pour la protection des informations classifiées et des informations ultra-secrètes par la National Security Agency (NSA) des États-Unis. Le mode 192 bits est parfois appelé « Mode Suite B » pour faire référence à la spécification de la NSA sur la cryptographie Suite B, qui a été remplacée par la CNSA en 2016.

Les modes WPA3-Enterprise et WPA3-Enterprise 192 bits sont disponibles à compter de Windows 10, version 2004 (build 19041) et Windows Server 2022. Toutefois, WPA3-Enterprise a été désigné en tant qu'algorithme d'authentification distinct dans Windows 11. Dans XML, cela est spécifié dans l'élément authEncryption .

Le tableau suivant répertorie les algorithmes requis par la suite CNSA.

Agrandir le tableau

Algorithm	Description	Parameters
AES (Advanced Encryption Standard)	Chiffrement par bloc symétrique	Clé 256 bits (AES-256)
Échange de clés ECDH (Elliptic Curve Diffie-Hellman)	Algorithme asymétrique utilisé pour établir un secret partagé (clé)	Courbe de module premier 384 bits (P-384)
Algorithme de signature numérique à courbe elliptique (ECDSA)	Algorithme asymétrique utilisé pour les signatures numériques	Courbe de module premier 384 bits (P-384)
algorithme de hachage sécurisé (Secure Hash Algorithm ou SHA)	Fonctions de hachage cryptographique	SHA-384
Échange de clés DH (Diffie-Hellman)	Algorithme asymétrique utilisé pour établir un secret partagé (clé)	Module 3072 bits

Algorithm	Description	Parameters
Rivest-Shamir-Adleman (RSA)	Algorithme asymétrique utilisé pour les signatures numériques ou l'établissement de clés	Module 3072 bits

Pour se conformer aux exigences de la CNSA, le mode WPA3-Enterprise 192 bits impose l'utilisation de EAP-TLS avec les suites de chiffrement restreintes suivantes :

- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
  - ECDHE et ECDSA avec la courbe de module premier 384 bits P-384
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` / `TLS_DHE_RSA_AES_256_GCM_SHA384`
  - ECDHE avec la courbe de module premier 384 bits P-384
  - RSA >= module 3 072 bits

> **Notes**
>
> P-384 est également appelé `secp384r1` ou `nistp384`. D'autres courbes elliptiques, telles que P-521, ne sont pas autorisées.
>
> SHA-384 fait partie de la famille de fonctions de hachage SHA-2. D'autres algorithmes et variantes comme SHA-512 ou SHA3-384 ne sont pas autorisés.

Windows prend uniquement en charge les suites de chiffrement `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384` et `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` pour le mode WPA3-Enterprise 192 bits. La suite de chiffrement `TLS_DHE_RSA_AES_256_GCM_SHA384` n'est pas prise en charge.

TLS 1.3 utilise de nouvelles suites TLS simplifiées, parmi lesquelles seule `TLS_AES_256_GCM_SHA384` est compatible avec le mode WPA3-Enterprise 192 bits. Étant donné que TLS 1.3 nécessite (EC)DHE et autorise les certificats ECDSA ou RSA, ainsi que le hachage AEAD et SHA384 AES-256, `TLS_AES_256_GCM_SHA384` équivaut à `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384` et `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. Toutefois, RFC 8446 exige que les applications compatibles TLS 1.3 prennent en charge P-256, ce qui est interdit par CNSA. Par conséquent, le mode WPA3-Enterprise 192 bits ne peut pas être entièrement conforme à TLS 1.3. Toutefois, il n'existe aucun problème d'interopérabilité connu avec TLS 1.3 et le mode WPA3-Enterprise 192 bits.

Pour configurer un réseau pour le mode WPA3-Enterprise 192 bits, Windows nécessite l'utilisation d'EAP-TLS avec un certificat qui répond aux exigences décrites précédemment.

Voir aussi

- Gestion des paramètres des nouvelles stratégies de réseau sans fil (IEEE 802.11)
- Gestion des paramètres de stratégie du nouveau réseau câblé (IEEE 802.3)
- Paramètres de sécurité avancés pour les stratégies de réseau câblé et sans fil

EAP - Ce qui a changé dans Windows 11

16/08/2025S'applique à: ✅ Windows 11, ✅ Windows 10

Windows 11 prend en charge WPA3-Enterprise, une norme de sécurité Wi-Fi qui définit un ensemble d'exigences relatives à la validation du certificat de serveur pour l'authentification EAP. Windows 11 prend également en charge TLS 1.3 par défaut. Cet article détaille les modifications du comportement de l'EAP dans Windows 11 en raison de ces fonctionnalités.

Comportement de validation du certificat de serveur mis à jour dans Windows 11

Dans les versions précédentes de Windows, y compris Windows 10, la logique de validation du certificat de serveur variait d'une méthode EAP à l'autre. Dans Windows 11, nous avons ajusté toutes les méthodes EAP pour qu'elles se comportent de manière cohérente et prévisible, ce qui est également cohérent avec la spécification WPA3-Enterprise. Ce nouveau comportement s'applique à toute authentification EAP à l'aide des méthodes EAP internes fournies avec Windows, y compris les scénarios Wi-Fi, Ethernet et VPN.

Windows approuve le certificat de serveur si l'une des conditions suivantes est remplie :

- L'empreinte du certificat de serveur a été ajoutée au profil.

  > ⓘ **Notes**
  >
  > Si l'utilisateur se connecte sans profil préconfiguré ou si les invites de validation du serveur sont activées dans le profil, l'empreinte est automatiquement ajoutée au profil si l'utilisateur accepte le serveur via l'invite d'interface utilisateur.

- Toutes les conditions suivantes sont respectées :

  1. La chaîne de certificats du serveur est approuvée par l'ordinateur ou l'utilisateur.
     - Cette approbation est basée sur le certificat racine présent dans le magasin racine approuvé de l'ordinateur ou de l'utilisateur, en fonction de l'authentification OneX.
  2. L'empreinte du certificat racine de confiance a été ajoutée au profil.
  3. Si la validation du nom du serveur est activée (recommandé), le nom correspond à celui spécifié dans le profil.
     - Pour plus d'informations, consultez Validation du serveur pour plus d'informations sur la configuration de la validation du nom du serveur dans le profil.

Problèmes potentiels de mise à niveau de Windows 10 vers Windows 11

Dans Windows 10, dans certaines circonstances, les authentifications PEAP et EAP-TLS pouvaient valider le serveur uniquement en fonction de la présence du certificat racine approuvé dans le magasin racine approuvé de Windows. Si vous constatez que l'authentification EAP échoue systématiquement après la mise à niveau vers Windows 11, vérifiez le profil de connexion pour vous assurer qu'il respecte les nouvelles exigences décrit ci-dessus.

Dans la plupart des cas, indiquer l'empreinte numérique du certificat racine approuvé dans le profil de configuration est suffisant pour résoudre le problème, à condition que le certificat racine soit déjà présent dans le magasin racine approuvé.

Une autre chose à noter est que la correspondance de nom de serveur est sensible à la casse dans Windows 11 version 21H2 (numéro de build 22000). La correspondance du nom du serveur a été ajustée pour être insensible à la casse dans Windows 11 version 22H2 (numéro de build 22621). Si vous utilisez la validation du nom du serveur, vérifiez que le nom spécifié dans le profil correspond exactement au nom du serveur ou effectuez une mise à niveau vers Windows 11 version 22H2 ou ultérieure.

Certificats génériques

Dans Windows 11, Windows ne rejette plus immédiatement les certificats de serveur qui contiennent un caractère générique (`*`) dans le nom commun du certificat (CN). Toutefois, il est recommandé d'utiliser un nom DNS dans le champ d'extension Subject Alternate Name (SubjectAltName/SAN), car si ce champ est présent, Windows ignorera les composants du CN pour effectuer la correspondance DNS. Le nom DNS SubjectAltName prend en charge un caractère générique dans Windows 11, comme dans les versions précédentes de Windows.

> **Notes**
>
> Toutes les conditions décrites ci-dessus pour approuver le certificat du serveur s'appliquent également aux certificats génériques.

Stratégies de désactivation TOD (Trust Override Disable) de WPA3-Enterprise

WPA3-Enterprise nécessite que l'appareil approuve le certificat du serveur : si la validation du serveur échoue, Windows n'entre pas dans la phase 2 de l'échange EAP. Si le certificat du

serveur n’est pas approuvé, l’utilisateur est invité à accepter le certificat du serveur. Ce comportement est appelé **User Override of Server Certificate** (UOSC). Pour désactiver l'UOSC pour les machines sans profil préconfiguré, il est possible de définir des stratégies **Trust Override Disable** (TOD) sur le certificat du serveur.

Les stratégies TOD sont indiquées dans l’extension **Stratégies de certificat** du certificat de serveur en incluant un OID spécifique. Les stratégies suivantes sont prises en charge :

- TOD-STRICT : Si le certificat du serveur n’est pas approuvé, l’utilisateur n'est pas invité à accepter le certificat du serveur. L’authentification échoue. Cette stratégie a l’OID `1.3.6.1.4.1.40808.1.3.1`.
- TOD-TOFU (Trust On First Use) : Si le certificat du serveur n’est pas approuvé, l’utilisateur est invité à accepter le certificat du serveur lors de la première connexion uniquement. Si l’utilisateur accepte le certificat du serveur, ce dernier est ajouté au profil et l’authentification continue. Toutefois, les connexions ultérieures nécessiteront que le certificat du serveur soit approuvé et ne demanderont plus de confirmation. Cette stratégie a l’OID `1.3.6.1.4.1.40808.1.3.2`.

TLS 1.3

Windows 11 activait TLS 1.3 par défaut au niveau système. EAP-TLS utilisait déjà TLS 1.3, mais PEAP et EAP-TTLS continuaient d’utiliser TLS 1.2. À partir de Windows 11 version 22H2 (numéro de build 22621), ces méthodes utilisent désormais TLS 1.3 par défaut.

Problèmes connus avec TLS 1.3 et Windows 11

- NPS ne prend pas en charge TLS 1.3 pour le moment.
- Certaines versions antérieures de serveurs RADIUS tiers peuvent indiquer à tort la prise en charge de TLS 1.3. Si vous rencontrez des problèmes d’authentification EAP-TLS avec TLS 1.3 dans Windows 11 22H2, vérifiez que le serveur RADIUS est à jour ou que TLS 1.3 est désactivé.
- La reprise de session n’est actuellement pas prise en charge. Les clients Windows effectuent toujours une authentification complète.

Configurer des profils et des paramètres EAP dans Windows

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10

Cet article présente des informations sur les méthodes couramment utilisées pour configurer les paramètres EAP (Extensible Authentication Protocol). Plus précisément, il décrit la configuration des profils EAP à l'aide d'outils en ligne de commande et XML. Il montre également comment configurer des paramètres et des profils EAP à l'aide de différentes interface utilisateur dans Windows.

Profils XML

Comme indiqué dans les profils XML pour EAP, les profils de connexion pour Wi-Fi, Ethernet et VPN sont des fichiers XML qui contiennent les options de configuration de la connexion. Ces profils peuvent être importés/exportés et modifiés manuellement. Lorsque des profils sont créés ou modifiés dans l'interface utilisateur (comme indiqué dans les sections suivantes), Windows définit en interne les options de configuration XML correspondantes. Par conséquent, vous pouvez utiliser l'interface utilisateur pour créer un profil, puis l'exporter pour afficher les options de configuration XML qui ont été définies.

> ⓘ **Notes**
>
> Toutes les options de configuration ne sont pas exposées dans l'interface utilisateur. Selon votre scénario, vous devrez peut-être modifier manuellement le profil XML pour définir les options de configuration souhaitées. Vous importez ensuite le profil mis à jour pour le déploiement.
>
> Par exemple, lors de l'utilisation de stratégies de gestion des appareils mobiles (GPM) (telles que Wi-Fi CSP), vous devez provisionner le profil XML complet.

Vous trouverez un exemple de profil Wi-Fi dans cet exemple.

Importer et exporter des profils à l'aide d'outils en ligne de commande

L'importation et l'exportation de profils à l'aide d'un outil en ligne de commande peuvent être utiles dans de nombreux scénarios. Par exemple, lorsque la configuration de GPM ou de stratégie de groupe n'est pas possible, l'option la plus rapide peut consister à utiliser ces commandes manuellement ou par script. Il peut également être utilisé pour exporter des profils après les avoir configurés via une autre interface utilisateur.

netsh

`netsh` est un outil en ligne de commande qui peut être utilisé pour afficher et configurer différents paramètres liés au réseau. Pour plus d'informations, consultez Netsh (Network Shell). `netsh` peut être appelé à partir de `cmd` et `powershell`. Le tableau suivant répertorie certaines commandes `netsh` courantes et des exemples d'importation et d'exportation de profils. Vous pouvez utiliser `/?` n'importe quelle `netsh` commande pour obtenir plus d'informations sur la commande, y compris la syntaxe.

Wi-Fi

Agrandir le tableau

Command	Description
`netsh wlan show profiles`	Affiche tous les profils Wi-Fi, y compris le nom du profil.
`netsh wlan show profiles name="ProfileName"`	Affiche des informations détaillées sur un profil de Wi-Fi spécifique.
`netsh wlan export profile name="ProfileName" folder="C:\Profiles"`	Exporte un profil Wi-Fi vers le dossier spécifié. Le dossier doit exister.
`netsh wlan add profile filename="C:\Profiles\ProfileName.xml"`	Ajoute un profil Wi-Fi à partir du fichier spécifié.
`netsh wlan delete profile name="ProfileName"`	Supprime un profil Wi-Fi.

PowerShell

PowerShell est un interpréteur de commandes et un langage de script qui peuvent être utilisés pour afficher et configurer différents paramètres. Il comprend diverses commandes (applets de commande) qui peuvent être utilisées pour importer et exporter des profils de connexion. Vous pouvez utiliser l'applet de commande Get-Help avec n'importe quelle applet de commande pour obtenir plus d'informations sur cette applet de commande, y compris la syntaxe.

VPN

Pour plus d'informations sur ces applets de commande, consultez Get-VpnConnection, Set-VpnConnection et Add-VpnConnection.

Agrandir le tableau

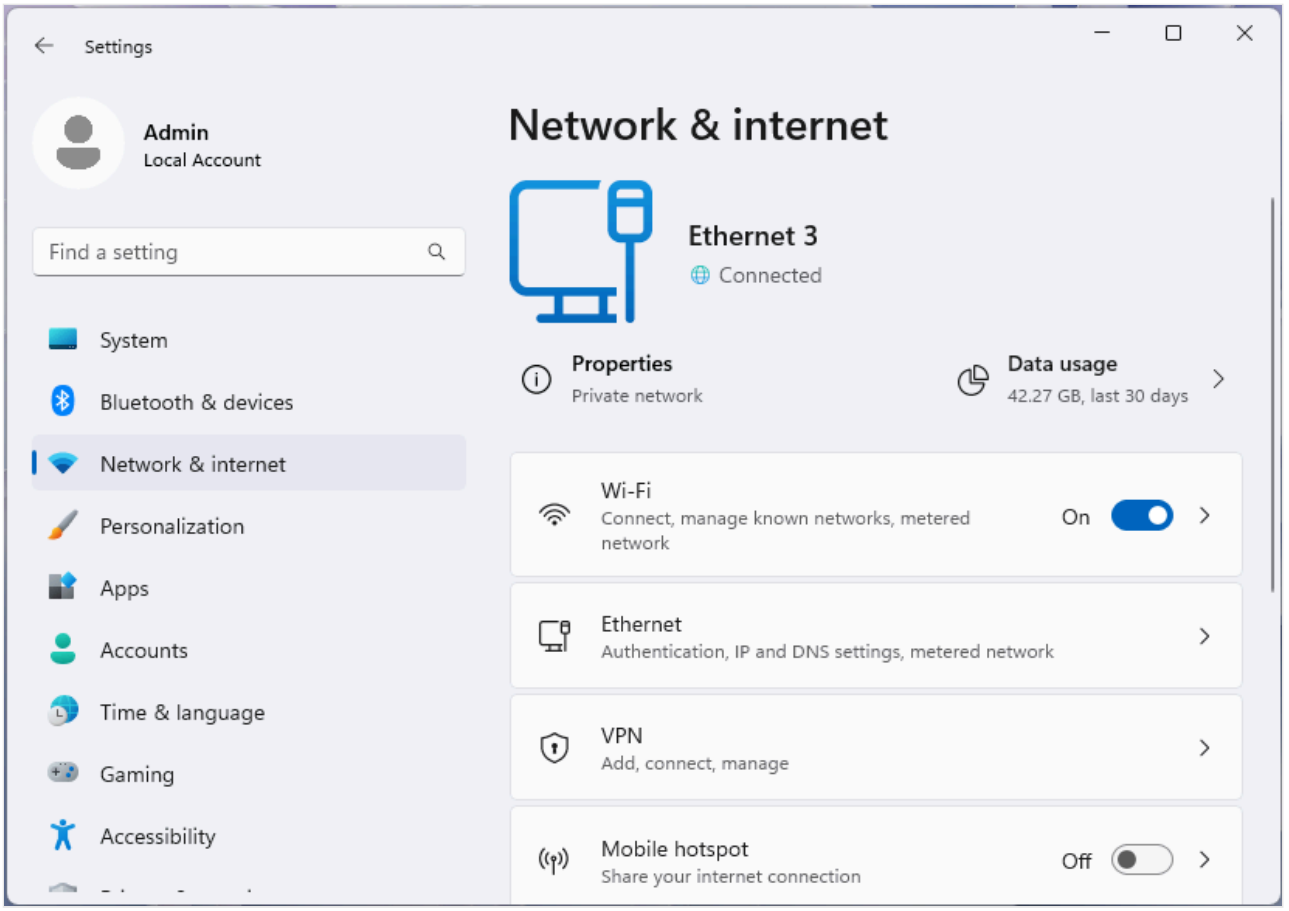
Command	Description
`Get-VpnConnection`	Affiche tous les profils VPN, y compris le nom du profil et d'autres détails.
`Get-VpnConnection -Name "ProfileName"`	Affiche des informations récapitulatives sur un profil VPN spécifique.
`(Get-VpnConnection -Name "ProfileName").EapConfigXmlStream.InnerXml | Out-File -FilePath "C:\Profiles\vpn_eap.xml"`	Exporte la configuration EAP d'un profil VPN spécifique dans un fichier.
`Set-VpnConnection -Name "ProfileName" -EapConfigXmlStream (Get-Content -Path "C:\Profiles\vpn_eap.xml")`	Importe la configuration EAP à partir d'un fichier et met à jour le profil VPN spécifié.

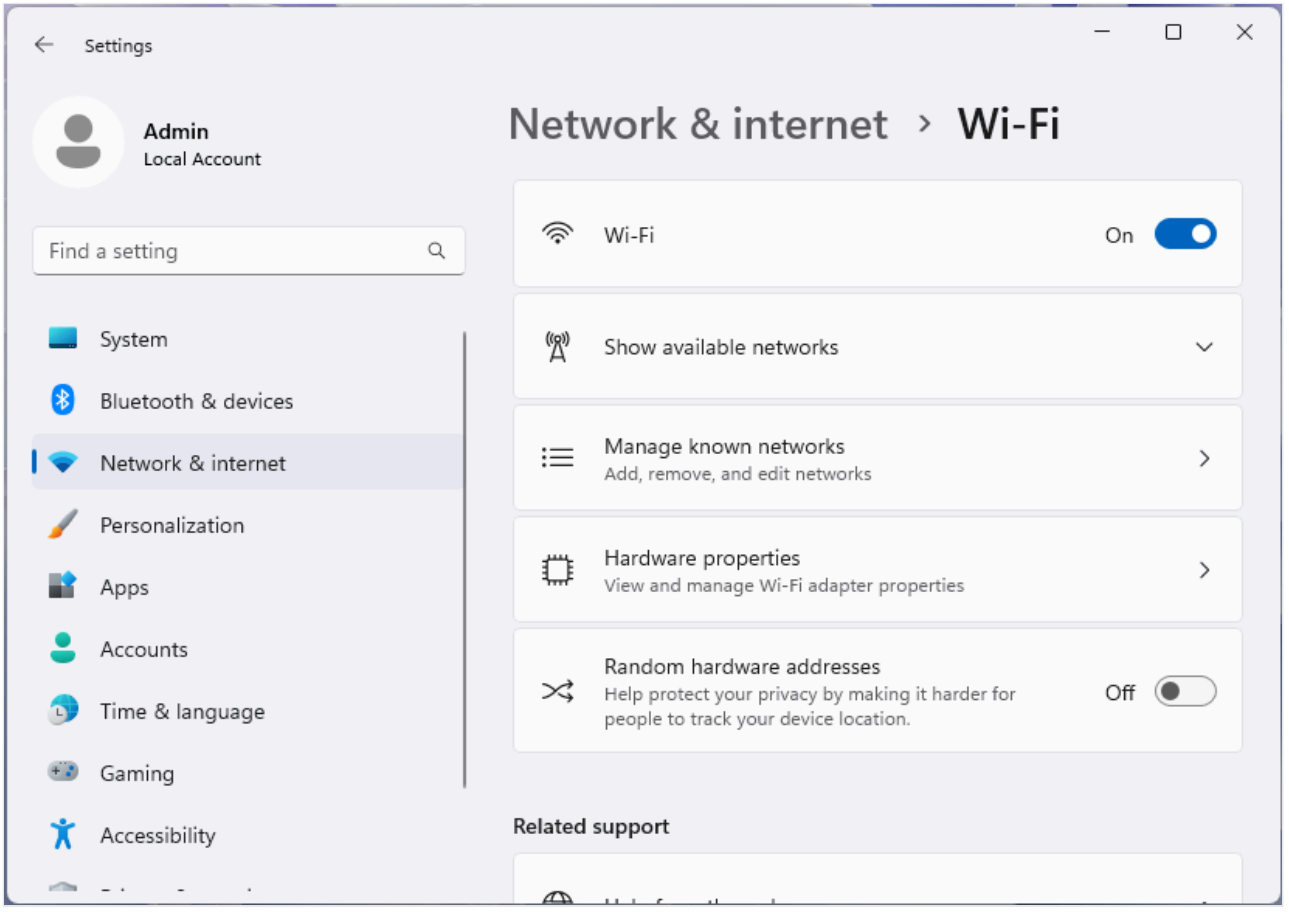
Application Paramètres (Windows de bureau)

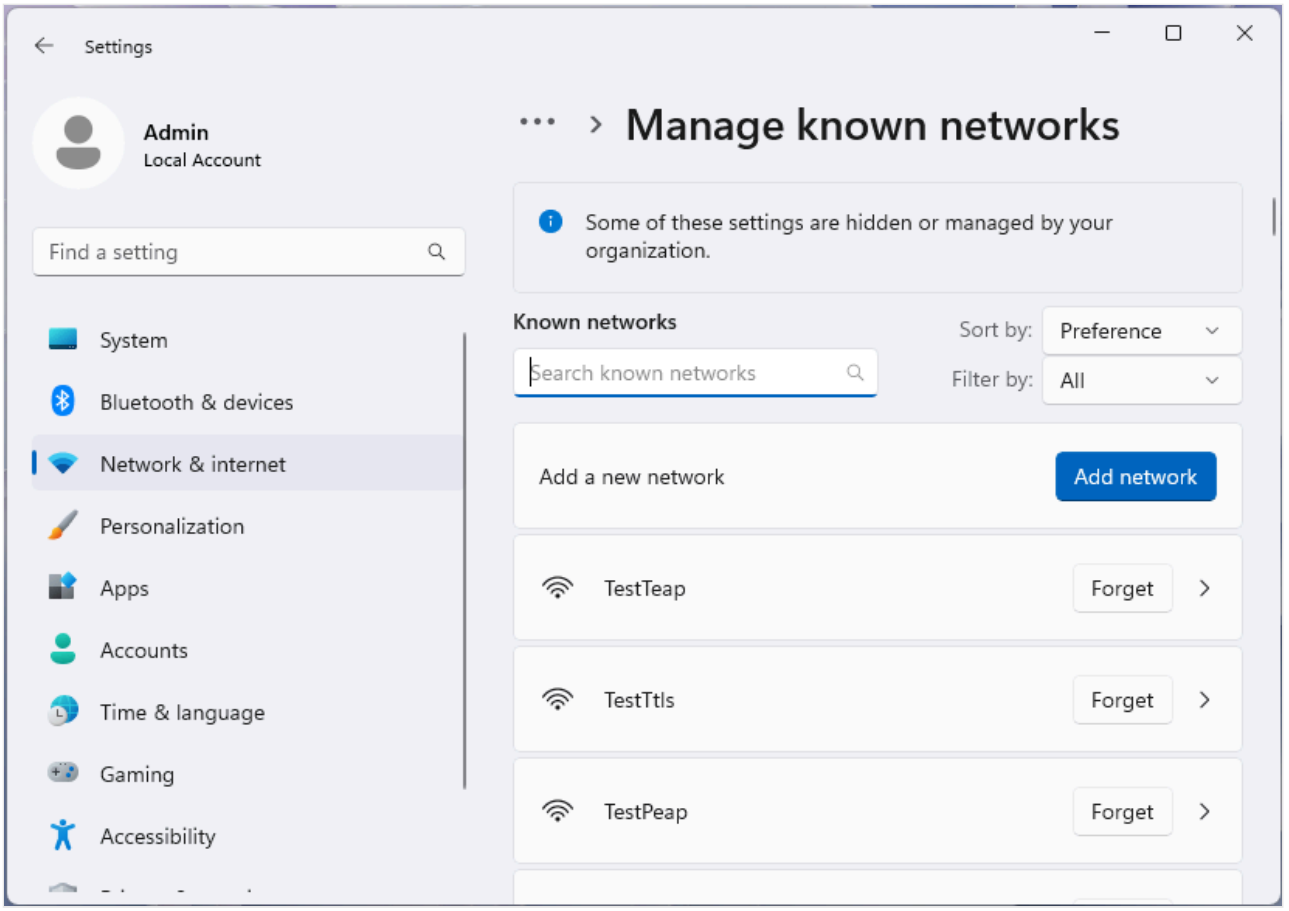
Sur le client de bureau Windows, de nombreux paramètres Wi-Fi, Ethernet et VPN courants peuvent être configurés via l'application Paramètres. Les captures d'écran suivantes montrent l'application Paramètres Windows 11, mais l'interface utilisateur est similaire dans Windows 10. Toutefois, certaines fonctionnalités et options peuvent être disponibles uniquement dans Windows 11.

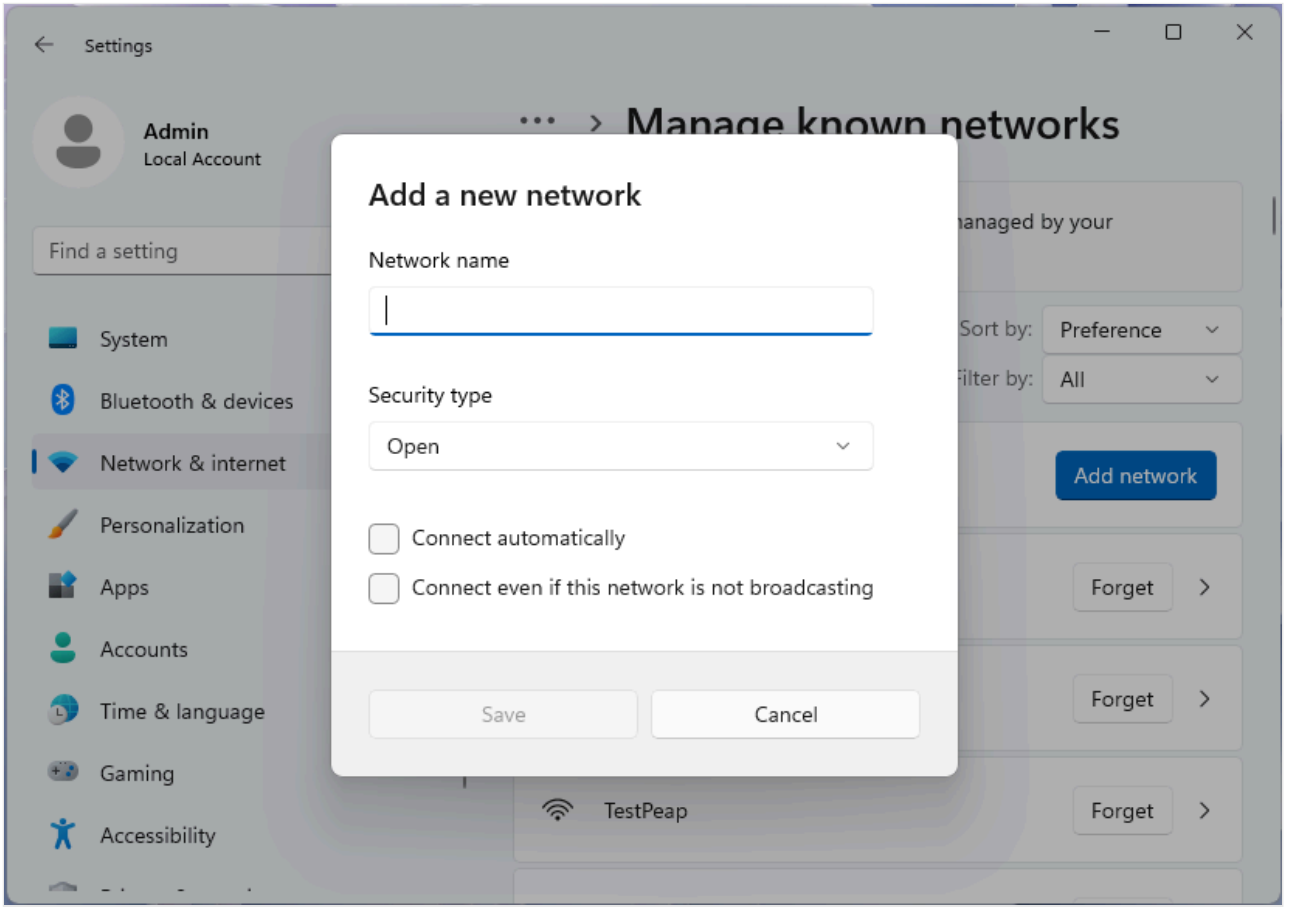
Wi-Fi

Windows 10 et Windows 11 prennent en charge l'ajout de profils Wi-Fi avec une configuration spécifique (y compris 802.1X) dans l'application Paramètres. Ce paramètre se trouve dans l'application Paramètres sous **Réseau et**>**Wi-Fi**>**Gérer les réseaux**> connus**Ajouter un réseau** :


Settings
Admin
Local Account
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Network & internet
Ethernet 3
Connected
Properties
Private network
Data usage
42.27 GB, last 30 days
Wi-Fi
Connect, manage known networks, metered network
On
Ethernet
Authentication, IP and DNS settings, metered network
VPN
Add, connect, manage
Mobile hotspot
Share your internet connection
Off

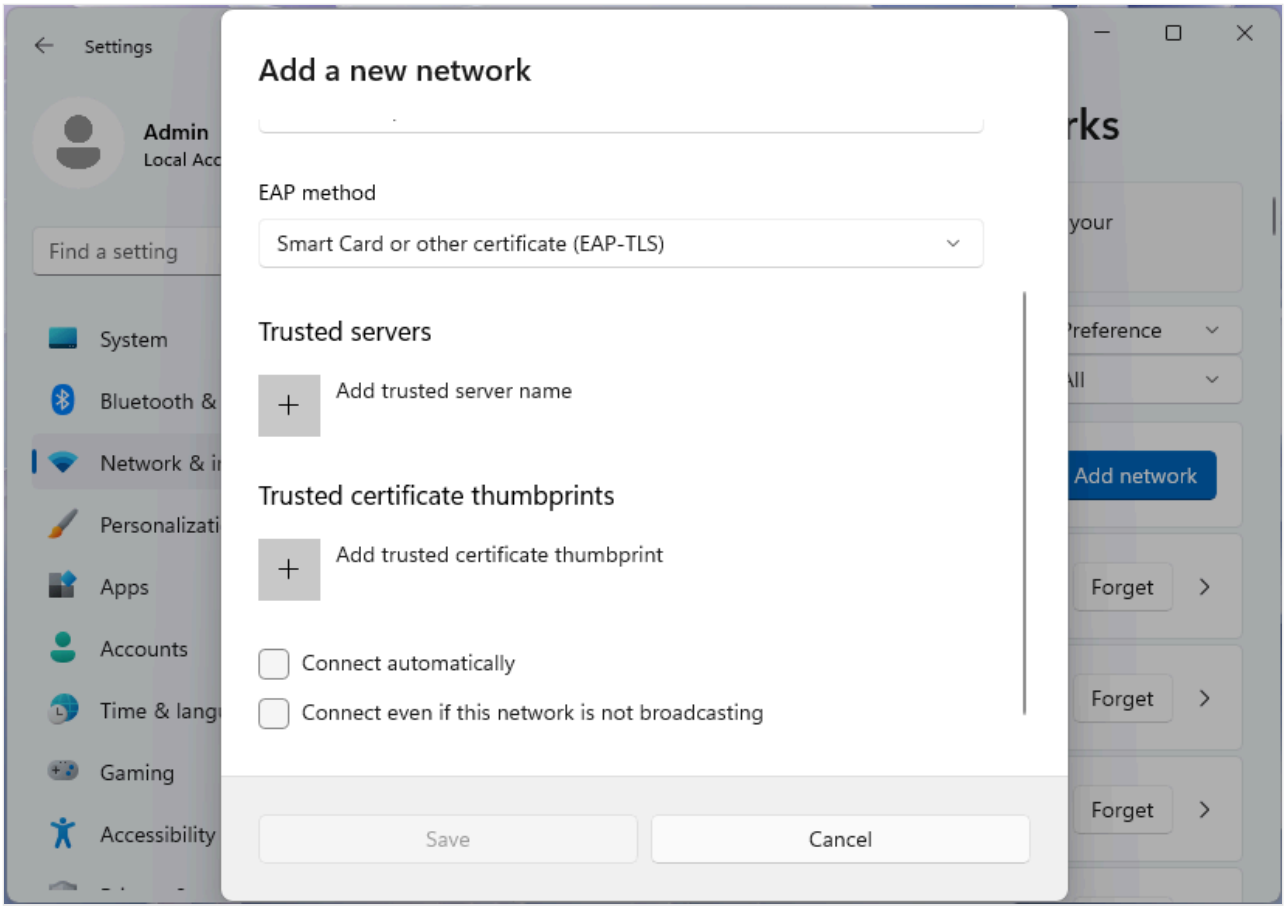

Settings
Admin
Local Account
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Network & internet › Wi-Fi
Wi-Fi
On
Show available networks
Manage known networks
Add, remove, and edit networks
Hardware properties
View and manage Wi-Fi adapter properties
Random hardware addresses
Help protect your privacy by making it harder for people to track your device location.
Off
Related support





Cette boîte de dialogue vous permet de configurer le SSID, le type de sécurité et d'autres paramètres pour le profil Wi-Fi. Lorsqu'un type de sécurité prenant en charge EAP est sélectionné, par exemple **WPA3-Enterprise AES**, la boîte de dialogue affiche une option

permettant de configurer les paramètres EAP :



Conseil

Une fois le réseau ajouté, vous ne pouvez pas modifier les paramètres EAP à l'aide de l'application Paramètres. Pour modifier les paramètres EAP, effectuez l'une des opérations suivantes :

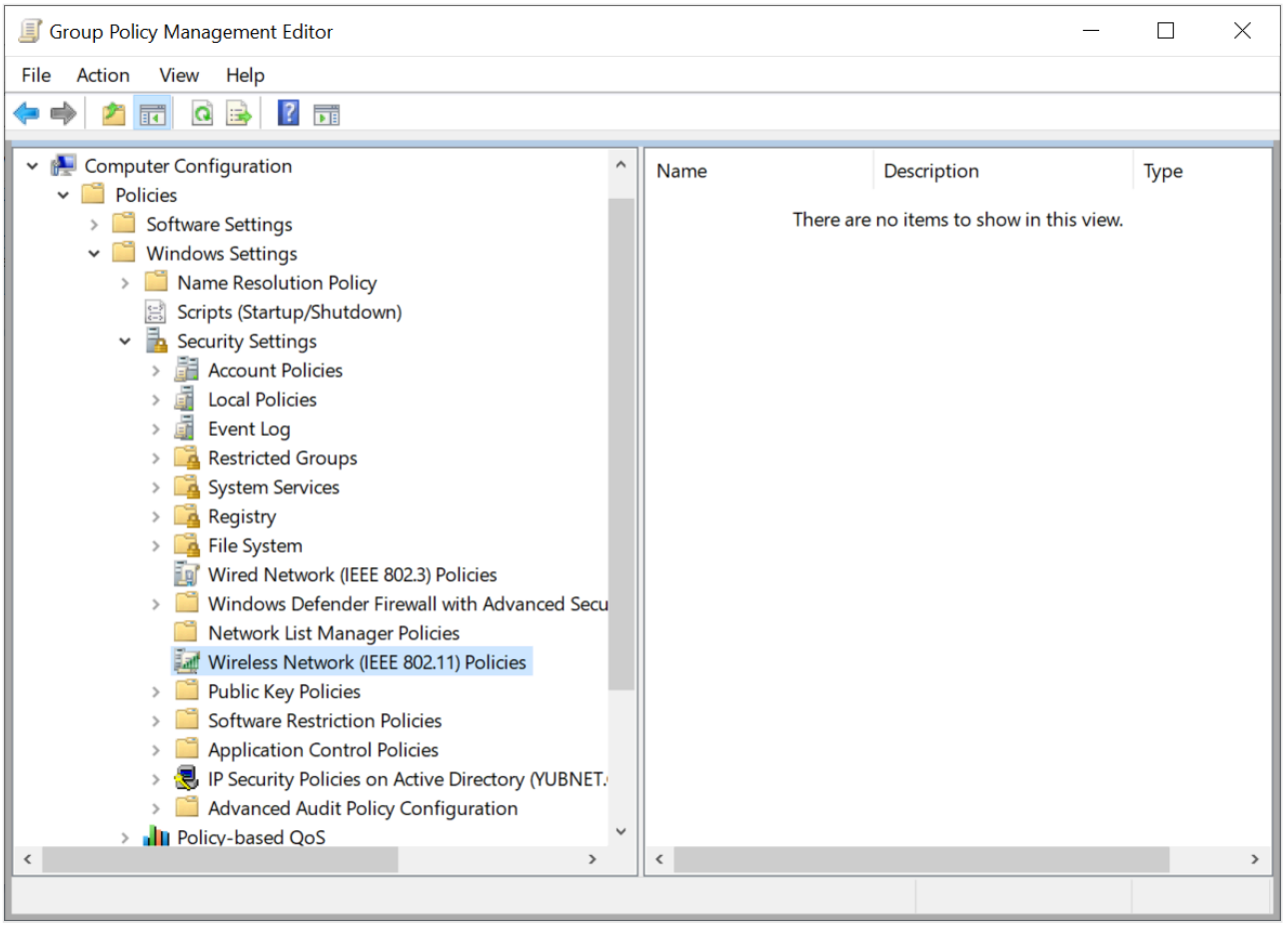
- Supprimez le profil et ajoutez-le à nouveau avec les paramètres appropriés.
- Utilisez les `netsh` commandes décrites dans netsh pour modifier manuellement le profil.

Éditeur de stratégie de groupe (bureau et serveur)

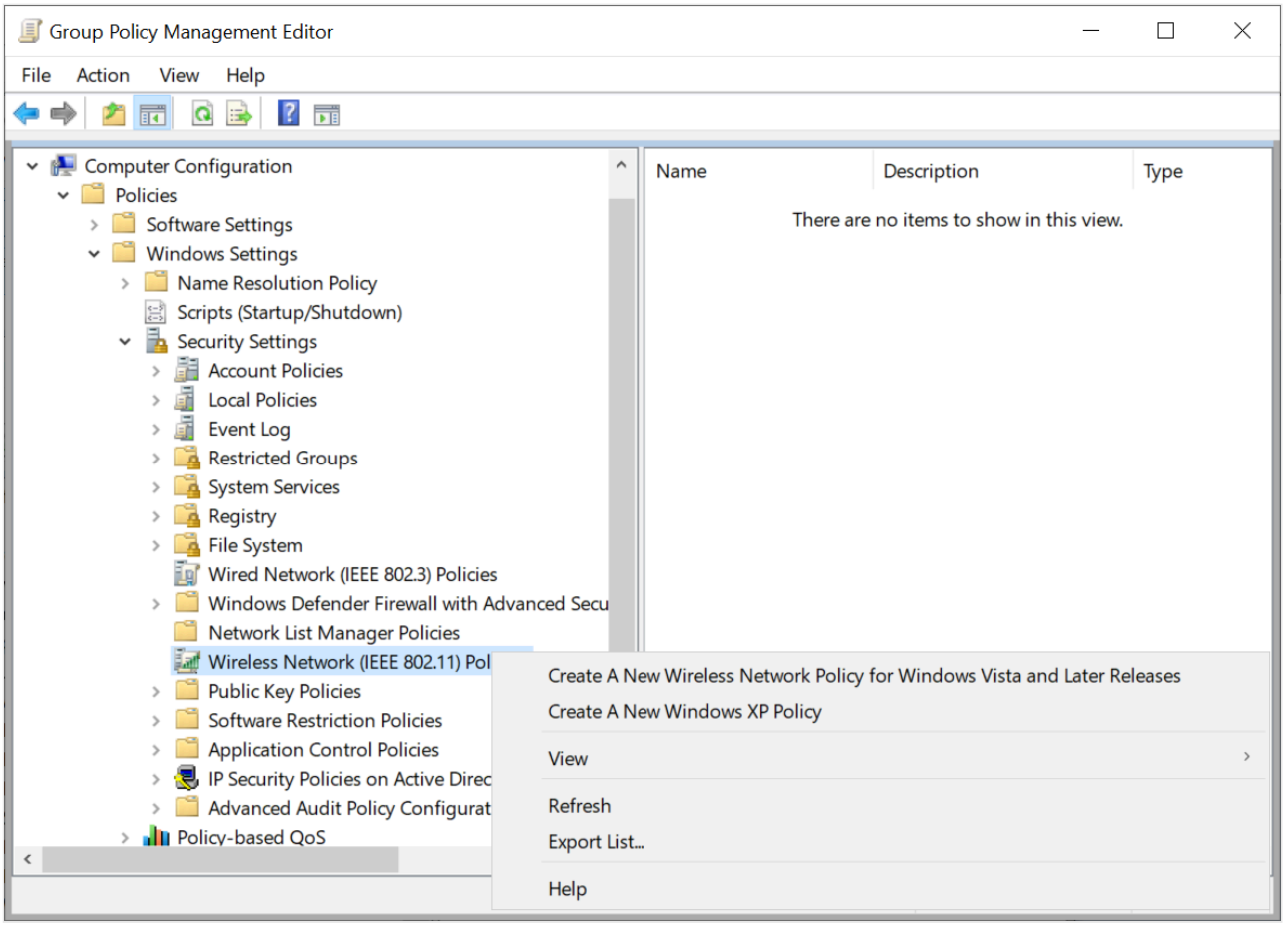
La stratégie de groupe est une infrastructure qui vous permet de gérer des configurations pour les utilisateurs et les ordinateurs. En utilisant la **stratégie de groupe**, vous pouvez configurer les paramètres Wi-Fi, Ethernet et VPN en fonction des règles que vous définissez. Les captures d'écran suivantes montrent l'éditeur de gestion des stratégies de groupe Windows Server 2022, mais l'interface utilisateur est similaire pour le Panneau de configuration Windows de bureau et l'éditeur de stratégie de groupe local. Pour plus d'informations sur les options présentées dans les captures d'écran suivantes, consultez EAP pour l'accès réseau.

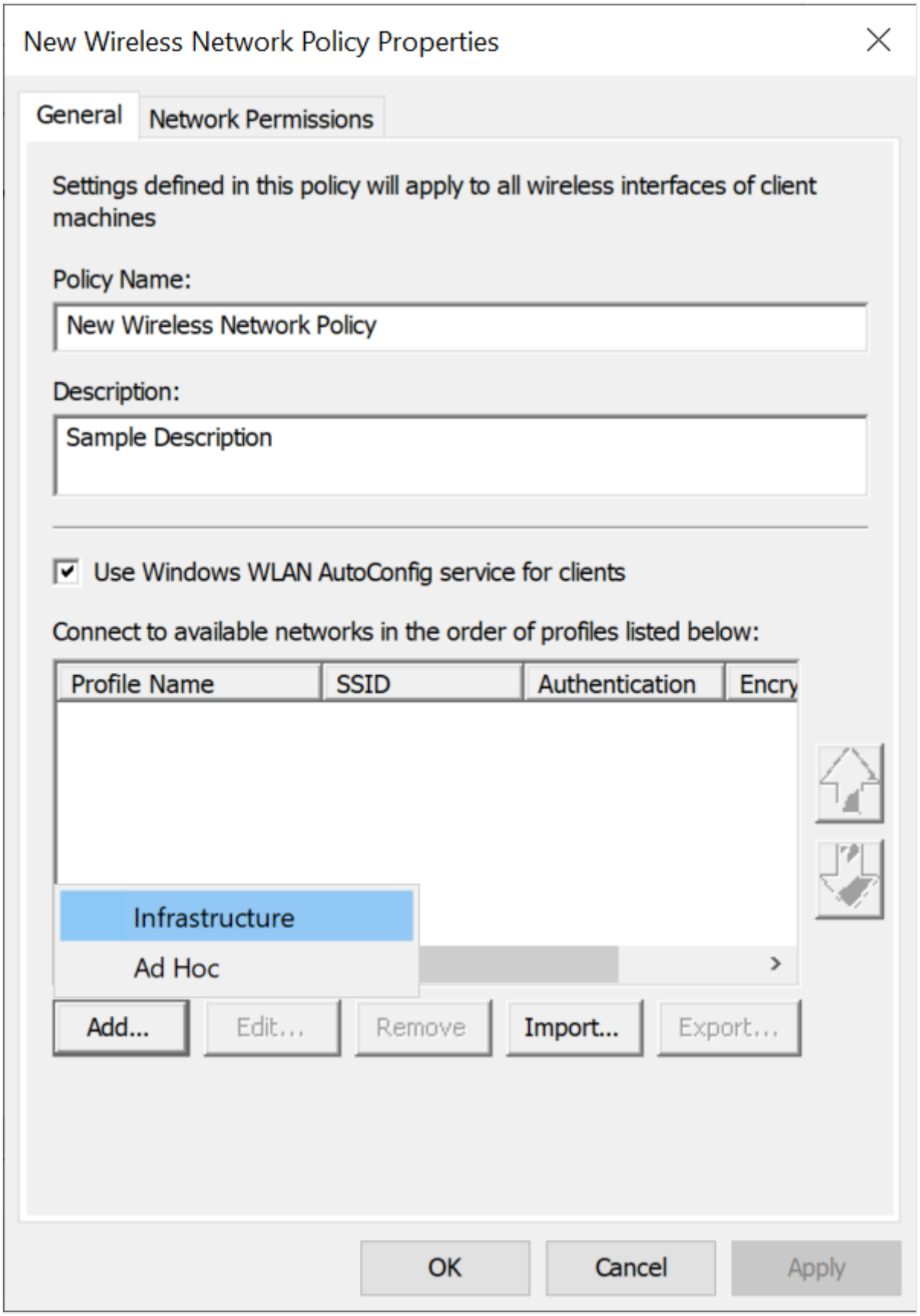
Wi-Fi

Les options **de stratégie de groupe** pour Wi-Fi se trouvent sous l'option Stratégies de **sécurité**paramètres de**sécurité**>> paramètres de l'ordinateur(>>**IEEE 802.11)** Stratégies :



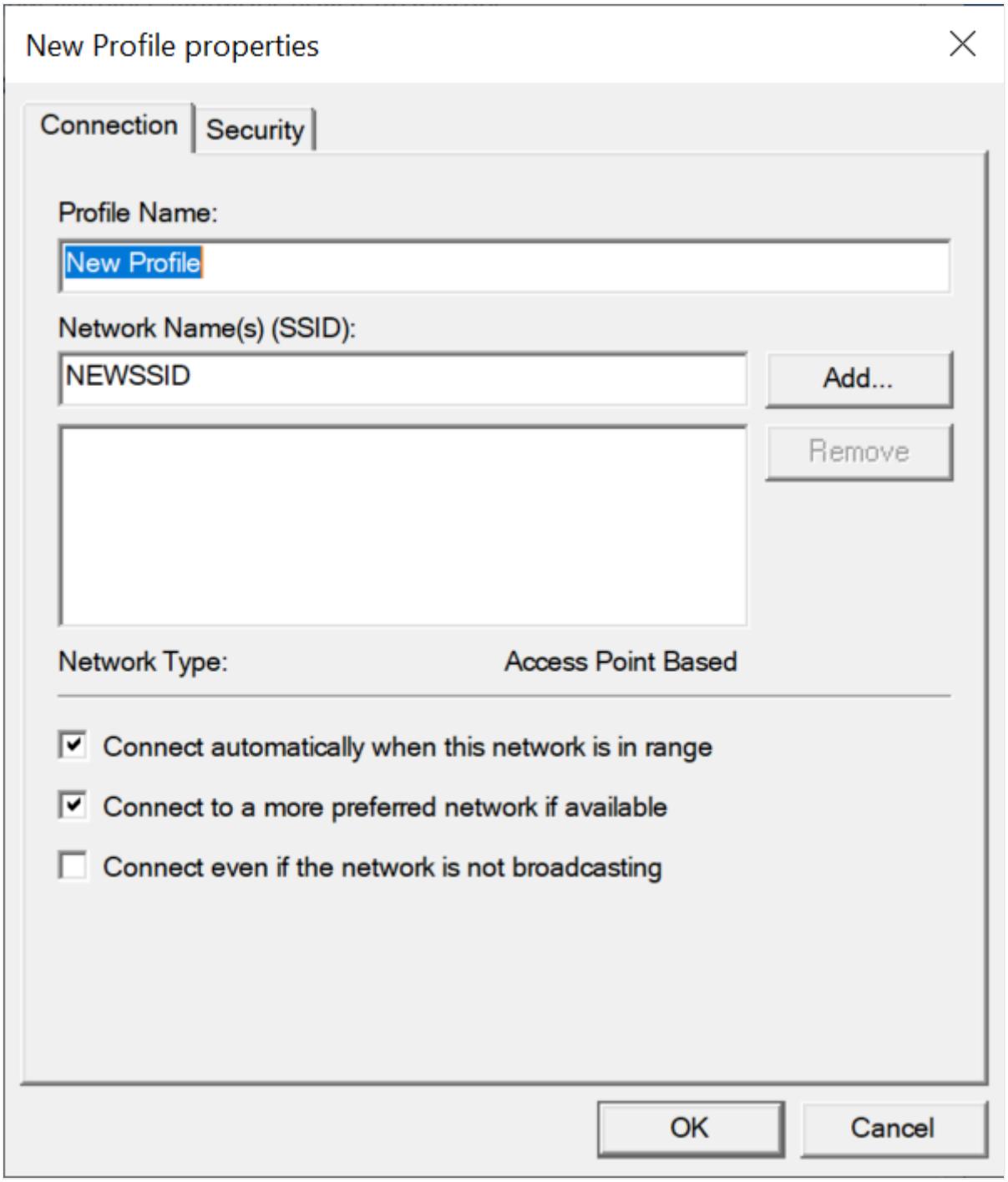
Le fait de cliquer avec le bouton droit sur les **stratégies de réseau sans fil (IEEE 802.11)** et de sélectionner **Créer une stratégie de réseau sans fil pour Windows Vista et versions ultérieures** ouvre la boîte de dialogue **Nouvelles propriétés de stratégie de réseau sans fil** :


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Pol
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Direc
Advanced Audit Policy Configurat
Policy-based QoS
Name
Description
Type
There are no items to show in this view.
Create A New Wireless Network Policy for Windows Vista and Later Releases
Create A New Windows XP Policy
View
Refresh
Export List...
Help



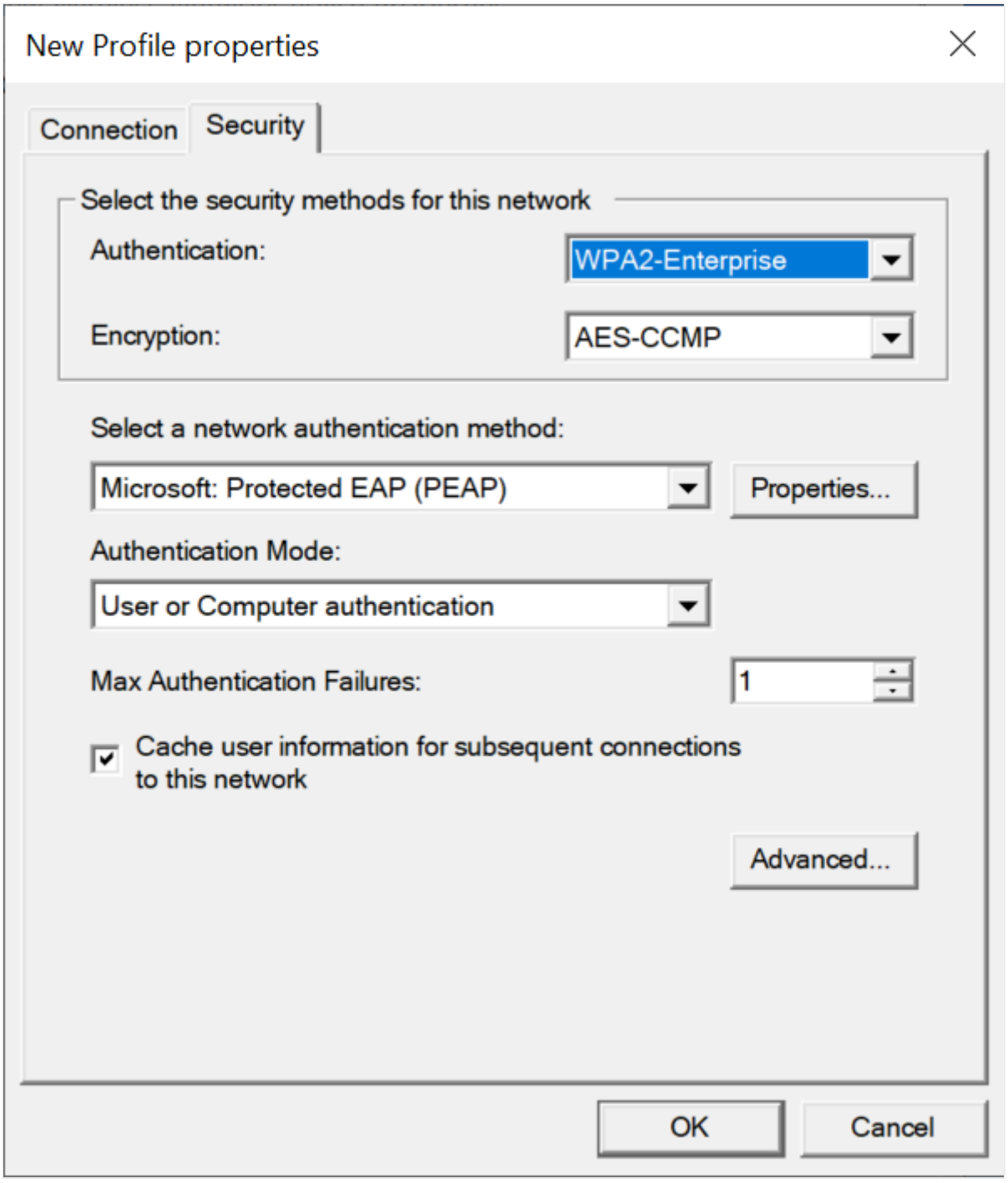
Cette boîte de dialogue vous permet de définir le nom de la stratégie, une description et **ajouter/des/** profils**Supprimer**, ainsi que des profils XML**d'importation** et **d'exportation**.

En sélectionnant **Ajouter** , puis en sélectionnant **Infrastructure** , la boîte de dialogue **Propriétés du nouveau profil** s'ouvre :



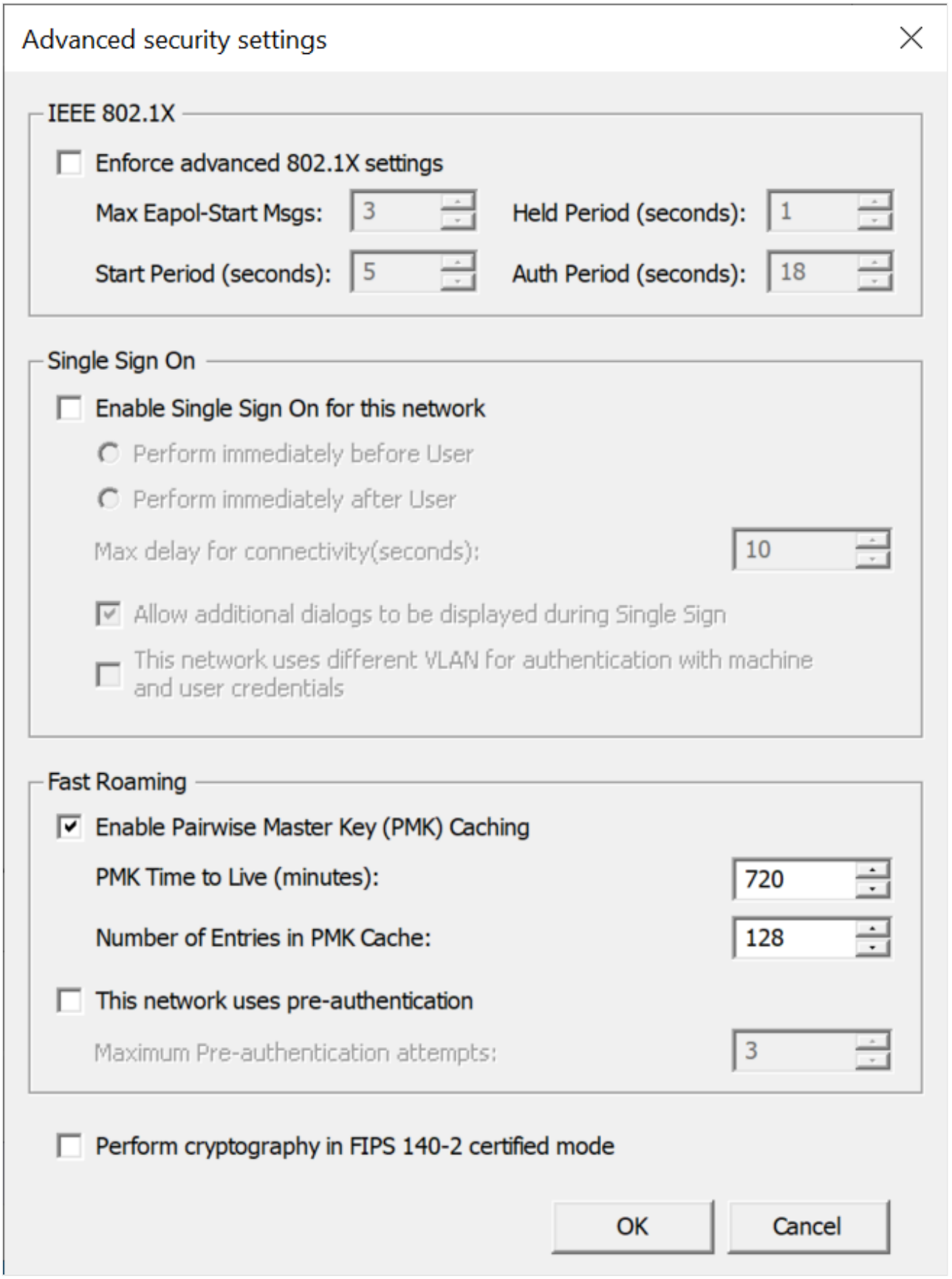
Cette boîte de dialogue vous permet de définir le **nom** du profil et d'ajouter les SSID auxquels le profil s'applique.

La sélection de **Sécurité** vous permet de configurer les paramètres EAP pour le profil :



Cette boîte de dialogue vous permet de configurer le type de sécurité et d'autres paramètres pour le profil Wi-Fi. Lorsqu'un type **d'authentification** prenant en charge l'authentification 802.1X est sélectionné (par exemple **WPA2-Enterprise**), les options de sécurité 802.1X sont visibles. Pour plus d'informations sur chaque méthode d'authentification réseau, consultez les méthodes EAP .

Lorsque le bouton **Avancé...** est sélectionné, la boîte de dialogue **Paramètres de sécurité avancés** s'affiche :



Cette boîte de dialogue vous permet de définir certains paramètres 802.1X avancés et des options d'authentification unique.

Conseil

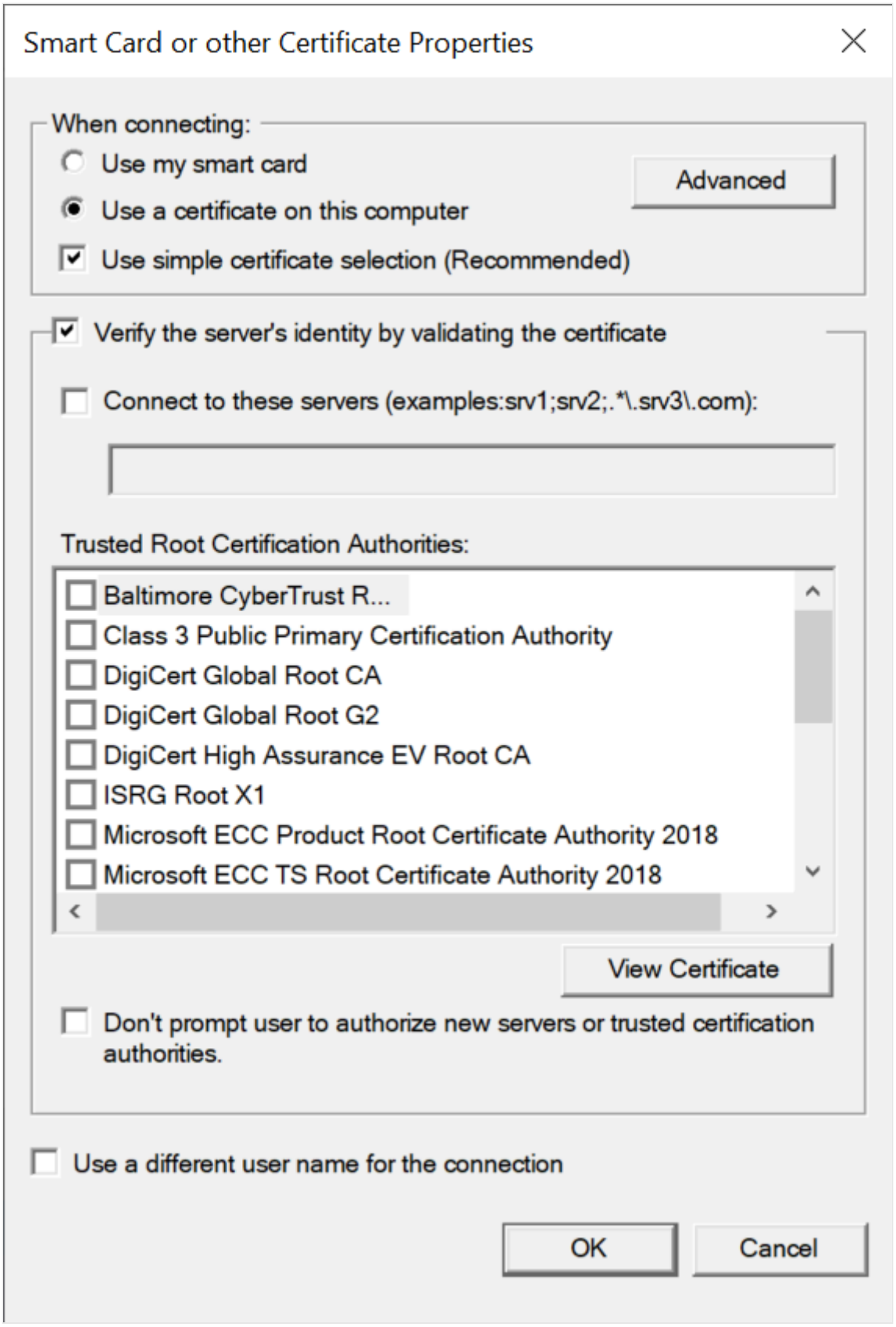
Tous les paramètres ne sont pas disponibles pour la configuration dans l'éditeur de stratégie de groupe. Toutefois, vous pouvez contourner ce problème en important un profil XML avec les paramètres souhaités. Pour plus d'informations, consultez **Profils XML**.

Méthodes EAP

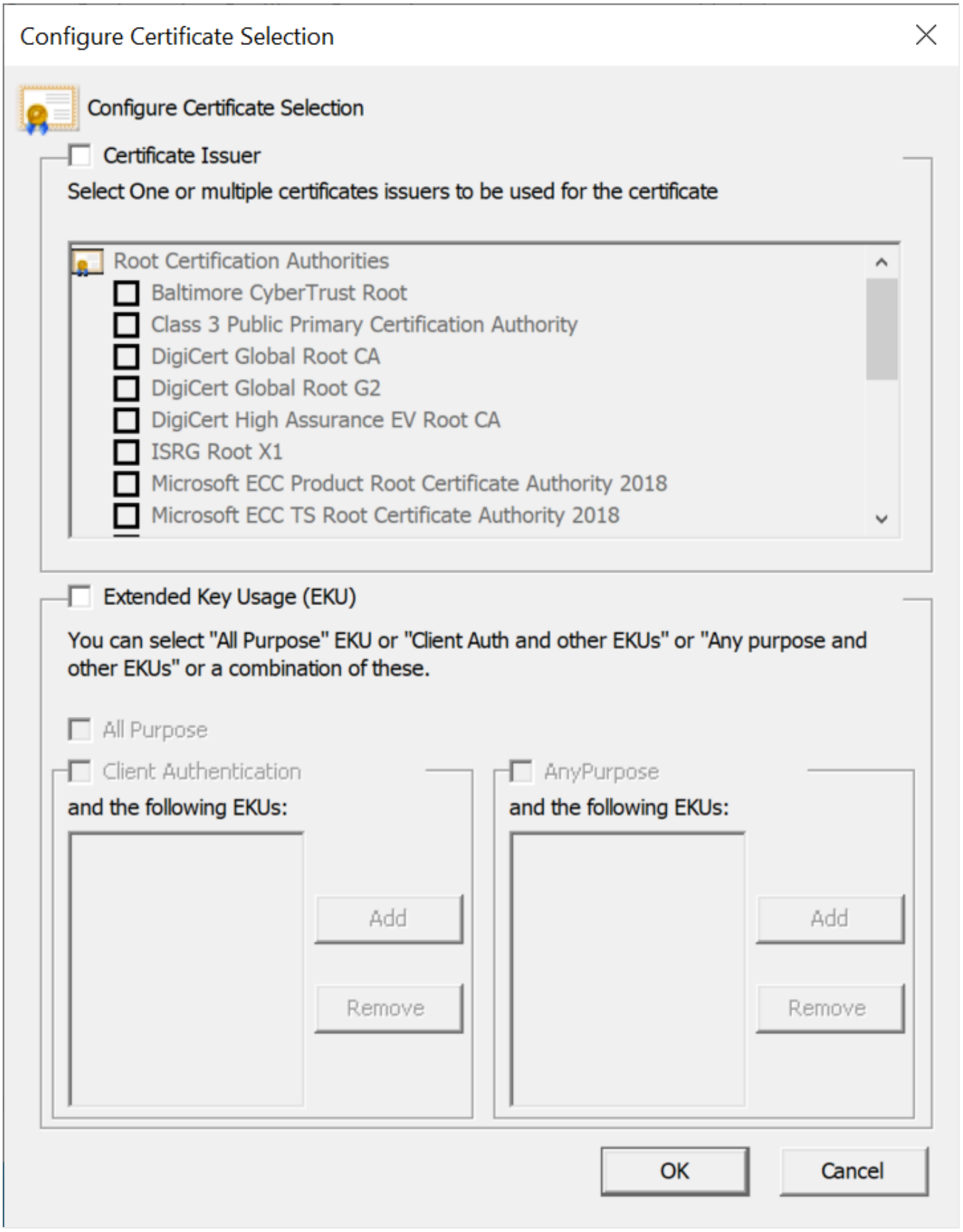
Pour obtenir une vue d'ensemble des différentes méthodes EAP, consultez méthodes d'authentification.

Microsoft : Carte à puce ou autre certificat

Pour plus d'informations sur cette boîte de dialogue, consultez EAP-TLS.

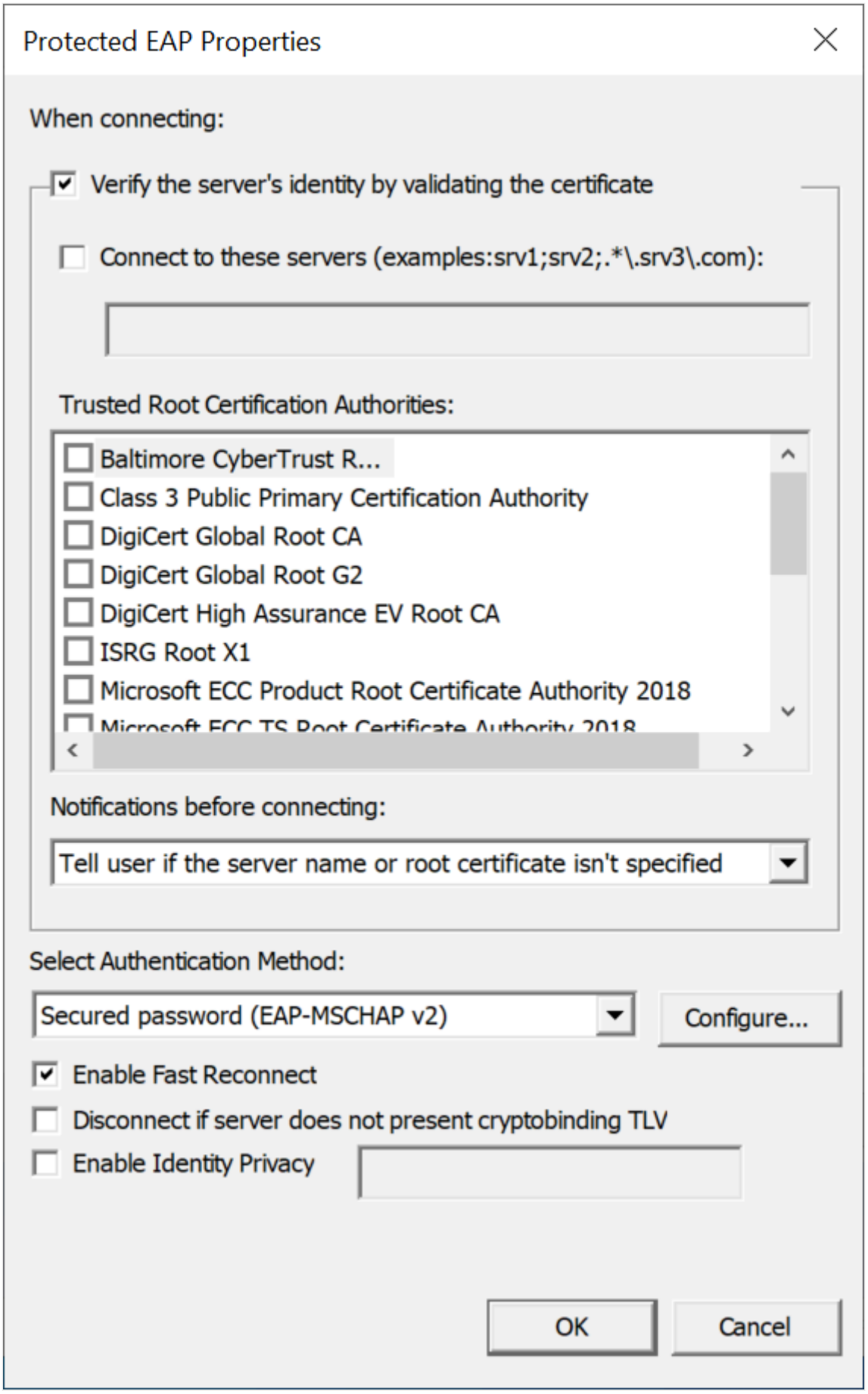


La sélection **avancée** ouvre la boîte de dialogue Configurer la sélection du certificat :

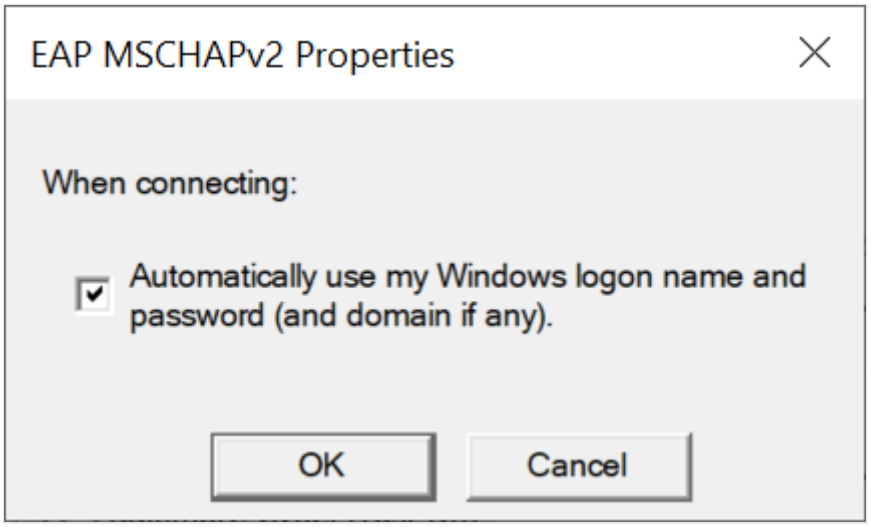


Microsoft : PEAP (Protected EAP)

Pour plus d'informations sur cette boîte de dialogue, consultez PEAP.

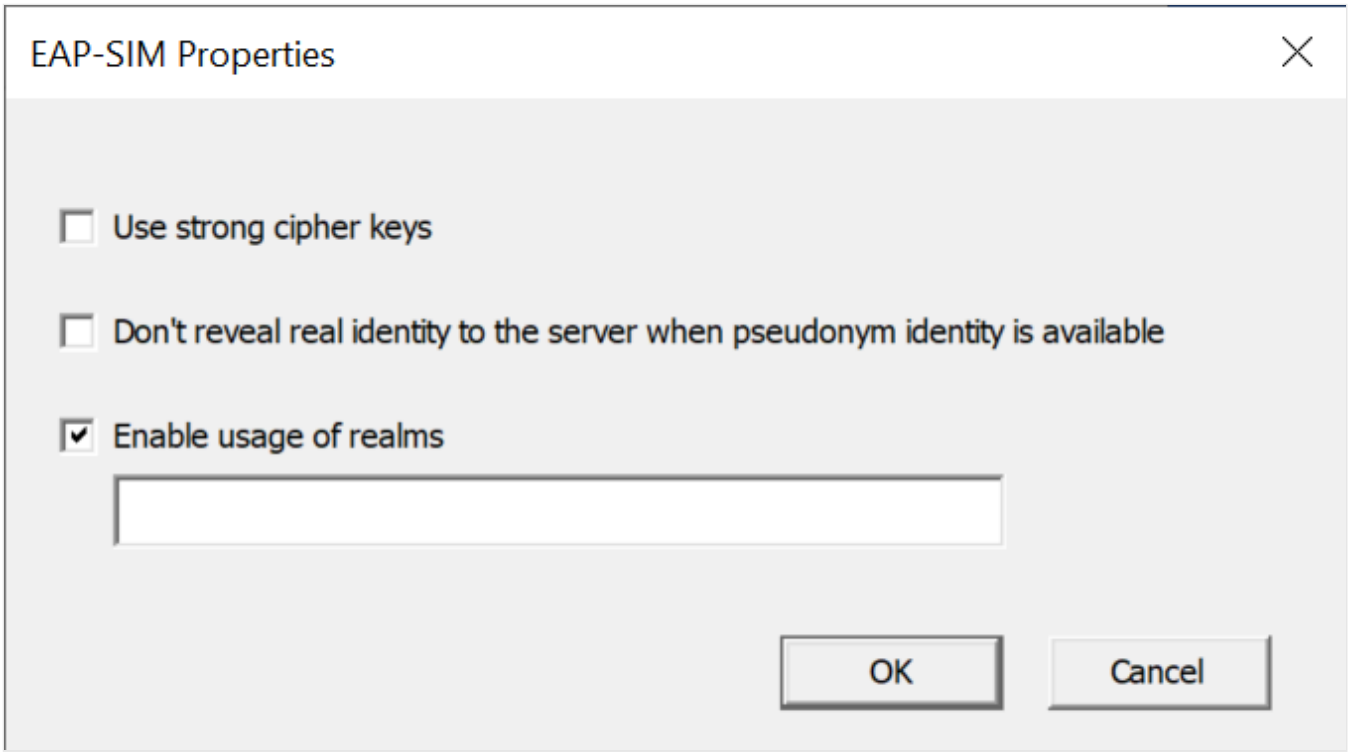


La sélection de **Configurer...** lorsque **le mot de passe sécurisé (EAP-MSCHAP v2)** est sélectionné ouvre la boîte de dialogue **EAP MSCHAPv2** :



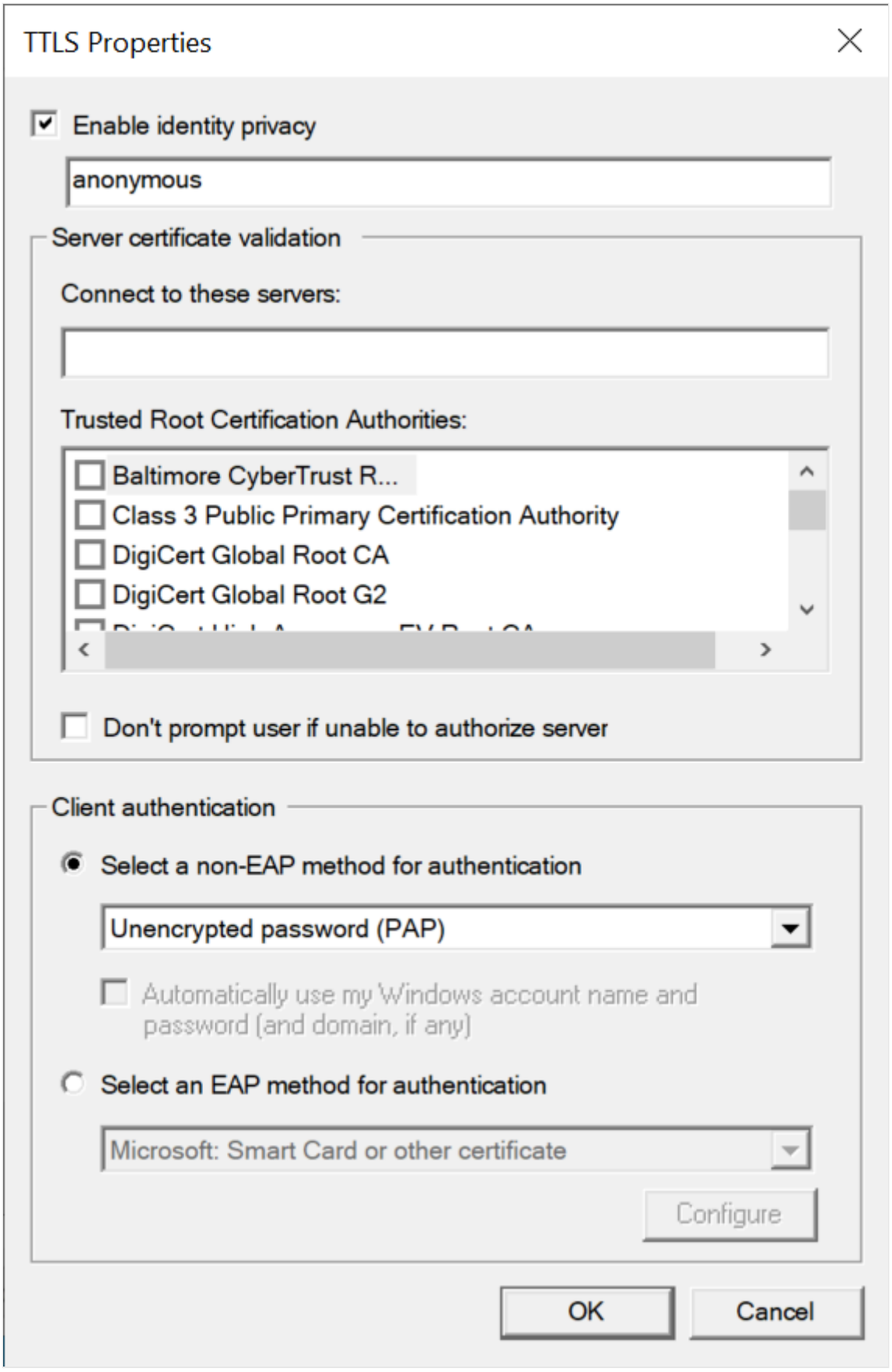
Microsoft : EAP-SIM

Pour plus d'informations sur cette boîte de dialogue, consultez EAP-SIM.



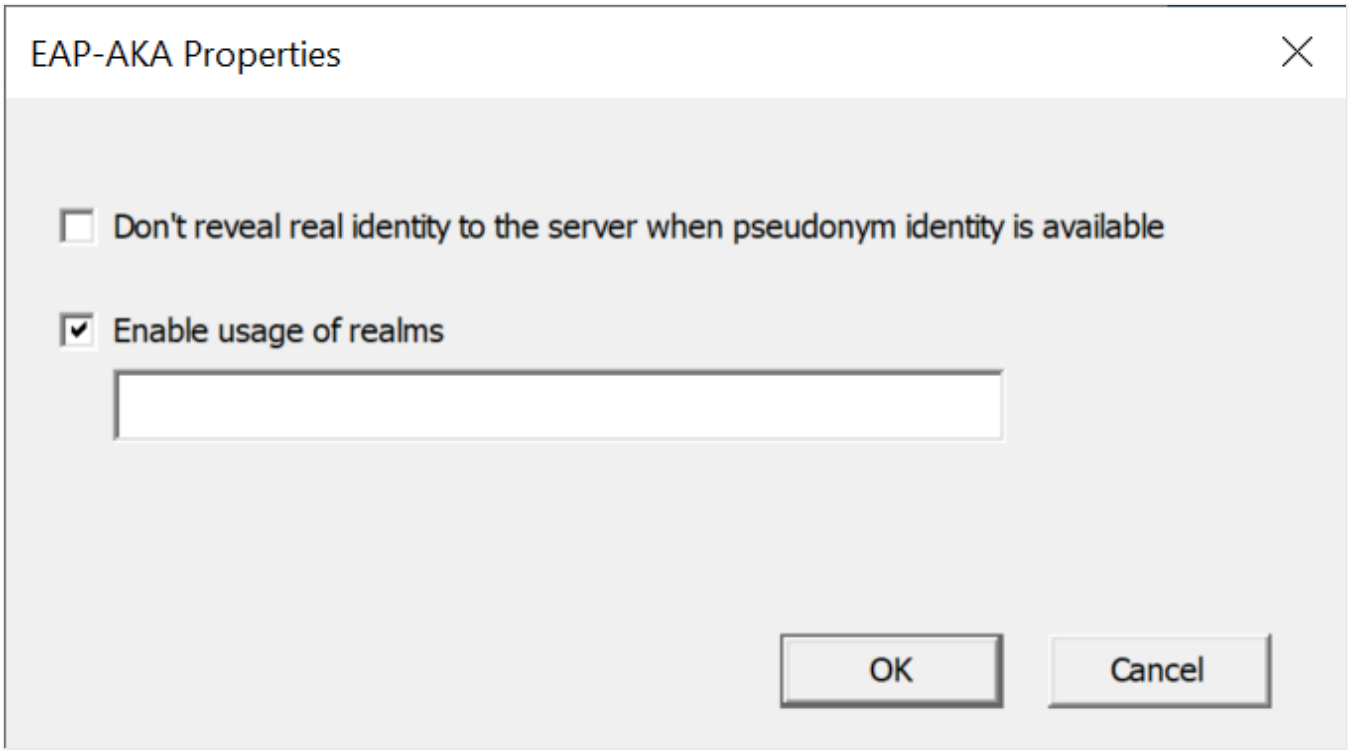
Microsoft : EAP-TTLS

Pour plus d'informations sur cette boîte de dialogue, consultez EAP-TTLS.



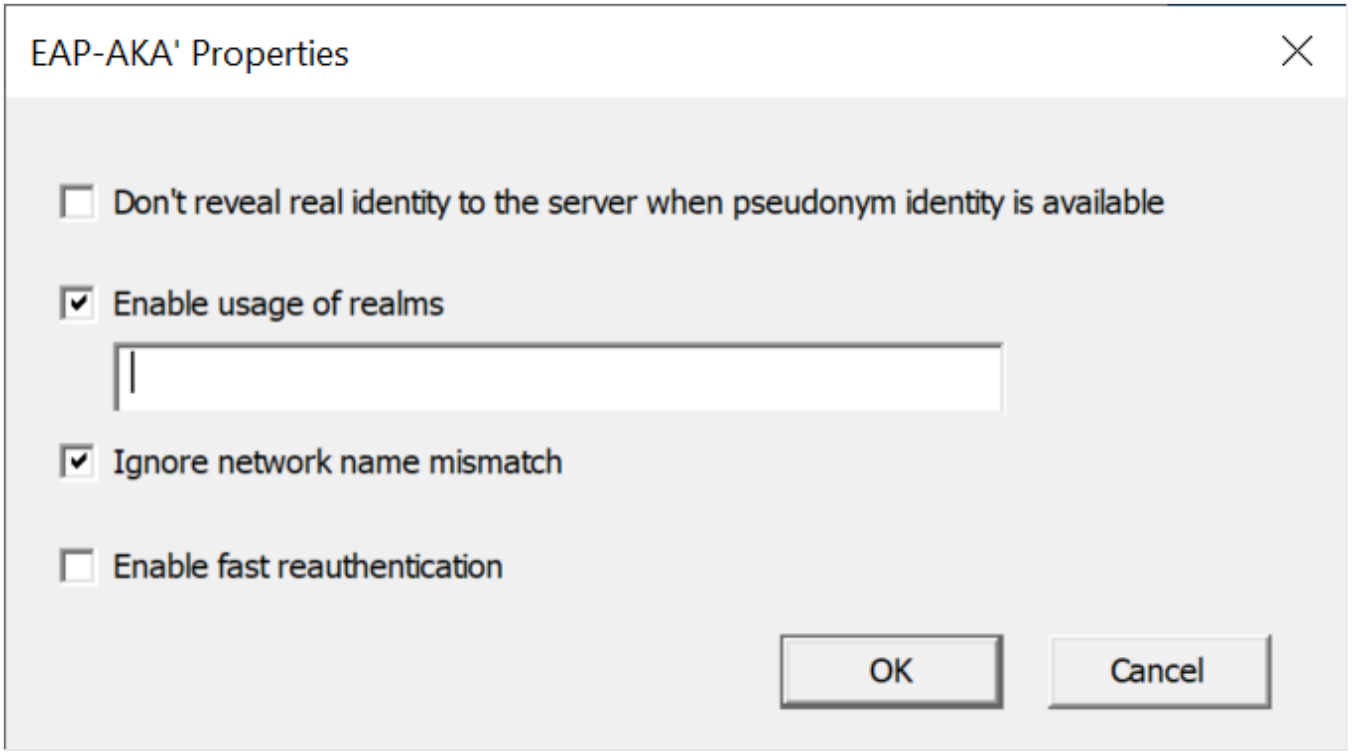
Microsoft : EAP-AKA

Pour plus d'informations sur cette boîte de dialogue, consultez EAP-AKA.



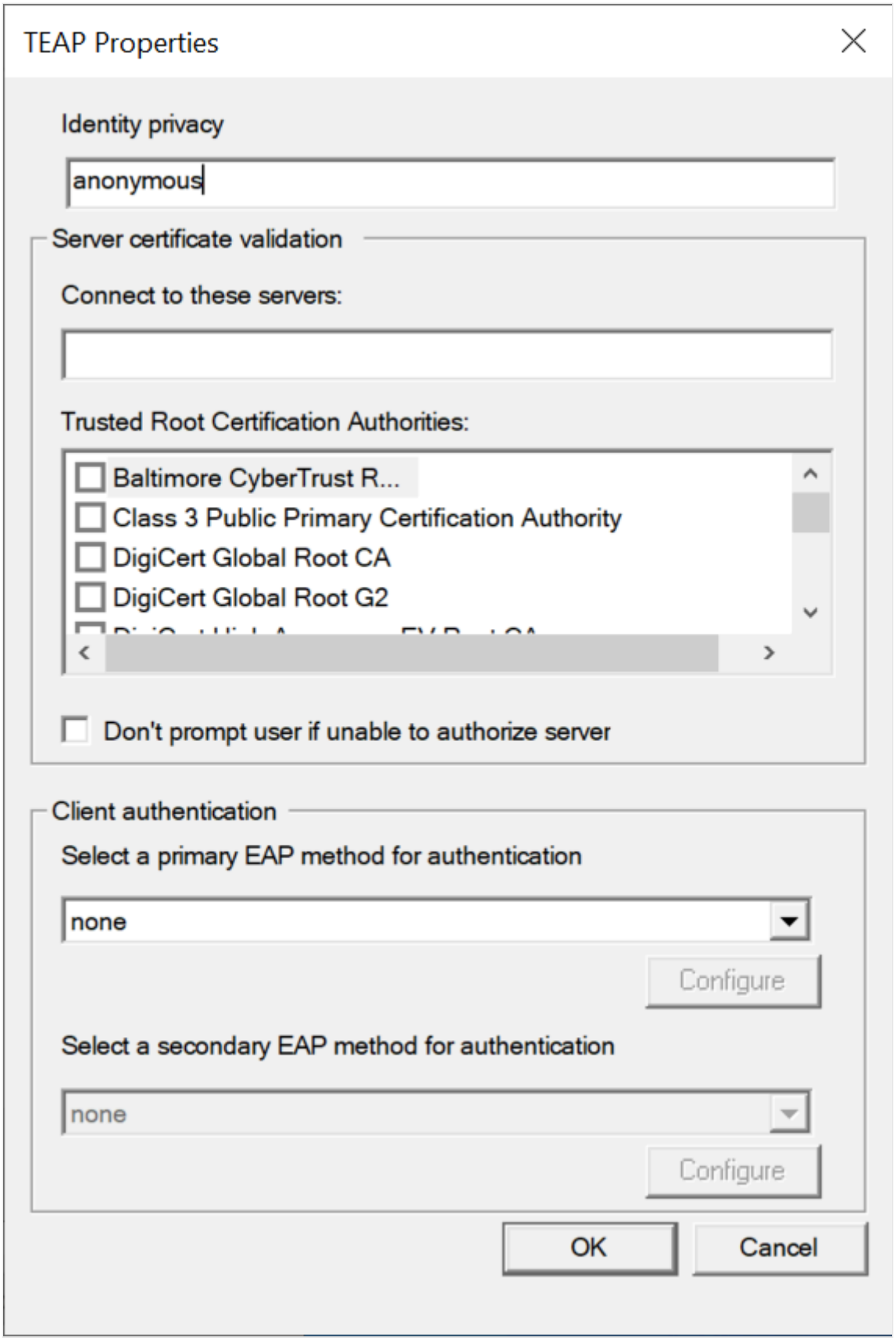
Microsoft : EAP-AKA'

Pour plus d'informations sur cette boîte de dialogue, consultez EAP-AKA ».



Microsoft : EAP-TEAP

Pour plus d'informations sur cette boîte de dialogue, consultez TEAP.



Contenu connexe

- Gestion des paramètres des nouvelles stratégies de réseau sans fil (IEEE 802.11)
- Gestion des paramètres de stratégie du nouveau réseau câblé (IEEE 802.3)
- Paramètres de sécurité avancés pour les stratégies de réseau câblé et sans fil

Passpoint

Passpoint, parfois appelé Point d'accès 2.0, est un standard pour l'authentification transparente auprès des points d'accès. Passpoint offre une connexion chiffrée entre le client et le point d'accès. Il utilise IEEE 802.11u pour communiquer avec le fournisseur avant d'établir une connexion. L'authentification et le chiffrement sont fournis à l'aide de WPA2-Enterprise ou WPA3-Enterprise, ainsi que l'une de plusieurs méthodes EAP.

Le tableau suivant décrit les types d'informations d'identification courants et les combinaisons de méthodes EAP utilisées pour Passpoint, ainsi que la prise en charge correspondante par méthode d'approvisionnement dans Windows 10 et 11.

Agrandir le tableau

type de justificatif	méthode EAP	Provisionnement depuis un site web ou une application	Approvisionnement par MDM ou stratégie de groupe	Provisionné depuis COSA par un opérateur mobile	Inscription en Ligne
Nom d'utilisateur et mot de passe	EAP-TTLS avec MS-CHAP-V2	Oui	Oui	Non	Oui (Windows 11 uniquement)
Nom d'utilisateur et mot de passe	PEAP avec MS-CHAP-V2	Oui	Oui	Non	Non
Nom d'utilisateur et mot de passe	TEAP avec MS-CHAP-V2	Oui	Oui	Non	Non
Certificat	EAP-TLS	Partiel*	Oui	Non	Non
Certificat	PEAP avec EAP-TLS	Partiel*	Oui	Non	Non
Certificat	EAP-TTLS avec EAP-TLS	Partiel*	Oui	Non	Non

type de justificatif	méthode EAP	Provisionnement depuis un site web ou une application	Approvisionnement par MDM ou stratégie de groupe	Provisionné depuis COSA par un opérateur mobile	Inscription en Ligne
Certificat	TEAP avec EAP-TLS	Partiel*	Oui	Non	Non
SIM	EAP-SIM	Oui	Oui	Oui (Windows 11 uniquement)	Non
SIM	EAP-AKA	Oui	Oui	Oui (Windows 11 uniquement)	Non
SIM	EAP-AKA'	Oui	Oui	Oui (Windows 11 uniquement)	Non

*Pour les informations d'identification basées sur des certificats, les certificats ne peuvent pas être directement associés au profil Wi-Fi et installés directement à partir d'un site web ou d'une application UWP. Toutefois, le profil peut toujours être approvisionné et le scénario fonctionne si les certificats sont installés via un autre mécanisme. Par exemple, les certificats peuvent être directement téléchargés et installés par l'utilisateur ou installés via une application Win32.

Méthodes d'approvisionnement

- à partir d'un site web
- à partir d'une application
- De COSA à l'authentification basée sur la carte SIM de l'opérateur mobile
- À partir de MDM, de la stratégie de groupe ou en utilisant des packages de provisionnement.
- Utilisation de l'inscription en ligne (OSU)

  Windows 11 prend en charge osU tel que défini dans la spécification Wi-Fi Alliance Passpoint avec certaines contraintes :
  - SSID d'inscription ouverte (OSEN n'est pas pris en charge)
  - Informations d'identification de nom d'utilisateur et de mot de passe à l'aide de EAP-TTLS (aucune autre méthode d'authentification ou type d'informations d'identification

n’est prise en charge)
    - La remédiation des abonnements et la mise à jour des stratégies ne sont pas prises en charge.

Format du profil

À l’exception de l’inscription en ligne, qui suit le format de PPS-MO standard, toutes les autres méthodes d’approvisionnement s’appuient sur le format XML WLANProfile XML. Les détails spécifiques de Passpoint sont spécifiés dans l’élément Hotspot2.

Informations sur le lieu

À partir de Windows 11, version 23H2, Windows prend en charge la fonctionnalité d'informations sur le lieu Passpoint, ce qui permet aux opérateurs réseau de fournir une URL web HTTPS qui renvoie à davantage d'informations sur le lieu. Lorsque le réseau fournit cette URL, Windows affiche un **lien d'information** sur le lieu en regard du réseau Wi-Fi connecté dans les Paramètres rapides. Pour les connexions automatiques, Windows affiche une notification qui lie directement à l’URL.

Appartenance au consortium itinérant

À compter de Windows 11, version 23H2, Windows inclut l’élément de sélection du consortium itinérant dans les trames de demande d’association si le profil correspondant inclut un identificateur d’organisation de consortium itinérant (RCOI).

Versions antérieures

Windows 8 et Windows 8.1 ne prennent pas en charge les parties de découverte ou d’inscription en ligne de Passpoint, mais elles prennent en charge WPA2-Enterprise et toutes les méthodes EAP requises par la spécification Passpoint. Par conséquent, Windows 8 et Windows 8.1 peuvent se connecter à un réseau passpoint lorsque l’utilisateur dispose déjà d’informations d’identification. Étant donné que Windows 8 et Windows 8.1 ne prennent pas en charge la découverte 802.11u, les opérateurs doivent provisionner Windows 8 ou Windows 8.1 avec des profils sans fil qui contiennent les SSID applicables pour leurs réseaux.

Windows 10 prend entièrement en charge passpoint Release 1, notamment la découverte et la création de profils, mais ne prend pas en charge l’inscription en ligne.

Contenu connexe

- protocole EAP (Extensible Authentication Protocol) pour l’accès réseau

---

Dernière mise à jour : 31/01/2025

Réseaux haute performance (HPN)

Article • 20/12/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local, versions 23H2 and 22H2

Les réseaux haute performance (HPN) jouent un rôle au niveau des besoins en traitement de données en temps réel. Par exemple, les activités telles que la réplication du centre de données, la reprise d'activité après sinistre du centre de données et le calcul distribué haute performance nécessitent un transfert de données en grande quantité ainsi qu'un faible temps de réponse du réseau. Les réseaux HPN offrant des fonctionnalités de connexion dynamique facilitent l'accès aux ressources réseau haute performance et leur gestion. Pour plus d'informations, consultez Configuration réseau requise pour Azure Local.

Les rubriques relatives aux réseaux haute performance sont les suivantes :

- Technologies de déchargement et d'optimisation du réseau
  - Fonctionnalités et technologies logicielles uniquement (SO)
  - Fonctionnalités et technologies intégrées logicielles et matérielles (SH)
  - Fonctionnalités et technologies matérielles uniquement (HO)
  - Propriétés avancées de carte réseau
- RSC dans le commutateur virtuel

Commentaires

Cette page a-t-elle été utile ? Yes No

Technologies de déchargement et d'optimisation du réseau

Article • 21/12/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local, versions 23H2 and 22H2

Dans cette rubrique, nous vous donnons un aperçu des différentes fonctionnalités de déchargement et d'optimisation du réseau disponibles dans Windows Server 2016 et expliquons comment elles contribuent à rendre la mise en réseau plus efficace. Ces technologies incluent les fonctionnalités et technologies logicielles uniquement (SO), les fonctionnalités et technologies intégrées logicielles et matérielles (SH) et les fonctionnalités et technologies matérielles uniquement (HO). Pour plus d'informations, consultez Configuration réseau requise pour Azure Local.

Les trois catégories de fonctionnalités réseau disponibles dans Windows Server 2016 sont les suivantes :

1. Fonctionnalités et technologies logicielles uniquement (SO) : ces fonctionnalités sont implémentées dans le cadre du système d'exploitation et sont indépendantes des cartes réseau sous-jacentes. Parfois, ces fonctionnalités nécessitent un réglage de la carte réseau pour un fonctionnement optimal. Par exemple, les fonctionnalités Hyper-V telles que vmQoS, les ACL et les fonctionnalités non Hyper-V telles que l'association de cartes réseau.

2. Fonctionnalités et technologies intégrées au logiciel et au matériel (SH) : ces fonctionnalités ont à la fois des composants logiciels et matériels. Le logiciel est intimement lié aux fonctionnalités matérielles requises pour que la fonctionnalité fonctionne. Par exemple, VMMQ, VMQ, Déchargement de la somme de contrôle IPv4 côté envoi et RSS.

3. Fonctionnalités et technologies matérielles uniquement (SH) : ces accélérations matérielles améliorent les performances réseau conjointement avec le logiciel, sans faire partie intégrante d'aucune fonctionnalité logicielle. Par exemple, la modération d'interruption, le contrôle de flux et le déchargement de somme de contrôle IPv4 côté réception.

4. Propriétés avancées de la carte réseau : vous pouvez gérer les cartes réseau et toutes les fonctionnalités via Windows PowerShell à l'aide de l'applet de commande NetAdapter. Vous pouvez également gérer les cartes réseau et toutes les fonctionnalités à l'aide du Panneau de configuration réseau (ncpa.cpl).

Conseil

- Les fonctionnalités et technologies SO sont disponibles dans toutes les architectures matérielles, quelles que soient la vitesse de la carte réseau ou les fonctionnalités de carte réseau.
- Les fonctionnalités SH et HO sont disponibles uniquement lorsque votre adaptateur réseau prend en charge les fonctionnalités ou technologies.

Commentaires

Cette page a-t-elle été utile ? Yes No

Fonctionnalités et technologies logicielles uniquement (SO)

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Ces fonctionnalités de logiciel sont implémentées dans le cadre du système d'exploitation et sont indépendantes des cartes réseau sous-jacentes. Parfois, ces fonctionnalités nécessitent un réglage de la carte réseau pour un fonctionnement optimal. Par exemple, les fonctionnalités Hyper-V telles que la qualité de service des machines virtuelles (vmQoS), les listes de contrôle d'accès (ACL) et les fonctionnalités non Hyper-V telles que l'association de cartes réseau. Pour plus d'informations, consultez Configuration réseau requise pour Azure Local.

Listes de contrôle d'accès (ACL)

Une fonctionnalité Hyper-V et SDNv1 pour la gestion de la sécurité d'une machine virtuelle. Cette fonctionnalité s'applique à la pile Hyper-V non virtualisée et à la pile HVNv1. Vous pouvez gérer des listes de contrôle d'accès Hyper-V via des applets de commande PowerShell Add-VMNetworkAdapterAcl et Remove-VMNetworkAdapterAcl .

Listes de contrôle d'accès étendues

Les listes de contrôle d'accès étendues du commutateur virtuel Hyper-V vous permettent de configurer les listes de contrôle d'accès de port étendu du commutateur virtuel Hyper-V pour fournir une protection pare-feu et appliquer des stratégies de sécurité pour les machines virtuelles clientes dans les centres de données. Dans la mesure où les listes de contrôle d'accès des ports sont configurées sur le commutateur virtuel Hyper-V plutôt qu'au sein des ordinateurs virtuels, l'administrateur peut gérer les stratégies de sécurité pour tous les clients dans un environnement mutualisé.

Vous pouvez gérer les listes de contrôle d'accès étendues du commutateur Hyper-V via les applets de commande PowerShell Add-VMNetworkAdapterExtendedAcl et Remove-VMNetworkAdapterExtendedAcl.

Conseil

Cette fonctionnalité s'applique à la pile HNVv1. Pour les listes de contrôle d'accès dans la pile SDN, reportez-vous aux listes de contrôle d'accès réseau à définition logicielle ci-dessous.

Pour plus d'informations sur les listes de contrôle d'accès de ports étendues dans cette bibliothèque, consultez Créer des stratégies de sécurité avec des listes de contrôle d'accès de ports étendues.

Association de cartes réseau

L'association de cartes réseau, également appelée liaison de cartes réseau, est l'agrégation de plusieurs ports de carte réseau dans une entité que l'hôte perçoit comme un seul port de carte réseau. L'association de cartes réseau protège contre la défaillance d'un seul port de carte réseau (ou du câble qui y est connecté). Par ailleurs, elle agrège le trafic réseau pour un débit plus rapide.

Avec Windows Server 2016 vous disposez de deux façons de faire une association :

1. Solution d'association Windows Server 2012
2. Switch Embedded Teaming (SET) de Windows Server 2016

RSC dans le commutateur virtuel (vSwitch)

Receive Segment Coalescing (RSC) dans le vSwitch est une fonctionnalité qui accepte les paquets qui font partie du même flux et qui arrive entre les interruptions réseau et les fusionne en un seul paquet avant de les remettre au système d'exploitation. Le commutateur virtuel dans Windows Server 2019 dispose de cette fonctionnalité. Pour plus d'informations sur cette fonctionnalité, consultez Recevoir la fusion de segments dans le commutateur virtuel.

Listes de contrôle d'accès de mise en réseau SDN (Software Defined Networking)

L'extension SDN dans Windows Server 2016 a amélioré les manières de prendre en charge les listes de contrôle d'accès. Dans la pile Windows Server 2016 SDN v2, listes de contrôle d'accès SDN sont utilisées à la place des listes de contrôle d'accès et des listes de contrôle d'accès étendues. Vous pouvez utiliser le contrôleur de réseau pour gérer les listes de contrôle d'accès SDN.

Qualité de service (QoS) des réseaux à définition logicielle

L'extension SDN dans Windows Server 2016 a amélioré les méthodes pour fournir un contrôle de bande passante (réservations de sortie, limites de sortie et limites d'entrée) sur une base de 5 tuples. En règle générale, ces stratégies sont appliquées au niveau vNIC ou vmNIC, mais vous pouvez les rendre beaucoup plus spécifiques. Dans la pile Windows Server 2016 SDN v2, la QoS SDN est utilisée à la place de vmQoS. Vous pouvez utiliser le contrôleur de réseau pour gérer les QoS SDN.

SET (Switch Embedded Teaming)

SET est une autre solution pour l'association de cartes réseau, que vous pouvez utiliser au sein des environnements qui incluent Hyper-V et la pile SDN (Software-Defined Networking) dans Windows Server 2016. La technologie SET intègre certaines fonctionnalités d'association de NIC dans le commutateur virtuel Hyper-V. Pour plus d'informations sur l'association incorporée du commutateur dans cette bibliothèque, consultez Accès direct à la mémoire à distance (RDMA) et Switch Embedded Teaming (SET).

Mise à l'échelle côté réception virtuelle (vRSS)

Le logiciel vRSS est utilisé pour répartir le trafic entrant destiné à une machine virtuelle sur plusieurs processeurs logiques de la machine virtuelle. Le logiciel vRSS donnent à la machine virtuelle la possibilité de gérer plus de trafic réseau qu'un seul processeur logique ne peut gérer.

Qualité de service des machines virtuelles (vmQoS)

La qualité de service des machines virtuelles est une fonctionnalité Hyper-V qui permet au commutateur de définir des limites sur le trafic généré par chaque machine virtuelle. Il permet également à une machine virtuelle de réserver une quantité de bande passante sur la connexion réseau externe afin qu'une machine virtuelle ne puisse pas priver une autre machine virtuelle de bande passante. Dans la pile Windows Server 2016 SDN v2, SDN QoS remplace vmQoS.

vmQoS peut définir des limites de sortie et des réservations de sortie. Vous devez déterminer le mode de réservation de sortie (poids relatif ou bande passante absolue) avant de créer le commutateur Hyper-V.

- Déterminez le mode de réservation de sortie avec le paramètre –MinimumBandwidthMode de l'applet de commande PowerShell New-VMSwitch.
- Définissez la valeur de la limite de sortie avec le paramètre –MaximumBandwidth sur l'applet de commande PowerShell Set-VMNetworkAdapter.
- Définissez la valeur de la réservation de sortie avec l'un des paramètres suivants de l'applet de commande PowerShell Set VMNetworkAdapter :
  - Si le paramètre –MinimumBandwidthMode sur l'applet de commande New-VMSwitch a la valeur Absolute, définissez le paramètre –MinimumBandwidthAbsolute sur l'applet de commande Set VMNetworkAdapter.
  - Si le paramètre –MinimumBandwidthMode sur l'applet de commande New-VMSwitch a la valeur Absolute, définissez le paramètre –MinimumBandwidthAbsolute sur l'applet de commande Set VMNetworkAdapter.

En raison des limitations de l'algorithme utilisé pour cette fonctionnalité, nous recommandons que le poids le plus élevé ou la bande passante absolue ne soit pas supérieur à 20 fois le poids le plus faible ou la bande passante absolue. Si davantage de contrôle est nécessaire, envisagez d'utiliser la pile SDN et la fonctionnalité SDN-QoS.

Fonctionnalités et technologies intégrées logicielles et matérielles (SH)

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Azure Stack HCI versions 21H2 et 20H2

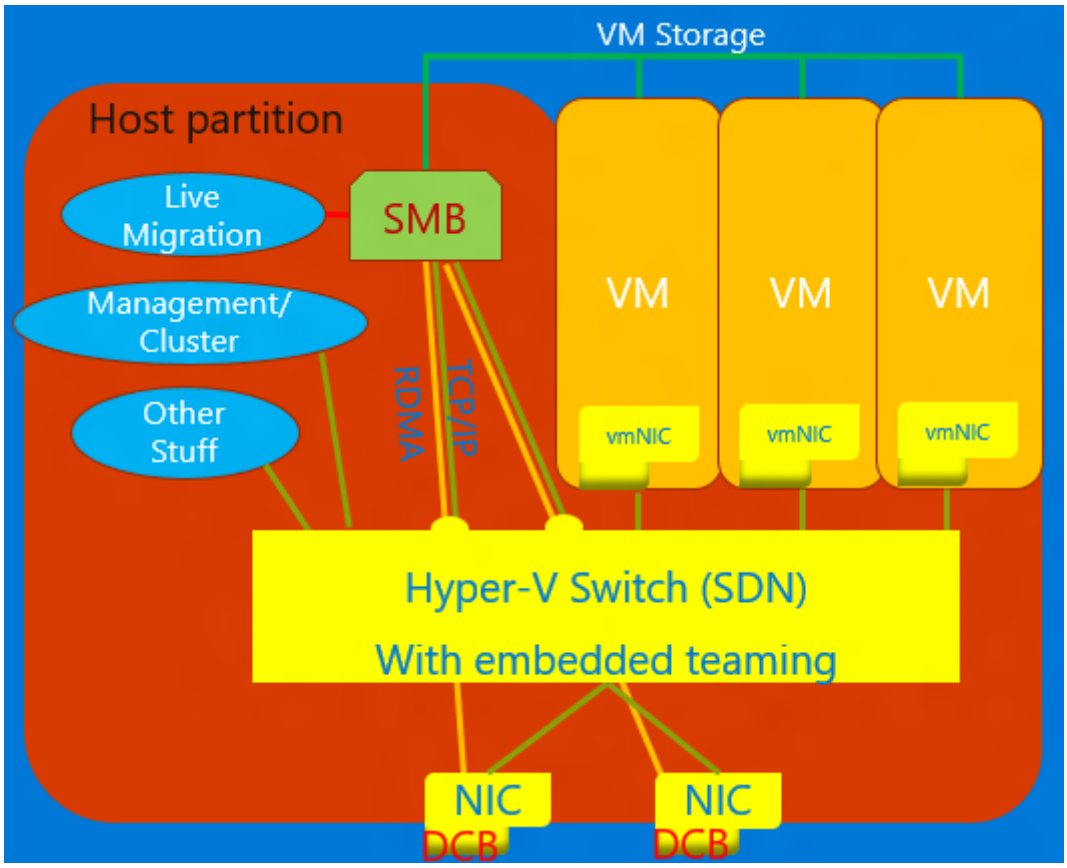
Ces fonctionnalités ont à la fois des composants logiciels et matériels. Le logiciel est intimement lié aux fonctionnalités matérielles requises pour que la fonctionnalité fonctionne. Par exemple, VMMQ, VMQ, Déchargement de la somme de contrôle IPv4 côté envoi et RSS. Pour en savoir plus, consultez Besoins relatifs aux réseaux hôtes pour Azure Stack HCI.

Conseil

Les fonctionnalités SH et HO sont disponibles si la carte réseau installée les prend en charge. Les descriptions de fonctionnalités ci-dessous expliquent comment déterminer si votre carte réseau prend en charge la fonctionnalité.

NIC Convergé

La carte réseau convergée est une technologie qui permet aux cartes réseau virtuelles de l'hôte Hyper-V d'exposer les services RDMA aux processus hôtes. Windows Server 2016 ne nécessite plus de cartes réseau distinctes pour RDMA. La fonctionnalité de carte réseau convergée permet aux cartes réseau virtuelles de la partition hôte (vNIC) d'exposer RDMA à la partition hôte et de partager la bande passante des cartes réseau entre le trafic RDMA et la machine virtuelle et tout autre trafic TCP/UDP de manière équitable et gérable.



Vous pouvez gérer l'opération de carte réseau convergée via VMM ou Windows PowerShell. Les applets de commande PowerShell sont les mêmes que celles utilisées pour RDMA (voir ci-dessous).

Pour utiliser la fonctionnalité de carte réseau convergée :

1. Veillez à configurer l'hôte pour DCB.
2. Veillez à activer RDMA sur la carte réseau ou, dans le cas d'une équipe SET, les cartes réseau sont liées au commutateur Hyper-V.
3. Veillez à activer RDMA sur les cartes réseau virtuelles désignées pour RDMA dans l'hôte.

Pour plus de détails sr Accès direct à la mémoire à distance (RDMA, Remote Direct Memory Access) et SET, consultez RDMA (accès direct à la mémoire à distance) et SET (Switch Embedded Teaming).

DCB (Data Center Bridging)

Le GCN est une suite de normes de l'Institute of Electrical and Electronics Engineers (IEEE) qui permet d'utiliser des tissus convergents dans les centres de données. DCB fournit une gestion de la bande passante basée sur la file d'attente matérielle dans un hôte avec la coopération du commutateur adjacent. Tout le trafic pour le stockage, la

mise en réseau des données, la communication Inter-Process de cluster (IPC) et la gestion partagent la même infrastructure réseau Ethernet. Dans Windows Server 2016, DCB peut être appliqué à n'importe quelle carte réseau individuellement et cartes réseau liées au commutateur Hyper-V.

Pour DCB, Windows Server utilise le contrôle de flux basé sur la priorité (PFC), standardisé dans IEEE 802.1Qbb. PFC crée une infrastructure réseau (presque) sans perte en empêchant le dépassement de capacité dans les classes de trafic. Windows Server utilise également la sélection de transmission améliorée (ETS), standardisée dans IEEE 802.1Qaz. ETS permet la division de la bande passante en parties réservées pour jusqu'à huit classes de trafic. Chaque classe de trafic a sa propre file d'attente de transmission et, grâce à l'utilisation de PFC, peut démarrer et arrêter la transmission au sein d'une classe.

Virtualisation de réseau Hyper-V

Version	Description
v1 (HNVv1)	La virtualisation de réseau Hyper-V (HNV), introduite dans Windows Server 2012, virtualise les réseaux clients sur une infrastructure réseau physique partagée. Les modifications à apporter à l'infrastructure réseau physique étant minimes, HNV confère aux fournisseurs de services l'agilité nécessaire pour déployer et migrer des charges de travail de locataire dans l'ensemble des trois clouds : le cloud du fournisseur de services, le cloud privé ou le cloud public Microsoft Azure.
v2 NVGRE (HNVv2 NVGRE)	Dans Windows Server 2016 et System Center Virtual Machine Manager, Microsoft fournit une solution de virtualisation de réseau de bout en bout qui comprend la passerelle RAS, l'équilibrage de charge logicielle, le contrôleur de réseau, etc. Pour plus d'informations, consultez Vue d'ensemble de la virtualisation de réseau Hyper-V dans Windows Server 2016.
v2 VxLAN (HNVv2 VxLAN)	Dans Windows Server 2016, fait partie de l'extension SDN, que vous gérez via le contrôleur de réseau.

Déchargement de tâches IPsec (IPsecTO)

Le déchargement de tâche IPsec est une fonctionnalité de carte réseau qui permet au système d'exploitation d'utiliser le processeur sur la carte réseau pour le travail de chiffrement IPsec.

> ⓘ **Important**

Le déchargement de tâches IPsec est une technologie héritée qui n'est pas prise en charge par la plupart des cartes réseau et, là où elle existe, elle est désactivée par défaut.

Réseau local virtuel privé (PVLAN).

Les PVLAN autorisent la communication uniquement entre les machines virtuelles sur le même serveur de virtualisation. Un réseau virtuel privé n'est pas lié à une carte réseau physique. Un réseau virtuel privé est isolé de l'ensemble du trafic réseau externe sur le serveur de virtualisation ainsi que tout trafic réseau entre le système d'exploitation de gestion et le réseau externe. Ce type de réseau est utile lorsque vous avez besoin de créer un environnement réseau isolé, comme un domaine de test isolé. Les piles Hyper-V et SDN prennent uniquement en charge le mode port isolé PVLAN.

Pour plus d'informations sur l'isolation PVLAN, consultez System Center : Blog de l'ingénierie Virtual Machine Manager.

Accès direct à la mémoire à distance (RDMA, Remote Direct Memory Access)

RDMA est une technologie de mise en réseau qui fournit une communication à débit élevé et à faible latence qui réduit l'utilisation du processeur. RDMA prend en charge la mise en réseau sans copie en permettant à la carte réseau de transférer des données directement vers ou à partir de la mémoire d'application. Compatible RDMA signifie que la carte réseau (physique ou virtuelle) est capable d'exposer RDMA à un client RDMA. En revanche, avec RDMA, une carte réseau compatible RDMA expose l'interface RDMA dans la pile.

Pour plus de détails sr Accès direct à la mémoire à distance (RDMA, Remote Direct Memory Access), consultez RDMA (accès direct à la mémoire à distance) et SET (Switch Embedded Teaming).

Receive Side Scaling (RSS)

RSS est une fonctionnalité de carte réseau qui sépare différents ensembles de flux et les transmet à différents processeurs pour le traitement. RSS parallélise le traitement réseau, ce qui permet à un hôte de mettre à l'échelle des débits de données très élevés.

Pour plus de détails, consultez Partage du trafic entrant (RSS, Receive Side Scaling).

SR-IOV (Single-Root Input-Output Virtualization)

SR-IOV permet au trafic de machine virtuelle de se déplacer directement de la carte réseau vers la machine virtuelle sans passer par l'hôte Hyper-V. SR-IOV est une amélioration incroyable des performances d'une machine virtuelle, mais l'hôte ne peut pas gérer ce canal. Utilisez SR-IOV uniquement lorsque la charge de travail est bien conduite, approuvée et généralement la seule machine virtuelle de l'hôte.

Le trafic qui utilise SR-IOV contourne le commutateur Hyper-V, ce qui signifie que les stratégies, par exemple les listes de contrôle d'accès ou la gestion de la bande passante, ne seront pas appliquées. Le trafic SR-IOV ne peut pas non plus être transmis via une fonctionnalité de virtualisation réseau. L'encapsulation NV-GRE ou VxLAN ne peut donc pas être appliquée. Utilisez SR-IOV uniquement pour des charges de travail fiables dans des situations spécifiques. En outre, vous ne pouvez pas utiliser les stratégies d'hôte, la gestion de la bande passante et les technologies de virtualisation.

À l'avenir, deux technologies permettront sr-IOV : les tables de flux génériques (GFT) et le déchargement de QoS matérielle (gestion de la bande passante dans la carte réseau) une fois que les cartes réseau de notre écosystème les prennent en charge. La combinaison de ces deux technologies rendrait SR-IOV utile pour toutes les machines virtuelles, permettrait d'appliquer des stratégies, des règles de virtualisation et de gestion de la bande passante, et pourrait entraîner de grands pas en avant dans l'application générale de SR-IOV.

Pour plus d'informations, consultez Vue d'ensemble de la virtualisation d'E/S racine unique (SR-IOV).

Déchargement TCP Chimney

TCP Chimney Offload, également appelé TCP Engine Offload (TOE), est une technologie qui permet à l'hôte de décharger tous les traitements TCP sur la carte réseau. Étant donné que la pile TCP Windows Server est presque toujours plus efficace que le moteur TOE, l'utilisation de TCP Chimney Offload n'est pas recommandée.

> **ⓘ Important**
>
> TCP Chimney Offload est une technologie déconseillée. Nous vous recommandons de ne pas utiliser TCP Chimney Offload, car Microsoft pourrait cesser de le prendre en charge à l'avenir.

Réseau local virtuel (VLAN)

VLAN est une extension de l'en-tête de trame Ethernet pour permettre le partitionnement d'un réseau local en plusieurs réseaux locaux virtuels, chacun utilisant son propre espace d'adressage. Dans Windows Server 2016, les réseaux locaux virtuels sont définis sur les ports du commutateur Hyper-V ou en définissant les interfaces d'équipe sur les équipes d'association de cartes réseau.

File d'attente d'ordinateurs virtuels (VMQ, Virtual Machine Queue)

VMQ est une fonctionnalité de carte réseau qui alloue une file d'attente pour chaque machine virtuelle. Chaque fois qu'Hyper-V est activé ; vous devez également activer VMQ. Dans Windows Server 2016, les VMQs utilisent les vPorts de commutateur de carte réseau avec une seule file d'attente affectée au vPort pour fournir les mêmes fonctionnalités.

VMMQ (Virtual Machine Multi-Queue)

VMMQ est une fonctionnalité de carte réseau qui permet au trafic d'une machine virtuelle de s'étendre sur plusieurs files d'attente, chacune traitée par un processeur physique différent. Le trafic est ensuite passé à plusieurs LPs dans la machine virtuelle comme il le serait dans vRSS, ce qui permet de fournir une bande passante réseau importante à la machine virtuelle.

Fonctionnalités et technologies matérielles uniquement (HO)

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Azure Stack HCI versions 21H2 et 20H2

Ces accélérations matérielles améliorent les performances réseau conjointement avec le logiciel, sans faire partie intégrante d'aucune fonctionnalité logicielle. Par exemple, la modération d'interruption, le contrôle de flux et le déchargement de somme de contrôle IPv4 côté réception. Pour plus d'informations, consultez Configuration réseau requise pour Azure Stack HCI.

Conseil

Les fonctionnalités SH et HO sont disponibles si la carte réseau installée les prend en charge. Les descriptions de fonctionnalités ci-dessous expliquent comment déterminer si votre carte réseau prend en charge la fonctionnalité.

Déchargement de la somme de contrôle d'adresse

Les déchargements de somme de contrôle d'adresse sont une fonctionnalité de carte réseau qui décharge le calcul des sommes de contrôle d'adresse (IP, TCP, UDP) sur le matériel de carte réseau pour l'envoi et la réception.

Sur le chemin de réception, le déchargement de la somme de contrôle calcule les sommes de contrôle dans les en-têtes IP, TCP et UDP (le cas échéant) et indique au système d'exploitation si les sommes de contrôle réussissent, échouent ou sont non vérifiées. Si la carte réseau affirme que les sommes de contrôle sont valides, le système d'exploitation accepte le paquet sans vérification supplémentaire. Si la carte réseau affirme que les sommes de contrôle ne sont pas valides ou ne sont pas vérifiées, la pile IP/TCP/UDP calcule à nouveau les sommes de contrôle en interne. Si la somme de contrôle calculée échoue, le paquet est ignoré.

Sur le chemin d'envoi, le déchargement de la somme de contrôle calcule et insère les sommes de contrôle dans l'en-tête IP, TCP ou UDP, le cas échéant.

La désactivation des déchargements de somme de contrôle sur le chemin d'envoi ne désactive pas le calcul de la somme de contrôle et l'insertion des paquets envoyés au pilote miniport à l'aide de la fonctionnalité LSO (Large Send Offload). Pour désactiver tous les calculs de déchargement de somme de contrôle, l'utilisateur doit également désactiver l'authentification LSO.

Gérer les déchargements de somme de contrôle d'adresse

Dans les propriétés avancées, il existe plusieurs propriétés distinctes :

- Déchargement de somme de contrôle IPv4
- Déchargement de somme de contrôle TCP (IPv4)
- Déchargement de somme de contrôle TCP (IPv6)
- Déchargement de somme de contrôle UDP (IPv4)
- Déchargement de somme de contrôle UDP (IPv6)

Par défaut, toutes ces options sont toujours activées. Nous vous recommandons de toujours activer tous ces déchargements.

Les déchargements de somme de contrôle peuvent être gérés à l'aide des applets de commande Enable-NetAdapterChecksumOffload et Disable-NetAdapterChecksumOffload. Par exemple, l'applet de commande suivante active les calculs de somme de contrôle TCP (IPv4) et UDP (IPv4) :

PowerShell

```
Enable-NetAdapterChecksumOffload -Name * -TcpIPv4 -UdpIPv4
```

Conseils sur l'utilisation des déchargements de somme de contrôle d'adresse

Les déchargements de somme de contrôle d'adresse doivent TOUJOURS être activés, indépendamment de la charge de travail ou des circonstances. Ces technologies de déchargement les plus élémentaires améliorent toujours les performances de votre réseau. Le déchargement de la somme de contrôle est également requis pour que d'autres déchargements sans état fonctionnent, notamment la mise à l'échelle côté réception (RSS), la fusion de segments de réception (RSC) et le déchargement d'envoi volumineux (LSO).

Modération des interruptions (IM)

La modération des interruptions met en mémoire tampon plusieurs paquets reçus avant d'interrompre le système d'exploitation. Lorsqu'une carte réseau reçoit un paquet, elle démarre un minuteur. Lorsque la mémoire tampon est saturée ou que le minuteur expire, selon la première éventualité, la carte réseau interrompt le système d'exploitation.

De nombreuses cartes réseau prennent en charge plus que la simple activation/désactivation de la modération des interruptions. La plupart des cartes réseau prennent en charge les concepts d'un taux faible, moyen et élevé pour la modération des interruptions. Les différents taux représentent des minuteurs plus courts ou longs et des ajustements de taille de mémoire tampon appropriés pour réduire la latence (modération faible des interruptions) ou les interruptions (modération élevée des interruptions).

Il y a un équilibre à trouver entre la réduction des interruptions et le retard excessif de la remise des paquets. En règle générale, le traitement des paquets est plus efficace avec la modération des interruptions activée. Les applications hautes performances ou à faible latence peuvent avoir besoin d'évaluer l'impact de la désactivation ou de la réduction de la modération des interruptions.

Trames Jumbo

Les trames Jumbo sont une fonctionnalité de carte réseau et réseau qui permet à une application d'envoyer des images beaucoup plus volumineuses que les 1 500 octets par défaut. En règle générale, la limite sur les trames Jumbo est d'environ 9 000 octets, mais peut être plus petite.

Aucune modification n'a été apportée à la prise en charge des trames Jumbo dans Windows Server 2012 R2.

Dans Windows Server 2016, vous trouverez un nouveau déchargement : MTU_for_HNV. Ce nouveau déchargement fonctionne avec les paramètres de trames Jumbo pour garantir que le trafic encapsulé ne nécessite pas de segmentation entre l'hôte et le commutateur adjacent. Cette nouvelle fonctionnalité de la pile SDN permet à la carte réseau de calculer automatiquement les MTU à publier et les MTU à utiliser sur le réseau. Ces valeurs de MTU sont différentes si un déchargement HNV est en cours d'utilisation. (Dans la table de compatibilité des fonctionnalités, tableau 1, MTU_for_HNV aurait les mêmes interactions que les déchargements HNVv2, car il est directement lié aux déchargements HNVv2.)

Déchargement d’envoi important (LSO, Large Send Offload)

L’authentification LSO permet à une application de transmettre un grand bloc de données à la carte réseau, et la carte réseau décompose les données en paquets qui correspondent à l’unité de transfert maximale (MTU) du réseau.

Receive Segment Coalescing (RSC)

Receive Segment Coalescing (RSC), également appelé déchargement des réceptions volumineuses, est une fonctionnalité de carte réseau qui accepte les paquets qui font partie du même flux qui arrive entre les interruptions réseau et les fusionne en un seul paquet avant de les remettre au système d’exploitation. RSC n’est pas disponible sur les cartes réseau liées au commutateur virtuel Hyper-V. Pour plus d’informations, consultez Receive Segment Coalescing (RSC).

Propriétés avancées de carte réseau

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez gérer les cartes réseau et toutes les fonctionnalités via Windows PowerShell à l'aide de l'applet de commande NetAdapter. Vous pouvez également gérer les cartes réseau et toutes les fonctionnalités à l'aide du Panneau de configuration réseau (ncpa.cpl). Pour plus d'informations, consultez Configuration réseau requise pour Azure Local.

1. Dans **Windows PowerShell**, exécutez l'applet de commande `Get-NetAdapterAdvancedProperty` sur deux modèles de cartes réseau différentes.

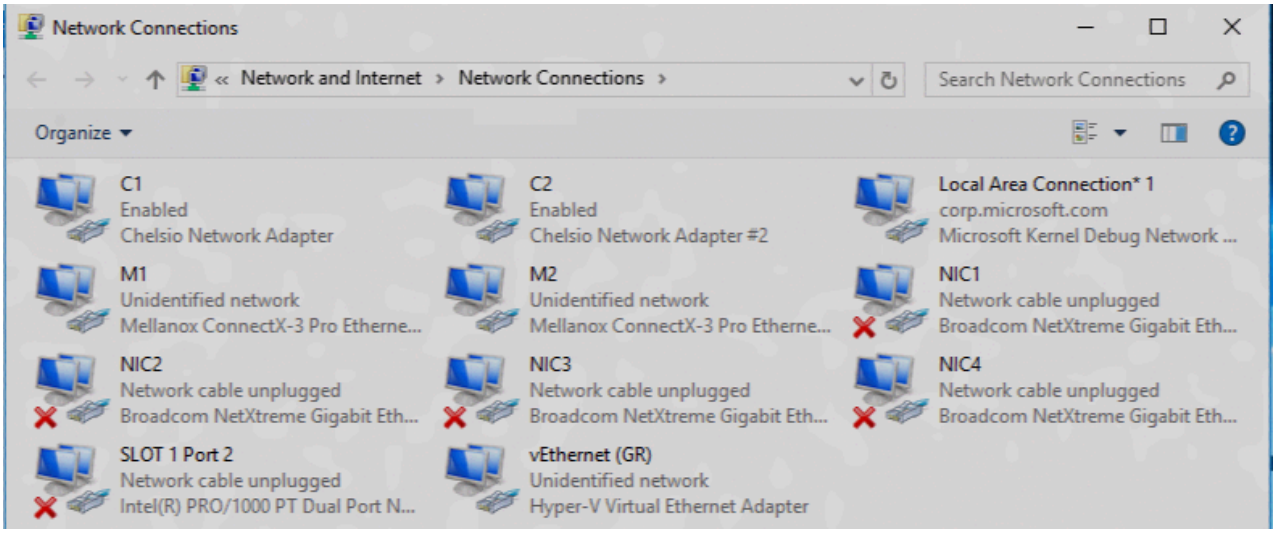
```
PS C:\> Get-NetAdapterAdvancedProperty m1

Name                    DisplayName                    DisplayValue                   RegistryKeyword RegistryValue
----                    -----------                    ------------                   --------------- -------------
M1                      Encapsulated Task Offload      Enabled                        *Encapsulate...  {1}
M1                      Flow Control                   Rx & Tx Enabled                *FlowControl     {3}
M1                      Header Data Split              Disabled                       *HeaderDataS...  {0}
M1                      Interrupt Moderation           Enabled                        *InterruptMo...  {1}
M1                      IPV4 Checksum Offload          Rx & Tx Enabled                *IPChecksumO...  {3}
M1                      Jumbo Packet                   1514                           *JumboPacket     {1514}
M1                      Large Send Offload V2 (IPv4)   Enabled                        *LsoV2IPv4       {1}
M1                      Large Send Offload V2 (IPv6)   Enabled                        *LsoV2IPv6       {1}
M1                      Maximum number of RSS Proce... 8                              *MaxRssProce...  {8}
M1                      NetworkDirect Functionality    Enabled                        *NetworkDirect   {1}
M1                      Preferred NUMA node            Default Settings               *NumaNodeId      {65535}
M1                      Maximum Number of RSS Queues   8                              *NumRSSQueues    {8}
M1                      Priority & Vlan Tag            Priority & VLAN Enabled        *PriorityVLA...  {3}
M1                      Quality Of Service             Enabled                        *QOS             {1}
M1                      Receive Buffers                512                            *ReceiveBuffers  {512}
M1                      Receive Side Scaling           Enabled                        *RSS             {1}
M1                      RSS Base Processor Number      0                              *RssBaseProc...  {0}
M1                      RSS Maximum Processor Number   63                             *RssMaxProcN...  {63}
M1                      RSS load balancing Profile     ClosestProcessor               *RSSProfile      {1}
M1                      SR-IOV                         Enabled                        *Sriov           {1}
M1                      TCP/UDP Checksum Offload (I... Rx & Tx Enabled                *TCPUDPCheck...  {3}
M1                      TCP/UDP Checksum Offload (I... Rx & Tx Enabled                *TCPUDPCheck...  {3}
M1                      Send Buffers                   2048                           *TransmitBuf...  {2048}
M1                      Virtual Machine Queues         Enabled                        *VMQ             {1}
M1                      VMQ VLAN Filtering             Enabled                        *VMQVlanFilt...  {1}
M1                      Force NDK to work with Glob... Disabled                       NdkWithGloba...  {0}
M1                      Locally Administered Address   --                             NetworkAddress   {--}
M1                      Transmit Control Blocks        16                             NumTcb           {16}
M1                      Receive Completion Method      Adaptive                       RecvCompleti...  {1}
M1                      R/RoCE Max Frame Size          Auto                           RoceMaxFrame...  {0}
M1                      Rx Interrupt Moderation Type   Adaptive                       RxIntModeration  {2}
M1                      Rx Interrupt Moderation Pro... Moderate                       RxIntModerat...  {1}
M1                      Number of Polls on Receive     10000                          ThreadPoll       {10000}
M1                      Tx Throughput Port Arbiter     Best Effort (Default)          TxBwPrecedence   {0}
M1                      Tx Interrupt Moderation Pro... Moderate                       TxIntModerat...  {1}
M1                      VLAN ID                        0                              VlanID           {0}
```

```
PS C:\> Get-NetAdapterAdvancedProperty c1

Name                    DisplayName                    DisplayValue                   RegistryKeyword RegistryValue
----                    -----------                    ------------                   --------------- -------------
C1                      Encapsulated Task Offload      Enabled                        *Encapsulate...  {1}
C1                      Flow Control                   Rx & Tx Enabled                *FlowControl     {3}
C1                      IPv4 Checksum Offload          Rx & Tx Enabled                *IPChecksumO...  {3}
C1                      Jumbo Packet                   1500                           *JumboPacket     {1500}
C1                      Large Send Offload V2 (IPv4)   Enabled                        *LsoV2IPv4       {1}
C1                      Large Send Offload V2 (IPv6)   Enabled                        *LsoV2IPv6       {1}
C1                      Maximum Number of RSS proce... 8                              *MaxRssProce...  {8}
C1                      NetworkDirect Functionality    Enabled                        *NetworkDirect   {1}
C1                      Maximum Number of RSS Queues   4                              *NumRSSQueues    {4}
C1                      Recv Segment Coalescing (IPv4) Enabled                        *RSCIPv4         {1}
C1                      Recv Segment Coalescing (IPv6) Enabled                        *RSCIPv6         {1}
C1                      Receive Side Scaling           Enabled                        *RSS             {1}
C1                      RSS Base processor             1                              *RssBaseProc...  {1}
C1                      RSS load balancing profile     NUMA Scaling Static            *RSSProfile      {4}
C1                      TCP Checksum Offload (IPv4)    Rx & Tx Enabled                *TCPChecksum...  {3}
C1                      TCP Checksum Offload (IPv6)    Rx & Tx Enabled                *TCPChecksum...  {3}
C1                      UDP Checksum Offload (IPv4)    Rx & Tx Enabled                *UDPChecksum...  {3}
C1                      UDP Checksum Offload (IPv6)    Rx & Tx Enabled                *UDPChecksum...  {3}
C1                      Virtual Machine Queues         Enabled                        *VMQ             {1}
C1                      VMQ LookAhead Split            Enabled                        *VMQLookahea...  {1}
C1                      VMQ VLAN ID Filtering          Enabled                        *VMQVlanFilt...  {1}
C1                      NetworkDirect Interrupt Mod... Enabled                        NDKIntrModer...  {1}
C1                      Locally Administered Address   --                             NetworkAddress   {--}
C1                      Rx Ethernet Queue Size         2048                           T4NicRespQue...  {2048}
C1                      Rx Offload Queue Size          512                            T4NicRxOfldQ...  {512}
C1                      TCP Offload                    Disabled                       T4NicTCPOffload  {0}
C1                      Tx Offload Queue Size          512                            T4NicTxOfldQ...  {512}
C1                      Tx Ethernet Queue Size         1024                           T4NicTxQueSize   {1024}
C1                      User Mode NetworkDirect        Enabled                        UserModeNetw...  {1}
C1                      VLAN Identifier                0                              VlanID           {0}
```

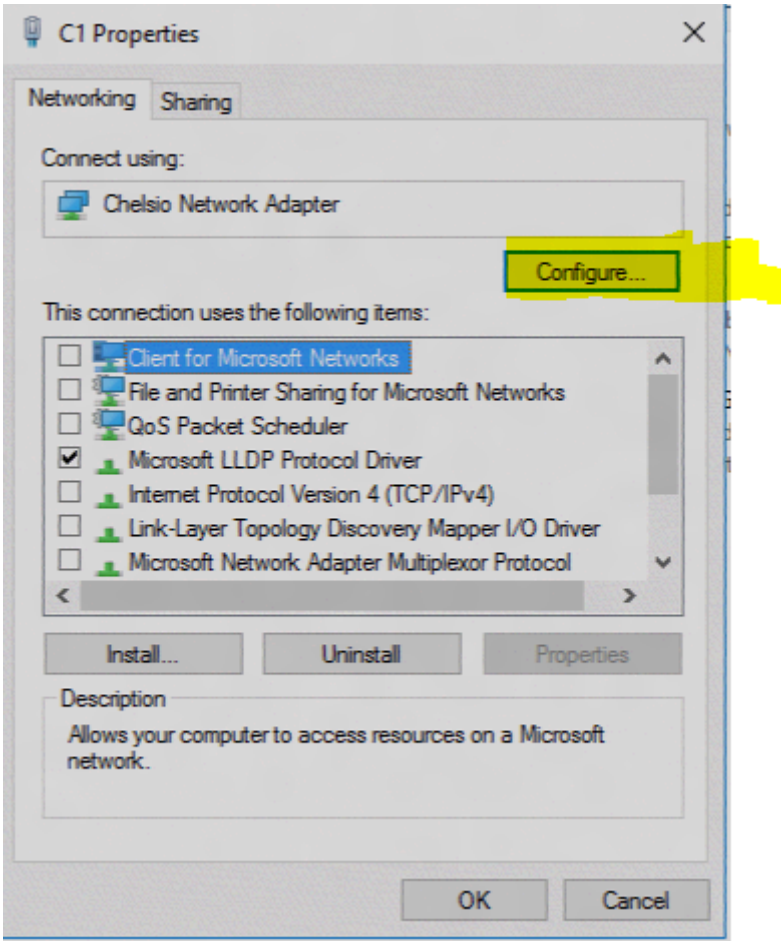
Il existe des similitudes et des différences dans ces deux listes de propriétés avancées de carte réseau.

2. Dans le **Panneau de configuration réseau** (ncpa.cpl), procédez comme suit :

a) Cliquez avec le bouton droit sur la carte réseau.

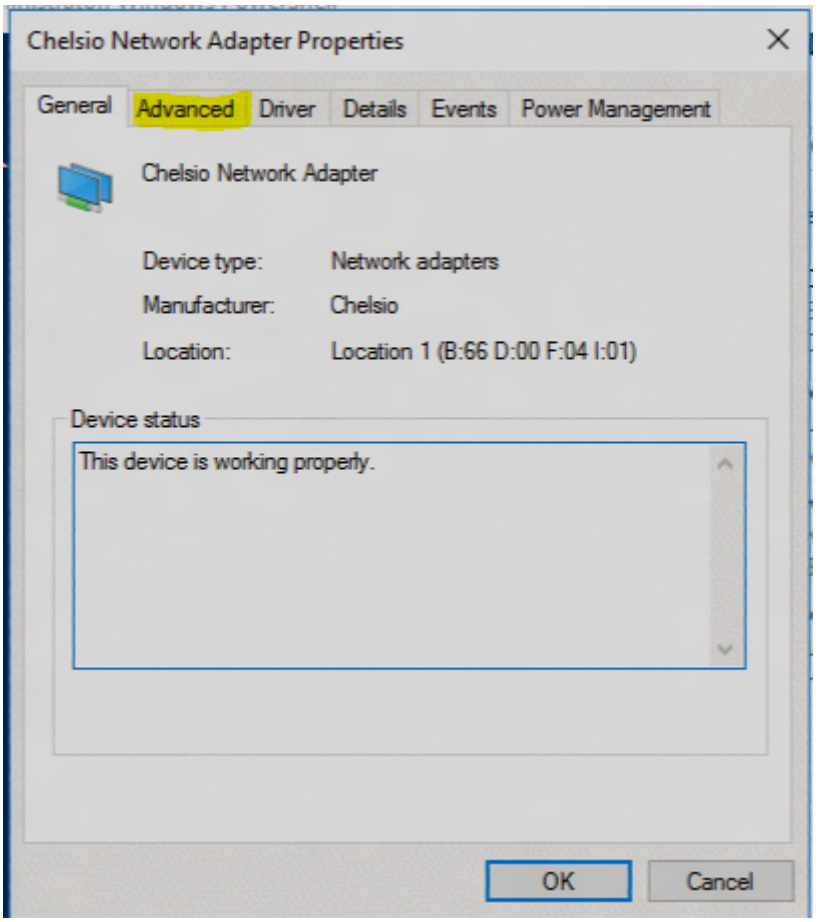


b. Dans la boîte de dialogue des propriétés, cliquez sur **Configurer**.



c. Cliquez sur l'onglet **Avancé** pour afficher les propriétés avancées.

Les éléments de cette liste sont corrélés aux éléments de la sortie `Get-NetAdapterAdvancedProperties`.


Chelsio Network Adapter Properties
General
Advanced
Driver
Details
Events
Power Management
Chelsio Network Adapter
Device type:
Network adapters
Manufacturer:
Chelsio
Location:
Location 1 (B:66 D:00 F:04 I:01)
Device status
This device is working properly.
OK
Cancel

RSC dans le commutateur virtuel (vSwitch)

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Le regroupement de segments de réception (RSC) dans le commutateur virtuel est une fonctionnalité de Windows Server 2019 et Mise à jour d'octobre 2018 de Windows 10 qui permet de réduire l'utilisation du processeur hôte et d'augmenter le débit des charges de travail virtuelles en fusionnant plusieurs segments TCP en segments moins nombreux, mais plus grands. Le traitement de segments moins importants (coalesced) est plus efficace que le traitement de nombreux, petits segments. Pour plus d'informations, consultez Configuration réseau requise pour Azure Local.

Windows Server 2012 et versions ultérieures ont inclus une version de déchargement uniquement matérielle (implémentée dans la carte réseau physique) de la technologie également appelée Coalescing du segment de réception. Cette version déchargée de RSC est toujours disponible dans les versions ultérieures de Windows. Toutefois, il est incompatible avec les charges de travail virtuelles et a été désactivé une fois qu'une carte réseau physique est attachée à un vSwitch. Pour plus d'informations sur la version matérielle uniquement de RSC, consultez Regroupement de segments de réception (RSC).

Scénarios qui tirent parti de RSC dans le vSwitch

Les charges de travail dont le chemin de données traverse un commutateur virtuel bénéficient de cette fonctionnalité.

Par exemple:

- Cartes réseau virtuelles hôtes, notamment :
  - Mise en réseau SDN (Software Defined Networking)
  - hôte Hyper-V
  - Espaces de stockage directs
- Cartes réseau virtuelles invitées Hyper-V
- Passerelles GRE de mise en réseau à définition logicielle
- Container

Les charges de travail qui ne sont pas compatibles avec cette fonctionnalité sont les suivantes :

- Passerelles IPSEC réseau définies par logiciel
- Cartes réseau virtuelles compatibles SR-IOV
- SMB Direct

Configurer RSC dans le vSwitch

Par défaut, sur les commutateurs virtuels externes, RSC est activé.

Afficher les paramètres actuels :

PowerShell

```
Get-VMSwitch -Name vSwitchName | Select-Object *RSC*
```

Activer ou désactiver RSC dans le vSwitch

> ⓘ **Important**
>
> Important : RSC dans le vSwitch peut être activé et désactivé à la volée sans impact sur les connexions existantes.

Désactiver RSC dans le vSwitch

PowerShell

```
Set-VMSwitch -Name vSwitchName -EnableSoftwareRsc $false
```

Ré-activer RSC dans le vSwitch

PowerShell

```
Set-VMSwitch -Name vSwitchName -EnableSoftwareRsc $True
```

Pour plus d'informations, consultez Set-VMSwitch.

API de service HCN (Host Compute Network) pour les machines virtuelles et les conteneurs

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

L'API du service HCN est une API Win32 exposée publiquement qui fournit un accès au niveau de la plateforme pour gérer les réseaux virtuels, les points de terminaison de réseaux virtuels et les stratégies associées. Ensemble, cela fournit la connectivité et la sécurité pour les machines virtuelles et les conteneurs s'exécutant sur un hôte Windows.

Les développeurs utilisent l'API de service HCN pour gérer la mise en réseau des machines virtuelles et des conteneurs dans leurs workflows d'application. L'API HCN a été conçue pour offrir la meilleure expérience aux développeurs. Les utilisateurs finaux n'interagissent pas directement avec ces API.

Fonctionnalités de l'API de service HCN

- Implémenté en tant qu'API C hébergée par le service réseau hôte (HNS) sur l'onCore/machine virtuelle.
- Permet de créer, modifier, supprimer et énumérer des objets HCN tels que des réseaux, des points de terminaison, des espaces de noms et des stratégies. Les opérations s'exécutent sur les handles des objets (par exemple, un handle réseau), et ces handles sont implémentés en interne à l'aide de handles de contexte RPC.
- Schema-based. La plupart des fonctions de l'API définissent les paramètres d'entrée et de sortie sous forme de chaînes contenant les arguments de l'appel de fonction en tant que documents JSON. Les documents JSON sont basés sur des schémas fortement typés et versionnés. Ces schémas font partie de la documentation publique.
- Une API d'abonnement/rappel est fournie pour permettre aux clients de s'inscrire aux notifications d'événements à l'échelle du service, tels que les créations et les suppressions réseau.
- L'API HCN fonctionne dans Pont du bureau (alias Centennial) applications s'exécutant dans les services système. L'API vérifie la liste de contrôle d'accès en récupérant le jeton utilisateur de l'appelant.

> **Conseil**
>
> L'API de service HCN est prise en charge dans les tâches en arrière-plan et les fenêtres non au premier plan.

Terminologie : hôte et calcul

Le service de calcul hôte permet aux appelants de créer et de gérer des machines virtuelles et des conteneurs sur un seul ordinateur physique. Il est nommé pour suivre la terminologie de l'industrie.

- **L'hôte** est largement utilisé dans le secteur de la virtualisation pour faire référence au système d'exploitation qui fournit des ressources virtualisées.
- **Le calcul** est utilisé pour faire référence aux méthodes de virtualisation qui sont plus larges que les machines virtuelles. Le service de réseau de calcul hôte permet aux appelants de créer et de gérer la mise en réseau pour les machines virtuelles et le conteneur sur un seul ordinateur physique.

Documents de configuration basés sur des schémas

Les documents de configuration basés sur des schémas bien définis sont une norme industrielle établie dans l'espace de virtualisation. La plupart des solutions de virtualisation, telles que Docker et Kubernetes, fournissent des API basées sur des documents de configuration. Plusieurs initiatives industrielles, avec la participation de Microsoft, favorisent un écosystème pour définir et valider ces schémas, tels qu'OpenAPI. Ces initiatives pilotent également la normalisation des définitions de schémas spécifiques pour les schémas utilisés pour les conteneurs, comme Open Container Initiative (OCI).

Le langage utilisé pour la création de documents de configuration est JSON, que vous utilisez en combinaison avec :

- Définitions de schéma qui définissent un modèle objet pour le document
- Validation de la conformité d'un document JSON à un schéma
- Conversion automatisée de documents JSON vers et à partir de représentations natives de ces schémas dans les langages de programmation utilisés par les appelants des API

Les définitions de schéma fréquemment utilisées sont OpenAPI et JSON Schema, ce qui vous permet de spécifier les définitions détaillées des propriétés dans un document, par

exemple :

- Ensemble de valeurs valide pour une propriété, par exemple 0-100 pour une propriété représentant un pourcentage.
- Définition d'énumérations, qui sont représentées sous la forme d'un ensemble de chaînes valides pour une propriété.
- Expression régulière pour le format attendu d'une chaîne.

Dans le cadre de la documentation des API HCN, nous prévoyons de publier le schéma de nos documents JSON en tant que spécification OpenAPI. Sur la base de cette spécification, les représentations spécifiques au langage du schéma peuvent permettre une utilisation sans risque de type des objets de schéma dans le langage de programmation utilisé par le client.

Example

Voici un exemple de flux de travail pour l'objet représentant un contrôleur SCSI dans le document de configuration d'une machine virtuelle.

```
enum IpamType
{
    [NewIn("2.0")] Static,
    [NewIn("2.0")] Dhcp,
};
class Ipam
{
    // Type : dhcp
    [NewIn("2.0"),OmitEmpty] IpamType   Type;
    [NewIn("2.0"),OmitEmpty] Subnet     Subnets[];
};
class Subnet : HCN.Schema.Common.Base
{
    [NewIn("2.0"),OmitEmpty] string         IpAddressPrefix;
    [NewIn("2.0"),OmitEmpty] SubnetPolicy   Policies[];
    [NewIn("2.0"),OmitEmpty] Route          Routes[];
};
enum SubnetPolicyType
{
    [NewIn("2.0")] VLAN
};
class SubnetPolicy
{
    [NewIn("2.0"),OmitEmpty] SubnetPolicyType                Type;
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Common.PolicySettings Data;
};
class PolicySettings
{
    [NewIn("2.0"),OmitEmpty]  string      Name;
```

```
};
class VlanPolicy : HCN.Schema.Common.PolicySettings
{
    [NewIn("2.0")] uint32 IsolationId;
};
class Route
{
    [NewIn("2.0"),OmitEmpty] string NextHop;
    [NewIn("2.0"),OmitEmpty] string DestinationPrefix;
    [NewIn("2.0"),OmitEmpty] uint16 Metric;
};
```

Conseil

Les annotations [NewIn(« 2.0 ») font partie de la prise en charge du contrôle de version pour les définitions de schéma. À partir de cette définition interne, nous générons les spécifications OpenAPI pour le schéma :

```
{
    "swagger" : "2.0",
    "info" : {
       "version" : "2.1",
       "title" : "HCN API"
    },
    "definitions": {
        "Ipam": {
            "type": "object",
            "properties": {
                "Type": {
                    "type": "string",
                    "enum": [
                        "Static",
                        "Dhcp"
                    ],
                    "description": " Type : dhcp"
                },
                "Subnets": {
                    "type": "array",
                    "items": {
                        "$ref": "#/definitions/Subnet"
                    }
                }
            }
        },
        "Subnet": {
            "type": "object",
            "properties": {
                "ID": {
                    "type": "string",
```

```
                    "pattern": "^[0-9A-Fa-f]{8}-([0-9A-Fa-f]{4}-){3}[0-9A-Fa-f]
{12}$"
                },
                "IpAddressPrefix": {
                    "type": "string"
                },
                "Policies": {
                    "type": "array",
                    "items": {
                        "$ref": "#/definitions/SubnetPolicy"
                    }
                },
                "Routes": {
                    "type": "array",
                    "items": {
                        "$ref": "#/definitions/Route"
                    }
                }
            }
        },
        "SubnetPolicy": {
            "type": "object",
            "properties": {
                "Type": {
                    "type": "string",
                    "enum": [
                        "VLAN",
                        "VSID"
                    ]
                },
                "Data": {
                    "$ref": "#/definitions/PolicySettings"
                }
            }
        },
        "PolicySettings": {
            "type": "object",
            "properties": {
                "Name": {
                    "type": "string"
                }
            }
        },
        "VlanPolicy": {
            "type": "object",
            "properties": {
                "Name": {
                    "type": "string"
                },
                "IsolationId": {
                    "type": "integer",
                    "format": "uint32"
                }
            }
        },
```

```
        "Route": {
            "type": "object",
            "properties": {
                "NextHop": {
                    "type": "string"
                },
                "DestinationPrefix": {
                    "type": "string"
                },
                "Metric": {
                    "type": "integer",
                    "format": "uint16"
                }
            }
        }
    }
}
```

Vous pouvez utiliser des outils, tels que Swagger, pour générer des représentations spécifiques au langage du langage de programmation de schéma utilisé par un client. Swagger prend en charge divers langages tels que C#, Go, Javascript et Python).

- Exemple de code C# généré pour l'objet IPAM et de sous-réseau de niveau supérieur.
- Exemple de code Go généré pour l'objet IPAM et de sous-réseau de niveau supérieur. Go est utilisé par Docker et Kubernetes, qui sont deux des consommateurs des API du service de réseau de calcul hôte. Go dispose d'une prise en charge intégrée pour le marshaling des types Go vers et à partir de documents JSON.

En plus de la génération et de la validation du code, vous pouvez utiliser des outils pour simplifier le travail avec les documents JSON, c'est-à-dire Visual Studio Code.

Objets de niveau supérieur définis dans le schéma HCN

Les objets de niveau supérieur sont les suivants :

- HostComputeNetwork
- HostComputeEndpoint
- HostComputeNamespace
- HostComputeLoadBalancer

```
class HostComputeNetwork : HCN.Schema.Common.Base
{
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.NetworkMode          Type;
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.NetworkPolicy        Policies[];
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.MacPool              MacPool;
```

```
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.DNS                 Dns;
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.Ipam                Ipams[];
};
class HostComputeEndpoint : HCN.Schema.Common.Base
{
    [NewIn("2.0"),OmitEmpty] string
HostComputeNetwork;
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.Endpoint.EndpointPolicy
Policies[];
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.Endpoint.IpConfig
IpConfigurations[];
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.DNS                    Dns;
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Network.Route                  Routes[];
    [NewIn("2.0"),OmitEmpty] string
MacAddress;
};
class HostComputeNamespace : HCN.Schema.Common.Base
{
    [NewIn("2.0"),OmitEmpty] uint32
NamespaceId;
    [NewIn("2.0"),OmitEmpty] Guid
NamespaceGuid;
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Namespace.NamespaceType        Type;
    [NewIn("2.0"),OmitEmpty] HCN.Schema.Namespace.NamespaceResource
Resources[];
};
class HostComputeLoadBalancer : HCN.Schema.Common.Base
{
    [NewIn("2.0"), OmitEmpty] string
HostComputeEndpoints[];
    [NewIn("2.0"), OmitEmpty] string
VirtualIPs[];
    [NewIn("2.0"), OmitEmpty] HCN.Schema.Network.Endpoint.Policy.PortMappingPolicy
PortMappings[];
    [NewIn("2.0"), OmitEmpty] HCN.Schema.LoadBalancer.LoadBalancerPolicy
Policies[];
};
```

Étapes suivantes

- En savoir plus sur les scénarios HCN courants.
- En savoir plus sur les handles de contexte RPC pour HCN.
- En savoir plus sur les schémas de document JSON HCN.

Scénarios courants

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Scénario : HCN

Créer un HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour créer un réseau de calcul hôte sur l'hôte qui peut être utilisé pour connecter des cartes réseau virtuelles à des Machines Virtuelles ou des conteneurs.

C++

```
using unique_hcn_network = wil::unique_any<
    HCN_NETWORK,
    decltype(&HcnCloseNetwork),
    HcnCloseNetwork>;
/// Creates a simple HCN Network, waiting synchronously to finish the task
void CreateHcnNetwork()
{
    unique_hcn_network hcnnetwork;
    wil::unique_cotaskmem_string result;
    std::wstring settings = LR"(
    {
        "SchemaVersion": {
            "Major": 2,
            "Minor": 0
        },
        "Owner" : "WDAGNetwork",
        "Flags" : 0,
        "Type"  : 0,
        "Ipams" : [
            {
                "Type" : 0,
                "Subnets" : [
                    {
                        "IpAddressPrefix" : "192.168.1.0/24",
                        "Policies" : [
                            {
                                "Type" : "VLAN",
                                "IsolationId" : 100,
                            }
                        ],
                        "Routes" : [
                            {
```

```
                                "NextHop" : "192.168.1.1",
                                "DestinationPrefix" : "0.0.0.0/0",
                            }
                        ]
                    }
                ],
            },
        ],
        "MacPool":  {
            "Ranges" : [
                {
                    "EndMacAddress":  "00-15-5D-52-CF-FF",
                    "StartMacAddress":  "00-15-5D-52-C0-00"
                }
            ],
        },
        "Dns" : {
            "Suffix" : "net.home",
            "ServerList" : ["10.0.0.10"],
        }
    }
    })";
    GUID networkGuid;
    HRESULT result = CoCreateGuid(&networkGuid);
    result = HcnCreateNetwork(
        networkGuid,              // Unique ID
        settings.c_str(),      // Compute system settings document
        &hcnnetwork,
        &result
        );
    if (FAILED(result))
    {
                    // UnMarshal  the result Json
     // ErrorSchema
        //   {
        //    "ErrorCode" : <uint32>,
        //    "Error" : <string>,
        //    "Success" : <bool>,
       //   }
        // Failed to create network
        THROW_HR(result);
    }
    // Close the Handle
    result = HcnCloseNetwork(hcnnetwork.get());
    if (FAILED(result))
    {
        // UnMarshal  the result Json
        THROW_HR(result);
    }
}
```

Supprimer un HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour ouvrir & Supprimer un réseau de calcul hôte

C++

```
    wil::unique_cotaskmem_string errorRecord;
    GUID networkGuid; // Initialize it to appropriate network guid value
    HRESULT hr = HcnDeleteNetwork(networkGuid, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal the result Json
        THROW_HR(hr);
    }
```

Énumérer tous les réseaux

Cet exemple montre comment utiliser l'API Du service de réseau de calcul hôte pour énumérer tous les réseaux de calcul hôtes.

C++

```
     wil::unique_cotaskmem_string resultNetworks;
     wil::unique_cotaskmem_string errorRecord;
     // Filter to select Networks based on properties
     std::wstring filter [] = LR"(
     {
         "Name"  : "WDAG",
     })";
     HRESULT result = HcnEnumerateNetworks(filter.c_str(), &resultNetworks,
&errorRecord);
     if (FAILED(result))
     {
         // UnMarshal  the result Json
         THROW_HR(result);
     }
```

Interroger les propriétés du réseau

Cet exemple montre comment utiliser l'API de service réseau de calcul hôte pour interroger les propriétés du réseau.

C++

```
    unique_hcn_network hcnnetwork;
    wil::unique_cotaskmem_string errorRecord;
    wil::unique_cotaskmem_string properties;
    std:wstring query = LR"(
```

```
    {
        // Future
    })";
    GUID networkGuid; // Initialize it to appropriate network guid value
    HRESULT hr = HcnOpenNetwork(networkGuid, &hcnnetwork, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
    hr = HcnQueryNetworkProperties(hcnnetwork.get(), query.c_str(),
&properties, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Scénario : point de terminaison HCN

Créer un point de terminaison HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour créer un point de terminaison de réseau de calcul hôte, puis l'ajouter à chaud à la machine virtuelle ou à un conteneur.

C++

```
using unique_hcn_endpoint = wil::unique_any<
    HCN_ENDPOINT,
    decltype(&HcnCloseEndpoint),
    HcnCloseEndpoint>;
void CreateAndHotAddEndpoint()
{
    unique_hcn_endpoint hcnendpoint;
    unique_hcn_network hcnnetwork;
    wil::unique_cotaskmem_string errorRecord;
    std::wstring settings[] = LR"(
    {
        "SchemaVersion": {
            "Major": 2,
            "Minor": 0
        },
        "Owner" : "Sample",
                    "Flags" : 0,
        "HostComputeNetwork" : "87fdcf16-d210-426e-959d-2a1d4f41d6d3",
        "DNS" : {
            "Suffix" : "net.home",
            "ServerList" : "10.0.0.10",
        }
```

```
    })";
    GUID endpointGuid;
    HRESULT result = CoCreateGuid(&endpointGuid);
    result = HcnOpenNetwork(
        networkGuid,              // Unique ID
        &hcnnetwork,
        &errorRecord
        );
    if (FAILED(result))
    {
        // Failed to find network
        THROW_HR(result);
    }
    result = HcnCreateEndpoint(
        hcnnetwork.get(),
        endpointGuid,              // Unique ID
        settings.c_str(),      // Compute system settings document
        &hcnendpoint,
        &errorRecord
        );
    if (FAILED(result))
    {
        // Failed to create endpoint
        THROW_HR(result);
    }
    // Can use the sample from HCS API Spec on how to attach this endpoint
    // to the VM using AddNetworkAdapterToVm
    result = HcnCloseEndpoint(hcnendpoint.get());
    if (FAILED(result))
    {
        // UnMarshal  the result Json
        THROW_HR(result);
    }
}
```

Supprimer un point de terminaison

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour supprimer un point de terminaison de réseau de calcul hôte.

C++

```
    wil::unique_cotaskmem_string errorRecord;
    GUID endpointGuid; // Initialize it to appropriate endpoint guid value
    HRESULT hr = HcnDeleteEndpoint(endpointGuid, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Modifier un point de terminaison

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour modifier un point de terminaison de réseau de calcul hôte.

C++

```
    unique_hcn_endpoint hcnendpoint;
    GUID endpointGuid; // Initialize it to appropriate endpoint guid value
    HRESULT hr = HcnOpenEndpoint(endpointGuid, &hcnendpoint, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
    std::wstring  ModifySettingAddPortJson = LR"(
    {
        "ResourceType" : 0,
        "RequestType" : 0,
        "Settings" : {
            "PortName" : "acbd341a-ec08-44c0-9d5e-61af0ee86902"
            "VirtualNicName" : "641313e1-7ae8-4ddb-94e5-3215f3a0b218-
-87fdcf16-d210-426e-959d-2a1d4f41d6d1"
            "VirtualMachineId" : "641313e1-7ae8-4ddb-94e5-3215f3a0b218"
        }
    }
    )";
    hr = HcnModifyEndpoint(hcnendpoint.get(),
ModifySettingAddPortJson.c_str(), &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Énumérer tous les points de terminaison

Cet exemple montre comment utiliser l'API Du service de réseau de calcul hôte pour énumérer tous les points de terminaison de réseau de calcul hôte.

C++

```
    wil::unique_cotaskmem_string errorRecord;
    wil::unique_cotaskmem_string resultEndpoints;
    wil::unique_cotaskmem_string errorRecord;
    // Filter to select Endpoint based on properties
    std::wstring filter [] = LR"(
    {
        "Name"  : "sampleNetwork",
    })";
```

```
    result = HcnEnumerateEndpoints(filter.c_str(), &resultEndpoints,
&errorRecord);
    if (FAILED(result))
    {
        THROW_HR(result);
    }
```

Propriétés du point de terminaison de requête

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour interroger toutes les propriétés d'un point de terminaison de réseau de calcul hôte.

C++

```
    unique_hcn_endpoint hcnendpoint;
    wil::unique_cotaskmem_string errorRecord;
    GUID endpointGuid; // Initialize it to appropriate endpoint guid value
    HRESULT hr = HcnOpenEndpoint(endpointGuid, &hcnendpoint, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
    wil::unique_cotaskmem_string properties;
    std:wstring query = LR"(
    {
        // Future
    })";
    hr = HcnQueryEndpointProperties(hcnendpoint.get(), query.c_str(),
&properties, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the errorRecord Json
        THROW_HR(hr);
    }
```

Scénario : espace de noms HCN

Créer un espace de noms HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour créer un espace de noms de réseau de calcul hôte sur l'hôte qui peut être utilisé pour connecter des points de terminaison et des conteneurs.

C++

```
using unique_hcn_namespace = wil::unique_any<
    HCN_NAMESPACE,
    decltype(&HcnCloseNamespace),
    HcnCloseNamespace>;
/// Creates a simple HCN Network, waiting synchronously to finish the task
void CreateHcnNamespace()
{
    unique_hcn_namespace handle;
    wil::unique_cotaskmem_string errorRecord;
    std::wstring settings = LR"(
    {
        "SchemaVersion": {
            "Major": 2,
            "Minor": 0
        },
        "Owner" : "Sample",
        "Flags" : 0,
        "Type" : 0,
    })";
    GUID namespaceGuid;
    HRESULT result = CoCreateGuid(&namespaceGuid);
    result = HcnCreateNamespace(
        namespaceGuid,              // Unique ID
        settings.c_str(),      // Compute system settings document
        &handle,
        &errorRecord
        );
    if (FAILED(result))
    {
                    // UnMarshal  the result Json
     // ErrorSchema
        //   {
        //    "ErrorCode" : <uint32>,
        //    "Error" : <string>,
        //    "Success" : <bool>,
       //   }
        // Failed to create network
        THROW_HR(result);
    }
    result = HcnCloseNamespace(handle.get());
    if (FAILED(result))
    {
        // UnMarshal  the result Json
        THROW_HR(result);
    }
}
```

Supprimer un espace de noms HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour supprimer un espace de noms de réseau de calcul hôte.

```C++
    wil::unique_cotaskmem_string errorRecord;
    GUID namespaceGuid; // Initialize it to appropriate namespace guid value
    HRESULT hr = HcnDeleteNamespace(namespaceGuid, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal the result Json
        THROW_HR(hr);
    }
```

Supprimer un espace de noms HCN

Cet exemple montre comment utiliser l'API Du service de réseau de calcul hôte pour modifier un espace de noms de réseau de calcul hôte.

```C++
    unique_hcn_namespace handle;
    GUID namespaceGuid; // Initialize it to appropriate namespace guid value
    HRESULT hr = HcnOpenNamespace(namespaceGuid, &handle, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
    wil::unique_cotaskmem_string errorRecord;
    static std::wstring  ModifySettingAddEndpointJson = LR"(
    {
        "ResourceType" : 1,
        "RequestType" : 0,
        "Settings" : {
            "EndpointId" : "87fdcf16-d210-426e-959d-2a1d4f41d6d1"
        }
    }
    )";
    hr = HcnModifyNamespace(handle.get(),
ModifySettingAddEndpointJson.c_str(), &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal the result Json
        THROW_HR(hr);
    }
    hr = HcnCloseNamespace(handle.get());
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Énumérer tous les espaces de noms

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour énumérer tous les espaces de noms de réseau de calcul hôte.

C++

```
    wil::unique_cotaskmem_string resultNamespaces;
    wil::unique_cotaskmem_string errorRecord;
    std::wstring filter [] = LR"(
    {
            // Future
    })";
    HRESULT hr = HcnEnumerateNamespace(filter.c_str(), &resultNamespaces,
&errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Propriétés de l'espace de noms de requête

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour interroger les propriétés de l'espace de noms du réseau de calcul hôte

C++

```
    unique_hcn_namespace handle;
    GUID namespaceGuid; // Initialize it to appropriate namespace guid value
    HRESULT hr = HcnOpenNamespace(namespaceGuid, &handle, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
    wil::unique_cotaskmem_string errorRecord;
    wil::unique_cotaskmem_string properties;
    std:wstring query = LR"(
    {
        // Future
    })";
    HRESULT hr = HcnQueryNamespaceProperties(handle.get(), query.c_str(),
&properties, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Scénario : équilibreur de charge HCN

Créer un équilibreur de charge HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour créer un réseau de calcul hôte Équilibreur de charge sur l'hôte qui peut être utilisé pour équilibrer la charge du point de terminaison entre le calcul.

C++

```
using unique_hcn_loadbalancer = wil::unique_any<
    HCN_LOADBALANCER,
    decltype(&HcnCloseLoadBalancer),
    HcnCloseLoadBalancer>;
/// Creates a simple HCN LoadBalancer, waiting synchronously to finish the
task
void CreateHcnLoadBalancer()
{
    unique_hcn_loadbalancer handle;
    wil::unique_cotaskmem_string errorRecord;
    std::wstring settings = LR"(
     {
        "SchemaVersion": {
            "Major": 2,
            "Minor": 0
        },
        "Owner" : "Sample",
        "HostComputeEndpoints" : [
            "87fdcf16-d210-426e-959d-2a1d4f41d6d1"
        ],
        "VirtualIPs" : [ "10.0.0.10" ],
        "PortMappings" : [
            {
                "Protocol" : 0,
                "InternalPort" : 8080,
                "ExternalPort" : 80,
            }
        ],
        "EnableDirectServerReturn" : true,
        "InternalLoadBalancer" : false,
    }
     )";
    GUID lbGuid;
    HRESULT result = CoCreateGuid(&lbGuid);
    HRESULT hr = HcnCreateLoadBalancer(
        lbGuid,               // Unique ID
        settings.c_str(),      // LoadBalancer settings document
        &handle,
        &errorRecord
        );
    if (FAILED(hr))
```

```
    {
                    // UnMarshal  the result Json
     // ErrorSchema
        //   {
        //    "ErrorCode" : <uint32>,
        //    "Error" : <string>,
        //    "Success" : <bool>,
       //   }
        // Failed to create network
        THROW_HR(hr);
    }
    hr = HcnCloseLoadBalancer(handle.get());
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
}
```

Supprimer un équilibreur de charge HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour supprimer un équilibreur de charge de réseau de calcul hôte.

C++

```
    wil::unique_cotaskmem_string errorRecord;
    GUID lbGuid; // Initialize it to appropriate loadbalancer guid value
    HRESULT hr = HcnDeleteLoadBalancer(lbGuid , &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal the result Json
        THROW_HR(hr);
    }
```

Modifier un équilibreur de charge HCN

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour modifier un équilibreur de charge de réseau de calcul hôte.

C++

```
    unique_hcn_loadbalancer handle;
    GUID lbGuid; // Initialize it to appropriate loadbalancer guid value
    HRESULT hr = HcnOpenLoadBalancer(lbGuid, &handle, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
```

```
        THROW_HR(hr);
    }
    wil::unique_cotaskmem_string errorRecord;
    static std::wstring  ModifySettingAddEndpointJson = LR"(
    {
        "ResourceType" : 1,
        "RequestType" : 0,
        "Settings" : {
            "EndpointId" : "87fdcf16-d210-426e-959d-2a1d4f41d6d1"
        }
    }
    )";
    hr = HcnModifyLoadBalancer(handle.get(),
ModifySettingAddEndpointJson.c_str(), &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal the result Json
        THROW_HR(hr);
    }
    hr = HcnCloseLoadBalancer(handle.get());
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Énumérer tous les équilibreurs de charge

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour énumérer toutes les équilibreurs de charge du réseau de calcul hôte.

C++

```
    wil::unique_cotaskmem_string resultLoadBalancers;
    wil::unique_cotaskmem_string errorRecord;
    std::wstring filter [] = LR"(
    {
         // Future
    })";
    HRESULT result = HcnEnumerateLoadBalancers(filter.c_str(), &
resultLoadbalancers, &errorRecord);
    if (FAILED(result))
    {
            // UnMarshal  the result Json
            THROW_HR(result);
    }
```

Requête propriétés de l'équilibreur de charge

Cet exemple montre comment utiliser l'API de service de réseau de calcul hôte pour interroger les propriétés équilibreur de charge du réseau de calcul hôte.

C++

```
    unique_hcn_loadbalancer handle;
    GUID lbGuid; // Initialize it to appropriate loadbalancer guid value
    HRESULT hr = HcnOpenLoadBalancer(lbGuid, &handle, &errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
    wil::unique_cotaskmem_string errorRecord;
    wil::unique_cotaskmem_string properties;
    std:wstring query = LR"(
    {
        "ID"  : "",
        "Type" : 0,
    })";
    hr = HcnQueryNProperties(handle.get(), query.c_str(), &properties,
&errorRecord);
    if (FAILED(hr))
    {
        // UnMarshal  the result Json
        THROW_HR(hr);
    }
```

Scénario : notifications HCN

Inscrire et annuler l'inscription des notifications à l'échelle du service

Cet exemple montre comment utiliser l'API de service réseau de calcul hôte pour inscrire et annuler l'inscription aux notifications à l'échelle du service. Cela permet à l'appelant de recevoir une notification (via la fonction de rappel qu'il a spécifiée lors de l'inscription) chaque fois qu'une opération à l'échelle du service telle qu'un événement de création de réseau s'est produite.

C++

```
using unique_hcn_callback = wil::unique_any<
    HCN_CALLBACK,
    decltype(&HcnUnregisterServiceCallback),
    HcnUnregisterServiceCallback>;
// Callback handle returned by registration api. Kept at
// global or module scope as it will automatically be
```

```
// unregistered when it goes out of scope.
unique_hcn_callback g_Callback;
// Event notification callback function.
void
CALLBACK
ServiceCallback(
    DWORD   NotificationType,
    void*   Context,
    HRESULT NotificationStatus,
    PCWSTR  NotificationData)
{
    // Optional client context
    UNREFERENCED_PARAMETER(context);
    // Reserved for future use
    UNREFERENCED_PARAMETER(NotificationStatus);
    switch (NotificationType)
    {
        case HcnNotificationNetworkCreate:
            // TODO: UnMarshal the NotificationData
            //
            // // Notification
            // {
            //     "ID" : Guid,
            //     "Flags" : <uint32>,
            // };
            break;
        case HcnNotificationNetworkDelete:
            // TODO: UnMarshal the NotificationData
            break;
        Default:
            // TODO: handle other events.
            break;
    }
}
/// Register for service-wide notifications
void RegisterForServiceNotifications()
{
    THROW_IF_FAILED(HcnRegisterServiceCallback(
        ServiceCallback,
        nullptr,
        &g_Callback));
}
/// Unregister from service-wide notifications
void UnregisterForServiceNotifications()
{
    // As this is a unique_hcn_callback, this will cause
HcnUnregisterServiceCallback to be invoked
    g_Callback.reset();
}
```

Étapes suivantes

- En savoir plus sur les handles de contexte RPC pour HCN.
- En savoir plus sur les schémas de document JSON HCN.

Commentaires

Cette page a-t-elle été utile ? Yes No

Poignées de contexte RPC pour HCN

30/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

HCN_Network

Un réseau HCN est une entité utilisée pour représenter un réseau informatique hôte et les ressources système et stratégies associées. Un réseau HCN peut généralement inclure :

- Un ensemble de métadonnées (ID, nom, type)
- Un commutateur virtuel
- Une carte réseau virtuelle hôte (agissant comme passerelle par défaut pour le réseau)
- Une instance NAT (si nécessaire par le type de réseau)
- Un ensemble de sous-réseaux et de pools MAC
- Toutes les stratégies à l'échelle du réseau à appliquer (par exemple, les listes de contrôle d'accès)

Les entités réseau HCN sont représentées à l'aide des handles de contexte RPC HCN_NETWORK.

```
/// Handle to an operation
DECLARE_HANDLE(HCN_NETWORK);
/// Return a list of existing Networks
///
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing properties of the specific Networks to
///                        return. By default, all networks are returned.
/// \retval Networks       Receives a JSON document with the list of Networks.
/// \retval ErrorRecord    Optional, receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnEnumerateNetworks(
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* Networks,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Create a Network
///
```

```
/// \param  Id              Specifies the unique ID for the new Network.
/// \param  Settings        JSON document specifying the settings of the new
Network.
/// \retval Network         Receives a handle to the new network.
/// \retval ErrorRecord     Optional. Receives a JSON document on failure with
extended result
///                         information. The caller must release the buffer using
///                         CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnCreateNetwork(
    _In_ REFGUID Id,
    _In_ PCWSTR Settings,
    _Out_ PHCN_NETWORK Network,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Opens a handle to an existing Network.
///
/// \param  Id              Unique ID of the existing network.
/// \retval Network         Receives a handle to the network.
/// \retval ErrorRecord     Optional. Receives a JSON document on failure with
extended result
///                         information. The caller must release the buffer using
///                         CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnOpenNetwork(
    _In_ REFGUID Id,
    _Out_ PHCN_NETWORK Network,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Modify the settings of a Network
///
/// \param  Network         Handle to a network.
/// \param  Settings        JSON document specifying the new settings of the
network.
/// \retval ErrorRecord     Optional. Receives a JSON document on failure with
extended result
///                         information. The caller must release the buffer using
///                         CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnModifyNetwork(
    _In_ HCN_NETWORK Network,
    _In_ PCWSTR Settings,
    _Outptr_opt_ PWSTR* ErrorRecord
```

```
    );
/// Query Network properties
///
/// \param  Network        Handle to a network.
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing specific properties of the network
///                        return. By default all properties are returned.
/// \retval Properties     Receives a JSON document with Network properties.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnQueryNetworkProperties(
    _In_ HCN_NETWORK Network,
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* Properties,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Delete a Network
///
/// \param  Id             Unique ID of the existing network.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnDeleteNetwork(
    _In_ REFGUID Id,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Close a handle to a Network
///
/// \param  Network        Handle to a network.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnCloseNetwork(
    _In_ HCN_NETWORK Network
    );
```

HCN_Endpoint

Un point de terminaison HCN est une entité utilisée pour représenter un point de terminaison IP sur un réseau HCN et les ressources système et stratégies associées. Un point de terminaison HCN se compose généralement des éléments suivants :

- Un ensemble de métadonnées (ID, nom, ID réseau parent)
- Son identité réseau (adresse IP, adresse MAC)
- Toutes les stratégies spécifiques au point de terminaison à appliquer (ACL, itinéraires)

Les entités de point de terminaison HCN sont représentées à l'aide des handles de contexte RPC HCN_ENDPOINT.

```
/// Handle to an operation
DECLARE_HANDLE(HCN_ENDPOINT);
/// Return a list of existing endpoints
///
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing properties of the specific endpoints to
///                        return. By default all Endpoints are returned.
/// \retval Endpoints      Receives a JSON document with the list of endpoints.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnEnumerateEndpoints(
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* Endpoints,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Create an Endpoint
///
/// \param  Id             Specifies the unique ID for the new endpoint.
/// \param  Network        Handle to the network on which endpoint is to be
created.
/// \param  Settings       JSON document specifying the settings of the new
endpoint.
/// \retval Endpoint       Receives a handle to the new endpoint.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
```

```
HcnCreateEndpoint(
    _In_ HCN_NETWORK Network,
    _In_ REFGUID Id,
    _In_ PCWSTR Settings,
    _Out_ PHCN_ENDPOINT Endpoint,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Opens a handle to an existing Endpoint.
///
/// \param  Id             Unique ID of the existing endpoint.
/// \retval Endpoint       Receives a handle to the endpoint.
/// \retval ErrorRecord    Optional, receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnOpenEndpoint(
    _In_ REFGUID Id,
    _Out_ PHCN_ENDPOINT Endpoint,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Modify the settings of an Endpoint
///
/// \param  Endpoint       Handle to an endpoint.
/// \param  Settings       JSON document specifying the new settings of the
endpoint.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnModifyEndpoint(
    _In_ HCN_ENDPOINT Endpoint,
    _In_ PCWSTR Settings,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Query Endpoint properties
///
/// \param  Endpoint       Handle to an endpoint.
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing specific properties of the endpoint
///                        return. By default all properties are returned.
/// \retval Properties     Receives a JSON document with endpoint properties.
/// \retval ErrorRecord    Optional, receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
```

```
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnQueryEndpointProperties(
    _In_ HCN_ENDPOINT Endpoint,
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* Properties,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Delete an Endpoint
///
/// \param  Id             Unique ID of the existing endpoint.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnDeleteEndpoint(
    _In_ REFGUID Id,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Close a handle to an endpoint
///
/// \param  Endpoint       Handle to an endpoint.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnCloseEndpoint(
    _In_ HCN_ENDPOINT Endpoint
    );
```

HCN_Namespace

Un espace de noms HCN est une entité utilisée pour représenter un espace de noms de réseau de calcul hôte. Les espaces de noms vous permettent de disposer d'environnements réseau isolés sur un seul hôte, où chaque espace de noms a ses propres interfaces réseau et sa propre table de routage, qui sont séparées des autres espaces de noms.

Les entités d'espace de noms HCN sont représentées à l'aide des handles de contexte RPC HCN_NAMESPACE.

```
/// Handle to an operation
DECLARE_HANDLE(HCN_NAMESPACE);
/// Return a list of existing namespaces
///
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing properties of the specific namespaces to
///                        return. By default all Namespaces are returned.
/// \retval Namespaces     Receives a JSON document with the list of namespaces.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnEnumerateNamespaces(
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* Namespaces,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Create a Namespace
///
/// \param  Id             Specifies the unique ID for the new namespace.
/// \param  Settings       JSON document specifying the settings of the new
namespace.
/// \retval Namespace      Receives a handle to the new namespace.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnCreateNamespace(
    _In_ REFGUID Id,
    _In_ PCWSTR Settings,
    _Out_ PHCN_NAMESPACE Namespace,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Opens a handle to an existing namespace.
///
/// \param  Id             Unique ID of the existing namespace.
/// \retval Namespace      Receives a handle to the namespace.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
```

```
HRESULT
WINAPI
HcnOpenNamespace(
    _In_ REFGUID Id,
    _Out_ PHCN_NAMESPACE Namespace,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Modify the settings of a namespace
///
/// \param  Namespace      Handle to a namespace.
/// \param  Settings       JSON document specifying the new settings of the
namespace.
/// \retval ErrorRecord    Optional, receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnModifyNamespace(
    _In_ HCN_NAMESPACE Namespace,
    _In_ PCWSTR Settings,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Query Namespace properties
///
/// \param  Namespace      Handle to a namespace.
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing specific properties of the namespace
///                        return. By default all properties are returned.
/// \retval Properties     Receives a JSON document with Namespace properties.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnQueryNamespaceProperties(
    _In_ HCN_NAMESPACE Namespace,
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* Properties,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Delete a Namespace
///
/// \param  Id             Unique ID of the existing namespace.
/// \retval ErrorRecord    Optional. Receives a JSON document on failure with
extended result
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
```

```
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnDeleteNamespace(
    _In_ REFGUID Id,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Close a handle to a Namespace
///
/// \param  Namespace      Handle to a namespace.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnCloseNamespace(
    _In_ HCN_NAMESPACE Namespace
    );
```

HCN_LoadBalancer

Un équilibreur de charge HCN est une entité utilisée pour représenter un équilibreur de charge de réseau de calcul hôte. Les équilibreurs de charge vous permettent de disposer de points de terminaison de réseau de calcul hôte à charge équilibrée. Les entités d'équilibreur de charge HCN sont représentées à l'aide des handles de contexte RPC HCN_LOADBALANCER.

```
/// Handle to an operation
DECLARE_HANDLE(HCN_LOADBALANCER);
//////
/// LoadBalancer methods
/// Return a list of existing load balancers
///
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing properties of the specific load balancers to
///                        return. By default all load balancers are returned.
/// \retval LoadBalancers    Receives a JSON document with the list of load
balancers.
/// \retval ErrorRecord    Optional. Receives a JSON document with extended
errorCode
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnEnumerateLoadBalancers(
```

```
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* LoadBalancer,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Create a load balancer
///
/// \param  Id             Specifies the unique ID for the new load balancer.
/// \param  Settings       JSON document specifying the settings of the new load
balancer.
/// \retval LoadBalancer     Receives a handle to the new LoadBalancer.
/// \retval ErrorRecord    Optional. Receives a JSON document with extended
errorCode
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnCreateLoadBalancer(
    _In_ REFGUID Id,
    _In_ PCWSTR Settings,
    _Out_ PHCN_LOADBALANCER LoadBalancer,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Opens a handle to an existing LoadBalancer.
///
/// \param  Id             Unique ID of the existing load balancer.
/// \retval LoadBalancer     Receives a handle to the load balancer.
/// \retval ErrorRecord    Optional. Receives a JSON document with extended
errorCode
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnOpenLoadBalancer(
    _In_ REFGUID Id,
    _Out_ PHCN_LOADBALANCER LoadBalancer,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Modify the settings of a PolcyList
///
/// \param  PolcyList      Handle to a PolcyList.
/// \param  Settings       JSON document specifying the new settings of the
PolcyList.
/// \retval ErrorRecord    Optional, receives a JSON document with extended
errorCode
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
```

```
HRESULT
WINAPI
HcnModifyLoadBalancer(
    _In_ HCN_LOADBALANCER LoadBalancer,
    _In_ PCWSTR Settings,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Query LoadBalancer properties
///
/// \param  LoadBalancer     Handle to a load balancer.
/// \param  Query          Optionally specifies a JSON document for a query
///                        containing specific properties of the load balancer
///                        return. By default all properties are returned.
/// \retval Properties     Receives a JSON document with LoadBalancer properties.
/// \retval ErrorRecord    Optional, receives a JSON document with extended
errorCode
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnQueryLoadBalancerProperties(
    _In_ HCN_LOADBALANCER LoadBalancer,
    _In_ PCWSTR Query,
    _Outptr_ PWSTR* Properties,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Delete a LoadBalancer
///
/// \param  Id             Unique ID of the existing load balancer.
/// \retval ErrorRecord    Optional. Receives a JSON document with extended
errorCode
///                        information. The caller must release the buffer using
///                        CoTaskMemFree.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnDeleteLoadBalancer(
    _In_ REFGUID Id,
    _Outptr_opt_ PWSTR* ErrorRecord
    );
/// Close a handle to a LoadBalancer
///
/// \param  LoadBalancer     Handle to a load balancer.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT
WINAPI
HcnCloseLoadBalancer(
    _In_ HCN_LOADBALANCER LoadBalancer
```

HCN_Notification_Callback

Ces fonctions permettent d'accéder à des opérations à l'échelle du service, telles que les notifications (par exemple, la réception de notifications relatives à la création d'un nouveau réseau).

```
/// Registers a callback function to receive notifications of service-wide events
such as network
/// creations/deletions.
///
/// \param  Callback           Function pointer to notification callback.
/// \param  Context            Context pointer.
/// \retval CallbackHandle     Receives a handle to a callback registered on a
service.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT WINAPI
HcnRegisterServiceCallback(
    _In_ HCN_NOTIFICATION_CALLBACK Callback,
    _In_ void* Context,
    _Out_ HCN_CALLBACK* CallbackHandle
    );
/// Unregisters from service-wide notifications
///
/// \retval CallbackHandle     Handle to a callback registered on a service.
///
/// \returns S_OK if successful; HResult error code on failures.
///
HRESULT WINAPI
HcnUnregisterServiceCallback(
    _In_ HCN_CALLBACK CallbackHandle
    );
```

Schémas de document HCN JSON

31/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

HCN schema

JSON

```
// Network
{
    "Id" : <string>,
    "Owner" : <string>,
    "SchemaVersion" : {
        "Major" : <uint32>,
        "Minor" : <uint32>
    },
    "Flags" : <enum bit mask>,
         // AsString; Values:
         // "None" (0),
         // "EnableDnsProxy" (1),
         // "EnableDhcpServer" (2),
         // "IsolateVSwitch" (8)
    "Type"  : <enum>,
         // AsString; Values:
         // "NAT" (0),
         // "ICS" (1),
         // "Transparent" (2)
    "Ipams" : [ {
         "Type" : <enum>,
             // AsString; Values:
             // "Static" (0),
             // "Dhcp" (1)
         "Subnets" : [ {
                "IpAddressPrefix" : <ip prefix in CIDR>,
                "Policies" : [ {
                        "Type" : <enum>,
                            // AsString; Values:
                            // "VLAN" (0)
                        "Data" : <any>
                 } ],
                "Routes" : [ {
                       "NextHop" : <ip address of the next hop gateway>,
                       "DestinationPrefix" : <ip prefix in cidr>,
                       "Metric" : <route metric in uint8>,
                 } ],
          } ],
     } ],
    "Policies" : [{
         "Type" : <enum>,
```

```
                // AsString; Values:
                // "NetAdapterName" (1),
                // "InterfaceConstraint" (2)
            "Data" : <any>
        }],
        "Dns" : {
            "Suffix" : <local connection specific suffix>,
            "Search" : [<list of additional suffixes>],
            "ServerList" : [<string>],
            "Options" : [<string>],
        },
        "MacPool" : {
            "Ranges" : [ {
                "StartMacAddress" : <string>,
                "EndMacAddress" : <string>
            } ],
        },
    }
```

Schéma de point de terminaison HCN

JSON

```
// Endpoint
{
    "Id" : <string>,
    "Owner" : <string>,
    "SchemaVersion" : {
        "Major" : <uint32>,
        "Minor" : <uint32>
    },
    "Flags" : <enum bit mask>,
        // AsString; Values:
        // "None" (0),
        // "DisableInterComputeCommunication" (2)
    "HostComputeNetwork" : <string>,
    "MacAddress" : <string>,
    "Policies" : [ {
        "Type" : <enum>,
            // AsString; Values:
            // "PortMapping" (0),
            // "ACL" (1)
        "Data" : <any>
    } ],
    "Dns" : {
        "Suffix" : <local connection specific suffix>,
        "Search" : [<list of additional suffixes>],
        "ServerList" : [<string>],
        "Options" : [<string>],
    },
    "IPConfigurations" : [ {
        "IPAddress" : <ip address>,
```

```
        "PrefixLength" : <prefix length uint16>,
    } ],
    "Routes" : [ {
        "NextHop" : <ip address of the next hop gateway>,
        "DestinationPrefix" : <ip prefix in cidr>,
        "Metric" : <route metric in uint8>,
    } ],
}
```

Schéma de stratégie HCN

JSON

```
// VlanPolicy
{
    "Type" : "VLAN",
    "IsolationId" : <uint32>,
}
// PortMappingPolicy
{
    "Type" : "PortMapping",
    "Protocol" : <enum>,
         // AsString; Values:
         // "Unknown" (0),
         // "ICMPv4" (1),
         // "IGMP" (2),
         // "TCP" (6),
         // "UDP" (17),
         // "ICMPv6" (58)
    "InternalPort" : <uint16>,
    "ExternalPort" : <uint16>,
}
```

Schéma de l’équilibreur de charge HCN

JSON

```
// Host Compute LoadBalancer
{
    "Id" : <string>,
    "Owner" : <string>,
    "SchemaVersion" : {
        "Major" : <uint32>,
        "Minor" : <uint32>
    },
    "Flags" : <enum bit mask>,
         // AsString; Values:
         // "None" (0),
         // "EnableDirectServerReturn" (1)
```

```
          // "EnableInternalLoadBalancer" (2)
    "HostComputeEndpoints" : [<Host compute Endpoint id>],
    "VirtualIPs" : [<Virtual IpAddress>],
    "PortMappings" : [ {
        "Type" : "PortMapping",
        "Protocol" : <enum>,
            // AsString; Values:
            // "Unknown" (0),
            // "ICMPv4" (1),
            // "IGMP" (2),
            // "TCP" (6),
            // "UDP" (17),
            // "ICMPv6" (58)
        "InternalPort" : <uint16>,
        "ExternalPort" : <uint16>,
    } ],
    "Policies" : [ {
         "Type" : <enum>,
             // AsString; Values:
             // "SourceVirtualIp" (0),
         "Data" : <any>
    } ],
}
```

Schéma d’espace de noms HCN

JSON

```
// Namespace
{
    "Id" : <string>,
    "Owner" : <string>,
    "SchemaVersion" : {
        "Major" : <uint32>,
        "Minor" : <uint32>
    },
    "NamespaceId" : <uint32>,
    "NamespaceGuid" : <guid>,
    "Type"  : <enum>,
              // AsString; Values:
              // "Host" (0),
              // "HostDefault" (1),
              // "Guest" (2),
              // "GuestDefault" (3)
    "Resources" : [ {
          "Type"  : <enum>,
              // AsString; Values:
              // "Container" (0),
              // "Endpoint" (1)
          "Data"  : <any>
```

```
    } ],
}
```

Schéma de notification HCN

JSON

```
// Notification
{
    "ID" : Guid,
    "Flags" : <uint32>,
};
```

Schéma d’erreur de résultat

JSON

```
// ErrorSchema
{
    "ErrorCode" : <uint32>,
    "Error" : <string>,
    "Success" : <bool>,
}
```

Exemple de code généré par C#

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

C#

```
/*
 * HCN API
 *
 * No description provided (generated by Swagger Codegen https://github.com/swagger-
api/swagger-codegen)
 *
 * OpenAPI spec version: 2.1
 *
 * Generated by: https://github.com/swagger-api/swagger-codegen.git
 */
using System;
using System.Linq;
using System.IO;
using System.Text;
using System.Text.RegularExpressions;
using System.Collections;
using System.Collections.Generic;
using System.Collections.ObjectModel;
using System.Runtime.Serialization;
using Newtonsoft.Json;
using Newtonsoft.Json.Converters;
using System.ComponentModel.DataAnnotations;
using SwaggerDateConverter = IO.Swagger.Client.SwaggerDateConverter;
namespace IO.Swagger.Model
{
    /// <summary>
    /// Ipam
    /// </summary>
    [DataContract]
    public partial class Ipam :  IEquatable<Ipam>, IValidatableObject
    {
        /// <summary>
        ///  Type : dhcp
        /// </summary>
        /// <value> Type : dhcp</value>
        [JsonConverter(typeof(StringEnumConverter))]
        public enum TypeEnum
        {
            /// <summary>
            /// Enum Static for value: Static
            /// </summary>
            [EnumMember(Value = "Static")]
            Static = 1,
```

```
            /// <summary>
            /// Enum Dhcp for value: Dhcp
            /// </summary>
            [EnumMember(Value = "Dhcp")]
            Dhcp = 2
        }
        /// <summary>
        ///  Type : dhcp
        /// </summary>
        /// <value> Type : dhcp</value>
        [DataMember(Name="Type", EmitDefaultValue=false)]
        public TypeEnum? Type { get; set; }
        /// <summary>
        /// Initializes a new instance of the <see cref="Ipam" /> class.
        /// </summary>
        /// <param name="Type"> Type : dhcp.</param>
        /// <param name="Subnets">Subnets.</param>
        public Ipam(TypeEnum? Type = default(TypeEnum?), List<Subnet> Subnets =
default(List<Subnet>))
        {
            this.Type = Type;
            this.Subnets = Subnets;
        }
        /// <summary>
        /// Gets or Sets Subnets
        /// </summary>
        [DataMember(Name="Subnets", EmitDefaultValue=false)]
        public List<Subnet> Subnets { get; set; }
        /// <summary>
        /// Returns the string presentation of the object
        /// </summary>
        /// <returns>String presentation of the object</returns>
        public override string ToString()
        {
            var sb = new StringBuilder();
            sb.Append("class Ipam {\n");
            sb.Append("  Type: ").Append(Type).Append("\n");
            sb.Append("  Subnets: ").Append(Subnets).Append("\n");
            sb.Append("}\n");
            return sb.ToString();
        }
        /// <summary>
        /// Returns the JSON string presentation of the object
        /// </summary>
        /// <returns>JSON string presentation of the object</returns>
        public string ToJson()
        {
            return JsonConvert.SerializeObject(this, Formatting.Indented);
        }
        /// <summary>
        /// Returns true if objects are equal
        /// </summary>
        /// <param name="input">Object to be compared</param>
        /// <returns>Boolean</returns>
        public override bool Equals(object input)
```

```
        {
            return this.Equals(input as Ipam);
        }
        /// <summary>
        /// Returns true if Ipam instances are equal
        /// </summary>
        /// <param name="input">Instance of Ipam to be compared</param>
        /// <returns>Boolean</returns>
        public bool Equals(Ipam input)
        {
            if (input == null)
                return false;
            return
                (
                    this.Type == input.Type ||
                    (this.Type != null &&
                    this.Type.Equals(input.Type))
                ) &&
                (
                    this.Subnets == input.Subnets ||
                    this.Subnets != null &&
                    this.Subnets.SequenceEqual(input.Subnets)
                );
        }
        /// <summary>
        /// Gets the hash code
        /// </summary>
        /// <returns>Hash code</returns>
        public override int GetHashCode()
        {
            unchecked // Overflow is fine, just wrap
            {
                int hashCode = 41;
                if (this.Type != null)
                    hashCode = hashCode * 59 + this.Type.GetHashCode();
                if (this.Subnets != null)
                    hashCode = hashCode * 59 + this.Subnets.GetHashCode();
                return hashCode;
            }
        }
        /// <summary>
        /// To validate all properties of the instance
        /// </summary>
        /// <param name="validationContext">Validation context</param>
        /// <returns>Validation Result</returns>
        IEnumerable<System.ComponentModel.DataAnnotations.ValidationResult>
IValidatableObject.Validate(ValidationContext validationContext)
        {
            yield break;
        }
    }
}
/*
 * HCN API
 *
```

```
 * No description provided (generated by Swagger Codegen https://github.com/swagger-
api/swagger-codegen)
 *
 * OpenAPI spec version: 2.1
 *
 * Generated by: https://github.com/swagger-api/swagger-codegen.git
 */
using System;
using System.Linq;
using System.IO;
using System.Text;
using System.Text.RegularExpressions;
using System.Collections;
using System.Collections.Generic;
using System.Collections.ObjectModel;
using System.Runtime.Serialization;
using Newtonsoft.Json;
using Newtonsoft.Json.Converters;
using System.ComponentModel.DataAnnotations;
using SwaggerDateConverter = IO.Swagger.Client.SwaggerDateConverter;
namespace IO.Swagger.Model
{
    /// <summary>
    /// Subnet
    /// </summary>
    [DataContract]
    public partial class Subnet :  IEquatable<Subnet>, IValidatableObject
    {
        /// <summary>
        /// Initializes a new instance of the <see cref="Subnet" /> class.
        /// </summary>
        /// <param name="ID">ID.</param>
        /// <param name="IpAddressPrefix">IpAddressPrefix.</param>
        /// <param name="Policies">Policies.</param>
        /// <param name="Routes">Routes.</param>
        public Subnet(string ID = default(string), string IpAddressPrefix =
default(string), List<SubnetPolicy> Policies = default(List<SubnetPolicy>),
List<Route> Routes = default(List<Route>))
        {
            this.ID = ID;
            this.IpAddressPrefix = IpAddressPrefix;
            this.Policies = Policies;
            this.Routes = Routes;
        }
        /// <summary>
        /// Gets or Sets ID
        /// </summary>
        [DataMember(Name="ID", EmitDefaultValue=false)]
        public string ID { get; set; }
        /// <summary>
        /// Gets or Sets IpAddressPrefix
        /// </summary>
        [DataMember(Name="IpAddressPrefix", EmitDefaultValue=false)]
        public string IpAddressPrefix { get; set; }
        /// <summary>
```

```
        /// Gets or Sets Policies
        /// </summary>
        [DataMember(Name="Policies", EmitDefaultValue=false)]
        public List<SubnetPolicy> Policies { get; set; }
        /// <summary>
        /// Gets or Sets Routes
        /// </summary>
        [DataMember(Name="Routes", EmitDefaultValue=false)]
        public List<Route> Routes { get; set; }
        /// <summary>
        /// Returns the string presentation of the object
        /// </summary>
        /// <returns>String presentation of the object</returns>
        public override string ToString()
        {
            var sb = new StringBuilder();
            sb.Append("class Subnet {\n");
            sb.Append("  ID: ").Append(ID).Append("\n");
            sb.Append("  IpAddressPrefix: ").Append(IpAddressPrefix).Append("\n");
            sb.Append("  Policies: ").Append(Policies).Append("\n");
            sb.Append("  Routes: ").Append(Routes).Append("\n");
            sb.Append("}\n");
            return sb.ToString();
        }
        /// <summary>
        /// Returns the JSON string presentation of the object
        /// </summary>
        /// <returns>JSON string presentation of the object</returns>
        public string ToJson()
        {
            return JsonConvert.SerializeObject(this, Formatting.Indented);
        }
        /// <summary>
        /// Returns true if objects are equal
        /// </summary>
        /// <param name="input">Object to be compared</param>
        /// <returns>Boolean</returns>
        public override bool Equals(object input)
        {
            return this.Equals(input as Subnet);
        }
        /// <summary>
        /// Returns true if Subnet instances are equal
        /// </summary>
        /// <param name="input">Instance of Subnet to be compared</param>
        /// <returns>Boolean</returns>
        public bool Equals(Subnet input)
        {
            if (input == null)
                return false;
            return
                (
                    this.ID == input.ID ||
                    (this.ID != null &&
                    this.ID.Equals(input.ID))
```

```
                ) &&
                (
                    this.IpAddressPrefix == input.IpAddressPrefix ||
                    (this.IpAddressPrefix != null &&
                    this.IpAddressPrefix.Equals(input.IpAddressPrefix))
                ) &&
                (
                    this.Policies == input.Policies ||
                    this.Policies != null &&
                    this.Policies.SequenceEqual(input.Policies)
                ) &&
                (
                    this.Routes == input.Routes ||
                    this.Routes != null &&
                    this.Routes.SequenceEqual(input.Routes)
                );
        }
        /// <summary>
        /// Gets the hash code
        /// </summary>
        /// <returns>Hash code</returns>
        public override int GetHashCode()
        {
            unchecked // Overflow is fine, just wrap
            {
                int hashCode = 41;
                if (this.ID != null)
                    hashCode = hashCode * 59 + this.ID.GetHashCode();
                if (this.IpAddressPrefix != null)
                    hashCode = hashCode * 59 + this.IpAddressPrefix.GetHashCode();
                if (this.Policies != null)
                    hashCode = hashCode * 59 + this.Policies.GetHashCode();
                if (this.Routes != null)
                    hashCode = hashCode * 59 + this.Routes.GetHashCode();
                return hashCode;
            }
        }
        /// <summary>
        /// To validate all properties of the instance
        /// </summary>
        /// <param name="validationContext">Validation context</param>
        /// <returns>Validation Result</returns>
        IEnumerable<System.ComponentModel.DataAnnotations.ValidationResult>
IValidatableObject.Validate(ValidationContext validationContext)
        {
            // ID (string) pattern
            Regex regexID = new Regex(@"^[0-9A-Fa-f]{8}-([0-9A-Fa-f]{4}-){3}[0-9A-Fa-
f]{12}$", RegexOptions.CultureInvariant);
            if (false == regexID.Match(this.ID).Success)
            {
                yield return new
System.ComponentModel.DataAnnotations.ValidationResult("Invalid value for ID, must
match a pattern of " + regexID, new [] { "ID" });
            }
            yield break;
```

```
        }
    }
}
```

Last updated on 17/07/2026

Exemple de code généré par Go

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Go

```go
/*
 * HCN API
 *
 * No description provided (generated by Swagger Codegen https://github.com/swagger-api/swagger-codegen)
 *
 * API version: 2.1
 * Generated by: Swagger Codegen (https://github.com/swagger-api/swagger-codegen.git)
 */
package swagger
type Ipam struct {
    //  Type : dhcp
    Type_ string `json:"Type,omitempty"`
    Subnets []Subnet `json:"Subnets,omitempty"`
}
/*
 * HCN API
 *
 * No description provided (generated by Swagger Codegen https://github.com/swagger-api/swagger-codegen)
 *
 * API version: 2.1
 * Generated by: Swagger Codegen (https://github.com/swagger-api/swagger-codegen.git)
 */
package swagger
type Subnet struct {
    ID string `json:"ID,omitempty"`
    IpAddressPrefix string `json:"IpAddressPrefix,omitempty"`
    Policies []SubnetPolicy `json:"Policies,omitempty"`
    Routes []Route `json:"Routes,omitempty"`
}
```

Last updated on 17/07/2026

Hyper-V commutateur virtuel

25/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Cette rubrique fournit une vue d'ensemble du commutateur virtuel Hyper-V, qui vous permet de connecter des machines virtuelles à des réseaux externes à l'hôte Hyper-V, y compris l'intranet de votre organisation et Internet.

Vous pouvez également vous connecter à des réseaux virtuels sur le serveur qui exécute Hyper-V lorsque vous déployez la mise en réseau définie par logiciel (SDN).

> ⓘ **Notes**
>
> Outre cette rubrique, la documentation suivante du commutateur virtuel Hyper-V est également disponible.
>
> - RDMA (Remote Direct Memory Access) et SET (Switch Embedded Teaming)
> - Applets de commande d'équipe du commutateur réseau dans Windows PowerShell
> - Nouveautés de VMM 2016
> - Configurer l'infrastructure de mise en réseau VMM
> - Hyper-V forum
> - Hyper-V : L'extension de commutateur virtuel WFP doit être activée si elle est requise par les extensions tierces
>
> Pour plus d'informations sur les autres technologies de mise en réseau, consultez Mise en réseau dans Windows Server 2016.

Le commutateur virtuel Hyper-V désigne un commutateur réseau Ethernet de couche 2 logiciel disponible dans le Gestionnaire Hyper-V lorsque vous installez le rôle serveur Hyper-V.

Le commutateur offre des fonctionnalités gérées par programme et extensibles pour connecter des machines virtuelles aux réseaux virtuels et au réseau physique à la fois. Qui plus est, le commutateur virtuel Hyper-V assure l'application de la stratégie de sécurité et d'isolement, ainsi que des niveaux de service.

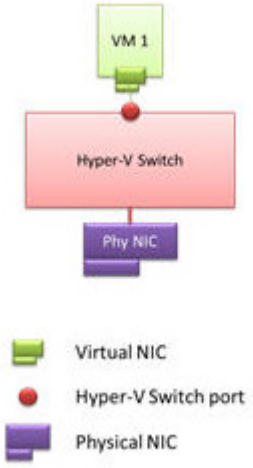
> ⓘ **Notes**

Le commutateur virtuel Hyper-V ne prend en charge qu'Ethernet et pas les autres technologies de réseau local (LAN) câblé, comme Infiniband et Fibre Channel.

Le commutateur virtuel Hyper-V inclut l'isolation des locataires, la mise en forme du trafic, la protection contre les ordinateurs virtuels malveillants et la résolution simplifiée des problèmes.

Grâce à sa prise en charge intégrée des pilotes de filtre de l'API NDIS (Network Device Interface Specification) et des pilotes de légende WFP (Windows Filtering Platform), le commutateur virtuel Hyper-V permet aux éditeurs de logiciels indépendants de créer des plug-ins extensibles (« extensions de commutateur virtuel ») pouvant offrir une mise en réseau et des fonctions de sécurité améliorées. Les extensions de commutateur virtuel que vous ajoutez au commutateur virtuel Hyper-V sont répertoriées dans la fonctionnalité Gestionnaire de commutateur virtuel du Gestionnaire Hyper-V.

L'illustration qui suit dévoile un ordinateur virtuel doté d'une carte réseau virtuelle connecté au commutateur virtuel Hyper-V via un port commuté.



Les capacités du commutateur virtuel Hyper-V vous offrent un plus grand nombre d'options pour l'application de l'isolement des locataires, la mise en forme et le contrôle du trafic réseau, ainsi que l'emploi de mesures de protection contre les ordinateurs virtuels malveillants.

Notes

Dans Windows Server 2016, une machine virtuelle avec une carte réseau virtuelle affiche avec précision le débit maximal de la carte réseau virtuelle. Pour afficher la vitesse de la carte réseau virtuelle dans **Connexions réseau**, cliquez avec le bouton droit sur l'icône de carte réseau virtuelle souhaitée, puis cliquez sur **État**. La boîte de dialogue **État** de la carte réseau virtuelle s'ouvre. Dans **Connexion**, la valeur **vitesse** correspond à la vitesse de la carte réseau physique installée sur le serveur.

Utilisations du commutateur virtuel Hyper-V

Voici quelques scénarios d'utilisation pour le commutateur virtuel Hyper-V.

Affichage de statistiques : un développeur chez un fournisseur de solutions de cloud hébergées implémente un package de gestion qui affiche l'état du commutateur virtuel Hyper-V. Le package de gestion peut demander les statistiques sur les fonctionnalités actuelles, les paramètres de configuration et des ports spécifiques sur tout le commutateur à l'aide de WMI. L'état du commutateur est ensuite affiché pour offrir aux administrateurs une vue d'ensemble.

Suivi des ressources : un fournisseur d'hébergement propose des services facturés en fonction de l'abonnement souscrit. Les différents niveaux d'abonnement offrent plusieurs niveaux de performance réseau. L'administrateur attribue des ressources pour respecter les contrats SLA de sorte que la disponibilité du réseau soit équilibrée. L'administrateur effectue le suivi par programme des informations, telles que l'usage en cours de la bande passante affectée et le nombre d'ordinateurs virtuels, que ce soit les files d'attente d'ordinateurs virtuels (VMQ) ou les canaux IOV. Le même programme enregistre en outre périodiquement les ressources utilisées en plus de celles assignées par ordinateur virtuel pour le suivi à double entrée ou pour les ressources.

Gestion de l'ordre des extensions du commutateur : une entreprise a installé des extensions sur leur hôte Hyper-V pour contrôler le trafic et signaler la détection d'intrusions. Lors de la maintenance, des extensions peuvent être mises à jour ce qui est susceptible de modifier l'ordre des extensions. Un simple script est exécuté pour rétablir l'ordre des extensions après leur mise à jour.

Extension de transfert gérant l'ID du réseau local virtuel : une société importante spécialisée dans la commutation met au point une extension de transfert qui applique toutes les stratégies de mise en réseau. Un des éléments gérés correspond aux ID de réseau local virtuel. Le commutateur virtuel cède le contrôle du réseau local virtuel à l'extension de transfert. L'installation de l'entreprise de commutation appelle par programme une interface de programmation d'applications (API) de WMI (Windows Management Instrumentation) qui active la transparence, indiquant ainsi au commutateur virtuel Hyper-V de passer et de n'entreprendre aucune action avec les étiquettes VLAN.

Fonctionnalité du commutateur virtuel Hyper-V

Voici certaines des fonctionnalités principales incluses dans le commutateur virtuel Hyper-V :

- **Protection contre l'empoisonnement (usurpation d'identité) du cache ARP/ND** : offre une protection contre tout ordinateur virtuel malveillant susceptible d'usurper une identité par empoisonnement du cache ARP (Address Resolution Protocol) dans le but de

subtiliser les adresses IP d'autres ordinateurs virtuels. Il fournit une protection contre les attaques pouvant être lancées contre IPv6 par usurpation ND (Neighbor Discovery).

- **Protection DHCP** : protège contre tout ordinateur virtuel malicieux se présentant comme un serveur DHCP (Dynamic Host Configuration Protocol) pour des attaques d'intercepteur (« man-in-the-middle »).
- **Listes de contrôle d'accès des ports** : permet un filtrage du trafic basé sur les adresses/plages MAC (Media Access Control) ou IP (Internet Protocol), ce qui permet de configurer l'isolement du réseau virtuel.
- **Mode Jonction à un ordinateur virtuel** : permet aux administrateurs de configurer un ordinateur virtuel spécifique sous forme d'appareil virtuel, puis de diriger le trafic des différents réseaux locaux virtuels vers l'ordinateur virtuel en question.
- **Analyse du trafic réseau** : permet aux administrateurs d'examiner le trafic qui transite par le commutateur réseau.
- **Réseau local virtuel isolé (privé)** : permet aux administrateurs de scinder le trafic sur plusieurs réseaux locaux virtuels afin d'établir plus facilement des communautés isolées de locataires.

La liste suivante récapitule les fonctionnalités qui améliorent l'utilisation du commutateur virtuel Hyper-V :

- **Prise en charge de la limitation de la bande passante et des pics d'activité réseau** : le minimum de bande passante assure une bande passante réservée. La bande passante maximale limite son exploitation par une machine virtuelle.
- **Prise en charge du marquage ECN** : le marquage ECN (Explicit Congestion Notification), également connu sous le nom de « protocole TCP de centre de données » (DCTCP), permet au commutateur physique et au système d'exploitation de réguler le trafic afin que les ressources de la mémoire tampon du commutateur ne soient pas surchargées, ce qui se traduit par un débit supérieur du trafic.
- **Diagnostics** : les diagnostics permettent un suivi simple des événements et des paquets qui transitent par le commutateur virtuel.

Gestion des adresses IP (IPAM)

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

La fonction de gestion des adresses IP (IPAM) est une suite d'outils intégrés permettant d'activer la planification, le déploiement, la gestion et la surveillance de bout en bout de votre infrastructure d'adresses IP, avec une expérience utilisateur enrichie. La fonction IPAM découvre automatiquement les serveurs d'infrastructure d'adresses IP et DNS sur votre réseau et vous permet de les gérer depuis une interface centrale.

> ⓘ **Notes**
>
> Outre cette rubrique, le contenu IPAM suivant est disponible.
>
> - Nouveautés de IPAM
> - Gérer IPAM
> - Applets de commande de serveur Gestion des adresses IP (IPAM) dans Windows PowerShell

Gérer IPAM

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Ce guide fournit des informations d'administration et de résolution des problèmes pour la fonctionnalité Gestion des adresses IP (IPAM) dans Windows Server 2016.

Dans Windows Server 2016, IPAM prend en charge les enregistrements de ressources DNS, le redirecteur conditionnel et la gestion de la zone DNS pour les serveurs DNS intégrés à Active Directory et les serveurs DNS adossés à un domaine. En outre, IPAM prend en charge le contrôle d'accès en fonction du rôle et toutes les fonctionnalités des versions précédentes de la technologie.

Ce guide comporte les rubriques suivantes :

- Gestion d'enregistrement de ressource DNS
- Gestion des zones DNS
- Gérer des ressources dans plusieurs forêts Active Directory
- Supprimer définitivement les données d'utilisation
- Contrôle d'accès en fonction du rôle

Voir aussi

Gestion des adresses IP (IPAM)

Gestion d'enregistrement de ressource DNS

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

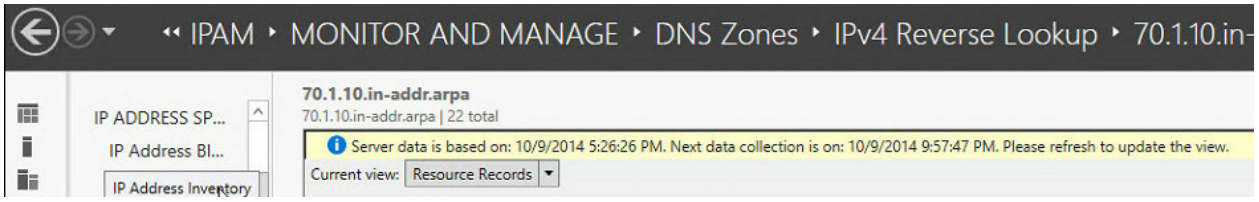
Cette rubrique fournit des informations sur la gestion des enregistrements de ressources DNS à l'aide d'IPAM.

> ⓘ **Notes**
>
> En plus de cette rubrique, les rubriques suivantes sur la gestion des enregistrements de ressources DNS sont disponibles dans cette section.
>
> - Ajouter un enregistrement de ressource DNS
> - Supprimer des enregistrements de ressources DNS
> - Filtrer la vue des enregistrements de ressources DNS
> - Voir les enregistrements de ressources DNS pour une adresse IP spécifique

Vue d'ensemble de la gestion des enregistrements de ressources

Quand vous déployez IPAM dans Windows Server 2016, vous pouvez effectuer une découverte des serveurs pour ajouter des serveurs DHCP et DNS à la console de gestion des serveurs IPAM. Le serveur IPAM collecte ensuite de manière dynamique les données DNS toutes les six heures à partir des serveurs DNS qu'il est configuré pour gérer. IPAM gère une base de données locale où il stocke ces données DNS. IPAM vous envoie une notification spécifiant le jour et l'heure où les données du serveur ont été collectées ainsi que le jour et l'heure de la prochaine collecte de données des serveurs DNS.

La barre d'état jaune dans l'illustration suivante montre l'emplacement de l'interface utilisateur des notifications IPAM.



Les données DNS collectées incluent des informations sur la zone DNS et sur les enregistrements de ressources. Vous pouvez configurer IPAM pour collecter les informations de zone de votre serveur DNS par défaut. IPAM collecte à la fois les zones basées sur des fichiers et les zones Active Directory.

> **Notes**
>
> IPAM collecte les données uniquement de serveurs DNS Microsoft joints à un domaine. Les serveurs DNS tiers et les serveurs qui ne sont pas joints à un domaine ne sont pas pris en charge par IPAM.

Vous trouverez ci-dessous une liste des types d'enregistrement de ressource DNS collectés par IPAM.

- Base de données AFS
- Adresse ATM
- CNAME
- DHCID
- DNAME
- Hôte A ou AAAA
- Informations sur l'hôte
- RNIS
- MX
- Serveurs de noms
- Pointeur (PTR)
- Personne responsable
- Router par
- Emplacement du service
- SOA
- SRV
- Texte

- Services connus
- WINS
- WINS-R
- X.25

Dans Windows Server 2016, IPAM assure l'intégration entre l'inventaire d'adresses IP, les zones DNS et les enregistrements de ressources DNS :

- Vous pouvez utiliser IPAM pour créer automatiquement un inventaire d'adresses IP à partir d'enregistrements de ressources DNS.
- Vous pouvez créer manuellement un inventaire d'adresses IP à partir d'enregistrements de ressources DNS A et AAAA.
- Vous pouvez voir les enregistrements de ressources DNS d'une zone DNS spécifique, et filtrer ces enregistrements en fonction du type, de l'adresse IP, des données d'enregistrement de ressource et d'autres options de filtrage.
- IPAM crée automatiquement un mappage entre les plages d'adresses IP et les zones de recherche inversée DNS.
- IPAM crée des adresses IP pour les enregistrements PTR présents dans la zone de recherche inversée, et qui sont inclus dans cette plage d'adresses IP. Vous pouvez également modifier manuellement ce mappage si nécessaire.

IPAM vous permet d'effectuer les opérations suivantes sur les enregistrements de ressources à partir de la console IPAM.

- Créer des enregistrements de ressources DNS
- Modifier des enregistrements de ressources DNS
- Supprimer des enregistrements de ressources DNS
- Créer des enregistrements de ressources associés

IPAM journalise automatiquement tous les changements que vous apportez à la configuration DNS à l'aide de la console IPAM.

Voir aussi

Gérer IPAM

Commentaires

Cette page a-t-elle été utile ? Yes No

Ajouter un enregistrement de ressource DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour ajouter un ou plusieurs nouveaux enregistrements de ressources DNS à l'aide de la console cliente IPAM.

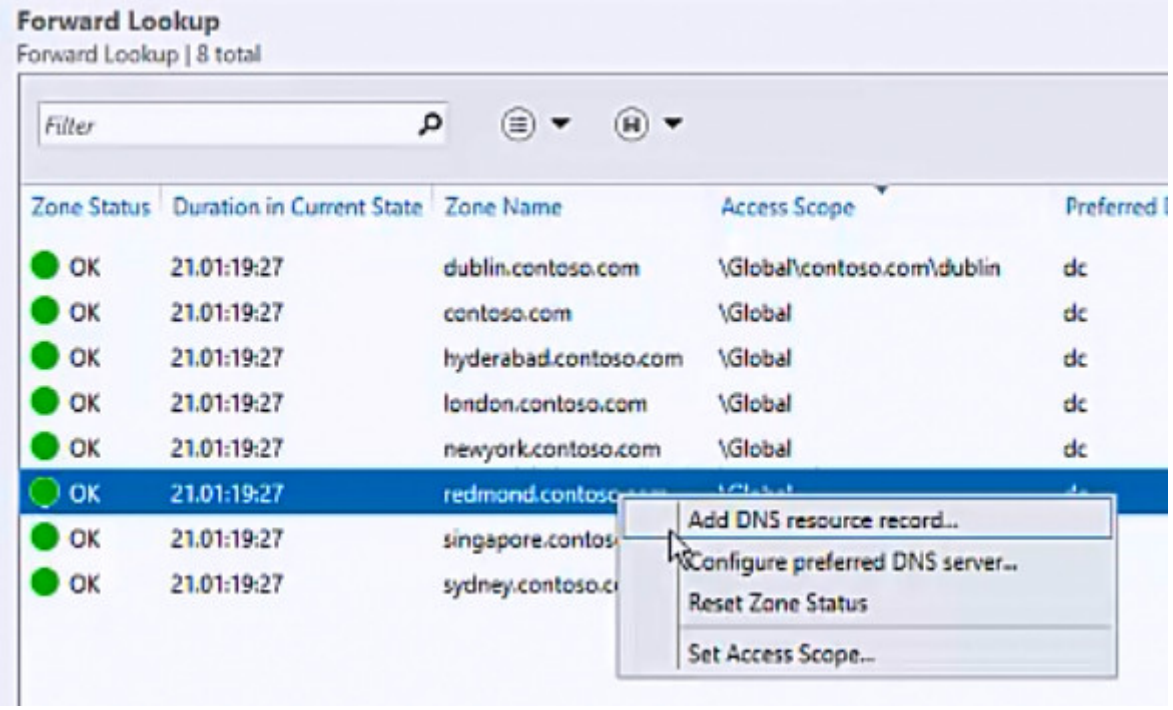
L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour ajouter un enregistrement de ressource DNS

1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.

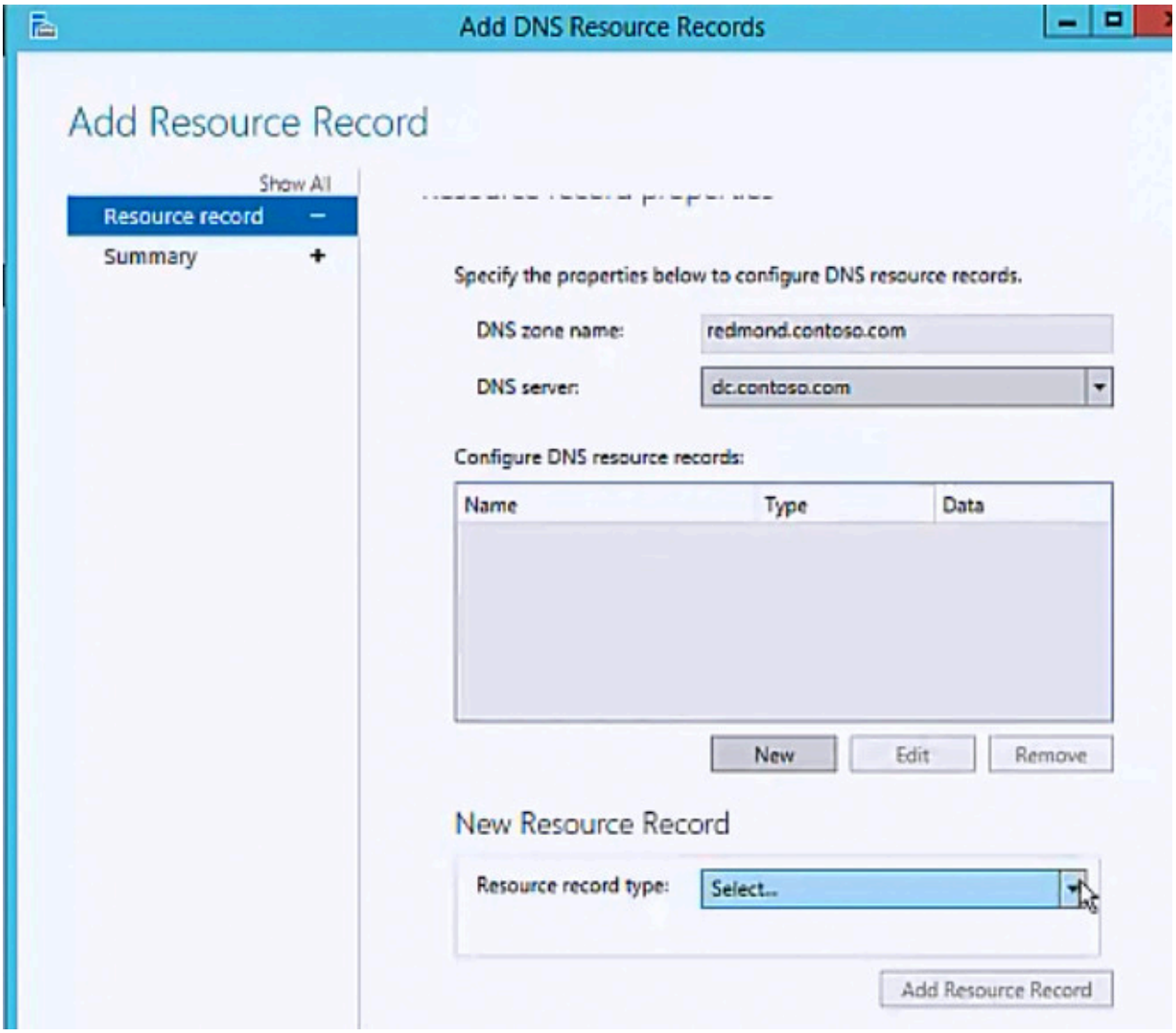
2. Dans le volet de navigation, dans **MONITOR AND MANAGE**, cliquez sur **Zones DNS**. Le volet de navigation se divise en un volet de navigation supérieur et un volet de navigation inférieur.

3. Dans le volet de navigation inférieur, cliquez sur **Recherche vers l'avant**. Toutes les zones de recherche directe DNS gérées par IPAM sont affichées dans les résultats de la recherche du volet d'affichage. Cliquez avec le bouton droit sur la zone dans laquelle vous souhaitez ajouter un enregistrement de ressource, puis cliquez sur **Ajouter un enregistrement de ressource DNS**.

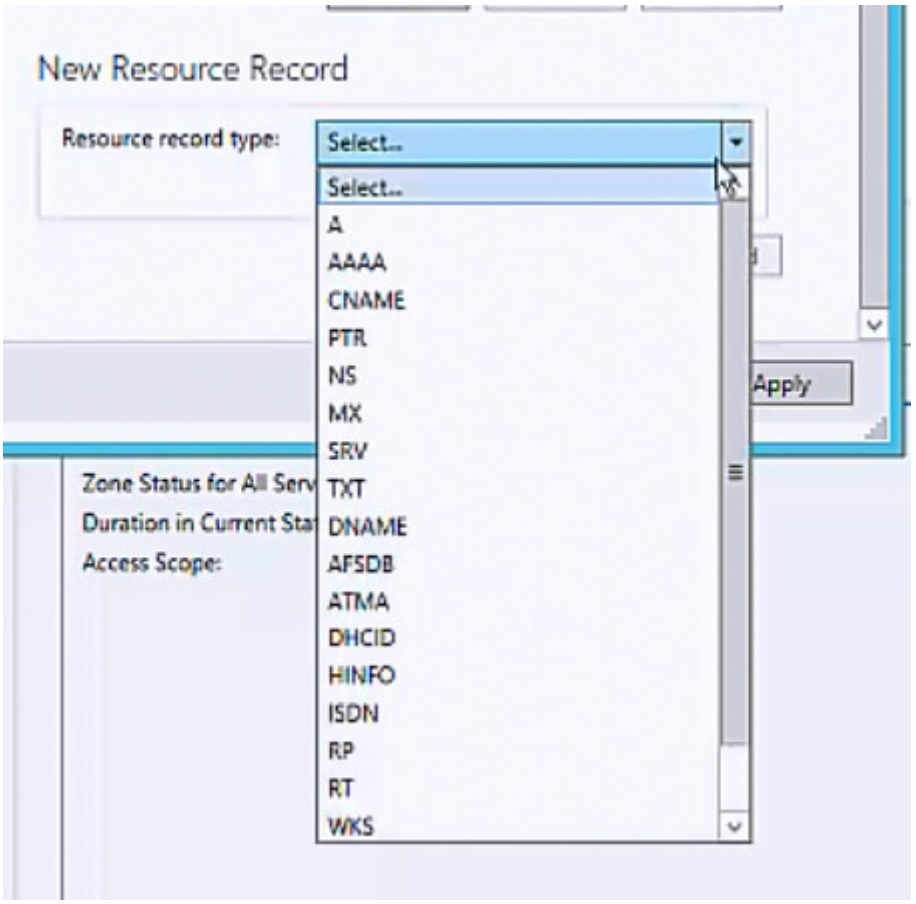


4. La boîte de dialogue **Ajouter des enregistrements de ressources DNS** s'ouvre. Dans **les propriétés d'enregistrement de** ressource, cliquez sur **serveur DNS** et sélectionnez le serveur DNS dans lequel vous souhaitez ajouter un ou plusieurs nouveaux enregistrements de ressources. Dans **Configurer les enregistrements de ressources DNS**, cliquez sur **Nouveau**.

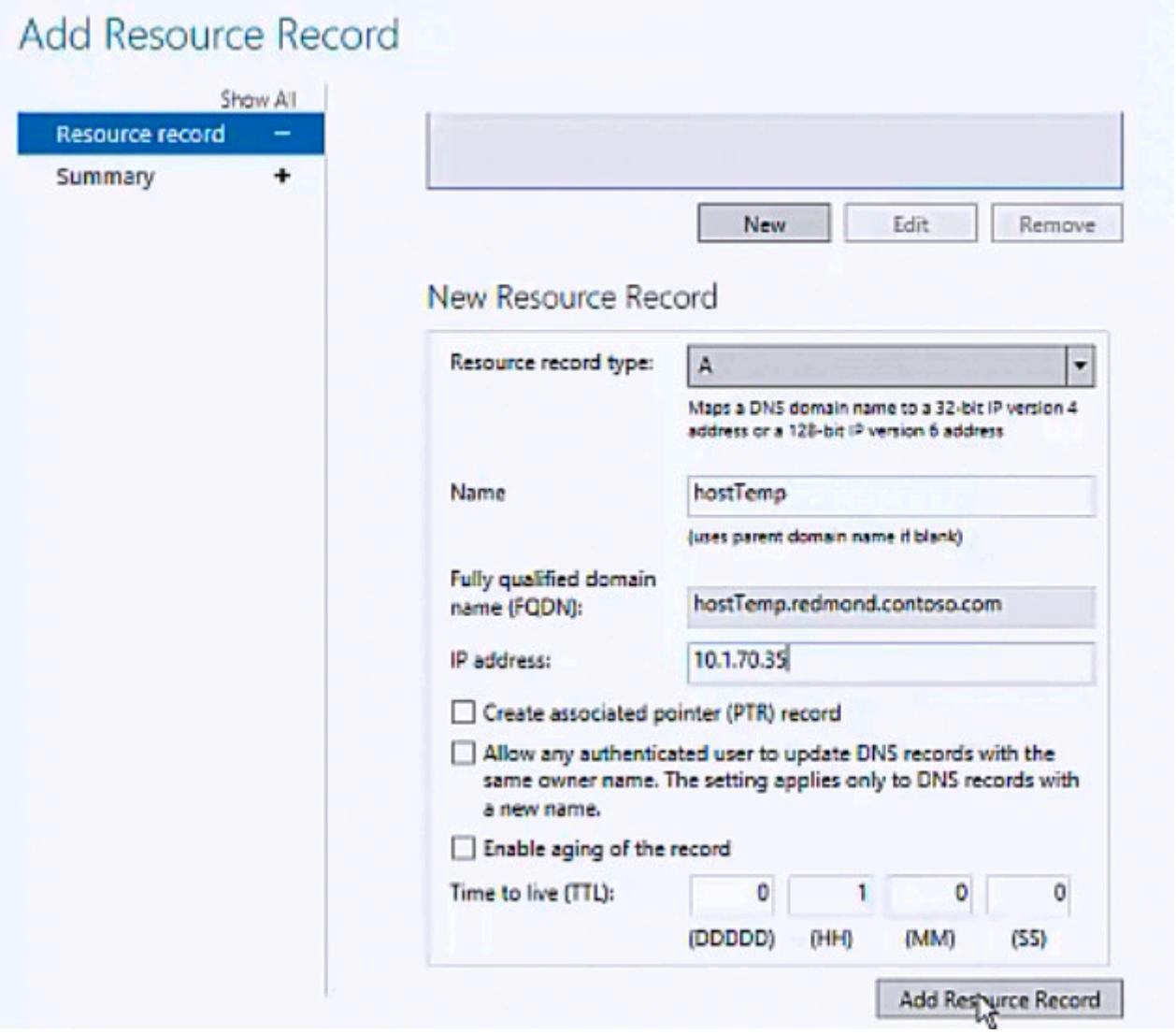
5. La boîte de dialogue s'étend pour afficher **un nouvel enregistrement de ressource**. Cliquez sur **Type d'enregistrement de ressource**.



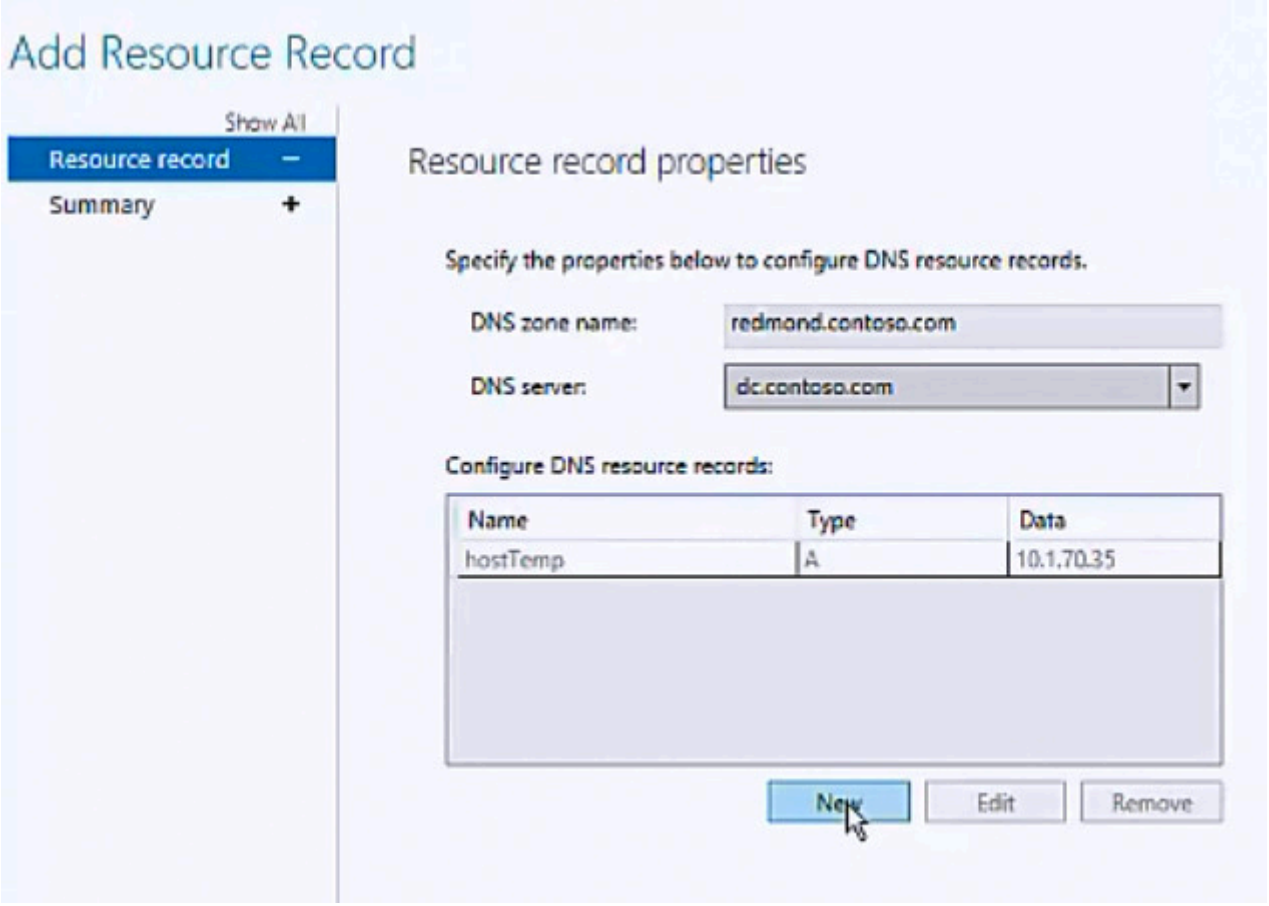
6. La liste des types d'enregistrements de ressources apparaît. Cliquez sur le type d'enregistrement de ressource que vous souhaitez ajouter.



7. Dans **Nouvel enregistrement de ressource,** dans **Nom**, tapez un nom d'enregistrement de ressource. Dans **Adresse IP**, tapez une adresse IP, puis sélectionnez les propriétés d'enregistrement de ressource appropriées pour votre déploiement. Cliquez sur **Ajouter un enregistrement de ressource**.

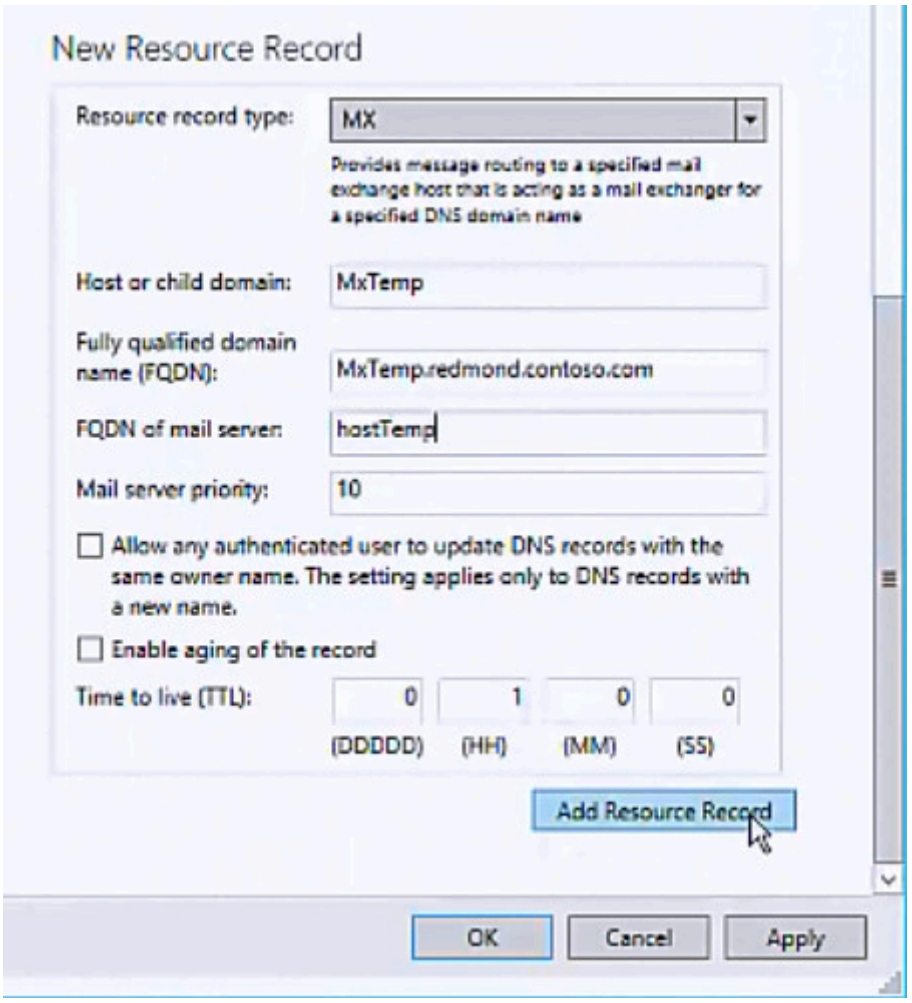


8. Si vous ne souhaitez pas créer d'enregistrements de ressources supplémentaires, cliquez sur **OK**. Si vous souhaitez créer d'autres enregistrements de ressources, cliquez sur **Nouveau**.

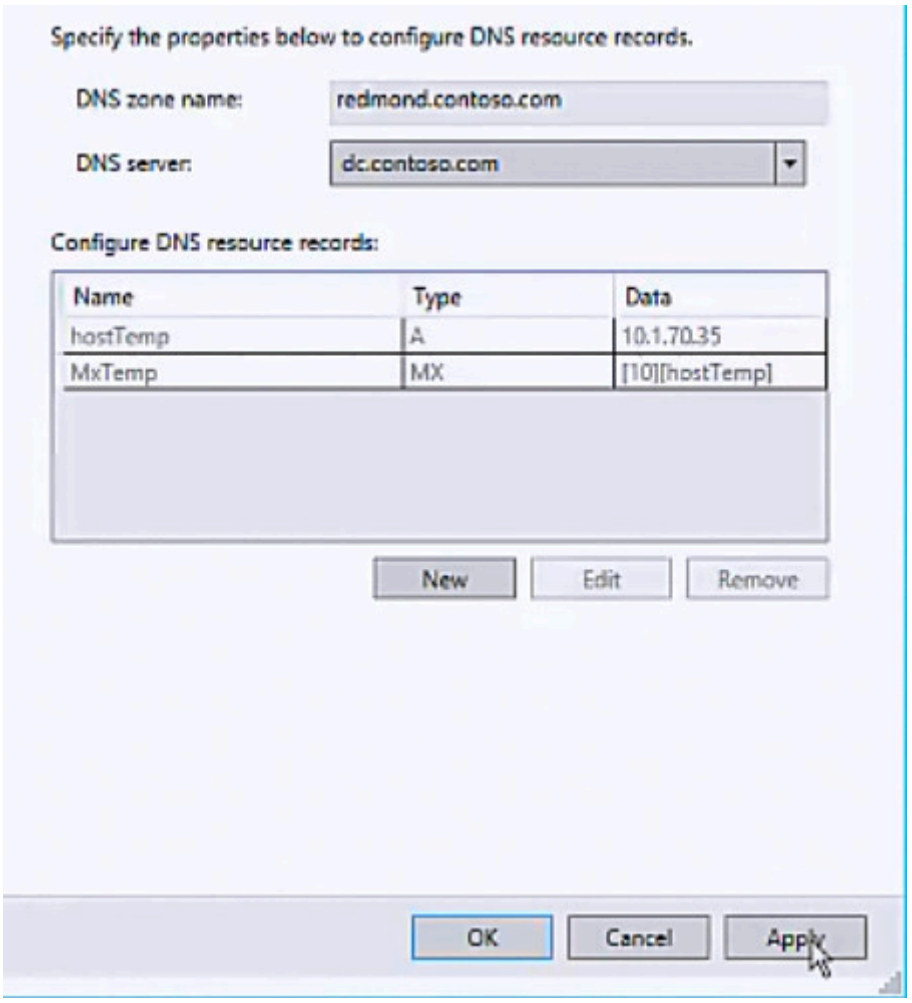


9. La boîte de dialogue s'étend pour afficher **un nouvel enregistrement de ressource**. Cliquez sur **Type d'enregistrement de ressource**. La liste des types d'enregistrements de ressources apparaît. Cliquez sur le type d'enregistrement de ressource que vous souhaitez ajouter.

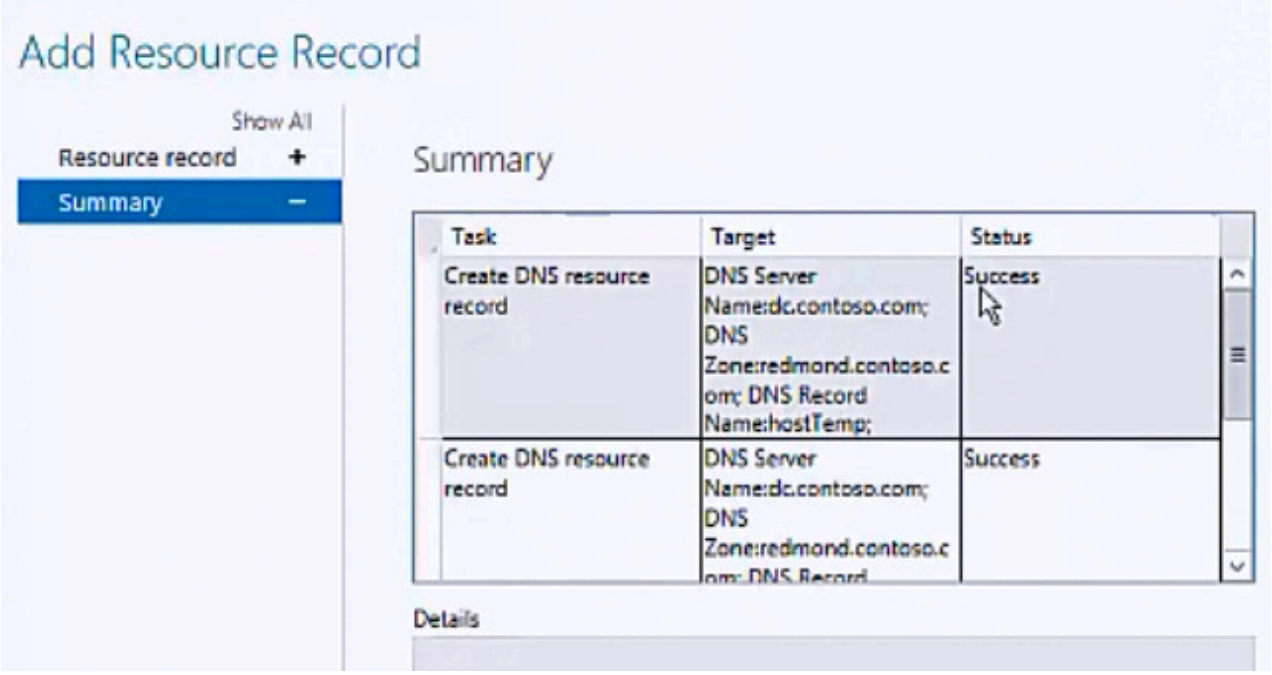
10. Dans **Nouvel enregistrement de ressource,** dans **Nom**, tapez un nom d'enregistrement de ressource. Dans **Adresse IP**, tapez une adresse IP, puis sélectionnez les propriétés d'enregistrement de ressource appropriées pour votre déploiement. Cliquez sur **Ajouter un enregistrement de ressource**.



11. Si vous souhaitez ajouter d'autres enregistrements de ressources, répétez le processus de création des enregistrements. Lorsque vous avez terminé de créer de nouveaux enregistrements de ressources, cliquez sur **Appliquer**.



12. La boîte de dialogue **Ajouter un enregistrement de** ressource affiche un résumé des enregistrements de ressources pendant que IPAM crée les enregistrements de ressources sur le serveur DNS que vous avez spécifié. Lorsque les enregistrements sont correctement créés, **l'état** de l'enregistrement est **Success**.



13. Cliquez sur **OK**.

Voir aussi

Gestion des enregistrements de ressources DNS- Gérer IPAM

Supprimer des enregistrements de ressources DNS

16/08/2025

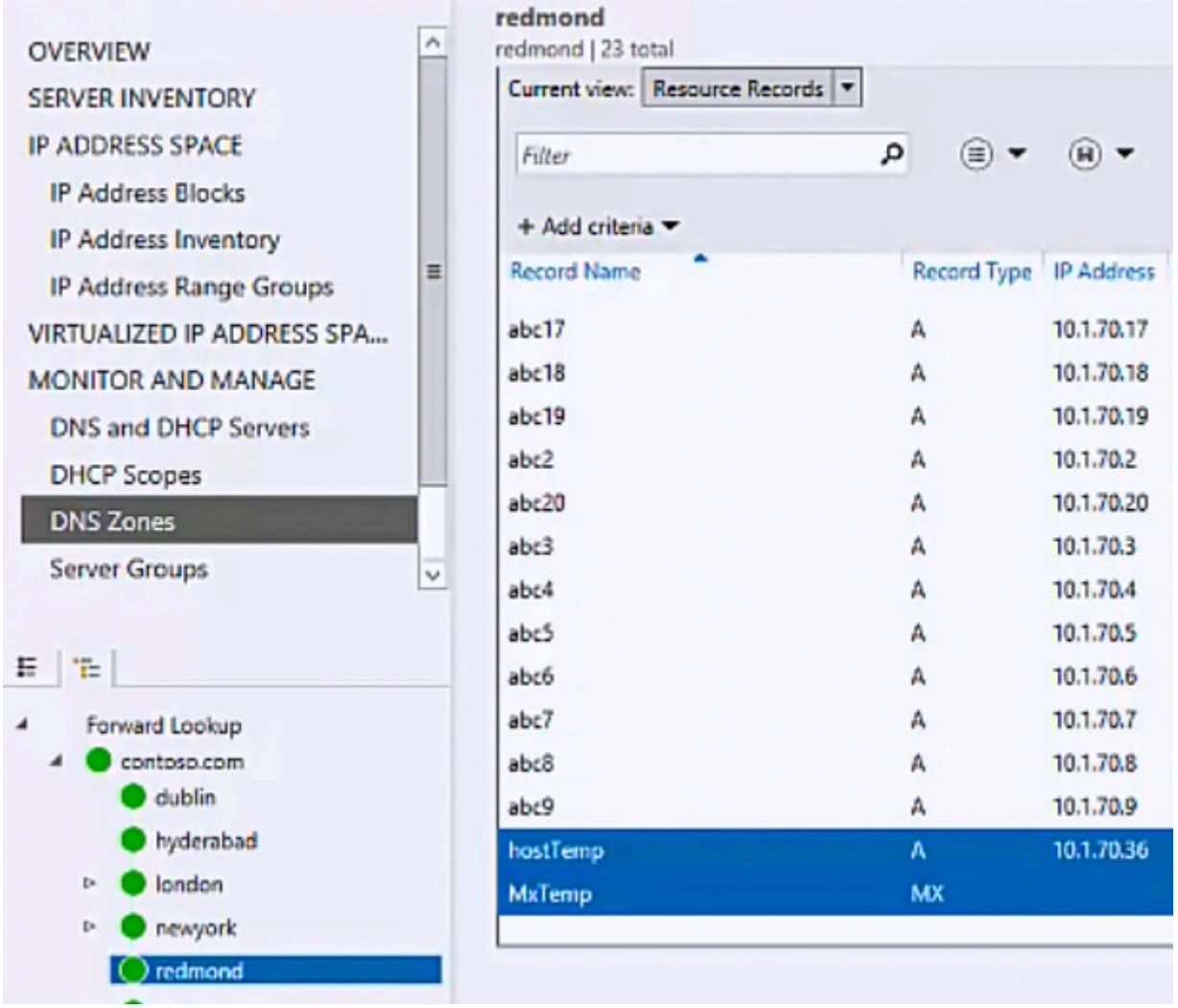
S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour supprimer un ou plusieurs enregistrements de ressources DNS à l'aide de la console cliente IPAM.

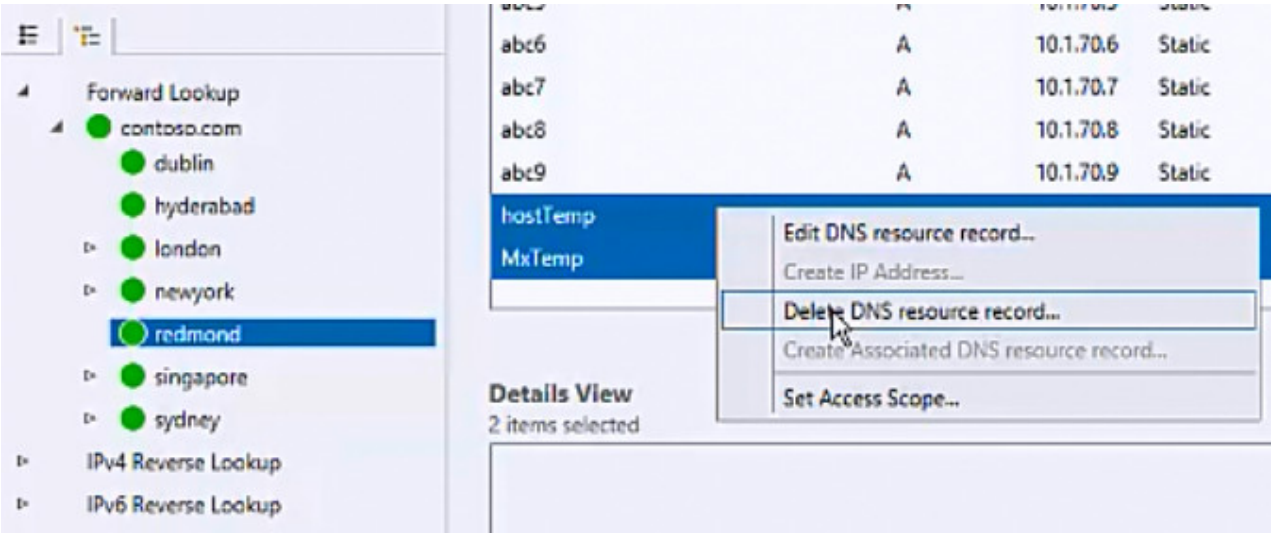
L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour supprimer des enregistrements de ressources DNS

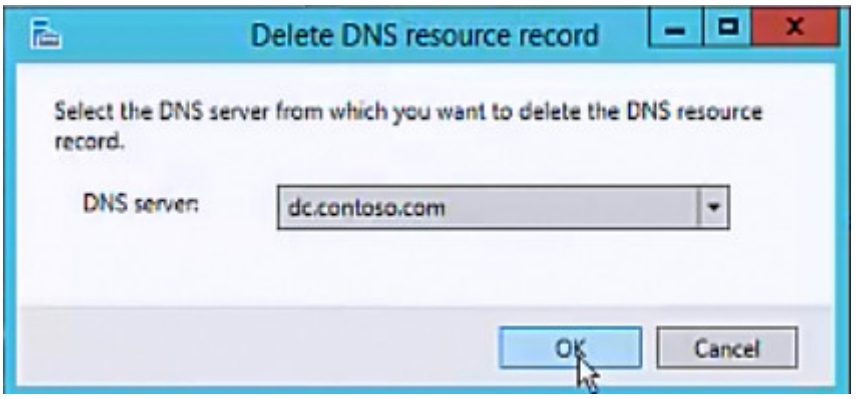
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.
2. Dans le volet de navigation, dans **MONITOR AND MANAGE**, cliquez sur **Zones DNS**. Le volet de navigation se divise en un volet de navigation supérieur et un volet de navigation inférieur.
3. Cliquez pour développer **la recherche vers l'avant** et le domaine où se trouvent les enregistrements de zone et de ressources que vous souhaitez supprimer. Cliquez sur la zone, puis dans le volet d'affichage, cliquez sur **Affichage actuel**. Cliquez sur **Enregistrements de ressources**.
4. Dans le volet d'affichage, recherchez et sélectionnez les enregistrements de ressources que vous souhaitez supprimer.



5. Cliquez avec le bouton droit sur les enregistrements sélectionnés, puis cliquez sur **Supprimer l'enregistrement de ressource DNS**.



6. La boîte de dialogue **Supprimer l'enregistrement de ressource DNS** s'ouvre. Vérifiez que le serveur DNS approprié est sélectionné. Si ce n'est pas le cas, cliquez sur **le serveur DNS** et sélectionnez le serveur à partir duquel vous souhaitez supprimer les enregistrements de ressources. Cliquez sur **OK**. IPAM supprime les enregistrements de ressources du serveur DNS.



Voir aussi

Gestion des enregistrements de ressources DNS- Gérer IPAM

Filtrer l’affichage des enregistrements de ressources DNS

16/08/2025

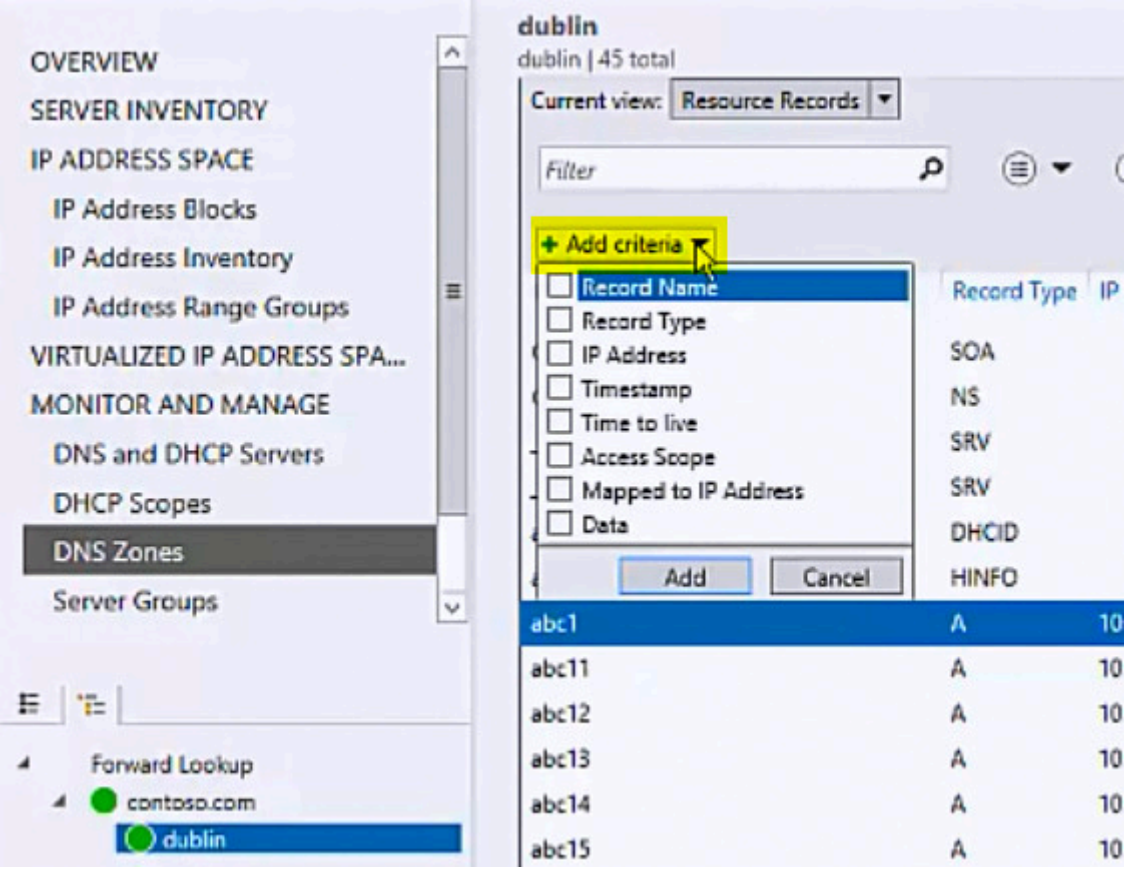
S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour filtrer la vue des enregistrements de ressources DNS dans la console cliente IPAM.

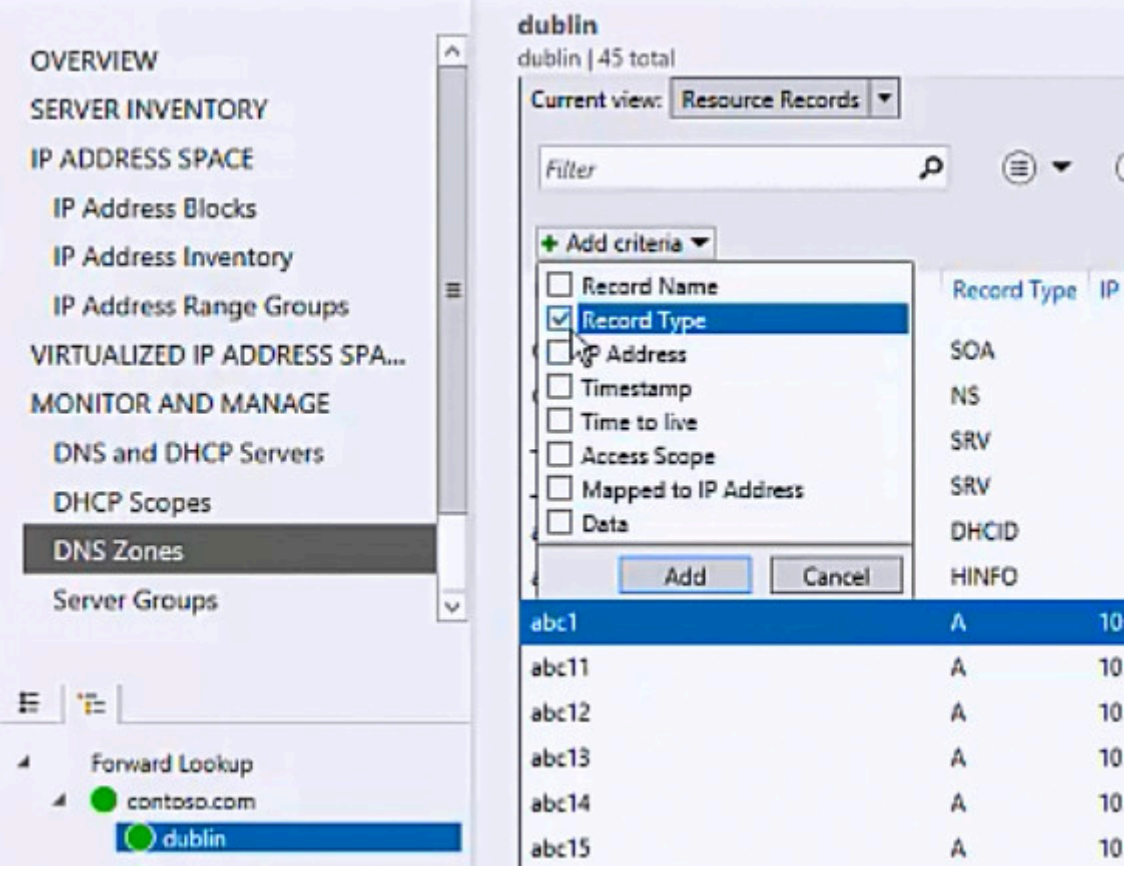
L’appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour filtrer la vue des enregistrements de ressources DNS

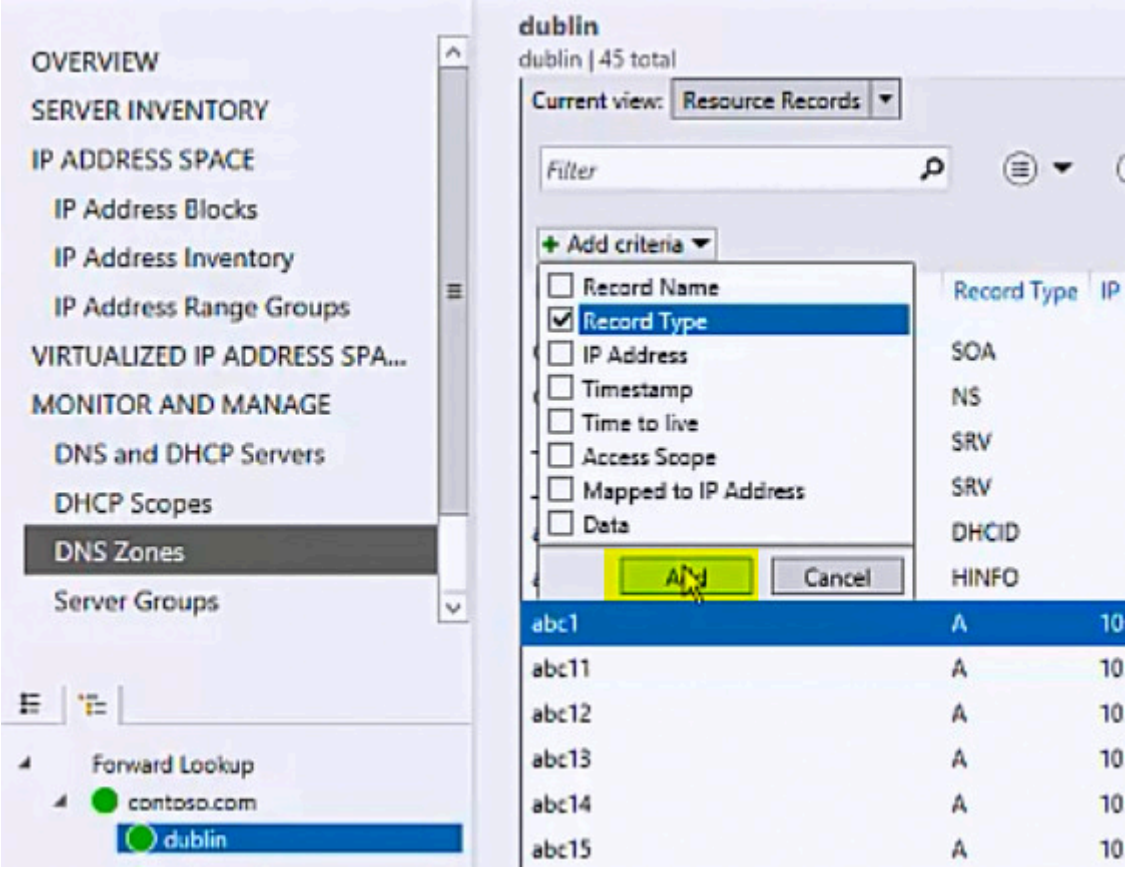
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s’affiche.
2. Dans le volet de navigation, dans **SURVEILLER ET GÉRER**, cliquez sur **Zones DNS**. Le volet de navigation se divise en un volet de navigation supérieur et un volet de navigation inférieur.
3. Dans le volet de navigation inférieur, cliquez sur **Recherche vers l’avant**. Toutes les zones de recherche directe DNS gérées par IPAM sont affichées dans les résultats de la recherche du volet d’affichage.
4. Cliquez sur la zone dont vous souhaitez voir et filtrer les enregistrements.
5. Dans le volet d’affichage, cliquez sur **Affichage actuel**, puis sur **Enregistrements de ressources**. Les enregistrements de ressources de la zone s’affichent dans le volet d’affichage.
6. Dans le volet d’affichage, cliquez sur **Ajouter des critères**.



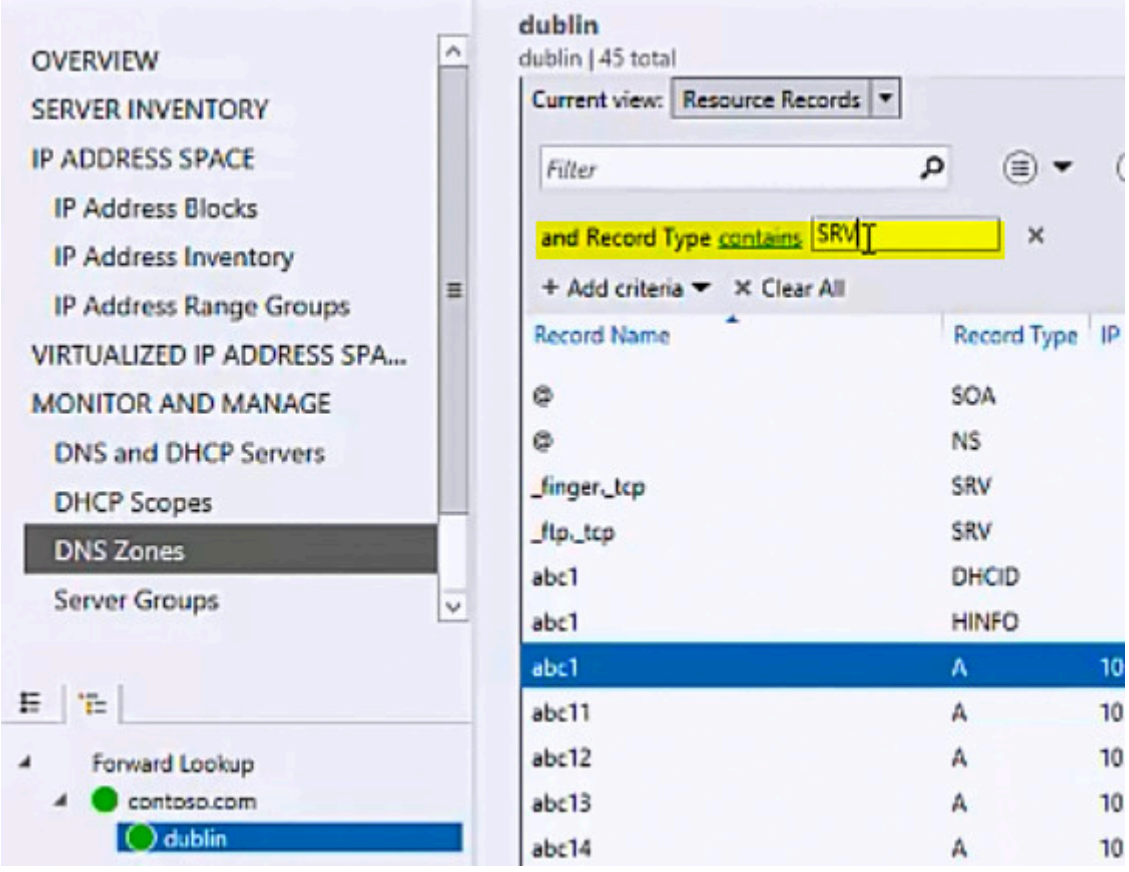
7. Sélectionnez un critère dans la liste déroulante. Par exemple, si vous souhaitez afficher un type d'enregistrement spécifique, cliquez sur **Type d'enregistrement**.



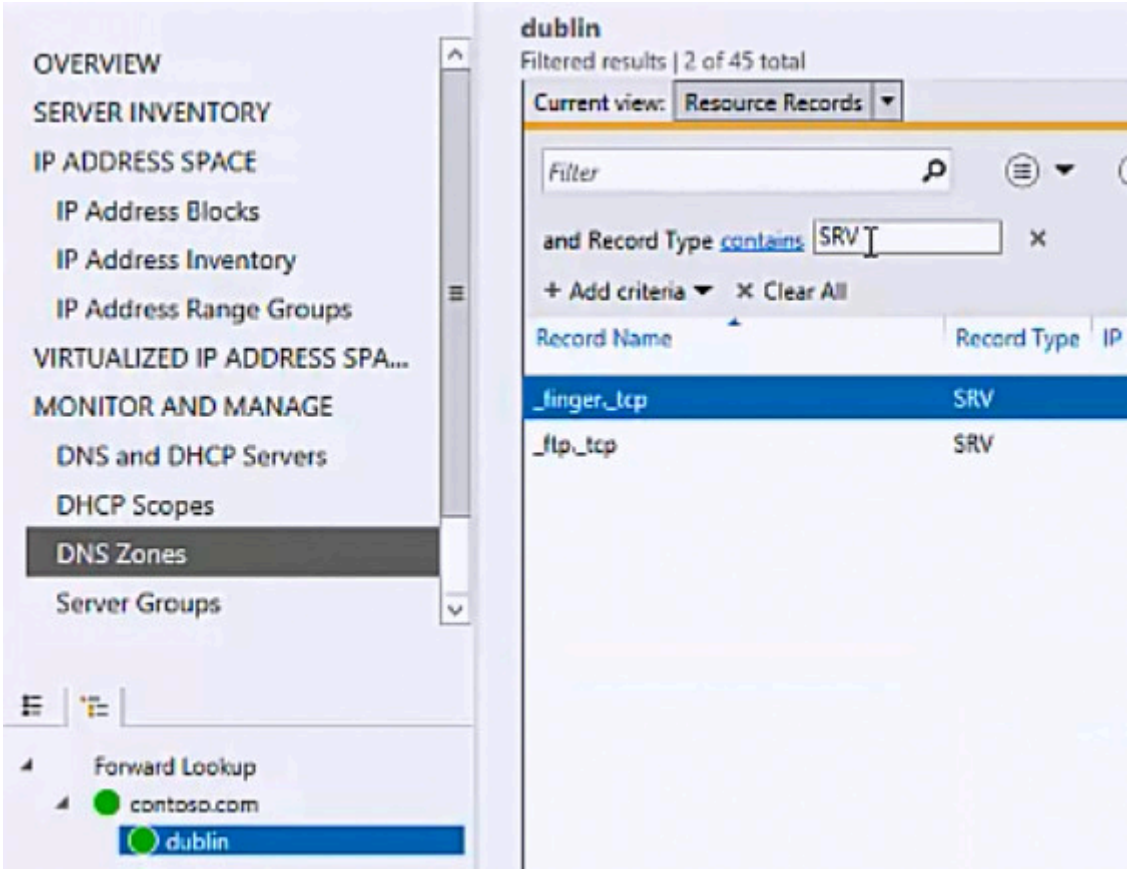
8. Cliquez sur **Ajouter**.



9. **Le type d'enregistrement** est ajouté en tant que paramètre de recherche. Entrez le texte correspondant au type d'enregistrement à rechercher. Par exemple, si vous souhaitez afficher uniquement les enregistrements SRV, tapez **SRV**.



10. Appuyez sur Entrée. Les enregistrements de ressources DNS sont filtrés en fonction des critères et de l'expression de recherche que vous avez spécifiés.



Voir aussi

Gestion des enregistrements de ressources DNSGérer IPAM

Afficher les enregistrements de ressources DNS pour une adresse IP spécifique

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

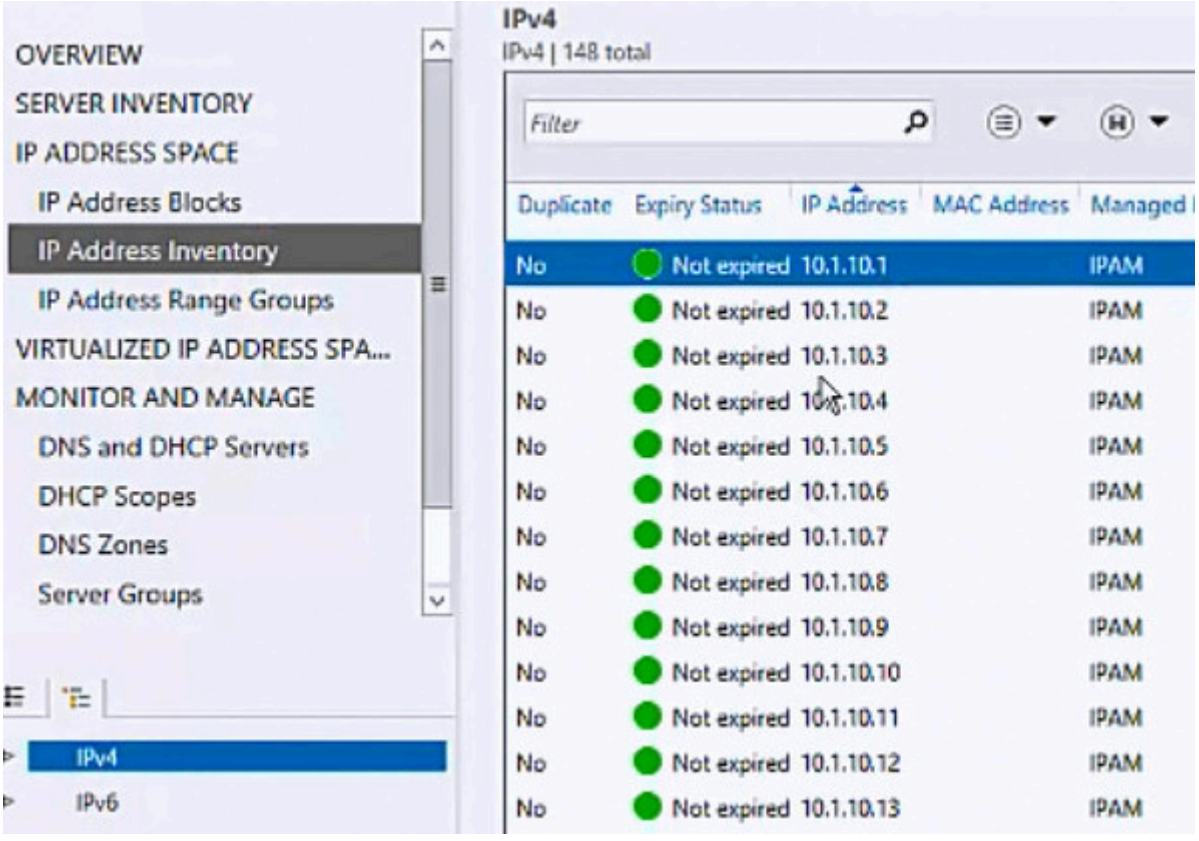
Vous pouvez utiliser cette rubrique pour afficher les enregistrements de ressources DNS associés à l'adresse IP de votre choix.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

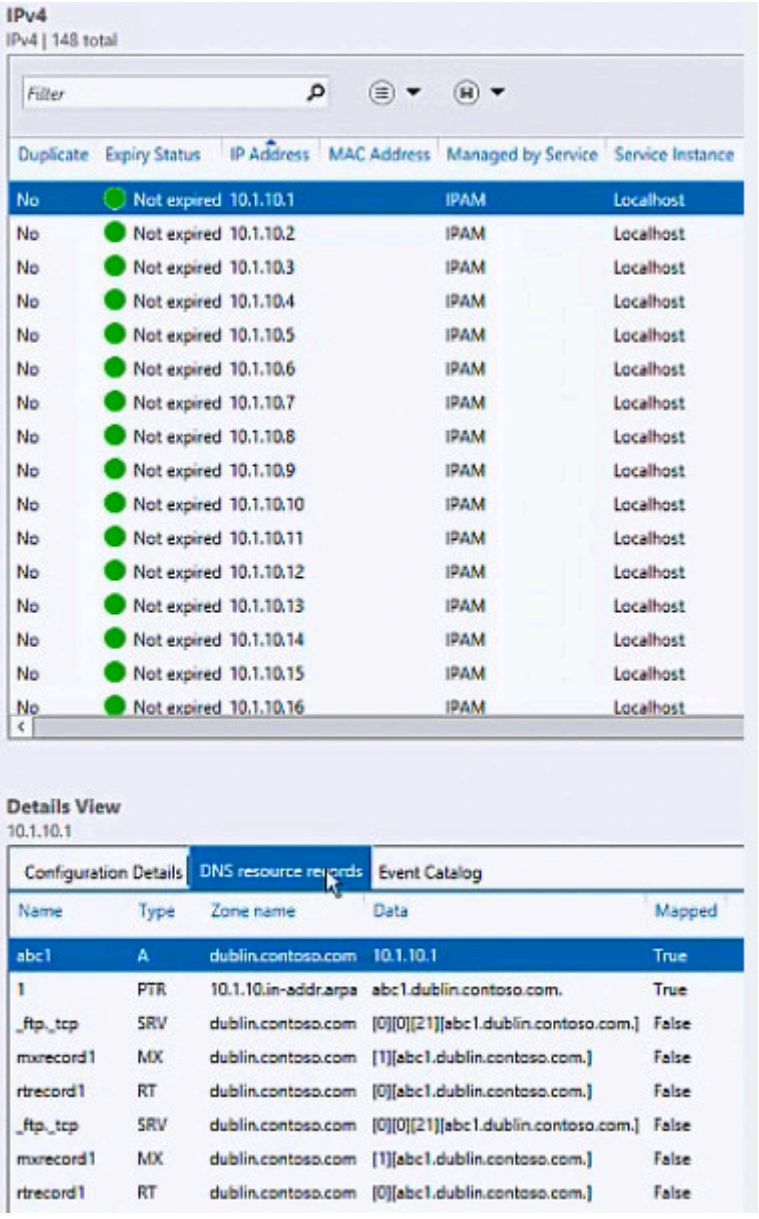
Pour afficher les enregistrements de ressources d'une adresse IP

1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.

2. Dans le panneau de navigation, dans **ESPACE D'ADRESSAGE IP**, cliquez sur **Inventaire d'adresses IP**. Dans le volet de navigation inférieur, cliquez sur **IPv4** ou **IPv6**. L'inventaire des adresses IP s'affiche dans la vue de recherche du volet d'affichage. Recherchez et sélectionnez l'adresse IP dont vous souhaitez afficher les enregistrements de ressources DNS.



3. Dans la **vue Détails** du volet d'affichage, cliquez sur **Enregistrements de ressources DNS**. Les enregistrements de ressources associés à l'adresse IP sélectionnée sont affichés.



Voir aussi

Gestion des enregistrements de ressources DNSGérer IPAM

Gestion des zones DNS

08/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cette rubrique fournit des informations sur la gestion des zones DNS à l'aide de la console cliente IPAM.

> ⓘ **Notes**
>
> En plus de cette rubrique, les rubriques suivantes relatives à la gestion des zones DNS IPAM sont disponibles dans cette section.
>
> - Créer une zone DNS
> - Modifier une zone DNS
> - Voir les enregistrements de ressources DNS pour une zone DNS
> - Voir les zones DNS

Quand vous déployez IPAM dans Windows Server 2016, vous pouvez utiliser IPAM pour gérer les zones DNS.

Dans la console IPAM, vous pouvez voir les enregistrements de ressources DNS d'une zone DNS spécifique, et filtrer ces enregistrements en fonction du type, de l'adresse IP, des données d'enregistrement de ressource et d'autres options de filtrage. De plus, vous pouvez modifier les enregistrements de ressources DNS pour des zones spécifiques

Voir aussi

Gérer IPAM

Créer une zone DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour créer une zone DNS à l'aide de la console cliente IPAM.

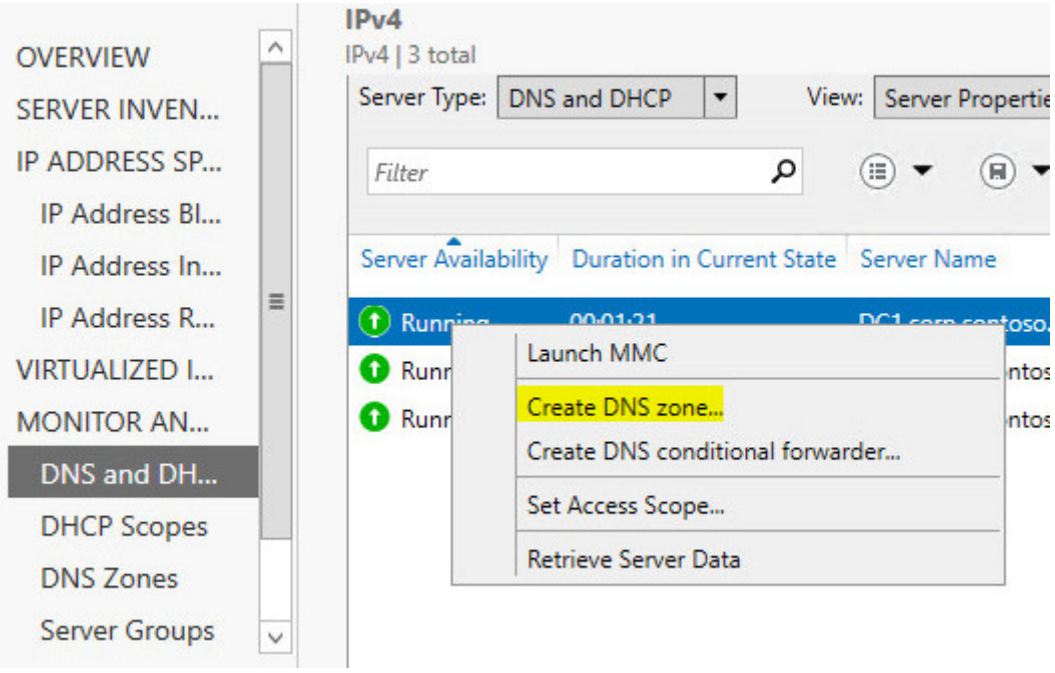
L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Création d'une zone DNS

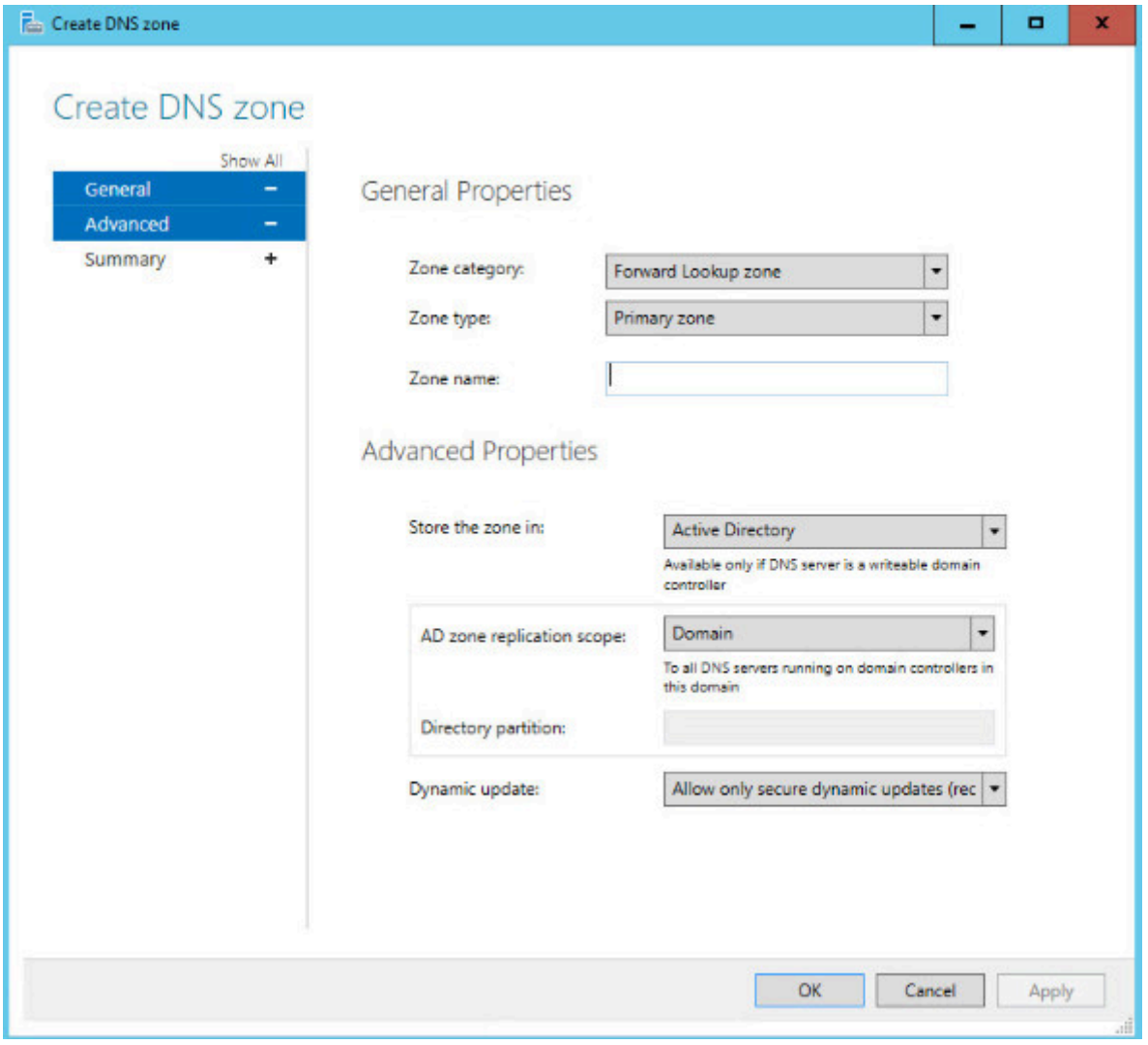
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.

2. Dans le volet de navigation, dans **SURVEILLER ET GÉRER**, cliquez sur **Serveurs DNS et DHCP**. Dans le volet d'affichage, cliquez sur **Type de serveur**, puis sur **DNS**. Tous les serveurs DNS gérés par IPAM sont répertoriés dans les résultats de la recherche.

3. Recherchez le serveur sur lequel vous souhaitez ajouter une zone, puis cliquez avec le bouton droit sur le serveur. Cliquez sur **Créer une zone DNS**.



4. La boîte de dialogue **Créer une zone DNS** s'ouvre. Dans **Propriétés générales**, sélectionnez une catégorie de zone, un type de zone, puis entrez un nom dans le **nom de la zone**. Sélectionnez également les valeurs appropriées pour votre déploiement dans **Propriétés avancées**, puis cliquez sur **OK**.



Voir aussi

Gestion des zones DNSGérer IPAM

Modifier une zone DNS

16/08/2025

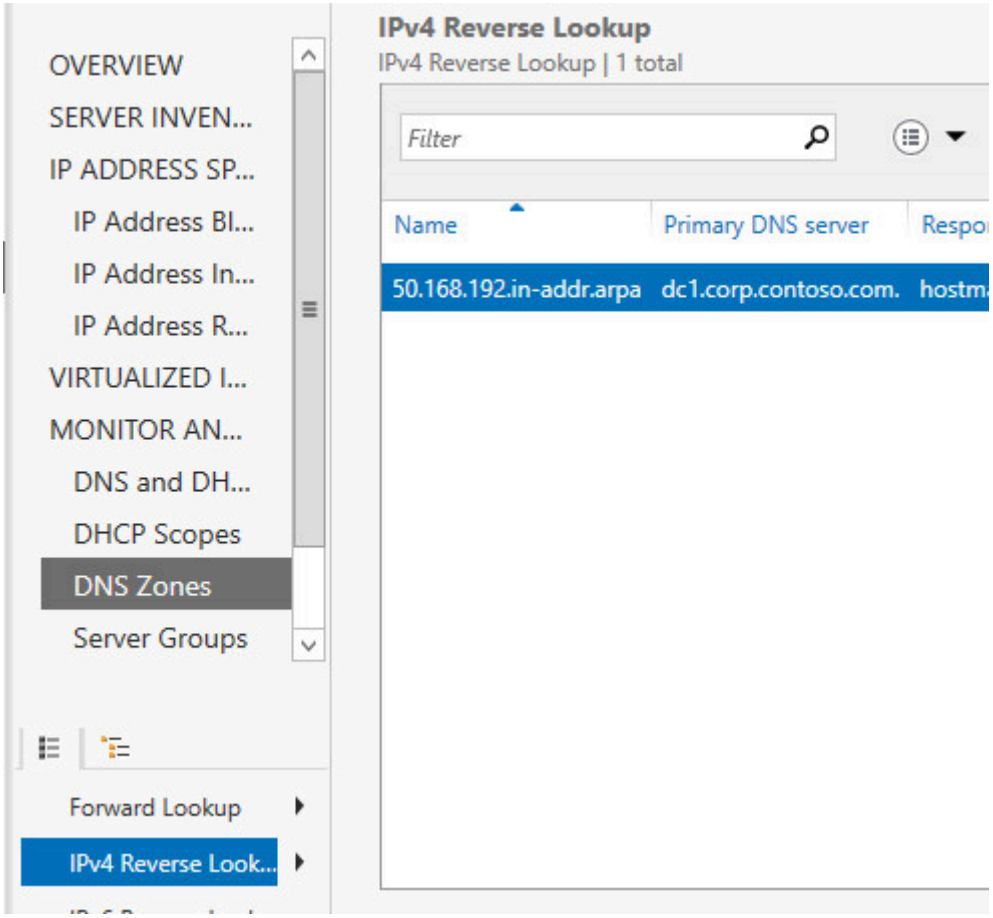
S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour modifier une zone DNS dans la console cliente IPAM.

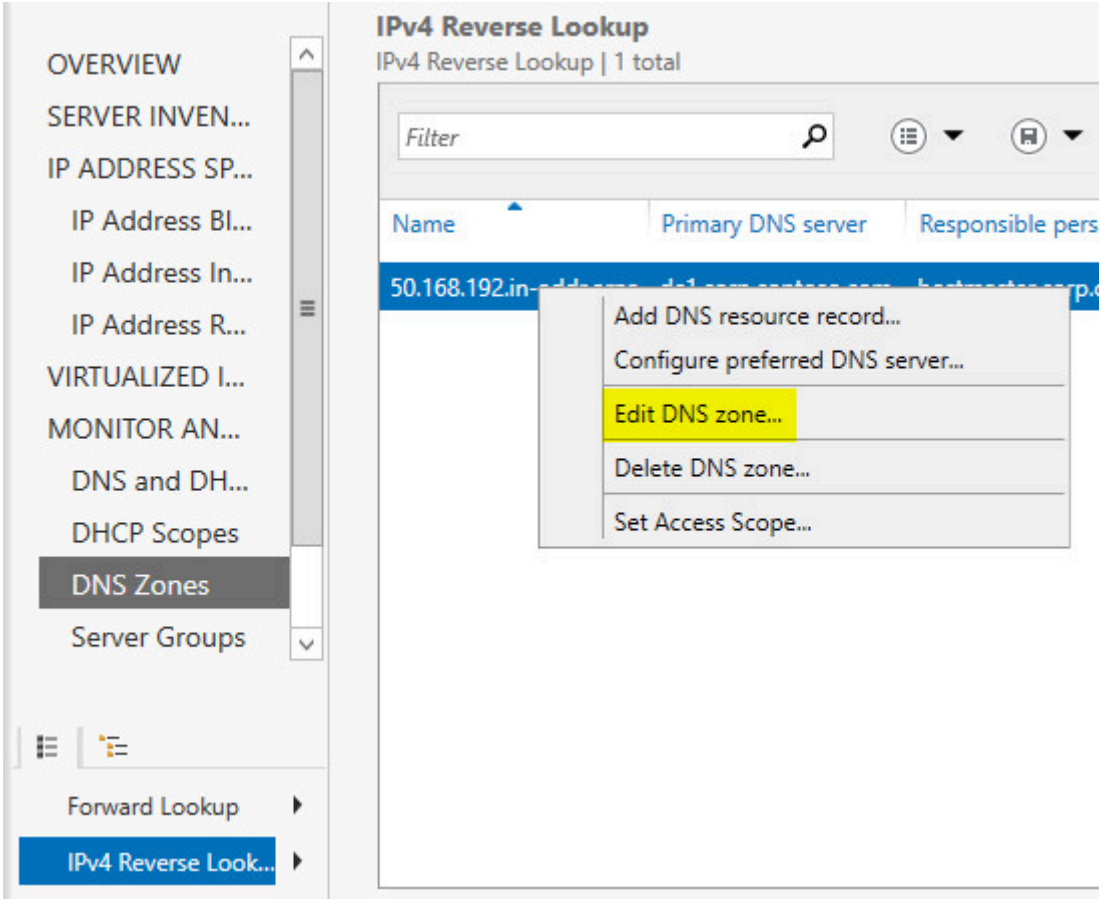
L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour modifier une zone DNS

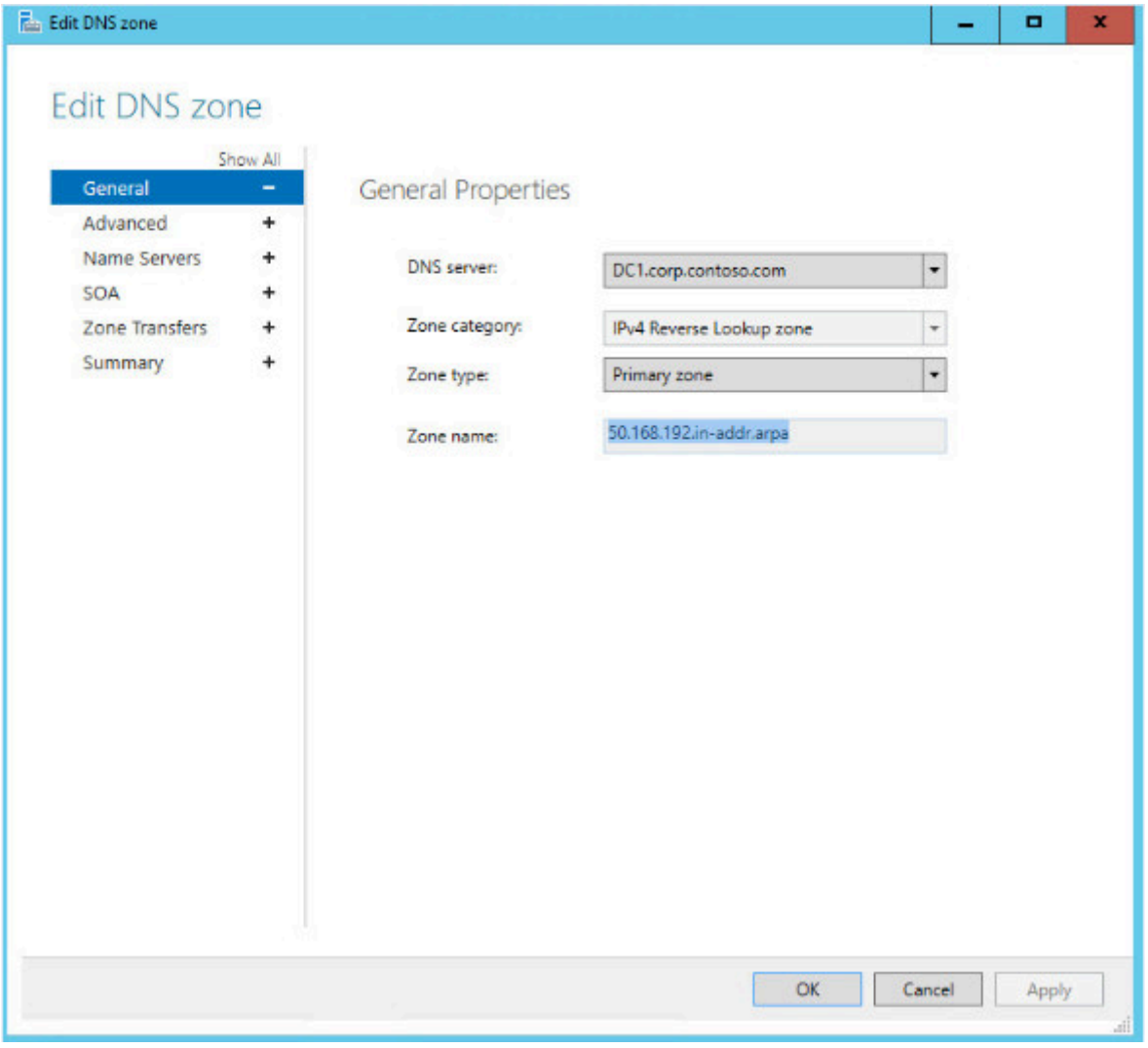
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.
2. Dans le volet de navigation, dans **MONITOR AND MANAGE**, cliquez sur **Zones DNS**. Le volet de navigation se divise en un volet de navigation supérieur et un volet de navigation inférieur.
3. Dans le volet de navigation inférieur, effectuez l'une des sélections suivantes :
    - Recherche vers l'avenir
    - Recherche inversée IPv4
    - Recherche inversée IPv6
4. Par exemple, sélectionnez Recherche inversée IPv4.



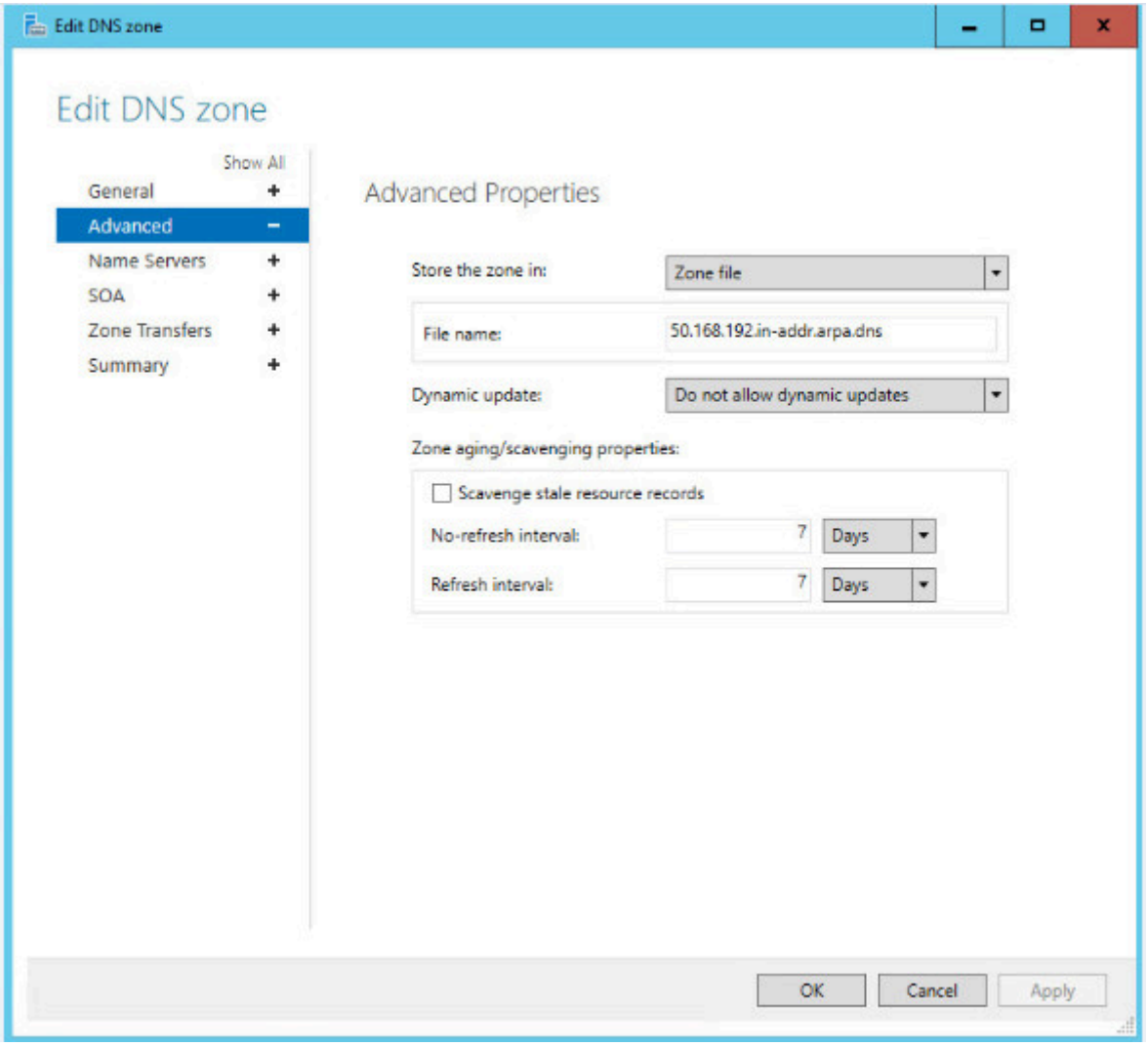
5. Dans le volet d'affichage, cliquez avec le bouton droit sur la zone à modifier, puis cliquez sur **Modifier la zone DNS**.



6. La boîte de dialogue **Modifier la zone DNS** s'ouvre avec la page **Général** sélectionnée. Si nécessaire, modifiez les propriétés de zone générale : **serveur DNS**, **catégorie zone** et **type zone**, puis cliquez sur **Appliquer** ou, si vos modifications sont terminées, **OK**.



7. Dans la boîte de dialogue **Modifier la zone DNS** , cliquez sur **Avancé**. La page des propriétés **de zone avancée** s'ouvre. Si nécessaire, modifiez les propriétés que vous souhaitez modifier, puis cliquez sur **Appliquer** ou, si vos modifications sont terminées, **OK**.



8. Si nécessaire, sélectionnez les noms de page de propriétés de zone supplémentaires (Serveurs de noms, SOA, Transferts de zone), apportez vos modifications, puis cliquez sur **Appliquer** ou **OK**. Pour passer en revue toutes vos modifications de zone, cliquez sur **Résumé**, puis sur **OK**.

Voir aussi

Gestion des zones DNS- Gérer IPAM

Afficher les enregistrements de ressources DNS pour une zone DNS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour voir comment afficher les enregistrements de ressources DNS pour une zone DNS dans la console cliente IPAM.

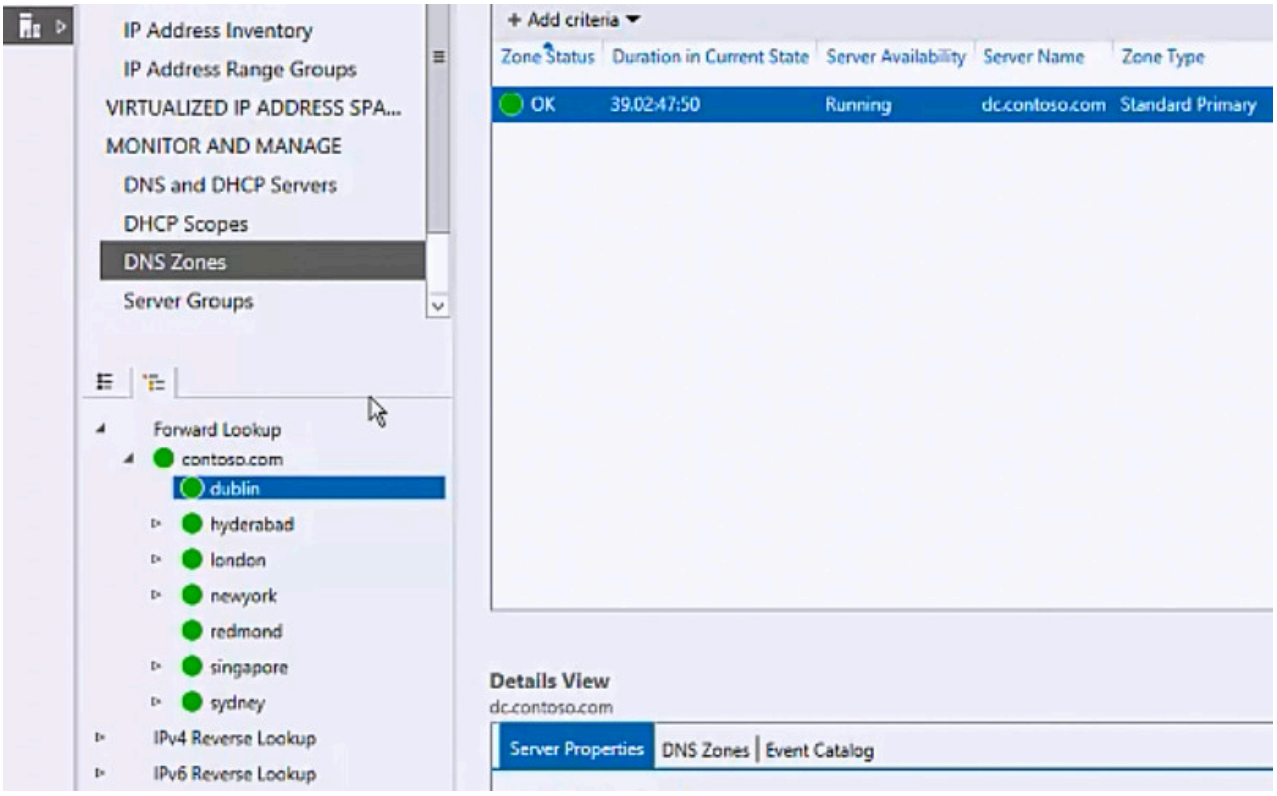
L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Afficher les enregistrements de ressources DNS pour une zone DNS

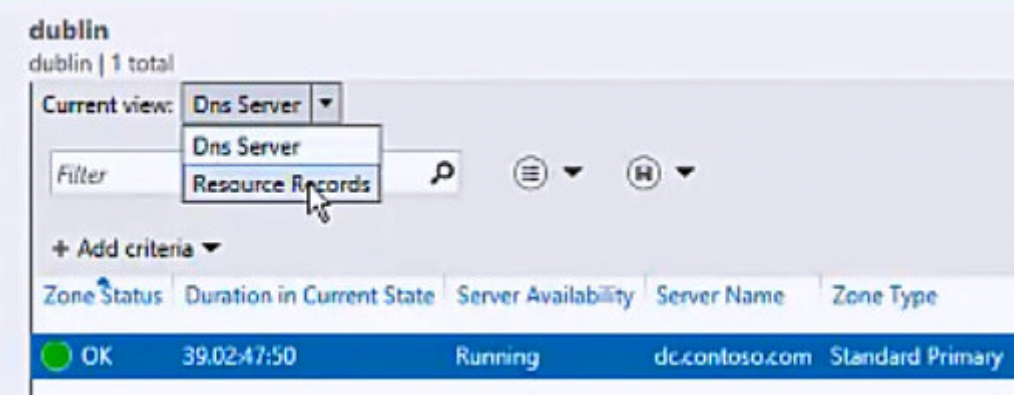
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.

2. Dans le volet de navigation, dans **MONITOR AND MANAGE**, cliquez sur **Zones DNS**. Le volet de navigation se divise en un volet de navigation supérieur et un volet de navigation inférieur.

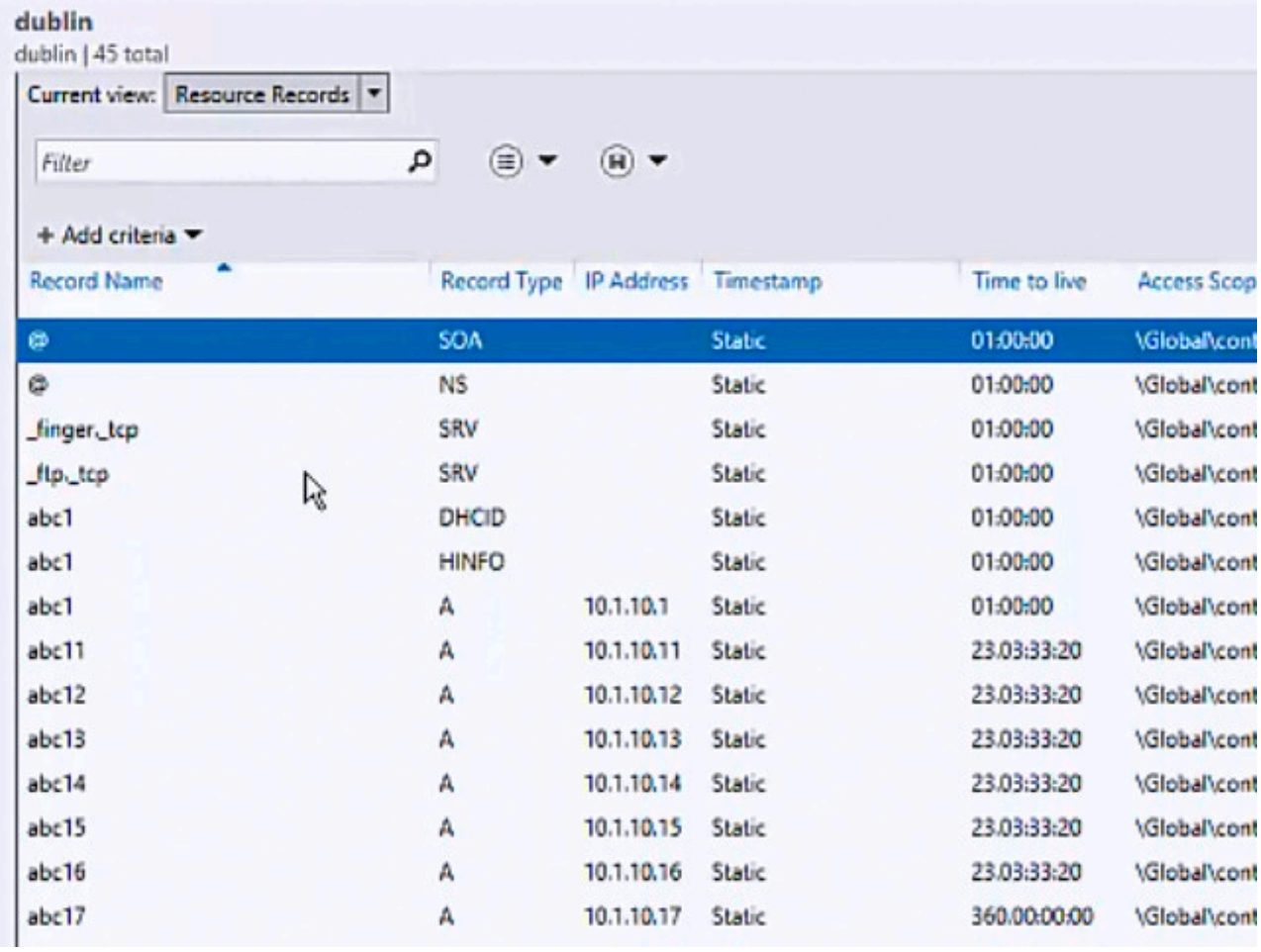
3. Dans le volet de navigation inférieur, cliquez sur **Recherche vers l'avant**, puis développez le domaine et la liste de zones pour localiser et sélectionner la zone à afficher. Par exemple, si vous avez une zone nommée dublin, cliquez sur **dublin**.



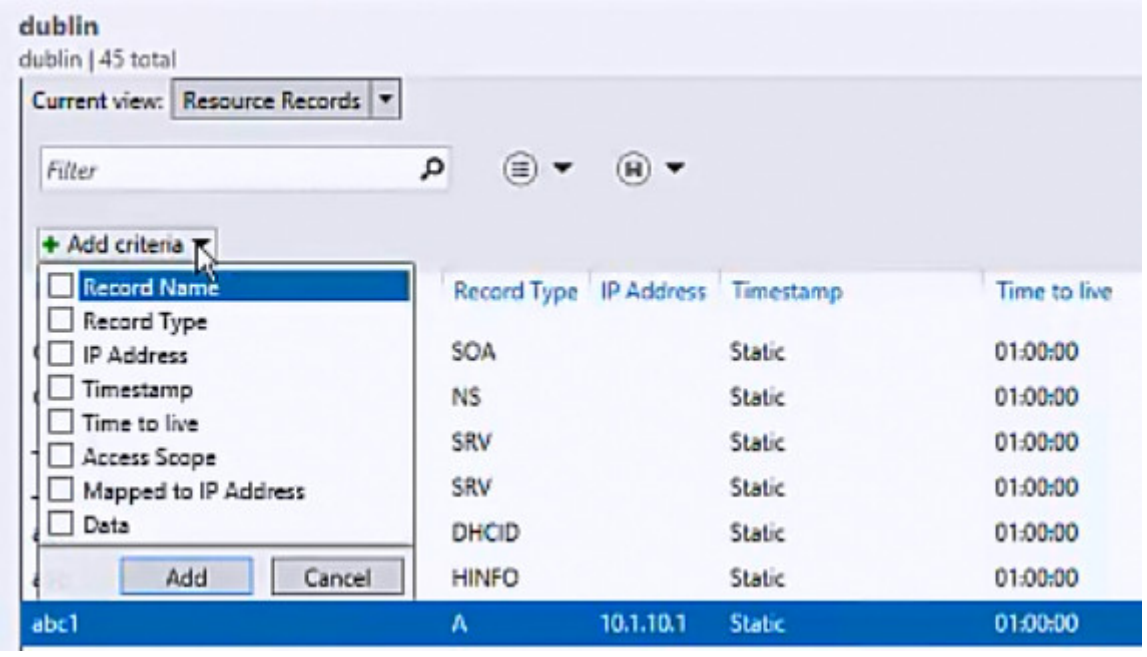
4. Dans le volet d'affichage, l'affichage par défaut est celui des serveurs DNS de la zone. Pour modifier l'affichage, cliquez sur **Affichage actuel**, puis sur **Enregistrements de ressources**.



5. Les enregistrements de ressources DNS pour la zone s'affichent. Pour filtrer les enregistrements, tapez le texte que vous souhaitez rechercher dans **Filter**.



6. Pour filtrer les enregistrements de ressources par type d'enregistrement, étendue d'accès ou autres critères, cliquez sur **Ajouter des critères**, puis effectuez des sélections dans la liste des critères, puis cliquez sur **Ajouter**.



Voir aussi

Gestion des zones DNS- Gérer IPAM

Afficher les zones DNS

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour afficher les zones DNS dans la console cliente IPAM.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour afficher les zones DNS dans la console cliente IPAM

1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.
2. Dans le volet de navigation, dans **SURVEILLER ET GÉRER**, cliquez sur **Zones DNS**. Le volet de navigation se divise en un volet de navigation supérieur et un volet de navigation inférieur.
3. Dans le volet de navigation inférieur, effectuez l'une des sélections suivantes :
    - Recherche vers l'avenir
    - Recherche inversée IPv4
    - Recherche inversée IPv6
    - Redirecteur conditionnel

Voir aussi

Gestion des zones DNSGérer IPAM

Gérer des ressources dans plusieurs forêts Active Directory

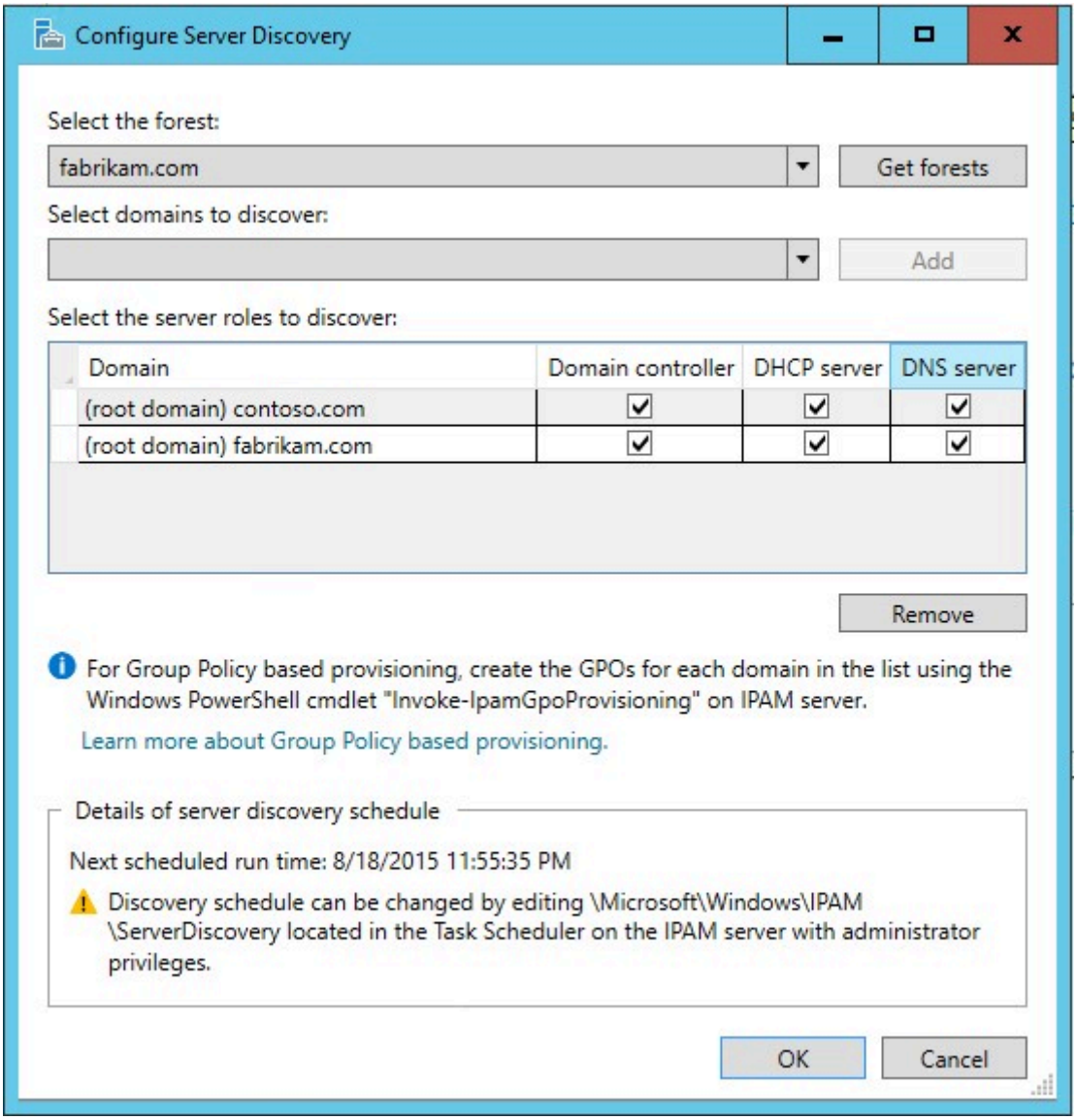
14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique afin de découvrir comment utiliser IPAM pour gérer les contrôleurs de domaine, les serveurs DHCP et les serveurs DNS dans plusieurs forêts Active Directory.

Pour utiliser IPAM afin de gérer des ressources dans les forêts Active Directory distantes, chaque forêt à gérer doit disposer d'une approbation bidirectionnelle avec la forêt où IPAM est installé.

Pour démarrer le processus de découverte des différentes forêts Active Directory, ouvrez le Gestionnaire de serveur, puis cliquez sur IPAM. Dans la console cliente IPAM, cliquez sur **Configurer la découverte de serveurs**, puis cliquez sur **Obtenir les forêts**. Cela permet de lancer une tâche en arrière-plan qui découvre les forêts approuvées et leurs domaines. À la fin du processus de découverte, cliquez sur **Configurer la découverte de serveurs**, ce qui entraîne l'ouverture de la boîte de dialogue suivante.



Notes

Pour le provisionnement basé sur des stratégies de groupe dans un scénario Active Directory interforêts, veillez à exécuter l'applet de commande Windows PowerShell suivante sur le serveur IPAM, et non sur les contrôleurs de domaine du domaine d'approbation. Par exemple, si votre serveur IPAM est joint à la forêt corp.contoso.com, et si la forêt d'approbation est fabrikam.com, vous pouvez exécuter l'applet de commande Windows PowerShell suivante sur le serveur IPAM dans corp.contoso.com à des fins de provisionnement basé sur des stratégies de groupe dans la forêt fabrikam.com. Pour exécuter cette applet de commande, vous devez être membre du groupe Administrateurs de domaine dans la forêt fabrikam.com.

PowerShell

```
    Invoke-IpamGpoProvisioning -Domain fabrikam.COM -GpoPrefixName IPAMSERVER -
IpamServerFqdn IPAM.CORP.CONTOSO.COM
```

Dans la boîte de dialogue **Configurer la découverte de serveurs**, cliquez sur **Sélectionner la forêt**, puis choisissez la forêt à gérer avec IPAM. Sélectionnez également les domaines que vous souhaitez gérer, puis cliquez sur **Ajouter**.

Dans **Sélectionner les rôles serveur à découvrir**, pour chaque domaine à gérer, spécifiez le type de serveur à découvrir. Les options sont **le contrôleur de domaine**, le **serveur DHCP** et le **serveur DNS**.

Par défaut, les contrôleurs de domaine, les serveurs DHCP et les serveurs DNS sont découverts. Si vous ne souhaitez pas découvrir l'un de ces types de serveur, vous devez décocher la case correspondant à cette option.

Dans l'exemple d'illustration ci-dessus, le serveur IPAM est installé dans la forêt contoso.com, et le domaine racine de la forêt fabrikam.com est ajouté pour la gestion IPAM. Les rôles serveur sélectionnés permettent à IPAM de découvrir et de gérer les contrôleurs de domaine, les serveurs DHCP et les serveurs DNS dans le domaine racine fabrikam.com et le domaine racine contoso.com.

Une fois que vous avez spécifié des forêts, des domaines et des rôles serveur, cliquez sur **OK**. IPAM effectue la découverte. À l'issue du processus de découverte, vous pouvez gérer les ressources de la forêt locale et de la forêt distante.

Supprimer définitivement les données d'utilisation

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour apprendre à supprimer les données d'utilisation de la base de données IPAM.

Vous devez être membre des **administrateurs IPAM**, du groupe **Administrateurs** de l'ordinateur local ou équivalent, pour effectuer cette procédure.

Pour vider la base de données IPAM

1. Ouvrez le Gestionnaire de serveur, puis accédez à l'interface client IPAM.
2. Accédez à l'un des emplacements suivants : **blocs d'adresses IP**, **inventaire des adresses IP** ou **groupes de plages d'adresses IP**.
3. Cliquez sur **TÂCHES**, puis sur **Vider les données d'utilisation**. La boîte de dialogue **Vider les données d'utilisation** s'ouvre.
4. Dans **Vider toutes les données d'utilisation le ou avant**, cliquez sur **Sélectionner une date**.
5. Choisissez la date pour laquelle vous souhaitez supprimer tous les enregistrements de base de données à la fois le et avant cette date.
6. Cliquez sur **OK**. IPAM supprime tous les enregistrements que vous avez spécifiés.

Contrôle d’accès en fonction du rôle

30/07/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cette rubrique fournit des informations sur l’utilisation du contrôle d’accès en fonction du rôle dans IPAM.

> ⓘ **Notes**
>
> En plus de cette rubrique, la documentation suivante sur le contrôle d’accès IPAM est disponible dans cette section.
>
> - Gérer le contrôle d’accès basé sur les rôles avec le Gestionnaire de serveur
> - Gérer le contrôle d’accès basé sur les rôles avec Windows PowerShell

Le contrôle d’accès en fonction du rôle vous permet de spécifier des privilèges d’accès à différents niveaux, notamment au niveau du serveur DNS, de la zone DNS et de l’enregistrement de ressource DNS. Le contrôle d’accès en fonction du rôle vous permet de spécifier quelles sont les personnes qui ont un contrôle précis sur les opérations de création, de modification et de suppression des différents types d’enregistrement de ressource DNS.

Vous pouvez configurer le contrôle d’accès pour que les actions des utilisateurs se limitent aux autorisations suivantes.

- Les utilisateurs peuvent modifier uniquement des enregistrements de ressources DNS spécifiques
- Les utilisateurs peuvent modifier les enregistrements de ressources DNS d’un type spécifique, par exemple PTR ou MX
- Les utilisateurs peuvent modifier les enregistrements de ressources DNS pour des zones spécifiques

See Also

Gérer le contrôle d’accès en fonction du rôle avec le Gestionnaire de serveurGérer le contrôle d’accès en fonction du rôle avec Windows PowerShellGérer IPAM

Gérer le contrôle d’accès basé sur les rôles avec le Gestionnaire de serveur

14/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser les rubriques suivantes pour gérer le contrôle d’accès en fonction du rôle à l’aide de Gestionnaire de serveur, qui dispose d’une interface utilisateur graphique.

- Créer un rôle d’utilisateur pour le contrôle d’accès
- Créer une stratégie d’accès
- Définir l’étendue d’accès pour une zone DNS
- Définir l’étendue d’accès pour des enregistrements de ressource DNS
- Afficher des rôles et des autorisations de rôle

Vous pouvez également utiliser Windows PowerShell pour gérer le contrôle d’accès en fonction du rôle IPAM. Pour plus d’informations, consultez Gérer le contrôle d’accès en fonction du rôle avec Windows PowerShell.

Voir aussi

Gérer IPAM

Créer un rôle d’utilisateur pour le contrôle d’accès

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

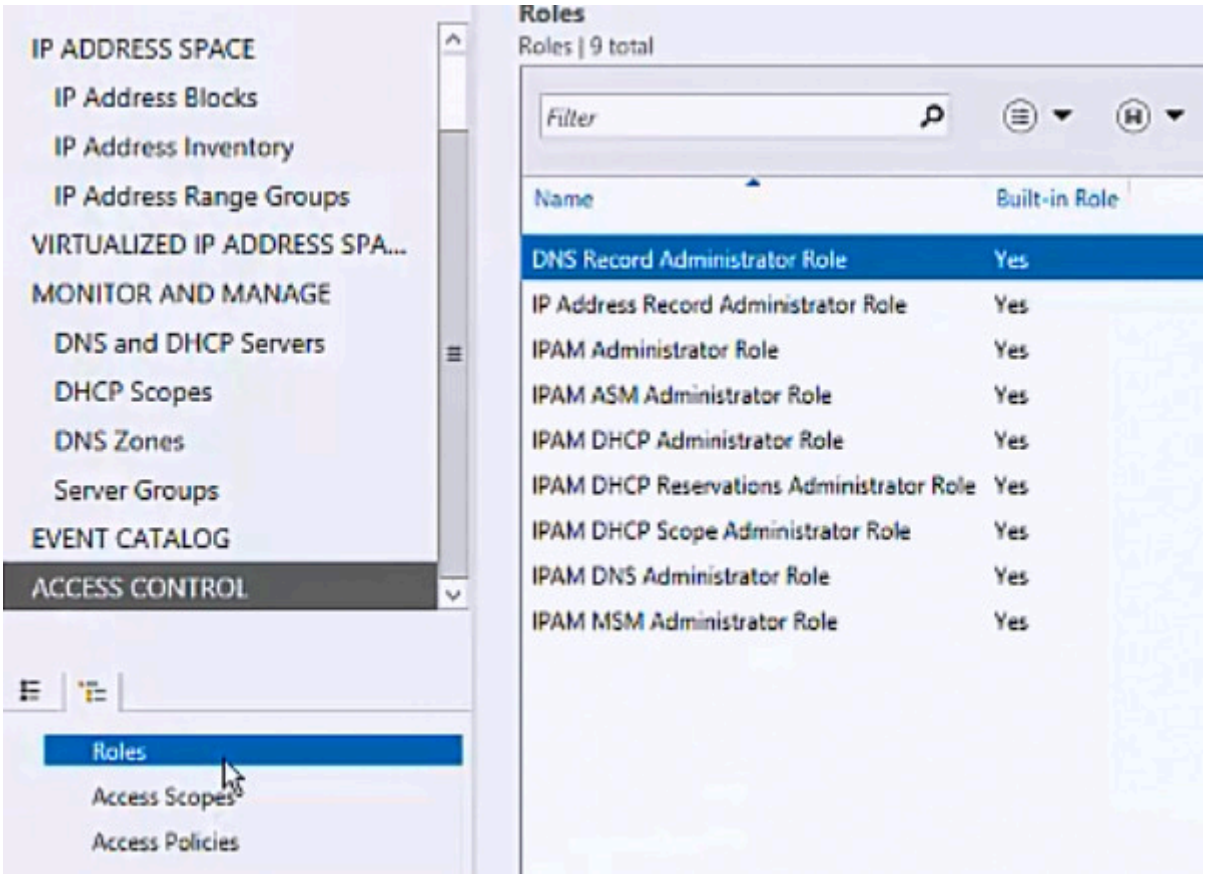
Vous pouvez utiliser cette rubrique pour créer un rôle d’utilisateur pour le contrôle d’accès dans la console cliente IPAM.

L’appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

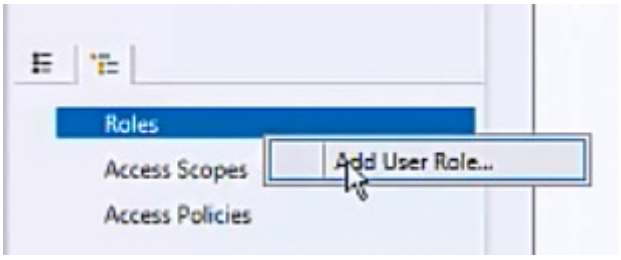
> ⓘ **Notes**
>
> Après avoir créé un rôle, vous pouvez créer une stratégie d’accès pour attribuer le rôle à un utilisateur ou à un groupe Active Directory spécifique. Pour plus d’informations, consultez Créer une stratégie d’accès.

Pour créer un rôle

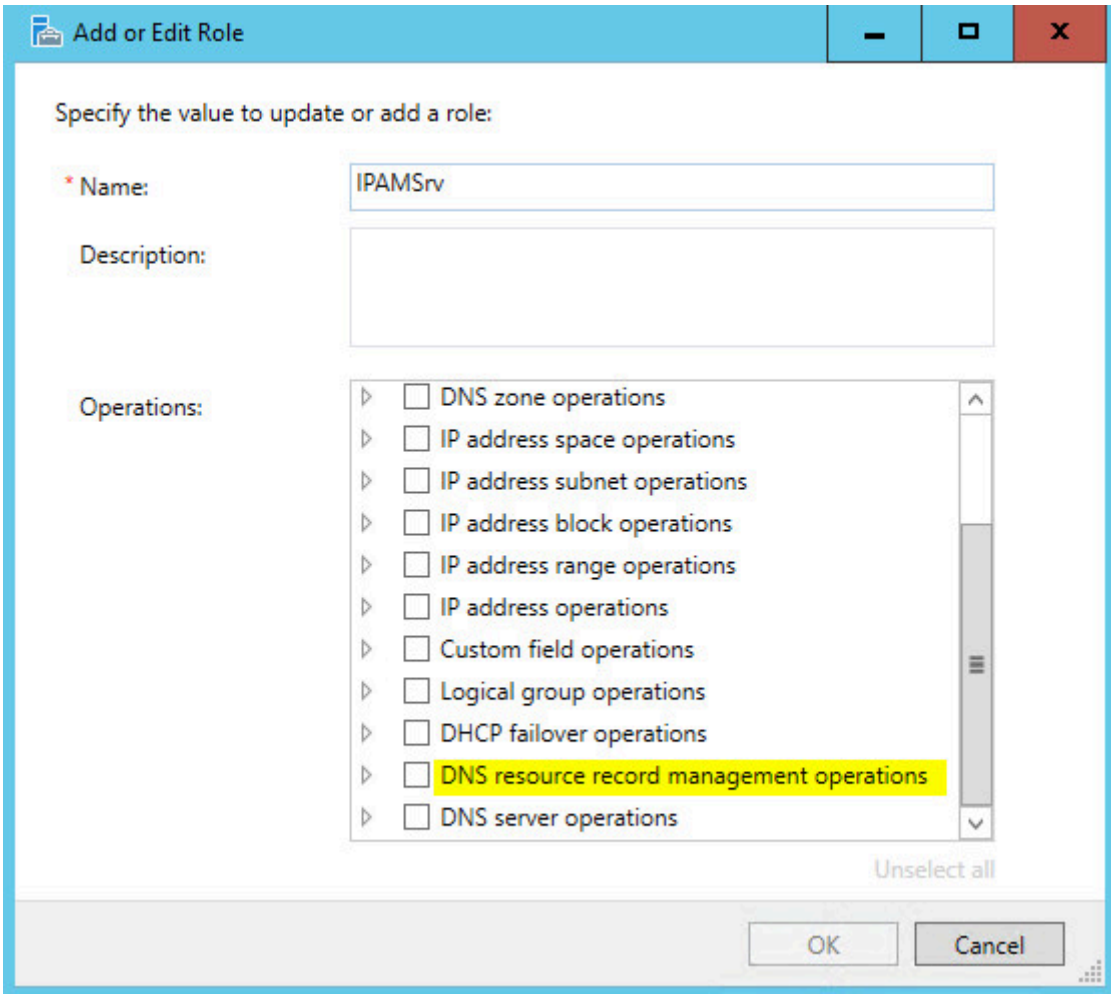
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s’affiche.
2. Dans le volet de navigation, cliquez sur **ACCESS CONTROL**, puis, dans le volet de navigation inférieur, cliquez sur **Rôles**.



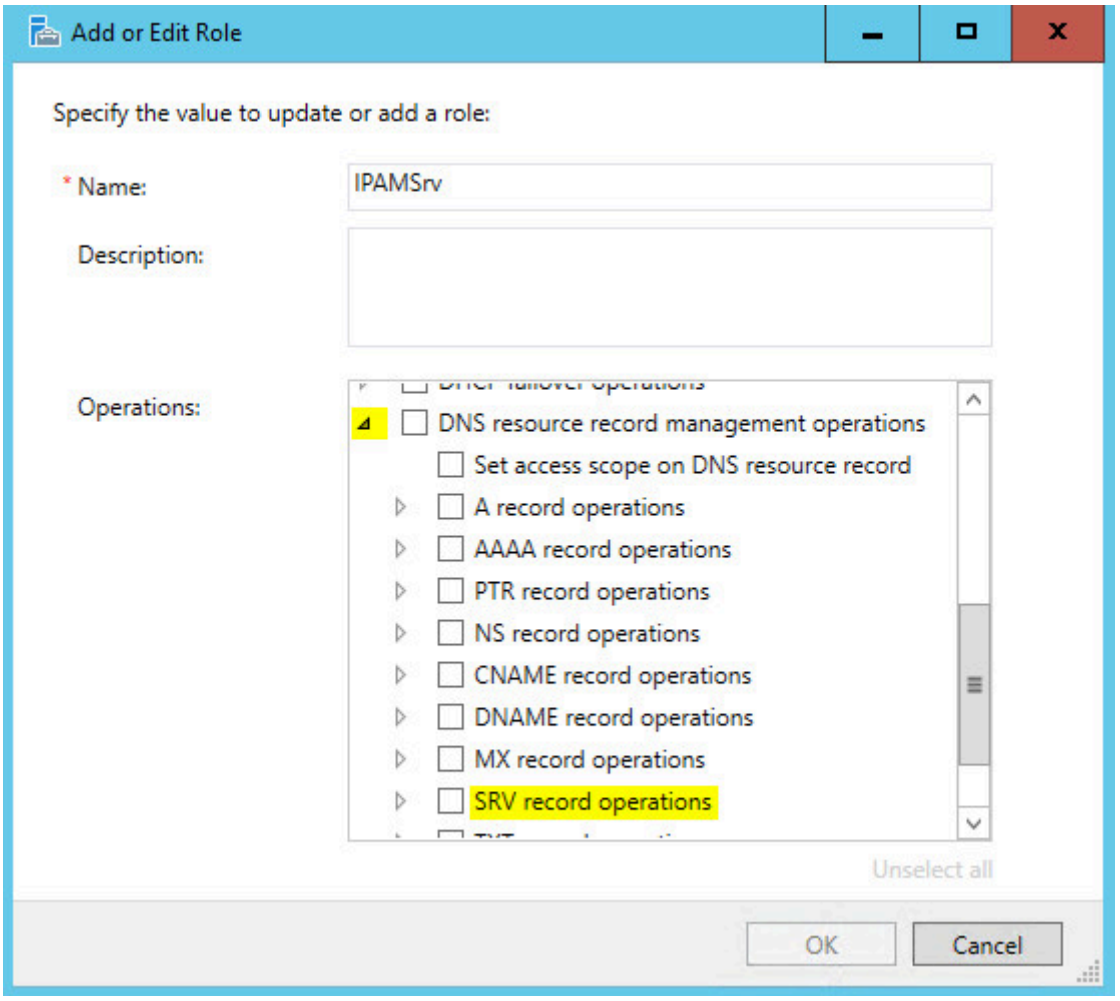
3. Cliquez avec le bouton droit sur **Rôles**, puis cliquez sur **Ajouter un rôle d'utilisateur**.



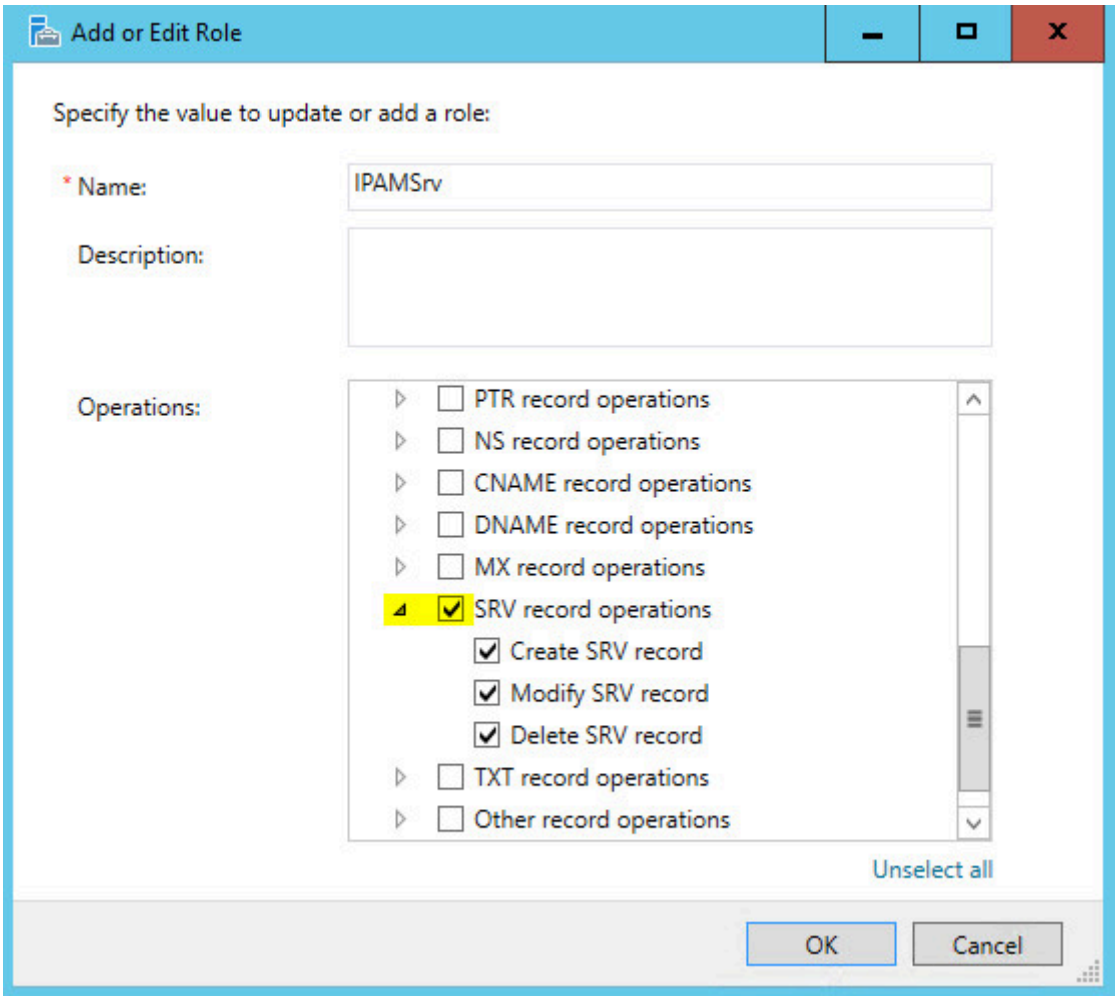
4. La boîte de dialogue **Ajouter ou modifier un rôle** s'ouvre. Dans **Nom**, tapez un nom pour le rôle qui efface la fonction de rôle. Par exemple, si vous souhaitez créer un rôle qui permet aux administrateurs de gérer les enregistrements de ressources DNS SRV, vous pouvez nommer le rôle **IPAMSrv**. Si nécessaire, faites défiler vers le bas dans **Operations** pour localiser le type d'opérations que vous souhaitez définir pour le rôle. Pour cet exemple, faites défiler jusqu'à **Opérations de gestion des enregistrements de ressources DNS**.



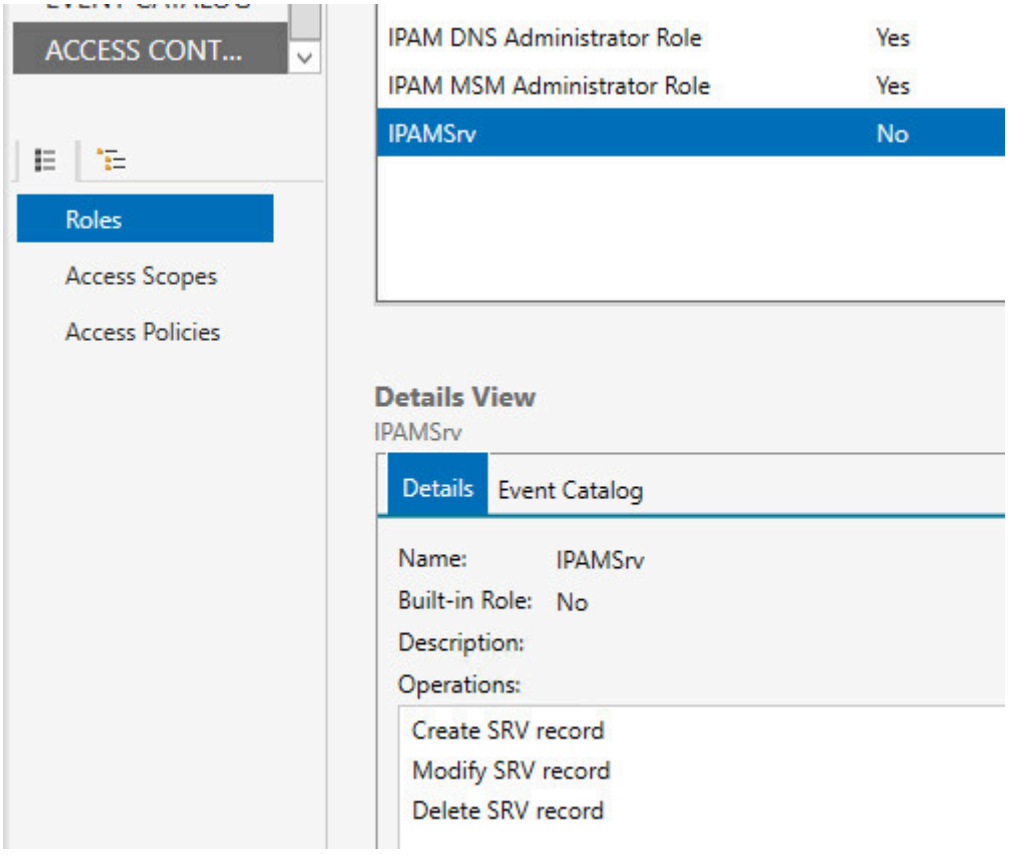
5. Développez **Opérations de gestion des enregistrements de ressources DNS**, puis recherchez les **Opérations d'enregistrement SRV**.



6. Développez et sélectionnez **Opérations d'enregistrement SRV**, puis cliquez sur **OK**.



7. Dans la console cliente IPAM, cliquez sur le rôle que vous venez de créer. En **mode Détails,** les opérations autorisées pour le rôle sont affichées.



Voir aussi

Contrôle d’accès en fonction du rôleGérer IPAM

Créer une stratégie d’accès

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

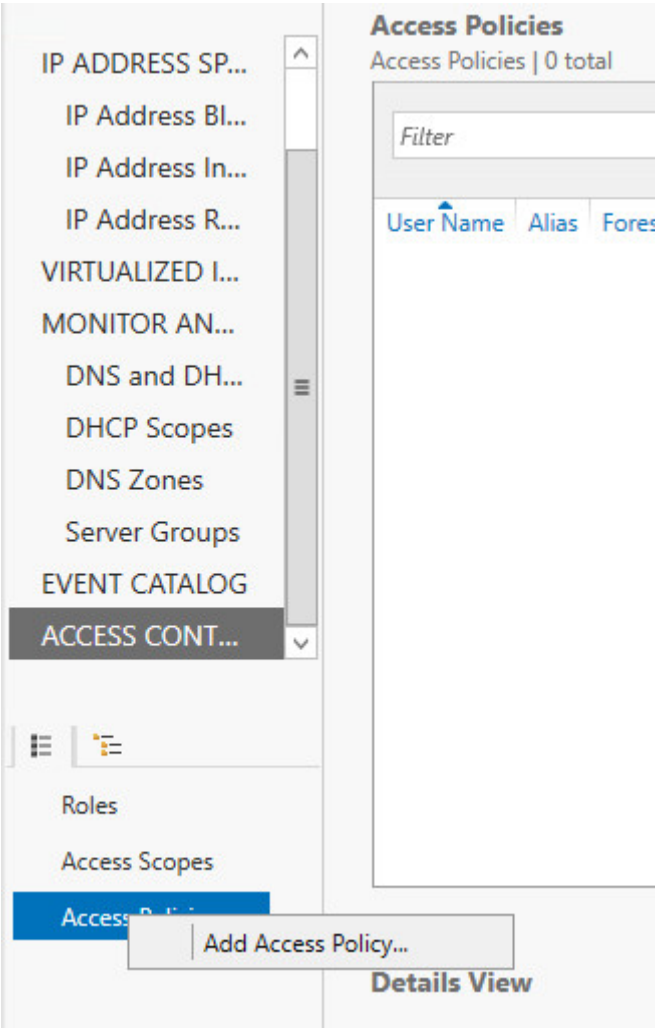
Vous pouvez utiliser cette rubrique pour créer une stratégie d’accès dans la console cliente IPAM.

L’appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

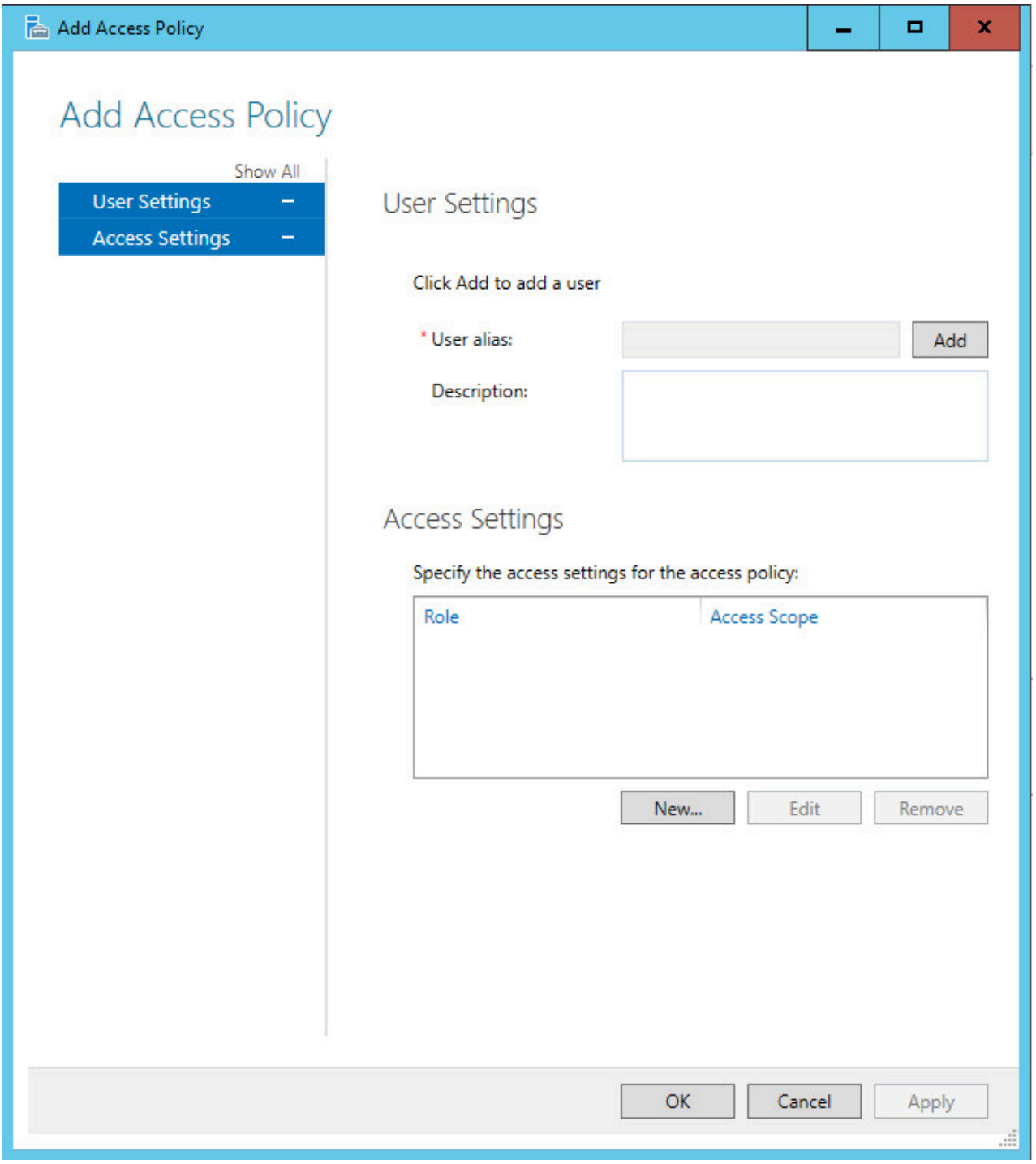
> ⓘ **Notes**
>
> Vous pouvez créer une stratégie d’accès pour un utilisateur spécifique ou pour un groupe d’utilisateurs dans Active Directory. Quand vous créez une stratégie d’accès, vous devez sélectionner un rôle IPAM intégré ou un rôle personnalisé que vous avez créé. Pour plus d’informations sur les rôles personnalisés, consultez Créer un rôle d’utilisateur pour le contrôle d’accès.

Pour créer une stratégie d’accès

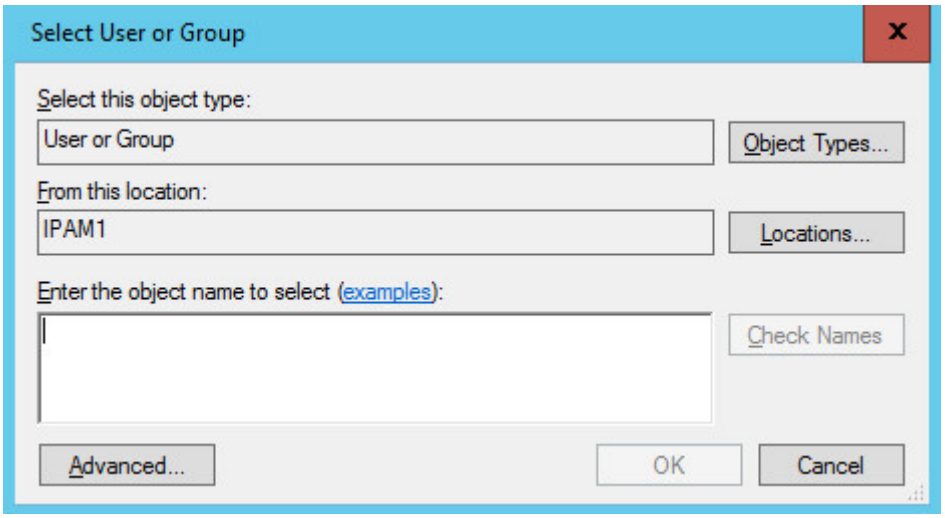
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s’affiche.
2. Dans le volet de navigation, cliquez sur **ACCESS CONTROL**. Dans le volet de navigation inférieur, cliquez avec le bouton droit sur **Stratégies d’accès**, puis cliquez sur **Ajouter une stratégie d’accès**.



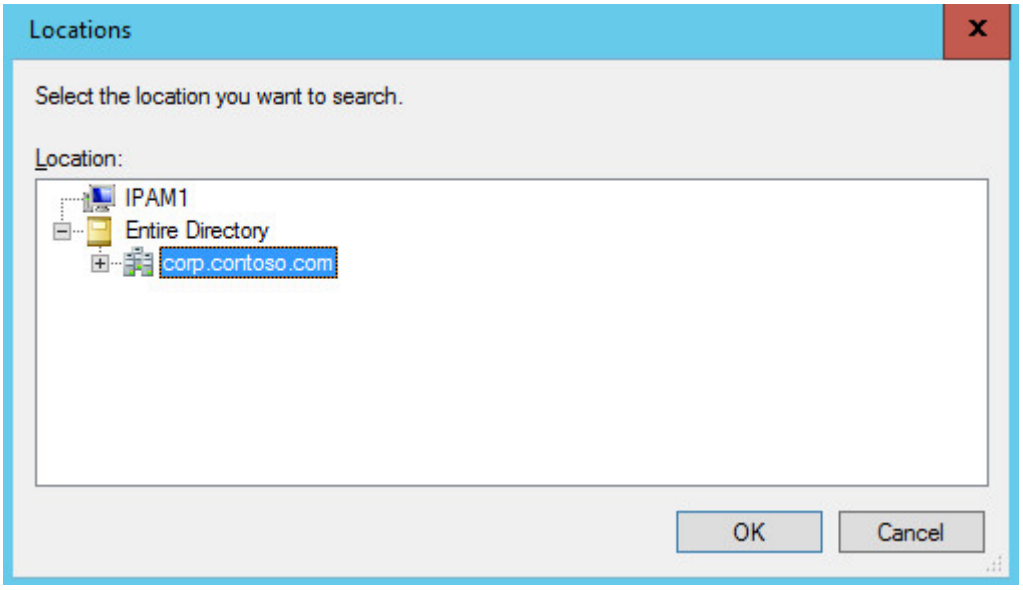
3. La boîte de dialogue **Ajouter une stratégie d'accès** s'ouvre. Dans **Paramètres utilisateur**, cliquez sur **Ajouter**.



4. La boîte de dialogue **Sélectionner un utilisateur ou un groupe** s'ouvre. Cliquez sur **Emplacements**.

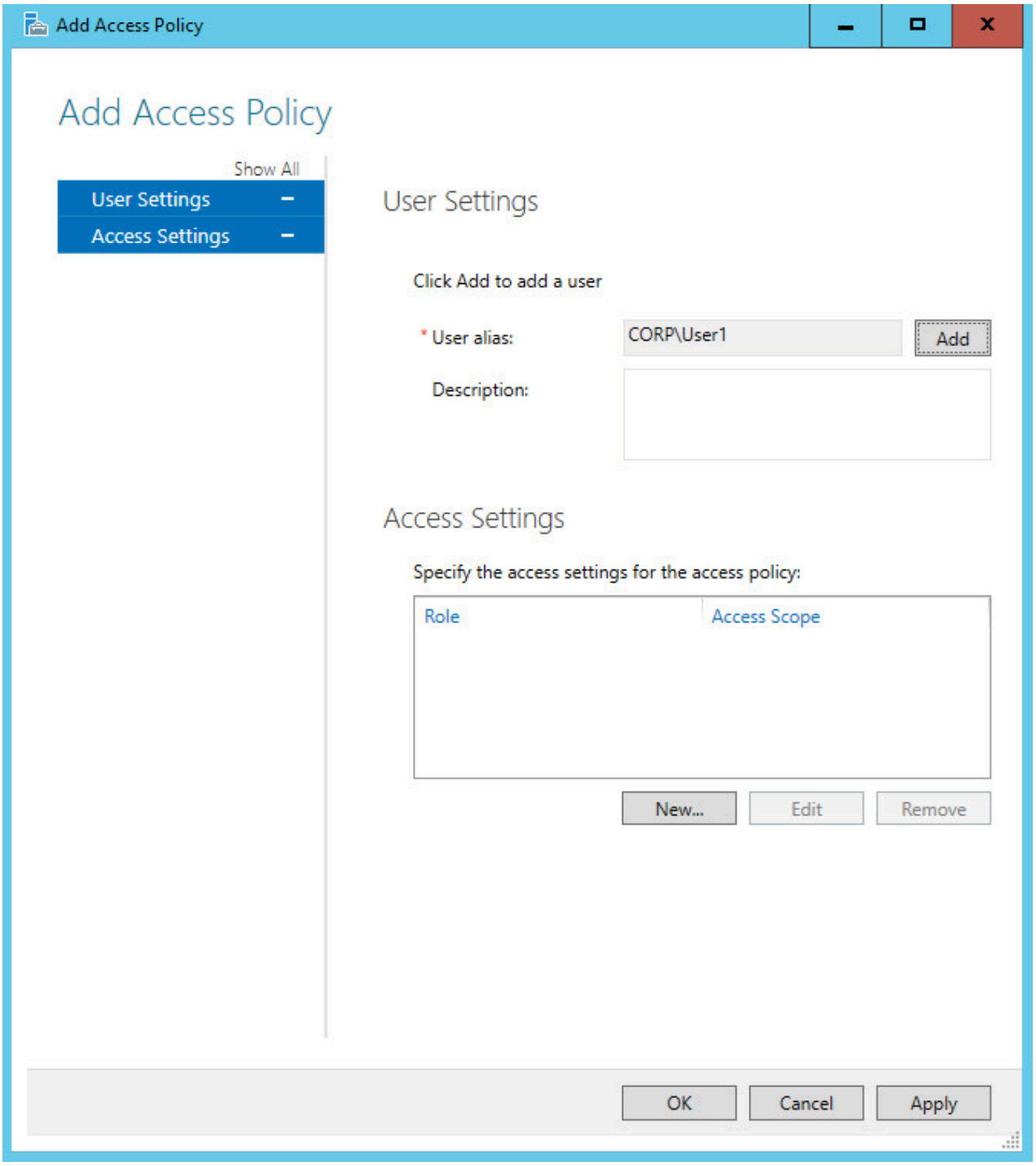


5. La boîte de dialogue **Emplacements s'ouvre** . Accédez à l'emplacement qui contient le compte d'utilisateur, sélectionnez l'emplacement, puis cliquez sur **OK**. La boîte de dialogue **Emplacements** se ferme.

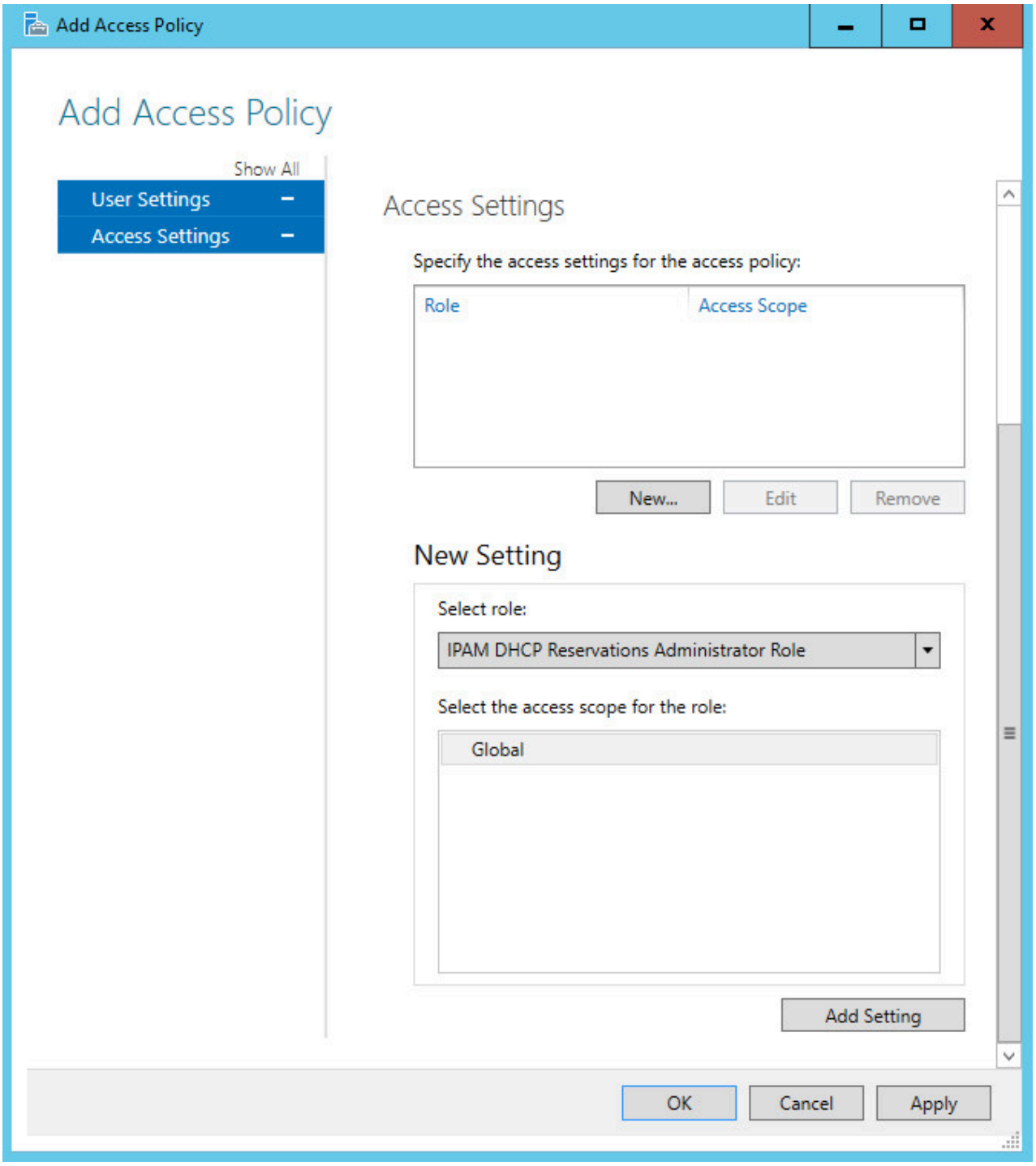


6. Dans la boîte de dialogue **Sélectionner un utilisateur ou un groupe**, dans **Entrez le nom de l'objet à sélectionner**, tapez le nom du compte d'utilisateur pour lequel vous souhaitez créer une stratégie d'accès. Cliquez sur **OK**.

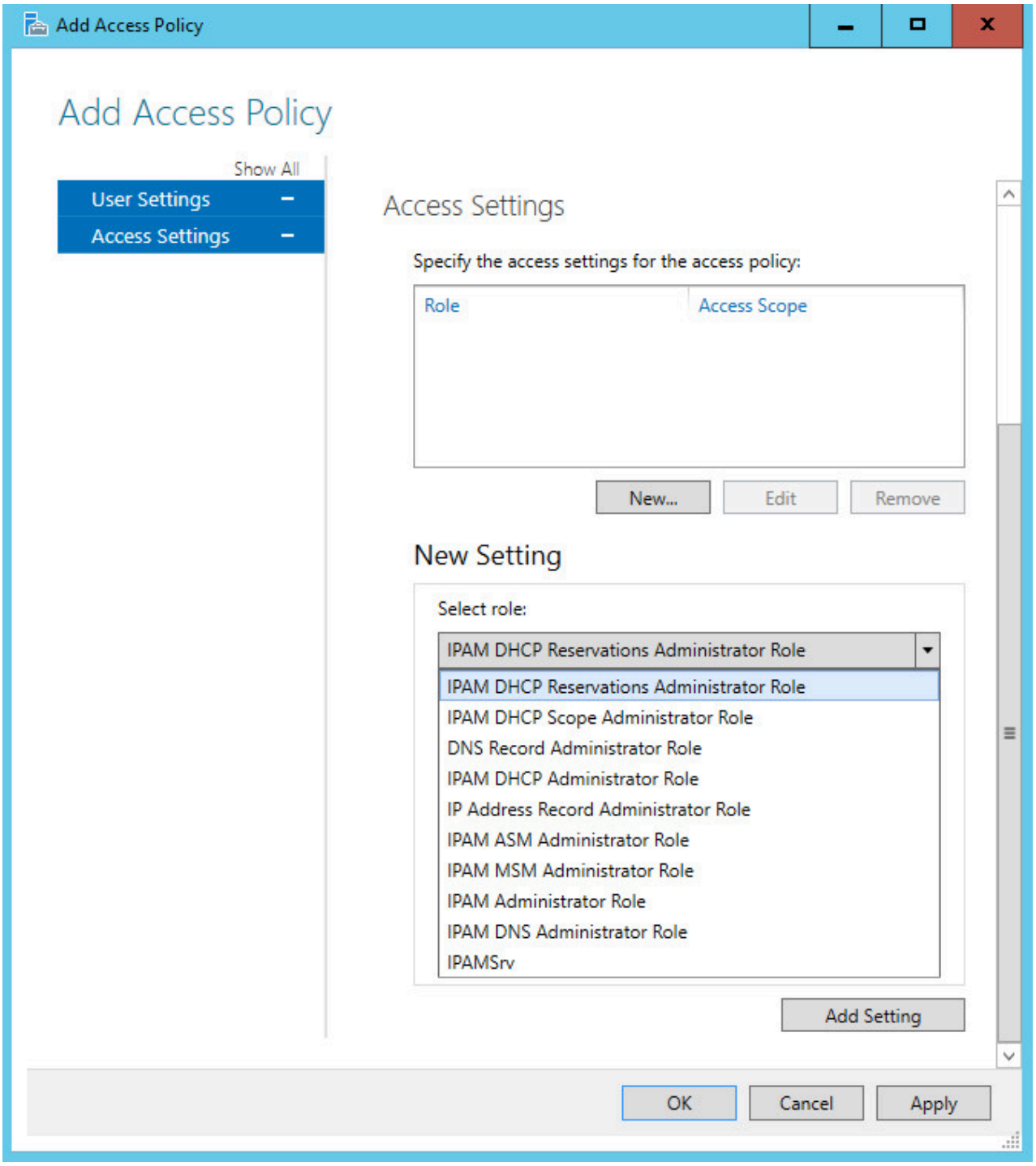
7. Dans **Ajouter une stratégie d'accès**, **Paramètres utilisateur**, l'**Alias de l'utilisateur** contient désormais le compte d'utilisateur auquel la stratégie s'applique. Dans **Paramètres d'accès**, cliquez sur **Nouveau**.



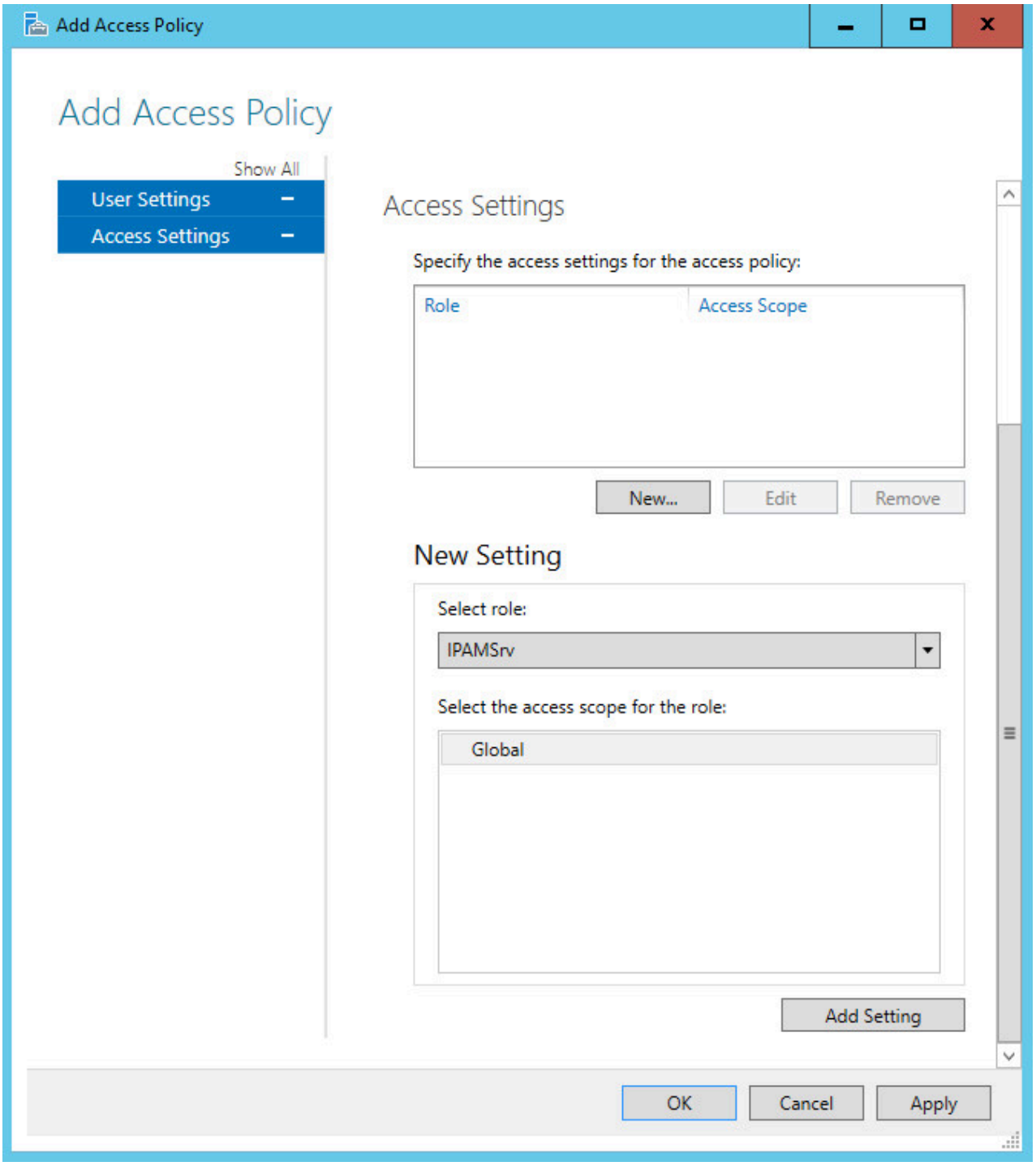
8. Dans **Ajouter une stratégie d'accès**, **Paramètres d'accès** est remplacé par **Nouveau paramètre**.



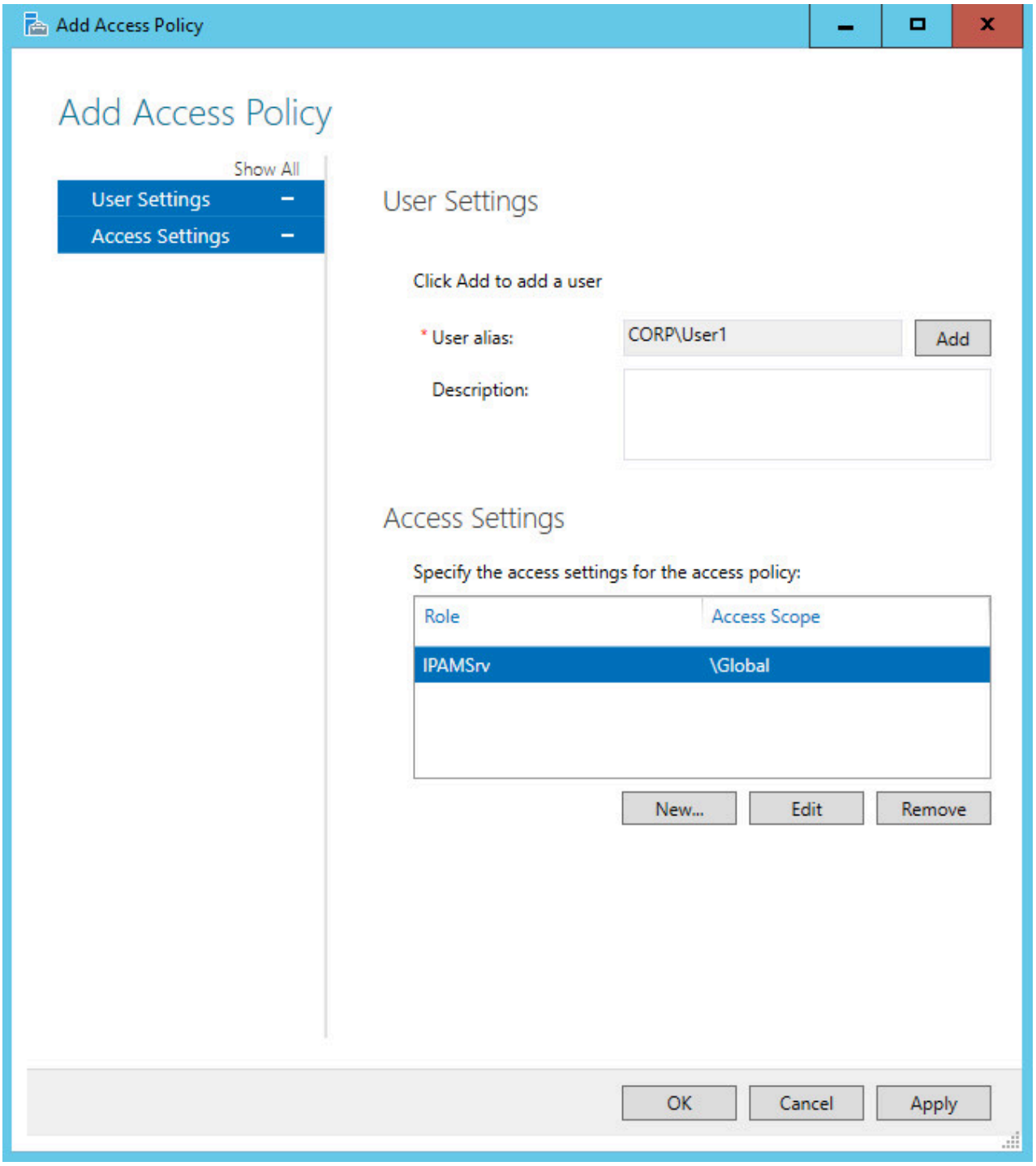
9. Cliquez sur **Sélectionner un rôle** pour développer la liste des rôles. Sélectionnez l'un des rôles intégrés ou, si vous avez créé des rôles, sélectionnez l'un des rôles que vous avez créés. Par exemple, si vous avez créé le rôle IPAMSrv à appliquer à l'utilisateur, cliquez sur **IPAMSrv**.



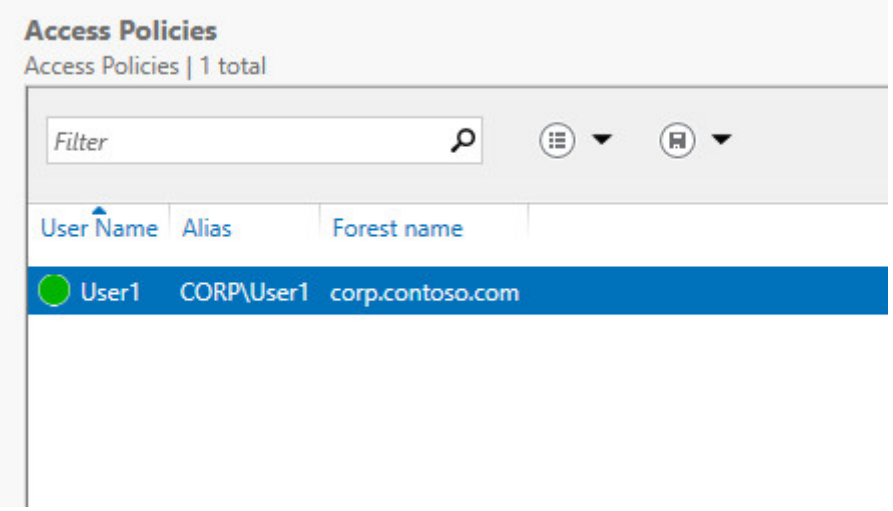
10. Cliquez sur **Ajouter un paramètre**.



11. Le rôle est ajouté à la stratégie d'accès. Pour créer des stratégies d'accès supplémentaires, cliquez sur **Appliquer**, puis répétez ces étapes pour chaque stratégie que vous souhaitez créer. Si vous ne souhaitez pas créer de stratégies supplémentaires, cliquez sur **OK**.



12. Dans le volet d'affichage de la console cliente IPAM, vérifiez que la nouvelle stratégie d'accès a été créée.



Voir aussi

Contrôle d'accès en fonction du rôleGérer IPAM

Définir l’étendue d’accès pour une zone DNS

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

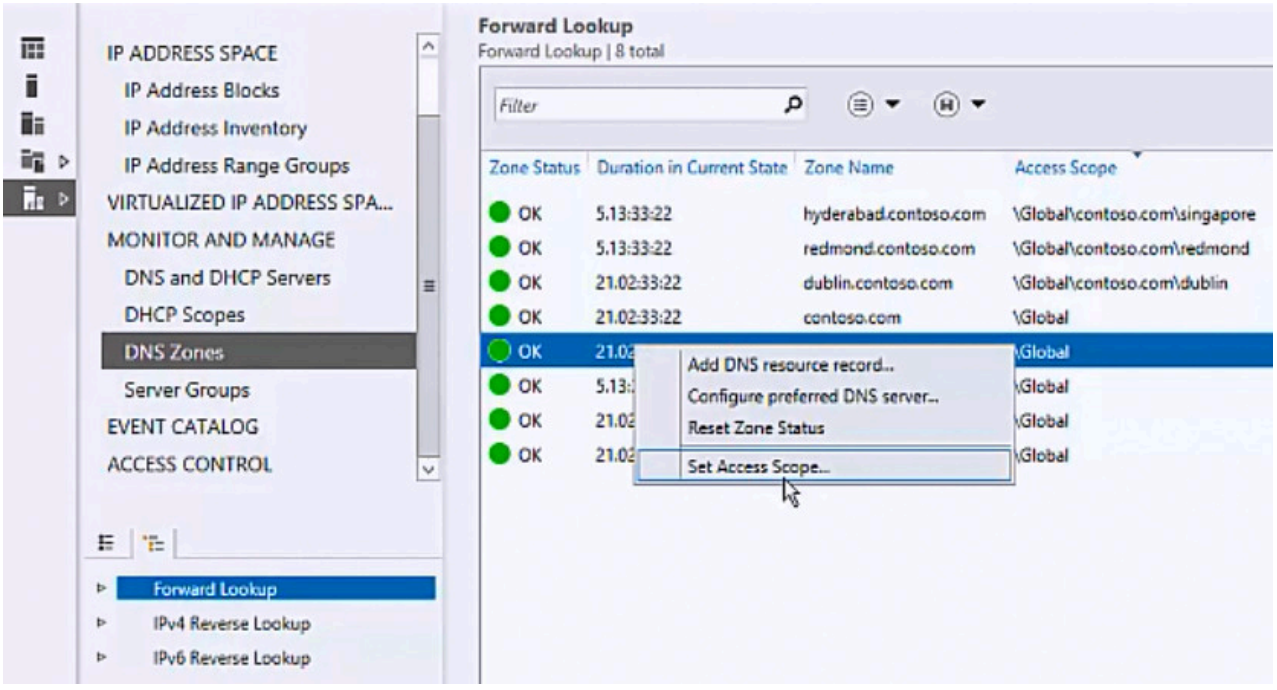
Vous pouvez utiliser cette rubrique pour définir l’étendue de l’accès à une zone DNS à l’aide de la console cliente IPAM.

L’appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

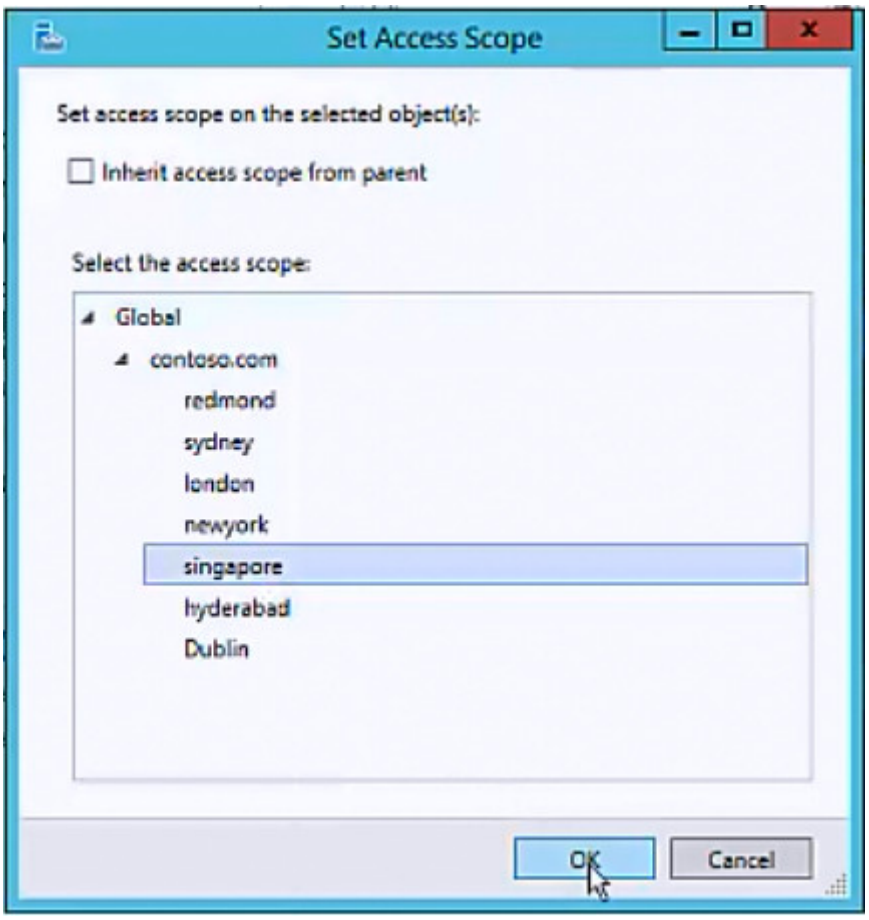
Pour définir l’étendue de l’accès à zone DNS

1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s’affiche.

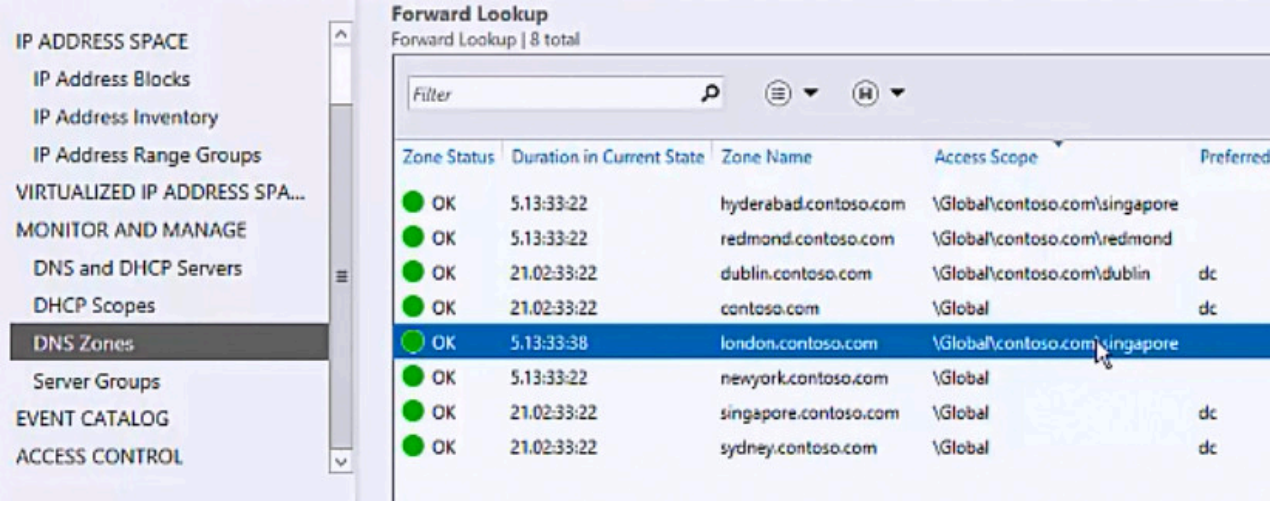
2. Dans le volet de navigation, cliquez sur **Zones DNS**. Dans le volet d’affichage, cliquez avec le bouton droit sur la zone DNS pour laquelle vous souhaitez modifier l’étendue d’accès, puis cliquez sur **Définir l’étendue d’accès**.



3. La boîte de dialogue **Définir l’étendue d’accès** s’ouvre. Si nécessaire pour votre déploiement, cliquez pour **désélectionner Hériter de l'étendue d'accès du parent**. Dans **Sélectionner l’étendue d’accès**, sélectionnez un élément, puis cliquez sur **OK**.



4. Dans le volet d'affichage de la console cliente IPAM, vérifiez que l'étendue de l'accès à la zone est modifiée.



Voir aussi

Contrôle d'accès en fonction du rôleGérer IPAM

Définir l’étendue d’accès pour des enregistrements de ressource DNS

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour définir l’étendue de l’accès à une zone DNS à l’aide de la console cliente IPAM.

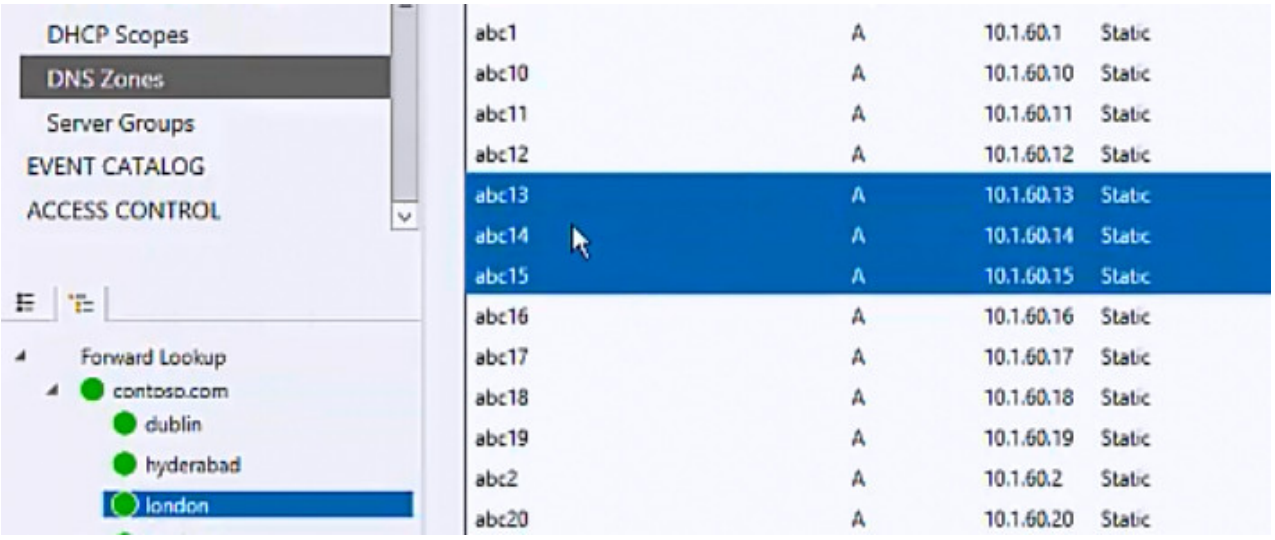
L’appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Définir l’étendue d’accès pour des enregistrements de ressource DNS

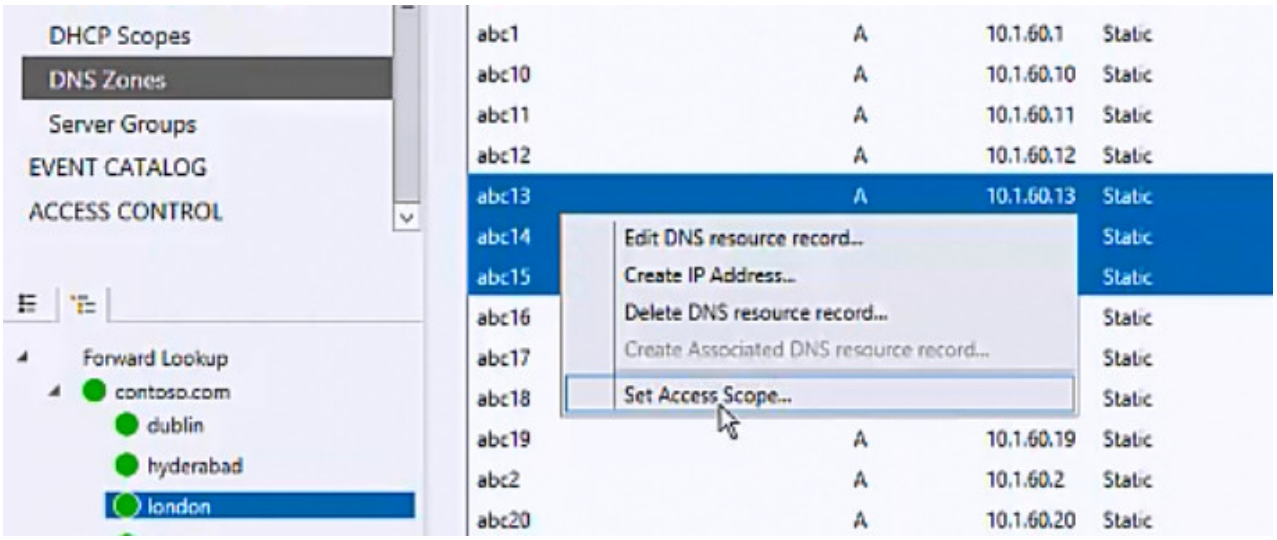
1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s’affiche.

2. Dans le volet de navigation, cliquez sur **Zones DNS**. Dans le volet de navigation inférieur, développez **Recherche vers l’avant** et recherchez et sélectionnez la zone qui contient les enregistrements de ressources dont vous souhaitez modifier l’étendue d’accès.

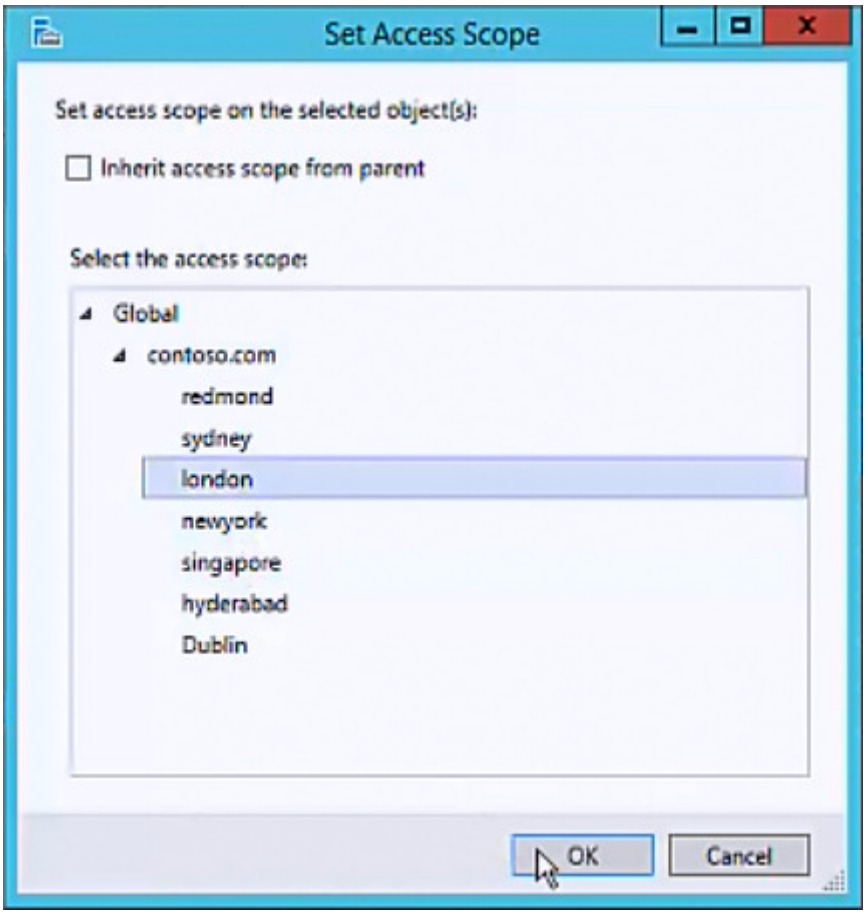
3. Dans le volet d’affichage, recherchez et sélectionnez les enregistrements de ressource dont vous souhaitez modifier l’étendue d’accès.



4. Cliquez avec le bouton droit sur les enregistrements sélectionnés, puis cliquez sur **Définir l’étendue de l’accès**.



5. La boîte de dialogue **Définir l'étendue de l'accès** s'ouvre. Si cela est nécessaire pour votre déploiement, cliquez pour désélectionner **Hériter de l'étendue d'accès du parent**. Dans **Sélectionner l'étendue de l'accès**, sélectionnez un élément, puis cliquez sur **OK**.



Voir aussi

Contrôle d'accès en fonction du rôleGérer IPAM

Afficher des rôles et des autorisations de rôle

16/08/2025

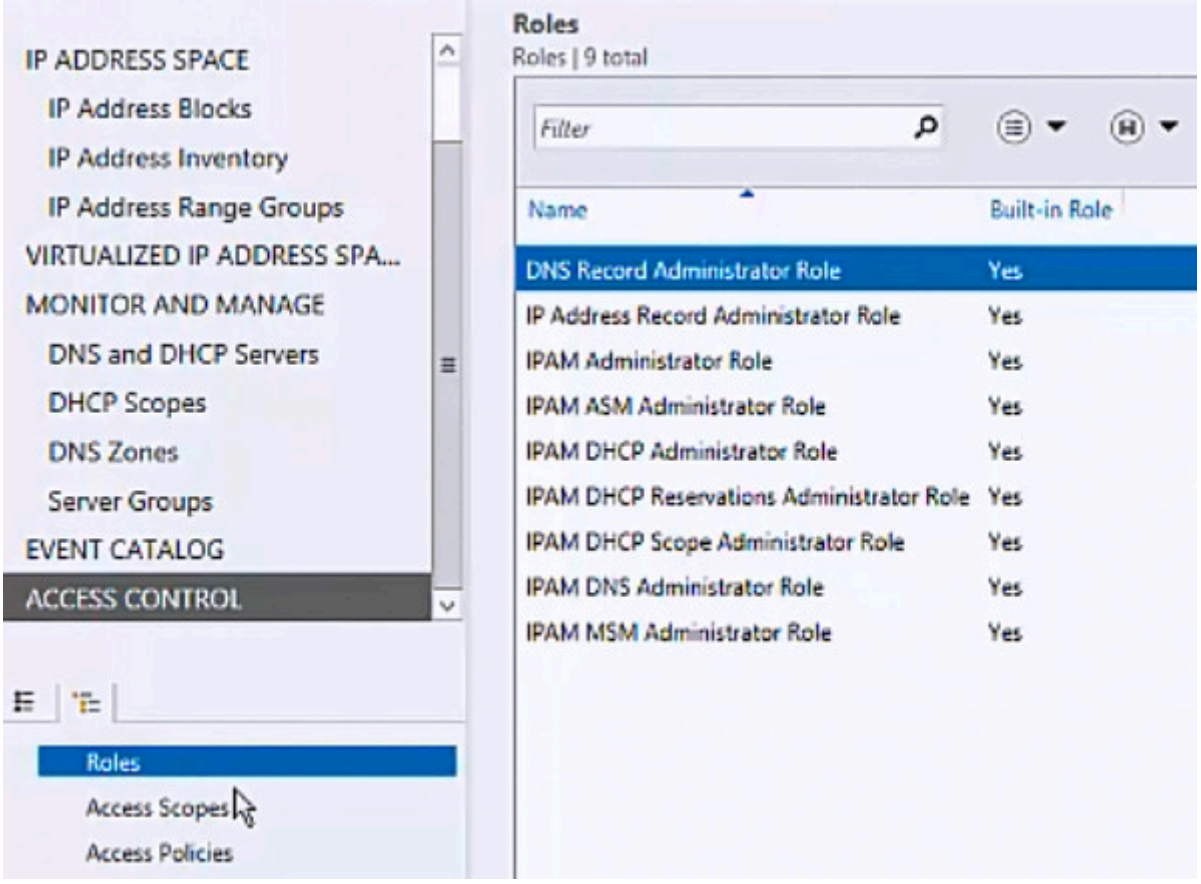
S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour voir les rôles d'utilisateur du contrôle d'accès dans la console cliente IPAM.

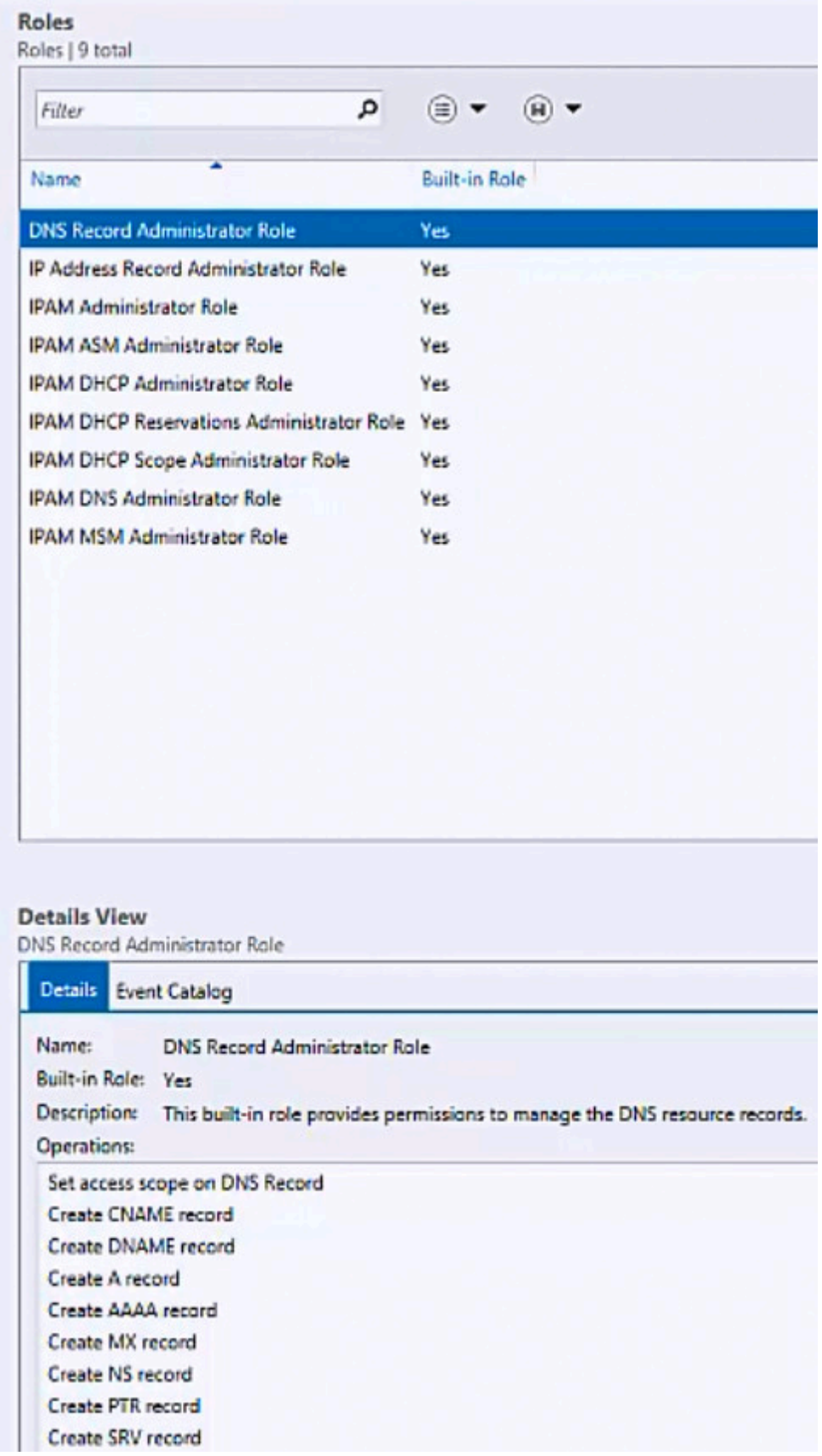
L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour voir les rôles du contrôle d'accès

1. Dans le Gestionnaire de serveur, cliquez sur **IPAM**. La console cliente IPAM s'affiche.
2. Dans le volet de navigation, cliquez sur **ACCESS CONTROL**.
3. Dans le volet de navigation inférieur, cliquez sur **Rôles**. Dans le volet d'affichage, les rôles sont listés.



4. Sélectionnez le rôle dont vous souhaitez voir les autorisations. Dans le volet d'informations inférieur, les opérations autorisées pour le rôle sont affichées.



Voir aussi

Contrôle d’accès en fonction du rôleGérer IPAM

Gérer le contrôle d'accès basé sur les rôles avec Windows PowerShell

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour apprendre à utiliser IPAM pour gérer le contrôle d'accès en fonction du rôle avec Windows PowerShell.

> **Notes**
>
> Pour obtenir la référence de commande Windows PowerShell IPAM, consultez les applets de commande IpamServer dans Windows PowerShell.

Les nouvelles commandes IPAM Windows PowerShell vous permettent de récupérer et de modifier les étendues d'accès des objets DNS et DHCP. Le tableau suivant illustre la commande appropriée à utiliser pour chaque objet IPAM.

Agrandir le tableau

IPAM, objet	Command	Description
Serveur DNS	Get-IpamDnsServer	Cet applet de commande retourne l'objet serveur DNS dans IPAM
DNS Zone	Get-IpamDnsZone	Cet applet de commande retourne l'objet zone DNS dans IPAM
Enregistrement de ressource DNS	Get-IpamResourceRecord	Cet applet de commande retourne l'objet d'enregistrement de ressource DNS dans IPAM
Redirecteur DNS conditionnel	Get-IpamDnsConditionalForwarder	Cet applet de commande retourne l'objet de redirecteur conditionnel DNS dans IPAM
Serveur DHCP	Get-IpamDhcpServer	Cet applet de commande retourne l'objet serveur DNS dans IPAM
DHCP Superscope	Get-IpamDhcpSuperscope	Cet applet de commande retourne l'objet superscope DNS dans IPAM
Étendue DHCP	Get-IpamDhcpScope	Cet applet de commande retourne l'objet étendue DNS dans IPAM

Dans l'exemple de sortie de commande suivant, l'applet `Get-IpamDnsZone` de commande récupère la **zone DNS dublin.contoso.com** .

```
PS C:\Users\Administrator.CONTOSO> Get-IpamDnsZone -ZoneType Forward -ZoneName
dublin.contoso.com

ZoneName             : dublin.contoso.com
ZoneType             : Forward
AccessScopePath      : \Global\Dublin
IsSigned             : False
DynamicUpdateStatus  : None
ScavengeStaleRecords : False
```

Définition d'étendues d'accès sur des objets IPAM

Vous pouvez définir des étendues d'accès sur des objets IPAM à l'aide de la commande `Set-IpamAccessScope`. Vous pouvez utiliser cette commande pour définir l'étendue d'accès sur une valeur spécifique pour un objet ou pour que les objets héritent de l'étendue d'accès des objets parents. Voici les objets que vous pouvez configurer avec cette commande.

- Étendue DHCP
- Serveur DHCP
- DHCP Superscope
- Redirecteur DNS conditionnel
- Enregistrements de ressources DNS
- Serveur DNS
- DNS Zone
- Bloc d'adresses IP
- Plage d'adresses IP
- Espace d'adressage IP
- Sous-réseau d'adresse IP

La syntaxe de la commande `Set-IpamAccessScope` est présentée ci-dessous.

```
NAME
    Set-IpamAccessScope

SYNTAX
    Set-IpamAccessScope [-IpamRange] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
[<CommonParameters>]

    Set-IpamAccessScope [-IpamDnsServer] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamDhcpServer] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamDhcpSuperscope] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamDhcpScope] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamDnsConditionalForwarder] -InputObject
<ciminstance[]> [-AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru]
[-CimSession <CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamDnsResourceRecord] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamDnsZone] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamAddressSpace] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
    [<CommonParameters>]

    Set-IpamAccessScope [-IpamSubnet] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
[<CommonParameters>]
```

```
    Set-IpamAccessScope [-IpamBlock] -InputObject <ciminstance[]> [-
AccessScopePath <string>] [-IsInheritedAccessScope] [-PassThru] [-CimSession
<CimSession[]>] [-ThrottleLimit <int>] [-AsJob] [-WhatIf] [-Confirm]
[<CommonParameters>]
```

Dans l'exemple suivant, l'étendue d'accès de la zone DNS **dublin.contoso.com** est modifiée de **Dublin** à **l'Europe**.

```
PS C:\Users\Administrator.CONTOSO> Get-IpamDnsZone -ZoneType Forward -ZoneName
dublin.contoso.com

ZoneName             : dublin.contoso.com
ZoneType             : Forward
AccessScopePath      : \Global\Dublin
IsSigned             : False
DynamicUpdateStatus  : None
ScavengeStaleRecords : False

PS C:\Users\Administrator.CONTOSO> $a = Get-IpamDnsZone -ZoneType Forward -
ZoneName dublin.contoso.com
PS C:\Users\Administrator.CONTOSO> Set-IpamAccessScope -IpamDnsZone -InputObject
$a -AccessScopePath \Global\Europe -PassThru

ZoneName             : dublin.contoso.com
ZoneType             : Forward
AccessScopePath      : \Global\Europe
IsSigned             : False
DynamicUpdateStatus  : None
ScavengeStaleRecords : False
```

NCSI overview

31/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **ⓘ Important**
>
> Akamai héberge désormais les serveurs de sonde NCSI publics, jusqu'ici hébergés par Azure Front Door. Ce changement s'est produit le 20 juin 2023. To learn more about how this change impacts you, see the NCSI FAQ page.

L'indicateur de statut de connectivité réseau (NCSI) est une fonctionnalité qui permet de fournir un affichage visuel du statut de connexion réseau actuel. L'icône NCSI se trouve en bas à droite de la barre des tâches par défaut. L'apparence de votre appareil dépend de la façon dont celui-cil est connecté au réseau et du système d'exploitation en cours d'exécution.

Agrandir le tableau

Icon	Description
	Connected (Wired)
	Connected (Wireless)
	Connecté (pas d'Internet)

Le statut du réseau peut être affiché en cliquant sur cette icône et vous pouvez consulter d'autres détails sur l'adaptateur réseau en suivant le lien **Paramètres réseau et Internet**. Selon la version de Windows que vous exécutez, les options de la barre des tâches de l'icône NCSI peuvent varier.

NCSI functionality

NCSI utilise des sondes réseau qui sont des requêtes réseau envoyées à un point de terminaison suivies d'une réponse. La sonde NCSI, appelée « sonde active », est une requête/réponse HTTP. Elle utilise également l'interrogation passive, appelée « sonde passive », qui examine passivement le trafic réseau pour déterminer la connectivité.

Quel est l'objectif de NCSI dans Windows ?

NCSI est le composant chargé de déterminer s'il existe une connectivité réseau et s'il s'agit d'Internet ou d'une connexion locale uniquement. NCSI a été développé pour éviter aux applications la tâche complexe de déterminer la configuration réseau par elles-mêmes. Chaque tentative d'exécution d'une tâche sur le réseau nécessite une attention constante pour déterminer si le réseau est toujours accessible. En cas de panne réseau, même par intermittence, l'application interrompt l'opération et teste le réseau en continu jusqu'à ce que la connexion soit stable.

NCSI prend en compte divers facteurs environnementaux tels que les proxys, les zones réactives ou les portails captifs. Il doit déterminer si le réseau détecté peut répondre à ses requêtes, s'il nécessite un accès Internet complet ou un accès privé d'entreprise. Les utilisateurs doivent attendre que NCSI soit termine ses vérifications soit dépasse le délai d'attente pendant que l'application décide comment gérer les scénarios de connectivité réseau restrictive ou inexistante.

Active probing

Une sonde active est une requête http envoyée à un serveur de sonde web pour une adresse NCSI spécifique. Le serveur hébergé par Microsoft sur Internet peut également être le serveur de sonde privé d'une entreprise, ce qui est un scénario plus rare. Lorsque NCSI envoie la sonde et reçoit une réponse valide, il considère que l'appareil client dispose d'une connectivité Internet.

Quand le NCSI ne détecte pas de connectivité internet, c'est que la sonde ne s'achève pas ou qu'elle s'achève avec un échec. Les raisons de l'échec peuvent être liées à l'appareil, à la configuration du réseau ou à d'autres problèmes environnementaux. Un exemple d'échec est la réception d'une réponse **HTTP 403 Interdit**, indiquant généralement qu'un proxy a bloqué la sonde sortante.

> ⚠ **Avertissement**
>
> Ne désactivez pas le sondage actif en tant que résolution d'un problème NCSI, car l'interrogation passive seule n'est pas capable de déterminer l'intégralité des problèmes de connectivité réseau.

Les hôtes et le contenu de la sonde HTTP sont prédéfinis et se trouvent dans le chemin du registre suivant :

registry

```
HKLM\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet
```

NCSI envoie des sondes actives IPv4 et IPv6 distinctes en parallèle. Si l'une des sondes réussit, NCSI détermine que l'appareil dispose d'une connectivité Internet.

Passive probing

Comme pour le sondage actif, le sondage passif utilise les informations apprises des paquets reçus pour déterminer le statut du réseau. Les deux méthodes de sondage se complètent mutuellement, car elles déterminent différemment les conditions réseau intermittentes. Certaines conditions empêchent les sondes actives de fonctionner correctement, telles qu'un routeur temporaire présentant un problème de connectivité intermittent lorsqu'un appareil client ne subit aucune modification de l'état de l'interface. Si des problèmes de connectivité intermittents entraînent des résultats faussement négatifs de la sonde active, l'interrogation passive peut déterminer l'état de la connectivité en fonction du trafic réseau. Cela permet de maintenir un état précis de la connectivité Internet.

> **Notes**
>
> Depuis Windows 11, NCSI est hébergé dans le service Network List Manager, également appelé Gestionnaire de profils réseau. Les itérations de système d'exploitation précédentes étaient hébergées dans le service NLA (Network Location Awareness).

L'objectif principal de la sonde passive est de mettre à jour le statut de la connectivité de NCSI pour toutes les interfaces réseau actives en fonction des données de paquet reçues. Pour chaque interface active, la sonde peut mettre à jour le statut vers Internet ou local en inspectant constamment les paquets entrants pour déterminer le nombre de sauts parcourus à partir de l'expéditeur.

Les sondages actifs et passifs peuvent rencontrer des problèmes. Pour plus d'informations, consultez les raisons de l'échec de la sonde réseau.

Proxies

NCSI fonctionne avec des proxys à l'aide d'informations de proxy stockées dans l'exécution de sondes actives. Les problèmes les plus courants liés aux sondes actives ne laissant pas d'espaces réseau d'entreprise à Internet sont dus aux raisons suivantes :

- Un proxy existe mais n'est pas encore découvert.
- Un proxy a été découvert, mais l'appareil client ne peut pas l'atteindre au moment de la sonde.
- Le fichier PAC (Proxy Auto-Config) est mal configuré et n'a pas été mappé `www.msftconnecttest.com` au bon proxy.

- Le proxy est incorrectement configuré.

NCSI détecte l'adresse proxy provisionnée manuellement à partir du chemin de registre suivant :

```registry
HKLM\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet\ManualProxies
```

> **Conseil**
>
> In Windows 10, users can perform manual proxy configuration by navigating to **Start**>**Settings**>**Network & Internet**>**Proxy**>**Manual proxy setup**.

Captive portals

NCSI détecte les proxys au sein d'une entreprise pour naviguer avec succès une sonde vers Internet. Il identifie également les obstacles en dehors d'un environnement d'entreprise pour les consommateurs sur des appareils mobiles. Les portails captifs se trouvent en grande partie dans les environnements publics tels que les aéroports, les hôpitaux, les cafés, etc., mais peuvent également être des passerelles dans les extensions satellites des réseaux d'entreprise.

Les portails captifs peuvent envoyer une redirection HTTP ou une réponse vide à la sonde au lieu de l'autoriser à passer par Internet. NCSI est en mesure de déterminer s'il se trouve derrière un portail captif tant que les conditions suivantes sont remplies :

- Une sonde HTTP active a été envoyée, mais pas via un proxy connu.
- La sonde a obtenu une réponse.
- La charge utile de la réponse ne correspondait pas au contenu attendu : `Microsoft Connect Test`.

See also

- Guide de résolution des problèmes NCSI
- NCSI FAQ

Comment collecter des données pour diagnostiquer les problèmes NCSI

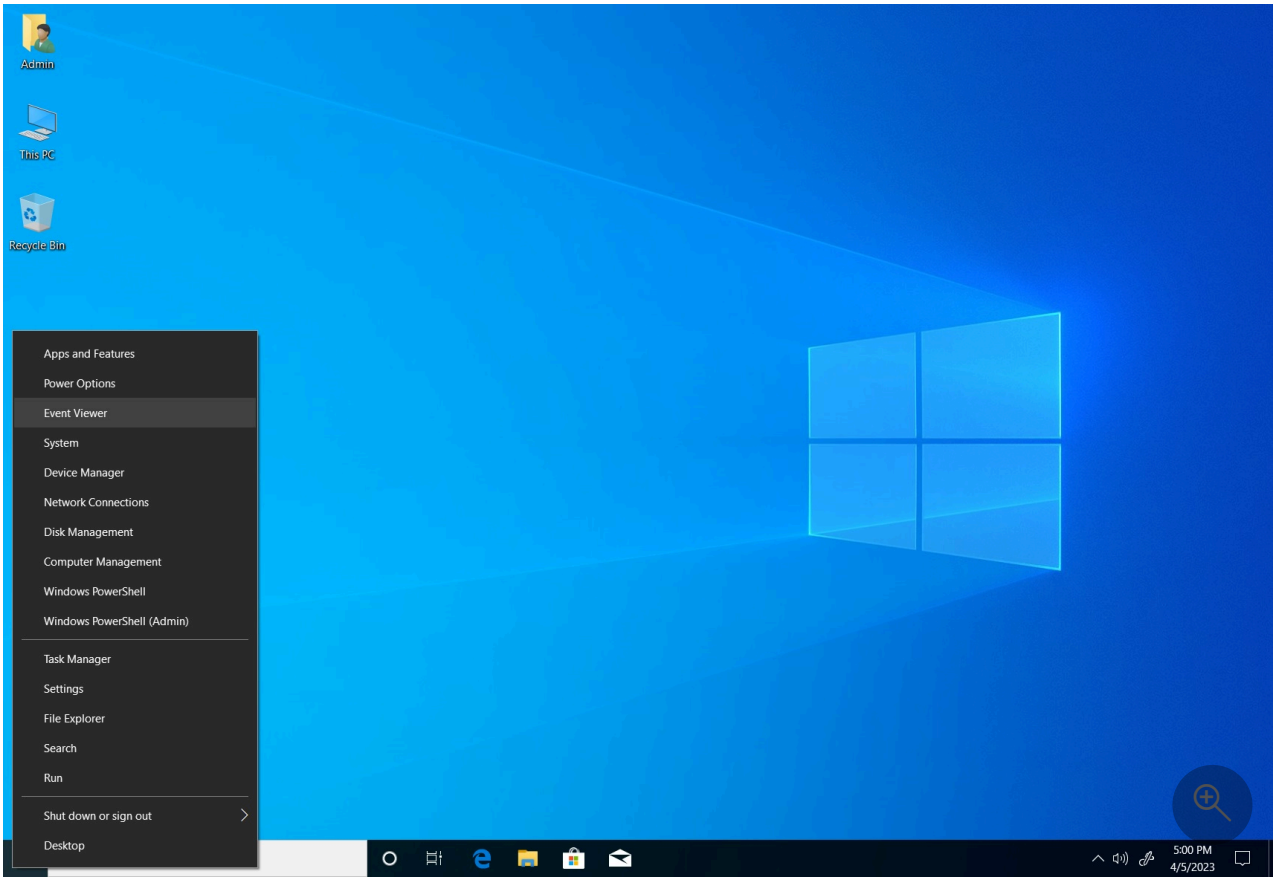
16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

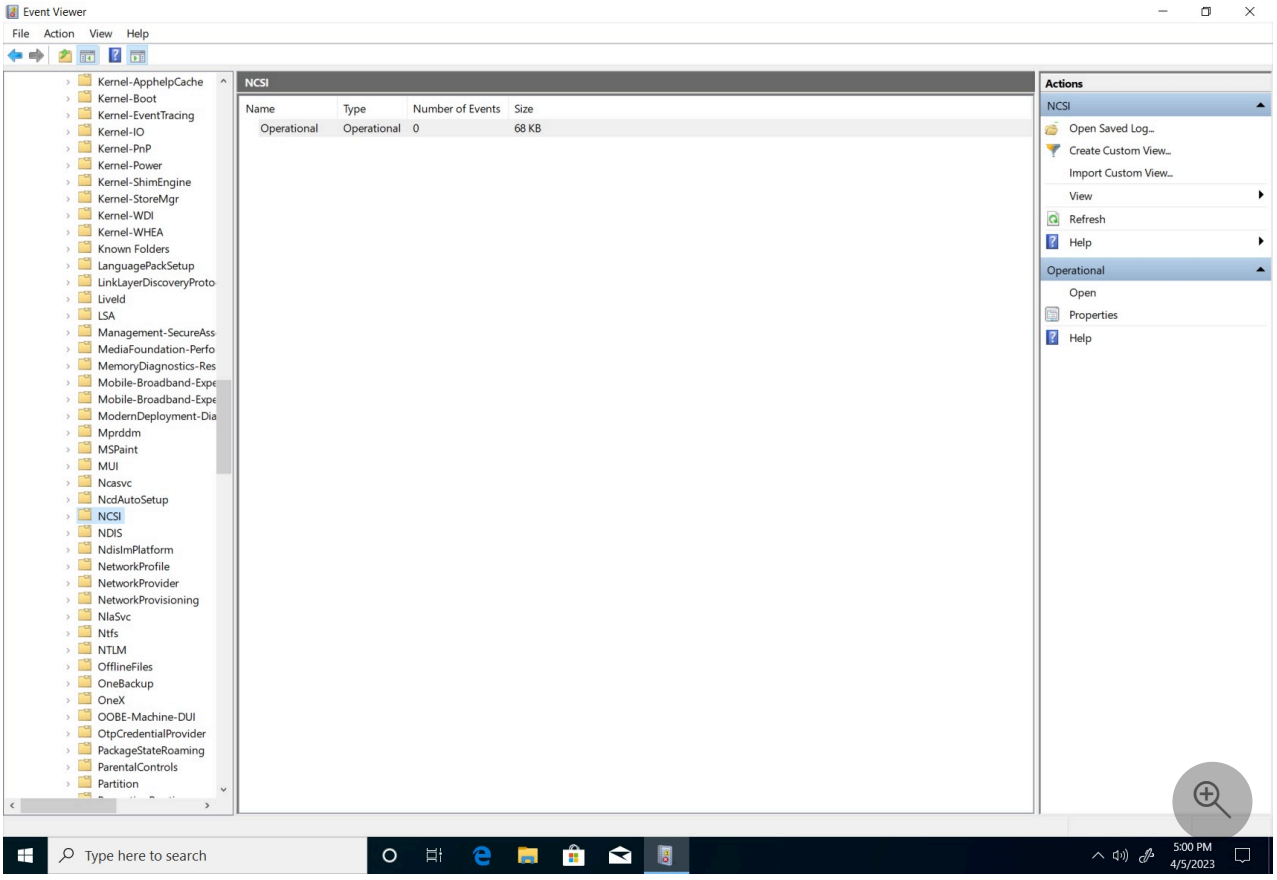
La résolution des problèmes NCSI (Network Connectivity Status Indicator) est généralement effectuée avec les données de capture de paquets, mais les journaux d'événements NCSI peuvent également être un outil utile lorsqu'ils sont corrélés avec le trafic de paquets. Ce guide aide les utilisateurs à diagnostiquer les problèmes NCSI à partir de scénarios courants.

Afficher les données du NCSI à l'aide de l'observateur d'événements

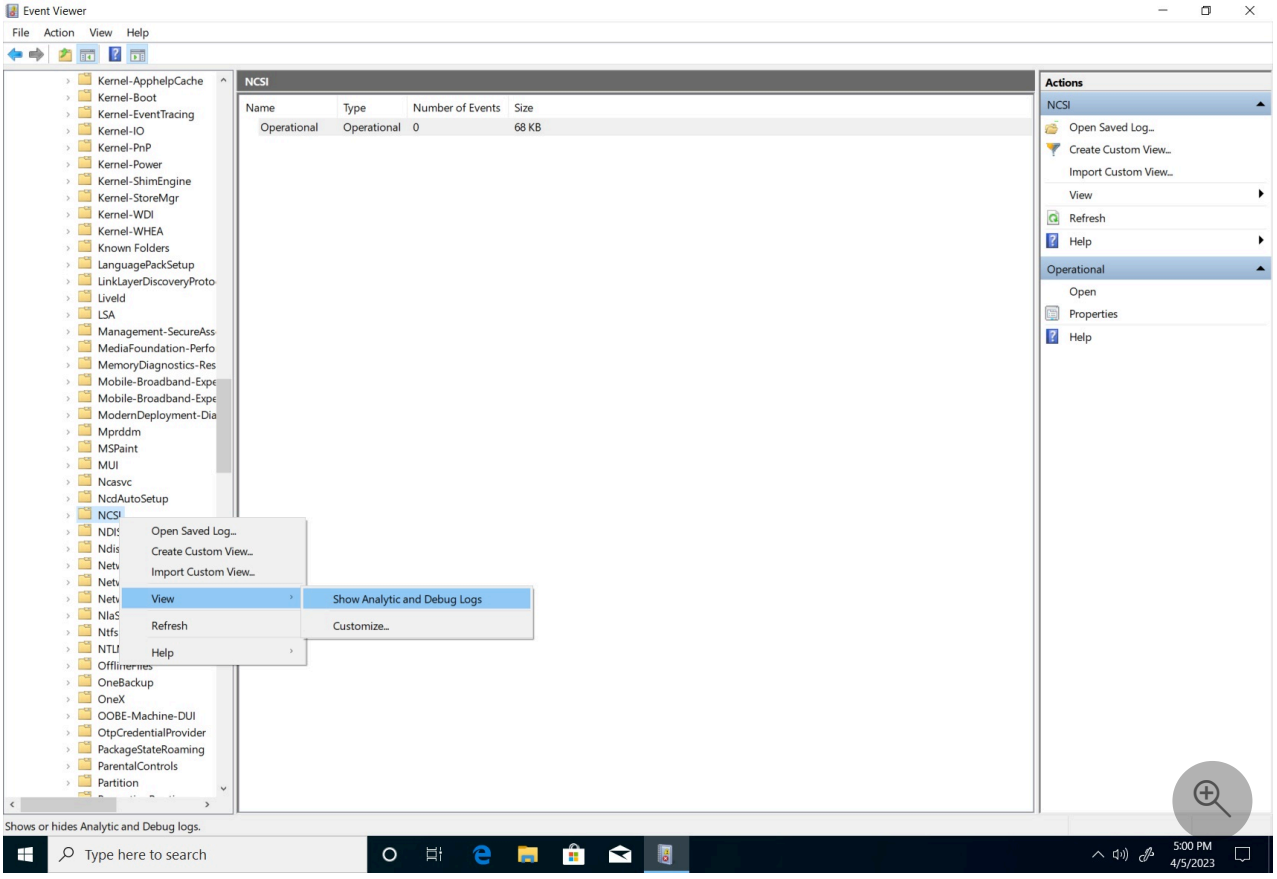
1. Pour ouvrir **l'Observateur d'événements**, cliquez avec le bouton droit sur **Démarrer**>**l'Observateur d'événements**.
   Vous pouvez également ouvrir l'invite d'exécution en appuyant sur **Win+R** et en tapant eventviewer.exe.



2. Développez **Applications et journaux de service**>**Microsoft**>**Windows**>**NCSI**.

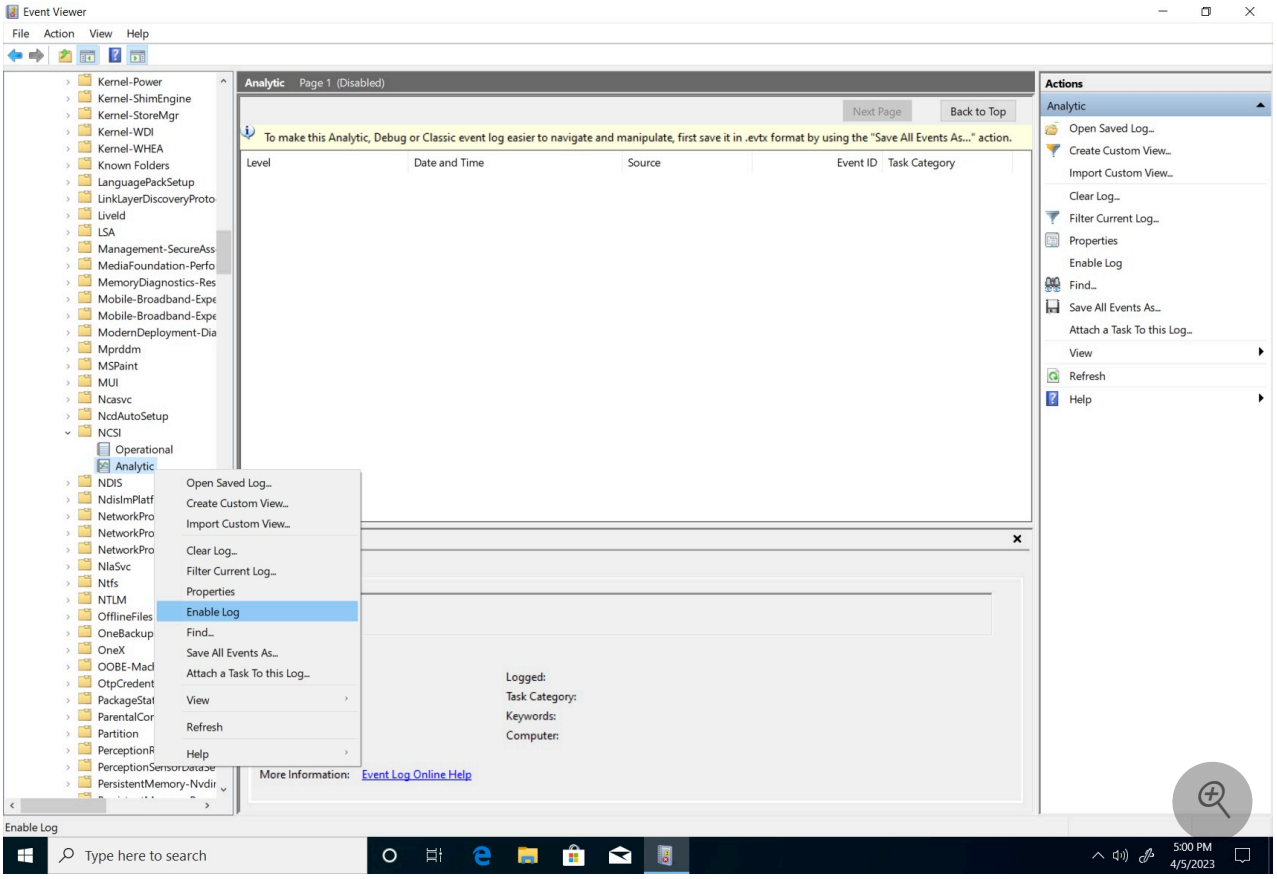


3. Cliquez avec le bouton droit sur **NCSI**, sélectionnez **Afficher les**>**journaux d'analyse et de débogage**.



4. Cliquez avec le bouton droit sur **Analytique** sous le dossier **NCSI** , sélectionnez **Activer le journal**.

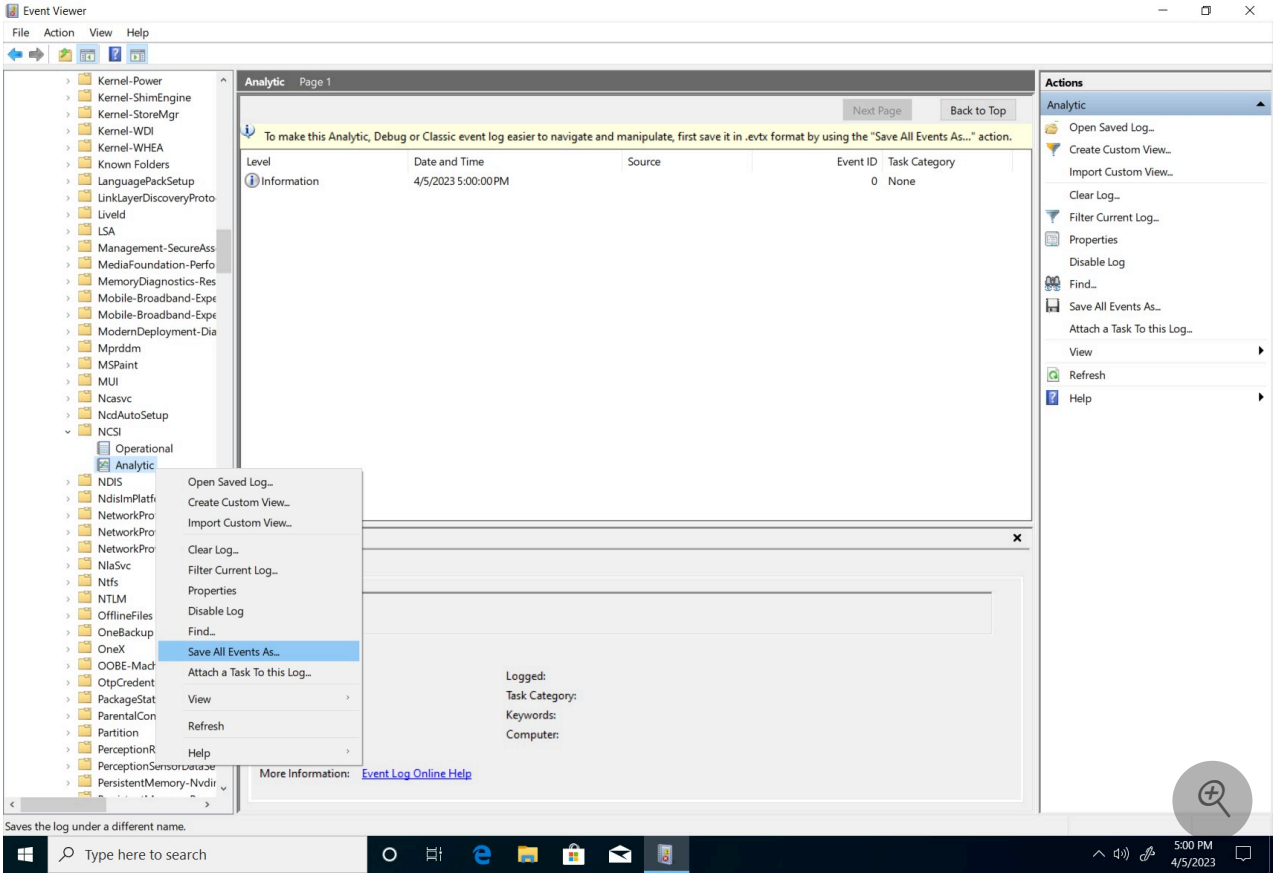
*Une boîte de dialogue peut vous avertir que vous risquez de perdre des événements de journaux d'analytique et de débogage lorsque la journalisation est activée. Sélectionnez **Ok** pour continuer.*



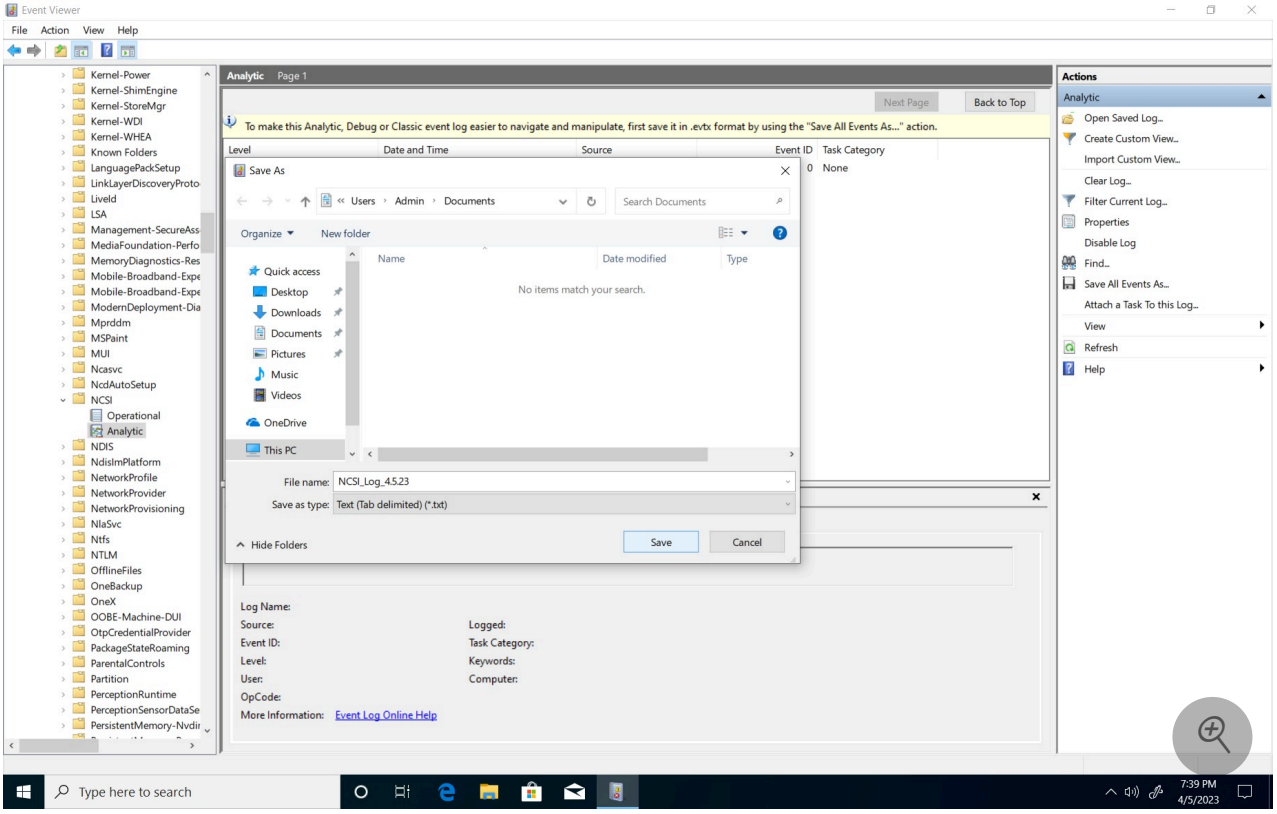
Récupérer les données NCSI à l'aide de l'observateur d'événements

*L'exécution des actions mentionnées ci-dessus facilite l'extraction de données. Pour faciliter l'analyse, convertissez les journaux générés au format texte. Dans **l'Observateur d'événements**, procédez comme suit :*

1. *Développez **Applications et journaux de service**>**Microsoft**>**Windows**>**NCSI**.*
2. *Cliquez avec le bouton droit sur **Analytique**, sélectionnez **Enregistrer tous les événements sous**.*



3. *La boîte de dialogue « Enregistrer sous » s'affiche. Définissez « Enregistrer sous type » sur texte (*.txt), nommez votre fichier et sélectionnez votre emplacement. Cliquez sur* ***Enregistrer****.*



Voici un exemple de sortie de connexion réussie :

Sortie

```
Information    4/26/2023 12:17:46 PM    Microsoft-Windows-NCSI    4013    Internet
Connectivity Detection    Active Internet Probe started on interface {611346db-
8fbb-473d-808b-6c7573b3ef4d}
Information    4/26/2023 12:17:46 PM    Microsoft-Windows-NCSI    4017    Internet
Connectivity Detection    Active Internet Probe (HTTP) started on interface
{611346db-8fbb-473d-808b-6c7573b3ef4d}
Information    4/26/2023 12:17:48 PM    Microsoft-Windows-NCSI    4005    Wait for
Internet Connectivity     Entered State: Internet Connectivity Interface Luid:
0x6008001000000
Information    4/26/2023 12:18:07 PM    Microsoft-Windows-NCSI    4018    Internet
Connectivity Detection    Active Internet Probe (HTTP) finished on interface
{611346db-8fbb-473d-808b-6c7573b3ef4d}
Information    4/26/2023 12:18:07 PM    Microsoft-Windows-NCSI    4014    Internet
Connectivity Detection    Active Internet Probe finished on interface {611346db-
8fbb-473d-808b-6c7573b3ef4d} (false)
```

Voici un exemple de sortie de connexion ayant échoué :

Sortie

```
Information    4/26/2023 12:01:02 PM    Microsoft-Windows-NCSI    4013    Internet
Connectivity Detection    Active Internet Probe started on interface {611346db-
8fbb-473d-808b-6c7573b3ef4d}
Information    4/26/2023 12:01:02 PM    Microsoft-Windows-NCSI    4017    Internet
Connectivity Detection    Active Internet Probe (HTTP) started on interface
{611346db-8fbb-473d-808b-6c7573b3ef4d}
Information    4/26/2023 12:01:04 PM    Microsoft-Windows-NCSI    4005    Wait for
Internet Connectivity     Entered State: Local Connectivity Interface Luid:
0x6008001000000
Information    4/26/2023 12:03:23 PM    Microsoft-Windows-NCSI    4018    Internet
Connectivity Detection    Active Internet Probe (HTTP) finished on interface
{611346db-8fbb-473d-808b-6c7573b3ef4d}
Warning        4/26/2023 12:03:23 PM    Microsoft-Windows-NCSI    4051    None
Active probe result code on interface {611346db-8fbb-473d-808b-6c7573b3ef4d}
(0x6008001000000 Family: V4) = 12007
```

*Mettre en corrélation les événements **NCSI analytiques** et **opérationnels** avec les horodatages de capture de paquets pour déterminer si la sonde active a été déclenchée, si elle s'est terminée et pourquoi elle a échoué. Pour en savoir plus sur les codes d'erreur Winhttp, consultez messages d'erreur (Winhttp.h).*

Comment reproduire un scénario de problème

Vous pouvez résoudre un problème en forçant une sonde active à voir si elle se termine. Le moyen le plus simple consiste à provoquer un événement de modification réseau. L'exemple suivant illustre cela sur les connexions câblées et sans fil :

Wired

1. *Déconnectez le câble Ethernet. (Vous pouvez également désactiver l'adaptateur réseau dans Paramètres réseau avancés.)*
2. *Utilisez un logiciel de capture de paquets, tel que wireshark, et attendez 30 secondes pour collecter les données.*
3. *Reconnectez le câble Ethernet. (Ou activez l'adaptateur réseau dans Paramètres réseau avancés s'il a été précédemment désactivé.)*
4. *Attendez 60 secondes avant d'arrêter la capture pour garantir suffisamment de temps pour que la sonde active tente de s'exécuter.*

Wireless

1. *Démarrez la capture de paquets avant la connexion.*
2. *Connectez-vous au réseau sans fil.*
3. *Attendez 60 secondes pour vous assurer que l'activité de sonde active s'est entièrement produite.*
4. *Arrêtez la capture réseau.*

Références supplémentaires

- *Vue d'ensemble de NCSI*
- *NCSI FAQ*

Réponses aux questions courantes sur NCSI

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

La section suivante fournit une foire aux questions simplifiée autour de l'indicateur d'état de connectivité réseau (NCSI) dans Windows.

> **ⓘ Important**
>
> Les serveurs de sonde NCSI publics, précédemment hébergés par Azure Front Door, ont été hébergés par Akamai depuis le 20 juin 2023.
>
> Microsoft recommande comme meilleures pratiques que les règles de pare-feu soient utilisées pour autoriser le trafic NCSI et ne doivent pas être basées sur des adresses IP. Si vous observez des sondes NCSI ayant échoué, vérifiez d'abord que les pare-feu d'entreprise ou les proxys pour les sondes clientes ne sont pas bloqués. Si les sondes ont fonctionné avant la date mentionnée, c'est l'ajout de règles autorisant les requêtes HTTP sortantes vers 13.107.4.52 qui est le problème.
>
> - Vous pouvez modifier vos règles de trafic sortant dans le **pare-feu Windows Defender avec sécurité avancée**. Pour cela, cliquez sur **Démarrer**>, tapez **wf.msc**>, puis sélectionnez **Entrée**. Une règle de trafic sortant doit être créée en fonction du service d'origine.
>
> - NLS (Network List Service) s'applique à :
> - Windows Server 2022 et ses itérations futures
> - Windows 11
>
> - Le service NLA (Network Location Awareness) s'applique à :
> - Itérations windows Server 2019 et précédentes
> - Itérations Windows 10 et précédentes
>
> Pour les utilisateurs derrière un pare-feu basé sur le matériel externe, nous recommandons aux clients de travailler avec leurs fournisseurs de matériel pour créer les règles appropriées pour leur environnement, car chacun possède des contrôles et des configurations différents dans l'implémentation. Les sondes NCSI suivent les mêmes exigences que les mises à jour Windows en ce qui concerne l'autorisation du passage des noms d'hôte et l'interdiction du mappage à des adresses IP spécifiques.

Quand les sondes actives sont-elles envoyées ?

Les sondes actives sont déclenchées par les événements suivants que les moniteurs NCSI indiquent que l'état du réseau peut avoir besoin d'être actualisé :

- Modifications de l'interface générale ou de la condition réseau.
- Détection ou modifications des proxys.
- Détection des zones critiques ou changements.

Lorsque de nouvelles conditions réseau sont remplies, qu'elles soient câblées, sans fil ou derrière un VPN, l'interface réseau est prête à être utilisée et les sondes actives testent la connectivité réseau. Par exemple, lorsqu'une connexion sans fil est établie :

```
[Microsoft-Windows-NCSI/Analytic ] Transitioning to State: Interface NetReady
Interface Luid: 0x47008000000000
```

Que se passe-t-il après la réussite d'une sonde active ?

Une sonde réussie fournit la sortie suivante :

```
[Microsoft-Windows-NCSI/Analytic ] Active Internet Probe finished on interface
{426b6867-b0e4-4ff9-a14b-dd6a4345c24e} (true) {426b6867-b0e4-4ff9-a14b-
dd6a4345c24e}, true, true, false, true, false
```

- Si la sonde n'a pas traversé un proxy, NCSI note cela.
- L'icône d'interface réseau change pour refléter que la connectivité Internet est accessible.
- Si l'interface est derrière un portail captif dans lequel les informations d'identification n'ont pas été fournies ou si elle n'autorise pas l'accès à Internet par défaut sans entrée supplémentaire, la capacité locale est définie. Pour plus d'informations, consultez les portails captives.

Qu'est-ce qui peut empêcher une sonde active de réussir ?

De nombreuses choses peuvent empêcher une sonde active d'atteindre le serveur de sonde Internet ou de recevoir une réponse d'un serveur atteignant le client avec succès. Elles sont les

suivantes :

- Erreurs de proxy, mauvaise configuration, conditions environnementales intermittentes.
- Problèmes de fichier PAC qui empêchent le routage des paquets vers le proxy correct ou le client qui ne reconnaît pas l'existence d'un proxy requis pour l'envoi de la sonde.
- Configuration VPN, retards de traitement de la configuration et mauvais itinéraire de la sonde vers un endroit où elle ne peut pas facilement atteindre Internet en raison de l'expiration du délai d'attente de la connectivité.
- Problèmes de résolution du serveur DNS (Domain Name System) pour les noms de recherche NCSI connus. Ces problèmes sont souvent intermittents et non des enregistrements manquants.

Comment la détection passive détermine-t-elle la connectivité ?

Si le nombre de sauts enregistré pour l'interface est au moins le minimum requis par le système, il met à jour la capacité de l'interface à Internet. Aucune autre sonde active n'est effectuée pour cette interface, sauf si l'un des événements décrits dans « Quand les sondes actives sont-elles envoyées ? » occurs.

Si NCSI voit que la connectivité est locale uniquement, les conditions suivantes sont remplies :

- Le nombre de sauts ne respecte pas la valeur minimale du système.
- Les données du nombre de sauts n'ont pas pu être récupérées pour l'interface spécifique.
- La table de routage n'a aucune entrée pour l'interface avec un prochain saut vers un serveur racine sur Internet.
- Les sondes actives sont activées, mais aucune sonde active ne s'est terminée avec succès depuis que l'interface est devenue connectée.

Quel est le nombre minimum de sauts système par défaut ?

Le nombre de tronçons par défaut est **8** , mais ce n'est pas toujours optimal pour les entreprises. La valeur **3** convient à la plupart des infrastructures d'entreprise.

> ⓘ **Notes**
>
> Microsoft déconseille aux utilisateurs qui ne font pas partie d'une entreprise de modifier cette valeur de nombre de sauts, car elle est susceptible de changer.

Quand et à quelle fréquence la sonde passive s'exécute-t-elle ?

Plusieurs facteurs influencent si une sonde passive doit s'exécuter en fonction des données d'interrogation passives. Les conditions suivantes doivent être remplies :

- Autorisée par la stratégie de groupe. Lorsque la stratégie de groupe n'est pas configurée, par défaut, elle est autorisée. Cela peut être vérifié dans la stratégie de groupe en accédant à **Configuration ordinateur\Modèles d'administration\Réseau\Indicateur de statut de connectivité réseau\Spécifier l'interrogation passive**.
- Un utilisateur est connecté ou s'est connecté au cours des 30 dernières secondes.

Si la sonde passive est autorisée à s'exécuter, elle le fait toutes les 15 secondes. Cela peut être substitué en modifiant la clé de Registre suivante :

registry

```
HKLM\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet\PassivePollPerio
d
```

Où se trouve le chemin du serveur de sonde web HTTP dans le Registre ?

Le contenu de la sonde ainsi que l'hôte de sonde DNS prédéfini se trouve dans le chemin suivant :

registry

```
HKLM\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet
```

> ⓘ **Notes**
>
> À compter de windows 10 build 14393 (1607), les requêtes de sonde web (HTTP) sont envoyées à `www.msftconnecttest.com/connecttest.txt`.

La réponse attendue pour HTTP 200 OK doit contenir la charge utile « Microsoft Connect Test », par exemple :

```
HTTP:Request, GET /connecttest.txt
HTTP:Response, Status: Ok, URL: /connecttest.txt
```

Avant, `www.msftncsi.com/ncsi.txt` a été utilisé, et la réponse attendue est HTTP 200 OK avec un contenu contenant « Microsoft NCSI ». Pour une sonde DNS, la requête est envoyée à `dns.msftncsi.com`. Par exemple:

```
Query for dns.msftncsi.com of type A on class Internet
Response - Success, 131.107.255.255
```

> **Notes**
>
> **4-c-0003.c-msedge.net** est généralement reconnaissable comme point d'entrée du réseau de services MSFT, qui inclut les serveurs de sonde Internet hébergés par Microsoft. Le « 4 » est pour IPv4. **6-c-0003.c-msedge.net** concerne IPv6.

Comment NCSI sait-il s'il faut utiliser une sonde HTTP ou DNS ?

À compter de Windows 11, HTTP est toujours utilisé. Vous pouvez voir l'activité DNS, mais son objectif est d'identifier où envoyer la sonde HTTP. Avant cela, si aucun proxy n'existe, NCSI effectue des sondes à l'aide de DNS. Example:

```
[Microsoft-Windows-NCSI/Analytic ] Active Internet Probe (DNS) started on
interface {426b6867-b0e4-4ff9-a14b-dd6a4345c24e}
```

Raisons de l'échec de la sonde réseau

Il existe plusieurs raisons pour lesquelles une sonde réseau peut échouer. Pour les échecs rencontrés, elle est journalisée dans l'observateur d'événements à des fins d'investigation.

Agrandir le tableau

Output	Description
ActiveDnsProbeFailed	La sonde DNS a échoué. **Vérifier via une capture de paquets.**
ActiveHttpProbeFailed	Le nom DNS du serveur de sonde n'a pas été résolu. NSCI a échoué avant de tenter d'envoyer la requête de sonde web. Cela peut être dû à une défaillance DNS, à un échec de connexion au serveur proxy, etc. **Vérifier via une capture de paquets.**
ActiveHttpProbeFailedButDnsSucceeded	Le nom DNS du serveur de sonde a été résolu, mais la sonde HTTP vers cette adresse IP résolue a échoué. **Utiliser une application de capture de paquets et vérifier la capture de données.**
ActiveHttpProbeFailedHotspotDetected	La sonde HTTP n'a pas réussi à passer un hotspot ou un portail captif. Cela est généralement déterminé lorsqu'une réponse HTTP 200 est reçue, mais la charge utile de réponse ne contient pas le fichier texte *connecttest.txt*. Vous pouvez également recevoir un code d'état HTTP autre que 200, tel que 302 ou 304. **Ce code d'état est normalement observé lors de la gestion des problèmes où la connexion sans fil ne peut pas être établie. Vérifiez par le biais d'une capture de paquets. L'utilisateur peut avoir besoin d'authentifier le point d'accès ou la configuration du point d'accès peut être modifié.**
NoAddress	L'adaptateur cible n'a pas d'adresse IP préférée affectée. **Il existe un problème plus important qui ne peut pas être résolu par le biais de NSCI.**
NoGlobalAddress	Identique à NoAddress mais spécifique aux interfaces IPV6.
NoRoute	L'interface sur laquelle la sonde est envoyée n'a aucun itinéraire vers Internet dans la table de routage. **Certains scénarios où cela peut se produire est lorsqu'un VPN nouvellement connecté n'a pas encore modifié la table de routage avec de nouveaux itinéraires ou dans des scénarios VPN de tunnel forcés dans lesquels une fois l'interface VPN connectée, l'interface physique passe à la connectivité locale à mesure que la table de routage a été modifiée.**

Output	Description
PassivePacketHops	**Pas de défaillance.** Les paquets reçus indiquent un niveau de connectivité. Cette raison de modification est utilisée lorsque la fonctionnalité est **déclenchée**, pas réduite.

Voici une sortie d'une défaillance de sonde :

```
[Microsoft-Windows-NCSI/Analytic ] Active Internet Probe finished on interface
{426b6867-b0e4-4ff9-a14b-dd6a4345c24e} (false) {426b6867-b0e4-4ff9-a14b-
dd6a4345c24e}, false, true, false, false, false

[Microsoft-Windows-NCSI/Operational ] Capability change on {426b6867-b0e4-4ff9-
a14b-dd6a4345c24e} (0x6008001000000 Family: V4 Capability: Local ChangeReason:
SuspectDnsProbeFailed) {426b6867-b0e4-4ff9-a14b-dd6a4345c24e}
```

Notes

Si l'échec de la sonde était dû au fait de traverser un proxy NCSI, fixe l'état de connectivité sur Aucun. Si la sonde ayant échoué ne traverse pas (passe directement), NCSI définit l'état de connectivité sur Local.

Quand ncSI quitte-t-il le mode point d'accès ?

Lorsque NCSI est en mesure d'obtenir une sonde active avec le contenu attendu correspondant « Microsoft Connect Test ». Il n'y a rien que NCSI puisse faire concernant le fait d'être derrière un point d'accès, si ce n'est de le détecter et d'en faire un rapport. Il incombe à l'utilisateur de s'authentifier auprès du point d'accès afin que le trafic soit autorisé sur Internet.

La responsabilité du NCSI envers le système de signaler avec précision la connectivité comme étant locale lorsque ses sondes sont redirigées. Seul le serveur de sonde hébergé sur Internet doit retourner le contenu attendu montrant la connectivité Internet.

Voici un exemple de ce qu'un échec de sonde peut relayer :

```
[Microsoft-Windows-NCSI/Analytic ] Active Internet Probe finished on interface
{426b6867-b0e4-4ff9-a14b-dd6a4345c24e} (false)
{426b6867-b0e4-4ff9-a14b-dd6a4345c24e}, false, true, false, false, false
```

```
[Microsoft-Windows-NCSI/Operational ] Capability change on {426b6867-b0e4-4ff9-
a14b-dd6a4345c24e}
(0x6008001000000 Family: V4 Capability: Local ChangeReason: SuspectDnsProbeFailed)
{426b6867-b0e4-4ff9-a14b-dd6a4345c24e}
```

Pourquoi Windows ouvre-t-il parfois un navigateur quand je me connecte à un réseau ?

Ce comportement est par conception. Windows souhaite que les utilisateurs sachent quand ils se connectent à un réseau qui nécessite l'authentification du portail captif. Windows permet d'afficher une petite fenêtre contextuelle pendant une courte durée pour encourager les utilisateurs à le sélectionner pour ouvrir un navigateur. Les utilisateurs passent souvent à côté, sans savoir qu'il ouvre un navigateur pour l'authentification. Pour plus d'informations, consultez un navigateur s'ouvre lors de la connexion à un réseau public ou d'entreprise.

Où puis-je trouver de la documentation publique indiquant que msftconnecttest.com doit figurer dans la liste blanche ?

La liste suivante d'URL mentionne ou implique `msftconnecttext.com`:

- indicateur d'état de connexion réseau
- Points de terminaison de connexion Windows 11 Entreprise
- Points de connexion pour les éditions autres que l'édition Entreprise de Windows
- Sondes actives NCSI et alerte de statut réseau

Comment Microsoft Office utilise-t-il NCSI pour déterminer la connectivité Internet ?

Pour ce faire, Microsoft Office effectue un appel d'API à **get_IsConnectedToInternet**. Si des applications telles que Microsoft Office ne peuvent indiquer aucune connectivité Internet, mais que vous êtes en mesure de parcourir des sites web, cela indique un problème NCSI. Si vous ne pouvez pas parcourir ou effectuer d'autres opérations réseau de base, il peut s'agir d'un problème réseau général et la résolution des problèmes NCSI ne s'applique pas.

L'icône réseau de la barre des tâches s'appuie sur NCSI et la même règle s'applique même si elle indique aucune activité réseau. Cela peut être dû à un problème réseau plus générique autre que NCSI.

Linux possède-t-il son propre NCSI ?

Linux n'a pas d'API intégrées (interface de programmation d'application) pour que les applications vérifient les modifications continues de connectivité Internet. Ils doivent implémenter leurs propres contrôles réseau à partir de la base, ou utiliser différents utilitaires Linux pour vérifier en permanence les conditions réseau.

En outre, certaines applications Linux n'effectuent pas de vérifications de connectivité. Ils envoient les paquets et gèrent les erreurs après le fait, tandis que NCSI permet aux applications d'alerter l'utilisateur des problèmes de connectivité immédiats.

> **Notes**
>
> L'entreprise doit s'assurer que son infrastructure ne bloque pas une sonde HTTP ou DNS active. Cela peut se produire si l'un des éléments suivants est mal configuré :
>
> - Pare-feu bloqués
> - Serveurs DNS
> - Tunneling VPN forcé
> - Serveurs proxy
> - Routers
> - Logiciel tiers interceptant la sonde
>
> Pour les consommateurs généraux, il existe moins d'obstacles potentiels qui ne nécessitent pas de configuration utilisateur prête à l'emploi. Des problèmes se produisent lorsque des VPN ou des logiciels tiers sont introduits, qui peuvent intercepter, malrouter ou retarder les sondes actives NCSI.

Voir aussi

- Vue d'ensemble de NCSI
- Guide de résolution des problèmes NCSI

Équilibrage de charge réseau

Article • 09/03/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Dans cette rubrique, nous vous proposons une vue d’ensemble de la fonctionnalité d’équilibrage de la charge réseau (NLB) dans Windows Server 2016. Vous pouvez utiliser l’équilibrage de charge réseau pour gérer deux ou plusieurs serveurs en tant que cluster virtuel unique. L’équilibrage de la charge réseau améliore la disponibilité et l’extensibilité des applications de serveur Internet, telles que celles utilisées sur les serveurs Web, FTP, de pare-feu, proxy, de réseau privé virtuel et sur d’autres serveurs critiques.

Notes

Windows Server 2016 inclut un nouvel équilibrage de la charge logicielle inspiré d’Azure en tant que composant de l’infrastructure SDN (Software Defined Networking). Utilisez l’équilibrage de la charge logicielle au lieu de l’équilibrage de la charge réseau si vous utilisez SDN, si vous utilisez des charges de travail non-Windows, si vous avez besoin de traduction d’adresses réseau sortantes (NAT) ou si vous avez besoin d’un équilibrage de charge de couche 3 (L3) ou non-TCP. Vous pouvez continuer à utiliser l’équilibrage de charge réseau avec Windows Server 2016 pour les déploiements non-SDN. Pour plus d’informations sur l’équilibrage de la charge logicielle, consultez **Équilibrage de la charge logicielle pour SDN**.

La fonctionnalité d’équilibrage de la charge réseau répartit le trafic entre plusieurs serveurs à l’aide du protocole réseau TCP/IP. En combinant plusieurs ordinateurs qui exécutent des applications dans un cluster virtuel unique, l’équilibrage de la charge réseau assure la fiabilité et les performances des serveurs Web et d’autres serveurs critiques.

Les serveurs d’un cluster d’équilibrage de la charge réseau sont appelés *hôtes* et chacun d’eux exécute une copie distincte des applications de serveurs. L’équilibrage de la charge réseau répartit les demandes de client entrantes entre les hôtes du cluster. Vous pouvez configurer la charge qui doit être gérée par chaque hôte. Vous pouvez également ajouter des hôtes de façon dynamique au cluster afin de traiter une charge accrue. L’équilibrage de la charge réseau dirige également tout le trafic vers un seul hôte désigné, appelé *hôte par défaut*.

L’équilibrage de la charge réseau permet de traiter tous les ordinateurs du cluster à l’aide du même ensemble d’adresses IP. Il permet également de conserver un ensemble d’adresses IP dédiées uniques pour chaque hôte. Pour les applications à charge équilibrée, en cas d’échec ou de passage hors connexion d’un hôte, la charge est automatiquement redistribuée entre les ordinateurs toujours en cours de fonctionnement. Lorsqu’il est prêt, l’ordinateur hors connexion peut rejoindre de manière transparente le cluster et récupérer sa part de la charge, ce qui permet aux autres ordinateurs du cluster de traiter moins de trafic.

Cas pratiques

L’équilibrage de la charge réseau est utile pour s’assurer que les applications sans état, par exemple les serveurs Web qui exécutent Internet Information Services (IIS), sont disponibles avec un temps d’interruption minimal et qu’elles sont extensibles (via l’ajout de serveurs supplémentaires au fur et à mesure de l’augmentation de la charge). Les sections suivantes expliquent comment l’équilibrage de la charge réseau prend en charge la haute disponibilité, l’extensibilité et la simplicité de gestion des serveurs en cluster qui exécutent ces applications.

Haute disponibilité

Un système à haute disponibilité offre de manière fiable un niveau de service acceptable avec un temps d’immobilisation très faible. Pour offrir une grande disponibilité, l’équilibrage de la charge réseau comprend des fonctionnalités intégrées qui peuvent assurer automatiquement les tâches répertoriées ci-dessous :

- détecter un hôte de cluster en panne ou hors connexion, puis le récupérer ;
- équilibrer la charge réseau lors de l’ajout ou de la suppression d’hôtes ;
- récupérer et redistribuer la charge dans un délai de dix secondes.

Extensibilité

L’extensibilité est la mesure de la capacité d’un ordinateur, d’un service ou d’une application à répondre à des besoins croissants de performances. Pour les clusters d’équilibrage de la charge réseau, l’extensibilité correspond à la possibilité d’ajouter un ou plusieurs systèmes à un cluster existant lorsque la charge totale du cluster dépasse ses capacités. Pour assurer cette extensibilité, l’équilibrage de la charge réseau vous permet d’effectuer les opérations listées ci-après :

- Équilibrer les demandes de charge dans le cluster d'équilibrage de la charge réseau pour des services TCP/IP individuels.
- Prendre en charge jusqu'à 32 ordinateurs dans un seul cluster.
- Équilibrer plusieurs demandes relatives à la charge du serveur (du même client ou de plusieurs clients) sur plusieurs hôtes du cluster.
- Ajouter des hôtes au cluster d'équilibrage de la charge réseau au fur et à mesure de l'augmentation de la charge, sans entraîner un échec du cluster.
- Supprimer des hôtes du cluster lorsque la charge diminue.
- Permettre des performances élevées et un faible temps système via une mise en œuvre entièrement en pipeline. Le traitement en pipeline permet d'envoyer les demandes au cluster d'équilibrage de la charge réseau sans attendre la réponse à une demande précédente.

Simplicité de gestion

Pour assurer cette simplicité de gestion, l'équilibrage de la charge réseau vous permet d'effectuer les opérations listées ci-après :

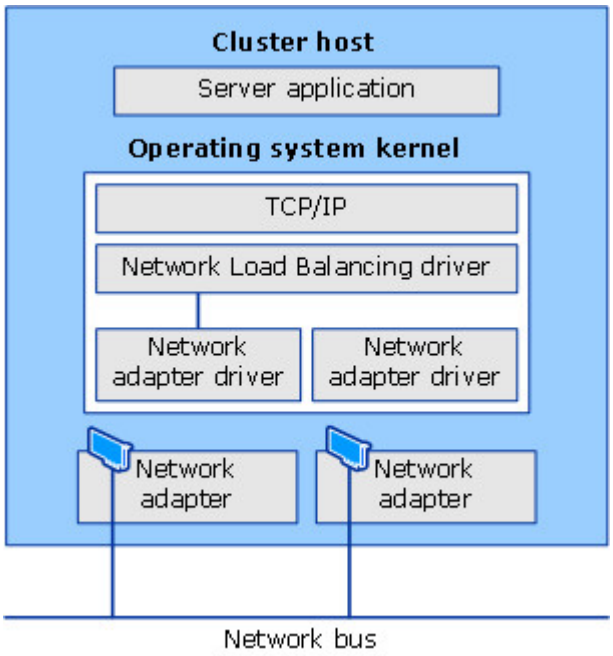
- Gérez et configurez plusieurs clusters d'équilibrage de la charge réseau et les hôtes du cluster à partir d'un seul ordinateur à l'aide du Gestionnaire de l'équilibrage de la charge réseau ou des applets de commande d'équilibrage de la charge réseau dans Windows PowerShell.
- Spécifier le comportement d'équilibrage de la charge pour un seul port IP ou un groupe de ports à l'aide de règles de gestion des ports.
- Définir des règles de port différentes pour chaque site Web. Si vous utilisez le même ensemble de serveurs à charge équilibrée pour plusieurs applications ou sites Web, les règles de port se basent sur l'adresse IP virtuelle de destination (à l'aide de clusters virtuels).
- Diriger toutes les demandes clientes vers un seul hôte à l'aide de règles à hôte unique optionnelles. L'équilibrage de la charge réseau route les demandes clientes vers un hôte particulier qui exécute des applications spécifiques.
- Bloquer l'accès réseau non souhaité à certains ports IP.
- Activer la prise en charge du protocole IGMP (Internet Group Management Protocol) sur les hôtes du cluster afin de limiter la saturation des ports commutés

(les paquets réseau entrants sont envoyés à tous les ports situés sur le commutateur) lors du fonctionnement en mode de multidiffusion.

- Démarrer, arrêter et contrôler les actions d'équilibrage de la charge réseau à distance, à l'aide de commandes ou de scripts Windows PowerShell.
- Afficher le journal des événements Windows pour vérifier les événements d'équilibrage de la charge réseau. L'équilibrage de la charge réseau consigne toutes les actions et modifications du cluster dans le journal des événements.

Fonctionnalités importantes

L'équilibrage de la charge réseau est installé en tant que composant du pilote réseau Windows Server standard. Ses opérations sont transparentes pour la pile de réseau TCP/IP. La figure suivante illustre la relation existante entre l'équilibrage de la charge réseau et les autres composants logiciels dans une configuration classique :



Voici les principales fonctionnalités de l'équilibrage de la charge réseau.

- Elle ne nécessite aucune modification du matériel pour pouvoir s'exécuter.
- Elle fournit des outils d'équilibrage de la charge réseau pour configurer et gérer plusieurs clusters, ainsi que tous les hôtes de cluster, à partir d'un seul ordinateur distant ou local.
- Elle permet aux clients d'accéder au cluster à l'aide d'un seul nom Internet logique et d'une seule adresse IP virtuelle, appelée adresse IP du cluster (elle conserve des noms individuels pour chaque ordinateur). L'équilibrage de la charge réseau autorise plusieurs adresses IP virtuelles pour les serveurs multirésidents.

Notes

Lorsque vous déployez des machines virtuelles en tant que clusters virtuels, l'équilibrage de la charge réseau ne nécessite pas de serveurs multirésidents avec plusieurs adresses IP virtuelles.

- L'équilibrage de la charge réseau peut être lié à plusieurs cartes réseau, ce qui vous permet de configurer plusieurs clusters indépendants sur chaque hôte. La prise en charge de plusieurs cartes réseau diffère des clusters virtuels en ce sens que les clusters virtuels vous permettent de configurer plusieurs clusters sur une seule carte réseau.
- Elle ne nécessite aucune modification des applications serveur pour que ces dernières puissent s'exécuter dans un cluster d'équilibrage de la charge réseau.
- Elle peut être configurée pour ajouter automatiquement un hôte au cluster si cet hôte de cluster tombe en panne et s'il est ensuite remis en ligne. L'hôte ajouté peut démarrer le traitement des nouvelles demandes adressées au serveur par les clients.
- Elle vous permet de mettre des ordinateurs hors connexion à des fins de maintenance préventive sans perturber les opérations de cluster sur les autres hôtes.

Configuration matérielle requise

Voici la configuration matérielle requise pour l'exécution d'un cluster d'équilibrage de la charge réseau.

- Tous les hôtes du cluster doivent résider sur le même sous-réseau.
- Il n'existe aucune restriction sur le nombre de cartes réseau de chaque hôte. Par ailleurs, les différents hôtes peuvent avoir un nombre distinct de cartes.
- Au sein de chaque cluster, toutes les cartes réseau doivent être soit multidiffusion, soit monodiffusion. L'équilibrage de la charge réseau ne prend pas en charge un environnement mixte de multidiffusion et de monodiffusion au sein d'un seul cluster.
- Si vous utilisez le mode de monodiffusion, la carte réseau qui permet de gérer le trafic entre le client et le cluster doit prendre en charge la modification de son adresse MAC (Media Access Control).

Configuration logicielle requise

Voici la configuration logicielle requise pour l'exécution d'un cluster d'équilibrage de la charge réseau.

- Seul le protocole TCP/IP peut être utilisé sur la carte pour laquelle l'équilibrage de la charge réseau est activé sur chaque hôte. N'ajoutez pas d'autres protocoles (par exemple, IPX) à cette carte.
- Les adresses IP des serveurs du cluster doivent être statiques.

> ⓘ **Notes**
>
> L'équilibrage de la charge réseau ne prend pas en charge le protocole DHCP (Dynamic Host Configuration Protocol). L'équilibrage de la charge réseau désactive le protocole DHCP sur chaque interface configurée.

Informations sur l'installation

Vous pouvez installer l'équilibrage de la charge réseau à l'aide du Gestionnaire de serveur ou des commandes Windows PowerShell pour l'équilibrage de la charge réseau.

Vous pouvez éventuellement installer les outils d'équilibrage de la charge réseau pour gérer un cluster d'équilibrage de la charge réseau local ou distant. Les outils à votre disposition sont le Gestionnaire d'équilibrage de la charge réseau et les applets de commande d'équilibrage de la charge réseau Windows PowerShell.

Installation avec le Gestionnaire de serveur

Dans le Gestionnaire de serveur, vous pouvez utiliser l'assistant Ajouter des rôles et des fonctionnalités pour ajouter la fonctionnalité d'**équilibrage de la charge réseau**. Lorsque vous terminez l'assistant, l'équilibrage de la charge réseau est installé et vous n'avez pas besoin de redémarrer l'ordinateur.

Installation avec Windows PowerShell

Pour installer l'équilibrage de la charge réseau à l'aide de Windows PowerShell, exécutez la commande suivante à une invite de Windows PowerShell avec élévation de privilèges sur l'ordinateur sur lequel vous souhaitez installer l'équilibrage de la charge réseau.

```
PowerShell
```

```
Install-WindowsFeature NLB -IncludeManagementTools
```

Une fois l'installation terminée, aucun redémarrage de l'ordinateur n'est nécessaire.

Pour plus d'informations, voir Install-WindowsFeature.

Gestionnaire d'équilibrage de la charge réseau

Pour ouvrir le Gestionnaire d'équilibrage de la charge réseau dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire d'équilibrage de la charge réseau**.

Ressources supplémentaires

Le tableau suivant contient des liens vers des informations supplémentaires concernant la fonctionnalité d'équilibrage de la charge réseau.

Type de contenu	Références
Déploiement	Guide de déploiement de l'équilibrage de la charge réseau | Configuration de l'équilibrage de la charge réseau avec les services Terminal
Operations	Gestion des clusters d'équilibrage de la charge réseau | Définition des paramètres d'équilibrage de la charge réseau | Contrôle des hôtes sur les clusters d'équilibrage de la charge réseau
Résolution des problèmes	Résolution des problèmes liés aux clusters d'équilibrage de la charge réseau | Événements et erreurs de cluster d'équilibrage de la charge réseau
Outils et paramètres	Applets de commande Windows PowerShell d'équilibrage de la charge réseau
Ressources communautaires	Forum sur la haute disponibilité (clustering)

Vue d'ensemble du serveur de stratégie réseau

Article • 07/05/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cet article fournit une vue d'ensemble du serveur de stratégie réseau (NPS) dans Windows Server. Vous pouvez utiliser NPS pour créer et appliquer des stratégies d'accès réseau à l'échelle de l'organisation pour l'authentification et l'autorisation de demande de connexion. Vous pouvez également configurer NPS en tant que proxy RADIUS (Remote Authentication Dial-In User Service). Lorsque vous utilisez NPS comme proxy RADIUS, NPS transfère les demandes de connexion à un serveur RADIUS NPS distant ou à d'autres serveurs RADIUS. Vous pouvez utiliser la configuration du proxy pour équilibrer la charge des demandes de connexion et les transférer vers le domaine approprié pour l'authentification et l'autorisation. NPS est installé lorsque vous installez le rôle NPAS (Network Policy and Access Services) dans Windows Server.

Fonctionnalités NPS

Vous pouvez utiliser NPS pour configurer et gérer de manière centralisée l'authentification, l'autorisation et la comptabilité de l'accès réseau. NPS offre les fonctionnalités suivantes à cet effet :

- **Serveur RADIUS**. Le serveur NPS effectue de façon centralisée les processus d'authentification, d'autorisation et de gestion des comptes pour les connexions sans fil, par commutateur d'authentification, par accès à distance et réseau privé virtuel (VPN). Lorsque vous utilisez NPS comme serveur RADIUS, vous configurez les composants suivants :
  - Serveurs d'accès réseau, tels que les points d'accès sans fil et les serveurs VPN. Vous les configurez en tant que clients RADIUS dans NPS.
  - Stratégies réseau que NPS utilise pour autoriser les demandes de connexion.
  - Gestion des comptes RADIUS. Ce composant est facultatif. Si vous le configurez, NPS enregistre les informations de comptabilité dans des fichiers de journal sur le disque dur local ou dans une base de données Microsoft SQL Server.

  Pour plus d'informations, consultez Clients RADIUS.

- **Proxy RADIUS**. Lorsque vous utilisez NPS comme proxy RADIUS, vous configurez des stratégies de demande de connexion qui indiquent à NPS :
  - Spécifiez les demandes de connexion à transférer vers d'autres serveurs RADIUS.

    - Définissez les serveurs RADIUS cibles auxquels ces demandes de connexion sont transférées.

  En outre, vous pouvez configurer NPS pour transférer des données comptables à des fins de journalisation vers un ou plusieurs ordinateurs au sein d'un groupe de serveurs RADIUS distant. Pour configurer NPS en tant que serveur proxy RADIUS, consultez les ressources suivantes :
    - Proxy RADIUS
    - Configurer des stratégies de demande de connexion

- **Gestion des comptes RADIUS**. Vous pouvez configurer NPS pour journaliser les événements sur un fichier journal local ou sur une instance locale ou distante de SQL Server. Pour plus d'informations, consultez journalisation NPS.

Vous pouvez configurer NPS avec n'importe quelle combinaison de ces fonctionnalités. Par exemple, vous pouvez configurer un déploiement NPS en tant que serveur RADIUS pour les connexions VPN. Vous pouvez également configurer ce même déploiement qu'un proxy RADIUS pour transférer certaines demandes de connexion. Plus précisément, il peut transférer certaines demandes aux membres d'un groupe de serveurs RADIUS distant pour l'authentification et l'autorisation dans un autre domaine.

> ⓘ **Important**
>
> Dans les versions précédentes de Windows Server, NPAS incluait la protection de l'accès réseau (NAP), l'autorité d'inscription d'intégrité (HRA) et le protocole d'autorisation des informations d'identification de l'hôte (HCAP). NAP, HRA et HCAP ont été déconseillés dans Windows Server 2012 R2 et ne sont pas disponibles dans Windows Server 2016 ou version ultérieure. Si vous disposez d'un déploiement NAP qui utilise des systèmes d'exploitation antérieurs à Windows Server 2016, vous ne pouvez pas migrer votre déploiement NAP vers Windows Server 2016 ou version ultérieure.

Options d'installation de Windows Server et NPS

La disponibilité des fonctionnalités NPS dépend des options que vous sélectionnez lors de l'installation de Windows Server :

- Lorsque vous utilisez l'option d'installation du serveur avec expérience utilisateur, le rôle NPAS est disponible sur Windows Server. Le rôle est disponible sur les éditions Standard et Datacenter.
- Lorsque vous utilisez l'option d'installation server Core, le rôle NPAS n'est pas disponible.

Serveur RADIUS et proxy

Vous pouvez utiliser NPS comme serveur RADIUS, proxy RADIUS ou les deux. Les sections suivantes fournissent des informations détaillées sur ces utilisations.

Serveur RADIUS

NPS est l'implémentation Microsoft de la norme RADIUS spécifiée par le Groupe de travail d'ingénierie Internet (IETF) dans request for comments (RFCs) 2865 et 2866. En tant que serveur RADIUS, NPS effectue une authentification de connexion centralisée, une autorisation et une comptabilité pour de nombreux types d'accès réseau. Parmi les types d'accès au réseau, citons l'accès sans fil, l'authentification des commutateurs, l'accès à distance par ligne commutée et VPN, ainsi que les connexions de routeur à routeur.

> **Notes**
>
> Pour plus d'informations sur le déploiement de NPS en tant que serveur RADIUS, consultez **Déployer un serveur de stratégie réseau**.

NPS prend en charge l'utilisation d'un ensemble hétérogène d'équipements sans fil, commutateur, accès à distance ou VPN. Vous pouvez utiliser NPS avec le service d'accès à distance, disponible dans Windows Server.

NPS utilise un domaine services de domaine Active Directory (AD DS) ou la base de données de comptes d'utilisateur du Gestionnaire de comptes de sécurité (SAM) locale pour authentifier les informations d'identification de l'utilisateur pour les tentatives de connexion. Lorsqu'un serveur exécutant NPS est membre d'un domaine AD DS, NPS utilise le service d'annuaire comme base de données de compte d'utilisateur. Dans ce cas, NPS fait partie d'une solution d'authentification unique. Le même ensemble d'informations d'identification est utilisé pour le contrôle d'accès réseau (authentification et autorisation de l'accès à un réseau) et pour se connecter à un domaine AD DS.

> **Notes**
>
> NPS utilise les propriétés rendez-vous du compte d'utilisateur et des stratégies réseau pour autoriser une connexion.

Les fournisseurs de services Internet (ISP) et les organisations qui maintiennent l'accès réseau ont un défi accru. Ils doivent gérer tous les types d'accès réseau à partir d'un point d'administration unique, quel que soit le type d'équipement d'accès réseau utilisé. La norme

RADIUS prend en charge cette fonctionnalité dans les environnements homogènes et hétérogènes. RADIUS est un protocole client-serveur qui permet aux équipements d'accès réseau (utilisés en tant que clients RADIUS), d'envoyer des demandes d'authentification et de gestion des comptes à un serveur RADIUS.

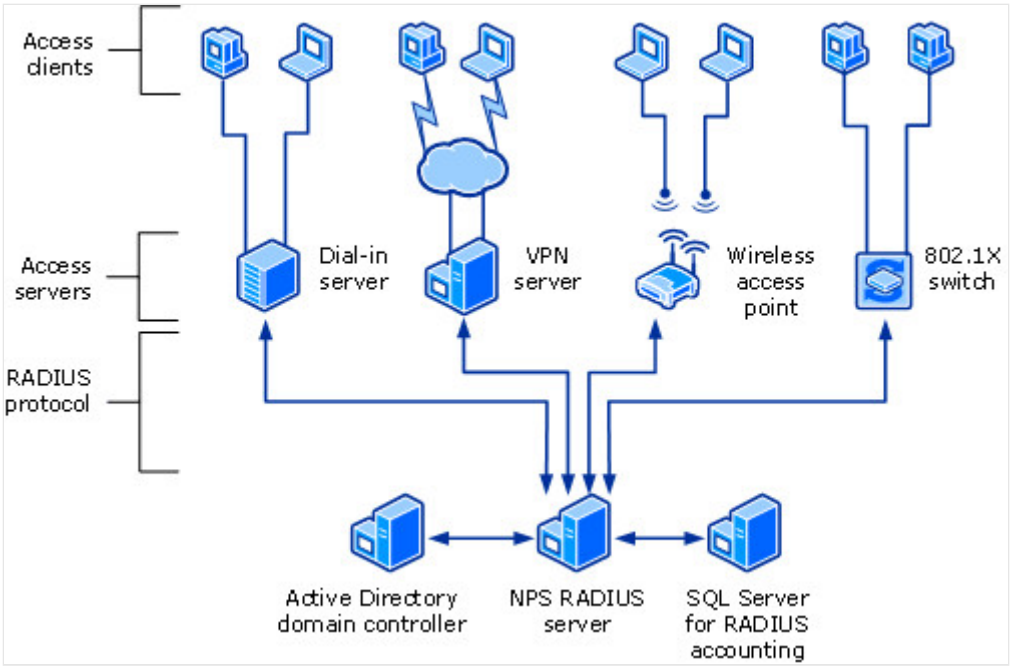
Un serveur RADIUS a accès aux informations de compte d'utilisateur et peut vérifier les informations d'authentification d'accès réseau. Si les informations d'identification de l'utilisateur sont authentifiées et que la tentative de connexion est autorisée, le serveur RADIUS autorise l'accès utilisateur en fonction des conditions spécifiées. Ensuite, le serveur RADIUS enregistre la connexion d'accès réseau dans un journal de comptabilité. L'utilisation de RADIUS permet aux données d'authentification, d'autorisation et de comptabilité de l'utilisateur d'accès réseau d'être collectées et conservées dans un emplacement central, plutôt que sur chaque serveur d'accès.

Utiliser NPS en tant que serveur RADIUS

Vous pouvez utiliser NPS comme serveur RADIUS dans les cas suivants :

- Vous utilisez un domaine AD DS ou la base de données des comptes d'utilisateur SAM locaux comme base de données de compte d'utilisateur pour les clients d'accès.
- Vous utilisez l'accès à distance sur plusieurs serveurs d'accès commuté, serveurs VPN ou routeurs de numérotation à la demande, et vous souhaitez centraliser à la fois la configuration des stratégies réseau et l'enregistrement des connexions.
- Vous externalisez votre accès par modem, VPN ou sans fil à un fournisseur de services. Les serveurs d'accès utilisent RADIUS pour authentifier et autoriser les connexions effectuées par les membres de votre organisation.
- Vous souhaitez centraliser l'authentification, l'autorisation et la comptabilité pour un ensemble hétérogène de serveurs d'accès.

Le diagramme suivant montre NPS en tant que serveur RADIUS pour différents clients d'accès.



Proxy RADIUS

En tant que proxy RADIUS, NPS transfère les messages d’authentification et de comptabilité aux serveurs RADIUS NPS et à d’autres serveurs RADIUS. Lorsque vous utilisez NPS comme proxy RADIUS, il route les messages RADIUS entre les clients RADIUS et les serveurs RADIUS. Les clients RADIUS sont également appelés serveurs d’accès réseau. Les serveurs RADIUS effectuent l’authentification, l’autorisation et la comptabilité de l’utilisateur pour la tentative de connexion.

Vous pouvez configurer un nombre illimité de clients RADIUS et de groupes de serveurs RADIUS distants dans NPS. Vous pouvez également configurer des clients RADIUS en spécifiant une plage d’adresses IP.

Lorsque vous utilisez NPS comme proxy RADIUS, il sert de point de basculement ou de routage central via lequel les messages d’accès RADIUS et de comptabilité circulent. NPS enregistre des informations dans un journal de comptabilité sur les messages transférés.

Utiliser NPS comme proxy RADIUS

Vous pouvez utiliser NPS comme proxy RADIUS dans les cas suivants :

- Vous êtes un fournisseur de services qui propose des services externalisés d'accès commuté, VPN, ou d'accès réseau sans fil à plusieurs clients. Vos systèmes nas (Network-attached Storage) envoient des demandes de connexion au proxy RADIUS NPS. En fonction de la partie domaine du nom d’utilisateur dans la demande de connexion, le proxy RADIUS NPS transfère la demande de connexion à un serveur RADIUS. Le client gère ce serveur, qui peut authentifier et autoriser la tentative de connexion.

- Vous souhaitez fournir l'authentification et l'autorisation pour les comptes d'utilisateur qui ne sont pas membres de l'un des domaines suivants :
  - Domaine auquel le déploiement NPS est membre.
  - Domaine qui a une approbation bidirectionnelle avec le domaine dans auquel le déploiement NPS est membre.

  Par exemple, les comptes d'utilisateur incluent des comptes dans des domaines non approuvés, des domaines approuvés unidirectionnels et d'autres forêts. Au lieu de configurer vos serveurs d'accès pour envoyer leurs demandes de connexion à un serveur RADIUS NPS, vous pouvez les configurer pour envoyer leurs demandes de connexion à un proxy RADIUS NPS. Le proxy RADIUS NPS utilise la partie nom de domaine du nom d'utilisateur et transfère la requête à un serveur RADIUS NPS dans le domaine ou la forêt appropriés. Les tentatives de connexion pour les comptes d'utilisateur d'un domaine ou d'une forêt peuvent être authentifiées pour les systèmes NAS d'un autre domaine ou forêt.

- Vous souhaitez effectuer l'authentification et l'autorisation à l'aide d'une base de données qui n'est pas une base de données de compte Windows. Dans ce cas, les demandes de connexion qui correspondent à un nom de domaine spécifié sont transférées à un serveur RADIUS qui a accès à une autre base de données de comptes d'utilisateur et de données d'autorisation. Parmi les autres bases de données utilisateur figurent les bases de données NetIQ eDirectory et SQL (Structured Query Language).

- Vous souhaitez traiter un grand nombre de demandes de connexion. Dans ce cas, au lieu de configurer vos clients RADIUS pour tenter d'équilibrer leurs demandes de connexion et de comptabilité sur plusieurs serveurs RADIUS, vous pouvez les configurer pour envoyer leurs demandes de connexion et de comptabilité à un proxy RADIUS NPS. Le proxy RADIUS NPS équilibre dynamiquement la charge des demandes de connexion et de comptabilité sur plusieurs serveurs RADIUS et augmente le traitement d'un grand nombre de clients RADIUS et d'authentifications par seconde.

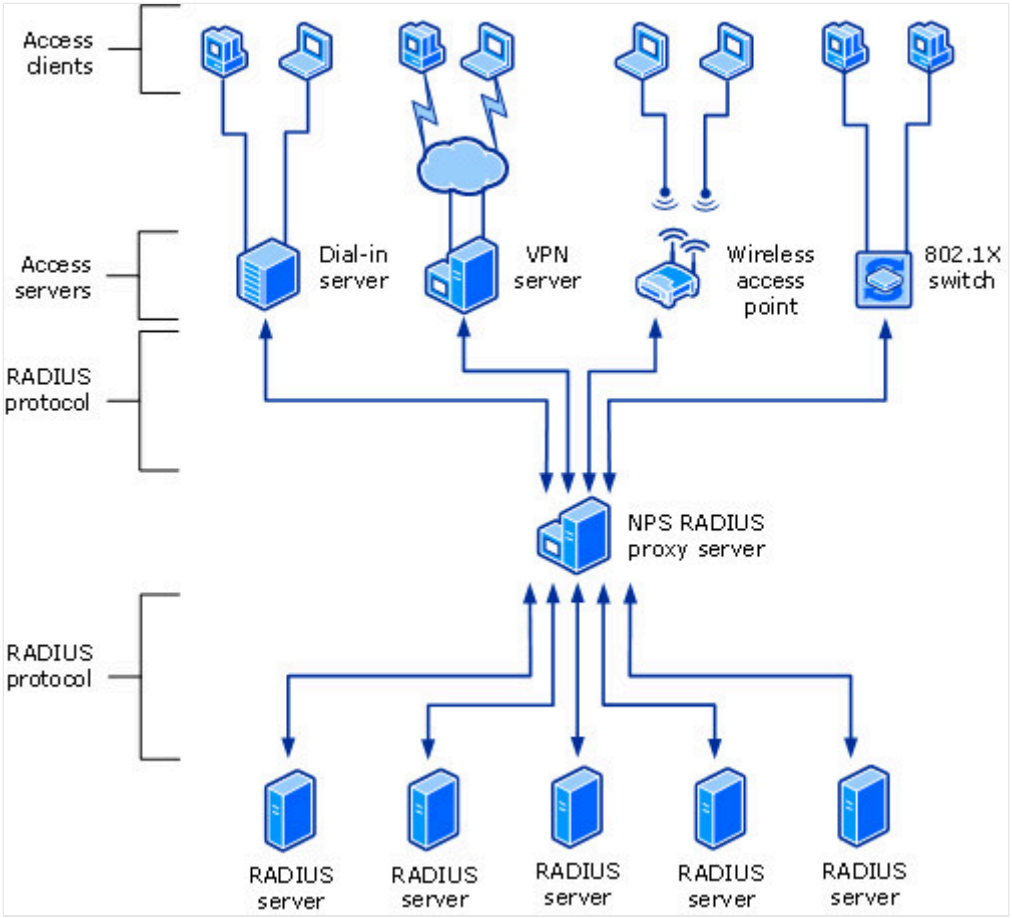
- Vous souhaitez fournir l'authentification et l'autorisation RADIUS pour les fournisseurs de services externalisés et réduire la configuration du pare-feu intranet. Un pare-feu intranet se trouve entre votre intranet et votre réseau de périmètre (le réseau entre votre intranet et Internet). Si vous placez NPS sur votre réseau de périmètre, le pare-feu entre votre réseau de périmètre et l'intranet doit autoriser le trafic à circuler entre NPS et plusieurs contrôleurs de domaine. Si vous remplacez le déploiement NPS par un proxy NPS, le pare-feu doit autoriser uniquement le trafic RADIUS à circuler entre le proxy NPS et un ou plusieurs déploiements NPS au sein de votre intranet.

> ⓘ **Important**

NPS prend en charge l'authentification entre les forêts sans proxy RADIUS lorsque le niveau fonctionnel de la forêt est Windows Server 2003 ou supérieur et qu'il existe une relation d'approbation bidirectionnelle entre les forêts. Toutefois, si vous utilisez l'une des infrastructures suivantes avec des certificats comme méthode d'authentification, vous devez utiliser un proxy RADIUS pour l'authentification entre les forêts :

- Protocole d'authentification extensible – Protocole TLS (EAP-TLS)
- Protocole d'authentification extensible protégé – Protocole TLS (PEAP-TLS)

Le diagramme suivant montre NPS en tant que proxy RADIUS entre les clients RADIUS et les serveurs RADIUS.



Avec NPS, les organisations peuvent également externaliser leur infrastructure d'accès à distance à un fournisseur de services, tout en conservant le contrôle de l'authentification, de l'autorisation et de la gestion des comptes utilisateur.

Vous pouvez créer des configurations NPS pour les scénarios suivants :

- Accès sans fil
- Accès à distance par modem de l'organisation ou par VPN
- Accès à distance externalisé ou accès sans fil
- Accès à Internet
- Accès authentifié aux ressources extranet pour les partenaires commerciaux

Exemples de configuration de serveur RADIUS et de proxy RADIUS

Les exemples de configuration suivants montrent comment configurer NPS en tant que serveur RADIUS et proxy RADIUS.

NPS en tant que serveur RADIUS

Cet exemple utilise la configuration suivante :

- NPS est configuré en tant que serveur RADIUS.
- La stratégie de demande de connexion par défaut est la seule stratégie configurée.
- Le serveur RADIUS NPS local traite toutes les demandes de connexion.

Le serveur RADIUS NPS peut authentifier et autoriser les comptes d'utilisateur qui se trouvent dans le domaine du serveur RADIUS NPS et dans les domaines approuvés.

NPS en tant que proxy RADIUS

Dans cet exemple, NPS est configuré en tant que proxy RADIUS qui transfère les demandes de connexion. Les requêtes sont transférées vers des groupes de serveurs RADIUS distants dans deux domaines non approuvés.

La stratégie de demande de connexion par défaut est supprimée. Deux nouvelles stratégies de demande de connexion sont créées pour transférer des demandes à chacun des deux domaines non approuvés.

Dans cet exemple, NPS ne traite aucune demande de connexion sur le serveur local.

NPS en tant que serveur RADIUS et proxy RADIUS

Cet exemple utilise deux stratégies de demande de connexion :

- Stratégie de demande de connexion par défaut, qui désigne que les demandes de connexion sont traitées localement.
- Nouvelle stratégie de demande de connexion. Il transfère les demandes de connexion à un serveur RADIUS NPS ou à un autre serveur RADIUS dans un domaine non approuvé.

La deuxième stratégie est nommée stratégie proxy. Il apparaît d'abord dans la liste triée des stratégies.

- Si une demande de connexion correspond à la stratégie proxy, la demande de connexion est transférée au serveur RADIUS dans le groupe de serveurs RADIUS distant.
- Si la demande de connexion ne correspond pas à la stratégie proxy, mais qu'elle correspond à la stratégie de demande de connexion par défaut, NPS traite la demande de connexion sur le serveur local.
- Si la demande de connexion ne correspond pas à une stratégie, elle est ignorée.

NPS en tant que serveur RADIUS avec des serveurs de comptabilité distants

Dans cet exemple, le serveur RADIUS NPS local n'est pas configuré pour effectuer la comptabilité. La stratégie de demande de connexion par défaut est révisée afin que les messages de comptabilité RADIUS soient transférés à un serveur RADIUS NPS ou à un autre serveur RADIUS dans un groupe de serveurs RADIUS distant.

Bien que les messages de comptabilité soient transférés dans cet exemple, les messages d'authentification et d'autorisation ne sont pas transférés. Le serveur RADIUS NPS local exécute les fonctions d'authentification et d'autorisation pour le domaine local et tous les domaines approuvés.

NPS avec un mappage entre les utilisateurs RADIUS distants et les utilisateurs Windows locaux

Dans cet exemple, NPS agit à la fois en tant que serveur RADIUS et en tant que proxy RADIUS. NPS gère chaque demande de connexion individuelle de la manière suivante :

- La demande d'authentification est transférée vers un serveur RADIUS distant.
- Un compte d'utilisateur Windows local est utilisé pour l'autorisation.

Pour implémenter cette configuration, vous devez configurer l'attribut **Remote RADIUS to Windows User Mapping** comme condition de la stratégie de demande de connexion. Vous créez également un compte d'utilisateur localement sur le serveur RADIUS. Ce compte doit avoir le même nom que le compte d'utilisateur distant sur lequel le serveur RADIUS distant effectue l'authentification.

Paramétrage

Pour configurer NPS en tant que serveur RADIUS, vous pouvez utiliser la configuration standard ou la configuration avancée dans la console NPS ou dans le Gestionnaire de serveur. Pour configurer NPS en tant que proxy RADIUS, vous devez utiliser la configuration avancée.

Configuration standard

Avec la configuration standard, des assistants sont fournis pour vous aider à configurer le service NPS dans les scénarios suivants :

- Serveur RADIUS pour les connexions d'accès à distance ou de réseau privé virtuel (VPN)
- Serveur RADIUS pour les connexions sans fil 802.1X ou câblées

Pour configurer NPS à l'aide d'un Assistant, ouvrez la console NPS, sélectionnez l'un des scénarios précédents, puis sélectionnez le lien de l'Assistant.

Configuration avancée

Lorsque vous utilisez la configuration avancée, vous configurez manuellement NPS en tant que serveur RADIUS ou proxy RADIUS.

Pour configurer NPS à l'aide de la configuration avancée, ouvrez la console NPS, puis **développez Configuration avancée**.

Les sections suivantes décrivent les éléments de configuration avancés fournis.

Configurer un serveur RADIUS

Pour configurer NPS en tant que serveur RADIUS, vous devez configurer les clients RADIUS, les stratégies réseau et la comptabilité RADIUS.

Pour obtenir des instructions sur la création de ces configurations, consultez les articles suivants :

- Configurer des clients RADIUS
- Configurer des stratégies réseau
- Configurer la comptabilité du serveur de stratégie réseau

Configurer un proxy RADIUS

Pour configurer NPS en tant que proxy RADIUS, vous devez configurer des clients RADIUS, des groupes de serveurs RADIUS distants et des stratégies de demande de connexion.

Pour obtenir des instructions sur la création de ces configurations, consultez les articles suivants :

- Configurer des clients RADIUS
- Configurer des groupes de serveurs RADIUS distants

- Configurer des stratégies de demande de connexion

Journalisation NPS

La journalisation NPS est également appelée comptabilité RADIUS. Vous pouvez configurer la journalisation NPS pour répondre à vos besoins si NPS est utilisé comme serveur RADIUS, proxy ou combinaison de ces configurations.

Pour configurer la journalisation NPS, vous devez configurer les événements que vous souhaitez journaliser et afficher avec l'Observateur d'événements, puis déterminer les autres informations que vous souhaitez journaliser. En outre, vous devez décider où stocker les journaux d'informations comptables et d'authentification des utilisateurs. Les options suivantes sont disponibles :

- Fichiers journaux texte stockés sur l'ordinateur local
- Une base de données SQL Server sur l'ordinateur local ou un ordinateur distant

Pour plus d'informations, consultez Configurer la comptabilité du serveur de stratégie réseau.

Contenu connexe

- Bonnes pratiques relatives au serveur de stratégie de réseau
- Bien démarrer avec le serveur de stratégie réseau
- Planifier un serveur NPS (Network Policy Server)
- Déployer le serveur de stratégie réseau (NPS)
- Gérer le serveur de stratégie réseau (NPS)
- Applets de commande NPS dans Windows PowerShell

Meilleures pratiques relatives au serveur NPS

30/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour en savoir plus sur les meilleures pratiques pour le déploiement et la gestion du serveur de stratégie réseau (NPS).

Les sections suivantes fournissent les meilleures pratiques pour différents aspects de votre déploiement NPS.

Accounting

Voici les meilleures pratiques pour la journalisation NPS.

Il existe deux types de comptabilité, ou journalisation, dans NPS :

- Journalisation des événements pour NPS. Vous pouvez utiliser la journalisation des événements pour enregistrer les événements NPS dans les journaux des événements système et de sécurité. Utilisé principalement pour l'audit et la résolution des problèmes de tentatives de connexion.
- Journalisation des demandes d'authentification utilisateurs et de gestion des comptes. Vous pouvez consigner les demandes d'authentification des utilisateurs et de gestion des comptes dans les fichiers journaux au format texte ou au format de base de données, ou vous pouvez vous connecter à une procédure stockée dans une base de données SQL Server 2000. La journalisation des demandes est principalement utilisée à des fins d'analyse des connexions et de facturation, et est également utile en tant qu'outil d'investigation de sécurité, vous fournissant une méthode de suivi de l'activité d'un attaquant.

Pour tirer le meilleur parti de la journalisation NPS :

- Activez la journalisation (initialement) pour les enregistrements d'authentification et de comptabilité. Modifiez ces sélections une fois que vous avez déterminé ce qui est approprié pour votre environnement.
- Assurez-vous que la journalisation des événements est configurée avec une capacité suffisante pour gérer vos journaux.

- Sauvegardez régulièrement tous les fichiers journaux, car ils ne peuvent pas être recréés lorsqu'ils sont endommagés ou supprimés.
- Utilisez l'attribut classe RADIUS pour suivre l'utilisation et simplifier l'identification du service ou de l'utilisateur à facturer pour l'utilisation. Bien que l'attribut Class généré automatiquement soit unique pour chaque requête, des enregistrements en double peuvent exister dans les cas où la réponse au serveur d'accès est perdue et la demande est renvoyée. Vous devrez peut-être supprimer les demandes en double de vos journaux pour suivre avec précision l'utilisation.
- If your network access servers and RADIUS proxy servers periodically send fictional connection request messages to NPS to verify that the NPS is online, use the **ping user-name** registry setting. Ce paramètre configure NPS pour rejeter automatiquement ces fausses demandes de connexion sans les traiter. En outre, NPS n'enregistre pas les transactions impliquant le nom d'utilisateur fictif dans les fichiers journaux, ce qui facilite l'interprétation du journal des événements.
- Désactiver le transfert de notifications NAS Vous pouvez désactiver le transfert des messages de démarrage et d'arrêt des messages des serveurs d'accès réseau (NAS) aux membres d'un groupe de serveurs RADIUS distant QUI EST configuré dans NPS. Pour plus d'informations, consultez Désactiver le transfert de notification NAS.

Pour plus d'informations, consultez Configuration du serveur NPS.

- Pour fournir un basculement et une redondance avec la journalisation SQL Server, placez deux ordinateurs exécutant SQL Server sur des sous-réseaux différents. Utilisez **l'Assistant Création de publication** SQL Server pour configurer la réplication de base de données entre les deux serveurs. Pour plus d'informations, consultez SQL Server documentation technique et Réplication SQL Server.

Authentication

Voici les meilleures pratiques pour l'authentification.

- Utilisez des méthodes d'authentification basées sur des certificats telles que le protocole PEAP (Protected Extensible Authentication Protocol) et le protocole EAP (Extensible Authentication Protocol) pour une authentification forte. N'utilisez pas de méthodes d'authentification par mot de passe uniquement, car elles sont vulnérables à diverses attaques et ne sont pas sécurisées. Pour l'authentification sans fil sécurisée, l'utilisation de PEAP-MS-CHAP v2 est recommandée, car le serveur NPS prouve son identité aux clients sans fil à l'aide d'un certificat de serveur, tandis que les utilisateurs prouvent leur identité avec leur nom d'utilisateur et leur mot de passe. Pour plus d'informations sur l'utilisation

de NPS dans votre déploiement sans fil, consultez Déployer Password-Based accès sans fil authentifié 802.1X.

- Déployez votre propre autorité de certification avec Active Directory® Certificate Services (AD CS) lorsque vous utilisez des méthodes d'authentification fortes basées sur des certificats, telles que PEAP et EAP, qui nécessitent l'utilisation d'un certificat de serveur sur les serveurs NPS. Vous pouvez également utiliser votre autorité de certification pour inscrire des certificats d'ordinateur et des certificats utilisateur. Pour plus d'informations sur le déploiement de certificats de serveur sur des serveurs NPS et d'accès à distance, consultez Déployer des certificats de serveur pour les déploiements câblés et sans fil 802.1X.

> **Important**
>
> Le serveur NPS (Network Policy Server) ne prend pas en charge l'utilisation des caractères ASCII étendus dans les mots de passe.

Configuration de l'ordinateur client

Voici les meilleures pratiques pour la configuration de l'ordinateur client.

- Configurez automatiquement tous vos ordinateurs clients 802.1X membres du domaine à l'aide de stratégie de groupe. Pour plus d'informations, consultez la section « Configurer les stratégies de réseau sans fil (IEEE 802.11) » dans la rubrique Déploiement de l'accès sans fil.

Installation suggestions

Voici les meilleures pratiques pour la journalisation NPS.

- Avant d'installer NPS, installez et testez chacun de vos serveurs d'accès réseau à l'aide de méthodes d'authentification locales avant de les configurer en tant que clients RADIUS dans NPS.

- After you install and configure NPS, save the configuration by using the Windows PowerShell command Export-NpsConfiguration. Enregistrez la configuration NPS avec cette commande chaque fois que vous reconfigurez le NPS.

> **Attention**

- Le fichier exporté contient des secrets partagés non chiffrés pour les clients RADIUS et les membres des groupes de serveurs RADIUS distants. Pour cette raison, veillez à enregistrer le fichier dans un emplacement sécurisé.
- Le processus d'exportation n'inclut pas les paramètres de journalisation pour Microsoft SQL Server dans le fichier exporté. Si vous importez le fichier exporté dans un autre serveur NPS, vous devez configurer manuellement la journalisation SQL Server sur le nouveau serveur.

Réglage des performances NPS

Voici les meilleures pratiques pour l'optimisation des performances NPS.

- Pour optimiser les temps de réponse d'authentification et d'autorisation NPS et réduire le trafic réseau, installez NPS sur un contrôleur de domaine.

- Lorsque des noms de principaux universels (UPN) ou des domaines Windows Server 2008 et Windows Server 2003 sont utilisés, NPS utilise le catalogue global pour authentifier les utilisateurs. Pour réduire le temps nécessaire à cette opération, installez NPS sur un serveur de catalogue global ou sur un serveur qui se trouve sur le même sous-réseau que le serveur de catalogue global.

- Lorsque vous avez configuré des groupes de serveurs RADIUS distants et que, dans **Stratégies de demande de connexion** NPS, vous décochez la case Enregistrer les informations de compte sur les serveurs dans le groupe de serveurs RADIUS distant suivant, ces groupes reçoivent toujours des messages de notification de démarrage et d'arrêt NAS. Cela crée un trafic réseau inutile. Pour éliminer ce trafic, désactivez le transfert de notification NAS pour les serveurs individuels de chaque groupe de serveurs RADIUS distant en décochant la case **Démarrer et arrêter les notifications réseau vers ce serveur** .

Utilisation de NPS dans les grandes organisations

Voici les meilleures pratiques pour l'utilisation de NPS dans les grandes organisations.

- Si vous utilisez des stratégies réseau pour restreindre l'accès à tous les groupes sauf à certains groupes, créez un groupe universel pour tous les utilisateurs pour lesquels vous souhaitez autoriser l'accès, puis créez une stratégie réseau qui accorde l'accès à ce groupe universel. Ne placez pas tous vos utilisateurs directement dans le groupe universel, en particulier si vous en avez un grand nombre sur votre réseau. Au lieu de cela,

créez des groupes distincts qui sont membres du groupe universel et ajoutez des utilisateurs à ces groupes.

- Utilisez un nom d'utilisateur principal pour faire référence aux utilisateurs chaque fois que possible. Un utilisateur peut avoir le même nom d'utilisateur principal, quelle que soit l'appartenance au domaine. Cette pratique offre une scalabilité qui peut être requise dans les organisations disposant d'un grand nombre de domaines.

- Si vous avez installé le serveur NPS (Network Policy Server) sur un ordinateur autre qu'un contrôleur de domaine et que le serveur NPS reçoit un grand nombre de demandes d'authentification par seconde, vous pouvez améliorer les performances du serveur NPS en augmentant le nombre d'authentifications simultanées autorisées entre le serveur NPS et le contrôleur de domaine. Pour plus d'informations, consultez Augmenter les authentifications simultanées traitées par NPS.

Security issues

Voici les meilleures pratiques pour réduire les problèmes de sécurité.

Lorsque vous administrez un NPS à distance, n'envoyez pas de données sensibles ou confidentielles (par exemple, des secrets partagés ou des mots de passe) sur le réseau en texte clair. Il existe deux méthodes recommandées pour l'administration à distance des serveurs NPS :

- Utilisez les services Bureau à distance pour accéder au serveur NPS. Lorsque vous utilisez les services Bureau à distance, les données ne sont pas envoyées entre le client et le serveur. Seule l'interface utilisateur du serveur (par exemple, le bureau du système d'exploitation et l'image de console NPS) est envoyée au client des services Bureau à distance, qui est nommé Connexion Bureau à distance dans Windows® 10. Le client envoie une entrée au clavier et à la souris, qui est traitée localement par le serveur sur lequel les services Bureau à distance sont activés. Lorsque les utilisateurs des services Bureau à distance se connectent, ils peuvent afficher uniquement leurs sessions clientes individuelles, qui sont gérées par le serveur et indépendantes les unes des autres. En outre, la connexion Bureau à distance fournit un chiffrement 128 bits entre le client et le serveur.

- Utilisez la sécurité du protocole Internet (IPsec) pour chiffrer les données confidentielles. Vous pouvez utiliser IPsec pour chiffrer la communication entre le serveur NPS et l'ordinateur client distant que vous utilisez pour administrer NPS. Pour administrer le serveur à distance, vous pouvez installer les Outils d'administration de serveur distant pour Windows 10 sur l'ordinateur client. Après l'installation, utilisez la console de gestion Microsoft (MMC) pour ajouter le composant logiciel enfichable NPS à la console.

> **Important**
>
> Vous pouvez installer les outils d'administration de serveur distant pour Windows 10 uniquement sur la version complète de Windows 10 Professionnel ou Windows 10 Entreprise.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Prise en main du serveur NPS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser les rubriques de cette section pour en savoir plus sur les fonctionnalités du serveur NPS (Network Policy Server).

> ⓘ **Notes**
>
> Pour obtenir des informations supplémentaire sur le serveur NPS, vous pouvez utiliser les sections de bibliothèque suivantes.
>
> - Planifier un serveur NPS (Network Policy Server)
> - Déployer un serveur NPS (Network Policy Server)
> - Gérer Serveur NPS (Network Policy Server)

Cette section contient les rubriques suivantes :

- Traitement des demandes de connexion
- Stratégies réseau
- Modèles NPS
- RADIUS Clients

Traitement des requêtes de connexion

Article • 09/03/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Vous pouvez utiliser cette rubrique pour en savoir plus sur le traitement des demandes de connexion dans le serveur NPS (Network Policy Server) pour Windows Server 2016.

Notes

En plus de cette rubrique, la documentation suivante sur le traitement des demandes est disponible.

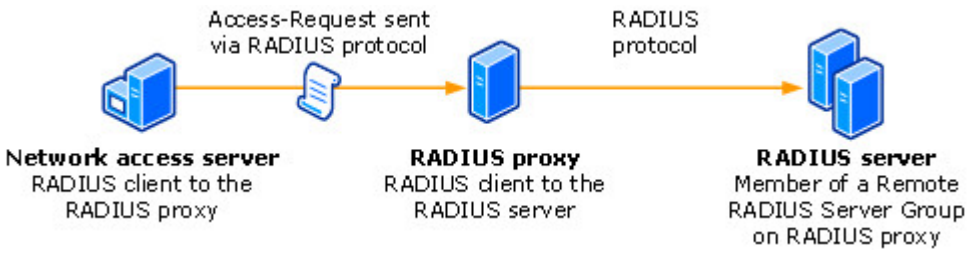
- **Stratégies de demande de connexion**
- **Noms de domaine**
- **Groupes de serveurs RADIUS distants**

Vous pouvez utiliser le traitement des demandes de connexion pour spécifier où est effectuée l’authentification des demandes de connexion (sur l’ordinateur local ou sur un serveur RADIUS distant membre d’un groupe de serveurs RADIUS distants).

Si vous souhaitez que le serveur local exécutant le serveur NPS (Network Policy Server) effectue l’authentification pour les demandes de connexion, vous pouvez utiliser la stratégie de demande de connexion par défaut sans configuration supplémentaire. En fonction de la stratégie par défaut, le serveur NPS authentifie les utilisateurs et les ordinateurs qui ont un compte dans le domaine local et dans les domaines approuvés.

Si vous souhaitez transférer les demandes de connexion à un serveur NPS ou autre serveur RADIUS distant, créez un groupe de serveurs RADIUS distants, puis configurez une stratégie de demande de connexion qui transfère les demandes à ce groupe de serveurs RADIUS distants. Avec cette configuration, le serveur NPS peut transférer les demandes d’authentification à n’importe quel serveur RADIUS, et les utilisateurs qui ont des comptes dans des domaines non approuvés peuvent être authentifiés.

L’illustration suivante montre le chemin d’un message Access-Request (demande d’accès) d’un serveur d’accès réseau vers un proxy RADIUS, puis vers un serveur RADIUS dans un groupe de serveurs RADIUS distants. Sur le proxy RADIUS, le serveur d’accès réseau est configuré comme un client RADIUS et, sur chaque serveur RADIUS, le proxy RADIUS est configuré comme un client RADIUS.



> ⓘ **Notes**
>
> Les serveurs d'accès réseau que vous utilisez avec le serveur NPS peuvent être des appareils de passerelle conformes au protocole RADIUS, comme les points d'accès sans fil 802.1X et les commutateurs d'authentification, les serveurs exécutant Accès à distance configurés comme serveurs VPN ou serveurs d'accès à distance, ou d'autres appareils compatibles RADIUS.

Si vous souhaitez que le serveur NPS traite certaines demandes d'authentification localement tout en transférant d'autres demandes à un groupe de serveurs RADIUS distants, configurez plusieurs stratégies de demande de connexion.

Pour configurer une stratégie de demande de connexion qui spécifie le serveur NPS ou le groupe de serveurs RADIUS qui traite les demandes d'authentification, consultez Stratégies de demande de connexion.

Pour spécifier le serveur NPS ou d'autres serveurs RADIUS auxquels les demandes d'authentification sont transférées, consultez Groupes de serveurs RADIUS distants.

Serveur NPS pour traiter les demandes de connexion de serveur RADIUS

Quand vous utilisez le serveur NPS comme serveur RADIUS, les messages RADIUS fournissent l'authentification, l'autorisation et la gestion des comptes pour les connexions d'accès réseau de la manière suivante :

1. Les serveurs d'accès, comme les serveurs d'accès réseau à distance, les serveurs VPN et les points d'accès sans fil, reçoivent des demandes de connexion des clients d'accès.

2. Le serveur d'accès, configuré pour utiliser RADIUS comme protocole d'authentification, d'autorisation et de gestion des comptes, crée un message Access-Request et l'envoie au serveur NPS.

3. Le serveur NPS évalue le message Access-Request.

4. Si nécessaire, le serveur NPS envoie un message Access-Challenge (défi d'accès) au serveur d'accès. Le serveur d'accès traite le défi et envoie un message Access-Request mis à jour au serveur NPS.

5. Les informations d'identification de l'utilisateur sont vérifiées et les propriétés de participation du compte d'utilisateur sont obtenues en utilisant une connexion sécurisée à un contrôleur de domaine.

6. La tentative de connexion est autorisée avec les propriétés de participation du compte d'utilisateur et des stratégies réseau.

7. Si la tentative de connexion est authentifiée et autorisée, le serveur NPS envoie un message Access-Accept (accès autorisé) au serveur d'accès. Si la tentative de connexion n'est pas authentifiée ou pas autorisée, le serveur NPS envoie un message Access-Reject (accès refusé) au serveur d'accès.

8. Le serveur d'accès termine le processus de connexion avec le client d'accès et envoie un message Accounting-Request (demande de gestion des comptes) au serveur NPS, où le message est journalisé.

9. Le serveur NPS envoie un message Accounting-Response (réponse de gestion des comptes) au serveur d'accès.

> ⓘ **Notes**
>
> Le serveur d'accès envoie également des messages Accounting-Request quand la connexion est établie, quand la connexion du client d'accès est fermée, et quand le serveur d'accès est démarré puis arrêté.

Serveur NPS pour traiter les demandes de connexion de proxy RADIUS

Quand le serveur NPS est utilisé comme proxy RADIUS entre un client RADIUS et un serveur RADIUS, les messages RADIUS pour les tentatives de connexion d'accès réseau sont transférés de la manière suivante :

1. Les serveurs d'accès, comme les serveurs d'accès réseau à distance, les serveurs de réseau privé virtuel (VPN) et les points d'accès sans fil, reçoivent des demandes de connexion des clients d'accès.

2. Le serveur d'accès, configuré pour utiliser RADIUS comme protocole d'authentification, d'autorisation et de gestion des comptes, crée un message

Access-Request et l'envoie au serveur NPS utilisé comme proxy RADIUS NPS.

3. Le proxy RADIUS NPS reçoit le message Access-Request et, en fonction des stratégies de demande de connexion configurées localement, détermine où transférer le message Access-Request.

4. Le proxy RADIUS NPS transfère le message Access-Request au serveur RADIUS approprié.

5. Le serveur RADIUS évalue le message Access-Request.

6. Si nécessaire, le serveur RADIUS envoie un message Access-Challenge au proxy RADIUS NPS, d'où il est transféré au serveur d'accès. Le serveur d'accès traite le défi avec le client d'accès et envoie un message Access-Request mis à jour au proxy RADIUS NPS, d'où il est transféré au serveur RADIUS.

7. Le serveur RADIUS authentifie et autorise la tentative de connexion.

8. Si la tentative de connexion est à la fois authentifiée et autorisée, le serveur RADIUS envoie un message Access-Accept au proxy RADIUS NPS, d'où il est transféré au serveur d'accès. Si la tentative de connexion n'est pas authentifiée ou pas autorisée, le serveur RADIUS envoie un message Access-Reject au proxy RADIUS NPS, d'où il est transféré au serveur d'accès.

9. Le serveur d'accès termine le processus de connexion avec le client d'accès et envoie un message Accounting-Request au proxy RADIUS NPS. Le proxy RADIUS NPS journalise les données de gestion des comptes et transfère le message au serveur RADIUS.

10. Le serveur RADIUS envoie un message Accounting-Response au proxy RADIUS NPS, d'où il est transféré au serveur d'accès.

Pour plus d'informations sur le serveur NPS, consultez Serveur NPS (Network Policy Server).

Stratégies de requête de connexion

Article • 06/10/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Vous pouvez utiliser cette rubrique pour apprendre à utiliser des stratégies de demande de connexion au serveur NPS (Network Policy Server) pour configurer le serveur NPS en tant que serveur RADIUS, proxy RADIUS ou les deux.

Notes

En plus de cette rubrique, la documentation suivante sur la stratégie de demande de connexion est disponible.

- **Configurer des stratégies de demande de connexion**
- **Configurer des groupes de serveurs RADIUS distants**

Les stratégies de demande de connexion sont des ensembles de conditions et de paramètres qui permettent aux administrateurs réseau de désigner les serveurs RADIUS (Remote Authentication Dial-In User Service) qui effectuent l’authentification et l’autorisation des demandes de connexion que le serveur exécutant le serveur NPS (Network Policy Server) reçoit des clients RADIUS. Les stratégies de demande de connexion peuvent être configurées pour désigner les serveurs RADIUS utilisés pour la gestion des comptes RADIUS.

Vous pouvez créer des stratégies de demande de connexion afin que certains messages de demande RADIUS envoyés à partir de clients RADIUS soient traités localement (le serveur NPS est utilisé comme serveur RADIUS) et que d’autres types de messages soient transférés vers un autre serveur RADIUS (le serveur NPS est utilisé comme proxy RADIUS).

Avec les stratégies de demande de connexion, vous pouvez utiliser NPS comme serveur RADIUS ou comme proxy RADIUS, en fonction de facteurs tels que les suivants :

- Heure de la journée et jour de la semaine
- Nom du domaine dans la demande de connexion
- Type de connexion demandé
- Adresse IP du client RADIUS

Les messages RADIUS Access-Request sont traités ou transférés par NPS uniquement si les paramètres du message entrant correspondent à au moins l’une des stratégies de

demande de connexion configurées sur le serveur NPS (Network Policy Server).

Si les paramètres de stratégie correspondent et que la stratégie exige que le serveur NPS (Network Policy Server) traite le message, il agit en tant que serveur RADIUS, authentifiant et autorisant la demande de connexion. Si les paramètres de stratégie correspondent et que la stratégie nécessite que le serveur NPS (Network Policy Server) transfère le message, il agit comme un proxy RADIUS et transfère la demande de connexion à un serveur RADIUS distant pour traitement.

Si les paramètres d'un message RADIUS Access-Request entrant ne correspondent pas à au moins l'une des stratégies de demande de connexion, un message Access-Reject est envoyé au client RADIUS et l'utilisateur ou l'ordinateur qui tente de se connecter au réseau se voit refuser l'accès.

Exemples de configuration

Les exemples de configuration suivants montrent comment utiliser des stratégies de demande de connexion.

NPS comme serveur RADIUS

La stratégie de demande de connexion par défaut est la seule stratégie configurée. Dans cet exemple, le serveur NPS (Network Policy Server) est configuré en tant que serveur RADIUS et toutes les demandes de connexion sont traitées par le serveur NPS local. Le serveur NPS (Network Policy Server) peut authentifier et autoriser les utilisateurs dont les comptes se trouvent dans le domaine du domaine NPS et dans les domaines approuvés.

NPS en tant que proxy RADIUS

La stratégie de demande de connexion par défaut est supprimée et deux nouvelles stratégies de demande de connexion sont créées pour transférer les demandes vers deux domaines différents. Dans cet exemple, le serveur NPS (Network Policy Server) est configuré en tant que proxy RADIUS. Le serveur NPS (Network Policy Server) ne traite aucune demande de connexion sur le serveur local. Au lieu de cela, il transfère les demandes de connexion au serveur NPS (Network Policy Server) ou à d'autres serveurs RADIUS configurés en tant que membres de groupes de serveurs RADIUS distants.

Serveur NPS (Network Policy Server) en tant que serveur RADIUS et proxy RADIUS

En plus de la stratégie de demande de connexion par défaut, une nouvelle stratégie de demande de connexion est créée qui transfère les demandes de connexion à un serveur NPS (Network Policy Server) ou à un autre serveur RADIUS dans un domaine non approuvé. Dans cet exemple, la stratégie de proxy apparaît en premier dans la liste ordonnée des stratégies. Si la demande de connexion correspond à la stratégie de proxy, la demande de connexion est transférée au serveur RADIUS dans le groupe de serveurs RADIUS distant. Si la demande de connexion ne correspond pas à la stratégie de proxy, mais à la stratégie de demande de connexion par défaut, le serveur NPS (Network Policy Server) traite la demande de connexion sur le serveur local. Si la demande de connexion ne correspond à aucune des stratégies, elle est ignorée.

Serveur NPS (Network Policy Server) en tant que serveur RADIUS avec des serveurs de gestion des comptes distants

Dans cet exemple, le serveur NPS (Network Policy Server) local n'est pas configuré pour effectuer la gestion des comptes et la stratégie de demande de connexion par défaut est révisée afin que les messages de gestion des comptes RADIUS soient transférés à un serveur NPS ou à un autre serveur RADIUS dans un groupe de serveurs RADIUS distant. Bien que les messages de gestion des comptes soient transférés, les messages d'authentification et d'autorisation ne sont pas transférés, et le serveur NPS (Network Policy Server) local exécute ces fonctions pour le domaine local et tous les domaines approuvés.

Serveur NPS (Network Policy Server) avec Remote RADIUS to Windows User Mapping

Dans cet exemple, le serveur NPS (Network Policy Server) agit à la fois comme serveur RADIUS et comme proxy RADIUS pour chaque demande de connexion individuelle en transférant la demande d'authentification à un serveur RADIUS distant tout en utilisant un compte d'utilisateur Windows local pour l'autorisation. Cette configuration est implémentée en configurant l'attribut Remote RADIUS to Windows User Mapping comme condition de la stratégie de demande de connexion. (En outre, un compte d'utilisateur doit être créé localement avec le même nom que le compte d'utilisateur distant sur lequel l'authentification est effectuée par le serveur RADIUS distant.)

Conditions de la stratégie de demande de connexion

Les conditions de stratégie de demande de connexion sont un ou plusieurs attributs RADIUS qui sont comparés aux attributs du message RADIUS Access-Request entrant. S'il existe plusieurs conditions, toutes les conditions du message de demande de connexion et de la stratégie de demande de connexion doivent correspondre pour que la stratégie soit appliquée par le serveur NPS (Network Policy Server).

Voici les attributs de condition disponibles que vous pouvez configurer dans les stratégies de demande de connexion.

Groupe d'attributs de propriétés de connexion

Le groupe d'attributs de propriétés de connexion contient les attributs suivants.

- **Protocole encadré**. Utilisé pour désigner le type de cadrage des paquets entrants. Par exemple, le protocole PPP (Point-to-Point), le protocole SLIP (Serial Line Internet Protocol), Frame Relay et X.25.
- **Type de service**. Utilisé pour désigner le type de service demandé. Les exemples incluent les connexions encadrées (par exemple, les connexions PPP) et les connexions (par exemple, les connexions Telnet). Pour plus d'informations sur les types de service RADIUS, consultez RFC 2865, « Remote Authentication Dial-in User Service (RADIUS) ».
- **Type de tunnel**. Utilisé pour désigner le type de tunnel en cours de création par le client demandeur. Les types de tunnel incluent le protocole PPTP (Point-to-Point Tunneling Protocol) et le protocole L2TP (Layer Two Tunneling Protocol).

Groupe d'attributs des restrictions de jour et d'heure

Le groupe d'attributs des restrictions de jour et d'heure contient l'attribut des restrictions de jour et d'heure. Avec cet attribut, vous pouvez désigner le jour de la semaine et l'heure de la tentative de connexion. Le jour et l'heure sont relatifs au jour et à l'heure du serveur NPS (Network Policy Server).

Groupe d'attributs de passerelle

Le groupe d'attributs de passerelle contient les attributs suivants.

- **ID de la station appelée**. Utilisé pour désigner le numéro de téléphone du serveur d'accès réseau. Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des indicatifs régionaux.
- **Identificateur du périphérique NAS (Network Attached Storage)**. Utilisé pour désigner le nom du serveur d'accès réseau. Cet attribut est une chaîne de

caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des identificateurs du périphérique NAS (Network Attached Storage).

- **Adresse IPv4 du périphérique NAS (Network Attached Storage)**. Utilisé pour désigner l'adresse IPv4 (Internet Protocol version 4) du serveur d'accès réseau (le client RADIUS). Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des réseaux IP.
- **Adresse IPv6 du périphérique NAS (Network Attached Storage)**. Utilisé pour désigner l'adresse IPv6 (Internet Protocol version 6) du serveur d'accès réseau (le client RADIUS). Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des réseaux IP.
- **Type de port du périphérique NAS (Network Attached Storage)**. Utilisé pour désigner le type de média utilisé par le client d'accès. Les exemples sont les lignes téléphoniques analogiques (appelées asynchrones), le réseau numérique à intégration de services (ISDN), les tunnels ou les réseaux privés virtuels (VPN), les réseaux sans fil IEEE 802.11 et Ethernet.

Groupe d'attributs d'identité de l'ordinateur

Le groupe d'attributs d'identité de l'ordinateur contient l'attribut d'identité de l'ordinateur. À l'aide de cet attribut, vous pouvez spécifier la méthode avec laquelle les clients sont identifiés dans la stratégie.

Groupe d'attributs des propriétés du client RADIUS

Le groupe d'attributs des propriétés du client RADIUS contient les attributs suivants.

- **ID de la station appelante**. Utilisé pour désigner le numéro de téléphone utilisé par l'appelant (le client d'accès). Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des indicatifs régionaux. Dans les authentifications 802.1x, l'adresse MAC est généralement renseignée et peut être mise en correspondance à partir du client. Ce champ est généralement utilisé pour les scénarios de contournement d'adresse Mac lorsque la stratégie de demande de connexion est configurée pour « Accepter les utilisateurs sans valider les informations d'identification ».
- **Nom convivial du client**. Utilisé pour désigner le nom de l'ordinateur client RADIUS qui demande l'authentification. Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier les noms des clients.
- **Adresse IPv4 du client**. Utilisé pour désigner l'adresse IPv4 du serveur d'accès réseau (le client RADIUS). Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des réseaux IP.

- **Adresse IPv6 du client**. Utilisé pour désigner l'adresse IPv6 du serveur d'accès réseau (le client RADIUS). Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des réseaux IP.
- **Fournisseur du client**. Utilisé pour désigner le fournisseur du serveur d'accès réseau qui demande l'authentification. Un ordinateur exécutant le service de routage et d'accès à distance est le fabricant du périphérique NAS (Network Attached Storage) Microsoft. Vous pouvez utiliser cet attribut pour configurer des stratégies distinctes pour différents fabricants de périphériques NAS (Network Attached Storage). Cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle.

Groupe d'attributs de nom d'utilisateur

Le groupe d'attributs de nom d'utilisateur contient l'attribut de nom d'utilisateur. À l'aide de cet attribut, vous pouvez désigner le nom d'utilisateur, ou une partie du nom d'utilisateur, qui doit correspondre au nom d'utilisateur fourni par le client d'accès dans le message RADIUS. Cet attribut est une chaîne de caractères qui contient généralement un nom de domaine et un nom de compte d'utilisateur. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier les noms des utilisateurs.

Paramètres de stratégie de demande de connexion

Les paramètres de stratégie de demande de connexion sont un ensemble de propriétés qui sont appliquées à un message RADIUS entrant. Les paramètres se composent des groupes de propriétés suivants.

- Authentification
- Comptabilité
- Manipulation d'attributs
- Transfert de la requête
- Avancé

Les sections suivantes fournissent des détails supplémentaires sur ces paramètres.

Authentification

À l'aide de ce paramètre, vous pouvez remplacer les paramètres d'authentification configurés dans toutes les stratégies réseau et vous pouvez désigner les méthodes et les types d'authentification requis pour se connecter à votre réseau.

> **Important**
>
> Si vous configurez une méthode d'authentification dans la stratégie de demande de connexion qui est moins sécurisée que la méthode d'authentification que vous configurez dans la stratégie réseau, la méthode d'authentification plus sécurisée que vous configurez dans la stratégie réseau est remplacée. Par exemple, si vous avez une stratégie réseau qui nécessite l'utilisation de l'authentification extensible protégée Protocol-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2), qui est une méthode d'authentification par mot de passe pour la connexion sans fil sécurisée, et que vous configurez également une stratégie de demande de connexion pour autoriser l'accès non authentifié, le résultat est qu'aucun client n'est tenu de s'authentifier à l'aide de PEAP-MS-CHAP v2. Dans cet exemple, tous les clients qui se connectent à votre réseau se voient accorder un accès non authentifié.

Comptabilité

À l'aide de ce paramètre, vous pouvez configurer la stratégie de demande de connexion pour transférer les informations de gestion des comptes à un serveur NPS (Network Policy Server) ou à un autre serveur RADIUS dans un groupe de serveurs RADIUS distant afin que le groupe de serveurs RADIUS distant effectue la gestion des comptes.

> **Notes**
>
> Si vous avez plusieurs serveurs RADIUS et que vous souhaitez obtenir des informations de gestion des comptes pour tous les serveurs stockés dans une base de données de gestion des comptes RADIUS centrale, vous pouvez utiliser le paramètre de gestion des comptes de la stratégie de demande de connexion dans une stratégie sur chaque serveur RADIUS pour transférer les données gestion des comptes de tous les serveurs vers un serveur NPS (Network Policy Server) ou un autre serveur RADIUS désigné comme serveur de gestion des comptes.

Les paramètres de gestion des comptes de la stratégie de demande de connexion fonctionnent indépendamment de la configuration de gestion des comptes du serveur NPS (Network Policy Server) local. En d'autres termes, si vous configurez le serveur NPS (Network Policy Server) local pour enregistrer les informations de gestion des comptes RADIUS dans un fichier local ou dans une base de données Microsoft SQL Server, il le fait, que vous configuriez ou non une stratégie de demande de connexion pour

transférer des messages de gestion des comptes à un groupe de serveurs RADIUS distant.

Si vous souhaitez que les informations de gestion des comptes soient enregistrées à distance, mais pas localement, vous devez configurer le serveur NPS (Network Policy Server) local pour ne pas effectuer de gestion des comptes, tout en configurant la gestion des comptes dans une stratégie de demande de connexion pour transférer les données de gestion des comptes à un groupe de serveurs RADIUS distant.

Manipulation d'attributs

Vous pouvez configurer un ensemble de règles de recherche et de remplacement qui manipulent les chaînes de texte de l'un des attributs suivants.

- User Name
- ID de la station appelée
- ID de la station appelante

Le traitement des règles de recherche et de remplacement se produit pour l'un des attributs précédents avant que le message RADIUS ne soit soumis aux paramètres d'authentification et de gestion des comptes. Les règles de manipulation d'attributs s'appliquent uniquement à un seul attribut. Vous ne pouvez pas configurer des règles de manipulation d'attribut pour chaque attribut. En outre, la liste des attributs que vous pouvez manipuler est une liste statique. Vous ne pouvez pas ajouter à la liste des attributs disponibles pour la manipulation.

> ⓘ **Notes**
>
> Si vous utilisez le protocole d'authentification MS-CHAP v2, vous ne pouvez pas manipuler l'attribut de nom d'utilisateur si la stratégie de demande de connexion est utilisée pour transférer le message RADIUS. La seule exception se produit lorsqu'une barre oblique inverse () est utilisée et que la manipulation affecte uniquement les informations situées à gauche de celle-ci. Une barre oblique inverse est généralement utilisée pour indiquer un nom de domaine (les informations à gauche de la barre oblique inverse) et un nom de compte d'utilisateur dans le domaine (les informations à droite de la barre oblique inverse). Dans ce cas, seules les règles de manipulation d'attributs qui modifient ou remplacent le nom de domaine sont autorisées.

Pour obtenir des exemples de manipulation du nom de domaine dans l'attribut de nom d'utilisateur, consultez la section « Exemples de manipulation du nom de domaine dans

l'attribut de nom d'utilisateur » dans la rubrique Utiliser des expressions régulières dans le serveur NPS (Network Policy Server).

Transfert de la requête

Vous pouvez définir les options de demande de transfert suivantes utilisées pour les messages RADIUS Access-Request :

- **Authentifier les demandes sur ce serveur**. En utilisant ce paramètre, le serveur NPS (Network Policy Server) utilise un domaine Windows NT 4.0, Active Directory ou la base de données de comptes d'utilisateur du Gestionnaire de comptes de sécurité (SAM) locale pour authentifier la demande de connexion. Ce paramètre spécifie également que la stratégie réseau correspondante configurée dans le serveur NPS (Network Policy Server), ainsi que les propriétés de numérotation du compte d'utilisateur, sont utilisées par le serveur NPS pour autoriser la demande de connexion. Dans ce cas, le serveur NPS (Network Policy Server) est configuré pour s'exécuter en tant que serveur RADIUS.

- **Transférer les demandes au groupe de serveurs RADIUS distant suivant**. En utilisant ce paramètre, le serveur NPS (Network Policy Server) transfère les demandes de connexion au groupe de serveurs RADIUS distant que vous spécifiez. Si le serveur NPS (Network Policy Server) reçoit un message Access-Accept valide qui correspond au message Access-Request, la tentative de connexion est considérée comme authentifiée et autorisée. Dans ce cas, le serveur NPS (Network Policy Server) agit comme un proxy RADIUS.

- **Accepter les utilisateurs sans valider les informations d'identification**. En utilisant ce paramètre, le serveur NPS (Network Policy Server) ne vérifie pas l'identité de l'utilisateur qui tente de se connecter au réseau et le serveur NPS ne tente pas de vérifier que l'utilisateur ou l'ordinateur a le droit de se connecter au réseau. Lorsque le serveur NPS (Network Policy Server) est configuré pour autoriser l'accès non authentifié et qu'il reçoit une demande de connexion, le serveur NPS envoie immédiatement un message Access-Accept au client RADIUS et l'utilisateur ou l'ordinateur se voit accorder l'accès réseau. Ce paramètre est utilisé pour certains types de tunneling obligatoire où le client d'accès est tunnelé avant que les informations d'identification de l'utilisateur soient authentifiées.

> ⓘ **Notes**
>
> Cette option d'authentification ne peut pas être utilisée lorsque le protocole d'authentification du client d'accès est MS-CHAP v2 ou EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), qui fournissent tous deux une

authentification mutuelle. Dans l'authentification mutuelle, le client d'accès prouve qu'il s'agit d'un client d'accès valide pour le serveur d'authentification (le serveur NPS (Network Policy Server)), et le serveur d'authentification prouve qu'il s'agit d'un serveur d'authentification valide pour le client d'accès. Lorsque cette option d'authentification est utilisée, le message Access-Accept est retourné. Toutefois, le serveur d'authentification ne fournit pas de validation au client d'accès et l'authentification mutuelle échoue.

Pour obtenir des exemples d'utilisation d'expressions régulières pour créer des règles d'acheminement qui transfèrent des messages RADIUS avec un nom de domaine spécifié à un groupe de serveurs RADIUS distant, consultez la section « Exemple de transfert de messages RADIUS par un serveur proxy » dans la rubrique Utiliser des expressions régulières dans le serveur NPS (Network Policy Server).

Avancé

Vous pouvez définir des propriétés avancées pour spécifier la série d'attributs RADIUS qui sont les suivants :

- Ajout au message de réponse RADIUS lorsque le serveur NPS (Network Policy Server) est utilisé comme serveur d'authentification ou de gestion des comptes RADIUS. Quand des attributs sont spécifiés à la fois sur une stratégie réseau et sur la stratégie de demande de connexion, les attributs envoyés dans le message de réponse RADIUS sont la combinaison des deux ensembles d'attributs.
- Ajouté au message RADIUS lorsque le serveur NPS (Network Policy Server) est utilisé comme proxy d'authentification ou de gestion des comptes RADIUS. Si l'attribut existe déjà dans le message transféré, il est remplacé par la valeur de l'attribut spécifié dans la stratégie de demande de connexion.

En outre, certains attributs disponibles pour la configuration sous l'onglet **Paramètres** de la stratégie de demande de connexion dans la catégorie **Avancé** fournissent des fonctionnalités spécialisées. Par exemple, vous pouvez configurer l'attribut **Remote RADIUS to Windows User Mapping** lorsque vous souhaitez fractionner l'authentification et l'autorisation d'une demande de connexion entre deux bases de données de comptes d'utilisateur.

L'attribut **Remote RADIUS to Windows User Mapping** spécifie que l'autorisation Windows a lieu pour les utilisateurs qui sont authentifiés par un serveur RADIUS distant. En d'autres termes, un serveur RADIUS distant effectue l'authentification sur un compte d'utilisateur dans une base de données de comptes d'utilisateurs distants, mais le serveur NPS (Network Policy Server) local autorise la demande de connexion sur un

compte d'utilisateur dans une base de données de comptes d'utilisateur locale. Cela est utile lorsque vous souhaitez autoriser les visiteurs à accéder à votre réseau.

Par exemple, les visiteurs des organisations partenaires peuvent être authentifiés par leur propre serveur RADIUS de l'organisation partenaire, puis utiliser un compte d'utilisateur Windows au sein de votre organisation pour accéder à un réseau local (LAN) invité sur votre réseau.

Les autres attributs qui fournissent des fonctionnalités spécialisées sont les suivants :

- **MS-Quarantine-IPFilter et MS-Quarantine-Session-Timeout**. Ces attributs sont utilisés lorsque vous déployez le contrôle de quarantaine d'accès réseau (NAQC) avec votre déploiement VPN de routage et d'accès à distance.
- **Passport-User-Mapping-UPN-Suffix**. Cet attribut vous permet d'authentifier les demandes de connexion avec les informations d'identification de compte d'utilisateur Windows Live™ ID.
- **Tunnel-Tag**. Cet attribut désigne le numéro d'ID de réseau local virtuel auquel la connexion doit être attribuée par le serveur NAS lorsque vous déployez des réseaux locaux virtuels (VLAN).

Stratégie de demande de connexion par défaut

Une stratégie de demande de connexion par défaut est créée lorsque vous installez le serveur NPS (Network Policy Server). Cette stratégie a la configuration suivante.

- L'authentification n'est pas configurée.
- La gestion des comptes n'est pas configurée pour transférer les informations de gestion des comptes à un groupe de serveurs RADIUS distant.
- L'attribut n'est pas configuré avec des règles de manipulation d'attribut qui transfèrent les demandes de connexion aux groupes de serveurs RADIUS distants.
- La demande de transfert est configurée pour que les demandes de connexion soient authentifiées et autorisées sur le serveur NPS (Network Policy Server) local.
- Les attributs avancés ne sont pas configurés.

La stratégie de demande de connexion par défaut utilise le serveur NPS (Network Policy Server) comme serveur RADIUS. Pour configurer un serveur exécutant le serveur NPS (Network Policy Server) en tant que proxy RADIUS, vous devez également configurer un groupe de serveurs RADIUS distant. Vous pouvez créer un groupe de serveurs RADIUS distant pendant que vous créez une stratégie de demande de connexion à l'aide de l'assistant de la nouvelle stratégie de demande de connexion. Vous pouvez supprimer la stratégie de demande de connexion par défaut ou vérifier que la stratégie de demande

de connexion par défaut est la dernière stratégie traitée par le serveur NPS (Network Policy Server) en la plaçant en dernier dans la liste ordonnée des stratégies.

Notes

Si le serveur NPS (Network Policy Server) et le service d'accès à distance sont installés sur le même ordinateur et que le service d'accès à distance est configuré pour l'authentification et la gestion des comptes Windows, il est possible que les demandes d'authentification et de gestion des comptes de l'accès à distance soient transférées à un serveur RADIUS. Cela peut se produire lorsque des demandes d'authentification et de gestion des comptes d'accès à distance correspondent à une stratégie de demande de connexion configurée pour les transférer à un groupe de serveurs RADIUS distant.

Noms de domaine

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Consultez cette rubrique pour comprendre l'utilisation des noms de domaine dans le cadre du traitement des demandes de connexion du serveur NPS (Network Policy Server).

L'attribut RADIUS User-Name est une chaîne de caractères qui contient généralement un emplacement de compte utilisateur et un nom de compte utilisateur. L'emplacement du compte utilisateur est également appelé domaine ou nom de domaine, et est semblable aux domaines DNS, aux domaines Active Directory® et aux domaines Windows NT 4.0. Par exemple, si un compte utilisateur se trouve dans la base de données des comptes utilisateur pour un domaine nommé example.com, example.com constitue le nom de domaine.

Dans un autre exemple, si l'attribut RADIUS User-Name contient le nom d'utilisateur user1@example.com, user1 est le nom du compte utilisateur et example.com est le nom de domaine. Les noms de domaine peuvent être présentés dans le nom d'utilisateur sous forme de préfixe ou de suffixe :

- **Example\user1**. Dans cet exemple, le nom de domaine **Example** est un préfixe ; c'est aussi le nom d'un domaine des services de domaine Active Directory® (AD DS).
- **user1@example.com**. Dans cet exemple, le nom de domaine **example.com** est un suffixe ; et il s'agit d'un nom de domaine DNS ou du nom d'un domaine AD DS.

Vous pouvez utiliser des noms de domaine configurés dans les stratégies de demande de connexion lors de la conception et du déploiement de votre infrastructure RADIUS, et ce, afin de garantir le routage des demandes de connexion depuis les clients RADIUS, également appelés serveurs d'accès réseau, vers les serveurs RADIUS qui peuvent authentifier et autoriser la demande de connexion.

Lorsque le serveur NPS est configuré en tant que serveur RADIUS selon la stratégie de demande de connexion par défaut, le serveur NPS traite les demandes de connexion associées au domaine dont le serveur NPS est membre et aux domaines approuvés.

Pour configurer le serveur NPS en tant que proxy RADIUS et transférer les demandes de connexion vers des domaines non approuvés, vous devez créer une nouvelle stratégie de demande de connexion. Dans la nouvelle stratégie de demande de connexion, vous devez configurer l'attribut Nom d'utilisateur avec le nom de domaine qui sera compris dans l'attribut User-Name des demandes de connexion que vous souhaitez transférer. Vous devez également configurer la stratégie de demande de connexion avec un groupe de serveurs RADIUS distant.

La stratégie de demande de connexion permet au serveur NPS de calculer les demandes de connexion à transférer au groupe de serveurs RADIUS distant en fonction de la partie de domaine de l'attribut User-Name.

Acquisition du nom de domaine

La partie du nom de domaine du nom d'utilisateur est fournie lorsque l'utilisateur tape des informations d'identification basées sur un mot de passe lors d'une tentative de connexion, ou lorsqu'un profil de gestionnaire de connexions (CM) sur l'ordinateur de l'utilisateur est configuré pour fournir le nom de domaine automatiquement.

Vous pouvez indiquer que les utilisateurs de votre réseau fournissent leur nom de domaine lorsqu'ils tapent leurs informations d'identification lors des tentatives de connexion réseau.

Par exemple, vous pouvez demander aux utilisateurs de taper leur nom d'utilisateur, y compris le nom du compte d'utilisateur et le nom du domaine, dans **Nom d'utilisateur** dans la boîte de dialogue **Connexion** lors de la connexion par modem ou à un réseau privé virtuel (VPN).

En outre, si vous créez un package de numérotation personnalisé à l'aide du kit d'administration de gestionnaire de connexions (CMAK), vous pouvez aider les utilisateurs en ajoutant automatiquement le nom de domaine au nom du compte utilisateur dans les profils CM installés sur les ordinateurs des utilisateurs. Par exemple, vous pouvez spécifier un nom de domaine et une syntaxe de nom d'utilisateur dans le profil CM afin que l'utilisateur n'ait plus qu'à spécifier le nom du compte utilisateur lorsqu'il tape ses informations d'identification. L'utilisateur n'a donc pas besoin de connaître ou de mémoriser le domaine dans lequel son compte utilisateur se trouve.

Pendant le processus d'authentification, après que les utilisateurs ont tapé leurs informations d'identification basées sur un mot de passe, le nom d'utilisateur est transféré du client d'accès au serveur d'accès réseau. Le serveur d'accès réseau génère une demande de connexion et inclut le nom de domaine dans l'attribut RADIUS User-Name dans le message Access-Request envoyé au proxy ou au serveur RADIUS.

Si le serveur RADIUS est un serveur NPS, le message Access-Request est évalué et comparé au jeu de stratégies de demande de connexion configurées. Les conditions de la stratégie de demande de connexion peuvent inclure la spécification du contenu de l'attribut User-Name.

Vous pouvez configurer un jeu de stratégies de demande de connexion spécifiques au nom de domaine dans l'attribut User-Name des messages entrants. Cela vous permet de créer des règles de routage qui transfèrent des messages RADIUS présentant un nom de domaine spécifique à un jeu spécifique de serveurs RADIUS lorsque le serveur NPS est utilisé en tant que proxy RADIUS.

Règles de manipulation d’attribut

Avant que le message RADIUS soit traité localement (lorsque le serveur NPS est utilisé en tant que serveur RADIUS) ou transféré vers un autre serveur RADIUS (lorsque le serveur NPS est utilisé en tant que proxy RADIUS), l’attribut User-Name dans le message peut être modifié par des règles de manipulation d’attribut. Vous pouvez configurer des règles de manipulation d’attributs pour l’attribut User-Name en sélectionnant **Nom d’utilisateur** sous l’onglet **Conditions** dans les propriétés d’une stratégie de demande de connexion. Les règles de manipulation d’attribut NPS utilisent la syntaxe d’expression régulière.

> ⓘ **Notes**
>
> La manipulation de domaine ne fonctionne pas avec le protocole PEAP.
> Le comportement souhaité peut être obtenu en effectuant une commutation vers EAP-TLS ou EAP-MSCHAPv2 aux fins de l’authentification, ou **en ajoutant un suffixe UPN au domaine** pour chaque nom de domaine supplémentaire à résoudre.

Vous pouvez configurer des règles de manipulation d’attribut propres à l’attribut User-Name pour effectuer les opérations suivantes :

- supprimer le nom de domaine du nom d’utilisateur (ce processus est également appelé suppression de domaine). Par exemple, le nom d’utilisateur user1@example.com est remplacé par user1 ;
- modifier le nom de domaine, mais pas sa syntaxe. Par exemple, le nom d’utilisateur user1@example.com est remplacé par user1@wcoast.example.com ;
- modifier la syntaxe du nom de domaine. Par exemple, le nom d’utilisateur example\user1 est remplacé par user1@example.com.

Lorsque l’attribut User-Name a été modifié en fonction des règles de manipulation d’attribut configurées, des paramètres supplémentaires de la première stratégie de demande de connexion correspondante sont utilisés pour déterminer si :

- le serveur NPS traite le message Access-Request localement (lorsqu’il est utilisé en tant que serveur RADIUS) ;
- le serveur NPS transfère le message à un autre serveur RADIUS (lorsqu’il est utilisé en tant que proxy RADIUS).

Configuration du nom de domaine fourni par le serveur NPS

Lorsque le nom d'utilisateur ne contient pas de nom de domaine, le serveur NPS en fournit un. Par défaut, le nom de domaine fourni par le serveur NPS est le domaine dont ce dernier est membre. Vous pouvez spécifier le nom de domaine fourni par le serveur NPS par le biais du paramètre de registre suivant :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\PPP\ControlProtocols\B
uiltIn\
Name:  DefaultDomain
Type:  REG_SZ
Value: the FQDN for the domain, like test.contoso.com
```

> ⊗ **Attention**
>
> Une modification incorrecte du Registre peut sérieusement endommager votre système. Avant toute modification du registre, il est conseillé de sauvegarder toutes les données importantes de votre ordinateur.

Certains serveurs d'accès réseau non Microsoft suppriment ou modifient le nom de domaine spécifié par l'utilisateur. Par conséquent, la demande d'accès réseau est authentifiée auprès du domaine par défaut, qui n'est peut-être pas le domaine du compte de l'utilisateur. Pour résoudre ce problème, configurez vos serveurs RADIUS pour modifier le nom d'utilisateur selon le bon format et avec le nom de domaine précis.

Groupes de serveurs RADIUS distants

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Quand vous configurez un serveur NPS (Network Policy Server) comme proxy RADIUS (Remote Authentication Dial-In User Service), vous utilisez le serveur NPS pour transférer les demandes de connexion aux serveurs RADIUS qui sont capables de traiter les demandes de connexion, parce qu'ils peuvent effectuer l'authentification et l'autorisation dans le domaine où se trouve le compte d'utilisateur ou d'ordinateur. Par exemple, si vous souhaitez transférer des demandes de connexion à un ou plusieurs serveurs RADIUS dans des domaines non approuvés, vous pouvez configurer le serveur NPS comme proxy RADIUS pour transférer les demandes aux serveurs RADIUS distants dans le domaine non approuvé.

> ⓘ **Notes**
>
> Les groupes de serveurs RADIUS distants ne sont pas liés aux groupes Windows et en sont séparés.

Pour configurer un serveur NPS comme proxy RADIUS, vous devez créer une stratégie de demande de connexion qui contient toutes les informations nécessaires pour que le serveur NPS évalue les messages à transférer et où les envoyer.

Quand vous configurez un groupe de serveurs RADIUS distants dans un serveur NPS et que vous configurez une stratégie de demande de connexion avec le groupe, vous désignez l'emplacement où le serveur NPS doit transférer les demandes de connexion.

Configuration de serveurs RADIUS pour un groupe

Un groupe de serveurs RADIUS distants est un groupe nommé qui contient un ou plusieurs serveurs RADIUS. Si vous configurez plusieurs serveurs, vous pouvez spécifier des paramètres d'équilibrage de charge pour déterminer l'ordre dans lequel les serveurs sont utilisés par le proxy, ou pour distribuer le flux de messages RADIUS sur tous les serveurs du groupe afin d'éviter de surcharger un ou plusieurs serveurs avec trop de demandes de connexion.

Chaque serveur du groupe a les paramètres suivants.

- **Nom ou adresse**. Chaque membre du groupe doit avoir un nom unique au sein du groupe. Le nom peut être une adresse IP ou un nom pouvant être résolu en son adresse IP.

- **Gestion des comptes et authentification**. Vous pouvez transférer des demandes d'authentification, des demandes de gestion des comptes ou les deux à chaque membre du groupe de serveurs RADIUS distants.

- **Équilibrage de charge**. Un paramètre de priorité est utilisé pour indiquer le membre du groupe qui est le serveur principal (la priorité est définie sur 1). Pour les membres du groupe qui ont la même priorité, un paramètre de pondération est utilisé pour calculer la fréquence à laquelle les messages RADIUS sont envoyés à chaque serveur. Vous pouvez utiliser des paramètres supplémentaires pour configurer la façon dont le serveur NPS détecte quand un membre du groupe est indisponible pour la première fois, et quand il redevient disponible après avoir été indisponible.

Une fois que vous avez configuré un groupe de serveurs RADIUS distants, vous pouvez spécifier le groupe dans les paramètres d'authentification et de gestion des comptes d'une stratégie de demande de connexion. Pour cette raison, vous pouvez commencer par configurer un groupe de serveurs RADIUS distants. Ensuite, vous pouvez configurer la stratégie de demande de connexion afin d'utiliser le groupe de serveurs RADIUS distants nouvellement configuré. Vous pouvez également utiliser l'Assistant Nouvelle stratégie de demande de connexion pour créer un groupe de serveurs RADIUS distants pendant que vous créez une stratégie de demande de connexion.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Stratégies réseau

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour obtenir une vue d'ensemble des stratégies réseau dans le serveur NPS.

> ⓘ **Notes**
>
> Outre cette rubrique, la documentation de stratégie réseau suivante est également disponible.
>
> - Autorisation d'accès
> - Configurer des stratégies réseau

Les stratégies réseau sont des ensembles de conditions, de contraintes et de paramètres qui vous permettent de désigner les personnes autorisées à se connecter au réseau et les circonstances dans lesquelles elles peuvent ou ne peuvent pas se connecter.

Lors du traitement des demandes de connexion en tant que serveur RADIUS (Remote Authentication Dial-In User Service), le serveur NPS effectue à la fois l'authentification et l'autorisation pour la demande de connexion. Pendant le processus d'authentification, le serveur NPS vérifie l'identité de l'utilisateur ou de l'ordinateur qui se connecte au réseau. Pendant le processus d'autorisation, le serveur NPS détermine si l'utilisateur ou l'ordinateur est autorisé à accéder au réseau.

Pour effectuer ces déterminations, le serveur NPS utilise des stratégies réseau configurées dans la console de serveur NPS. Le serveur NPS examine également les propriétés de numérotation du compte d'utilisateur dans Active Directory® Domain Services (AD DS) pour effectuer l'autorisation.

Stratégies réseau - Un ensemble ordonné de règles

Les stratégies réseau peuvent être considérées en tant que règles. Chaque règle dispose d'un ensemble de conditions et de paramètres. Le serveur NPS compare les conditions de la règle aux propriétés des demandes de connexion. Si une correspondance se produit entre la règle et la demande de connexion, les paramètres définis dans la règle sont appliqués à la connexion.

Lorsque plusieurs stratégies réseau sont configurées dans le serveur NPS, il s'agit d'un ensemble ordonné de règles. Le serveur NPS vérifie chaque demande de connexion par

rapport à la première règle de la liste, puis par rapport à la deuxième, et ainsi de suite, jusqu'à ce qu'une correspondance soit trouvée.

Chaque stratégie réseau a un paramètre **d'état** de stratégie qui vous permet d'activer ou de désactiver la stratégie. Lorsque vous désactivez une stratégie réseau, le serveur NPS n'évalue pas la stratégie lors de l'autorisation des demandes de connexion.

> ⓘ **Notes**
>
> Si vous souhaitez que NPS évalue une stratégie réseau lors de l'exécution d'une autorisation pour les demandes de connexion, vous devez configurer le paramètre **d'état** de la stratégie en sélectionnant la case à cocher Stratégie activée.

Propriétés de stratégie réseau

Il existe quatre catégories de propriétés pour chaque stratégie réseau :

Overview

Ces propriétés vous permettent de spécifier si la stratégie est activée, si la stratégie accorde ou refuse l'accès et si une méthode de connexion réseau spécifique ou un type de serveur d'accès réseau (NAS) sont requis pour les demandes de connexion. Les propriétés de vue d'ensemble vous permettent également de spécifier si les propriétés de numérotation des comptes d'utilisateur sont ignorées dans AD DS. Si vous sélectionnez cette option, seuls les paramètres de la stratégie réseau sont utilisés par le serveur NPS pour déterminer si la connexion est autorisée.

Conditions

Ces propriétés vous permettent de spécifier les conditions que la demande de connexion doit avoir pour correspondre à la stratégie réseau ; si les conditions configurées dans la stratégie correspondent à la demande de connexion, le serveur NPS applique les paramètres désignés dans la stratégie réseau à la connexion. Par exemple, si vous spécifiez l'adresse IPv4 du serveur d'accès au réseau (adresse IPv4 NAS) comme condition de la stratégie réseau et que le serveur NPS reçoit une demande de connexion à partir d'un NAS qui a l'adresse IP spécifiée, la condition dans la stratégie correspond à la demande de connexion.

Constraints

Les contraintes sont des paramètres supplémentaires de la stratégie réseau qui sont requis pour correspondre à la demande de connexion. Si une contrainte n'est pas mise en correspondance par la demande de connexion, le serveur NPS rejette automatiquement la demande. Contrairement à la réponse du serveur NPS à des conditions sans correspondance dans la stratégie réseau, si une contrainte n'est pas correspondante, le serveur NPS refuse la demande de connexion sans évaluer les stratégies réseau supplémentaires.

Settings

Ces propriétés vous permettent de spécifier les paramètres que le serveur NPS applique à la demande de connexion, si toutes les conditions de stratégie réseau de la stratégie correspondent.

Lorsque vous ajoutez une nouvelle stratégie réseau à l'aide de la console de serveur NPS, vous devez utiliser l'Assistant de Nouvelle stratégie réseau. Après avoir créé une stratégie réseau à l'aide de l'Assistant, vous pouvez la personnaliser en double-cliquant sur la stratégie dans la console de serveur NPS pour obtenir les propriétés de la stratégie.

Pour obtenir des exemples de syntaxe de correspondance de modèle, afin de spécifier des attributs de stratégie réseau, consultez Utiliser des expressions régulières dans le serveur NPS.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Access Permission

30/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Access permission is configured on the **Overview** tab of each network policy in Network Policy Server (NPS).

Ce paramètre vous permet de configurer la stratégie pour accorder ou refuser l'accès aux utilisateurs si les conditions et les contraintes de la stratégie réseau sont mises en correspondance par la demande de connexion.

Les paramètres d'autorisation d'accès ont l'effet suivant :

- **Grant access**. L'accès est accordé si la demande de connexion correspond aux conditions et contraintes configurées dans la stratégie.
- **Deny access**. L'accès est refusé si la demande de connexion correspond aux conditions et contraintes configurées dans la stratégie.

L'autorisation d'accès est également accordée ou refusée en fonction de votre configuration des propriétés rendez-vous de chaque compte d'utilisateur.

> ⓘ **Notes**
>
> Les comptes d'utilisateur et leurs propriétés, telles que les propriétés d'accès rendez-vous, sont configurés dans le Utilisateurs et ordinateurs Active Directory ou le composant logiciel enfichable Microsoft Management Console (MMC) Utilisateurs et groupes locaux, selon que les services de domaine Active Directory® (AD DS) sont installés ou non.

Le paramètre de compte d'utilisateur **Autorisation d'accès réseau**, qui est configuré sur les propriétés rendez-vous des comptes d'utilisateur, remplace le paramètre d'autorisation d'accès à la stratégie réseau. Lorsque l'autorisation d'accès réseau sur un compte d'utilisateur est définie sur l'option **Contrôler l'accès via la stratégie réseau NPS**, le paramètre d'autorisation d'accès à la stratégie réseau détermine si l'accès à l'utilisateur est accordé ou refusé.

> ⓘ **Notes**
>
> Dans Windows Server 2016, la valeur par défaut de **l'autorisation d'accès réseau** dans les propriétés de numérotation du compte d'utilisateur AD DS est **Contrôler l'accès via la stratégie réseau NPS**.

Lorsque NPS évalue les demandes de connexion par rapport aux stratégies réseau configurées, il effectue les actions suivantes :

- Si les conditions de la première stratégie ne sont pas réunies, NPS évalue la stratégie suivante et continue ce processus jusqu'à ce qu'une correspondance soit trouvée ou que toutes les stratégies aient été évaluées pour une correspondance.
- Si les conditions et les contraintes d'une stratégie sont réunies, NPS accorde ou refuse l'accès, en fonction de la valeur du paramètre Autorisation d'accès dans la stratégie.
- Si les conditions d'une stratégie correspondent mais que les contraintes de la stratégie ne correspondent pas, NPS rejette la demande de connexion.
- Si les conditions de toutes les stratégies ne correspondent pas, NPS rejette la demande de connexion.

Ignorer les propriétés de numérotation du compte d'utilisateur

Vous pouvez configurer la stratégie réseau NPS pour ignorer les propriétés d'accès rendez-vous des comptes d'utilisateur en activant ou en désactivant la case à cocher **Ignorer les propriétés de numérotation des comptes d'utilisateur** sous l'onglet **Vue d'ensemble** d'une stratégie réseau.

Normalement, lorsque NPS effectue l'autorisation d'une demande de connexion, il vérifie les propriétés rendez-vous du compte d'utilisateur, où la valeur du paramètre d'autorisation d'accès réseau peut affecter si l'utilisateur est autorisé à se connecter au réseau. Lorsque vous configurez NPS pour ignorer les propriétés rendez-vous des comptes d'utilisateur pendant l'autorisation, les paramètres de stratégie réseau déterminent si l'utilisateur a accès au réseau.

Les propriétés rendez-vous des comptes d'utilisateur contiennent les éléments suivants :

- Autorisation d'accès réseau
- Caller-ID
- Callback options
- Adresse IP statique
- Static routes

Pour prendre en charge plusieurs types de connexions pour lesquelles NPS fournit l'authentification et l'autorisation, il peut être nécessaire de désactiver le traitement des propriétés de connexion de compte d'utilisateur. Cela peut être effectué pour prendre en charge les scénarios dans lesquels des propriétés d'accès rendez-vous spécifiques ne sont pas requises.

Par exemple, les propriétés d'ID de l'appelant, de rappel, d'adresse IP statique et d'itinéraires statiques sont conçues pour un client qui compose un serveur d'accès réseau (NAS), et non pour les clients qui se connectent à des points d'accès sans fil. Un point d'accès sans fil qui reçoit ces paramètres dans un message RADIUS de NPS peut ne pas être en mesure de les traiter, ce qui peut entraîner la déconnexion du client sans fil.

Lorsque NPS fournit l'authentification et l'autorisation aux utilisateurs qui composent et accèdent au réseau de votre organisation via des points d'accès sans fil, vous devez configurer les propriétés d'accès rendez-vous pour prendre en charge les connexions rendez-vous (en définissant les propriétés de numérotation) ou les connexions sans fil (en ne définissant pas les propriétés de numérotation).

Vous pouvez utiliser NPS pour activer le traitement des propriétés rendez-vous pour le compte d'utilisateur dans certains scénarios (par exemple, rendez-vous) et pour désactiver le traitement des propriétés rendez-vous dans d'autres scénarios (par exemple, sans fil 802.1X et commutateur d'authentification).

Vous pouvez également utiliser **Ignorer les propriétés rendez-vous du compte d'utilisateur** pour gérer le contrôle d'accès réseau via des groupes et le paramètre d'autorisation d'accès sur la stratégie réseau. Lorsque vous activez la case à cocher **Ignorer les propriétés rendez-vous du compte d'utilisateur**, l'autorisation d'accès réseau sur le compte d'utilisateur est ignorée.

Le seul inconvénient de cette configuration est que vous ne pouvez pas utiliser les propriétés de numérotation de compte d'utilisateur supplémentaires de l'ID de l'appelant, du rappel, de l'adresse IP statique et des itinéraires statiques.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Modèles NPS

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Les modèles NPS (Network Policy Server) vous permettent de créer des éléments de configuration, comme des clients RADIUS (Remote Authentication Dial-In User Service) ou des secrets partagés, que vous pouvez réutiliser sur le serveur NPS local et exporter pour une utilisation sur d'autres serveurs NPS.

Les modèles NPS sont conçus pour réduire le temps et le coût nécessaires pour configurer NPS sur un ou plusieurs serveurs. Les types de modèles NPS suivants peuvent être configurés dans Gestion des modèles :

- Secrets partagés
- RADIUS Clients
- Serveurs RADIUS distants
- Filtres IP
- Groupe de serveurs de mise à jour

La configuration d'un modèle diffère de la configuration directe du serveur NPS. La création d'un modèle n'affecte pas la fonctionnalité du serveur NPS. C'est seulement quand vous sélectionnez le modèle à l'emplacement approprié dans la console NPS que le modèle affecte la fonctionnalité NPS.

Par exemple, si vous configurez un client RADIUS dans la console NPS sous Clients et serveurs RADIUS, vous modifiez la configuration NPS pour que le serveur NPS communique avec un de vos serveurs d'accès réseau (NAS). (L'étape suivante consiste à configurer le NAS pour communiquer avec NPS.) Toutefois, si vous configurez un nouveau modèle de clients RADIUS dans la console NPS sous **Gestion des** modèles plutôt que de créer un client **RADIUS sous Clients et serveurs RADIUS**, vous avez créé un modèle, mais vous n'avez pas encore modifié la fonctionnalité NPS. Pour modifier la fonctionnalité NPS, vous devez sélectionner le modèle à l'emplacement approprié dans la console NPS.

Création de modèles

Pour créer un modèle, ouvrez la console NPS, cliquez avec le bouton droit sur un type de modèle, tel que **filtres IP**, puis cliquez sur **Nouveau**. Une nouvelle boîte de dialogue de propriétés de modèle s'ouvre, où vous pouvez configurer votre modèle.

Utilisation de modèles localement

Vous pouvez utiliser un modèle que vous avez créé dans **Gestion des modèles** en accédant à un emplacement dans la console NPS où le modèle peut être appliqué. Par exemple, si vous créez un modèle Secrets partagés que vous voulez appliquer à une configuration de client RADIUS, dans **Clients et serveurs RADIUS** et **Clients RADIUS**, ouvrez les propriétés du client RADIUS. Dans **Sélectionner un modèle Secrets partagés existant**, sélectionnez le modèle que vous avez créé précédemment dans la liste des modèles disponibles.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Clients RADIUS

Article • 09/03/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Un serveur d’accès réseau (NAS) est un appareil qui fournit un certain niveau d’accès à un réseau plus grand. Un NAS utilisant une infrastructure RADIUS est également un client RADIUS, qui envoie des demandes de connexion et des messages de gestion des comptes à un serveur RADIUS pour l’authentification, l’autorisation et la gestion des comptes.

Notes

Les ordinateurs clients, comme les ordinateurs portables et autres ordinateurs exécutant des systèmes d’exploitation clients, ne sont pas des clients RADIUS. Les clients RADIUS sont des serveurs d’accès réseau (par exemple, des points d’accès sans fil, des commutateurs d’authentification 802.1X, des serveurs de réseau privé virtuel (VPN) et des serveurs d’accès à distance), car ils utilisent le protocole RADIUS pour communiquer avec des serveurs RADIUS, comme les serveurs NPS (Network Policy Server).

Pour déployer un serveur NPS comme serveur RADIUS ou proxy RADIUS, vous devez configurer des clients RADIUS dans le serveur NPS.

Exemples de client RADIUS

Voici des exemples de serveurs d’accès réseau :

- Serveurs d’accès réseau qui fournissent une connectivité d’accès à distance à un réseau d’organisation ou à Internet. Par exemple, un ordinateur exécutant le système d’exploitation Windows Server 2016 et le service d’accès à distance qui fournit des services d’accès à distance traditionnels ou de réseau privé virtuel (VPN) à un intranet d’organisation.
- Points d’accès sans fil qui fournissent un accès de couche physique à un réseau d’organisation en utilisant des technologies de transmission et de réception sans fil.
- Commutateurs qui fournissent un accès de couche physique au réseau d’une organisation, en utilisant des technologies LAN traditionnelles, comme Ethernet.

- Proxys RADIUS qui transfèrent les demandes de connexion aux serveurs RADIUS membres d'un groupe de serveurs RADIUS distants configuré sur le proxy RADIUS.

Messages Access-Request (demande d'accès) RADIUS

Les clients RADIUS créent des messages Access-Request RADIUS et les transfèrent à un proxy RADIUS ou à un serveur RADIUS, ou transfèrent à un serveur RADIUS les messages Access-Request qu'ils ont reçus d'un autre client RADIUS, mais qu'ils n'ont pas créés eux-mêmes.

Les clients RADIUS ne traitent pas les messages Access-Request en effectuant l'authentification, l'autorisation et la gestion des comptes. Seuls les serveurs RADIUS ont ces fonctions.

Le serveur NPS, toutefois, peut être configuré comme proxy RADIUS et serveur RADIUS simultanément, afin de traiter certains messages Access-Request et transférer d'autres messages.

Serveur NPS comme client RADIUS

Le serveur NPS agit comme un client RADIUS quand vous le configurez comme proxy RADIUS pour transférer les messages Access-Request à d'autres serveurs RADIUS à des fins de traitement. Quand vous utilisez le serveur NPS comme proxy RADIUS, les étapes de configuration générales suivantes sont nécessaires :

1. Les serveurs d'accès réseau, comme les points d'accès sans fil et les serveurs VPN, sont configurés avec l'adresse IP du proxy NPS comme serveur RADIUS ou serveur d'authentification désigné. Cela permet aux serveurs d'accès réseau, qui créent les messages Access-Request en fonction des informations qu'ils reçoivent des clients d'accès, de transférer les messages au proxy NPS.

2. Le proxy NPS est configuré en ajoutant chaque serveur d'accès réseau comme client RADIUS. Cette étape de configuration permet au proxy NPS de recevoir des messages des serveurs d'accès réseau et de communiquer avec eux pendant l'authentification. Par ailleurs, les stratégies de demande de connexion sur le proxy NPS sont configurées pour spécifier les messages Access-Request à transférer à un ou plusieurs serveurs RADIUS. Ces stratégies sont également configurées avec un groupe de serveurs RADIUS distants, qui indique au serveur NPS où envoyer les messages qu'il reçoit des serveurs d'accès réseau.

3. Le serveur NPS ou d'autres serveurs RADIUS qui sont membres du groupe de serveurs RADIUS distants sur le proxy NPS sont configurés pour recevoir des messages du proxy NPS. Pour ce faire, configurez le proxy NPS comme client RADIUS.

Propriétés du client RADIUS

Quand vous ajoutez un client RADIUS à la configuration NPS dans la console NPS ou en utilisant les commandes netsh pour NPS ou les commandes Windows PowerShell, vous configurez le serveur NPS pour recevoir des messages Access-Request RADIUS d'un serveur d'accès réseau ou d'un proxy RADIUS.

Quand vous configurez un client RADIUS dans le serveur NPS, vous pouvez désigner les propriétés suivantes :

Nom du client

Nom convivial pour le client RADIUS, qui facilite l'identification en cas d'utilisation du composant logiciel enfichable NPS ou des commandes netsh pour NPS.

Adresse IP

Adresse IPv4 (Internet Protocol version 4) ou nom DNS (Domain Name System) du client RADIUS.

Client-Vendor

Fournisseur du client RADIUS. Sinon, vous pouvez utiliser la valeur standard RADIUS pour Client-Vendor.

Secret partagé

Chaîne de texte utilisée comme mot de passe entre les clients RADIUS, les serveurs RADIUS et les proxys RADIUS. Quand l'attribut Message Authenticator est utilisé, le secret partagé est également utilisé comme clé pour chiffrer les messages RADIUS. Cette chaîne doit être configurée sur le client RADIUS et dans le composant logiciel enfichable NPS.

Attribut Message Authenticator

Décrit dans RFC 2869, « Extensions RADIUS », hachage MD5 (Message Digest 5) de l'ensemble du message RADIUS. Si l'attribut RADIUS Message Authenticator est présent, il est vérifié. Si la vérification échoue, le message RADIUS est ignoré. Si les paramètres de client nécessitent l'attribut Message Authenticator et qu'il n'est pas présent, le message RADIUS est ignoré. L'utilisation de l'attribut Message Authenticator est recommandée.

> ⓘ **Notes**
>
> L'attribut Message Authenticator est nécessaire et activé par défaut quand vous utilisez l'authentification EAP (Extensible Authentication Protocol).

Pour plus d'informations sur le serveur NPS, consultez Serveur NPS (Network Policy Server).

Planifier un serveur NPS (Network Policy Server)

31/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cette rubrique fournit des liens à des informations sur la planification des déploiements NPS et proxy.

> ⓘ **Notes**
>
> Pour obtenir des informations supplémentaire sur le serveur NPS, vous pouvez utiliser les sections de bibliothèque suivantes.
>
> - Prise en main du serveur NPS
> - Déployer un serveur NPS (Network Policy Server)
> - Gérer un serveur NPS (Network Policy Server)

Cette section comprend les rubriques suivantes.

- Planifier un serveur NPS en tant que serveur RADIUS
- Planifier un serveur NPS en tant que proxy RADIUS

Planifier un serveur NPS en tant que serveur RADIUS

Article • 11/03/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local, versions 23H2 and 22H2

Lorsque vous déployez un serveur NPS (Network Policy Server) en tant que serveur RADIUS (Remote Authentication Dial-In User Service), NPS effectue l'authentification, l'autorisation et la gestion des comptes pour les demandes de connexion pour le domaine local et pour les domaines qui approuvent le domaine local. Vous pouvez utiliser ces instructions de planification pour simplifier votre déploiement RADIUS.

Ces instructions de planification n'incluent pas les circonstances dans lesquelles vous souhaitez déployer NPS en tant que proxy RADIUS. Lorsque vous déployez NPS en tant que proxy RADIUS, NPS transfère les demandes de connexion à un serveur exécutant NPS ou à d'autres serveurs RADIUS dans des domaines distants, des domaines non approuvés, ou les deux.

Avant de déployer NPS en tant que serveur RADIUS sur votre réseau, suivez les instructions suivantes pour planifier votre déploiement.

- Planifiez la configuration NPS.
- Planifiez les clients RADIUS.
- Planifiez l'utilisation des méthodes d'authentification.
- Planifiez les stratégies réseau.
- Planifier la gestion des comptes de serveur NPS.

Planifiez la configuration NPS.

Vous devez décider du domaine dans lequel le serveur NPS est membre. Pour les environnements à plusieurs domaines, un serveur NPS peut authentifier les informations d'identification des comptes d'utilisateur dans le domaine dont il est membre et pour tous les domaines qui approuvent le domaine local du serveur NPS. Pour permettre au serveur NPS de lire les propriétés d'accès au réseau des comptes d'utilisateur pendant le processus d'autorisation, veuillez ajouter le compte d'ordinateur du serveur NPS au groupe RAS et NPS pour chaque domaine.

Une fois que vous avez déterminé l'appartenance au domaine du serveur NPS, le serveur doit être configuré pour communiquer avec les clients RADIUS, également appelés serveurs d'accès réseau, à l'aide du protocole RADIUS. En outre, vous pouvez configurer les types d'événements enregistrés par NPS dans le journal des événements et entrer une description pour le serveur.

Étapes clés

Pendant la planification de la configuration du serveur NPS, vous pouvez utiliser les étapes suivantes.

- Déterminez les ports RADIUS que le serveur NPS utilise pour recevoir les messages RADIUS des clients RADIUS. Les ports UDP par défaut sont 1812 et 1645 pour les messages d'authentification RADIUS et les ports 1813 et 1646 pour les messages de comptabilité RADIUS.
- Si le serveur NPS est configuré avec plusieurs cartes réseau, déterminez les cartes sur lesquelles vous souhaitez autoriser le trafic RADIUS.
- Déterminez les types d'événements que vous souhaitez que NPS enregistre dans le journal des événements. Vous pouvez consigner les demandes d'authentification rejetées, les demandes d'authentification réussies ou les deux types de demandes.
- Déterminez si vous déployez plusieurs serveurs NPS. Pour fournir une tolérance de panne pour l'authentification et la gestion des comptes basées sur RADIUS, utilisez au moins deux serveurs NPS. Un serveur NPS est utilisé comme serveur RADIUS principal et l'autre est utilisé comme sauvegarde. Chaque client RADIUS est ensuite configuré sur les deux serveurs NPS. Si le serveur NPS principal devient indisponible, les clients RADIUS envoient des messages Access-Request au serveur NPS de remplacement.
- Planifiez le script utilisé pour copier une configuration NPS vers d'autres serveurs NPS pour économiser sur la surcharge administrative et empêcher la configuration incorrecte d'un serveur. NPS fournit les commandes `Netsh` qui vous permettent de copier tout ou partie d'une configuration NPS à importer sur un autre serveur NPS. Vous pouvez exécuter les commandes manuellement dans l'invite `Netsh`. Toutefois, si vous enregistrez votre séquence de commandes en tant que script, vous pouvez exécuter le script à une date ultérieure si vous décidez de modifier vos configurations de serveur.

Planifiez les clients RADIUS

Les clients RADIUS sont des serveurs d'accès réseau, tels que des points d'accès sans fil, des serveurs de réseau privé virtuel (VPN), des commutateurs compatibles 802.1X et des serveurs d'accès à distance. Les proxy RADIUS, qui transfèrent les messages de demande de connexion aux serveurs RADIUS, sont également des clients RADIUS. Le serveur NPS prend en charge tous les serveurs d'accès réseau et les proxys RADIUS conformes au protocole RADIUS, comme décrit dans RFC 2865, « Service RADIUS (Remote Authentication Dial-in User Service) » et RFC 2866, « Radius Accounting ».

> ⓘ **Important**
>
> Les clients d'accès, tels que les ordinateurs clients, ne sont pas des clients RADIUS. Seuls les serveurs d'accès réseau et les serveurs proxy qui prennent en charge le protocole RADIUS sont des clients RADIUS.

En outre, les points d'accès sans fil et les commutateurs doivent être capables d'authentification 802.1X. Si vous souhaitez déployer le protocole EAP (Extensible Authentication Protocol) ou le protocole PEAP (Protected Extensible Authentication Protocol), les points d'accès et les commutateurs doivent prendre en charge l'utilisation d'EAP.

Pour tester l'interopérabilité de base des connexions PPP pour les points d'accès sans fil, configurez le point d'accès et le client d'accès pour utiliser le protocole PAP (Password Authentication Protocol). Utilisez des protocoles d'authentification PPP supplémentaires, tels que PEAP, jusqu'à ce que vous ayez testé ceux que vous envisagez d'utiliser pour l'accès réseau.

Étapes clés

Pendant la planification des clients RADIUS, vous pouvez effectuer les étapes suivantes.

- Documentez les attributs spécifiques au fournisseur (VSA) que vous devez configurer dans le serveur NPS. Si vos serveurs d'accès réseau nécessitent des VSA, journalisez les informations VSA pour une utilisation ultérieure lorsque vous configurez vos stratégies réseau dans le serveur NPS.

- Documentez les adresses IP des clients RADIUS et votre serveur NPS pour simplifier la configuration de tous les appareils. Lorsque vous déployez vos clients RADIUS, vous devez les configurer pour qu'ils utilisent le protocole RADIUS, avec l'adresse IP NPS entrée comme serveur d'authentification. Lorsque vous configurez NPS pour communiquer avec vos clients RADIUS, vous devez entrer les adresses IP du client RADIUS dans le module complémentaire NPS.

- Créez des secrets partagés pour la configuration sur les clients RADIUS et dans le composant logiciel enfichable du serveur NPS. Vous devez configurer des clients du protocole RADIUS avec un secret partagé ou un mot de passe, que vous saisirez également dans le composant logiciel enfichable NPS lorsque vous configurez les clients RADIUS dans ce dernier.

Planifiez l'utilisation des méthodes d'authentification.

Le serveur NPS prend en charge les méthodes d'authentification par mot de passe et par certificat. Toutefois, tous les serveurs d'accès réseau ne prennent pas en charge les mêmes méthodes d'authentification. Dans certains cas, vous pouvez déployer une méthode d'authentification différente en fonction du type d'accès réseau.

Par exemple, vous pourriez souhaiter déployer à la fois l'accès sans fil et l'accès VPN pour votre organisation, mais vous utilisez une méthode d'authentification différente pour chaque type d'accès : EAP-TLS pour les connexions VPN, en raison de la sécurité renforcée que fournit EAP avec Transport Layer Security (EAP-TLS) et PEAP-MS-CHAP v2 pour les connexions sans fil 802.1X.

PEAP avec Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2) fournit une fonctionnalité nommée reconnect rapide conçue pour être utilisée avec des ordinateurs portables et d'autres appareils sans fil. La reconnexion rapide permet aux clients sans fil de se déplacer entre des points d'accès sans fil sur le même réseau sans être ré-authentifiés chaque fois qu'ils sont associés à un nouveau point d'accès. Cela offre une meilleure expérience aux utilisateurs sans fil et leur permet de se déplacer d'un point d'accès à l'autre sans avoir à ressaisir leurs informations d'identification. En raison de la reconnexion rapide et de la sécurité que fournit PEAP-MS-CHAP v2, PEAP-MS-CHAP v2 est un choix logique en tant que méthode d'authentification pour les connexions sans fil.

Pour les connexions VPN, EAP-TLS est une méthode d'authentification basée sur des certificats qui fournit une sécurité forte qui protège le trafic réseau, même s'il est transmis sur Internet à partir d'ordinateurs domestiques ou mobiles vers vos serveurs VPN d'organisation.

Méthodes d'authentification basée sur un certificat

Les méthodes d'authentification basées sur les certificats présentent l'avantage d'offrir une sécurité forte et l'inconvénient d'être plus difficiles à déployer que les méthodes d'authentification par mot de passe.

PeAP-MS-CHAP v2 et EAP-TLS sont des méthodes d'authentification basées sur des certificats, mais il existe de nombreuses différences entre elles et la façon dont elles sont déployées.

EAP-TLS

EAP-TLS utilise des certificats pour l'authentification client et serveur, et vous oblige à déployer une infrastructure à clé publique (PKI) dans votre organisation. Le déploiement d'une infrastructure à clé publique peut être complexe et nécessite une phase de planification indépendante de la planification de l'utilisation de NPS en tant que serveur RADIUS.

Avec EAP-TLS, le serveur NPS inscrit un certificat de serveur auprès d'une autorité de certification et le certificat est enregistré sur l'ordinateur local dans le magasin de certificats. Pendant le processus d'authentification, l'authentification du serveur se produit lorsque le serveur NPS envoie son certificat de serveur au client d'accès pour prouver son identité au client d'accès. Le client d'accès examine différentes propriétés de certificat pour déterminer si le certificat est valide et approprié pour une utilisation lors de l'authentification du serveur. Si le certificat de serveur répond aux exigences minimales du certificat de serveur et est émis par une autorité de certification approuvée par le client d'accès, le serveur NPS est correctement authentifié par le client.

De même, l'authentification du client se produit pendant le processus d'authentification lorsque le client envoie son certificat client au serveur NPS pour prouver son identité au serveur NPS. Le serveur NPS examine le certificat et, si le certificat client répond aux exigences minimales du certificat client et est émis par une autorité de certification approuvée par le serveur NPS, le client d'accès est correctement authentifié par le serveur NPS.

Bien qu'il soit nécessaire que le certificat de serveur soit stocké dans le magasin de certificats sur le serveur NPS, le certificat client ou utilisateur peut être stocké dans le magasin de certificats sur le client ou sur une carte à puce.

Pour que ce processus d'authentification réussisse, il est nécessaire que tous les ordinateurs disposent du certificat d'autorité de certification de votre organisation dans le magasin de certificats des autorités de certification racines approuvées pour l'ordinateur local et l'utilisateur actuel.

PEAP-MS-CHAP v2

La méthode PEAP-MS-CHAP v2 utilise un certificat pour l'authentification du serveur et des informations d'identification basées sur un mot de passe pour l'authentification

utilisateur. Étant donné que les certificats sont utilisés uniquement pour l'authentification du serveur, vous n'êtes pas obligé de déployer une infrastructure à clé publique pour utiliser PEAP-MS-CHAP v2. Lorsque vous déployez PEAP-MS-CHAP v2, vous pouvez obtenir un certificat de serveur pour le serveur NPS de l'une des deux manières suivantes :

- Vous pouvez installer les services de certificats Active Directory (AD CS), puis inscrire automatiquement des certificats auprès des serveurs NPS. Si vous utilisez cette méthode, vous devez également inscrire le certificat d'autorité de certification sur les ordinateurs clients qui se connectent à votre réseau afin qu'ils approuvent le certificat émis pour le serveur NPS.

- Vous pouvez acheter un certificat de serveur auprès d'une autorité de certification publique telle que VeriSign. Si vous utilisez cette méthode, veillez à sélectionner une autorité de certification déjà approuvée par les ordinateurs clients. Pour déterminer si les ordinateurs clients approuvent une autorité de certification, ouvrez le composant logiciel enfichable Microsoft Management Console (MMC) Certificats sur un ordinateur client, puis affichez le magasin Autorités de certification racines approuvées pour l'ordinateur local et pour l'utilisateur actuel. S'il existe un certificat de l'autorité de certification dans ces magasins de certificats, l'ordinateur client approuve l'autorité de certification et approuve donc tout certificat émis par l'autorité de certification.

Pendant le processus d'authentification avec la méthode PEAP-MS-CHAP v2, l'authentification du serveur se produit lorsque le serveur NPS envoie son certificat de serveur à l'ordinateur client. Le client d'accès examine différentes propriétés de certificat pour déterminer si le certificat est valide et approprié pour une utilisation lors de l'authentification du serveur. Si le certificat de serveur répond aux exigences minimales du certificat de serveur et est émis par une autorité de certification approuvée par le client d'accès, le serveur NPS est correctement authentifié par le client.

L'authentification utilisateur se produit lorsqu'un utilisateur tente de se connecter au réseau entre des informations d'identification basées sur un mot de passe et tente de se connecter. Le serveur NPS reçoit les informations d'identification et effectue l'authentification et l'autorisation. Si l'utilisateur est authentifié et autorisé avec succès, et si l'ordinateur client a correctement authentifié le serveur NPS, la demande de connexion est accordée.

Étapes clés

Pendant la planification de l'utilisation des méthodes d'authentification, vous pouvez effectuer les étapes suivantes.

- Identifiez les types d’accès réseau que vous envisagez d’offrir, tels que la connexion sans fil, le VPN, le commutateur compatible 802.1X et l’accès à distance.
- Déterminez la ou les méthodes d’authentification que vous souhaitez utiliser pour chaque type d’accès. Il est recommandé d’utiliser les méthodes d’authentification basées sur des certificats qui fournissent une sécurité forte ; Toutefois, il peut ne pas être pratique de déployer une infrastructure à clé publique, de sorte que d’autres méthodes d’authentification peuvent fournir un meilleur équilibre entre ce dont vous avez besoin pour votre réseau.
- Si vous déployez EAP-TLS, planifiez votre déploiement PKI. Cela inclut la planification des modèles de certificats que vous allez utiliser pour les certificats de serveur et les certificats d’ordinateur client. Cela comprend également de déterminer l’inscription des certificats sur les ordinateurs membres et non membres du domaine, et déterminer si vous souhaitez utiliser des cartes à puce.
- Si vous déployez PEAP-MS-CHAP v2, déterminez si vous souhaitez installer AD CS pour émettre des certificats de serveur sur vos serveurs NPS ou si vous souhaitez acheter des certificats de serveur auprès d’une autorité de certification publique, par exemple VeriSign.

Planifiez les stratégies réseau

Les stratégies réseau sont utilisées par le serveur NPS pour déterminer si les demandes de connexion reçues des clients RADIUS sont autorisées. Le serveur NPS utilise également les propriétés de connexion du compte d'utilisateur pour prendre une décision d'autorisation.

Étant donné que les stratégies réseau sont traitées dans l’ordre dans lequel elles apparaissent dans le composant logiciel enfichable de serveur NPS, prévoyez de placer vos stratégies les plus restrictives en premier dans la liste des stratégies. Pour chaque demande de connexion, le serveur NPS tente de faire correspondre les conditions de la stratégie avec les propriétés de la demande de connexion. Le serveur NPS examine chaque stratégie réseau dans l’ordre jusqu’à ce qu’il trouve une correspondance. S’il ne trouve pas de correspondance, la demande de connexion est rejetée.

Étapes clés

Pendant la planification des stratégies réseau, vous pouvez effectuer les étapes suivantes.

- Déterminez l’ordre de traitement préféré du serveur NPS des stratégies réseau, du plus restrictif au moins restrictif.
- Déterminez l’état de la stratégie. La valeur de l’état de stratégie peut être activée ou désactivée. Si la stratégie est activée, le serveur NPS évalue la stratégie lors de l’exécution de l’autorisation. Si la stratégie n’est pas activée, elle n’est pas évaluée.
- Déterminez le type de la stratégie. Vous devez déterminer si la stratégie est conçue pour accorder l’accès lorsque les conditions de la stratégie sont mises en correspondance par la demande de connexion ou si la stratégie est conçue pour refuser l’accès lorsque les conditions de la stratégie sont mises en correspondance par la demande de connexion. Par exemple, si vous souhaitez refuser explicitement l’accès sans fil aux membres d’un groupe Windows, vous pouvez créer une stratégie réseau qui spécifie le groupe, la méthode de connexion sans fil et qui a un paramètre de type de stratégie Refuser l’accès.
- Déterminez si vous souhaitez que le serveur NPS ignore les propriétés de connexion à distance des comptes d'utilisateurs qui sont membres du groupe sur lequel la stratégie est fondée. Lorsque ce paramètre n’est pas activé, les paramètres de connexion téléphonique des comptes d’utilisateur remplacent les paramètres configurés dans les stratégies réseau. Par exemple, si une stratégie réseau est configurée pour accorder l’accès à un utilisateur, mais que les propriétés de numérotation du compte d’utilisateur pour cet utilisateur sont définies pour refuser l’accès, l’accès est refusé à l’utilisateur. Toutefois, si vous activez le paramètre de type de stratégie Ignorer les propriétés de numérotation au compte d’utilisateur, l’accès au réseau est accordé au même utilisateur.
- Déterminez si la stratégie utilise le paramètre de source de la stratégie. Ce paramètre vous permet de spécifier facilement une source pour toutes les demandes d’accès. Les sources possibles sont une passerelle TS (Terminal Services Gateway), un serveur d’accès à distance (VPN ou accès à distance), un serveur DHCP, un point d’accès sans fil et un serveur d’autorité d’enregistrement d’intégrité. Vous pouvez également spécifier une source spécifique au fournisseur.
- Déterminez les conditions qui doivent être mises en correspondance pour que la stratégie réseau soit appliquée.
- Déterminez les paramètres appliqués si les conditions de la stratégie réseau sont mises en correspondance par la demande de connexion.
- Déterminez si vous souhaitez utiliser, modifier ou supprimer les stratégies réseau par défaut.

Planifier la gestion des comptes du serveur NPS

NPS offre la possibilité de journaliser les données comptables RADIUS, telles que l'authentification utilisateur et les demandes de gestion des comptes, dans trois formats : format IAS, format compatible avec la base de données et journalisation Microsoft SQL Server.

Le format IAS et le format compatible avec la base de données créent des fichiers journaux sur le serveur NPS local au format de fichier texte.

La journalisation par SQL Server offre la possibilité de journaliser dans une base de données compatible XML pour SQL Server 2000 ou SQL Server 2005, en prolongeant l'enregistrement RADIUS pour tirer parti des avantages de la journalisation dans une base de données relationnelle.

Étapes clés

Pendant la planification de la gestion des comptes du serveur NPS, vous pouvez utiliser les étapes suivantes.

- Déterminez si vous souhaitez stocker les données de comptabilité NPS dans des fichiers journaux ou dans une base de données SQL Server.

Gestion des comptes de serveur NPS à l'aide de fichiers journaux locaux

L'enregistrement des demandes d'authentification et de gestion des comptes des utilisateurs dans les fichiers journaux est principalement utilisé à des fins d'analyse et de facturation des connexions, et est également utile en tant qu'outil d'investigation de sécurité, qui vous fournit une méthode pour suivre l'activité d'un utilisateur malveillant après une attaque.

Étapes clés

Pendant la planification de la gestion des comptes du serveur NPS à l'aide de fichiers journaux locaux, vous pouvez effectuer les étapes suivantes.

- Déterminez le format de fichier texte que vous souhaitez utiliser pour vos fichiers journaux de serveur NPS.

- Choisissez le type d'informations que vous souhaitez journaliser. Vous pouvez enregistrer les demandes de gestion des comptes, les demandes d'authentification et l'état périodique.
- Déterminez l'emplacement du disque dur où vous souhaitez stocker vos fichiers journaux.
- Concevez votre solution de sauvegarde de fichier journal. L'emplacement du disque dur où vous stockez vos fichiers journaux doit être un emplacement qui vous permet de sauvegarder facilement vos données. En outre, l'emplacement du disque dur doit être protégé en configurant la liste de contrôle d'accès (ACL) pour le dossier où sont stockés les fichiers journaux.
- Déterminez à quelle fréquence vous souhaitez que de nouveaux fichiers journaux soient créés. Si vous souhaitez créer des fichiers journaux en fonction de la taille de fichier, déterminez la taille de fichier maximale autorisée avant qu'un nouveau fichier journal ne soit créé par le serveur NPS.
- Déterminez si vous souhaitez que le serveur NPS supprime les fichiers journaux plus anciens si le disque dur manque d'espace de stockage.
- Déterminez l'application ou les applications que vous souhaitez utiliser pour afficher les données comptables et produire des rapports.

Journalisation du serveur NPS SQL Server

La journalisation SQL Server de serveur NPS est utilisée lorsque vous avez besoin d'informations d'état de session, à des fins de création de rapports et d'analyse des données, ainsi que pour centraliser et simplifier la gestion de vos données comptables.

Le serveur NPS offre la possibilité d'utiliser la journalisation SQL Server pour enregistrer les demandes d'authentification utilisateur et de gestion des comptes reçues d'un ou de plusieurs serveurs d'accès réseau à une source de données sur un ordinateur exécutant Microsoft SQL Server Desktop Engine (MSDE 2000), ou toute version de SQL Server postérieure à SQL Server 2000.

Les données comptables sont transmises du serveur NPS au format XML à une procédure stockée dans la base de données, qui prend en charge à la fois le langage de requête structurée (SQL) et le langage XML (SQLXML). L'enregistrement des demandes d'authentification et de gestion des comptes des utilisateurs dans une base de données SQL Server xml permet à plusieurs serveurs NPS d'avoir une seule source de données.

Étapes clés

Pendant la planification de la gestion des comptes du serveur NPS à l'aide de la journalisation NPS SQL Server, vous pouvez utiliser les étapes suivantes.

- Déterminez si vous ou un autre membre de votre organisation avez de l'expérience de développement de bases de données relationnelles SQL Server 2000 ou SQL Server 2005 et si vous comprenez comment utiliser ces produits pour créer, modifier, administrer et gérer les bases de données SQL Server.
- Déterminez si SQL Server est installé sur le serveur NPS ou sur un ordinateur distant.
- Concevez la procédure stockée que vous allez utiliser dans votre base de données SQL Server pour traiter les fichiers XML entrants qui contiennent des données de comptabilité NPS.
- Concevez la structure et le flux de réplication de base de données SQL Server.
- Déterminez l'application ou les applications que vous souhaitez utiliser pour afficher les données comptables et produire des rapports.
- Prévoyez d'utiliser des serveurs d'accès réseau qui envoient l'attribut Class dans toutes les demandes de gestion des comptes. L'attribut Class est envoyé au client RADIUS dans un message Access-Accept et est utile pour mettre en corrélation les messages Accounting-Request avec des sessions d'authentification. Si l'attribut Class est envoyé par le serveur d'accès réseau dans les messages de demande de gestion des comptes, il peut être utilisé pour faire correspondre les enregistrements de gestion des comptes et d'authentification. La combinaison des attributs Unique-Serial-Number, Service-Reboot-Time et Server-Address doit être une identification unique pour chaque authentification acceptée par le serveur.
- Prévoyez d'utiliser des serveurs d'accès réseau qui prennent en charge la gestion des comptes intermédiaire.
- Prévoyez d'utiliser des serveurs d'accès réseau qui envoient des messages Accounting-on et Accounting-off.
- Prévoyez d'utiliser des serveurs d'accès réseau qui prennent en charge le stockage et le transfert des données comptables. Les serveurs d'accès réseau qui prennent en charge cette fonctionnalité peuvent stocker des données de comptabilité lorsque le serveur d'accès réseau ne peut pas communiquer avec le serveur NPS. Lorsque le serveur NPS est disponible, le serveur d'accès réseau transfère les enregistrements stockés au serveur NPS, ce qui offre une fiabilité accrue dans la comptabilité sur les serveurs d'accès réseau qui ne fournissent pas cette fonctionnalité.

- Prévoyez de toujours configurer l'attribut Acct-Interim-Interval dans les stratégies réseau. L'attribut Acct-Interim-Interval définit l'intervalle (en secondes) entre chaque mise à jour intermédiaire envoyée par le serveur d'accès réseau. Selon RFC 2869, la valeur de l'attribut Acct-Interim-Interval ne doit pas être inférieure à 60 secondes (1 minute) et ne doit pas être inférieure à 600 secondes (10 minutes), ce qui signifie que les valeurs supérieures à 600 secondes réduisent la fréquence des mises à jour reçues par le serveur RADIUS. Pour plus d'informations, consultez la RFC 2869.

- Vérifiez que la journalisation de l'état périodique est activée sur vos serveurs NPS.

Commentaires

Cette page a-t-elle été utile ? Yes No

Planifier un serveur NPS en tant que proxy RADIUS

Article • 17/04/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Lorsque vous déployez un serveur NPS (Network Policy Server) en tant que proxy RADIUS (Remote Authentication Dial-In User Service), NPS reçoit les demandes de connexion des clients RADIUS, tels que des serveurs d’accès réseau ou d’autres proxys RADIUS, puis transfère ces demandes de connexion aux serveurs NPS ou à d’autres serveurs RADIUS. Vous pouvez utiliser ces directives de planification pour simplifier votre déploiement RADIUS.

Ces directives de planification n’incluent pas les circonstances dans lesquelles vous souhaitez déployer NPS en tant que serveur RADIUS. Lorsque vous déployez NPS en tant que serveur RADIUS, NPS effectue l’authentification, l’autorisation et la gestion des comptes des demandes de connexion pour le domaine local et pour les domaines qui approuvent le domaine local.

Avant de déployer NPS en tant que proxy RADIUS sur votre réseau, suivez les directives suivantes pour planifier votre déploiement.

- Planifiez la configuration NPS.
- Planifiez les clients RADIUS.
- Planifiez les groupes de serveurs RADIUS distants.
- Planifiez les règles de manipulation des attributs pour le transfert de messages.
- Planifiez les stratégies de requête de connexion.
- Planifier la gestion des comptes du serveur NPS (Network Policy Server).

Planifiez la configuration du serveur NPS (Network Policy Server)

Lorsque vous utilisez NPS comme proxy RADIUS, NPS transfère les demandes de connexion à un serveur NPS ou à d’autres serveurs RADIUS pour traitement. Pour cette raison, l’appartenance au domaine du proxy NPS n’est pas pertinente. Le proxy n’a pas besoin d’être inscrit dans Active Directory Domain Services (AD DS), car il n’a pas besoin

d'accéder aux propriétés de numérotation des comptes d'utilisateur. En outre, vous n'avez pas besoin de configurer des stratégies réseau sur un proxy NPS, car le proxy n'effectue pas d'autorisations pour les demandes de connexion. Le proxy NPS peut être un membre de domaine ou serveur autonome sans appartenance à un domaine.

NPS doit être configuré de manière à communiquer avec les clients RADIUS, également appelés serveurs d'accès réseau, à l'aide du protocole RADIUS. En outre, vous pouvez configurer les types d'événements enregistrés par NPS dans le journal des événements et entrer une description pour le serveur.

Étapes clés

Pendant la planification de la configuration du proxy NPS, vous pouvez effectuer les étapes suivantes.

- Déterminez les ports RADIUS utilisés par le proxy NPS pour recevoir des messages RADIUS à partir de clients RADIUS et pour envoyer des messages RADIUS aux membres des groupes de serveurs RADIUS distants. Par défaut, les ports du protocole UDP sont 1812 et 1645 pour les messages d'authentification RADIUS et sont 1813 et 1646 pour les messages de gestion des comptes RADIUS.

- Si le proxy NPS est configuré avec plusieurs cartes réseau, déterminez les cartes sur lesquelles vous souhaitez autoriser le trafic RADIUS.

- Déterminez les types d'événements que vous souhaitez que NPS enregistre dans le journal des événements. Vous pouvez consigner les demandes de connexion rejetées, les demandes de connexion réussies ou les deux.

- Déterminez si vous déployez plusieurs proxies NPS. Pour fournir une tolérance de panne, utilisez au moins deux proxies NPS. Un proxy NPS est utilisé comme proxy RADIUS principal et l'autre est utilisé comme sauvegarde. Chaque client RADIUS est ensuite configuré sur les deux proxies NPS. Si le proxy NPS principal devient indisponible, les clients RADIUS envoient des messages de demande d'accès au proxy NPS de remplacement.

- Planifiez le script utilisé pour copier une configuration NPS vers d'autres proxies NPS, afin d'économiser sur la surcharge administrative et d'éviter la configuration incorrecte d'un serveur. NPS fournit les commandes Netsh qui vous permettent de copier tout ou partie d'une configuration de proxy NPS pour l'importer sur un autre proxy NPS. Vous pouvez exécuter les commandes manuellement à l'invite Netsh. Toutefois, si vous enregistrez votre séquence de commandes en tant que script, vous pouvez exécuter le script à une date ultérieure si vous décidez de modifier vos configurations de proxy.

Planifiez les clients RADIUS

Les clients RADIUS sont des serveurs d'accès réseau, tels que des points d'accès sans fil, des serveurs de réseau privé virtuel (VPN), des commutateurs compatibles 802.1X et des serveurs d'accès à distance. Les proxies RADIUS, qui transfèrent les messages de demande de connexion aux serveurs RADIUS, sont également des clients RADIUS. Le serveur NPS prend en charge tous les serveurs d'accès réseau et les proxies RADIUS conformes au protocole RADIUS, comme décrit dans RFC 2865, « Service RADIUS (Remote Authentication Dial-in User Service) » et RFC 2866, « Gestion des comptes Radius ».

En outre, les points d'accès sans fil et les commutateurs doivent être capables de réaliser l'authentification 802.1X. Si vous souhaitez déployer le protocole EAP (Extensible Authentication Protocol) ou le protocole PEAP (Protected Extensible Authentication Protocol), les points d'accès et les commutateurs doivent prendre en charge l'utilisation d'EAP.

Pour tester l'interopérabilité de base des connexions PPP pour les points d'accès sans fil, configurez le point d'accès et le client d'accès pour utiliser le protocole PAP (Password Authentication Protocol). Utilisez des protocoles d'authentification PPP supplémentaires, tels que PEAP, jusqu'à ce que vous ayez testé ceux que vous envisagez d'utiliser pour l'accès réseau.

Étapes clés

Pendant la planification des clients RADIUS, vous pouvez effectuer les étapes suivantes.

- Documentez les attributs spécifiques au fournisseur (VSA) que vous devez configurer dans le serveur NPS. Si vos périphériques NAS (Network Attached Storage) nécessitent des VSA, journalisez les informations VSA pour une utilisation ultérieure lorsque vous configurez vos stratégies réseau dans le serveur NPS.

- Documentez les adresses IP des clients RADIUS et votre proxy NPS pour simplifier la configuration de tous les appareils. Lorsque vous déployez vos clients RADIUS, vous devez les configurer pour qu'ils utilisent le protocole RADIUS, avec l'adresse IP du proxy NPS entrée comme serveur d'authentification. Lorsque vous configurez NPS pour communiquer avec vos clients RADIUS, vous devez entrer les adresses IP du client RADIUS dans le composant logiciel enfichable du serveur NPS.

- Créez des secrets partagés pour la configuration sur les clients RADIUS et dans le composant logiciel enfichable du serveur NPS. Vous devez configurer les clients RADIUS avec un secret partagé, ou un mot de passe, que vous allez également

entrer dans le composant logiciel enfichable du serveur NPS lors de la configuration des clients RADIUS dans le serveur NPS.

Planifiez les groupes de serveurs RADIUS distants.

Lorsque vous configurez un groupe de serveurs RADIUS distant sur un proxy NPS, vous indiquez au proxy NPS où envoyer tout ou partie des messages de demande de connexion qu'il reçoit des serveurs d'accès réseau et des proxies NPS ou d'autres proxies RADIUS.

Vous pouvez utiliser NPS comme proxy RADIUS pour transférer les demandes de connexion à un ou plusieurs groupes de serveurs RADIUS distants, chaque groupe pouvant contenir un ou plusieurs serveurs RADIUS. Lorsque vous souhaitez que le proxy NPS transfère des messages à plusieurs groupes, configurez une stratégie de demande de connexion par groupe. La stratégie de demande de connexion contient des informations supplémentaires, telles que des règles de manipulation d'attribut, qui indiquent au proxy NPS quels messages envoyer au groupe de serveurs RADIUS distant spécifié dans la stratégie.

Vous pouvez configurer des groupes de serveurs RADIUS distants à l'aide des commandes Netsh pour NPS, en configurant des groupes directement dans le composant logiciel enfichable NPS sous Groupes de serveurs RADIUS distants, ou en exécutant l'Assistant Nouvelle stratégie de demande de connexion.

Étapes clés

Pendant la planification des groupes de serveurs RADIUS distants, vous pouvez effectuer les étapes suivantes.

- Déterminez les domaines qui contiennent les serveurs RADIUS vers lesquels vous souhaitez que le proxy NPS transfère les demandes de connexion. Ces domaines contiennent les comptes d'utilisateur des utilisateurs qui se connectent au réseau via les clients RADIUS que vous déployez.
- Déterminez si vous devez ajouter de nouveaux serveurs RADIUS dans les domaines où RADIUS n'est pas déjà déployé.
- Documentez les adresses IP des serveurs RADIUS que vous souhaitez ajouter aux groupes de serveurs RADIUS distants.

- Déterminez le nombre de groupes de serveurs RADIUS distants que vous devez créer. Dans certains cas, il est préférable de créer un groupe de serveurs RADIUS distant par domaine, puis d'ajouter les serveurs RADIUS du domaine au groupe. Toutefois, il peut arriver que vous disposiez d'une grande quantité de ressources dans un domaine, notamment un grand nombre d'utilisateurs ayant des comptes d'utilisateur dans le domaine, d'un grand nombre de contrôleurs de domaine et d'un grand nombre de serveurs RADIUS. Votre domaine peut également couvrir une grande zone géographique, ce qui vous amène à avoir des serveurs d'accès réseau et de serveurs RADIUS à des emplacements distants les uns des autres. Dans ces cas et éventuellement dans d'autres cas, vous pouvez créer plusieurs groupes de serveurs RADIUS distants par domaine.

- Créez des secrets partagés pour la configuration sur le proxy NPS et sur les serveurs RADIUS distants.

Planifiez les règles de manipulation des attributs pour le transfert de messages

Les règles de manipulation des attributs, configurées dans les stratégies de demande de connexion, vous permettent d'identifier les messages de demande d'accès que vous souhaitez transférer à un groupe de serveurs RADIUS distant spécifique.

Vous pouvez configurer NPS pour transférer toutes les demandes de connexion à un groupe de serveurs RADIUS distant sans avoir recours aux règles de manipulation d'attribut.

Toutefois, si vous disposez de plusieurs emplacements vers lesquels vous souhaitez transférer les demandes de connexion, vous devez créer une stratégie de demande de connexion pour chaque emplacement, puis configurer la stratégie avec le groupe de serveurs RADIUS distant vers lequel vous souhaitez transférer les messages, ainsi qu'avec les règles de manipulation d'attribut qui indiquent à NPS quels messages transférer.

Vous pouvez créer des règles pour les attributs suivants.

- ID de la station appelée. Numéro de téléphone du serveur d'accès réseau (périphérique NAS). La valeur de cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de correspondance de modèle pour spécifier des indicatifs régionaux.

- ID de la station appelante. Numéro de téléphone utilisé par l'appelant. La valeur de cet attribut est une chaîne de caractères. Vous pouvez utiliser la syntaxe de

correspondance de modèle pour spécifier des indicatifs régionaux.

- Nom d'utilisateur. Nom d'utilisateur fourni par le client d'accès et inclus par le périphérique NAS (Network Attached Storage) dans le message de demande d'accès RADIUS. La valeur de cet attribut est une chaîne de caractères qui contient généralement un nom de domaine et un nom de compte d'utilisateur.

Pour remplacer ou convertir correctement des noms de domaine au nom d'utilisateur d'une demande de connexion, vous devez configurer des règles de manipulation d'attribut pour l'attribut Nom de l'utilisateur sur la stratégie de demande de connexion appropriée.

Étapes clés

Pendant la planification des règles de manipulation d'attribut, vous pouvez effectuer les étapes suivantes.

- Planifiez le routage des messages à partir du périphérique NAS via le proxy vers les serveurs RADIUS distants pour vérifier que vous disposez d'un chemin d'accès logique avec lequel transférer les messages vers les serveurs RADIUS.
- Déterminez un ou plusieurs attributs que vous souhaitez utiliser pour chaque stratégie de demande de connexion.
- Documentez les règles de manipulation d'attribut que vous envisagez d'utiliser pour chaque stratégie de demande de connexion et faites correspondre les règles au groupe de serveurs RADIUS distant vers lequel les messages sont transférés.

Planifiez les stratégies de demande de connexion.

La stratégie de demande de connexion par défaut est configurée pour NPS lorsqu'elle est utilisée en tant que serveur RADIUS. Des stratégies de demande de connexion supplémentaires peuvent être utilisées pour définir des conditions plus spécifiques, pour créer des règles de manipulation d'attribut qui indiquent à NPS quels messages transférer aux groupes de serveurs RADIUS distants et pour spécifier des attributs avancés. Utilisez l'Assistant Nouvelle stratégie de demande de connexion pour créer des stratégies de demande de connexion communes ou personnalisées.

Étapes clés

Pendant la planification des stratégies de demande de connexion, vous pouvez effectuer les étapes suivantes.

- Supprimez la stratégie de demande de connexion par défaut sur chaque serveur exécutant NPS qui fonctionne uniquement en tant que proxy RADIUS.
- Planifiez les conditions et paramètres supplémentaires requis pour chaque stratégie, en combinant ces informations avec le groupe de serveurs RADIUS distant et les règles de manipulation d'attribut planifiées pour la stratégie.
- Concevez le plan pour distribuer les stratégies de demande de connexion communes à tous les proxies NPS. Créez des stratégies communes à plusieurs proxies NPS sur un seul serveur NPS, puis utilisez les commandes Netsh pour NPS afin d'importer les stratégies de demande de connexion et la configuration du serveur sur tous les autres proxies.

Planifier la gestion des comptes du serveur NPS

Lorsque vous configurez NPS en tant que proxy RADIUS, vous pouvez le configurer pour effectuer la gestion des comptes RADIUS à l'aide de fichiers journaux au format NPS, de fichiers journaux de format compatible avec la base de données ou de journalisation NPS SQL Server.

Vous pouvez également transférer des messages de gestion des comptes à un groupe de serveurs RADIUS distant qui effectue la gestion des comptes à l'aide de l'un de ces formats de journalisation.

Étapes clés

Pendant la planification de la gestion des comptes du serveur NPS, vous pouvez effectuer les étapes suivantes.

- Déterminez si vous souhaitez que le proxy NPS effectue des services de gestion des comptes ou transfère les messages afférents à un groupe de serveurs RADIUS distant pour la gestion des comptes.
- Prévoyez de désactiver la gestion des comptes du proxy NPS local si vous envisagez de transférer les messages de gestion des comptes à d'autres serveurs.
- Planifiez les étapes de configuration de la stratégie de demande de connexion si vous envisagez de transférer les messages de gestion des comptes à d'autres

serveurs. Si vous désactivez la gestion des comptes locale pour le proxy NPS, toutes les stratégie de demande de connexion que vous configurez sur ce proxy doivent avoir le transfert des messages de gestion des comptes activé et configuré correctement.

- Déterminez le format de journalisation que vous souhaitez utiliser : fichiers journaux au format IAS, fichiers journaux de format compatibles avec la base de données ou journalisation NPS SQL Server.

Pour configurer l'équilibrage de charge pour NPS en tant que proxy RADIUS, consultez la sectionÉquilibrage de charge du serveur proxy NPS.

Déployer un serveur NPS (Network Policy Server)

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Vous pouvez utiliser cette rubrique pour obtenir des informations sur le déploiement du serveur NPS.

> ⓘ **Notes**
>
> Pour obtenir des informations supplémentaire sur le serveur NPS, vous pouvez utiliser les sections de bibliothèque suivantes.
>
> - Prise en main du serveur NPS
> - Planifier un serveur NPS (Network Policy Server)
> - Gérer le serveur NPS (Network Policy Server)

Le guide du réseau de base Windows Server 2016 comprend une section sur la planification et l'installation du serveur NPS, et les technologies présentées dans le guide servent de prérequis pour le déploiement de NPS dans un domaine Active Directory. Pour plus d'informations, consultez la section « Déployer NPS1 » dans le guide du réseau de base Windows Server 2016.

Déployer des certificats NPS pour l'accès VPN et 802.1X

Si vous souhaitez déployer des méthodes d'authentification comme EAP (Extensible Authentication Protocol) et Protected EAP qui nécessitent l'utilisation de certificats de serveur sur votre NPS, vous pouvez déployer des certificats NPS en vous aidant du guide Déployer des certificats de serveur pour des déploiements câblés et sans fil 802.1X.

Déployer NPS pour l'accès sans fil 802.1X

Pour déployer NPS pour l'accès sans fil, vous pouvez utiliser le guide Déployer un accès sans fil authentifié 802.1X basé sur des mots de passe.

Déployer NPS pour l'accès VPN Windows 10

Vous pouvez utiliser NPS afin de traiter les demandes de connexion Always On VPN (Virtual Private Network) pour les employés distants qui utilisent des ordinateurs et des appareils exécutant Windows 10.

Pour plus d'informations, consultez le tutoriel de déploiement d'Always On VPN pour l'accès à distance pour Windows Server 2016 et Windows 10.

Commentaires

Cette page a-t-elle été utile ? Yes No

Gérer Serveur NPS (Network Policy Server)

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser les rubriques de cette section pour gérer le serveur de stratégie réseau.

> ⓘ **Notes**
>
> Pour obtenir des informations supplémentaire sur le serveur NPS, vous pouvez utiliser les sections de bibliothèque suivantes.
>
> - Prise en main du serveur NPS
> - Planifier un serveur NPS (Network Policy Server)
> - Déployer un serveur NPS (Network Policy Server)

Cette section contient les rubriques suivantes :

- Gestion des serveurs NPS avec les Outils d'administration
- Configurer des stratégies de demande de connexion
- Configurer des pare-feu pour le trafic RADIUS
- Configurer des stratégies réseau
- Configurer la gestion des comptes de serveur NPS (Network Policy Server)
- Configurer des clients RADIUS
- Configurer des groupes de serveurs RADIUS distants
- Gérer les certificats utilisés avec les serveurs NPS
- Gérer les NPS
- Gérer les modèles NPS

Gestion des serveurs NPS avec les Outils d'administration

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour en savoir plus sur les outils que vous pouvez utiliser pour gérer vos serveurs NPS (Network Policy Server).

Après avoir installé le serveur NPS (Network Policy Server), vous pouvez administrer des serveurs NPS :

- Localement, à l'aide du composant logiciel enfichable NPS Microsoft Management Console(MMC), de la console NPS statique dans Outils d'administration, des commandes Windows PowerShell ou des commandes Netsh (Network Shell) pour NPS.
- À partir d'un serveur NPS distant, en utilisant le composant logiciel enfichable MMC NPS, les commandes Netsh pour NPS, les commandes Windows PowerShell pour NPS ou la connexion Bureau à distance.
- À partir d'une station de travail distante, en utilisant la connexion Bureau à distance en combinaison avec d'autres outils, tels que la console MMC NPS ou Windows PowerShell.

> **Notes**
>
> Dans Windows Server 2016, vous pouvez gérer le serveur NPS local à l'aide de la console NPS. Pour gérer les serveurs NPS (Network Policy Server) distants et locaux, vous devez utiliser le composant logiciel enfichable MMC NPS.

> **Notes**
>
> La console NPS et le composant logiciel enfichable MMC NPS présentent une limite de 256 caractères pour tous les paramètres utilisant une valeur de chaîne. Cela inclut tous les paramètres qui peuvent être configurés à l'aide d'expressions régulières. Pour configurer des valeurs de chaîne supérieures à 256 caractères, vous pouvez utiliser les commandes NPS NETSH. Les valeurs de chaîne configurées dépassant 256 caractères ne peuvent pas être modifiées dans la console NPS ou le composant logiciel enfichable MMC NPS sans les invalider.

Les sections suivantes fournissent des instructions sur la gestion de vos serveurs NPS (Network Policy Server) locaux et distants.

Configurer le serveur NPS local à l'aide de la console NPS

Une fois que vous avez installé le serveur NPS (Network Policy Server), vous pouvez utiliser cette procédure pour gérer le serveur NPS local à l'aide de la console MMC NPS.

Informations d'identification administratives

Pour réaliser cette procédure, vous devez être membre du groupe Administrateurs.

Pour configurer le serveur NPS (Network Policy Server) local à l'aide de la console NPS

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Serveur de stratégie réseau**. La console NPS s'ouvre.

2. Dans la console NPS, cliquez sur NPS (local). Dans le volet d'informations, choisissez **Configuration standard** ou **Configuration avancée**, puis effectuez l'une des opérations suivantes en fonction de votre sélection :

    - Si vous choisissez **Configuration standard**, sélectionnez un scénario dans la liste, puis suivez les instructions pour démarrer un Assistant configuration.
    - Si vous choisissez **Configuration avancée**, cliquez sur la flèche pour développer les **options de configuration avancée**, puis passez en revue et configurez les options disponibles en fonction de la fonctionnalité NPS souhaitée : serveur RADIUS, proxy RADIUS ou les deux.

Gérer plusieurs serveurs NPS (Network Policy Server) à l'aide du composant logiciel enfichable MMC NPS

Vous pouvez utiliser cette procédure pour gérer le serveur NPS (Network Policy Server) local et plusieurs serveurs NPS distants à l'aide du composant logiciel enfichable MMC NPS.

Avant d'effectuer la procédure ci-dessous, vous devez installer le serveur NPS (Network Policy Server) sur l'ordinateur local et sur les ordinateurs distants.

En fonction des conditions du réseau et du nombre de serveurs NPS (Network Policy Server) que vous gérez à l'aide du composant logiciel enfichable MMC NPS, la réponse du composant logiciel enfichable MMC peut être lente. En outre, le trafic de configuration du serveur NPS (Network Policy Server) est envoyé sur le réseau au cours d'une session d'administration à

distance à l'aide du composant logiciel enfichable NPS. Assurez-vous que votre réseau est physiquement sécurisé et que les utilisateurs malveillants n'ont pas accès à ce trafic réseau.

Informations d'identification administratives

Pour réaliser cette procédure, vous devez être membre du groupe Administrateurs.

Gérer plusieurs serveurs NPS (Network Policy Server) à l'aide du composant logiciel enfichable NPS

1. Pour ouvrir la console MMC, exécutez Windows PowerShell en tant qu'administrateur. Dans Windows PowerShell, tapez **mmc**, puis appuyez sur Entrée. La console Microsoft Management Console s'ouvre.
2. Dans la console MMC, dans le menu **Fichier** , cliquez sur **Ajouter/Supprimer le composant logiciel enfichable**. La boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** s'ouvre.
3. Dans **Ajouter ou supprimer des composants logiciels enfichables**, dans **Composants logiciels enfichables disponibles**, faites défiler la liste, cliquez sur **Serveur NPS (Network Policy Server)**, puis sur **Ajouter**. La boîte de dialogue **Sélectionner un ordinateur** s'ouvre.
4. Dans **Sélectionner un ordinateur**, vérifiez que **l'ordinateur local (l'ordinateur sur lequel cette console est en cours d'exécution)** est sélectionné, puis cliquez sur **OK**. Le composant logiciel enfichable du serveur NPS local est ajouté à la liste des **composants logiciels enfichables sélectionnés**.
5. Dans **Ajouter ou supprimer des composants logiciels enfichables**, dans **Composants logiciels enfichables disponibles**, vérifiez que l'option **Serveur NPS (Network Policy Server)** est toujours sélectionnée, puis cliquez sur **Ajouter**. La boîte de dialogue **Sélectionner un ordinateur** s'ouvre à nouveau.
6. Dans **Sélectionner un ordinateur**, cliquez sur **Un autre ordinateur**, puis tapez l'adresse IP ou le nom de domaine complet (FQDN) du serveur NPS distant que vous souhaitez gérer à l'aide du composant logiciel enfichable NPS. Si vous le souhaitez, vous pouvez cliquer sur **Parcourir** pour parcourir le répertoire de l'ordinateur que vous souhaitez ajouter. Cliquez sur **OK**.
7. Répétez les étapes 5 et 6 pour ajouter d'autres serveurs NPS (Network Policy Server) au composant logiciel enfichable NPS. Lorsque vous avez ajouté tous les serveurs NPS que vous souhaitez gérer, cliquez sur **OK**.
8. Pour enregistrer le composant logiciel enfichable NPS pour une utilisation ultérieure, cliquez sur **Fichier**, puis sur **Enregistrer**. Dans la boîte de dialogue **Enregistrer** sous, accédez à l'emplacement du disque dur où vous souhaitez enregistrer le fichier, tapez un nom pour votre fichier Microsoft Management Console (.msc), puis cliquez sur **Enregistrer**.

Gérer un serveur NPS (Network Policy Server) à l'aide d'une connexion Bureau à distance

Vous pouvez utiliser cette procédure pour gérer un serveur NPS (Network Policy Server) distant à l'aide d'une connexion Bureau à distance.

En utilisant la connexion Bureau à distance, vous pouvez gérer à distance vos serveurs NPS. Vous pouvez également gérer à distance les serveurs NPS à partir de n'importe quel système d'exploitation client Windows actuel.

Vous pouvez utiliser la connexion Bureau à distance pour gérer plusieurs serveurs NPS (Network Policy Server) à l'aide de l'une des deux méthodes.

1. Créez une connexion Bureau à distance à chacun de vos serveurs NPS (Network Policy Server) individuellement.
2. Utilisez le Bureau à distance pour vous connecter à un serveur NPS (Network Policy Server), puis utilisez la console MMC NPS sur ce serveur pour gérer d'autres serveurs distants. Pour plus d'informations, consultez la section précédente **Gérer plusieurs serveurs NPS (Network Policy Server) à l'aide du composant logiciel enfichable MMC NPS**.

Informations d'identification administratives

Pour réaliser cette procédure, vous devez être membre du groupe Administrateurs sur le serveur NPS (Network Policy Server).

Pour gérer un serveur NPS (Network Policy Server) à l'aide d'une connexion Bureau à distance

1. Sur chaque serveur NPS que vous souhaitez gérer à distance, dans le Gestionnaire de serveur, sélectionnez **Serveur local**. Dans le volet d'informations du Gestionnaire de serveur, affichez le paramètre **Bureau à distance** et effectuez l'une des opérations suivantes.
   a. Si la valeur du paramètre **Bureau à distance** est **Activée**, vous n'avez pas besoin d'effectuer certaines étapes de cette procédure. Passez à l'étape 4 pour commencer à configurer les autorisations utilisateur Bureau à distance.
   b. Si le paramètre **Bureau à distance** est **Désactivé**, cliquez sur le mot **Désactivé**. La boîte de dialogue **Propriétés système** s'ouvre sous l'onglet **Remote** .
2. Dans **Bureau à distance**, cliquez sur **Autoriser les connexions à distance à cet ordinateur**. La boîte de dialogue **Connexion Bureau à distance** s'ouvre. Effectuez l'une des opérations suivantes.

   a. Pour personnaliser les connexions réseau autorisées, cliquez sur **Pare-feu Windows avec sécurité avancée**, puis configurez les paramètres que vous souhaitez autoriser.
   b. Pour activer la connexion Bureau à distance pour toutes les connexions réseau sur l'ordinateur, cliquez sur **OK**.
3. Dans **Propriétés système**, dans **Le Bureau à distance**, déterminez s'il faut autoriser **les connexions uniquement à partir d'ordinateurs exécutant le Bureau à distance avec l'authentification au niveau du réseau** et effectuer votre sélection.
4. Cliquez sur **Sélectionner des utilisateurs**. La boîte de dialogue **Utilisateurs Bureau à distance** s'ouvre.
5. Dans **Utilisateurs Bureau à distance**, pour accorder à un utilisateur l'autorisation de se connecter à distance au serveur NPS (Network Policy Server), cliquez sur **Ajouter**, puis tapez le nom d'utilisateur du compte de l'utilisateur. Cliquez sur **OK**.
6. Répétez l'étape 5 pour chaque utilisateur pour lequel vous souhaitez accorder l'autorisation d'accès à distance au serveur NPS (Network Policy Server). Lorsque vous avez terminé d'ajouter des utilisateurs, cliquez sur **OK** pour fermer la boîte de dialogue **Utilisateurs du Bureau à distance** , puis **à** nouveau pour fermer la boîte de dialogue **Propriétés système** .
7. Pour vous connecter à un serveur NPS distant que vous avez configuré à l'aide des étapes précédentes, cliquez sur **Démarrer**, faites défiler la liste alphabétique, puis cliquez sur **Accessoires Windows**, puis sur **Connexion Bureau à distance**. La boîte de dialogue **Connexion Bureau à distance** s'ouvre.
8. Dans la boîte de dialogue **Connexion Bureau à distance**, dans **Ordinateur**, tapez le nom ou l'adresse IP du serveur NPS (Network Policy Server). Si vous préférez, cliquez sur **Options**, **configurez** des options de connexion supplémentaires, puis cliquez sur Enregistrer pour enregistrer la connexion pour une utilisation répétée.
9. Cliquez sur **Se connecter**, puis, lorsque vous y êtes invité, fournissez les informations d'identification du compte d'utilisateur pour un compte disposant des autorisations nécessaires pour vous connecter et configurer le serveur NPS.

Utiliser des commandes NPS Netsh pour gérer un serveur NPS (Network Policy Server)

Vous pouvez utiliser des commandes dans le contexte NPS Netsh pour afficher et définir la configuration de la base de données d'authentification, d'autorisation, de comptabilité et d'audit utilisée à la fois par le serveur NPS (Network Policy Server) et le service d'accès à distance. Utilisez des commandes dans le contexte NPS Netsh pour :

- Configurez ou reconfigurez un serveur NPS (Network Policy Server), y compris tous les aspects de serveur NPS qui sont également disponibles pour la configuration à l'aide de la console NPS dans l'interface Windows.

- Exportez la configuration d'un serveur NPS (Network Policy Server) (le serveur source), y compris les clés de Registre et le magasin de configuration NPS, sous la forme d'un script Netsh.
- Importez la configuration dans un autre serveur NPS (Network Policy Server) à l'aide d'un script Netsh et du fichier de configuration exporté à partir du serveur NPS (Network Policy Server) source.

Vous pouvez exécuter ces commandes à partir de l'invite de commandes ou de Windows PowerShell. Vous pouvez également exécuter des commandes netsh nps dans des scripts et des fichiers batch.

Informations d'identification administratives

Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs sur l'ordinateur local.

Pour entrer le contexte NPS Netsh sur un serveur NPS (Network Policy Server)

1. Ouvrez l'invite de commandes ou Windows PowerShell.
2. Tapez **netsh**, puis appuyez sur Entrée.
3. Tapez **nps**, puis appuyez sur Entrée.
4. Pour afficher la liste des commandes disponibles, tapez un point d'interrogation (?) et appuyez sur Entrée.

Pour plus d'informations sur les commandes Netsh NPS, voir Commandes Netsh pour Network Policy Server dans Windows Server 2008. Ces commandes sont toujours présentes dans les dernières versions de Windows Server et Windows 11. Vous pouvez donc utiliser netsh dans ces environnements, même si l'utilisation de Windows PowerShell est recommandée.

Utilisation de Windows PowerShell pour gérer les serveurs NPS (Network Policy Server)

Vous pouvez utiliser les commandes Windows PowerShell pour gérer les serveurs NPS (Network Policy Server). Pour plus d'informations, consultez les rubriques de référence des commandes Windows PowerShell suivantes.

- Applets de commande du serveur NPS (Network Policy Server) dans Windows PowerShell. Vous pouvez utiliser ces commandes netsh dans Windows Server 2012 R2 ou des systèmes d'exploitation ultérieurs.

- Module NPS. Vous pouvez utiliser ces commandes netsh dans Windows Server 2016 et les versions ultérieures.

Pour plus d'informations sur l'administration du serveur NPS (Network Policy Server), consultez Gérer le serveur NPS (Network Policy Server).

Configurer des stratégies de requête de connexion

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour créer et configurer des stratégies de demande de connexion qui indiquent si le serveur NPS local traite les demandes de connexion ou les transfère au serveur RADIUS distant pour traitement.

Les stratégies de demande de connexion sont des ensembles de conditions et de paramètres qui permettent aux administrateurs réseau de désigner les serveurs RADIUS (Remote Authentication Dial-In User Service) qui effectuent l'authentification et l'autorisation des demandes de connexion que le serveur exécutant le serveur NPS (Network Policy Server) reçoit des clients RADIUS.

La stratégie de demande de connexion par défaut utilise NPS comme serveur RADIUS et traite toutes les demandes d'authentification localement.

Pour configurer un serveur exécutant NPS de manière à ce qu'il agisse en tant que proxy RADIUS et transfère les demandes de connexion à d'autres serveurs NPS ou RADIUS, vous devez configurer un groupe de serveurs RADIUS distant en plus d'ajouter une nouvelle stratégie de demande de connexion qui spécifie les conditions et les paramètres auxquels les demandes de connexion doivent correspondre.

Vous pouvez créer un groupe de serveurs RADIUS distants pendant que vous créez une stratégie de demande de connexion avec l'Assistant Nouvelle stratégie de demande de connexion.

Si vous ne souhaitez pas que le serveur NPS agisse en tant que serveur RADIUS et traite les demandes de connexion localement, vous pouvez supprimer la stratégie de demande de connexion par défaut.

Si vous souhaitez que le serveur NPS agisse à la fois en tant que serveur RADIUS, en traitant les demandes de connexion localement, et en tant que proxy RADIUS, en transférant certaines demandes de connexion vers un groupe de serveurs RADIUS distant, ajoutez une nouvelle stratégie à l'aide de la procédure suivante, puis vérifiez que la stratégie de demande de connexion par défaut est la dernière stratégie traitée en la plaçant en dernier dans la liste des stratégies.

Ajouter une stratégie de demande de connexion

L’appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour ajouter une nouvelle stratégie de demande de connexion

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau** pour ouvrir la console NPS.
2. Dans l’arborescence de la console, double-cliquez sur **Stratégies**.
3. Cliquez avec le bouton droit sur **Stratégies de demande de connexion**, puis cliquez sur **Nouvelle stratégie de demande de connexion**.
4. Utilisez l’Assistant Nouvelle stratégie de demande de connexion pour configurer votre stratégie de demande de connexion et, si vous n’en avez pas configuré précédemment, un groupe de serveurs RADIUS distant.

Pour plus d’informations sur la gestion du serveur NPS, consultez Gérer le serveur de stratégie réseau.

Pour plus d’informations sur NPS, consultez Serveur de stratégie réseau (NPS).

Configurer des pare-feu pour le trafic RADIUS

Article • 06/10/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Les pare-feu peuvent être configurés pour autoriser ou bloquer les types de trafic IP vers et depuis l'ordinateur ou l'appareil sur lequel le pare-feu s'exécute. Si les pare-feux ne sont pas correctement configurés pour autoriser le trafic RADIUS entre les clients RADIUS, les proxys RADIUS et les serveurs RADIUS, l'authentification de l'accès réseau peuvent échouer, empêchant les utilisateurs d'accéder aux ressources réseau.

Vous devrez peut-être configurer deux types de pare-feu pour autoriser le trafic RADIUS :

- Windows Defender pare-feu avec sécurité avancée sur le serveur local exécutant le serveur NPS (Network Policy Server).
- Pare-feu s'exécutant sur d'autres ordinateurs ou périphériques matériels.

Pare-feu Windows sur le serveur NPS local

Par défaut, le serveur NPS envoie et reçoit le trafic RADIUS à l'aide des ports protocole UDP (User Datagram Protocol) 1812, 1813, 1645 et 1646. Le pare-feu Windows Defender sur le serveur NPS doit être configuré automatiquement, avec des exceptions, lors de l'installation du serveur NPS, pour permettre l'envoi et la réception de ce trafic RADIUS.

Avec Server 2019, cette exception de pare-feu nécessite une modification de l'identificateur de sécurité du compte de service pour détecter et autoriser efficacement le trafic RADIUS. Si cette modification de l'identificateur de sécurité n'est pas exécutée, le pare-feu supprime le trafic RADIUS. À partir d'une invite de commandes avec élévation de privilèges, exécutez `sc sidtype IAS unrestricted`. Cette commande modifie le service IAS (RADIUS) pour qu'il utilise un SID unique au lieu de le partager avec d'autres services SERVICE RÉSEAU.

Par conséquent, si vous utilisez les ports UDP par défaut, vous n'avez pas besoin de modifier la configuration du pare-feu Windows Defender pour autoriser le trafic RADIUS vers et à partir des serveurs NPS.

Dans certains cas, vous pouvez modifier les ports utilisés par NPS pour le trafic RADIUS. Si vous configurez NPS et vos serveurs d'accès réseau pour envoyer et recevoir le trafic

RADIUS sur des ports autres que les ports par défaut, vous devez effectuer les opérations suivantes :

- Supprimez les exceptions qui autorisent le trafic RADIUS sur les ports par défaut.
- Créez de nouvelles exceptions qui autorisent le trafic RADIUS sur les nouveaux ports.

Pour plus d'informations, consultez Configurer les informations de port UDP de serveur NPS.

Autres pare-feu

Dans la configuration la plus courante, le pare-feu est connecté à Internet et le serveur NPS est une ressource intranet connectée au réseau de périmètre.

Pour atteindre le contrôleur de domaine dans l'intranet, le serveur NPS peut avoir :

- Une interface sur le réseau de périmètre et une interface sur l'intranet (le routage IP n'est pas activé).
- Une interface unique sur le réseau de périmètre. Dans cette configuration, le serveur NPS communique avec les contrôleurs de domaine via un autre pare-feu qui connecte le réseau de périmètre à l'intranet.

Configuration du pare-feu Internet

Le pare-feu connecté à Internet doit être configuré avec des filtres d'entrée et de sortie sur son interface Internet (et, éventuellement, son interface de périmètre réseau), pour permettre le transfert de messages RADIUS entre les clients de serveur NPS et RADIUS ou les proxys sur Internet. Des filtres supplémentaires peuvent être utilisés pour permettre le passage du trafic vers des serveurs web, des serveurs VPN et d'autres types de serveurs sur le réseau de périmètre.

Des filtres de paquets d'entrée et de sortie distincts peuvent être configurés sur l'interface Internet et l'interface réseau de périmètre.

Configurer des filtres d'entrée sur l'interface Internet

Configurez les filtres de paquets d'entrée suivants sur l'interface Internet du pare-feu pour autoriser les types de trafic suivants :

- Adresse IP de destination de l'interface réseau de périmètre et du port de destination UDP de 1812 (0x714) du serveur NPS. Ce filtre autorise le trafic

d'authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2865. Si vous utilisez un autre port, remplacez ce numéro de port par 1812.

- Adresse IP de destination de l'interface réseau de périmètre et du port de destination UDP de 1813 (0x715) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2866. Si vous utilisez un autre port, remplacez ce numéro de port par 1813.
- Adresse IP de destination (facultative) de l'interface réseau de périmètre et du port de destination UDP de 1645 (0x66D) du serveur NPS. Ce filtre autorise le trafic d'authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP utilisé par les anciens clients RADIUS.
- Adresse IP de destination (facultative) de l'interface réseau de périmètre et du port de destination UDP de 1646 (0x66E) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP utilisé par les anciens clients RADIUS.

Configurer des filtres de sortie sur l'interface Internet

Configurez les filtres de sortie suivants sur l'interface Internet du pare-feu pour autoriser les types de trafic suivants :

- Adresse IP source de l'interface réseau de périmètre et du port source UDP de 1812 (0x714) du serveur NPS. Ce filtre autorise le trafic d'authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2865. Si vous utilisez un autre port, remplacez ce numéro de port par 1812.
- Adresse IP source de l'interface réseau de périmètre et du port source UDP de 1813 (0x715) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS depuis le serveur NPS vers les clients RADIUS basés sur Internet. Il s'agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2866. Si vous utilisez un autre port, remplacez ce numéro de port par 1813.
- Adresse IP source de l'interface réseau de périmètre et du port source UDP de 1645 (0x66D) du serveur NPS. Ce filtre autorise le trafic d'authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP utilisé par les anciens clients RADIUS.
- Adresse IP source (facultative) de l'interface réseau de périmètre et du port source UDP de 1646 (0x66E) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS depuis le serveur NPS vers les clients RADIUS basés sur Internet. Il s'agit du port UDP utilisé par les anciens clients RADIUS.

Configurer des filtres d’entrée sur l’interface réseau de périmètre

Configurez les filtres d’entrée suivants sur l’interface de réseau de périmètre du pare-feu pour autoriser les types de trafic suivants :

- Adresse IP source de l’interface réseau de périmètre et du port source UDP de 1812 (0x714) du serveur NPS. Ce filtre autorise le trafic d’authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s’agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2865. Si vous utilisez un autre port, remplacez ce numéro de port par 1812.
- Adresse IP source de l’interface réseau de périmètre et du port source UDP de 1813 (0x715) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS depuis le serveur NPS vers les clients RADIUS basés sur Internet. Il s’agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2866. Si vous utilisez un autre port, remplacez ce numéro de port par 1813.
- Adresse IP source de l’interface réseau de périmètre et du port source UDP de 1645 (0x66D) du serveur NPS. Ce filtre autorise le trafic d’authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s’agit du port UDP utilisé par les anciens clients RADIUS.
- Adresse IP source (facultative) de l’interface réseau de périmètre et du port source UDP de 1646 (0x66E) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS depuis le serveur NPS vers les clients RADIUS basés sur Internet. Il s’agit du port UDP utilisé par les anciens clients RADIUS.

Configurer des filtres de sortie sur l’interface réseau de périmètre

Configurez les filtres de sortie suivants sur l’interface de réseau de périmètre du pare-feu pour autoriser les types de trafic suivants :

- Adresse IP de destination de l’interface réseau de périmètre et du port de destination UDP de 1812 (0x714) du serveur NPS. Ce filtre autorise le trafic d’authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s’agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2865. Si vous utilisez un autre port, remplacez ce numéro de port par 1812.
- Adresse IP de destination de l’interface réseau de périmètre et du port de destination UDP de 1813 (0x715) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s’agit du port UDP par défaut utilisé par le serveur NPS, tel que défini dans RFC 2866. Si vous utilisez un autre port, remplacez ce numéro de port par 1813.

- Adresse IP de destination (facultative) de l'interface réseau de périmètre et du port de destination UDP de 1645 (0x66D) du serveur NPS. Ce filtre autorise le trafic d'authentification RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP utilisé par les anciens clients RADIUS.
- Adresse IP de destination (facultative) de l'interface réseau de périmètre et du port de destination UDP de 1646 (0x66E) du serveur NPS. Ce filtre autorise le trafic de gestion des comptes RADIUS des clients RADIUS basés sur Internet vers le serveur NPS. Il s'agit du port UDP utilisé par les anciens clients RADIUS.

Pour plus de sécurité, vous pouvez utiliser les adresses IP de chaque client RADIUS qui envoie les paquets via le pare-feu pour définir des filtres pour le trafic entre le client et l'adresse IP du serveur NPS sur le réseau de périmètre.

Filtres sur l'interface réseau de périmètre

Configurez les filtres de paquets d'entrée suivants sur l'interface de réseau de périmètre du pare-feu intranet pour autoriser les types de trafic suivants :

- Adresse IP source de l'interface réseau de périmètre du serveur NPS. Ce filtre autorise le trafic à partir du serveur NPS sur le réseau de périmètre.

Configurez les filtres de sortie suivants sur l'interface de réseau de périmètre du pare-feu intranet pour autoriser les types de trafic suivants :

- Adresse IP de destination de l'interface réseau de périmètre du serveur NPS. Ce filtre autorise le trafic vers le serveur NPS sur le réseau de périmètre.

Filtres sur l'interface intranet

Configurez les filtres d'entrée suivants sur l'interface intranet du pare-feu pour autoriser les types de trafic suivants :

- Adresse IP de destination de l'interface réseau de périmètre du serveur NPS. Ce filtre autorise le trafic vers le serveur NPS sur le réseau de périmètre.

Configurez les filtres de paquets de sortie suivants sur l'interface intranet du pare-feu pour autoriser les types de trafic suivants :

- Adresse IP source de l'interface réseau de périmètre du serveur NPS. Ce filtre autorise le trafic à partir du serveur NPS sur le réseau de périmètre.

Pour plus d'informations sur la gestion du serveur NPS (Network Policy Server), consultez Gérer le serveur NPS (Network Policy Server).

Pour plus d’informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Configurer des stratégies réseau

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour configurer des stratégies réseau dans le serveur NPS (Network Policy Server).

Ajouter une stratégie réseau

Le serveur NPS (Network Policy Server) utilise des stratégies réseau et les propriétés de numérotation des comptes d'utilisateur pour déterminer si une demande de connexion est autorisée à se connecter au réseau.

Vous pouvez utiliser cette procédure pour configurer une nouvelle stratégie réseau dans la console du serveur NPS ou dans la console d'accès à distance.

Exécution d'une autorisation

Quand le serveur NPS autorise une demande de connexion, il compare la demande à chaque stratégie réseau de la liste triée des stratégies, en commençant par la première stratégie, puis en descendant dans la liste des stratégies configurées. Si le serveur NPS trouve une stratégie dont les conditions correspondent à la demande de connexion, le serveur NPS utilise la stratégie de correspondance et les propriétés de numérotation du compte d'utilisateur pour effectuer l'autorisation. Si les propriétés de numérotation du compte d'utilisateur sont configurées pour accorder ou contrôler l'accès via une stratégie réseau et que la demande de connexion est autorisée, le serveur NPS applique les paramètres configurés dans la stratégie réseau à la connexion.

Si le serveur NPS ne trouve pas de stratégie réseau qui correspond à la demande de connexion, la demande de connexion est rejetée, sauf si les propriétés de numérotation du compte d'utilisateur sont définies pour accorder l'accès.

Si les propriétés de numérotation du compte d'utilisateur sont définies pour refuser l'accès, la demande de connexion est refusée par le serveur NPS.

Paramètres clés

Lorsque vous utilisez l'Assistant Nouvelle stratégie réseau pour créer une stratégie réseau, la valeur que vous spécifiez dans la **méthode de connexion réseau** est utilisée pour configurer

automatiquement la condition **type** de stratégie :

- Si vous conservez la valeur par défaut Unspecified, la stratégie réseau que vous créez est évaluée par le serveur NPS pour tous les types de connexions réseau qui utilisent n'importe quel type de serveur d'accès réseau (NAS).
- Si vous spécifiez une méthode de connexion réseau, le serveur NPS évalue la stratégie réseau uniquement si la demande de connexion provient du type de serveur d'accès réseau que vous spécifiez.

Dans la page **Autorisation d'accès** , vous devez sélectionner **Access accordé** si vous souhaitez que la stratégie autorise les utilisateurs à se connecter à votre réseau. Si vous souhaitez que la stratégie empêche les utilisateurs de se connecter à votre réseau, sélectionnez **Accès refusé**.

Si vous souhaitez que l'autorisation d'accès soit déterminée par les propriétés de numérotation du compte d'utilisateur dans Active Directory® Domain Services (AD DS), vous pouvez cocher la case **Accès déterminé par les propriétés de numérotation de l'utilisateur**.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour ajouter une stratégie réseau

1. Ouvrez la console NPS, puis double-cliquez sur **Stratégies**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**. L'Assistant Nouvelle stratégie réseau s'ouvre.
3. Utilisez l'Assistant Nouvelle stratégie réseau pour créer une stratégie.

Créer à l'aide d'un Assistant des stratégies réseau pour l'accès è distance ou le VPN

Vous pouvez utiliser cette procédure pour créer des stratégies de demande de connexion et des stratégies réseau qui nécessitent le déploiement de serveur de numérotation ou de serveurs de réseau virtuel privé (VPN) en tant que client RADIUS (Remote Authentication Dial-In User Service) sur le serveur NPS RADIUS.

> ⓘ **Notes**
>
> Les ordinateurs clients, comme les ordinateurs portables et autres ordinateurs exécutant des systèmes d'exploitation clients, ne sont pas des clients RADIUS. Les clients RADIUS sont des serveurs d'accès réseau (par exemple, des points d'accès sans fil, des

commutateurs d'authentification 802.1X, des serveurs de réseau privé virtuel (VPN) et des serveurs d'accès à distance), car ces périphériques utilisent le protocole RADIUS pour communiquer avec des serveurs RADIUS, comme les serveurs NPS (Network Policy Server).

Cette procédure explique comment ouvrir l'Assistant Nouvelle connexion d'accès à distance ou de réseau privé virtuel dans le serveur NPS.

Après avoir exécuté l'Assistant, les stratégies suivantes sont créées :

- Une stratégie de demande de connexion
- Une stratégie réseau

Vous pouvez exécuter l'Assistant Nouvelle connexion d'accès à distance ou de réseau privé virtuel chaque fois que vous avez besoin de créer de nouvelles stratégies pour les serveurs d'accès à distance et les serveurs VPN.

L'exécution de l'Assistant Nouvelle connexion d'accès à distance ou de réseau privé virtuel n'est pas la seule étape nécessaire pour déployer des serveurs d'accès à distance ou VPN en tant que clients RADIUS sur le serveur NPS. Les deux méthodes d'accès réseau nécessitent le déploiement de composants matériels et logiciels supplémentaires.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour créer à l'aide d'un Assistant des stratégies pour accès à distance ou le VPN

1. Ouvrez la console du serveur NPS. S'il n'est pas déjà sélectionné, cliquez sur **NPS (local)**. Si vous souhaitez créer des stratégies sur un serveur NPS distant, sélectionnez le serveur.

2. Dans **Prise en main** et **configuration standard**, sélectionnez **le serveur RADIUS pour les connexions rendez-vous ou VPN**. Le texte et les liens situés sous le texte changent pour refléter votre sélection.

3. Cliquez sur **Configurer un VPN ou un accès à distance à l'aide d'un Assistant**. L'Assistant Nouvelles connexions d'accès à distance ou de réseau privé virtuel s'ouvre.

4. Suivez les instructions de l'Assistant pour terminer la création de vos nouvelles stratégies.

Créer des stratégies réseau pour le réseau 802.1X câblé ou sans fil à l'aide d'un Assistant

Vous pouvez utiliser cette procédure pour créer la stratégie de demande de connexion et la stratégie réseau nécessaires pour déployer des commutateurs d'identification 802.1X ou des points d'accès sans fil 802.1X en tant que clients RADIUS (Remote Authentication Dial-In User Service) sur le serveur NPS RADIUS.

Cette procédure explique comment démarrer l'Assistant Nouvelles connexions câblées et sans fil sécurisées IEEE 802.1X dans le serveur NPS.

Après avoir exécuté l'Assistant, les stratégies suivantes sont créées :

- Une stratégie de demande de connexion
- Une stratégie réseau

Vous pouvez exécuter l'Assistant Nouvelles connexions câblées et sans fil sécurisées IEEE 802.1X chaque fois que vous devez créer de nouvelles stratégies pour l'accès 802.1X.

L'exécution de l'Assistant Nouvelles connexions câblées et sans fil sécurisées IEEE 802.1X n'est pas la seule étape requise pour déployer des commutateurs d'authentification et des points d'accès sans fil 802.1X en tant que clients RADIUS sur le serveur NPS. Les deux méthodes d'accès réseau nécessitent le déploiement de composants matériels et logiciels supplémentaires.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour créer des stratégies pour le réseau 802.1X câblé ou sans fil à l'aide d'un Assistant

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.

2. S'il n'est pas déjà sélectionné, cliquez sur **NPS (local)**. Si vous souhaitez créer des stratégies sur un serveur NPS distant, sélectionnez le serveur.

3. Dans **Prise en main** et **configuration standard**, sélectionnez **le serveur RADIUS pour les connexions sans fil ou câblées 802.1X**. Le texte et les liens situés sous le texte changent pour refléter votre sélection.

4. Cliquez sur **Configurer 802.1X à l'aide d'un Assistant**. L'Assistant Nouvelles connexions câblées et sans fil sécurisées IEEE 802.1X s'ouvre.

5. Suivez les instructions de l'Assistant pour terminer la création de vos nouvelles stratégies.

Configurer le serveur NPS afin d'ignorer les propriétés de numérotation du compte d'utilisateur

Utilisez cette procédure pour configurer une stratégie réseau NPS afin d'ignorer les propriétés de numérotation des comptes d'utilisateur dans Active Directory pendant le processus d'autorisation. Les comptes d'utilisateurs dans Utilisateurs et ordinateurs Active Directory ont des propriétés de numérotation qui sont évaluées par le serveur NPS pendant le processus d'autorisation, sauf si la propriété **Autorisation d'accès au réseau** du compte d'utilisateur est définie sur **Contrôler l'accès via la Stratégie réseau NPS**.

Vous pouvez configurer le serveur NPS pour ignorer les propriétés de numérotation des comptes d'utilisateur dans Active Directory dans deux circonstances :

- Lorsque vous souhaitez simplifier l'autorisation NPS à l'aide de la stratégie réseau, mais que toutes vos comptes d'utilisateur n'ont pas la propriété **d'autorisation d'accès réseau** définie pour **contrôler l'accès via la stratégie réseau NPS**. Par exemple, certains comptes d'utilisateur peuvent avoir la propriété **Autorisation d'accès réseau** du compte d'utilisateur définie sur **Refuser l'accès** ou **Autoriser l'accès**.

- Lorsque d'autres propriétés de numérotation de comptes d'utilisateur ne s'appliquent pas au type de connexion configuré dans la stratégie réseau. Par exemple, les propriétés autres que le paramètre **d'autorisation d'accès réseau** s'appliquent uniquement aux connexions commutées ou VPN, mais la stratégie réseau que vous créez concerne les connexions sans fil ou de commutateur authentifiant.

Vous pouvez utiliser cette procédure pour configurer le serveur NPS afin d'ignorer les propriétés de numérotation du compte d'utilisateur. Si une demande de connexion correspond à la stratégie réseau où cette case à cocher est cochée, le serveur NPS n'utilise pas les propriétés de numérotation du compte d'utilisateur pour déterminer si l'utilisateur ou l'ordinateur est autorisé à accéder au réseau. Seuls les paramètres de la stratégie réseau sont utilisés pour déterminer l'autorisation.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.

2. Double-cliquez sur **Stratégies**, cliquez sur **Stratégies réseau**, puis dans le volet d'informations, double-cliquez sur la stratégie que vous souhaitez configurer.

3. Dans la boîte de dialogue **Propriétés** de stratégie, sous l'onglet **Vue d'ensemble** , dans **Autorisation d'accès**, activez la case à cocher Ignorer les propriétés de numérotation du **compte d'utilisateur** , puis cliquez sur **OK**.

Pour configurer le serveur NPS afin d'ignorer les propriétés de numérotation du compte d'utilisateur

Configurer le serveur NPS pour les VLAN (réseaux locaux virtuels)

Lorsque vous utilisez des serveurs d'accès réseau prenant en charge le VLAN et le serveur NPS dans Windows Server 2016, vous pouvez fournir à des groupes d'utilisateurs un accès uniquement aux ressources réseau correspondant à leurs autorisations de sécurité. Par exemple, vous pouvez fournir aux visiteurs un accès sans fil à Internet sans leur permettre d'accéder au réseau de votre organisation.

En outre, les VLAN vous permettent de regrouper logiquement des ressources réseau existants dans différents emplacements physiques ou sur différents sous-réseaux physiques. Par exemple, les membres de votre service commercial et les ressources de leur réseau, telles que les ordinateurs clients, les serveurs et les imprimantes, peuvent se trouver dans plusieurs bâtiments différents de votre organisation, mais vous pouvez placer toutes ces ressources sur un seul VLAN qui utilise la même plage d'adresses IP. Le VLAN fonctionne ensuite comme un seul sous-réseau, par rapport à l'utilisateur final.

Vous pouvez également utiliser des VLAN lorsque vous souhaitez séparer un réseau entre différents groupes d'utilisateurs. Une fois que vous avez déterminé comment définir vos groupes, vous pouvez créer des groupes de sécurité dans le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, puis ajouter des membres aux groupes.

Configurer une stratégie réseau pour les VLAN

Vous pouvez utiliser cette procédure pour configurer une stratégie réseau qui affecte des utilisateurs à un VLAN. Lorsque vous utilisez du matériel réseau prenant en charge les VLAN, tels que des routeurs, des commutateurs et des contrôleurs d'accès, vous pouvez configurer une stratégie réseau pour indiquer aux serveurs d'accès de placer des membres de groupes Active Directory spécifiques sur des VLAN spécifiques. Cette possibilité de regrouper logiquement des ressources réseau avec des VLAN permet de faire preuve de flexibilité lors de la conception et de l'implémentation de solutions réseau.

Lorsque vous configurez les paramètres d'une stratégie réseau NPS à utiliser avec des réseaux locaux virtuels, vous devez configurer les attributs **Tunnel-Medium-Type**, **Tunnel-Pvt-Group-ID**, **Tunnel-Type** et **Tunnel-Tag**.

Cette procédure est fournie à titre indicatif; car votre configuration réseau peut nécessiter des paramètres différents de ceux qui sont décrits ci-dessous.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour configurer une stratégie réseau pour les VLAN

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.

2. Double-cliquez sur **Stratégies**, cliquez sur **Stratégies réseau**, puis dans le volet d'informations, double-cliquez sur la stratégie que vous souhaitez configurer.

3. Dans la boîte de dialogue **Propriétés** de stratégie, cliquez sur l'onglet **Paramètres** .

4. Dans **les propriétés** de stratégie, dans **Paramètres**, dans **les attributs RADIUS**, vérifiez que **Standard** est sélectionné.

5. Dans le volet d'informations, dans **Attributs**, l'attribut **Service-Type** est configuré avec une valeur par défaut **framed**. Par défaut, pour les stratégies avec des méthodes d'accès vpn et rendez-vous, l'attribut **Framed-Protocol** est configuré avec une valeur **PPP**. Pour spécifier des attributs de connexion supplémentaires requis pour les réseaux locaux virtuels, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un attribut RADIUS standard** s'ouvre.

6. Dans **Ajouter un attribut RADIUS standard**, dans Attributs, faites défiler vers le bas et ajoutez les attributs suivants :

    - **Tunnel-Medium-Type**. Sélectionnez une valeur appropriée aux sélections précédentes que vous avez effectuées pour la stratégie. Par exemple, si la stratégie réseau que vous configurez est une stratégie sans fil, sélectionnez **Valeur : 802 (inclut tous les supports 802 plus le format canonique Ethernet)**.

    - **Tunnel-Pvt-Group-ID**. Entrez l'entier qui représente le numéro de VLAN auquel les membres du groupe seront affectés.

    - **Tunnel-Type**. Sélectionnez **Réseaux locaux virtuels (VLAN).**

7. Dans **Ajouter un attribut RADIUS standard**, cliquez sur **Fermer**.

8. Si votre serveur d'accès réseau (NAS) nécessite l'utilisation de l'attribut **Tunnel-Tag** , procédez comme suit pour ajouter l'attribut **Tunnel-Tag** à la stratégie réseau. Si votre documentation NAS ne mentionne pas cet attribut, ne l'ajoutez pas à la stratégie. Si nécessaire, ajoutez les attributs comme suit :

    - Dans **Propriétés** de stratégie, dans **Paramètres**, dans **Attributs RADIUS**, cliquez sur **Fournisseur spécifique**.
    - Dans le volet d'informations, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un attribut spécifique au fournisseur** s'ouvre.
    - Dans **Attributs**, faites défiler vers le bas et sélectionnez **Tunnel-Tag**, puis cliquez sur **Ajouter**. La boîte de dialogue **Informations sur l'attribut** s'ouvre.
    - Dans **Valeur d'attribut**, tapez la valeur que vous avez obtenue à partir de votre documentation matérielle.

Configurer la taille de charge utile EAP

Dans certains cas, les routeurs ou les pare-feu suppriment des paquets, car ils sont configurés pour abandonner les paquets qui nécessitent une fragmentation.

Lorsque vous déployez le serveur NPS avec des stratégies réseau qui utilisent le protocole EAP (Extensible Authentication Protocol) avec le protocole TLS (Transport Layer Security) ou EAP-TLS, comme méthode d'authentification, l'unité de transmission maximale (MTU) par défaut utilisée par le serveur NPS pour les charges utiles EAP est de 1 500 octets.

Cette taille maximale pour la charge utile EAP peut créer des messages RADIUS qui nécessitent une fragmentation par un routeur ou un pare-feu entre le serveur NPS et un client RADIUS. Si tel est le cas, un routeur ou un pare-feu positionné entre le client RADIUS et le serveur NPS peut abandonner en mode silencieux certains fragments, ce qui entraîne l'échec de l'authentification et l'incapacité du client d'accès à se connecter au réseau.

Utilisez la procédure suivante pour réduire la taille maximale utilisée par le serveur NPS pour les charges utiles EAP en ajustant l'attribut Framed-MTU dans une stratégie réseau à une valeur ne dépassant pas 1 344.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour configurer l'attribut Framed-MTU

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.

2. Double-cliquez sur **Stratégies**, cliquez sur **Stratégies réseau**, puis dans le volet d'informations, double-cliquez sur la stratégie que vous souhaitez configurer.

3. Dans la boîte de dialogue **Propriétés** de stratégie, cliquez sur l'onglet **Paramètres** .

4. Dans **Paramètres**, dans **attributs RADIUS**, cliquez sur **Standard**. Dans le volet d'informations, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un attribut RADIUS standard** s'ouvre.

5. Dans **Attributs**, faites défiler vers le bas jusqu'à ce que vous cliquez sur **Framed-MTU**, puis cliquez sur **Ajouter**. La boîte de dialogue **Informations sur l'attribut** s'ouvre.

6. Dans **Valeur d'attribut**, tapez une valeur égale ou inférieure à **1344**. Cliquez sur **OK**, cliquez sur **Fermer**, puis sur **OK**.

Pour plus d'informations sur les stratégies réseau, consultez Stratégies réseau.

Pour obtenir des exemples de syntaxe de correspondance de modèle pour spécifier des attributs de stratégie réseau, consultez Utiliser des expressions régulières dans NPS.

Pour plus d'informations sur NPS, consultez Serveur de stratégie réseau (NPS).

Configurer la comptabilité du serveur de stratégie réseau

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Il existe trois types de journalisation pour le serveur de stratégie réseau (NPS) :

- **Journalisation des événements**. Utilisé principalement pour l'audit et la résolution des problèmes de tentatives de connexion. Vous pouvez configurer la journalisation des événements NPS en obtenant les propriétés NPS dans la console NPS.
- **Journalisation des demandes d'authentification utilisateur et de comptabilité dans un fichier local**. Utilisé principalement à des fins d'analyse de connexion et de facturation. Également utile en tant qu'outil d'investigation de sécurité, car il vous fournit une méthode de suivi de l'activité d'un utilisateur malveillant après une attaque. Vous pouvez configurer l'enregistrement des fichiers locaux à l'aide de l'Assistant de Configuration d'Accounting.
- **Journalisation des demandes d'authentification et de comptabilité des utilisateurs dans une base de données conforme à Microsoft SQL Server XML**. Utilisé pour permettre à plusieurs serveurs exécutant NPS d'avoir une source de données. Fournit également les avantages de l'utilisation d'une base de données relationnelle. Vous pouvez configurer la journalisation SQL Server à l'aide de l'Assistant Configuration de la gestion des comptes.

Utiliser l'Assistant de configuration de la comptabilité

À l'aide de l'Assistant Configuration de la comptabilité, vous pouvez configurer les quatre paramètres de comptabilité suivants :

- **Journalisation SQL uniquement**. À l'aide de ce paramètre, vous pouvez configurer un lien de données vers un serveur SQL Server qui permet au serveur NPS de se connecter et d'envoyer des données comptables au serveur SQL. En outre, l'Assistant peut configurer la base de données sur le serveur SQL afin de s'assurer qu'elle est compatible avec la journalisation NPS SQL Server.
- **Journalisation de texte uniquement**. À l'aide de ce paramètre, vous pouvez configurer NPS pour consigner les données de comptabilité dans un fichier texte.
- **Journalisation parallèle**. À l'aide de ce paramètre, vous pouvez configurer la liaison de données et la base de données SQL Server. Vous pouvez également configurer la

journalisation des fichiers texte afin que NPS se connecte simultanément au fichier texte et à la base de données SQL Server.
- **Journalisation SQL avec sauvegarde**. À l'aide de ce paramètre, vous pouvez configurer la liaison de données et la base de données SQL Server. En outre, vous pouvez configurer la journalisation de fichiers texte utilisée par NPS si la journalisation SQL Server échoue.

En plus de ces paramètres, la journalisation SQL Server et la journalisation de texte vous permettent de spécifier si NPS continue de traiter les demandes de connexion en cas d'échec de la journalisation. Vous pouvez spécifier cela dans la section **Action d'échec de journalisation** dans les propriétés de journalisation des fichiers locaux, dans les propriétés de journalisation SQL Server et pendant l'exécution de l'Assistant de Configuration de la comptabilité.

Pour exécuter l'Assistant Configuration de la gestion des comptes

Pour exécuter l'Assistant Configuration de la comptabilité, procédez comme suit :

1. Ouvrez la console NPS ou le composant logiciel enfichable MMC (Microsoft Management Console) NPS.
2. Dans l'arborescence de la console, cliquez sur **Comptabilité**.
3. Dans le volet d'informations, dans **Comptabilité**, cliquez sur **Configurer la comptabilité**.

Configurer les propriétés du fichier journal NPS

Vous pouvez configurer le serveur de stratégie réseau (NPS) pour effectuer la comptabilité RADIUS pour les demandes d'authentification des utilisateurs, les messages Access-Accept, les messages Access-Reject, les demandes de comptes-rendus et leurs réponses, ainsi que les mises à jour régulières de l'état. Vous pouvez utiliser cette procédure pour configurer les fichiers journaux dans lesquels vous souhaitez stocker les données comptables.

Pour plus d'informations sur l'interprétation des fichiers journaux, consultez Interpréter les fichiers journaux du format de base de données NPS.

Pour empêcher les fichiers journaux de remplir le disque dur, il est fortement recommandé de les conserver sur une partition distincte de la partition système. Voici plus d'informations sur la configuration de la comptabilité pour NPS :

- Pour envoyer les données du fichier journal pour la collecte par un autre processus, vous pouvez configurer NPS pour écrire dans un canal nommé. Pour utiliser des canaux nommés, définissez le dossier du fichier journal sur \.\pipe ou \ComputerName\pipe. Le programme de serveur de canal nommé crée un canal nommé appelé \.\pipe\iaslog.log

pour accepter les données. Dans la boîte de dialogue Propriétés du fichier local, dans Créer un fichier journal, sélectionnez Jamais (taille de fichier illimitée) lorsque vous utilisez des canaux nommés.

- Le répertoire du fichier journal peut être créé à l'aide de variables d'environnement système (au lieu de variables utilisateur), telles que %systemdrive%, %systemroot%et %windir%. Par exemple, le chemin suivant, à l'aide de la variable d'environnement %windir%, localise le fichier journal dans le répertoire système dans le sous-dossier \System32\Logs (autrement dit, %windir%\System32\Logs).

- Le changement de format de fichier journal n'entraîne pas la création d'un nouveau journal. Si vous modifiez les formats de fichier journal, le fichier actif au moment de la modification contiendra un mélange des deux formats (les enregistrements au début du journal auront le format précédent, et les enregistrements à la fin du journal auront le nouveau format).

- Si la comptabilité RADIUS échoue en raison d'un disque dur complet ou d'autres causes, NPS arrête le traitement des demandes de connexion, empêchant les utilisateurs d'accéder aux ressources réseau.

- NPS permet de se connecter à une base de données Microsoft® SQL Server™ en plus, ou au lieu de se connecter à un fichier local.

L'appartenance au groupe **Administrateurs de domaine** est la valeur minimale requise pour effectuer cette procédure.

Pour configurer les propriétés du fichier journal NPS

1. Ouvrez la console NPS ou le composant logiciel enfichable MMC (Microsoft Management Console) NPS.
2. Dans l'arborescence de la console, cliquez sur **Comptabilité**.
3. Dans le volet d'informations, dans **Propriétés du fichier journal**, cliquez sur **Modifier les propriétés du fichier journal**. La boîte de dialogue **Propriétés du fichier journal s'ouvre** .
4. Dans **Les propriétés du fichier journal**, sous l'onglet **Paramètres** , dans **Journaliser les informations suivantes**, veillez à choisir de journaliser suffisamment d'informations pour atteindre vos objectifs comptables. Par exemple, si vos journaux d'activité doivent accomplir la corrélation de session, activez toutes les cases à cocher.
5. Dans **Action d'échec de journalisation**, sélectionnez **Si la journalisation échoue, ignorez les demandes de connexion** si vous souhaitez que NPS arrête le traitement des messages Access-Request lorsque les fichiers journaux sont pleins ou indisponibles pour une raison quelconque. Si vous souhaitez que NPS continue de traiter les demandes de connexion en cas d'échec de la journalisation, ne cochez pas cette case.

6. Dans la boîte de dialogue **Propriétés du fichier journal** , cliquez sur l'onglet **Fichier journal** .
7. Sous l'onglet **Fichier journal** , dans **Répertoire**, tapez l'emplacement où vous souhaitez stocker les fichiers journaux NPS. L'emplacement par défaut est le dossier systemroot\System32\LogFiles.
   Si vous ne fournissez pas d'indication du chemin d'accès complet dans le **répertoire de fichiers journaux**, le chemin d'accès par défaut est utilisé. Par exemple, si vous tapez **NPSLogFile** dans le **répertoire de fichiers journaux**, le fichier se trouve à %systemroot%\System32\NPSLogFile.
8. Au **format**, cliquez sur **DTS Conforme**. Si vous préférez, vous pouvez plutôt sélectionner un format de fichier hérité, tel **qu'ODBC (hérité)** ou **IAS (hérité).**
   Les types de fichiers hérités ODBC et **IAS** contiennent un sous-ensemble des informations envoyées par NPS à sa base de données SQL Server. Le format XML du type de fichier **conforme DTS** est identique au format XML utilisé par NPS pour importer des données dans sa base de données SQL Server. Par conséquent, le format de fichier **conforme DTS** fournit un transfert plus efficace et complet des données dans la base de données SQL Server standard pour NPS.
9. Dans **Créer un fichier journal**, pour configurer NPS pour démarrer de nouveaux fichiers journaux à intervalles spécifiés, cliquez sur l'intervalle que vous souhaitez utiliser :

   - Pour un volume de transactions lourd et une activité de journalisation, cliquez sur **Quotidien**.
   - Pour les volumes de transactions moindres et l'activité de journalisation, cliquez sur **Hebdomadaire** ou **Mensuel**.
   - Pour stocker toutes les transactions dans un fichier journal, cliquez sur **Jamais (taille de fichier illimitée)**.
   - Pour limiter la taille de chaque fichier journal, cliquez **lorsque le fichier journal atteint cette taille**, puis tapez une taille de fichier après laquelle un nouveau journal est créé. La taille par défaut est 10 mégaoctets (Mo).

10. Si vous souhaitez que NPS supprime les anciens fichiers journaux pour créer de l'espace disque pour les nouveaux fichiers journaux lorsque le disque dur est proche de la capacité, vérifiez que **lorsque le disque est entièrement supprimé, les fichiers journaux plus anciens** sont sélectionnés. Cette option n'est pas disponible, cependant, si la valeur de **Créer un fichier journal** n'est **jamais (taille de fichier illimitée)**. En outre, si le fichier journal le plus ancien est le fichier journal actuel, il n'est pas supprimé.

Configurer la journalisation SQL Server NPS

Vous pouvez utiliser cette procédure pour consigner les données de comptabilité RADIUS dans une base de données locale ou distante exécutant Microsoft SQL Server.

> ⓘ **Notes**
>
> NPS met en forme les données de comptabilité en tant que document XML qu'il envoie à la procédure stockée **report_event** dans la base de données SQL Server que vous désignez dans NPS. Pour que la journalisation SQL Server fonctionne correctement, vous devez disposer d'une procédure stockée nommée **report_event** dans la base de données SQL Server qui peut recevoir et analyser les documents XML à partir de NPS.

L'appartenance aux administrateurs de domaine, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour configurer la journalisation SQL Server dans NPS

1. Ouvrez la console NPS ou le composant logiciel enfichable MMC (Microsoft Management Console) NPS.
2. Dans l'arborescence de la console, cliquez sur **Comptabilité**.
3. Dans le volet d'informations, dans **propriétés de journalisation SQL Server**, cliquez sur **Modifier les propriétés de journalisation SQL Server**. La boîte de dialogue **Propriétés de journalisation SQL Server** s'ouvre.
4. Dans **Journaliser les informations suivantes**, sélectionnez les informations que vous souhaitez enregistrer :

    - Pour enregistrer toutes les demandes de comptabilité, cliquez sur **Demandes de comptabilité**.
    - Pour consigner les demandes d'authentification, cliquez sur **Demandes d'authentification**.
    - Pour enregistrer l'état de la comptabilité périodique, cliquez sur **État de comptabilité périodique**.
    - Pour enregistrer l'état périodique, tel que les demandes comptables intermédiaires, cliquez sur **État périodique**.

5. Pour configurer le nombre de sessions simultanées autorisées entre le serveur exécutant NPS et SQL Server, tapez un **nombre dans le nombre maximal de sessions simultanées**.
6. Pour configurer la source de données SQL Server, dans **journalisation SQL Server**, cliquez sur **Configurer**. La boîte de dialogue **Propriétés du lien de données** s'ouvre. Sous l'onglet **Connexion** , spécifiez les éléments suivants :

    - Pour spécifier le nom du serveur sur lequel la base de données est stockée, tapez ou sélectionnez un nom dans **Sélectionner ou entrez un nom de serveur**.
    - Pour spécifier la méthode d'authentification avec laquelle se connecter au serveur, cliquez sur **Utiliser la sécurité intégrée windows NT**. Vous pouvez également cliquer

sur **Utiliser un nom d'utilisateur et un mot de passe spécifiques**, puis tapez les informations d'identification dans **Nom d'utilisateur** et **Mot de passe**.
    - Pour autoriser un mot de passe vide, cliquez sur **Mot de passe vide**.
    - Pour stocker le mot de passe, cliquez sur **Autoriser l'enregistrement du mot de passe**.
    - Pour spécifier la base de données à laquelle se connecter sur l'ordinateur exécutant SQL Server, cliquez sur **Sélectionner la base de données sur le serveur**, puis sélectionnez un nom de base de données dans la liste.
7. Pour tester la connexion entre NPS et SQL Server, cliquez sur **Tester la connexion**. Cliquez sur **OK** pour fermer les **propriétés du lien de données**.
8. Dans **Action d'échec de journalisation**, sélectionnez **Activer la journalisation des fichiers texte pour le basculement** si vous souhaitez que NPS continue avec la journalisation des fichiers texte si la journalisation SQL Server échoue.
9. Dans **Action d'échec de journalisation**, sélectionnez **Si la journalisation échoue, ignorez les demandes de connexion** si vous souhaitez que NPS arrête le traitement des messages Access-Request lorsque les fichiers journaux sont pleins ou indisponibles pour une raison quelconque. Si vous souhaitez que NPS continue de traiter les demandes de connexion en cas d'échec de la journalisation, ne cochez pas cette case.

Nom d'utilisateur Ping

Certains serveurs proxy RADIUS et serveurs d'accès réseau envoient régulièrement des demandes d'authentification et de comptabilité (appelées requêtes ping) pour vérifier que le serveur NPS est présent sur le réseau. Ces requêtes ping incluent des noms d'utilisateur fictifs. Lorsque NPS traite ces demandes, les journaux d'événements et de comptabilité se remplissent d'enregistrements de refus d'accès, ce qui rend plus difficile de suivre les enregistrements valides.

Lorsque vous configurez une entrée de Registre pour le **nom d'utilisateur ping**, NPS correspond à la valeur d'entrée du Registre par rapport à la valeur de nom d'utilisateur dans les requêtes ping par d'autres serveurs. Une entrée de Registre **de noms d'utilisateur ping** spécifie le nom d'utilisateur fictif (ou un modèle de nom d'utilisateur, avec des variables, qui correspondent au nom d'utilisateur fictif) envoyé par les serveurs proxy RADIUS et les serveurs d'accès réseau. Lorsque NPS reçoit des requêtes ping qui correspondent à la valeur d'entrée du registre du **nom d'utilisateur ping** , NPS rejette les demandes d'authentification sans traiter la demande. NPS n'enregistre pas les transactions impliquant le nom d'utilisateur fictif dans les fichiers journaux, ce qui facilite l'interprétation du journal des événements.

Le nom d'utilisateur Ping n'est pas installé par défaut. Vous devez ajouter **un nom d'utilisateur ping** au Registre. Vous pouvez ajouter une entrée au Registre à l'aide de l'Éditeur de Registre.

Attention

Une modification incorrecte du Registre peut gravement endommager votre système. Avant toute modification du registre, il est conseillé de sauvegarder toutes les données importantes de votre ordinateur.

Pour ajouter un nom d'utilisateur ping au registre

Le nom d'utilisateur Ping peut être ajouté à la clé de Registre suivante en tant que valeur de chaîne par un membre du groupe Administrateurs local :

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IAS\Parameters`

- **Nom** : `ping user-name`
- **Type** : `REG_SZ`
- **Données** : *Nom d'utilisateur*

Conseil

Pour indiquer plusieurs noms d'utilisateur pour une valeur **de nom d'utilisateur ping** , entrez un modèle de nom, tel qu'un nom DNS, y compris des caractères génériques, dans **Les données**.

Configurer des clients RADIUS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour configurer des serveurs d'accès réseau en tant que clients RADIUS dans le serveur NPS.

Lorsque vous ajoutez un nouveau serveur d'accès réseau (serveur VPN, point d'accès sans fil, commutateur d'authentification ou serveur d'accès à distance) à votre réseau, vous devez ajouter le serveur en tant que client RADIUS dans le serveur NPS, puis configurer le client RADIUS pour qu'il communique avec le serveur NPS.

> ⓘ **Important**
>
> Les ordinateurs clients, comme les ordinateurs portables et autres ordinateurs exécutant des systèmes d'exploitation clients, ne sont pas des clients RADIUS. Les clients RADIUS sont des serveurs d'accès réseau, tels que les points d'accès sans fil, les commutateurs compatibles 802.1X, les serveurs de réseau privé virtuel (VPN) et les serveurs d'accès à distance, car ils utilisent le protocole RADIUS pour communiquer avec les serveurs RADIUS tels que les serveurs de stratégie réseau (NPS).

Cette étape est également nécessaire lorsque votre serveur NPS est membre d'un groupe de serveurs RADIUS distant configuré sur un proxy de serveur NPS. Dans ce cas, en plus d'effectuer les étapes de cette tâche sur le proxy de serveur NPS, vous devez effectuer les opérations suivantes :

- Sur le proxy de serveur NPS, configurez un groupe de serveurs RADIUS distant qui contient le serveur NPS.
- Sur le serveur NPS distant, configurez le proxy de serveur NPS en tant que client RADIUS.

Pour effectuer les procédures décrites dans cette rubrique, vous devez disposer d'au moins un serveur d'accès réseau (serveur VPN, point d'accès sans fil, commutateur d'authentification ou serveur d'accès à distance) ou proxy NPS physiquement installé sur votre réseau.

Configurez le serveur d'accès réseau

Utilisez cette procédure pour configurer des serveurs d'accès réseau à utiliser avec le serveur NPS. Lorsque vous déployez des serveurs d'accès réseau (NAS) en tant que clients RADIUS,

vous devez configurer les clients pour qu'ils communiquent avec les serveurs NPS où ils sont configurés en tant que clients.

Cette procédure fournit des instructions générales sur les paramètres que vous devez utiliser pour configurer vos NAS. Pour obtenir des instructions spécifiques sur la configuration de l'appareil que vous déployez sur votre réseau, consultez la documentation de votre produit NAS.

Configurez le serveur d'accès réseau

1. Sur le NAS, dans **les paramètres RADIUS**, sélectionnez **l'authentification** RADIUS sur le port UDP (User Datagram Protocol) **1812** et **la comptabilité RADIUS** sur le port UDP **1813**.
2. Dans **le serveur d'authentification** ou **le serveur RADIUS**, spécifiez votre serveur NPS par adresse IP ou nom de domaine complet (FQDN), en fonction des exigences du NAS.
3. Dans **secret** ou **secret partagé**, tapez un mot de passe fort. Lorsque vous configurez le NAS en tant que client RADIUS dans le serveur NPS, vous utilisez le même mot de passe. Ne l'oubliez donc pas.
4. Si vous utilisez PEAP ou EAP comme méthode d'authentification, configurez le NAS pour utiliser l'authentification EAP.
5. Si vous configurez un point d'accès sans fil, dans **SSID**, spécifiez un identificateur de jeu de services (SSID), qui est une chaîne alphanumérique qui sert de nom réseau. Ce nom est diffusé par les points d'accès aux clients sans fil et est visible par les utilisateurs à vos points d'accès à fidélité sans fil (Wi-Fi).
6. Si vous configurez un point d'accès sans fil, dans **802.1X et WPA**, activez **l'authentification IEEE 802.1X** si vous souhaitez déployer PEAP-MS-CHAP v2, PEAP-TLS ou EAP-TLS.

Ajouter le serveur d'accès réseau en tant que client RADIUS dans le serveur NPS

Utilisez cette procédure pour ajouter un serveur d'accès réseau en tant que client RADIUS dans le serveur NPS. Vous pouvez utiliser cette procédure pour configurer un NAS en tant que client RADIUS à l'aide de la console de serveur NPS.

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs** .

Pour ajouter un serveur d'accès réseau en tant que client RADIUS dans le serveur NPS

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.

2. Dans la console NPS, double-cliquez sur **Clients et serveurs RADIUS**. Cliquez avec le bouton droit sur **Clients RADIUS**, puis cliquez sur **Nouveau client RADIUS**.
3. Dans **Nouveau client RADIUS**, vérifiez que la case **Activer ce client RADIUS** est cochée.
4. Dans **Nouveau client RADIUS**, dans **Nom convivial**, tapez un nom d'affichage pour le NAS. Dans **Adresse (IP ou DNS),** tapez l'adresse IP NAS ou le nom de domaine complet (FQDN). Si vous entrez le nom de domaine complet, cliquez sur **Vérifier** si vous souhaitez vérifier que le nom est correct et mappé à une adresse IP valide.
5. Dans **Nouveau client RADIUS**, dans **Fournisseur**, spécifiez le nom du fabricant NAS. Si vous n'êtes pas sûr du nom du fabricant NAS, sélectionnez **RADIUS standard**.
6. Dans **Nouveau client RADIUS**, dans **Secret partagé**, effectuez l'une des opérations suivantes :

    - Vérifiez que **le manuel** est sélectionné, puis dans **le secret partagé**, tapez le mot de passe fort qui est également entré sur le NAS. Retapez le secret partagé dans **Confirmer le secret partagé**.
    - Sélectionnez **Générer**, puis cliquez sur **Générer** pour générer automatiquement un secret partagé. Enregistrez le secret partagé généré pour la configuration sur le NAS, afin qu'il puisse communiquer avec le serveur NPS.

7. Dans **Nouveau client RADIUS**, dans **Options supplémentaires**, si vous utilisez des méthodes d'authentification autres que EAP et PEAP, et si votre NAS prend en charge l'utilisation de l'attribut d'authentificateur de message, sélectionnez **Les messages de demande d'accès doivent contenir l'attribut Message Authenticator**.
8. Cliquez sur **OK**. Votre NAS apparaît dans la liste des clients RADIUS configurés sur le serveur NPS.

Configurer des clients RADIUS par plage d'adresses IP dans Windows Server 2016 Datacenter

Si vous exécutez Windows Server 2016 Datacenter, vous pouvez configurer des clients RADIUS dans le serveur NPS par plage d'adresses IP. Cela vous permet d'ajouter un grand nombre de clients RADIUS (tels que des points d'accès sans fil) à la console NPS à la fois, plutôt que d'ajouter chaque client RADIUS individuellement.

Vous ne pouvez pas configurer les clients RADIUS par plage d'adresses IP si vous exécutez NPS sur Windows Server 2016 Standard.

Utilisez cette procédure pour ajouter un groupe de serveurs d'accès réseau (NAS) en tant que clients RADIUS qui sont tous configurés avec des adresses IP de la même plage d'adresses IP.

Tous les clients RADIUS de la plage doivent utiliser la même configuration et le même secret partagé.

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs** .

Pour configurer des clients RADIUS par plage d'adresses IP

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.
2. Dans la console NPS, double-cliquez sur **Clients et serveurs RADIUS**. Cliquez avec le bouton droit sur **Clients RADIUS**, puis cliquez sur **Nouveau client RADIUS**.
3. Dans **Nouveau client RADIUS**, dans **Nom convivial**, tapez un nom d'affichage pour la collection de NAS.
4. Dans **Adresse (IP ou DNS),** tapez la plage d'adresses IP pour les clients RADIUS à l'aide de la notation CIDR (Classless Inter-Domain Routing). Par exemple, si la plage d'adresses IP des services NAS est 10.10.0.0, tapez **10.10.0.0/16**.
5. Dans **Nouveau client RADIUS**, dans **Fournisseur**, spécifiez le nom du fabricant NAS. Si vous n'êtes pas sûr du nom du fabricant NAS, sélectionnez **RADIUS standard**.
6. Dans **Nouveau client RADIUS**, dans **Secret partagé**, effectuez l'une des opérations suivantes :

    - Vérifiez que **le manuel** est sélectionné, puis dans **le secret partagé**, tapez le mot de passe fort qui est également entré sur le NAS. Retapez le secret partagé dans **Confirmer le secret partagé**.
    - Sélectionnez **Générer**, puis cliquez sur **Générer** pour générer automatiquement un secret partagé. Enregistrez le secret partagé généré pour la configuration sur le NAS, afin qu'il puisse communiquer avec le serveur NPS.

7. Dans **Nouveau client RADIUS**, dans **Options supplémentaires**, si vous utilisez des méthodes d'authentification autres que EAP et PEAP, et si votre NAS prend en charge l'utilisation de l'attribut d'authentificateur de message, sélectionnez **Les messages de demande d'accès doivent contenir l'attribut Message Authenticator**.
8. Cliquez sur **OK**. Vos NAS apparaissent dans la liste des clients RADIUS configurés sur le serveur NPS.

Pour plus d'informations, consultez Clients RADIUS.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Configurer des groupes de serveurs RADIUS distants

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour configurer des groupes de serveurs RADIUS distants lorsque vous souhaitez configurer NPS pour agir en tant que serveur proxy et transférer les demandes de connexion à d'autres serveurs NPS pour traitement.

Ajouter un groupe de serveurs RADIUS distant

Vous pouvez utiliser cette procédure pour ajouter un nouveau groupe de serveurs RADIUS distant dans le composant logiciel enfichable Serveur de stratégie réseau (NPS).

Lorsque vous configurez NPS en tant que proxy RADIUS, vous créez une stratégie de demande de connexion que NPS utilise pour déterminer les demandes de connexion à transférer à d'autres serveurs RADIUS. En outre, la stratégie de demande de connexion est configurée en spécifiant un groupe de serveurs RADIUS distant qui contient un ou plusieurs serveurs RADIUS, qui indique à NPS où envoyer les demandes de connexion qui correspondent à la stratégie de demande de connexion.

> ⓘ **Notes**
>
> Vous pouvez également configurer un nouveau groupe de serveurs RADIUS distants pendant le processus de création d'une stratégie de demande de connexion.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour ajouter un groupe de serveurs RADIUS distant

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau** pour ouvrir la console NPS.
2. Dans l'arborescence de la console, double-cliquez sur **Clients et serveurs RADIUS**, cliquez avec le bouton droit sur **Groupes de serveurs RADIUS distants**, puis cliquez sur **Nouveau**.
3. La boîte de dialogue **Nouveau groupe de serveurs RADIUS distant** s'ouvre. Dans **le nom du groupe**, tapez un nom pour le groupe de serveurs RADIUS distant.

4. **Dans les serveurs RADIUS**, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter des serveurs RADIUS** s'ouvre. Tapez l'adresse IP du serveur RADIUS que vous souhaitez ajouter au groupe, ou tapez le nom de domaine complet (FQDN) du serveur RADIUS, puis cliquez sur **Vérifier**.
5. Dans **Ajouter des serveurs RADIUS**, cliquez sur l'onglet **Authentification/Comptabilité** . Dans **secret partagé** et **Confirmer le secret partagé**, tapez le secret partagé. Vous devez utiliser le même secret partagé lorsque vous configurez l'ordinateur local en tant que client RADIUS sur le serveur RADIUS distant.
6. Si vous n'utilisez pas EAP (Extensible Authentication Protocol) pour l'authentification, cliquez sur **Demande doit contenir l'attribut d'authentificateur de message**. EAP utilise l'attribut Message-Authenticator par défaut.
7. Vérifiez que les numéros de port d'authentification et de gestion des comptes sont corrects pour votre déploiement.
8. Si vous utilisez un autre secret partagé pour la comptabilité, dans **Comptabilité**, décochez **la case Utiliser le même secret partagé pour l'authentification et la comptabilité** , puis tapez le secret partagé de **comptabilité dans secretpartagé et confirmez le secret partagé**.
9. Si vous ne souhaitez pas transférer les messages de démarrage et d'arrêt du serveur d'accès réseau au serveur RADIUS distant, désactivez la case à cocher **Transférer les notifications de démarrage et d'arrêt du serveur d'accès réseau vers ce serveur**.

Pour plus d'informations sur la gestion du serveur NPS, consultez Gérer le serveur de stratégie réseau.

Pour plus d'informations sur NPS, consultez Serveur de stratégie réseau (NPS).

Gérer les certificats utilisés avec les serveurs NPS

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Si vous déployez une méthode d'authentification basée sur un certificat, comme EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), PEAP-TLS (Protected Extensible Authentication Protocol-Transport Layer Security) et PEAP-MS-CHAP v2 (PEAP-Microsoft Challenge Handshake Authentication Protocol version 2), vous devez inscrire un certificat de serveur sur tous vos serveurs NPS. Le certificat de serveur doit :

- Répondre aux exigences minimales de certificat de serveur, comme décrit dans Configurer des modèles de certificat pour les exigences PEAP et EAP
- Être émis par une autorité de certification approuvée par les ordinateurs clients. Une autorité de certification est approuvée quand son certificat existe dans le magasin de certificats Autorités de certification racines de confiance de l'utilisateur actuel et de l'ordinateur local.

Les instructions suivantes vous aident à gérer les certificats NPS dans les déploiements où l'autorité de certification racine de confiance est une autorité de certification tierce, comme Verisign, ou une autorité de certification que vous avez déployée pour votre infrastructure à clé publique (PKI) en utilisant les services de certificats Active Directory (AD CS).

Gestion de l'expiration du certificat

Dans le serveur de stratégie réseau (NPS) sur Windows Server, le certificat de serveur que vous liez à une stratégie réseau n'est pas mis à jour automatiquement lorsqu'elle expire. Lorsque le certificat appliqué à une stratégie expire, un administrateur doit mettre à jour manuellement chaque stratégie qui utilise l'authentification basée sur un certificat pour référencer un nouveau certificat non expiré. Tant que vous n'avez pas mis à jour la stratégie, les clients qui s'appuient sur cette stratégie ne peuvent pas s'authentifier correctement.

> ⓘ **Remarque**

Cette étape manuelle n'est pas requise sur les serveurs NPS configurés pour l'inscription automatique des certificats. En utilisant l'inscription automatique, le certificat de serveur est renouvelé automatiquement avant son expiration, et NPS continue d'utiliser le certificat renouvelé sans intervention de l'administrateur.

Vous devez répéter la procédure suivante pour chaque stratégie réseau configurée pour utiliser l'authentification par certificat (par exemple, EAP-TLS, PEAP-TLS ou PEAP-MS-CHAP v2).

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour mettre à jour le certificat sur une stratégie réseau

1. Ouvrez la console **du serveur de stratégie réseau** .
2. Dans l'arborescence de la console, développez **Stratégies**, puis sélectionnez **Stratégies réseau**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur la stratégie à mettre à jour, puis sélectionnez **Propriétés**.
4. Sélectionnez l'onglet **Contraintes** , puis sélectionnez **Méthodes d'authentification**.
5. Dans la liste **Types EAP** , sélectionnez le type EAP qui utilise le certificat arrivant à expiration, puis sélectionnez **Modifier**.
6. Dans la liste déroulante **Certificat émis,** sélectionnez le nouveau certificat (non expiré), puis sélectionnez **OK**.
7. Sélectionnez **Appliquer**, puis **ok** pour fermer les propriétés de stratégie.
8. Répétez les étapes précédentes pour chaque stratégie réseau configurée pour l'authentification basée sur des certificats.
9. Redémarrez le service IAS (**Network Policy Server**) pour que la modification prenne effet. À partir d'une invite de commandes avec élévation de privilèges, exécutez :

   Invite de commandes Windows

   ```
   net stop ias && net start ias
   ```

Pour valider le certificat lié à une stratégie réseau

Pour confirmer le certificat qu'une stratégie réseau utilise actuellement, exportez la configuration NPS, recherchez la stratégie par nom et lisez l'empreinte numérique du certificat configuré à partir de l'objet blob de configuration EAP.

1. Dans une invite PowerShell ouverte avec des privilèges élevés, exécutez l'extrait de code suivant. Définissez `$PolicyName` le nom de la stratégie réseau que vous souhaitez valider.

   PowerShell

   ```
   $PolicyName = "EAP configured network policy"  # Change this to your policy name
   (case-insensitive)
   $NPSConfigPath = "$env:TEMP\nps-config.xml"
   Export-NpsConfiguration -Path $NPSConfigPath
   $blob = (([xml](Get-Content "$env:TEMP\nps-config.xml" -
   Raw)).SelectNodes("//RadiusProfiles//*[@name]") | Where-Object { $_.name -ieq
   $PolicyName }).Properties.msEAPConfiguration.'#text'
   $found = [regex]::Matches($blob, '14000000([0-9a-f]{40})') | ForEach-Object {
   $_.Groups[1].Value.ToUpper() } | Select-Object -Unique
   if (-not $found) { "No certificate thumbprint found in policy '$PolicyName'" }
   elseif ($found.Count -eq 1) { "Bound certificate thumbprint:$found" } else {
   "WARNING: multiple candidate thumbprints found, manual review of $NPSConfigPath
   needed:`n$($found -join "`n")" }
   ```

2. Comparez l'empreinte renvoyée à celle du certificat que la stratégie est censée utiliser (par exemple, dans le composant logiciel enfichable **Certificats** sous le magasin **Ordinateur local**>**Personnel**). Si elles correspondent, la politique est liée au certificat attendu.

Changer l'expiration du handle TLS en cache

Pendant les processus d'authentification initiale pour EAP-TLS, PEAP-TLS et PEAP-MS-CHAP v2, le serveur NPS met en cache une partie des propriétés de connexion TLS du client qui se connecte. Le client met également en cache une partie des propriétés de connexion TLS du serveur NPS.

Chaque collection individuelle de ces propriétés de connexion TLS est appelée handle TLS.

Les ordinateurs clients peuvent mettre en cache les handles TLS de plusieurs authentificateurs, tandis que les serveurs NPS peuvent mettre en cache les handles TLS de nombreux ordinateurs clients.

Les handles TLS mis en cache sur le client et le serveur permettent au processus de réauthentification d'être plus rapide. Par exemple, quand un ordinateur sans fil se réauthentifie sur un serveur NPS, le serveur NPS peut examiner le handle TLS du client sans fil et rapidement déterminer que la connexion du client est une reconnexion. Le serveur NPS autorise la connexion sans effectuer l'authentification complète.

De la même manière, le client examine le handle TLS du serveur NPS, détermine qu'il s'agit d'une reconnexion et n'a pas besoin d'effectuer l'authentification du serveur.

Sur les ordinateurs exécutant Windows 10 et Windows Server 2016, l'expiration du handle TLS par défaut est définie sur 10 heures.

Dans certains cas, vous pouvez augmenter ou diminuer le délai d'expiration du handle TLS.

Par exemple, vous pouvez réduire le délai d'expiration du handle TLS quand le certificat d'un utilisateur est révoqué par un administrateur et que le certificat a expiré. Dans ce scénario, l'utilisateur peut toujours se connecter au réseau si un serveur NPS a un handle TLS en cache qui n'a pas expiré. La réduction de l'expiration du handle TLS peut empêcher les utilisateurs qui ont des certificats révoqués de se reconnecter.

> **Remarque**
>
> La meilleure solution dans ce scénario est de désactiver le compte d'utilisateur dans Active Directory, ou de supprimer le compte d'utilisateur du groupe Active Directory qui est autorisé à se connecter au réseau dans la stratégie réseau. Toutefois, la propagation de ces changements à tous les contrôleurs de domaine peut également être retardée en raison de la latence de réplication.

Configurer la durée d'expiration du handle TLS sur les ordinateurs clients

Vous pouvez utiliser cette procédure pour changer la durée de mise en cache du handle TLS d'un serveur NPS sur les ordinateurs clients. Dès qu'un serveur NPS est authentifié, les ordinateurs clients mettent en cache les propriétés de connexion TLS du serveur NPS dans un handle TLS. Le handle TLS a une durée par défaut de 10 heures (36 000 000 millisecondes). Vous pouvez augmenter ou diminuer la durée d'expiration du handle TLS avec la procédure suivante.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

> **Important**
>
> Cette procédure doit être effectuée sur un serveur NPS, et non sur un ordinateur client.

Pour configurer la durée d'expiration du handle TLS sur les ordinateurs clients

1. Sur un serveur NPS, ouvrez l'Éditeur du Registre.
2. Accédez à la clé de Registre **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL**
3. Dans le menu **Modifier**, cliquez sur **Nouveau**, puis sur **Clé**.
4. Tapez **ClientCacheTime**, puis appuyez sur Entrée.
5. Cliquez avec le bouton droit sur **ClientCacheTime**, cliquez sur **Nouveau**, puis sur **Valeur DWORD (32 bits).**
6. Tapez la durée, en millisecondes, pendant laquelle vous voulez que les ordinateurs clients mettent en cache le handle TLS d'un serveur NPS après la première tentative d'authentification réussie du serveur NPS.

Configurer la durée d'expiration du handle TLS sur les serveurs NPS

Utilisez cette procédure pour changer la durée de mise en cache du handle TLS des ordinateurs clients sur les serveurs NPS. Dès qu'un client d'accès est authentifié, les serveurs NPS mettent en cache les propriétés de connexion TLS de l'ordinateur client dans un handle TLS. Le handle TLS a une durée par défaut de 10 heures (36 000 000 millisecondes). Vous pouvez augmenter ou diminuer la durée d'expiration du handle TLS avec la procédure suivante.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

> **Important**
>
> Cette procédure doit être effectuée sur un serveur NPS, et non sur un ordinateur client.

Pour configurer la durée d'expiration du handle TLS sur les serveurs NPS

1. Sur un serveur NPS, ouvrez l'Éditeur du Registre.

2. Accédez à la clé de Registre **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL**

3. Dans le menu **Modifier**, cliquez sur **Nouveau**, puis sur **Clé**.

4. Tapez **ServerCacheTime**, puis appuyez sur Entrée.

5. Cliquez avec le bouton droit sur **ServerCacheTime**, cliquez sur **Nouveau**, puis sur **Valeur DWORD (32 bits).**

6. Tapez la durée, en millisecondes, pendant laquelle vous voulez que les serveurs NPS mettent en cache le handle TLS d'un ordinateur client après la première tentative d'authentification réussie du client.

Obtenir le hachage SHA-1 d'un certificat d'autorité de certification racine de confiance

Utilisez cette procédure pour obtenir le hachage SHA-1 (Secure Hash Algorithm) d'une autorité de certification racine de confiance pour un certificat installé sur l'ordinateur local. Dans certaines circonstances, par exemple, quand vous déployez une stratégie de groupe, vous devez désigner un certificat avec le hachage SHA-1 du certificat.

Quand vous utilisez une stratégie de groupe, vous pouvez désigner un ou plusieurs certificats d'autorité de certification racine de confiance que les clients doivent utiliser pour authentifier le serveur NPS pendant le processus d'authentification mutuelle avec EAP ou PEAP. Pour désigner un certificat d'autorité de certification racine de confiance que les clients doivent utiliser pour valider le certificat de serveur, vous pouvez entrer le hachage SHA-1 du certificat.

Cette procédure montre comment obtenir le hachage SHA-1 d'un certificat d'autorité de certification racine de confiance en utilisant le composant logiciel enfichable MMC (Microsoft Management Console) Certificats.

Pour effectuer cette procédure, vous devez être membre du groupe **Utilisateurs** sur l'ordinateur local.

Pour obtenir le hachage SHA-1 d'un certificat d'autorité de certification racine de confiance

1. Dans la boîte de dialogue Exécuter ou Windows PowerShell, tapez **mmc**, puis appuyez sur Entrée. La console MMC s'affiche. Dans la console MMC, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**. La boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** s'ouvre.

2. Dans **Ajouter ou supprimer des composants logiciels enfichables**, dans **Composants logiciels enfichables disponibles**, double-cliquez sur **Certificats**. L'Assistant Composant logiciel enfichable Certificats s'ouvre. Cliquez sur **Compte d'ordinateur**, puis sur **Suivant**.

3. Dans **Sélectionner un ordinateur**, vérifiez que **l'ordinateur local (l'ordinateur sur lequel cette console s'exécute)** est sélectionné, cliquez sur **Terminer**, puis sur **OK**.

4. Dans le volet de gauche, double-cliquez sur **Certificats (ordinateur local)**, puis double-cliquez sur le dossier **Autorités de certification racines de confiance**.

5. Le dossier **Certificats** est un sous-dossier du dossier **Autorités de certification racines approuvées**. Cliquez sur le dossier **Certificats** .

6. Dans le volet d'informations, accédez au certificat de votre autorité de certification racine de confiance. Double-cliquez sur le certificat. La boîte de dialogue **Certificat** s'ouvre.

7. Dans la boîte de dialogue **Certificat** , cliquez sur l'onglet **Détails** .

8. Dans la liste des champs, faites défiler vers et sélectionnez **Empreinte numérique**.

9. Dans le volet inférieur, la chaîne hexadécimale qui représente le hachage SHA-1 de votre certificat s'affiche. Sélectionnez le hachage SHA-1 et appuyez sur le raccourci clavier Windows de la commande Copier (Ctrl+C) pour copier le hachage dans le Presse-papiers Windows.

10. Ouvrez l'emplacement où vous souhaitez coller le hachage SHA-1, placez le curseur au bon endroit, puis appuyez sur le raccourci clavier Windows de la commande Coller (CTRL+V).

Pour plus d'informations sur les certificats et le serveur NPS, consultez Configurer des modèles de certificat pour les exigences PEAP et EAP.

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Last updated on 26/05/2026

Vue d'ensemble de la liste de révocation des certificats du serveur de stratégie réseau

28/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Une liste de révocation de certificats répertorie les certificats numériques qui ont été révoqués par l'autorité de certification avant leur date d'expiration prévue. Un certificat numérique est utilisé pour vérifier l'identité d'un utilisateur, d'un ordinateur ou d'une autre entité dans un environnement en réseau.

Si une méthode d'authentification basée sur un certificat, comme EAP-TLS ou PEAP-TLS, est utilisée, le client envoie des certificats au serveur de stratégie réseau (NPS). Par défaut, le NPS vérifie l'état de révocation de tous les certificats de la chaîne de certificats. If the certificate revocation check fails for **any** of the certificates in the chain, the connection attempt is denied. Une autorité de certification publie les informations sur les certificats révoqués dans une liste de révocation de certificats.

La vérification de la révocation de certificat peut empêcher l'accès client si la liste de révocation de certificats d'un certificat de la chaîne a expiré ou n'est pas disponible. Pour éviter cela, concevez votre infrastructure à clé publique (PKI) pour une haute disponibilité des listes de révocation de certificats. Par exemple, configurez plusieurs points de distribution de liste de révocation de certificats pour chaque autorité de certification dans la hiérarchie des certificats et configurez des calendriers de publication qui garantissent que la liste de révocation de certificats la plus récente est toujours disponible. La vérification de la révocation de certificat est aussi précise que la liste de révocation de certificats sur le NPS. Les listes de révocation de certificats sont publiées par l'autorité de certification selon un calendrier qui peut être configuré et mis en cache sur un serveur NPS pendant leur durée de validité.

Si un certificat est révoqué, la nouvelle liste de révocation de certificats, qui contient le certificat qui vient d'être révoqué, n'est pas automatiquement publiée. De plus, la liste de révocation de certificats du serveur NPS n'est pas mise à jour tant que la liste de révocation de certificats mise en cache est valide. Le certificat révoqué peut toujours être utilisé pour s'authentifier jusqu'à ce que la nouvelle liste de révocation de certificats soit publiée par l'autorité de certification et mise à jour sur le NPS. Pour éviter que cela ne se produise, l'administrateur réseau doit publier manuellement la liste de révocation de certificats mise à jour et la mettre à jour manuellement sur le serveur NPS. Demandez à l'administrateur de l'infrastructure à clé publique comment publier la liste de révocation de certificats.

> **Important**
>
> Lorsque vous utilisez des certificats pour l'authentification des ordinateurs ou des utilisateurs, assurez-vous que les listes de révocation de certificats sont publiées à un emplacement principal et à au moins un emplacement secondaire accessibles par tous les ordinateurs, en particulier par tous les serveurs NPS et autres serveurs RADIUS. Si les serveurs NPS tentent d'effectuer une validation de liste de révocation de certificats d'utilisateur ou d'ordinateur, mais qu'ils ne parviennent pas à localiser les listes de révocation de certificats, le serveur NPS rejette toutes les tentatives de connexion basées sur un certificat, et l'authentification échoue.

Échecs de la vérification de la révocation de certificat

La vérification de la révocation d'un certificat peut échouer pour les raisons suivantes :

- Le certificat a été révoqué.
- Le certificat n'inclut pas les informations de la liste de révocation de certificats.
- La liste de révocation de certificats pour le certificat n'est pas accessible ou n'est pas disponible. Les autorités de certification gèrent les listes de révocation de certificats et les publient sur les points de distribution de ces listes. Les points de distribution des listes de révocation de certificats sont inclus dans la propriété 'CRL Distribution Points' du certificat. Si les points de distribution des listes de révocation de certificats sont injoignables, la vérification de la révocation du certificat échoue, et la demande d'accès est refusée. Si le certificat ne comprend aucun point de distribution de liste de révocation de certificats, la vérification de la révocation échoue, et la demande d'accès est refusée.
- L'éditeur de la liste de révocation de certificats n'a pas délivré le certificat. La liste de révocation de certificats inclut l'autorité de certification de publication. Si l'autorité de certification de publication de la liste de révocation de certificats ne correspond pas à l'autorité de certification émettrice du certificat en cours de vérification, la vérification de la révocation du certificat échoue et la demande d'accès est refusée.
- La liste de révocation de certificats n'est pas à jour. Une liste de révocation de certificats n'est valable que pour une durée limitée. Si la liste de révocation de certificats a expiré, elle est considérée comme non valide, la vérification de la révocation du certificat échoue, et la demande d'accès est refusée. Les nouvelles listes de révocation de certificats doivent être publiées avant la date d'expiration de la dernière liste de révocation de certificats publiée.

Next steps

Le comportement de la vérification de la révocation de certificat sur le NPS peut être modifié avec les paramètres du registre. Pour plus d'informations sur la modification de ces paramètres, consultez Configurer les paramètres de registre de vérification de la liste de révocation de certificats du serveur de stratégie réseau.

Configurer les paramètres de registre de vérification de la liste de révocation de certificats du serveur de stratégie réseau

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Lorsque vous utilisez un serveur de stratégie réseau (NPS) pour appliquer l'authentification basée sur les certificats pour l'accès au réseau, il est important de configurer des listes de révocation de certificats pour garantir que seuls les certificats valides sont acceptés. Les listes de révocation de certificats sont utilisées pour vérifier si un certificat numérique a été révoqué par l'autorité de certification avant sa date d'expiration prévue. Dans un NPS, les listes de révocation de certificats peuvent être configurées pour être vérifiées pendant le processus d'authentification afin de garantir que seuls des certificats valides sont utilisés pour l'accès au réseau. La configuration des listes de révocation de certificats du NPS est une étape clé dans la mise en œuvre d'une infrastructure d'accès réseau sécurisée.

Prerequisites

Le rôle **Services de stratégie et d'accès réseau** est requis pour configurer votre appareil en tant que serveur NPS. Pour en savoir plus, consultez Installer ou désinstaller des rôles, services de rôle ou fonctionnalités.

Comprendre les paramètres du registre de la liste de révocation de certificats du NPS

Les paramètres de Registre pour le serveur NPS peuvent être configurés dans le chemin d'accès du Registre suivant et sont entrés en tant qu'entrée **DWORD** avec la valeur **0** pour **désactivé**, ou **1** pour **activé** :

registry

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13\
```

Les clés suivantes sont définies sur **0** par défaut.

Agrandir le tableau

Name	Description
IgnoreNoRevocationCheck	Lorsqu'il est **désactivé**, un client EAP-TLS ne peut pas se connecter, sauf si le serveur effectue une vérification de révocation de la chaîne de certificats (y compris le certificat racine) du client et vérifie qu'aucun des certificats n'a été révoqué. Lorsqu'il est **activé**, le serveur NPS permet à EAP-TLS clients de se connecter même quand NPS n'effectue pas ou ne peut pas effectuer de vérification de révocation de la chaîne de certificats (à l'exclusion du certificat racine) du client. Vous pouvez utiliser cette entrée pour authentifier les clients lorsque le certificat n'inclut pas de points de distribution de liste de révocation de certificats, tels que les certificats émis par des autorités de certification autres que Microsoft.
IgnoreRevocationOffline	En **cas de désactivation**, le serveur NPS n'autorise pas les clients à se connecter, sauf s'il peut effectuer une vérification de révocation de leur chaîne de certificats et vérifier qu'aucun des certificats n'est révoqué. Lorsque le NPS ne parvient pas à se connecter à un serveur qui stocke une liste de révocation, le certificat ne passe pas le contrôle de révocation et l'authentification échoue. Lorsqu'il est **activé**, le serveur NPS permet à EAP-TLS clients de se connecter même lorsqu'un serveur qui stocke une liste de révocation de certificats n'est pas disponible sur le réseau et empêche l'échec de validation de certificat en raison de conditions réseau médiocres.
NoRevocationCheck	Lorsque **désactivé**, la vérification de la révocation de certificats est activée pour la liste de révocation de certificats NPS. Lorsque le client présente un certificat au serveur NPS, le serveur vérifie si le certificat a été révoqué par l'autorité de certification émettrice avant d'autoriser le client à se connecter au réseau. Si le certificat a été révoqué, l'accès est refusé au client. Lorsqu'il est **activé**, le serveur NPS empêche EAP-TLS d'effectuer une vérification de révocation du certificat du client. Le contrôle de révocation vérifie que le certificat du client et les certificats de sa chaîne de certificats n'ont pas été révoqués.
NoRootRevocationCheck	**Lorsqu'elle est désactivée**, cette entrée élimine uniquement la vérification de révocation du certificat d'autorité de certification racine du client. Un contrôle de révocation est toujours effectué sur le reste de la chaîne de certificats du client. Lorsqu'il est **activé**, le serveur NPS empêche EAP-TLS d'effectuer une vérification de révocation du certificat d'autorité de certification racine du client. Cette entrée authentifie les clients lorsque le certificat n'inclut pas de points

Name	Description
	de distribution de liste de révocation de certificats. En outre, cette entrée peut éviter les retards liés à la certification, qui se produisent lorsqu'une liste de révocation de certificats est hors ligne ou a expiré.

Modification des paramètres du registre de la liste de révocation de certificats du NPS

> ⚠ **Avertissement**
>
> Une modification incorrecte du Registre peut sérieusement endommager votre système. Avant toute modification du registre, il est conseillé de sauvegarder toutes les données importantes de votre ordinateur.

La modification du registre peut être effectuée à l'aide de l'éditeur de registre (regedit.exe), de l'invite de commande ou de PowerShell. Les exemples suivants décrivent l'activation du paramètre de Registre **NoRevocationCheck** et les mêmes étapes s'appliquent à l'activation ou à la désactivation des paramètres de liste de révocation de certificats associés.

Éditeur de Registre

Ces étapes vous permettent d'activer **NoRevocationCheck** sur votre appareil :

1. Sur votre bureau, sélectionnez **Démarrer**, tapez **l'Éditeur du Registre**, cliquez avec le bouton droit sur **l'Éditeur du Registre** , puis sélectionnez **Exécuter en tant qu'administrateur**.
2. Dans **l'Éditeur du Registre**, accédez à **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13**.
3. Dans le volet supérieur, sélectionnez **Modifier**>**le**> nouveau type**DWORD**>**NoRevocationCheck**, puis **appuyez sur Entrée**.
4. Double-cliquez sur votre nouvelle entrée de Registre, remplacez la valeur **par 1**, puis sélectionnez **OK**.

Pour désactiver cette entrée, remplacez la valeur de **1** à **0**.

Pour mettre à jour manuellement la liste de révocation de certificats sur votre serveur NPS, exécutez ces commandes dans l'invite de commande ou PowerShell :

```
certutil -urlcache * delete
certutil -setreg chain\ChainCacheResyncFiletime @now
```

Configurer des modèles de certificat pour les exigences PEAP et EAP

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Tous les certificats utilisés pour l'authentification d'accès réseau avec les protocoles EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), PEAP-TLS (Protected Extensible Authentication Protocol-Transport Layer Security) et PEAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) doivent répondre aux exigences des certificats X.509 et fonctionner pour les connexions qui utilisent SSL/TLS (Secure Socket Layer/Transport Level Security). Les certificats client et serveur ont des exigences supplémentaires.

> ⓘ **Important**
>
> Cet article fournit des instructions pour configurer des modèles de certificat. Pour utiliser ces instructions, vous devez déployer votre propre infrastructure à clé publique (PKI) avec Active Directory Certificate Services (AD CS) si nécessaire.

Conditions minimales requises pour le certificat de serveur

Avec PEAP-MS-CHAP v2, PEAP-TLS ou EAP-TLS comme méthode d'authentification, le serveur NPS doit utiliser un certificat de serveur qui répond aux conditions minimales requises pour le certificat de serveur.

Les ordinateurs clients peuvent être configurés pour valider les certificats de serveur à l'aide de l'option **Valider le certificat de serveur** sur l'ordinateur client ou dans la stratégie de groupe.

L'ordinateur client accepte la tentative d'authentification du serveur lorsque le certificat du serveur répond aux conditions requises suivantes :

- Le nom de l'objet contient une valeur. Si vous émettez un certificat vers votre serveur exécutant le serveur NPS (Network Policy Server) avec un nom d'objet vide, le certificat ne pourra pas authentifier le NPS. Pour configurer le modèle de certificat avec un nom d'objet :

    1. Ouvrez Modèles de certificats.

2. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Nom du sujet**, puis sélectionnez **Construire à partir de ces informations Active Directory**.
4. Dans **Format du nom de l'objet**, sélectionnez une valeur autre que **Aucun**.

- Le certificat d'ordinateur sur le serveur :
  - Chaînes vers une autorité de certification (CA) racine de confiance qui inclut l'objectif `Server Authentication` dans les extensions EKU (l'identifiant d'objet (OID) pour `Server Authentication` est `1.3.6.1.5.5.7.3.1`), et réussit :
    - Vérifications effectuées par CryptoAPI
    - Vérifications spécifiées dans la stratégie d'accès à distance ou la stratégie réseau

- Configurez le certificat de serveur avec le paramètre de chiffrement requis :

  1. Ouvrez Modèles de certificats.
  2. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis sélectionnez **Propriétés**.
  3. Sélectionnez l'onglet **Cryptographie** et assurez-vous de configurer ce qui suit :
     - **Catégorie de fournisseur :** par exemple, **fournisseur de stockage de clés**
     - **Nom de l'algorithme :** par exemple **, RSA**
     - **Fournisseurs :** par exemple, **fournisseur de stockage de clés logicielles Microsoft**
     - **Taille de clé minimale :** par exemple, **2 048**
     - **Algorithme de hachage :** par exemple, **SHA256**
  4. Cliquez sur **Suivant**.

- L'extension Autre nom de l'objet (SubjectAltName), si elle est utilisée, doit contenir le nom DNS du serveur. Pour configurer le modèle de certificat avec le nom DNS (Domain Name System) du serveur d'inscription :

  1. Ouvrez Modèles de certificats.
  2. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis sélectionnez **Propriétés**.
  3. Sélectionnez l'onglet **Nom du sujet**, puis sélectionnez **Construire à partir de ces informations Active Directory**.
  4. Dans **Inclure cette information dans le nom de substitution du sujet**, sélectionnez **Nom DNS**.

Lorsque les utilisateurs utilisent PEAP et EAP-TLS, NPS affiche une liste de tous les certificats installés dans le magasin de certificats d'ordinateur, avec les exceptions suivantes :

- Les certificats qui ne contiennent pas l'objectif `Server Authentication` dans les extensions EKU ne sont pas affichés.
- Les certificats qui ne contiennent pas de nom d'objet ne sont pas affichés.
- Les certificats basés sur le registre et l'ouverture de session par carte à puce ne sont pas affichés.

Pour plus d'informations, consultez Déployer des certificats de serveur pour des déploiements câblés et sans fil 802.1X.

Conditions minimales requises pour les certificats client

Avec EAP-TLS ou PEAP-TLS, le serveur accepte la tentative d'authentification du client lorsque le certificat répond aux exigences suivantes :

- Le certificat client est émis par une autorité de certification d'entreprise ou mappé à un compte d'utilisateur ou d'ordinateur dans Active Directory Domain Services (AD DS).
- Le certificat d'utilisateur ou d'ordinateur sur le client :
  - Chaine vers une autorité de certification racine de confiance qui inclut l'objectif `Client Authentication` dans les extensions EKU (l'OID pour `Client Authentication` est `1.3.6.1.5.5.7.3.2`), et réussit :
    - Vérifications effectuées par CryptoAPI
    - Vérifications spécifiées dans la stratégie d'accès à distance ou la stratégie réseau
    - Les vérifications de l'identifiant de l'objet du certificat spécifiées dans la stratégie du réseau NPS.
- Le client 802.1X n'utilise pas de certificats basés sur le registre qui sont des certificats d'ouverture de session par carte à puce ou protégés par mot de passe.
- Pour les certificats utilisateur, l'extension Autre nom de l'objet (SubjectAltName) dans le certificat contient le nom d'utilisateur principal (UPN). Pour configurer l'UPN dans le modèle de certificat :
  1. Ouvrez Modèles de certificats.
  2. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis sélectionnez **Propriétés**.

3. Sélectionnez l'onglet **Nom du sujet**, puis sélectionnez **Construire à partir de ces informations Active Directory**.
4. Dans **Inclure ces informations dans un autre nom d'objet**, sélectionnez **Nom d'utilisateur principal (UPN).**

- Pour les certificats d'ordinateur, l'extension Subject Alternative Name (SubjectAltName) dans le certificat doit contenir le nom de domaine complet (FQDN) du client, également appelé *nom DNS*. Pour configurer ce nom dans le modèle de certificat :

  1. Ouvrez Modèles de certificats.
  2. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis sélectionnez **Propriétés**.
  3. Sélectionnez l'onglet **Nom du sujet**, puis sélectionnez **Construire à partir de ces informations Active Directory**.
  4. Dans **Inclure cette information dans le nom de substitution du sujet**, sélectionnez **Nom DNS**.

Avec PEAP-TLS et EAP-TLS, les clients affichent la liste de tous les certificats installés dans le composant logiciel enfichable Certificats, avec les exceptions suivantes :

- Les clients sans fil n'affichent pas les certificats basés sur le registre et l'ouverture de session par carte à puce.

- Les clients sans fil et les clients VPN n'affichent pas les certificats protégés par mot de passe.

- Les certificats qui ne contiennent pas l'objectif `Client Authentication` dans les extensions EKU ne sont pas affichés.

Voir aussi

- Serveur de stratégie réseau (NPS).

- Protocole EAP (Extensible Authentication Protocol) pour l'accès réseau.

- Exigences de certificat lorsque vous utilisez EAP-TLS ou PEAP avec EAP-TLS

Gérer des serveurs NPS

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Vous pouvez utiliser les rubriques de cette section pour gérer les NPS.

> ⓘ **Notes**
>
> Pour obtenir des informations supplémentaire sur le serveur NPS, vous pouvez utiliser les sections de bibliothèque suivantes.
>
> - Prise en main du serveur NPS
> - Déployer un serveur NPS (Network Policy Server)

Cette section contient les rubriques suivantes :

- Configurer un serveur NPS sur un ordinateur multirésident
- Configurer des informations de port UDP NPS
- Désactiver le transfert de notifications NAS
- Exporter une configuration de serveur NPS pour importation sur un autre serveur
- Augmenter les authentifications simultanées traitées par serveur NPS
- Installer un serveur NPS (Network Policy Server)
- Équilibrage de charge du serveur proxy NPS
- Inscrire un serveur NPS dans un domaine Active Directory
- Désinscrire un serveur NPS d'un domaine Active Directory
- Utiliser des expressions régulières dans NPS
- Vérifier la configuration après des changements sur le serveur NPS

Commentaires

Cette page a-t-elle été utile ? Yes No

Configurer un serveur NPS sur un ordinateur multirésident

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour configurer un serveur NPS avec plusieurs adaptateurs réseau.

Lorsque vous utilisez plusieurs adaptateurs réseau sur un serveur exécutant un serveur NPS (Network Policy Server), vous pouvez configurer les éléments suivants :

- Les adaptateurs réseau qui envoient et ne reçoivent pas le trafic RADIUS (Remote Authentication Dial-In User Service).
- Sur une base par adaptateur réseau, si NPS surveille le trafic RADIUS sur le protocole Internet version 4 (IPv4), IPv6 ou à la fois IPv4 et IPv6.
- Les numéros de port UDP sur lesquels le trafic RADIUS est envoyé et reçu par protocole (IPv4 ou IPv6), par adaptateur réseau.

Par défaut, le serveur NPS écoute le trafic RADIUS sur les ports 1812, 1813, 1645 et 1646 pour IPv6 et IPv4 pour tous les adaptateurs réseau installés. Étant donné que NPS utilise automatiquement tous les adaptateurs réseau pour le trafic RADIUS, vous devez uniquement spécifier les adaptateurs réseau que vous souhaitez que NPS utilise pour le trafic RADIUS lorsque vous souhaitez empêcher NPS d'utiliser un adaptateur réseau spécifique.

> ⓘ **Notes**
>
> Si vous désinstallez IPv4 ou IPv6 sur un adaptateur réseau, le serveur NPS ne surveille pas le trafic RADIUS pour le protocole désinstallé.

Sur un serveur NPS sur lequel plusieurs adaptateurs réseau sont installés, vous pouvez configurer NPS pour envoyer et recevoir le trafic RADIUS uniquement sur les adaptateurs que vous spécifiez.

Par exemple, un adaptateur réseau installé dans le serveur NPS peut conduire à un segment réseau qui ne contient pas de clients RADIUS, tandis qu'un deuxième adaptateur réseau fournit à NPS un chemin d'accès réseau à ses clients RADIUS configurés. Dans ce scénario, il est important d'indiquer à NPS d'utiliser le deuxième adaptateur réseau pour tout le trafic RADIUS.

Dans un autre exemple, si votre serveur NPS a trois adaptateurs réseau installés, mais que vous souhaitez que NPS utilise uniquement deux adaptateurs pour le trafic RADIUS, vous pouvez

configurer les informations de port pour les deux adaptateurs uniquement. En excluant la configuration de port pour le troisième adaptateur, vous empêchez NPS d'utiliser l'adaptateur pour le trafic RADIUS.

Utilisation d'un adaptateur réseau

Pour configurer NPS pour écouter et envoyer le trafic RADIUS sur un adaptateur réseau, utilisez la syntaxe suivante dans la boîte de dialogue Propriétés de NPS (Network Policy Server) dans la console NPS :

- Syntaxe du trafic IPv4 : IPAddress:UDPport , où IPAddress est l'adresse IPv4 configurée sur l'adaptateur réseau sur lequel vous souhaitez envoyer le trafic RADIUS, et UDPport est le numéro de port RADIUS que vous souhaitez utiliser pour l'authentification RADIUS ou le trafic de comptabilité.
- Syntaxe du trafic IPv6 : [IPv6Address] : UDPport , où les crochets entourant IPv6Address sont requis, IPv6Address est l'adresse IPv6 configurée sur l'adaptateur réseau sur lequel vous souhaitez envoyer le trafic RADIUS, et UDPport est le numéro de port RADIUS que vous souhaitez utiliser pour l'authentification RADIUS ou le trafic de comptabilité.

Les caractères suivants peuvent être utilisés comme délimiteurs pour configurer l'adresse IP et les informations de port UDP :

- Délimiteur d'adresse/de port : deux-points (:)
- Délimiteur de port : virgule (,)
- Délimiteur d'interface : point-virgule (;)

Configuration des serveurs d'accès réseau

Assurez-vous que vos serveurs d'accès réseau sont configurés avec les mêmes numéros de port UDP RADIUS que vous configurez sur vos serveurs NPS. Les ports UDP standard RADIUS définis dans les RFC 2865 et 2866 sont 1812 pour l'authentification et 1813 pour la comptabilité. Toutefois, certains serveurs d'accès sont configurés par défaut pour utiliser le port UDP 1645 pour les demandes d'authentification et le port UDP 1646 pour les requêtes de comptabilité.

> **ⓘ Important**
>
> Si vous n'utilisez pas les numéros de port RADIUS par défaut, vous devez configurer des exceptions sur le pare-feu de l'ordinateur local afin d'autoriser le trafic RADIUS sur les

nouveaux ports. Pour plus d'informations, consultez [Configurer des pare-feux pour le trafic RADIUS](#).

Configurer le serveur NPS multi-hébergement

Vous pouvez utiliser la procédure suivante pour configurer votre serveur NPS multi-hébergement.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour spécifier l'adaptateur réseau et les ports UDP utilisés par NPS pour le trafic RADIUS

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau** pour ouvrir la console NPS.

2. Cliquez avec le bouton droit sur **Serveur NPS (Network Policy Server)**, puis cliquez sur **Propriétés**.

3. Cliquez sur l'onglet **Ports** , puis ajoutez l'adresse IP de la carte réseau que vous souhaitez utiliser pour le trafic RADIUS vers les numéros de port existants. Par exemple, si vous souhaitez utiliser l'adresse IP 192.168.1.2 et les ports RADIUS 1812 et 1645 pour les demandes d'authentification, remplacez le paramètre de port de **1812 1645** par **192.168.1.2:1812,1645**. Si vos ports UDP d'authentification RADIUS et de comptabilité RADIUS sont différents des valeurs par défaut, modifiez les paramètres de port en conséquence.

4. Pour utiliser plusieurs paramètres de port pour les demandes d'authentification ou de gestion des comptes, séparez les numéros de port par des virgules.

Pour plus d'informations sur les ports UDP NPS, consultez Configurer les informations de port UDP NPS.

Pour plus d'informations sur le serveur NPS, consultez Serveur NPS (Network Policy Server).

Configurer des informations de port UDP NPS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser la procédure suivante pour configurer les ports utilisés par le serveur NPS (Network Policy Server) pour le trafic d'authentification et de gestion des comptes par protocole RADIUS (Remote Authentication Dial-In User Service).

Par défaut, le serveur NPS écoute le trafic RADIUS sur les ports 1812, 1813, 1645 et 1646 pour le protocole Internet version 6 (IPv6) et IPv4 pour toutes les cartes réseau installées.

> ⓘ **Notes**
>
> Si vous désinstallez IPv4 ou IPv6 sur un adaptateur réseau, le serveur NPS ne surveille pas le trafic RADIUS pour le protocole désinstallé.

Les valeurs de port 1812 pour l'authentification et de 1813 pour la gestion des comptes sont des ports RADIUS standard définis par l'Internet Engineering Task Force (IETF) dans les RFC 2865 et 2866. Toutefois, par défaut, de nombreux serveurs d'accès utilisent les ports 1645 pour les demandes d'authentification et 1646 pour les demandes de gestion des comptes. Quel que soit les numéros de port que vous décidez d'utiliser, assurez-vous que le serveur NPS et votre serveur d'accès sont configurés pour utiliser les mêmes.

> [IMPORTANT] Si vous n'utilisez pas les numéros de port RADIUS par défaut, vous devez configurer des exceptions sur le pare-feu de l'ordinateur local afin d'autoriser le trafic RADIUS sur les nouveaux ports. Pour plus d'informations, consultez Configurer des pare-feux pour le trafic RADIUS.

L'appartenance aux **administrateurs de domaine**, ou équivalent, est la condition minimale requise pour effectuer cette procédure.

Pour configurer des informations de port UDP NPS

1. Ouvrez la console du serveur NPS.
2. Cliquez avec le bouton droit sur **Serveur NPS (Network Policy Server)**, puis cliquez sur **Propriétés**.

3. Cliquez sur l'onglet **Ports** , puis examinez les paramètres des ports. Si vos ports UDP d'authentification RADIUS et de comptabilité RADIUS varient selon les valeurs par défaut fournies (1812 et 1645 pour l'authentification, et 1813 et 1646 pour la comptabilité), tapez vos paramètres de port dans **Authentification** et **comptabilité**.
4. Pour utiliser plusieurs paramètres de port pour les demandes d'authentification ou de gestion des comptes, séparez les numéros de port par des virgules.

Pour plus d'informations sur la gestion du serveur NPS (Network Policy Server), consultez Gérer le serveur NPS (Network Policy Server).

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Désactiver le transfert de notification NAS dans NPS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette procédure pour désactiver le transfert des messages de démarrage et d'arrêt des messages des serveurs d'accès réseau (NAS) aux membres d'un groupe de serveurs RADIUS distant configuré dans NPS.

Lorsque vous avez configuré des groupes de serveurs RADIUS distants et que, dans **Stratégies de demande de connexion** NPS, vous décochez la case **Transférer les demandes de gestion des comptes à ce groupe de serveurs RADIUS distants**, ces groupes reçoivent toujours des messages de notification de démarrage et d'arrêt NAS.

Cela crée un trafic réseau inutile. Pour éliminer ce trafic, désactivez le transfert de notification NAS pour des serveurs individuels dans chaque groupe de serveurs RADIUS distant.

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs** .

Pour désactiver le transfert de notification NAS

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Serveur de stratégie réseau**. La console NPS s'ouvre.

2. Dans la console NPS, double-cliquez sur **Clients et serveurs RADIUS**, cliquez sur **Groupes de serveurs RADIUS distants**, puis double-cliquez sur le groupe de serveurs RADIUS distant que vous souhaitez configurer. La boîte de dialogue **Propriétés** du groupe de serveurs RADIUS distant s'ouvre.

3. Double-cliquez sur le membre du groupe que vous souhaitez configurer, puis cliquez sur l'onglet **Authentification/comptabilité** .

4. Dans **Comptabilité**, désactivez la case à **cocher Démarrer et arrêter les notifications du serveur d'accès réseau vers ce serveur** , puis cliquez sur **OK**.

5. Répétez les étapes 3 et 4 pour tous les membres du groupe que vous souhaitez configurer.

Pour plus d'informations sur la gestion du serveur NPS (Network Policy Server), consultez Gérer le serveur NPS (Network Policy Server).

Pour plus d’informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Exporter une configuration de serveur NPS pour importation sur un autre serveur

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez exporter l'ensemble de la configuration NPS (y compris les clients et serveurs RADIUS, la stratégie réseau, la stratégie de demande de connexion, le Registre et la configuration de journalisation) à partir d'un NPS pour importation sur un autre NPS.

Utilisez l'un des outils suivants pour exporter la configuration NPS :

- Dans Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012, vous pouvez utiliser Netsh ou Windows PowerShell.
- Dans Windows Server 2008 R2 et Windows Server 2008, utilisez Netsh.

> ⓘ **Important**
>
> N'utilisez pas cette procédure si la base de données NPS source a un numéro de version supérieur à celui de la base de données NPS de destination. Vous pouvez afficher le numéro de version de la base de données NPS à partir de l'affichage de la commande **netsh nps show config** .

> ⓘ **Notes**
>
> L'importation d'une configuration NPS écrase la configuration existante. Il n'est pas possible d'ajouter des paramètres à la configuration existante en les important.

Étant donné que les configurations NPS ne sont pas chiffrées dans le fichier XML exporté, son envoi sur un réseau peut présenter un risque de sécurité. Prenez donc des précautions lors du déplacement du fichier XML du serveur source vers les serveurs de destination. Par exemple, ajoutez le fichier à un fichier d'archive chiffré et protégé par un mot de passe avant de le déplacer. En outre, stockez le fichier dans un emplacement sécurisé pour empêcher les utilisateurs malveillants d'y accéder.

> ⓘ **Notes**
>
> Si la journalisation SQL Server est configurée sur le serveur NPS source, les paramètres de journalisation SQL Server ne sont pas exportés vers le fichier XML. Après avoir importé le

fichier sur un autre serveur NPS, vous devez configurer manuellement la journalisation SQL Server.

Exportez et importez la configuration NPS à l'aide de Windows PowerShell

Pour Windows Server 2012 et versions ultérieures du système d'exploitation, vous pouvez exporter la configuration NPS à l'aide de Windows PowerShell.

La syntaxe de commande pour l'exportation de la configuration NPS est la suivante.

PowerShell

```
Export-NpsConfiguration -Path <filename>
```

Le tableau suivant répertorie les paramètres de l'applet **de commande Export-NpsConfiguration** dans Windows PowerShell. Les paramètres en gras sont requis.

Agrandir le tableau

Parameter	Description
Path	Spécifie le nom et l'emplacement du fichier XML vers lequel vous souhaitez exporter la configuration NPS.

Informations d'identification d'administration

Pour réaliser cette procédure, vous devez être membre du groupe Administrateurs.

Exemple d'exportation

Dans l'exemple suivant, la configuration NPS est exportée vers un fichier XML situé sur le lecteur local. Pour exécuter cette commande, exécutez Windows PowerShell en tant qu'administrateur sur le NPS source, entrez la commande suivante, puis appuyez sur Entrée.

PowerShell

```
Export-NpsConfiguration –Path c:\config.xml
```

Pour plus d'informations, consultez Export-NpsConfiguration.

Après avoir exporté la configuration NPS, copiez le fichier XML sur le serveur de destination.

La syntaxe de commande pour importer la configuration NPS sur le serveur de destination est la suivante.

PowerShell

```
Import-NpsConfiguration [-Path] <String> [ <CommonParameters>]
```

Exemple d'importation

La commande suivante importe les paramètres du fichier nommé C:\Npsconfig.xml vers NPS. Pour exécuter cette commande, exécutez Windows PowerShell en tant qu'administrateur sur le NPS de destination, entrez la commande suivante, puis appuyez sur Entrée.

PowerShell

```
Import-NpsConfiguration -Path "C:\Npsconfig.xml"
```

Pour plus d'informations, consultez Import-NpsConfiguration.

Exportez et importez la configuration NPS à l'aide de Netsh

Vous pouvez utiliser Network Shell (Netsh) pour exporter la configuration NPS à l'aide de la commande **netsh nps export** .

Lorsque la commande **netsh nps import** est exécutée, NPS est automatiquement actualisé avec les paramètres de configuration mis à jour. Vous n'avez pas besoin d'arrêter NPS sur l'ordinateur de destination pour exécuter la commande **netsh nps import** . Toutefois, si la console NPS ou le composant logiciel enfichable MMC NPS est ouvert pendant l'importation de la configuration, les modifications apportées à la configuration du serveur ne sont pas visibles tant que vous n'avez pas actualisé la vue.

> ⓘ **Notes**
>
> Lorsque vous utilisez la commande **netsh nps export** , vous devez fournir au paramètre **de commande exportPSK** la valeur **YES**. Ce paramètre et cette valeur indiquent explicitement que vous comprenez que vous exportez la configuration NPS et que le fichier XML exporté contient des secrets partagés non chiffrés pour les clients RADIUS et les membres des groupes de serveurs RADIUS distants.

Informations d'identification d'administration

Pour réaliser cette procédure, vous devez être membre du groupe Administrateurs.

Pour copier une configuration NPS vers un autre NPS à l'aide des commandes Netsh

1. Sur le serveur NPS source, ouvrez **l'invite de commandes**, tapez **netsh**, puis appuyez sur Entrée.

2. À l'invite **netsh** , tapez **nps**, puis appuyez sur Entrée.

3. À l'invite **netsh nps** , tapez **export filename**="*path\file.xml*" **exportPSK=YES**, où *chemin* est l'emplacement du dossier où vous souhaitez enregistrer le fichier de configuration NPS, et *le fichier* est le nom du fichier XML que vous souhaitez enregistrer. Appuyez sur Entrée.

   Il stocke les paramètres de configuration (y compris les paramètres du Registre) dans un fichier XML. Le chemin peut être relatif ou absolu, ou il peut s'agir d'un chemin d'accès UNC (Universal Naming Convention). Après avoir appuyé sur Entrée, un message s'affiche indiquant si l'exportation vers le fichier a réussi.

4. Copiez le fichier que vous avez créé dans le serveur NPS de destination.

5. À une invite de commandes sur le serveur NPS de destination, entrez **netsh nps import filename**="*path\file.xml*", puis appuyez sur Entrée. Un message s'affiche indiquant si l'importation à partir du fichier XML a réussi.

Références supplémentaires

- Interpréteur de commande réseau (Netsh)

Augmenter les authentifications simultanées traitées par serveur NPS

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour obtenir des instructions sur la configuration des authentifications simultanées du serveur NPS (Network Policy Server).

Si vous avez installé le serveur NPS (Network Policy Server) sur un ordinateur autre qu'un contrôleur de domaine et que le serveur NPS reçoit un grand nombre de demandes d'authentification par seconde, vous pouvez améliorer les performances du serveur NPS en augmentant le nombre d'authentifications simultanées autorisées entre le serveur NPS et le contrôleur de domaine.

Pour ce faire, vous devez modifier la clé de registre suivante :

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`

Ajoutez une nouvelle valeur DWORD nommée **MaxConcurrentApi** et affectez-lui une valeur de 150.

> ⊗ **Attention**
>
> Si vous affectez une valeur à **MaxConcurrentApi** trop élevée, votre serveur NPS peut placer une charge excessive sur votre contrôleur de domaine.

Pour plus d'informations sur MaxConcurrentApi, consultez Comment optimiser les performances pour l'authentification NTLM à l'aide du paramètre MaxConcurrentApi

Pour plus d'informations sur la gestion du serveur NPS (Network Policy Server), consultez Gérer le serveur NPS (Network Policy Server).

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Installer le serveur de stratégie réseau

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour installer le serveur de stratégie réseau (NPS) à l'aide de Windows PowerShell ou de l'Assistant Ajout de rôles et de fonctionnalités. NPS est un service de rôle du rôle serveur Services de stratégie et d'accès réseau.

> ⓘ **Notes**
>
> Par défaut, NPS écoute le trafic RADIUS sur les ports 1812, 1813, 1645 et 1646 sur toutes les cartes réseau installées. Si le Pare-feu Windows avec Advanced Security est activé lorsque vous installez NPS, les exceptions de pare-feu pour ces ports sont automatiquement créées pendant le processus d'installation pour le trafic IPv6 (Internet Protocol version 6) et IPv4. Si vos serveurs d'accès réseau sont configurés pour envoyer le trafic RADIUS sur des ports autres que ceux par défaut, supprimez les exceptions créées dans le Pare-feu Windows avec Advanced Security pendant l'installation de NPS et créez des exceptions pour les ports que vous utilisez pour le trafic RADIUS.

Informations d'identification administratives

Pour effectuer cette procédure, vous devez être membre du groupe **Administrateurs de domaine** .

Pour installer NPS à l'aide de Windows PowerShell

Pour effectuer cette procédure à l'aide de Windows PowerShell, exécutez Windows PowerShell en tant qu'administrateur, tapez la commande suivante, puis appuyez sur Entrée.

```
Install-WindowsFeature NPAS -IncludeManagementTools
```

Pour installer NPS à l'aide du Gestionnaire de serveur

1. Sur NPS1, dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant d'ajout de rôles et de fonctionnalités s'ouvre.

2. Dans **Avant de commencer**, cliquez sur **Suivant**.

> ⓘ **Notes**
>
> La page **Avant de commencer** de l'Assistant Ajout de rôles et de fonctionnalités n'est pas affichée si vous avez précédemment sélectionné **Ignorer cette page par défaut** lorsque l'Assistant Ajout de rôles et de fonctionnalités a été exécuté.

3. Dans **Sélectionner le type d'installation**, vérifiez que **Role-Based ou l'installation basée sur les fonctionnalités** est sélectionnée, puis cliquez sur **Suivant**.

4. Dans **Sélectionner un serveur de destination**, vérifiez que **sélectionnez un serveur à partir du pool de serveurs** . Dans le **pool de serveurs**, vérifiez que l'ordinateur local est sélectionné. Cliquez sur **Suivant**.

5. Dans **Sélectionner des rôles de serveur**, dans **Rôles**, sélectionnez **Stratégie réseau et Services d'accès**. Une boîte de dialogue s'ouvre pour demander s'il doit ajouter des fonctionnalités requises pour les services de stratégie réseau et d'accès. Cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**

6. Dans **Sélectionner des fonctionnalités**, cliquez sur **Suivant**, puis, dans **Stratégie réseau et Services d'accès**, passez en revue les informations fournies, puis cliquez sur **Suivant**.

7. Dans **Sélectionner des services de rôle**, cliquez sur **Serveur de stratégie réseau**. Dans **Ajouter des fonctionnalités requises pour le serveur de stratégie réseau**, cliquez sur **Ajouter des fonctionnalités**. Cliquez sur **Suivant**.

8. Dans **Confirmer les sélections d'installation**, cliquez sur **Redémarrer automatiquement le serveur de destination si nécessaire**. Lorsque vous êtes invité à confirmer cette sélection, cliquez sur **Oui**, puis sur **Installer**. La page Progression de l'installation affiche l'état pendant le processus d'installation. Une fois le processus terminé, le message « Installation réussie sur *ComputerName* » s'affiche, où *ComputerName* est le nom de l'ordinateur sur lequel vous avez installé le serveur de stratégie réseau. Cliquez sur **Fermer**.

Pour plus d'informations, consultez Gérer les serveurs NPS.

Equilibrage de charge du serveur proxy NPS

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Les clients du protocole RADIUS (Remote Authentication Dial-In User Service), qui sont des serveurs d'accès réseau tels que des serveurs de réseau privé virtuel (VPN) et des points d'accès sans fil, créent des demandes de connexion et les envoient aux serveurs RADIUS tels que NPS. Dans certains cas, un serveur NPS (Network Policy Server) peut recevoir un trop grand nombre de demandes de connexion à la fois, ce qui entraîne une dégradation du niveau de performance ou une surcharge. Lorsqu'un serveur NPS est surchargé, il est judicieux d'ajouter d'autres NPS à votre réseau et de configurer l'équilibrage de charge. Lorsque vous répartissez uniformément les demandes de connexion entrantes entre plusieurs serveurs NPS pour éviter la surcharge d'un ou plusieurs NPS, cela est appelé équilibrage de charge.

L'équilibrage de charge est particulièrement utile pour :

- Organisations qui utilisent l'authentification extensible Protocol-Transport Layer Security (EAP-TLS) ou le protocole PEAP (Protected Extensible Authentication Protocol)-TLS pour l'authentification. Étant donné que ces méthodes d'authentification utilisent des certificats pour l'authentification du serveur et pour l'authentification de l'utilisateur ou de l'ordinateur client, la charge sur les proxys RADIUS et les serveurs est plus lourde que lorsque des méthodes d'authentification basées sur un mot de passe sont utilisées.
- Organisations qui ont besoin de maintenir une disponibilité continue des services.
- Fournisseurs de services Internet (ISP) qui externalisent l'accès VPN pour d'autres organisations. Les services VPN externalisés peuvent générer un volume important de trafic d'authentification.

Il existe deux méthodes que vous pouvez utiliser pour équilibrer la charge des demandes de connexion envoyées à vos serveurs NPS :

- Configurez vos serveurs d'accès réseau pour envoyer des demandes de connexion à plusieurs serveurs RADIUS. Par exemple, si vous avez 20 points d'accès sans fil et deux serveurs RADIUS, configurez chaque point d'accès pour envoyer des demandes de connexion aux deux serveurs RADIUS. Vous pouvez équilibrer la charge et fournir un basculement sur chaque serveur d'accès réseau en configurant le serveur d'accès pour envoyer des demandes de connexion à plusieurs serveurs RADIUS dans un ordre de priorité spécifié. Cette méthode d'équilibrage de charge est généralement idéale pour les petites organisations qui ne déploient pas un grand nombre de clients RADIUS.

- Utilisez NPS configuré comme proxy RADIUS pour équilibrer la charge des demandes de connexion entre plusieurs serveurs NPS ou d'autres serveurs RADIUS. Par exemple, si vous avez 100 points d'accès sans fil, un proxy NPS et trois serveurs RADIUS, vous pouvez configurer les points d'accès pour envoyer tout le trafic au proxy NPS. Sur le proxy NPS, configurez l'équilibrage de charge afin que le proxy distribue uniformément les demandes de connexion entre les trois serveurs RADIUS. Cette méthode d'équilibrage de charge est idéale pour les moyennes et grandes organisations qui ont de nombreux clients et serveurs RADIUS.

Dans de nombreux cas, la meilleure approche de l'équilibrage de charge consiste à configurer les clients RADIUS pour envoyer des demandes de connexion à deux serveurs proxy NPS, puis à configurer les proxys NPS pour équilibrer la charge entre les serveurs RADIUS. Cette approche fournit à la fois le basculement et l'équilibrage de charge pour les proxys NPS et les serveurs RADIUS.

Priorité et poids du serveur RADIUS

Pendant le processus de configuration du proxy NPS, vous pouvez créer des groupes de serveurs RADIUS distants, puis ajouter des serveurs RADIUS à chaque groupe. Pour configurer l'équilibrage de charge, vous devez disposer de plusieurs serveurs RADIUS par groupe de serveurs RADIUS distant. Lors de l'ajout de membres du groupe, ou après avoir créé un serveur RADIUS en tant que membre du groupe, vous pouvez accéder à la boîte de dialogue Ajouter un serveur RADIUS pour configurer les éléments suivants sous l'onglet Équilibrage de charge :

- **Priority**. La priorité spécifie l'ordre d'importance du serveur RADIUS pour le serveur proxy NPS. Le niveau de priorité doit se voir attribuer une valeur qui est un entier, par exemple 1, 2 ou 3. Plus le nombre est faible, plus la priorité que le proxy NPS accorde au serveur RADIUS est élevée. Par exemple, si le serveur RADIUS se voit attribuer la priorité la plus élevée de 1, le proxy NPS envoie d'abord les demandes de connexion au serveur RADIUS ; si les serveurs de priorité 1 ne sont pas disponibles, NPS envoie ensuite les demandes de connexion aux serveurs RADIUS avec priorité 2, et ainsi de suite. Vous pouvez attribuer la même priorité à plusieurs serveurs RADIUS, puis utiliser le paramètre Poids pour équilibrer la charge entre eux.

- **Weight**. NPS utilise ce paramètre Poids pour déterminer le nombre de demandes de connexion à envoyer à chaque membre du groupe lorsque les membres du groupe ont le même niveau de priorité. Le paramètre Poids doit se voir attribuer une valeur comprise entre 1 et 100, et la valeur représente un pourcentage de 100 %. Par exemple, si le groupe de serveurs RADIUS distant contient deux membres qui ont tous deux un niveau de priorité de 1 et une évaluation de poids de 50, le proxy NPS transfère 50 % des demandes de connexion à chaque serveur RADIUS.

- **Paramètres avancés**. Ces paramètres de basculement permettent à NPS de déterminer si le serveur RADIUS distant n'est pas disponible. Si NPS détermine qu'un serveur RADIUS n'est pas disponible, il peut commencer à envoyer des demandes de connexion à d'autres membres du groupe. Avec ces paramètres, vous pouvez configurer le nombre de secondes pendant lesquelles le proxy NPS attend une réponse du serveur RADIUS avant qu'il ne considère la demande supprimée ; le nombre maximal de demandes supprimées avant que le proxy NPS identifie le serveur RADIUS comme indisponible ; et le nombre de secondes qui peuvent s'écouler entre les requêtes avant que le proxy NPS identifie le serveur RADIUS comme indisponible.

Configurer l'équilibrage de la charge du proxy NPS

Avant de configurer l'équilibrage de charge, créez un plan de déploiement qui inclut le nombre de groupes de serveurs RADIUS distants dont vous avez besoin, les serveurs qui sont membres de chaque groupe particulier et les paramètres Priorité et Poids pour chaque serveur.

> ⓘ **Notes**
>
> Les étapes suivantes supposent que vous avez déjà déployé et configuré des serveurs RADIUS.

Pour configurer NPS en tant que serveur proxy et transférer les demandes de connexion des clients RADIUS vers des serveurs RADIUS distants, vous devez effectuer les actions suivantes :

1. Déployez vos clients RADIUS (serveurs VPN, serveurs d'accès à distance, serveurs de passerelle Terminal Services, commutateurs d'authentification 802.1X et points d'accès sans fil 802.1X) et configurez-les pour envoyer des demandes de connexion à vos serveurs proxy NPS.

2. Sur le proxy NPS, configurez les serveurs d'accès réseau en tant que clients RADIUS. Pour plus d'informations, consultez Configurer des clients RADIUS.

3. Sur le proxy NPS, créez un ou plusieurs groupes de serveurs RADIUS distants. Au cours de ce processus, ajoutez des serveurs RADIUS aux groupes de serveurs RADIUS distants. Pour plus d'informations, consultez Configurer les groupes de serveur RADIUS à distance.

4. Sur le proxy NPS, pour chaque serveur RADIUS que vous ajoutez à un groupe de serveurs RADIUS distant, cliquez sur l'onglet **Équilibrage de charge** du serveur RADIUS, puis configurez **priorité**, **poids** et **paramètres avancés**.

5. Sur le proxy NPS, configurez des stratégies de demande de connexion pour transférer les demandes d'authentification et de comptabilité aux groupes de serveurs RADIUS distants.

Vous devez créer une stratégie de demande de connexion par groupe de serveurs RADIUS distant. Pour plus d'informations, consultez Configurer les stratégies de demande de connexion.

Inscrire un serveur NPS dans un domaine Active Directory

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour inscrire un serveur exécutant le serveur NPS (Network Policy Server) dans Windows Server 2016 dans le domaine NPS par défaut ou dans un autre domaine.

Inscrire un serveur NPS dans son domaine par défaut

Vous pouvez utiliser cette procédure pour inscrire un serveur NPS (Network Policy Server) dans le domaine auquel appartient le serveur.

Les serveurs NPS (Network Policy Server) doivent être inscrits dans Active Directory pour avoir le droit de lire les propriétés de numérotation des comptes d'utilisateurs pendant le processus d'autorisation. L'inscription d'un serveur NPS ajoute le serveur au groupe **serveurs RAS et IAS** dans Active Directory.

L'appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer ces procédures.

Pour inscrire un serveur NPS dans son domaine par défaut

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console serveur NPS (Network Policy Server) s'ouvre.
2. Cliquez avec le bouton droit sur **NPS (local),** puis cliquez sur **Inscrire le serveur dans Active Directory**. La boîte de dialogue **Serveur de stratégie réseau** s'ouvre.
3. Dans **le serveur de stratégie réseau**, cliquez sur **OK**, puis sur **OK** à nouveau.

Enregistrer un serveur NPS (Network Policy Server) dans un autre domaine

Pour fournir à un serveur NPS l'autorisation de lire les propriétés rendez-vous des comptes d'utilisateur dans Active Directory, le serveur NPS doit être inscrit dans le domaine où résident

les comptes.

Vous pouvez utiliser cette procédure pour inscrire un serveur NPS (Network Policy Server) dans le domaine où le serveur NPS n’est pas membre.

L’appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer ces procédures.

Pour enregistrer un serveur NPS (Network Policy Server) dans un autre domaine

1. Sur le contrôleur de domaine, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. La console Utilisateurs et ordinateurs Active Directory s'ouvre.

2. Dans l’arborescence de la console, accédez au domaine dans lequel vous souhaitez que le serveur NPS lit les informations de compte d’utilisateur, puis cliquez sur le dossier **Utilisateurs** .

3. Dans le volet d’informations, cliquez avec le bouton droit sur **SERVEURs RAS et IAS**, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés des serveurs RAS et IAS** s’ouvre.

4. Dans la boîte de dialogue **Propriétés des serveurs RAS et IAS** , cliquez sur l’onglet **Membres** , ajoutez chacun des serveurs NPS que vous souhaitez inscrire dans le domaine, puis cliquez sur **OK**.

Pour inscrire un serveur NPS dans un autre domaine à l’aide des commandes Netsh pour NPS

1. Ouvrez l’invite de commandes ou Windows PowerShell.

2. Tapez ce qui suit à l’invite de commandes : **netsh nps add registeredserver***domainserver*, puis appuyez sur Entrée.

> ⓘ **Notes**
>
> Dans la commande précédente, *le domaine* est le nom de domaine DNS du domaine dans lequel vous souhaitez inscrire le serveur NPS, et le *serveur* est le nom de l’ordinateur NPS.

Désinscrire un serveur NPS d’un domaine Active Directory

14/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans le processus de gestion de votre déploiement NPS, il peut être utile de déplacer un serveur NPS vers un autre domaine, de remplacer un serveur NPS ou de mettre hors service un serveur NPS.

Lorsque vous déplacez ou désaffectez un serveur NPS, vous pouvez annuler l’inscription du serveur NPS dans les domaines Active Directory où le serveur NPS est autorisé à lire les propriétés des comptes d’utilisateur dans Active Directory.

L’appartenance aux **administrateurs** ou équivalente est la condition minimale requise pour effectuer ces procédures.

Pour annuler l’inscription d’un serveur NPS

1. Sur le contrôleur de domaine, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. La console Utilisateurs et ordinateurs Active Directory s'ouvre.

2. Cliquez sur **Utilisateurs**, puis double-cliquez sur **Serveurs RAS et IAS**.

3. Cliquez sur l’onglet **Membres** , puis sélectionnez le serveur NPS que vous souhaitez annuler l’inscription.

4. Cliquez sur **Supprimer**, sur **Oui**, puis sur **OK**.

Utiliser des expressions régulières dans NPS

08/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cette rubrique explique l'utilisation d'expressions régulières aux fins de la correspondance de modèles dans NPS, dans Windows Server. Vous pouvez utiliser cette syntaxe pour spécifier les conditions des attributs de stratégie réseau et des domaines RADIUS.

> **Notes**
>
> La console NPS et le composant logiciel enfichable MMC NPS présentent une limite de 256 caractères pour tous les paramètres utilisant une valeur de chaîne. Cela inclut tous les paramètres qui peuvent être configurés à l'aide d'expressions régulières. Pour configurer des valeurs de chaîne supérieures à 256 caractères, utilisez les commandes NPS NETSH. Les valeurs de chaîne configurées supérieures à 256 caractères ne peuvent pas être modifiées dans la console NPS ni dans le composant logiciel enfichable MMC NPS sans qu'elles soient invalidées.

Référence de correspondance de motifs

Vous pouvez vous référer au tableau suivant lors de la création d'expressions régulières selon une syntaxe de correspondance de modèles. Notez que les modèles d'expression régulière sont souvent entourés de barres obliques (/).

Agrandir le tableau

Character	Description	Example
`\`	Indique que le caractère qui suit est un caractère spécial ou doit être interprété littéralement.	`/n/ matches the character "n" while the sequence /\n/ matches a line feed or newline character.`
`^`	Correspond au début de l'entrée ou de la ligne.	
`$`	Correspond à la fin de l'entrée ou de la ligne.	
`*`	Correspond au caractère précédant à zéro ou plusieurs reprises.	`/zo*/ matches either "z" or "zoo."`

Character	Description	Example
`+`	Correspond au caractère précédant à une ou plusieurs reprises.	`/zo+/ matches "zoo" but not "z."`
`?`	Correspond au caractère précédant à zéro ou une reprise.	`/a?ve?/ matches the "ve" in "never."`
`.`	Correspond à n'importe quel caractère unique à l'exception d'un caractère de ligne nouvelle.	
`(pattern)`	Correspond à un « modèle » et mémorise la correspondance. Pour faire correspondre les caractères `(` littéraux et `)` (parenthèses), utilisez `\(` ou `\)`.	
`x | y`	Correspond à x ou y.	
`{n}`	Correspond exactement à n reprises (n est un nombre entier non négatif).	`/o{2}/ does not match the "o" in "Bob," but matches the first two instances of the letter o in "foooood."`
`{n,}`	Correspond au moins à n reprises (n est un nombre entier non négatif).	`/o{2,}/ does not match the "o" in "Bob" but matches all of the instances of the letter o in "foooood." /o{1,}/ is equivalent to /o+/.`
`{n,m}`	Correspond à au moins n et à au plus m reprises (m et n sont des nombres entiers non négatifs).	`/o{1,3}/ matches the first three instances of the letter o in "fooooood."`
`[xyz]`	Correspond à l'un des caractères entourés (jeu de caractères).	`/[abc]/ matches the "a" in "plain."`
`[^xyz]`	Correspond à tous les caractères qui ne sont pas entourés (jeu de caractères négatif).	`/[^abc]/ matches the "p" in "plain."`
`\b`	Correspond à une délimitation de mot (par exemple, une espace).	`/ea*r\b/ matches the "er" in "never early."`
`\B`	Correspond à une délimitation de non-mot.	`/ea*r\B/ matches the "ear" in "never early."`
`\d`	Correspond à un caractère numérique (équivalent aux chiffres compris entre 0 et 9).	
`\D`	Correspond à un caractère non numérique (équivalent à `[^0-9]`).	

Character	Description	Example
`\f`	Correspond au caractère de présentation de page suivante.	
`\n`	Correspond au caractère de présentation de ligne suivante.	
`\r`	Correspond à un caractère de retour chariot.	
`\s`	Correspond à n'importe quel caractère d'espace blanche, notamment l'espace, la tabulation et la présentation de page suivante (équivalent à `[ \f\n\r\t\v]`).	
`\S`	Correspond à n'importe quel caractère d'espace non blanche (équivalent à `[^ \f\n\r\t\v]`).	
`\t`	Correspond à un caractère de tabulation.	
`\v`	Correspond à un caractère de tabulation verticale.	
`\w`	Correspond à n'importe quel caractère de mot, notamment le trait de soulignement (équivalent à `[A-Za-z0-9_]`).	
`\W`	Correspond à n'importe quel caractère de non-mot, à l'exclusion du trait de soulignement (équivalent à `[^A-Za-z0-9_]`).	
`\num`	Fait référence aux correspondances mémorisées (`?num`, num état un nombre entier positif). Cette option peut être utilisée uniquement dans la zone **de texte Remplacer** lors de la configuration de la manipulation d'attributs.	`\1` remplace les données stockées dans la première correspondance mémorisée.
`/n/`	Permet l'insertion de codes ASCII dans des expressions régulières (`?n`, n étant une valeur d'échappement octale, hexadécimale ou décimale).	

Exemples d'attributs de stratégie réseau

Les exemples suivants décrivent l'utilisation de la syntaxe de correspondance de modèles pour spécifier des attributs de stratégie réseau :

- Pour spécifier l'ensemble des numéros de téléphone de l'indicatif régional 899, la syntaxe est la suivante :

  `899.*`

- Pour spécifier une plage d'adresses IP commençant par 192.168.1, la syntaxe est la suivante :

  `192\.168\.1\..+`

Exemples de manipulation du nom de domaine dans l'attribut Nom d'utilisateur

> ⓘ **Notes**
>
> La manipulation de domaine ne fonctionne pas avec le protocole PEAP.
> Le comportement souhaité peut être obtenu en effectuant une commutation vers EAP-TLS ou EAP-MSCHAPv2 aux fins de l'authentification, ou **en ajoutant un suffixe UPN au domaine** pour chaque nom de domaine supplémentaire à résoudre.

Les exemples suivants décrivent l'utilisation de la syntaxe de correspondance de modèle pour manipuler les noms de domaine pour l'attribut Nom d'utilisateur, qui se trouve sous l'onglet **Attribut** dans les propriétés d'une stratégie de demande de connexion.

Pour supprimer la partie de domaine de l'attribut Nom d'utilisateur

Dans un scénario d'accès par ligne commutée externalisé dans lequel un fournisseur de services Internet (ISP) achemine les demandes de connexion vers un serveur NPS de l'organisation, le proxy RADIUS du fournisseur de services Internet peut nécessiter un nom de domaine pour acheminer la demande d'authentification. Toutefois, le serveur NPS peut ne pas reconnaître la partie de nom de domaine du nom d'utilisateur. Par conséquent, le nom de domaine doit être supprimé par le proxy RADIUS du fournisseur de services Internet avant d'être transféré au serveur NPS de l'organisation.

- Trouver : @microsoft\.com

- Replace:

Pour remplacer *user@example.microsoft.com* par *example.microsoft.com\user*

- Trouver: `(.*)@(.*)`

- Remplacer: `$2\$1`

Pour remplacer *domain\user* par *specific_domain\user*

- Trouver: `(.*)\\(.*)`

- Remplacer : *specific_domain* `\$2`

Pour remplacer *user* par *user@specific_domain*

- Trouver: `$`
- Remplacer : @*specific_domain*

Exemple de transfert de message RADIUS par un serveur proxy

Vous pouvez créer des règles de routage qui transfèrent des messages RADIUS présentant un nom de domaine spécifié à un jeu de serveurs RADIUS lorsque le serveur NPS est utilisé en tant que proxy RADIUS. La syntaxe suivante est recommandée pour le routage des demandes selon le nom de domaine.

- **Nom NetBIOS** : `WCOAST`
- **Modèle** : `^wcoast\\`

Dans l'exemple suivant, wcoast.microsoft.com est un suffixe de nom principal d'utilisateur unique (UPN) pour le domaine DNS ou Active Directory wcoast.microsoft.com. À l'aide du modèle fourni, le proxy NPS peut acheminer les messages en fonction du nom netBIOS de domaine ou du suffixe UPN.

- **Nom NetBIOS** : `WCOAST`
- **Suffixe UPN** : `wcoast.microsoft.com`
- **Modèle** : `^wcoast\\|@wcoast\.microsoft\.com$`

Pour plus d'informations sur la gestion du serveur NPS (Network Policy Server), consultez Gérer le serveur NPS (Network Policy Server).

Pour plus d'informations sur le serveur NPS (Network Policy Server), consultez Serveur NPS (Network Policy Server).

Vérifier la configuration après des changements sur le serveur NPS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour vérifier la configuration NPS après un changement d'adresse IP ou de nom sur le serveur.

Vérifier la configuration après un changement d'adresse IP NPS

Dans certains cas, vous pouvez avoir besoin de changer l'adresse IP d'un proxy ou serveur NPS, par exemple, quand vous déplacez le serveur vers un autre sous-réseau IP.

Si vous changez l'adresse IP d'un proxy ou serveur NPS, vous devez reconfigurer des parties de votre déploiement NPS.

Utilisez le guide général suivant pour vous aider à vérifier qu'un changement d'adresse IP n'interrompt pas l'authentification, l'autorisation ou la gestion des comptes d'accès réseau sur votre réseau pour les serveurs RADIUS NPS et les serveurs proxy RADIUS.

Vous devez être membre des **administrateurs** ou équivalents pour effectuer ces procédures.

Pour vérifier la configuration après un changement d'adresse IP NPS

1. Reconfigurez tous les clients RADIUS, comme les points d'accès sans fil et les serveurs VPN, avec la nouvelle adresse IP du serveur NPS.

2. Si le serveur NPS est membre d'un groupe de serveurs RADIUS distants, reconfigurez le proxy NPS avec la nouvelle adresse IP du serveur NPS.

3. Si vous avez configuré le serveur NPS pour utiliser la journalisation SQL Server, vérifiez que la connectivité entre l'ordinateur exécutant SQL Server et le serveur NPS fonctionne toujours correctement.

4. Si vous avez déployé IPsec pour sécuriser le trafic RADIUS entre votre serveur NPS et un proxy NPS ou d'autres serveurs ou appareils, reconfigurez la stratégie IPsec ou la règle de

sécurité de connexion dans le Pare-feu Windows avec Advanced Security pour utiliser la nouvelle adresse IP du serveur NPS.

5. Si le serveur NPS est multihébergé et que vous avez configuré le serveur pour qu'il soit lié à une carte réseau spécifique, reconfigurez les paramètres de port NPS avec la nouvelle adresse IP.

Pour vérifier la configuration après un changement d'adresse IP du proxy NPS

1. Reconfigurez tous les clients RADIUS, comme les points d'accès sans fil et les serveurs VPN, avec la nouvelle adresse IP du proxy NPS.

2. Si le proxy NPS est multihébergé et que vous avez configuré le proxy pour qu'il soit lié à une carte réseau spécifique, reconfigurez les paramètres de port NPS avec la nouvelle adresse IP.

3. Reconfigurez tous les membres de tous les groupes de serveurs RADIUS distants avec l'adresse IP du serveur proxy. Pour ce faire, au niveau de chaque serveur NPS qui a le proxy NPS configuré comme client RADIUS :

   a. Double-cliquez sur **NPS (local),** double-cliquez sur **Clients et serveurs RADIUS**, cliquez sur **Clients RADIUS**, puis dans le volet d'informations, double-cliquez sur le client RADIUS que vous souhaitez modifier.

   b. Dans **les propriétés** du client RADIUS, dans **Adresse (IP ou DNS),** tapez la nouvelle adresse IP du proxy NPS.

4. Si vous avez configuré le proxy NPS pour utiliser la journalisation SQL Server, vérifiez que la connectivité entre l'ordinateur exécutant SQL Server et le proxy NPS fonctionne toujours correctement.

Vérifier la configuration après le renommage d'un serveur NPS

Dans certains cas, vous pouvez avoir besoin de changer le nom d'un serveur NPS ou d'un proxy, par exemple, quand vous reconcevez les conventions de nommage de vos serveurs.

Si vous changez le nom d'un proxy ou serveur NPS, vous devez reconfigurer des parties de votre déploiement NPS.

Utilisez le guide général suivant pour vous aider à vérifier que le changement de nom d'un serveur n'interrompt pas l'authentification, l'autorisation ou la gestion des comptes d'accès réseau.

Vous devez être membre des **administrateurs** ou équivalents pour effectuer cette procédure.

Pour vérifier la configuration après un changement de nom du serveur NPS ou du proxy

1. Si le serveur NPS est membre d'un groupe de serveurs RADIUS distants et que le groupe est configuré avec des noms d'ordinateur plutôt que des adresses IP, reconfigurez le groupe de serveurs RADIUS distants avec le nouveau nom NPS.

2. Si des méthodes d'authentification basée sur un certificat sont déployées sur le serveur NPS, le changement de nom rend non valide le certificat de serveur. Vous pouvez demander un nouveau certificat à l'administrateur de l'autorité de certification ou, si l'ordinateur est un membre du domaine et que vous inscrivez automatiquement des certificats sur les membres de domaine, vous pouvez actualiser la stratégie de groupe pour obtenir un nouveau certificat à travers l'inscription automatique. Pour actualiser la stratégie de groupe :

   a. Ouvrez l'invite de commandes ou Windows PowerShell.

   b. Tapez **gpupdate**, puis appuyez sur Entrée.

3. Une fois que vous avez un nouveau certificat de serveur, demandez à l'administrateur de l'autorité de certification de révoquer l'ancien certificat.

   Une fois l'ancien certificat révoqué, le serveur NPS continue à l'utiliser jusqu'à ce que l'ancien certificat expire. Par défaut, l'ancien certificat reste valide pendant une durée maximale d'une semaine et 10 heures. Cette période peut varier selon que l'expiration de la liste de révocation de certificats (CRL) et l'expiration de la durée du cache TLS (Transport Layer Security) ont été modifiées par rapport aux valeurs par défaut. L'expiration de la liste CRL est définie par défaut sur une semaine, celle du cache TLS sur 10 heures.

   Toutefois, si vous souhaitez configurer le serveur NPS pour utiliser immédiatement le nouveau certificat, vous pouvez reconfigurer manuellement les stratégies réseau avec le nouveau certificat.

4. Une fois l'ancien certificat expiré, le serveur NPS commence automatiquement à utiliser le nouveau certificat.

5. Si vous avez configuré le serveur NPS pour utiliser la journalisation SQL Server, vérifiez que la connectivité entre l'ordinateur exécutant SQL Server et le serveur NPS fonctionne toujours correctement.

Collecte des données utilisateur du serveur de stratégie réseau

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Ce document explique comment rechercher les informations utilisateur collectées par le serveur de stratégie réseau (NPS) si vous souhaitez la supprimer.

> **Notes**
>
> Si vous voulez voir ou supprimer des données personnelles, consultez les conseils de Microsoft sur le site Demandes des personnes concernées pour Windows concernant le RGPD. Si vous recherchez des informations générales sur le RGPD, consultez la section RGPD du portail d'approbation de services.

Informations collectées par NPS

- Timestamp
- Horodateur d'événements
- Username
- Nom d'utilisateur complet
- Adresse IP du client
- Fournisseur du client
- Nom convivial du client
- Type d'authentification
- De nombreux autres champs concernant le protocole RADIUS

Collecter des données à partir de NPS

Si les données comptables sont activées et configurées, les enregistrements des tentatives d'authentification NPS d'un utilisateur peuvent être obtenus à partir de SQL Server ou des fichiers journaux en fonction de la configuration.

Si les données de comptabilité sont configurées pour SQL Server, interrogez tous les enregistrements WHERE User_Name = `'<username>'`.

Si les données comptables sont configurées pour un fichier journal, recherchez dans ce fichier journal le `<username>` pour trouver toutes les entrées de journal.

Les entrées du journal des événements Network Policy et Access Services sont considérées comme duplicatives aux données comptables et n’ont pas besoin d’être collectées.

Si les données comptables ne sont pas activées, les enregistrements des tentatives d'authentification NPS d'un utilisateur peuvent être obtenus à partir du journal des événements des Services de stratégie de réseau et d'accès en recherchant le `<username>`.

Gérer les modèles NPS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser des modèles NPS (Network Policy Server) pour créer des éléments de configuration, comme des clients RADIUS (Remote Authentication Dial-In User Service) ou des secrets partagés, que vous pouvez réutiliser sur le serveur NPS local et exporter pour une utilisation sur d'autres serveurs NPS.

Gestion des modèles fournit un nœud dans la console NPS où vous pouvez créer, modifier, supprimer, dupliquer et consulter l'utilisation de modèles NPS. Les modèles NPS sont conçus pour réduire le temps et le coût nécessaires pour configurer NPS sur un ou plusieurs serveurs.

Les types de modèles NPS suivants peuvent être configurés dans Gestion des modèles.

- **Secrets partagés**. Ce type de modèle vous permet de spécifier un secret partagé que vous pouvez réutiliser (en sélectionnant le modèle à l'emplacement approprié dans la console NPS) quand vous configurez des clients et serveurs RADIUS.
- **Clients RADIUS**. Ce type de modèle vous permet de configurer des paramètres de client RADIUS que vous pouvez réutiliser en sélectionnant le modèle à l'emplacement approprié dans la console NPS.
- **Serveurs RADIUS distants**. Ce modèle vous permet de configurer des paramètres de serveur RADIUS distant que vous pouvez réutiliser en sélectionnant le modèle à l'emplacement approprié dans la console NPS.
- **Filtres IP**. Ce modèle vous permet de créer des filtres IPv4 (Internet Protocol version 4) et IPv6 (Internet Protocol version 6) que vous pouvez réutiliser (en sélectionnant le modèle à l'emplacement approprié dans la console NPS) quand vous configurez des stratégies réseau.

Créer un modèle NPS

La configuration d'un modèle diffère de la configuration directe du serveur NPS. La création d'un modèle n'affecte pas la fonctionnalité du serveur NPS. C'est seulement quand vous sélectionnez le modèle à l'emplacement approprié dans la console NPS et que vous appliquez le modèle que le modèle affecte la fonctionnalité NPS.

Par exemple, si vous configurez un client RADIUS dans la console NPS sous **Clients et serveurs RADIUS**, vous modifiez la configuration NPS pour que le serveur NPS communique avec un de

vos serveurs d'accès réseau. (L'étape suivante est de configurer le serveur d'accès réseau (NAS) pour communiquer avec le serveur NPS.)

Toutefois, si vous configurez un nouveau modèle **de clients RADIUS** dans la console NPS sous **Gestion des** modèles plutôt que de créer un client **RADIUS sous Clients et serveurs RADIUS**, vous avez créé un modèle, mais vous n'avez pas encore modifié la fonctionnalité NPS. Pour modifier la fonctionnalité NPS, vous devez appliquer le modèle à partir de l'emplacement approprié dans la console NPS.

La procédure suivante fournit des instructions pour créer un modèle.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour créer un modèle NPS

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.
2. Dans la console NPS, développez **Gestion des modèles**, cliquez avec le bouton droit sur un type de modèle, tel que **les clients RADIUS**, puis cliquez sur **Nouveau**.
3. Une nouvelle boîte de dialogue de propriétés de modèle s'ouvre, où vous pouvez configurer votre modèle.

Appliquer un modèle NPS

Vous pouvez utiliser un modèle que vous avez créé dans **Gestion des modèles** en accédant à un emplacement dans la console NPS où vous pouvez appliquer le modèle. Par exemple, si vous souhaitez appliquer un modèle Secrets partagés à une configuration de client RADIUS, vous pouvez utiliser la procédure suivante.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour appliquer un modèle NPS

1. Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur Serveur de stratégie **réseau**. La console NPS s'ouvre.
2. Dans la console NPS, développez **Clients et serveurs RADIUS**, puis **Clients RADIUS**.

3.In **clients RADIUS**, dans le volet d'informations, cliquez avec le bouton droit sur le client RADIUS auquel vous souhaitez appliquer le modèle NPS, puis cliquez sur **Propriétés**.

4. Dans la boîte de dialogue des propriétés du client RADIUS, dans **Sélectionner un modèle de secrets partagés existant**, sélectionnez le modèle à appliquer dans la liste des modèles.

Exporter ou importer des modèles NPS

Vous pouvez exporter des modèles à utiliser sur d'autres serveurs NPS, ou vous pouvez importer des modèles dans **Gestion des modèles** à utiliser sur l'ordinateur local.

L'appartenance aux **administrateurs**, ou équivalente, est la condition minimale requise pour effectuer cette procédure.

Pour exporter ou importer des modèles NPS

1. Pour exporter des modèles NPS, dans la console NPS, cliquez avec le bouton droit sur **Gestion des modèles**, puis cliquez sur **Exporter des modèles dans un fichier**.

2. Pour importer des modèles NPS, dans la console NPS, cliquez avec le bouton droit sur **Gestion des modèles**, puis cliquez sur **Importer des modèles à partir d'un ordinateur ou importez** des **modèles à partir d'un fichier**.

Réglage des performances du sous-système réseau

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour une vue d'ensemble du sous-système réseau et pour obtenir des liens vers d'autres rubriques de ce guide.

> ⓘ **Notes**
>
> En plus de cette rubrique, les sections suivantes de ce guide fournissent des recommandations de réglage des performances pour les appareils réseau et la pile réseau.
>
> - Choix d'une carte réseau
> - Configurer l'ordre des interfaces réseau
> - Réglage des performances des cartes réseau
> - Compteurs de performance liées au réseau
> - Outils d'analyse des performances pour les charges de travail de réseau

L'optimisation des performances du sous-système réseau, en particulier pour les charges de travail réseau intensives, peut impliquer chaque couche de l'architecture réseau, qui est également appelée pile réseau. Ces couches sont largement divisées dans les sections suivantes.

1. **Interface réseau**. Il s'agit de la couche la plus basse de la pile réseau et elle contient le pilote réseau qui communique directement avec l'adaptateur réseau.

2. **Spécification de l'interface du pilote réseau (NDIS)**. NDIS expose des interfaces pour le pilote en dessous et pour les couches supérieures, telles que la pile de protocoles.

3. **Pile de protocoles**. La pile de protocoles implémente des protocoles tels que TCP/IP et UDP/IP. Ces couches exposent l'interface de couche de transport pour les couches situées au-dessus d'elles.

4. **Pilotes système**. Il s'agit généralement de clients qui utilisent une extension TDX (transport data extension) ou une interface WSK (Winsock Kernel) pour exposer des interfaces aux applications en mode utilisateur. L'interface WSK a été introduite dans Windows Server 2008 et Windows® Vista, et elle est exposée par AFD.sys. L'interface

améliore les performances en éliminant le basculement entre le mode utilisateur et le mode noyau.

5. **applicationsUser-Mode**. Il s'agit généralement de solutions Microsoft ou d'applications personnalisées.

Le tableau ci-dessous fournit une illustration verticale des couches de la pile réseau, y compris des exemples d'éléments qui s'exécutent dans chaque couche.

5	**User-Mode Applications**	WMS	DNS	IIS
4	**System Drivers**	AFD.sys	HTTP.sys	
3	**Protocol Stack**	TCP/IP	UDP/IP	VPN
2	**NDIS**	Network Driver Interface Specification (NDIS)		
1	**Network interface**	Network driver		

Choix d'une carte réseau

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour découvrir certaines des fonctionnalités des adaptateurs réseau qui peuvent affecter vos choix d'achat.

Les applications gourmandes en réseau nécessitent des cartes réseau hautes performances. Cette section explore certaines considérations relatives au choix des adaptateurs réseau, ainsi que la façon de configurer différents paramètres d'adaptateur réseau pour obtenir les meilleures performances réseau.

> **Conseil**
>
> Vous pouvez configurer les paramètres d'adaptateur réseau à l'aide de Windows PowerShell. Pour plus d'informations, consultez **Applets de commande d'adaptateurs réseau dans Windows PowerShell**.

Fonctionnalités de déchargement

Le déchargement des tâches de l'unité de traitement centrale (UC) vers l'adaptateur réseau peut réduire l'utilisation du processeur sur le serveur, ce qui améliore les performances globales du système.

La pile réseau dans les produits Microsoft peut décharger une ou plusieurs tâches sur un adaptateur réseau si vous sélectionnez un adaptateur réseau qui dispose des fonctionnalités de déchargement appropriées. Le tableau suivant fournit une brève vue d'ensemble des différentes fonctionnalités de déchargement disponibles dans Windows Server 2016.

Agrandir le tableau

Type de déchargement	Description
Calcul de la somme de contrôle pour TCP	La pile réseau peut décharger le calcul et la validation des sommes de contrôle TCP (Transmission Control Protocol) sur les chemins d'envoi et de réception du code. Il peut également décharger le calcul et la validation des sommes de contrôle IPv4 et IPv6 sur les chemins d'envoi et de réception du code.
Calcul de la somme de contrôle pour	La pile réseau peut décharger le calcul et la validation des sommes de contrôle UDP (User Datagram Protocol) sur les chemins d'accès d'envoi et de réception du

Type de déchargement	Description
UDP	code.
Calcul de la somme de contrôle pour IPv4	La pile réseau peut décharger le calcul et la validation des sommes de contrôle IPv4 sur les chemins d'envoi et de réception du code.
Calcul de la somme de contrôle pour IPv6	La pile réseau peut décharger le calcul et la validation des sommes de contrôle IPv6 sur les chemins d'accès au code d'envoi et de réception.
Segmentation des paquets TCP volumineux	La couche de transport TCP/IP prend en charge le déchargement d'envoi volumineux v2 (LSOv2). Avec LSOv2, la couche de transport TCP/IP peut décharger la segmentation de paquets TCP volumineux sur la carte réseau.
RSS (Receive Side Scaling)	RSS est une technologie de pilote réseau qui permet une distribution efficace du traitement des réceptions réseau entre plusieurs processeurs dans les systèmes multiprocesseurs. Plus de détails sur RSS sont fournis plus loin dans cette rubrique.
Fusion de segment de réception (RSC)	RSC est la possibilité de regrouper les paquets afin de réduire le traitement d'en-tête nécessaire à l'exécution de l'hôte. Un maximum de 64 Ko de charge utile reçue peut être fusionné en un seul paquet plus grand pour le traitement. Plus de détails sur RSC sont fournis plus loin dans cette rubrique.

Partage du trafic entrant

Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008 R2, et Windows Server 2008 prennent en charge le partage du trafic entrant (RSS, Receive Side Scaling).

Certains serveurs sont configurés avec plusieurs processeurs logiques qui partagent des ressources matérielles (comme un cœur physique) et qui sont traités comme des homologues multithreading (SMT) simultanés. La technologie Intel Hyper-Threading en est un exemple. RSS dirige le traitement réseau vers jusqu'à un processeur logique par cœur. Par exemple, sur un serveur avec Intel Hyper-Threading, 4 cœurs et 8 processeurs logiques, RSS n'utilise pas plus de 4 processeurs logiques pour le traitement réseau.

RSS distribue les paquets d'E/S réseau entrants entre les processeurs logiques afin que les paquets qui appartiennent à la même connexion TCP soient traités sur le même processeur logique, ce qui préserve l'ordre.

RSS équilibre également la charge du trafic de monodiffusion et de multidiffusion UDP, et achemine les flux associés (qui sont déterminés par le hachage des adresses source et de destination) vers le même processeur logique, en conservant l'ordre des arrivées associées. Cela permet d'améliorer la scalabilité et les performances des scénarios nécessitant beaucoup

de réception pour les serveurs qui ont moins d'adaptateurs réseau que les processeurs logiques éligibles.

Configuration de RSS

Dans Windows Server 2016, vous pouvez configurer RSS à l'aide d'applets de commande Windows PowerShell et de profils RSS.

Vous pouvez définir des profils RSS à l'aide du paramètre **–Profile** de l'applet de commande Windows PowerShell **Set-NetAdapterRss** .

Commandes Windows PowerShell pour la configuration RSS

Les applets de commande suivantes vous permettent de voir et de modifier les paramètres RSS par adaptateur réseau.

> ⓘ **Notes**
>
> Pour obtenir une référence de commande détaillée pour chaque applet de commande, y compris la syntaxe et les paramètres, vous pouvez cliquer sur les liens suivants. En outre, vous pouvez transmettre le nom de l'applet de commande à **Get-Help** à l'invite Windows PowerShell pour plus d'informations sur chaque commande.

- Disable-NetAdapterRss. Cette commande désactive RSS sur l'adaptateur réseau que vous spécifiez.
- Enable-NetAdapterRss. Cette commande active RSS sur l'adaptateur réseau que vous spécifiez.
- Get-NetAdapterRss. Cette commande récupère les propriétés RSS de la carte réseau que vous spécifiez.
- Set-NetAdapterRss. Cette commande définit les propriétés RSS sur l'adaptateur réseau que vous spécifiez.

Profils RSS

Vous pouvez utiliser le paramètre **–Profile** de l'applet de commande Set-NetAdapterRss pour spécifier les processeurs logiques auxquels sont attribués la carte réseau. Les valeurs disponibles pour ce paramètre sont les suivantes :

- **Closest**. Les numéros de processeur logiques proches du processeur RSS de base de l'adaptateur réseau sont préférés. Avec ce profil, le système d'exploitation peut

rééquilibrer les processeurs logiques dynamiquement en fonction de la charge.

- **ClosestStatic**. Les numéros de processeur logiques proches du processeur RSS de base de l'adaptateur réseau sont préférés. Avec ce profil, le système d'exploitation ne rééquilibrée pas dynamiquement les processeurs logiques en fonction de la charge.
- **NUMA**. Les numéros de processeur logique sont généralement sélectionnés sur différents nœuds NUMA pour distribuer la charge. Avec ce profil, le système d'exploitation peut rééquilibrer les processeurs logiques dynamiquement en fonction de la charge.
- **NUMAStatic**. Il s'agit du **profil par défaut**. Les numéros de processeur logique sont généralement sélectionnés sur différents nœuds NUMA pour distribuer la charge. Avec ce profil, le système d'exploitation ne rééquilibrera pas dynamiquement les processeurs logiques en fonction de la charge.
- **Conservative**. RSS utilise le moins de processeurs possible pour gérer la charge. Cette option aide à réduire le nombre d'interruptions.

Selon le scénario et les caractéristiques de la charge de travail, vous pouvez également utiliser d'autres paramètres de l'applet de commande Windows PowerShell **Set-NetAdapterRss** pour spécifier les éléments suivants :

- Par carte réseau, combien de processeurs logiques peuvent être utilisés pour RSS.
- Décalage de départ de la plage de processeurs logiques.
- Nœud à partir duquel la carte réseau alloue de la mémoire.

Voici les paramètres **Set-NetAdapterRs supplémentaires** que vous pouvez utiliser pour configurer RSS :

> ⓘ **Notes**
>
> Dans l'exemple de syntaxe de chaque paramètre ci-dessous, le nom de la carte réseau **Ethernet** est utilisé comme exemple de valeur pour le paramètre **–Name** de la commande **Set-NetAdapterRss** . Lorsque vous exécutez l'applet de commande, vérifiez que le nom de la carte réseau que vous utilisez est approprié pour votre environnement.

- * **MaxProcessors** : définit le nombre maximal de processeurs RSS à utiliser. Cela garantit que le trafic d'application est lié à un nombre maximal de processeurs sur une interface donnée. Exemple de syntaxe :

  ```
  Set-NetAdapterRss –Name "Ethernet" –MaxProcessors <value>
  ```

- * **BaseProcessorGroup** : définit le groupe de processeurs de base d'un nœud NUMA. Cela a un impact sur le tableau de processeurs utilisé par RSS. Exemple de syntaxe :

```
Set-NetAdapterRss -Name "Ethernet" -BaseProcessorGroup <value>
```

- * **MaxProcessorGroup** : définit le groupe de processeurs Max d'un nœud NUMA. Cela a un impact sur le tableau de processeurs utilisé par RSS. Cette définition restreindrait un groupe de processeurs maximal afin que l'équilibrage de charge soit aligné dans un groupe k. Exemple de syntaxe :

  ```
  Set-NetAdapterRss -Name "Ethernet" -MaxProcessorGroup <value>
  ```

- * **BaseProcessorNumber** : définit le numéro de processeur de base d'un nœud NUMA. Cela a un impact sur le tableau de processeurs utilisé par RSS. Cela permet de partitionner des processeurs sur plusieurs cartes réseau. Il s'agit du premier processeur logique dans la plage de processeurs RSS qui est affecté à chaque adaptateur. Exemple de syntaxe :

  ```
  Set-NetAdapterRss -Name "Ethernet" -BaseProcessorNumber <Byte Value>
  ```

- * **NumaNode : nœud NUMA** à partir duquel chaque carte réseau peut allouer de la mémoire. Il peut s'agir d'un k-groupe ou de k-groupes différents. Exemple de syntaxe :

  ```
  Set-NetAdapterRss -Name "Ethernet" -NumaNodeID <value>
  ```

- * **NumberofReceiveQueues** : si vos processeurs logiques semblent sous-utilisés pour le trafic de réception (par exemple, comme indiqué dans le Gestionnaire des tâches), vous pouvez essayer d'augmenter le nombre de files d'attente RSS de la valeur par défaut de 2 à la valeur maximale prise en charge par votre carte réseau. Votre adaptateur réseau peut proposer des options permettant de changer le nombre de files d'attente RSS dans le pilote. Exemple de syntaxe :

  ```
  Set-NetAdapterRss -Name "Ethernet" -NumberOfReceiveQueues <value>
  ```

Pour plus d'informations, cliquez sur le lien suivant pour télécharger Mise en réseau scalable : élimination du goulot d'étranglement du traitement de réception — Présentation de RSS au format Word.

Présentation des performances RSS

Le paramétrage RSS nécessite de comprendre la configuration et la logique d'équilibrage de charge. Pour vérifier que les paramètres RSS ont pris effet, vous pouvez passer en revue la sortie lorsque vous exécutez l'applet de commande Windows PowerShell **Get-NetAdapterRss** . Voici un exemple de sortie de cette applet de commande.

```
PS C:\Users\Administrator> get-netadapterrss
Name                            : testnic 2
InterfaceDescription            : Broadcom BCM5708C NetXtreme II GigE (NDIS VBD
Client) #66
Enabled                         : True
NumberOfReceiveQueues           : 2
Profile                         : NUMAStatic
BaseProcessor: [Group:Number]   : 0:0
MaxProcessor: [Group:Number]    : 0:15
MaxProcessors                   : 8

IndirectionTable: [Group:Number]:
     0:0    0:4    0:0    0:4    0:0    0:4    0:0    0:4
…
(# indirection table entries are a power of 2 and based on # of processors)
…
                           0:0    0:4    0:0    0:4    0:0    0:4    0:0    0:4
```

Outre l'écho des paramètres qui ont été définis, l'aspect clé de la sortie est la sortie de la table d'indirection. La table d'indirection affiche les compartiments de table de hachage utilisés pour distribuer le trafic entrant. Dans cet exemple, la notation n:c désigne la paire d'index Numa K-Group:CPU utilisée pour diriger le trafic entrant. Nous voyons exactement 2 entrées uniques (0:0 et 0:4), qui représentent respectivement k-group 0/cpu0 et k-group 0/cpu 4.

Il n'existe qu'un k-group pour ce système (k-group 0) et une entrée de table d'indirection n (où n <= 128). Étant donné que le nombre de files d'attente de réception est défini sur 2, seuls 2 processeurs (0:0, 0:4) sont choisis, même si le nombre maximal de processeurs est défini sur 8. En effet, la table d'indirection hachage le trafic entrant pour utiliser uniquement 2 processeurs sur les 8 disponibles.

Pour utiliser pleinement les processeurs, le nombre de files d'attente de réception RSS doit être égal ou supérieur au nombre maximal de processeurs. Dans l'exemple précédent, la file d'attente de réception doit être définie sur 8 ou plus.

Association d'adaptateurs réseau et RSS

RSS peut être activé sur un adaptateur réseau qui est associé à un autre adaptateur d'interface réseau à l'aide de l'association d'adaptateurs réseau. Dans ce scénario, seule l'adaptateur réseau physique sous-jacent peut être configuré pour utiliser RSS. Un utilisateur ne peut pas définir d'applets de commande RSS sur l'adaptateur réseau associé.

Fusion de segment de réception (RSC)

Receive Segment Coalescing (RSC) améliore les performances en réduisant le nombre d'en-têtes IP qui sont traités pour une quantité donnée de données reçues. Il doit être utilisé pour aider à mettre à l'échelle les performances des données reçues en regroupant (ou en fusionnant) les paquets plus petits en unités plus grandes.

Cette approche peut affecter la latence avec des avantages principalement observés dans les gains de débit. RSC est recommandé pour augmenter le débit pour les charges de travail lourdes reçues. Envisagez de déployer des adaptateurs réseau qui prennent en charge RSC.

Sur ces cartes réseau, assurez-vous que RSC est activé (il s'agit du paramètre par défaut), sauf si vous avez des charges de travail spécifiques (par exemple, une faible latence, un réseau à faible débit) qui montrent que RSC est désactivé.

Présentation des diagnostics RSC

Vous pouvez diagnostiquer RSC à l'aide des applets de commande Windows PowerShell **Get-NetAdapterRsc** et **Get-NetAdapterStatistics**.

Voici un exemple de sortie lorsque vous exécutez l'applet de commande Get-NetAdapterRsc.

```
PS C:\Users\Administrator> Get-NetAdapterRsc

Name                        IPv4Enabled  IPv6Enabled  IPv4Operational
IPv6Operational               IPv4FailureReason              IPv6Failure
                                              Reason
----                           -----------  -----------  --------------- ---------
------ ----------------- ------------
Ethernet                        True         False        True            False
NoFailure       NicProperties
```

L'applet de commande **Get** indique si RSC est activé dans l'interface et si TCP permet à RSC d'être dans un état opérationnel. La raison de l'échec fournit des détails sur l'échec d'activation de RSC sur cette interface.

Dans le scénario précédent, IPv4 RSC est pris en charge et opérationnel dans l'interface. Pour comprendre les échecs de diagnostic, vous pouvez voir les octets fusionnés ou les exceptions provoqués. Cela donne une indication des problèmes de fusion.

Voici un exemple de sortie lorsque vous exécutez l'applet de commande Get-NetAdapterStatistics.

```
PS C:\Users\Administrator> $x = Get-NetAdapterStatistics "myAdapter"
PS C:\Users\Administrator> $x.rscstatistics

CoalescedBytes       : 0
CoalescedPackets     : 0
CoalescingEvents     : 0
CoalescingExceptions : 0
```

RSC et virtualisation

RSC est uniquement pris en charge dans l'hôte physique lorsque l'adaptateur réseau hôte n'est pas lié au commutateur virtuel Hyper-V. RSC est désactivé par le système d'exploitation lorsque l'hôte est lié au commutateur virtuel Hyper-V. En outre, les machines virtuelles ne bénéficient pas de RSC, car les adaptateurs réseau virtuels ne prennent pas en charge RSC.

RSC peut être activé pour une machine virtuelle lorsque la virtualisation d'entrée/sortie racine unique (SR-IOV) est activée. Dans ce cas, les fonctions virtuelles prennent en charge la fonctionnalité RSC ; par conséquent, les machines virtuelles bénéficient également de RSC.

Ressources des adaptateurs réseau

Quelques adaptateurs réseau gèrent activement leurs ressources pour obtenir des performances optimales. Plusieurs cartes réseau vous permettent de configurer manuellement des ressources à l'aide de l'onglet **Mise en réseau avancée** pour la carte. Pour ces adaptateurs, vous pouvez définir les valeurs d'un certain nombre de paramètres, y compris le nombre de mémoires tampons de réception et d'envoi de mémoires tampons.

La configuration des ressources d'adaptateur réseau est simplifiée par l'utilisation des applets de commande Windows PowerShell suivantes.

- Get-NetAdapterAdvancedProperty
- Set-NetAdapterAdvancedProperty
- Enable-NetAdapter
- Enable-NetAdapterBinding
- Enable-NetAdapterChecksumOffload
- Enable-NetAdapterIPSecOffload
- Enable-NetAdapterLso

- Enable-NetAdapterPowerManagement
- Enable-NetAdapterQos
- Enable-NetAdapterRDMA
- Enable-NetAdapterSriov

Pour plus d'informations, consultez Applets de commande d'adaptateurs réseau dans Windows PowerShell.

Pour obtenir des liens vers toutes les rubriques de ce guide, consultez Réglage des performances du sous-système réseau.

Configurer l'ordre des interfaces réseau

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Dans Windows Server 2016 et Windows 10, vous pouvez utiliser la métrique d'interface pour configurer l'ordre des interfaces réseau.

Cela est différent dans les versions précédentes de Windows et Windows Server, ce qui vous a permis de configurer l'ordre de liaison des cartes réseau à l'aide de l'interface utilisateur ou des commandes **INetCfgComponentBindings ::MoveBefore** et **INetCfgComponentBindings ::MoveAfter**. Ces deux méthodes de classement des interfaces réseau ne sont pas disponibles dans Windows Server 2016 et Windows 10.

À la place, vous pouvez utiliser la nouvelle méthode pour définir l'ordre énuméré des cartes réseau en configurant la métrique d'interface de chaque carte. Vous pouvez configurer la métrique d'interface à l'aide de la commande Set-NetIPInterface Windows PowerShell.

Lorsque des itinéraires de trafic réseau sont choisis et que vous avez configuré le paramètre **InterfaceMetric** de la commande **Set-NetIPInterface** , la métrique globale utilisée pour déterminer la préférence d'interface correspond à la somme de la métrique d'itinéraire et de la métrique d'interface. En règle générale, la métrique d'interface donne priorité à une interface particulière, comme l'utilisation de la connexion câblée si des connexions câblées et sans fil sont disponibles.

L'exemple de commande Windows PowerShell suivant montre l'utilisation de ce paramètre.

PowerShell

```
Set-NetIPInterface -InterfaceIndex 12 -InterfaceMetric 15
```

L'ordre dans lequel les cartes apparaissent dans une liste est déterminé par la métrique d'interface IPv4 ou IPv6. Pour plus d'informations, consultez la fonction GetAdaptersAddresses.

Pour obtenir des liens vers toutes les rubriques de ce guide, consultez Réglage des performances du sous-système réseau.

Réglage des performances de la carte réseau dans Windows Server

16/08/2025

S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cet article explique comment optimiser les performances de la carte réseau dans les environnements Windows Server. Le réglage des performances de la carte réseau peut améliorer considérablement le débit, réduire la latence et optimiser l'utilisation des ressources pour vos charges de travail de serveur.

Les variables suivantes déterminent les paramètres de réglage adéquats de vos adaptateurs réseau :

- La carte réseau et son jeu de fonctionnalités
- Le type de charge de travail que le serveur réalise
- Les ressources matérielles et logicielles du serveur
- Vos objectifs de performances pour le serveur

Les paramètres de réglage optimaux dépendent de votre configuration matérielle spécifique, des exigences de charge de travail et des objectifs de performances. Avant d'implémenter des modifications, évaluez vos performances réseau actuelles et identifiez les possibilités d'amélioration. Certaines fonctionnalités et certains paramètres peuvent varier d'une version à l'autre.

Les sections qui suivent décrivent certaines options de réglage des performances.

Fonctionnalités de déchargement

Les fonctionnalités de déchargement réseau transfèrent les tâches de traitement du processeur vers la carte réseau, ce qui réduit la surcharge système et améliore les performances réseau globales. Les fonctionnalités de déchargement courantes incluent le déchargement de somme de contrôle TCP, le déchargement d’envoi important (LSO) et la mise à l’échelle côté réception (RSS).

L’activation des fonctionnalités de déchargement de la carte réseau est souvent bénéfique. Toutefois, l’adaptateur réseau n'est pas toujours suffisamment puissant pour gérer les capacités de déchargement lorsque le débit est élevé. Par exemple, considérez une carte réseau avec des ressources matérielles limitées. Dans ce cas, l’activation des fonctionnalités de déchargement de segmentation peut réduire le débit maximal durable de l’adaptateur. Toutefois, si le débit réduit est acceptable, vous devez activer les fonctionnalités de déchargement de segmentation.

Certains adaptateurs réseau exigent que vous activiez les fonctionnalités de déchargement indépendamment pour les chemins d'envoi et de réception.

> ⓘ **Important**
>
> N'utilisez pas les fonctionnalités de déchargement **IPsec Task Offload** ou **TCP Chimney Offload**. Ces technologies sont déconseillées dans Windows Server 2016 et peuvent nuire aux performances du serveur et du réseau. En outre, Microsoft peut ne plus prendre en charge ces technologies à l'avenir.

Mise à l'échelle côté réception (RSS) pour les serveurs web

RSS peut améliorer l'extensibilité web et les performances lorsque le serveur comprend moins de cartes réseau que de processeurs logiques. Lorsque l'ensemble du trafic web passe par les adaptateurs réseau, le serveur peut prendre en charge les demandes web entrantes provenant de connexions différentes peuvent être traitées simultanément dans différents processeurs.

> ⓘ **Important**
>
> Évitez d'utiliser des adaptateurs réseau non RSS et des adaptateurs réseau compatibles RSS sur le même serveur. En raison de la logique de distribution de charge dans RSS et du protocole HTTP (Hypertext Transfer Protocol), les performances peuvent être fortement dégradées si un adaptateur réseau ne prenant pas en charge RSS accepte le trafic sur un serveur équipé d'une ou plusieurs adaptateurs réseau prenant en charge RSS. Dans ce cas, vous devez utiliser des cartes réseau compatibles RSS ou désactiver RSS sous l'onglet **Propriétés avancées de** la carte réseau.
>
> Pour déterminer si une carte réseau est compatible RSS, vous pouvez afficher les informations RSS sous l'onglet **Propriétés avancées** de la carte réseau.

Profils RSS et files d'attente RSS

Le profil RSS prédéfini par défaut est `NUMAStatic`. Avant de commencer à utiliser les profils RSS, passez en revue les profils existants pour comprendre quand ils sont bénéfiques et comment ils s'appliquent à votre environnement et matériel réseau.

Par exemple, ouvrez **le Gestionnaire** des tâches et passez en revue les processeurs logiques sur votre serveur. S'ils semblent sous-utilisés pour la réception de trafic, vous pouvez essayer

d'augmenter le nombre de files d'attente RSS de la valeur par défaut (2) à la valeur maximale prise en charge par votre carte réseau. Votre carte réseau peut proposer des options permettant de changer le nombre de files d'attente RSS dans le pilote.

Ressources des cartes réseau

Pour les adaptateurs réseau qui autorisent la configuration manuelle des ressources, comme les tampons de réception et d'envoi, vous devez augmenter les ressources allouées.

Certaines cartes réseau définissent des tampons de réception faibles afin de conserver la mémoire allouée depuis l'hôte. Cela conduit à des paquets ignorés et des performances réduites. Par conséquent, dans les scénarios de réception intensive, nous vous recommandons d'augmenter la valeur du tampon de réception à son maximum.

Si une carte réseau ne propose pas la configuration manuelle des ressources, soit elle configure les ressources de manière dynamique, soit les ressources sont définies sur une valeur fixe qui ne peut pas être modifiée.

Modération des interruptions

Pour contrôler la modération de l'interruption, certains adaptateurs réseau proposent différents niveaux de modération de l'interruption, des paramètres de fusion de tampons différents (parfois séparément pour les tampons d'envoi et de réception), ou les deux.

Vous devez envisager la modération des interruptions pour les charges de travail liées au processeur. Lors de l’utilisation de la modération de l'interruption, réfléchissez au compromis entre les ressources processeur économisées côté hôte et la latence, versus les ressources processeur supplémentaires économisées côté hôte en raison des interruptions plus nombreuses et de la latence plus faible. Si la carte réseau n'effectue pas de modération des interruptions, mais qu'elle expose la coalescence des tampons, vous pouvez améliorer les performances en augmentant le nombre de tampons fusionnés pour permettre un plus grand nombre de tampons par envoi ou réception.

Traitement des paquets à faible latence

De nombreuses cartes réseaux proposent des options permettant d'optimiser la latence induite par le système d'exploitation. La latence est la durée qui sépare le traitement d'un paquet entrant par le pilote réseau et le renvoi du paquet par ce pilote. Cette durée est généralement mesurée en microsecondes. À titre de comparaison, la durée de transmission de paquets sur de longues distances est généralement mesurée en millisecondes (un ordre de magnitude plus grand). Ce réglage ne réduit pas la durée de transit d'un paquet.

La liste suivante contient quelques suggestions de réglage des performances pour les réseaux sensibles à la microseconde :

- Si votre BIOS le prend en charge, définissez le BIOS de l'ordinateur sur **Hautes performances**, avec `C-states` désactivé. Certains systèmes offrent des performances plus élevées si le système d'exploitation contrôle la gestion de l'alimentation. Vous pouvez vérifier et ajuster vos paramètres de gestion de l'alimentation à partir des paramètres d'alimentation ou à l'aide de la commande `powercfg`. Pour plus d'informations, voir Options de ligne de commande Powercfg.

- Définissez le profil de gestion de l'alimentation du système d'exploitation sur **Système hautes performances**. Ce paramètre ne fonctionne pas correctement si le BIOS système est défini pour désactiver le contrôle du système d'exploitation de la gestion de l'alimentation.

- Activez les déchargements statiques. Par exemple, activez les paramètres Sommes de contrôle UDP, Sommes de contrôle TCP et Envoyer un déchargement volumineux (LSO).

- Si le trafic est multi-diffusé, par exemple lors de la réception d'un trafic multidiffusion à volume élevé, activez RSS.

- Désactivez le paramètre **De modération des interruptions** pour les pilotes de carte réseau qui nécessitent la latence la plus faible possible. Rappelez-vous que cette configuration peut utiliser plus de temps processeur et qu'il représente un compromis.

- Gérez les interruptions de carte réseau et les appels de procédure différés (DPC) sur un processeur cœur qui partage le cache d'UC avec le cœur qui est utilisé par le programme (thread utilisateur) qui traite le paquet. Le réglage de l'affinité processeur peut être utilisé pour diriger un processus vers certains processeurs logiques avec la configuration RSS. L'utilisation du même cœur pour le thread d'interruption, le thread DPC et le thread de mode utilisateur réduit les performances à mesure que la charge augmente du fait de la compétition entre ISR, DPC et le thread pour utiliser le cœur.

Interruptions d'administration système

De nombreux systèmes matériels utilisent des interruptions de gestion du système (SMI) pour différentes fonctions de maintenance, telles que la création de rapports d'erreurs mémoire de code de correction d'erreurs (ECC), la gestion de la compatibilité USB héritée, le contrôle du ventilateur et la gestion des paramètres d'alimentation contrôlés par le BIOS.

L'interface SMI est l'interruption de priorité la plus élevée sur le système et place le processeur en mode de gestion. Ce mode préempte toute autre activité alors que SMI exécute une routine

de service d’interruption, généralement contenue dans le BIOS. Malheureusement, ce comportement peut conduire à des pointes de latence de 100 microsecondes ou davantage.

Si vous avez besoin d'une latence très faible, demandez à votre fournisseur de matériel une version du BIOS qui réduit au maximum les SMI. Ces versions du BIOS sont fréquemment appelées *BIOS à faible latence* ou *BIOS sans SMI*. Dans certains cas, une plateforme matérielle ne peut pas complètement éliminer l'activité SMI car elle est utilisée pour contrôler des fonctions essentielles (ventilateurs de refroidissement par exemple).

Le système d'exploitation ne peut pas contrôler les SMI car le processeur logique s'exécute dans un mode de maintenance spécial qui empêche l'intervention du système d'exploitation.

Réglage automatique de la fenêtre de réception TCP

La pile réseau Windows utilise une fonctionnalité nommée de *niveau de réglage automatique de la fenêtre de réception TCP* pour négocier la taille de la fenêtre de réception TCP. Cette fonctionnalité peut négocier une taille de fenêtre de réception définie pour chaque communication TCP pendant l'établissement d'une liaison TCP et améliorer les performances des connexions TCP.

Auparavant, la pile réseau Windows utilisait une fenêtre de réception de taille fixe de 65 535 octets qui limitait le débit potentiel global des connexions. Le débit total réalisable des connexions TCP peut limiter les scénarios d’utilisation du réseau. Le réglage automatique de la fenêtre de réception TCP permet à ces scénarios d'utiliser entièrement le réseau.

Pour une fenêtre de réception TCP qui a une taille particulière, vous pouvez utiliser l'équation suivante pour calculer le débit total d'une seule connexion :

> *Débit total réalisable en octets = Taille de la fenêtre de réception TCP en octets* * (1 / *latence de connexion en secondes*)

Par exemple, pour une connexion de 1 Gbits/s qui a une latence de 10 ms, le débit total réalisable n'est que de 51 Mbits/s. Cette valeur est raisonnable pour une infrastructure réseau d’entreprise volumineuse. Toutefois, en utilisant le réglage automatique pour ajuster la fenêtre de réception, la connexion peut atteindre le débit de ligne complet de 1 Gbit/s.

Certaines applications définissent la taille de la fenêtre de réception TCP. Si l'application ne définit pas la taille de la fenêtre de réception, la vitesse de la liaison détermine la taille comme suit :

Agrandir le tableau

Vitesse de liaison	Taille de la fenêtre de réception
Moins de 1 Mbits/s	8 Ko
De 1 Mbits/s à 100 Mbits/s	17 Ko
De 100 Mbits/s à 10 Gbits/s	64 Ko
10 Gbits/s ou plus rapide	128 Ko

Par exemple, sur un ordinateur sur lequel une carte réseau de 1 Gbit/s est installée, la taille de la fenêtre doit être de 64 Ko.

Cette fonctionnalité utilise également pleinement d'autres fonctionnalités pour améliorer les performances réseau. Ces fonctionnalités incluent le reste des options TCP définies dans RFC 1323. Les ordinateurs sous Windows peuvent utiliser ces fonctionnalités pour négocier des tailles de fenêtre de réception TCP plus petites, mais mises à l'échelle à une valeur définie en fonction de la configuration. Ce comportement est plus facile à gérer pour les appareils réseau.

> **Notes**
>
> Vous pouvez rencontrer un problème dans lequel l'appareil réseau n'est pas conforme à **l'option de mise à l'échelle de la fenêtre TCP** telle que définie dans RFC 1323 et, par conséquent, ne prend pas en charge le facteur d'échelle. Dans ce cas, contactez le fournisseur de votre appareil réseau.

Niveaux de mise en forme automatique

Vous pouvez définir le réglage automatique de la fenêtre de réception TCP sur l'un des cinq niveaux. Le niveau par défaut est **Normal**. Le tableau ci-dessous décrit les niveaux.

Agrandir le tableau

Level	Valeur hexadécimale	Comments
Normal (valeur par défaut)	0x8 (facteur d'échelle 8)	Définissez la fenêtre de réception TCP pour qu'elle augmente pour prendre en charge presque tous les scénarios.
Disabled	Aucun facteur d'échelle disponible	Définissez la fenêtre de réception TCP à sa valeur par défaut.

Level	Valeur hexadécimale	Comments
Restricted	0x4 (facteur d'échelle 4)	Définissez la fenêtre de réception TCP pour qu'elle augmente au-delà de sa valeur par défaut, mais limitez cette croissance dans certains scénarios.
Hautement restreint	0x2 (facteur d'échelle 2)	Définissez la fenêtre de réception TCP pour qu'elle augmente au-delà de sa valeur par défaut, mais faites-le de manière très prudente.
Experimental	0xE (facteur d'échelle 14)	Définissez la fenêtre de réception TCP pour augmenter pour répondre aux scénarios extrêmes.

Si vous utilisez une application pour capturer des paquets réseau, l'application doit signaler des données qui ressemblent aux exemples suivants pour différents paramètres de niveau de réglage automatique de fenêtre.

Niveau de réglage automatique : Normal (état par défaut)

Cet exemple montre la sortie d'un outil de capture de paquets lorsque le niveau de mise en forme automatique de la fenêtre de réception TCP est défini sur **Normal**. Le facteur d'échelle est de 8.

Sortie

```
Frame: Number = 492, Captured Frame Length = 66, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[D8-FE-E3-65-F3-
FD],SourceAddress:[C8-5B-76-7D-FA-7F]
+ Ipv4: Src = 192.169.0.5, Dest = 192.169.0.4, Next Protocol = TCP, Packet ID =
2667, Total IP Length = 52
- Tcp: [Bad CheckSum]Flags=......S., SrcPort=60975, DstPort=Microsoft-DS(445),
PayloadLen=0, Seq=4075590425, Ack=0, Win=64240 ( Negotiating scale factor 0x8 ) =
64240
SrcPort: 60975
DstPort: Microsoft-DS(445)
SequenceNumber: 4075590425 (0xF2EC9319)
AcknowledgementNumber: 0 (0x0)
+ DataOffset: 128 (0x80)
+ Flags: ......S. ----------------------------------------------------------> SYN
Flag set
Window: 64240 ( Negotiating scale factor 0x8 ) = 64240 ---------> TCP Receive
Window set as 64K as per NIC Link bitrate. Note it shows the 0x8 Scale Factor.
Checksum: 0x8182, Bad
UrgentPointer: 0 (0x0)
- TCPOptions:
+ MaxSegmentSize: 1
+ NoOption:
+ WindowsScaleFactor: ShiftCount: 8 ----------------------------> Scale factor,
defined by AutoTuningLevel
```

```
+ NoOption:
+ NoOption:
+ SACKPermitted:
```

Niveau de réglage automatique : Désactivé

Cet exemple montre la sortie d'un outil de capture de paquets lorsque le niveau de mise en forme automatique de la fenêtre de réception TCP est **défini sur Désactivé**. Le facteur d'échelle n'est pas utilisé.

Sortie

```
Frame: Number = 353, Captured Frame Length = 62, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[D8-FE-E3-65-F3-
FD],SourceAddress:[C8-5B-76-7D-FA-7F]
+ Ipv4: Src = 192.169.0.5, Dest = 192.169.0.4, Next Protocol = TCP, Packet ID =
2576, Total IP Length = 48
- Tcp: [Bad CheckSum]Flags=......S., SrcPort=60956, DstPort=Microsoft-DS(445),
PayloadLen=0, Seq=2315885330, Ack=0, Win=64240 ( ) = 64240
SrcPort: 60956
DstPort: Microsoft-DS(445)
SequenceNumber: 2315885330 (0x8A099B12)
AcknowledgementNumber: 0 (0x0)
+ DataOffset: 112 (0x70)
+ Flags: ......S. ----------------------------------------------------------> SYN
Flag set
Window: 64240 ( ) = 64240 ----------------------------------------> TCP Receive
Window set as 64K as per NIC Link bitrate. Note there is no Scale Factor defined.
In this case, Scale factor is not being sent as a TCP Option, so it will not be
used by Windows.
Checksum: 0x817E, Bad
UrgentPointer: 0 (0x0)
- TCPOptions:
+ MaxSegmentSize: 1
+ NoOption:
+ NoOption:
+ SACKPermitted:
```

Niveau de réglage automatique : Restreint

Cet exemple montre la sortie d'un outil de capture de paquets lorsque le niveau de mise en forme automatique de la fenêtre de réception TCP est défini sur **Restricted**. Le facteur d'échelle est de 4.

Sortie

```
Frame: Number = 3, Captured Frame Length = 66, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[D8-FE-E3-65-F3-
```

```
FD],SourceAddress:[C8-5B-76-7D-FA-7F]
+ Ipv4: Src = 192.169.0.5, Dest = 192.169.0.4, Next Protocol = TCP, Packet ID =
2319, Total IP Length = 52
- Tcp: [Bad CheckSum]Flags=......S., SrcPort=60890, DstPort=Microsoft-DS(445),
PayloadLen=0, Seq=1966088568, Ack=0, Win=64240 ( Negotiating scale factor 0x4 ) =
64240
SrcPort: 60890
DstPort: Microsoft-DS(445)
SequenceNumber: 1966088568 (0x75302178)
AcknowledgementNumber: 0 (0x0)
+ DataOffset: 128 (0x80)
+ Flags: ......S. ---------------------------------------------------------> SYN
Flag set
Window: 64240 ( Negotiating scale factor 0x4 ) = 64240 ---------> TCP Receive
Window set as 64K as per NIC Link bitrate. Note it shows the 0x4 Scale Factor.
Checksum: 0x8182, Bad
UrgentPointer: 0 (0x0)
- TCPOptions:
+ MaxSegmentSize: 1
+ NoOption:
+ WindowsScaleFactor: ShiftCount: 4 -------------------------------> Scale factor,
defined by AutoTuningLevel.
+ NoOption:
+ NoOption:
+ SACKPermitted:
```

Niveau de réglage automatique : Très restreint

Cet exemple montre la sortie d’un outil de capture de paquets lorsque le niveau de mise en forme automatique de la fenêtre de réception TCP est défini sur **Hautement restreint**. Le facteur d'échelle est de 2.

Sortie

```
Frame: Number = 115, Captured Frame Length = 66, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[D8-FE-E3-65-F3-
FD],SourceAddress:[C8-5B-76-7D-FA-7F]
+ Ipv4: Src = 192.169.0.5, Dest = 192.169.0.4, Next Protocol = TCP, Packet ID =
2388, Total IP Length = 52
- Tcp: [Bad CheckSum]Flags=......S., SrcPort=60903, DstPort=Microsoft-DS(445),
PayloadLen=0, Seq=1463725706, Ack=0, Win=64240 ( Negotiating scale factor 0x2 ) =
64240
SrcPort: 60903
DstPort: Microsoft-DS(445)
SequenceNumber: 1463725706 (0x573EAE8A)
AcknowledgementNumber: 0 (0x0)
+ DataOffset: 128 (0x80)
+ Flags: ......S. ---------------------------------------------------------> SYN
Flag set
Window: 64240 ( Negotiating scale factor 0x2 ) = 64240 ---------> TCP Receive
Window set as 64K as per NIC Link bitrate. Note it shows the 0x2 Scale Factor.
```

```
Checksum: 0x8182, Bad
UrgentPointer: 0 (0x0)
- TCPOptions:
+ MaxSegmentSize: 1
+ NoOption:
+ WindowsScaleFactor: ShiftCount: 2 ----------------------------> Scale factor,
defined by AutoTuningLevel
+ NoOption:
+ NoOption:
+ SACKPermitted:
```

Niveau de réglage automatique : Expérimental

Cet exemple montre la sortie d'un outil de capture de paquets lorsque le niveau de mise en forme automatique de la fenêtre de réception TCP est défini sur **Expérimental**. Le facteur d'échelle est de 14.

Sortie

```
Frame: Number = 238, Captured Frame Length = 66, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[D8-FE-E3-65-F3-
FD],SourceAddress:[C8-5B-76-7D-FA-7F]
+ Ipv4: Src = 192.169.0.5, Dest = 192.169.0.4, Next Protocol = TCP, Packet ID =
2490, Total IP Length = 52
- Tcp: [Bad CheckSum]Flags=......S., SrcPort=60933, DstPort=Microsoft-DS(445),
PayloadLen=0, Seq=2095111365, Ack=0, Win=64240 ( Negotiating scale factor 0xe ) =
64240
SrcPort: 60933
DstPort: Microsoft-DS(445)
SequenceNumber: 2095111365 (0x7CE0DCC5)
AcknowledgementNumber: 0 (0x0)
+ DataOffset: 128 (0x80)
+ Flags: ......S. -------------------------------------------------------> SYN
Flag set
Window: 64240 ( Negotiating scale factor 0xe ) = 64240 ---------> TCP Receive
Window set as 64K as per NIC Link bitrate. Note it shows the 0xe Scale Factor.
Checksum: 0x8182, Bad
UrgentPointer: 0 (0x0)
- TCPOptions:
+ MaxSegmentSize: 1
+ NoOption:
+ WindowsScaleFactor: ShiftCount: 14 ----------------------------> Scale factor,
defined by AutoTuningLevel
+ NoOption:
+ NoOption:
+ SACKPermitted:
```

Vérifier et configurer le niveau de mise en forme automatique de la fenêtre de réception TCP

Vous pouvez utiliser les applets de commande Windows PowerShell ou la commande Windows `netsh` pour passer en revue ou modifier le niveau de réglage automatique de la fenêtre de réception TCP.

> **Notes**
>
> À compter de Windows Server 2019, vous ne pouvez plus utiliser le registre pour configurer la taille de la fenêtre de réception TCP. Pour plus d'informations sur les paramètres déconseillés, consultez Paramètres TCP dépréciés.

PowerShell

Vous pouvez utiliser l'applet de commande `Get-NetTCPSetting` pour passer en revue ou modifier le niveau de mise en forme automatique. Pour passer en revue et modifier le paramètre actuel :

1. Ouvrez PowerShell en tant qu'administrateur et exécutez l'applet de commande suivante :

   PowerShell

   ```
   Get-NetTCPSetting | Select SettingName,AutoTuningLevelLocal
   ```

   Le résultat ressemble à l'exemple suivant :

   Sortie

   ```
   SettingName          AutoTuningLevelLocal
   -----------          --------------------
   Automatic
   InternetCustom       Normal
   DatacenterCustom     Normal
   Compat               Normal
   Datacenter           Normal
   Internet             Normal
   ```

2. Pour modifier le paramètre, exécutez la commande suivante. Veillez à définir `<value>` sur le niveau de réglage automatique souhaité. Pour plus d'informations, consultez Set-NetTCPSetting.

```powershell
Set-NetTCPSetting -AutoTuningLevelLocal <value>
```

Plateforme de filtrage Windows

La plateforme de filtrage Windows (WPF), introduite avec Windows Server 2008, fournit des API aux éditeurs de logiciels indépendants autres que Microsoft pour créer des filtres de traitement de paquets. Le WFP permet aux logiciels tiers d'inspecter, de modifier ou de filtrer le trafic réseau à différentes couches de la pile réseau. Bien que cette fonctionnalité soit essentielle pour les applications de sécurité, elle peut introduire une surcharge de performances si elle n'est pas implémentée correctement. Les logiciels pare-feu et antivirus en sont des exemples.

Un filtre WFP mal écrit peut réduire significativement les performances de mise en réseau d'un serveur. Pour plus d'informations, consultez Portage de paquets - Transférer les pilotes et applications vers le PAM dans le Centre de développement Windows.

Paramètres TCP dépréciés

Les paramètres de registre suivants de Windows Server 2003 ne sont plus pris en charge et sont ignorés dans les versions ultérieures.

- **TcpWindowSize**
- **NumTcbTablePartitions**
- **MaxHashTableSize**

Tous ces paramètres se trouvaient dans la sous-clé de registre suivante : `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Compteurs de performance liées au réseau

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Cette rubrique répertorie les compteurs pertinents pour la gestion des performances liées au réseau et contient les sections suivantes.

- Utilisation des ressources
- Problèmes potentiels liés au réseau
- Performance de la fusion côté réception (RSC)

Disponibilité des ressources

Les compteurs de performances suivants sont pertinents pour l'utilisation des ressources réseau.

- IPv4, IPv6
  - Datagrams reçus/s
  - Datagrammes envoyés/s
- TCPv4, TCPv6
  - Segments reçus/s
  - Segments envoyés/s
  - Segments retransmis/s
- Interface réseau (*), carte réseau (*)
  - Octets reçus/s
  - Octets envoyés/s
  - Paquets reçus/s
  - Paquets envoyés/s
  - Longueur de la file d'attente de sortie

Ce compteur correspond à la longueur de la file d'attente des paquets en sortie (en paquets). Si cette valeur est supérieure à 2, des retards se produisent. Vous devez trouver le goulot d'étranglement et l'éliminer, si possible. Étant donné que NDIS met en file d'attente les requêtes, cette longueur doit toujours être égale à 0.

- Informations sur le processeur
  - % temps processeur
  - Interrupts/sec
  - DPCs mis en file d'attente/s

    Ce compteur est une vitesse moyenne à laquelle les DPC ont été ajoutés à la file d'attente DPC du processeur logique. Chaque processeur logique a sa propre file d'attente DPC. Ce compteur mesure la vitesse à laquelle les DPC sont ajoutés à la file d'attente, et non le nombre de DPC dans la file d'attente. Il affiche la différence entre les valeurs observées dans les deux derniers échantillons, divisée par la durée de l'intervalle d'échantillon.

Problèmes potentiels liés au réseau

Les compteurs de performances suivants sont pertinents pour les problèmes potentiels liés au réseau.

- Interface réseau (*), carte réseau (*)
  - Paquets reçus et rejetés
  - Paquets reçus, erreurs
  - Paquets sortants rejetés
  - Paquets sortants, erreurs
- WFPv4, WFPv6
  - Paquets ignorés/s
- UDPv4, UDPv6
  - Datagrammes reçus, erreurs
- TCPv4, TCPv6
  - Échecs de connexion
  - Réinitialisation des connexions

- Stratégie QoS réseau
  - Paquets supprimés
  - Paquets supprimés/s
- Activité de la carte d'interface réseau par processeur
  - Indications sur la réception des ressources faibles/s
  - Paquets reçus de ressources faibles/s
- Microsoft Winsock BSP
  - Datagrammes supprimés
  - Datagrammes supprimés/s
  - Connexions rejetées
  - Connexions rejetées/s

Performance de la fusion côté réception (RSC)

Les compteurs de performances suivants sont pertinents pour les performances RSC.

- Carte réseau(*)
  - Connexions TCP actives RSC
  - Taille moyenne des paquets TCP RSC
  - Paquets fusionnés RSC TCP/s
  - Exceptions TCP RSC/s

Pour obtenir des liens vers toutes les rubriques de ce guide, consultez Réglage des performances du sous-système réseau.

Outils d'analyse des performances pour les charges de travail de réseau

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour en savoir plus sur les outils de performances.

Cette rubrique contient des sections sur l'outil de trafic entre le client et le serveur et la taille de la fenêtre TCP/IP.

Outil de trafic entre le client et le serveur

L'outil de trafic entre le client et le serveur (ctsTraffic) vous permet de créer et de vérifier le trafic réseau.

Pour plus d'informations et pour télécharger l'outil, consultez ctsTraffic (trafic client à serveur).

Taille de la fenêtre TCP/IP

Pour les adaptateurs de 1 Go, les paramètres indiqués dans le tableau précédent doivent fournir un bon débit, car NTttcp définit la taille de la fenêtre TCP par défaut sur 64 K par le biais d'une option de processeur logique spécifique (SO_RCVBUF) pour la connexion. Cela offre de bonnes performances sur un réseau à faible latence.

En revanche, pour les réseaux à latence élevée ou pour les adaptateurs de 10 Go, la valeur de taille de fenêtre TCP par défaut pour NTttcp génère des performances moins optimales. Dans les deux cas, vous devez ajuster la taille de la fenêtre TCP pour autoriser le produit avec un délai de bande passante supérieur.

Vous pouvez définir statiquement la taille de la fenêtre TCP sur une valeur élevée à l'aide de l'option **-rb**. Cette option désactive le réglage automatique de la fenêtre TCP et nous vous recommandons de l'utiliser uniquement si l'utilisateur comprend parfaitement le changement de comportement TCP/IP qui en résulte. Par défaut, la taille de la fenêtre TCP est définie sur une valeur suffisante et s'ajuste uniquement en cas de charge importante ou sur des liens à latence élevée.

Pour plus d'informations, consultez Réglage des performances du sous-système réseau.

Moniteur de paquets (Pktmon)

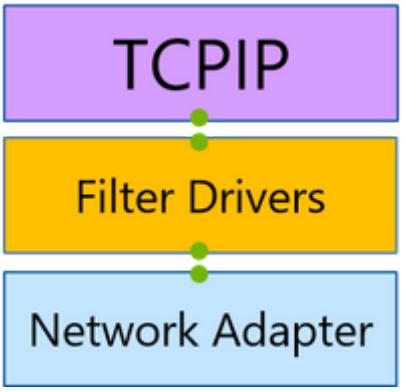
16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

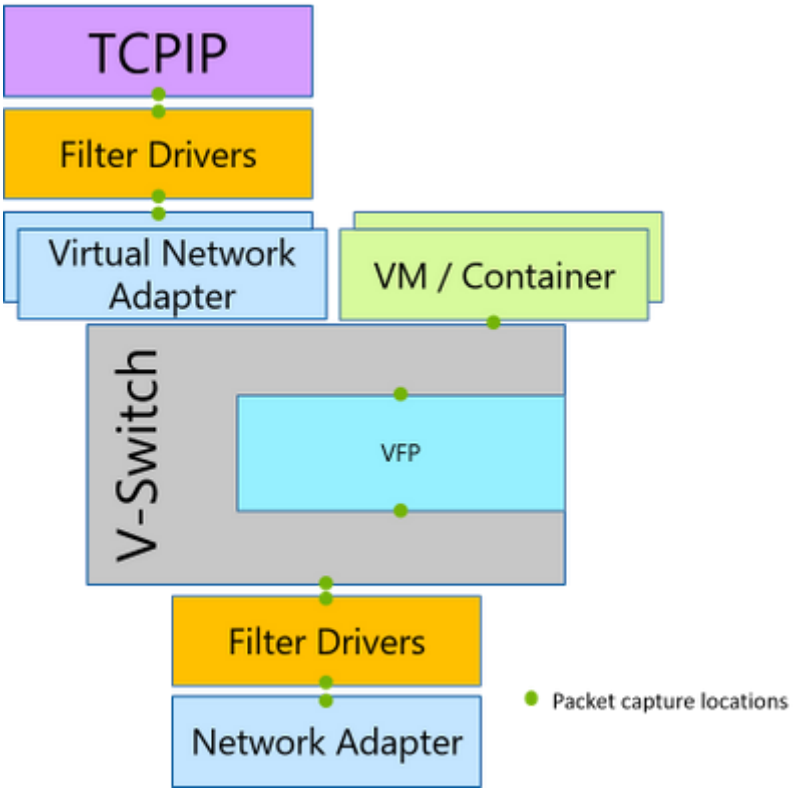
Le moniteur de paquets (Pktmon) est un outil de diagnostic réseau multicomposants intégré pour Windows. Il peut être utilisé pour la capture de paquets, la détection des suppressions de paquets, le filtrage et le comptage des paquets. L'outil est particulièrement utile dans les scénarios de virtualisation, tels que la mise en réseau de conteneurs et le SDN, car il fournit une visibilité au sein de la pile de mise en réseau. Il est disponible en boîte via la commande pktmon.exe et via les extensions Windows Admin Center.

Overview

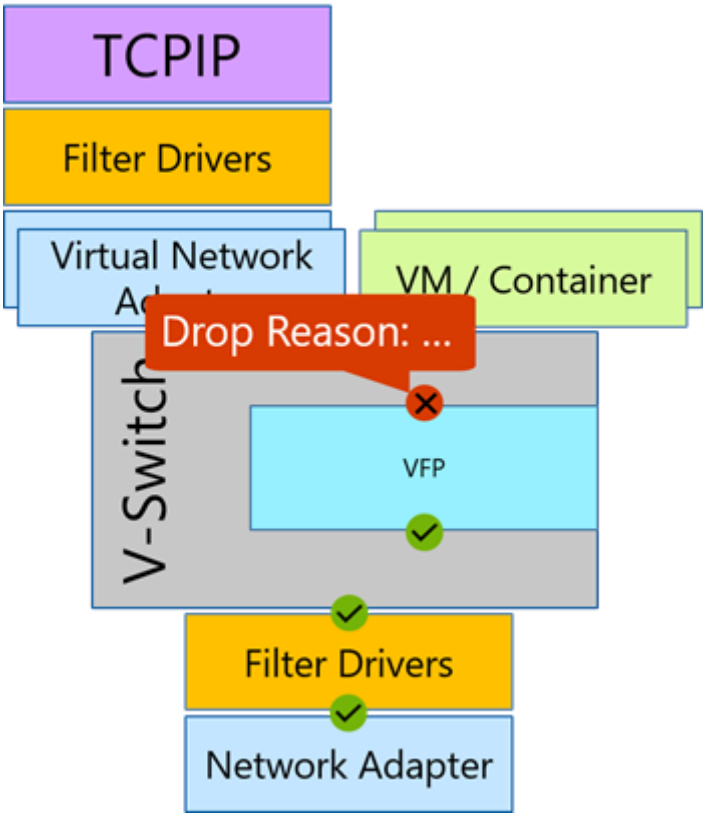
Tout ordinateur qui communique sur le réseau est doté d'au moins un adaptateur réseau. Tous les composants entre cet adaptateur et une application forment une pile de mise en réseau : un ensemble de composants réseau qui traitent et déplacent le trafic réseau. Dans les scénarios traditionnels, la pile de mise en réseau est petite, et tout le routage et le basculement de paquets se produisent sur des appareils externes.



Toutefois, avec l'avènement de la virtualisation de réseau, la taille de la pile de mise en réseau s'est multipliée. Cette pile de mise en réseau étendue comprend désormais des composants tels que le commutateur virtuel qui gèrent le traitement et le basculement de paquets. Un environnement aussi flexible permet une meilleure utilisation des ressources et une isolation de sécurité, mais il laisse également plus de place aux erreurs de configuration qui peuvent être difficiles à diagnostiquer. Le moniteur de paquets fournit une visibilité améliorée au sein de la pile de mise en réseau, qui est souvent nécessaire pour identifier ces erreurs.



Le moniteur de paquets intercepte les paquets dans plusieurs emplacements de la pile de mise en réseau, exposant ainsi la route des paquets. Si un paquet a été supprimé par un composant pris en charge dans la pile réseau, Packet Monitor signale cette suppression de paquet. Cela permet aux autorisateurs de distinguer entre un composant qui représente la destination prévue d’un paquet et un composant qui interfère avec un paquet. En outre, Packet Monitor rapporte les raisons de chute ; par exemple, MTU incompatible ou VLAN filtré, etc. Ces raisons de chute identifient la cause principale du problème sans qu'il soit nécessaire d'explorer toutes les possibilités. Le moniteur de paquets fournit également des compteurs de paquets pour chaque point d’interception, ce qui permet de procéder à un examen du flux de paquets global sans avoir besoin d’effectuer une analyse fastidieuse des journaux.



Meilleures pratiques

Utilisez ces bonnes pratiques pour rationaliser votre analyse réseau.

- Vérifiez l'aide de la ligne de commande pour connaître les arguments et les fonctionnalités (`pktmon /?`).
- Configurez des filtres de paquets correspondant à votre scénario (ajout de filtre pktmon).
- Vérifiez les compteurs de paquets pendant l'expérience pour une vue de haut niveau (compteurs pktmon).
- Examinez le journal pour obtenir une analyse détaillée (pktmon au format pktmon.etl).

Functionality

Le moniteur de paquets fournit les fonctionnalités suivantes :

- Surveillance et comptage des paquets dans plusieurs emplacements au sein de la pile de mise en réseau
- Détection de la suppression de paquets dans plusieurs emplacements de la pile
- Filtrage de paquets runtime flexible avec prise en charge de l'encapsulation
- Prise en charge générale de la journalisation et du suivi (événements ETW et WPP)
- Analyse du journal TXT basée sur l'analyse des paquets TcpDump
- Plusieurs modes de journalisation, notamment : temps réel, volume en mémoire élevé, multifichiers, circulaire

- Prise en charge du type de média Ethernet, Wi-Fi et haut débit mobile
- Prise en charge du format PCAPNG

Prise en main du moniteur de paquets

Les ressources suivantes sont disponibles pour vous aider à commencer à utiliser le moniteur de paquets.

Syntaxe et mise en forme des commandes Pktmon

Le moniteur de paquets est disponible en boîtier via la commande pktmon.exe sur le système d'exploitation Vibranium (build 19041).

Extension Packet Monitoring dans Windows Admin Center

L'extension du moniteur de paquets vous permet d'exploiter et d'utiliser le moniteur de paquets via Windows Admin Center. L'extension vous aide à diagnostiquer votre réseau en capturant et en affichant le trafic réseau via la pile réseau dans un journal facile à suivre et à manipuler.

Extension SDN Data Path Diagnostics dans Windows Admin Center

Le diagnostic du chemin d'accès de données SDN est un outil de l'extension de surveillance SDN de Windows Admin Center. L'outil automatise les captures de paquets basées sur le moniteur de paquets en fonction des divers scénarios SDN et présente la sortie dans un affichage unique facile à suivre et à manipuler.

Prise en charge du Moniteur réseau Microsoft (Netmon)

Le moniteur de paquets génère des journaux au format ETL. Ces journaux peuvent être analysés à l'aide de Microsoft Network Monitor (Netmon) à l'aide d'analyseurs spéciaux.

Prise en charge de Wireshark (format pcapng)

Le moniteur de paquets peut convertir les journaux au format pcapng. Ces journaux peuvent être analysés à l'aide de Wireshark (ou de tout autre analyseur pcapng).

Envoi de commentaires à l'équipe d'ingénierie

Signalez les bogues ou envoyez des commentaires via le hub de commentaires en procédant comme suit :

1. Lancez **le Hub de commentaires** via le menu **Démarrer** .
2. Sélectionnez le bouton **Signaler un problème** ou **Suggérer une fonctionnalité**.
3. Formulez un titre de commentaires explicite dans la zone **Résumer votre problème**.
4. Fournissez les détails et les étapes à suivre pour reproduire le problème dans la zone **Donner plus de détails**.
5. Sélectionnez **Réseau et Internet** comme catégorie supérieure, puis **Moniteur de paquets (pktmon.exe)** comme sous-catégorie.
6. Pour nous aider à identifier le bogue et le corriger plus rapidement, effectuez des captures d'écran, joignez le journal de sortie de pktmon et/ou recréez le problème.
7. Sélectionnez **Soumettre**.

Mise en forme des commandes Pktmon

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Le moniteur de paquets (Pktmon) est un outil de diagnostic réseau multicomposants intégré pour Windows. Il peut être utilisé pour la capture de paquets, la détection de la suppression de paquets, le filtrage et le comptage de paquets. L'outil est particulièrement utile dans les scénarios de virtualisation, tels que la mise en réseau de conteneurs et le SDN, car il fournit une visibilité au sein de la pile de mise en réseau. Le moniteur de paquets est disponible dans la boîte via la commande pktmon.exe sur Windows 10 et Windows Server 2019 (version 1809 et ultérieures). Vous pouvez utiliser cette rubrique pour apprendre à comprendre la syntaxe pktmon, la mise en forme des commandes et la sortie. Pour obtenir la liste complète des commandes, consultez la syntaxe pktmon.

Démarrage rapide

Pour commencer à utiliser des scénarios génériques, procédez comme suit :

1. Identifiez le type de paquets nécessaires à la capture, tels que des adresses IP, des ports ou des protocoles spécifiques associés au paquet.

2. Vérifiez la syntaxe pour appliquer des filtres de capture et appliquez les filtres pour les paquets identifiés à l'étape précédente.

   PowerShell

   ```
   C:\Test> pktmon filter add help
   C:\Test> pktmon filter add <filters>
   ```

3. Démarrez la capture et activez l'enregistrement des paquets.

   PowerShell

   ```
   C:\Test> pktmon start -c
   ```

4. Reproduisez le problème en cours de diagnostic. Interrogez des compteurs pour confirmer la présence du trafic attendu et obtenir une vue d'ensemble de la façon dont le trafic a transité dans l'ordinateur.

   PowerShell

```
C:\Test> pktmon counters
```

5. Arrêtez la capture et récupérez les journaux au format txt à des fins d'analyse.

PowerShell

```
C:\Test> pktmon stop
C:\Test> pktmon etl2txt <etl file>
```

Pour obtenir des instructions sur l'analyse de la sortie txt, consultez Analyser la sortie du moniteur de paquets.

Filtres de capture

Il est vivement recommandé d'appliquer des filtres avant de commencer une capture de paquets, car la résolution des problèmes de connectivité à une destination particulière est plus facile lorsque vous vous concentrez sur un seul flux de paquets. La capture de *tout* le trafic réseau peut rendre la sortie trop bruyante pour analyser. Pour qu'un paquet soit signalé, il doit correspondre à toutes les conditions spécifiées dans au moins un filtre. Jusqu'à 32 filtres sont pris en charge à la fois.

Par exemple, l'ensemble de filtres suivant capture tout le trafic ICMP à partir de ou vers l'adresse IP 10.0.0.10, ainsi que tout trafic sur le port 53.

PowerShell

```
C:\Test> pktmon filter add -i 10.0.0.10 -t icmp
C:\Test> pktmon filter add -p 53
```

Fonctionnalité de filtrage

- Packet Monitor prend en charge le filtrage par adresses MAC, adresses IP, ports, EtherType, protocole de transport et ID de réseau local virtuel.
- Le moniteur de paquets ne fait pas la distinction entre la source et la destination en ce qui concerne l'adresse MAC, l'adresse IP ou les filtres de port.
- Pour filtrer davantage les paquets TCP, une liste facultative d'indicateurs TCP à correspondre peut être fournie. Les indicateurs pris en charge sont FIN, SYN, RST, PSH, ACK, URG, ECE et CWR.

- Par exemple, le filtre suivant capture tous les paquets SYN envoyés ou reçus par l'adresse IP 10.0.0.10 :

PowerShell

```
C:\Test> pktmon filter add -i 10.0.0.10 -t tcp syn
```

- Le moniteur de paquets peut appliquer un filtre aux paquets internes encapsulés, en plus du paquet externe si l'indicateur **[-e]** a été ajouté à un filtre. Les méthodes d'encapsulation prises en charge sont VXLAN, GRE, NVGRE et IP-in-IP. Le port VXLAN personnalisé est facultatif et la valeur par défaut est 4789.

Pour plus d'informations, voir Syntaxe de filtre pktmon.

Capture de paquets et d'événements généraux

Le moniteur de paquets peut capturer des paquets via le paramètre **[-c]** avec la commande de démarrage. Cela permet la capture et la journalisation des paquets, ainsi que les compteurs de paquets. Pour activer les compteurs de paquets uniquement sans journaliser le paquet, ajoutez le paramètre **[-o]** à la commande de démarrage. Pour plus d'informations sur les compteurs de paquets, consultez la section Compteurs de paquets ci-dessous.

Vous pouvez sélectionner des composants à surveiller via le paramètre **[--comp].** Il peut s'agir uniquement de cartes réseau ou d'une liste d'ID de composant, et il s'agit par défaut de tous les composants. Vous pouvez également filtrer par état de propagation de paquets (supprimés ou sortants) à l'aide du paramètre **[--type].**

En plus de capturer des paquets, Packet Monitor permet de capturer des événements généraux tels que etW et WPP en déclarant le paramètre **[-t]** et en spécifiant les fournisseurs via le paramètre **[-p].** Utilisez « pktmon stop » pour arrêter toutes les collectes de données.

Par exemple, la commande suivante capture les paquets des adaptateurs réseau uniquement :

PowerShell

```
C:\Test> pktmon start -c --comp nics
```

La commande suivante capture uniquement les paquets supprimés qui passent par les composants 4 et 5, et les enregistre :

PowerShell

```
C:\Test> pktmon start -c --comp 4,5 --type drop
```

Cette commande capture les paquets et les événements de journal à partir du fournisseur « Microsoft-Windows-TCPIP » :

PowerShell

```
C:\Test> pktmon start --capture --trace -p Microsoft-Windows-TCPIP
```

Fonctionnalité de journalisation des paquets

- Packet Monitor prend en charge plusieurs modes de journalisation :
  - Circulaire : les nouveaux paquets remplacent les plus anciens lorsque la taille de fichier maximale est atteinte. Il s'agit du mode de journalisation par défaut.
  - Plusieurs fichiers : un nouveau fichier journal est créé lorsque la taille de fichier maximale est atteinte. Les fichiers journaux sont numérotés séquentiellement : PktMon1.etl, PktMon2.etl, etc. Appliquez ce mode de journalisation pour conserver tous les journaux, mais méfiez-vous de l'utilisation du stockage. Remarque : utilisez l'horodatage de création de fichier de chaque fichier journal comme indication d'une période spécifique dans la capture.
  - Temps réel : les paquets sont affichés à l'écran en temps réel. Aucun fichier journal n'est créé. Pour arrêter la surveillance, appuyez sur Ctrl+C.
  - Mémoire : les événements sont écrits dans une mémoire tampon circulaire. La taille de la mémoire tampon est spécifiée par le paramètre **[-s].** Le contenu de la mémoire tampon est écrit dans un fichier journal après l'arrêt de la capture. Utilisez ce mode de journalisation pour les scénarios très bruyants afin de capturer une quantité énorme de trafic en très peu de temps dans la mémoire tampon. En utilisant d'autres modes de journalisation, un trafic peut être perdu.

- Spécifiez la quantité de paquets à journaliser via le paramètre **[-p].** Consignez l'intégralité du paquet de chaque paquet, quelle que soit sa taille, en définissant ce paramètre sur 0. La valeur par défaut est 128 octets, qui doit inclure les en-têtes de la plupart des paquets.

- Spécifiez la taille du fichier journal via le paramètre **[-s].** Il s'agit de la taille maximale du fichier en mode de journalisation circulaire avant que Le Moniteur de paquets commence à remplacer les paquets plus anciens par les paquets plus récents. Il s'agit également de la taille maximale de chaque fichier en mode de journalisation multi-fichiers avant que le moniteur de paquets crée un fichier pour journaliser les paquets suivants. Vous pouvez également utiliser ce paramètre pour définir la taille de la mémoire tampon pour le mode de journalisation de la mémoire.

Pour plus d'informations, voir syntaxe de démarrage pktmon.

Analyse et mise en forme des paquets

Packet Monitor génère des fichiers journaux au format ETL. Il existe plusieurs façons de mettre en forme le fichier ETL à des fins d'analyse :

- Convertissez le journal au format texte (option par défaut) et analysez-le avec l'outil d'éditeur de texte comme TextAnalysisTool.NET. Les données de paquets sont affichées au format TCPDump. Suivez le guide ci-dessous pour savoir comment analyser la sortie dans le fichier texte.
- Convertissez le journal au format pcapng pour l'analyser à l'aide de Wireshark*
- Ouvrir le fichier ETL avec Network Monitor*

> **Notes**
>
> Utilisez les liens hypertexte ci-dessus pour apprendre à parser et analyser les journaux de Packet Monitor dans **Wireshark** et **Network Monitor**.

Pour plus d'informations, voir syntaxe de mise en forme pktmon.

Analysez la sortie du moniteur de paquets

Le moniteur de paquets capture un instantané du paquet par chaque composant de la pile réseau. En conséquence, il y aura plusieurs instantanés de chaque paquet (représentés dans l'image ci-dessous par les lignes de la zone bleue). Chacun de ces instantanés de paquets est représenté par deux lignes (zones rouge et verte). Il existe au moins une ligne qui inclut des données sur l'instance de paquet à partir de l'horodatage. Juste après, il y a au moins une ligne (en gras dans l'image ci-dessous) pour afficher le paquet brut analysé au format texte (sans horodatage) ; il peut s'agir de plusieurs lignes si le paquet est encapsulé, comme le paquet dans la zone verte.

```
15:28:31.543472100 PktGroupId 8444249301319686, PktNumber 1, Appearance 1, Direction Tx , Type Ethernet , Component 110, Edge 1, Filter 1, OriginalSize 74, LoggedSize 74
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543485300 PktGroupId 8444249301319686, PktNumber 1, Appearance 2, Direction Tx , Type Ethernet , Component 76, Edge 1, Filter 1, OriginalSize 74, LoggedSize 74
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543488300 PktGroupId 8444249301319686, PktNumber 1, Appearance 3, Direction Tx , Type Ethernet , Component 32, Edge 1, Filter 1, OriginalSize 74, LoggedSize 74
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543496100 PktGroupId 8444249301319686, PktNumber 1, Appearance 4, Direction Tx , Type Ethernet , Component 32, Edge 2, Filter 1, OriginalSize 74, LoggedSize 74
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543498500 PktGroupId 8444249301319686, PktNumber 1, Appearance 5, Direction Tx , Type Ethernet , Component 22, Edge 1, Filter 1, OriginalSize 74, LoggedSize 74
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543639700 PktGroupId 8444249301319686, PktNumber 1, Appearance 6, Direction Tx , Type Ethernet , Component 22, Edge 2, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543642200 PktGroupId 8444249301319686, PktNumber 1, Appearance 7, Direction Tx , Type Ethernet , Component 9, Edge 1, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543653900 PktGroupId 8444249301319686, PktNumber 1, Appearance 8, Direction Rx , Type Ethernet , Component 9, Edge 1, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543656000 PktGroupId 8444249301319686, PktNumber 1, Appearance 9, Direction Rx , Type Ethernet , Component 22, Edge 2, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543659700 PktGroupId 8444249301319686, PktNumber 1, Appearance 10, Direction Rx , Type Ethernet , Component 22, Edge 1, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543661800 PktGroupId 8444249301319686, PktNumber 1, Appearance 11, Direction Rx , Type Ethernet , Component 32, Edge 2, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543665300 PktGroupId 8444249301319686, PktNumber 1, Appearance 12, Direction Rx , Type Ethernet , Component 32, Edge 1, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543667900 PktGroupId 8444249301319686, PktNumber 1, Appearance 13, Direction Rx , Type Ethernet , Component 76, Edge 1, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543675500 PktGroupId 8444249301319686, PktNumber 1, Appearance 14, Direction Tx , Type Ethernet , Component 54, Edge 1, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:31.543677700 PktGroupId 8444249301319686, PktNumber 1, Appearance 15, Direction Tx , Type Ethernet , Component 1, Edge 1, Filter 1, OriginalSize 124, LoggedSize 124
    00-1D-D8-34-1C-11 > 00-1D-D8-34-1C-0D, ethertype IPv4 (0x0800), length 124: 10.10.182.100.8925 > 10.10.182.98.4789: VXLAN, flags [I] (0x08), vni 4096
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 29, length 40
15:28:42.640076400 PktGroupId 8444249301319687, PktNumber 1, Appearance 1, Direction Tx , Type Ethernet , Component 110, Edge 1, Filter 1, OriginalSize 74, LoggedSize 74
    00-33-11-11-22-33 > 00-11-11-11-22-33, ethertype IPv4 (0x0800), length 74: 10.0.0.31 > 10.0.0.11: ICMP echo reply, id 1, seq 30, length 40
```

Pour mettre en corrélation tous les instantanés des mêmes paquets, surveillez les valeurs PktGroupId et PktNumber (en surbrillance en jaune) ; tous les instantanés du même paquet doivent avoir ces 2 valeurs en commun. La valeur Apparence (mise en surbrillance en bleu) agit comme un compteur pour chaque capture instantanée suivante du même paquet. Par exemple, le premier instantané du paquet (où le paquet est apparu pour la première fois dans la pile réseau) a la valeur 1 pour l'apparence, l'instantané suivant a la valeur 2, et ainsi de suite.

Chaque instantané de paquet a un ID de composant (souligné dans l'image ci-dessus) indiquant le composant associé à l'instantané. Pour résoudre le nom du composant et les paramètres, recherchez cet ID de composant dans la liste des composants en bas du fichier journal. Une partie du tableau des composants est illustrée dans l'image ci-dessous mettant en surbrillance « Composant 1 » en jaune (il s'agissait du composant où le dernier instantané ci-dessus a été capturé). Les composants avec 2 bords signalent 2 instantanés à chaque bord (comme les instantanés avec apparence 3 et apparence 4 par exemple dans l'image ci-dessus).

En bas de chaque fichier journal, la liste des filtres est présentée comme indiqué dans l'image ci-dessous (mise en surbrillance en bleu). Chaque filtre affiche le ou les paramètres spécifiés (Protocole ICMP dans l'exemple ci-dessous) et des zéros pour le reste des paramètres.

```
15:28:55.327911200 Property: Component 4, MiniportIfIndex = 42
15:28:55.327912100 Drop Counters: Component 4, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 0, Bytes Out 0
15:28:55.327912700 Component 3, Type Protocol , Name tcpip.sys, TCPIP
15:28:55.327913000 Property: Component 3, EtherType = ARP
15:28:55.327913400 Property: Component 3, EtherType = IPv4
15:28:55.327913700 Property: Component 3, MiniportIfIndex = 1
15:28:55.327914200 Property: Component 3, NdisObject = 1
15:28:55.327915000 Drop Counters: Component 3, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 0, Bytes Out 0
15:28:55.327916100 Flow Counters: Component 3, Edge Lower, Edge Id 1, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 0, Bytes Out 0
15:28:55.328211700 Component 2, Type Filter , Name wfplwfs.sys, WFP 802.3 MAC Layer LightWeight Filter
15:28:55.328212100 Property: Component 2, OptDataPath = 1
15:28:55.328212500 Property: Component 2, LowerIfIndex = 44
15:28:55.328212800 Property: Component 2, MiniportIfIndex = 1
15:28:55.328213200 Property: Component 2, IfIndex = 45
15:28:55.328213600 Property: Component 2, NdisObject = 1
15:28:55.328214500 Drop Counters: Component 2, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 0, Bytes Out 0
15:28:55.328215600 Flow Counters: Component 2, Edge Lower, Edge Id 2, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 0, Bytes Out 0
15:28:55.328216600 Flow Counters: Component 2, Edge Upper, Edge Id 1, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 0, Bytes Out 0
15:28:55.328248500 Component 1, Type Miniport , Name mlx4eth63.sys, Mellanox ConnectX-3 Pro Ethernet Adapter
15:28:55.328248900 Property: Component 1, PhysAddress = 0xF4521442D1B0
15:28:55.328249400 Property: Component 1, NdisMedium = Ethernet
15:28:55.328249800 Property: Component 1, IfGuid = {8b9e16e1-63ca-4537-88bc-386f28c2ef31}
15:28:55.328250300 Property: Component 1, IfIndex = 8
15:28:55.328250800 Property: Component 1, NdisObject = 1
15:28:55.328251600 Drop Counters: Component 1, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 0, Bytes Out 0
15:28:55.328252600 Flow Counters: Component 1, Edge Upper, Edge Id 1, Direction In = Rx , Packets In 0, Bytes In 0, Direction Out = Tx , Packets Out 2, Bytes Out 248
15:28:55.328270700 Packet Filter 1, Name , MAC-1 0x000000000000, MAC-2 0x000000000000, EtherType 0, VlanId 0, IP-1 0.0.0.0, IP-2 0.0.0.0, Protocol ICMP , Port-1 0, Port-2 0, TCPFlags 0
```

Pour les paquets supprimés, le mot « drop » s'affiche avant l'une des lignes représentant l'instantané où le paquet a été supprimé. Chaque paquet supprimé fournit également une valeur dropReason. Ce paramètre dropReason fournit une brève description de la raison de la suppression de paquets ; par exemple, incompatibilité MTU, VLAN filtré, etc.

```
14:23:32.933063200 PktGroupId 4503599627370498, PktNumber 1, Appearance 13, Direction Rx , Type Ethernet , Component 32, Edge 1, Filter 1, OriginalSize 74, LoggedSize 74
        00-11-11-11-22-33 > 00-33-11-11-22-33, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.13 (00-33-11-11-22-33) tell 10.0.0.11, length 28
14:23:32.933064700 PktGroupId 4503599627370498, PktNumber 1, Appearance 14, Direction Rx , Type Ethernet , Component 76, Edge 1, Filter 1, OriginalSize 74, LoggedSize 74
        00-11-11-11-22-33 > 00-33-11-11-22-33, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.13 (00-33-11-11-22-33) tell 10.0.0.11, length 28
14:23:32.933069800 Drop: PktGroupId 4503599627370498, PktNumber 1, Appearance 15, Direction Egress, Type Ethernet , Component 110, Edge 1, Filter 1, DropReason Filtered VLAN, DropLocation 0xE000201F, OriginalSize 74, LoggedSize 74
        Drop: 00-11-11-11-22-33 > 00-33-11-11-22-33, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.13 (00-33-11-11-22-33) tell 10.0.0.11, length 28
```

Compteurs de paquets

Les compteurs du moniteur de paquets fournissent une vue d'ensemble du trafic réseau dans toute la pile réseau sans devoir analyser un journal, ce qui peut être un processus coûteux. Examinez les modèles de trafic en interrogeant les **compteurs de paquets avec des compteurs pktmon** après avoir démarré la capture du moniteur de paquets. Réinitialisez les compteurs à zéro à l'aide de **pktmon reset** ou arrêtez complètement la surveillance à l'aide de **pktmon stop**.

- Les compteurs sont organisés en liant des piles avec des adaptateurs réseau en haut et des protocoles en bas.
- Tx/Rx : les compteurs sont séparés en deux colonnes pour les directions Envoyer (Tx) et Recevoir (Rx).
- Bords : les composants signalent la propagation de paquets lorsqu'un paquet franchit une limite de composant (bord). Chaque composant peut avoir un ou plusieurs bords. Les pilotes miniport ont généralement un seul bord supérieur, les protocoles ont un seul bord inférieur et les pilotes de filtre ont des bords supérieur et inférieur.
- Gouttes : les compteurs de suppression de paquets sont signalés dans la même table.

Dans l'exemple suivant, une nouvelle capture a été démarrée, puis la commande **pktmon counters** a été utilisée pour interroger les compteurs avant l'arrêt de la capture. Les compteurs

affichent un paquet unique qui sort de la pile réseau, à partir de la couche de protocole jusqu'à la carte réseau physique, et sa réponse revenant dans l'autre sens. Si le ping ou la réponse était manquant, il est facile de le détecter via les compteurs.

```
D:\tmp>pktmon counter

Intel(R) Ethernet Connection (2) I218-LM
 Id Name                    Counter  Direction  Packets   Bytes | Direction  Packets   Bytes
 -- ----                    -------  ---------  -------   ----- | ---------  -------   -----
 11 Intel(R) Ethernet Con... Upper    Rx               1      74 | Tx               1      74
                                                                 |
 26 Netmon Filter            Lower    Rx               1      74 | Tx               1      74
                             Upper    Rx               1      74 | Tx               1      74
 25 WFP Native Filter        Lower    Rx               1      74 | Tx               1      74
                             Upper    Rx               1      74 | Tx               1      74
 24 QoS Packet Scheduler     Lower    Rx               0       0 | Tx               1      74
                             Upper    Rx               0       0 | Tx               1      74
                                                                 |
 58 TCPIP (NDIS)             Lower    Rx               1      74 | Tx               1      74
 51 NDISUIO                  Lower    Rx               1      74 | Tx               0       0
```

Dans l'exemple suivant, les gouttes sont signalées sous la colonne « Compteur ». Récupérez la raison de la dernière suppression pour chaque composant en demandant des données de compteurs au format JSON à l'aide de **pktmon counters --json** ou analysez le journal de sortie pour obtenir des informations plus détaillées.

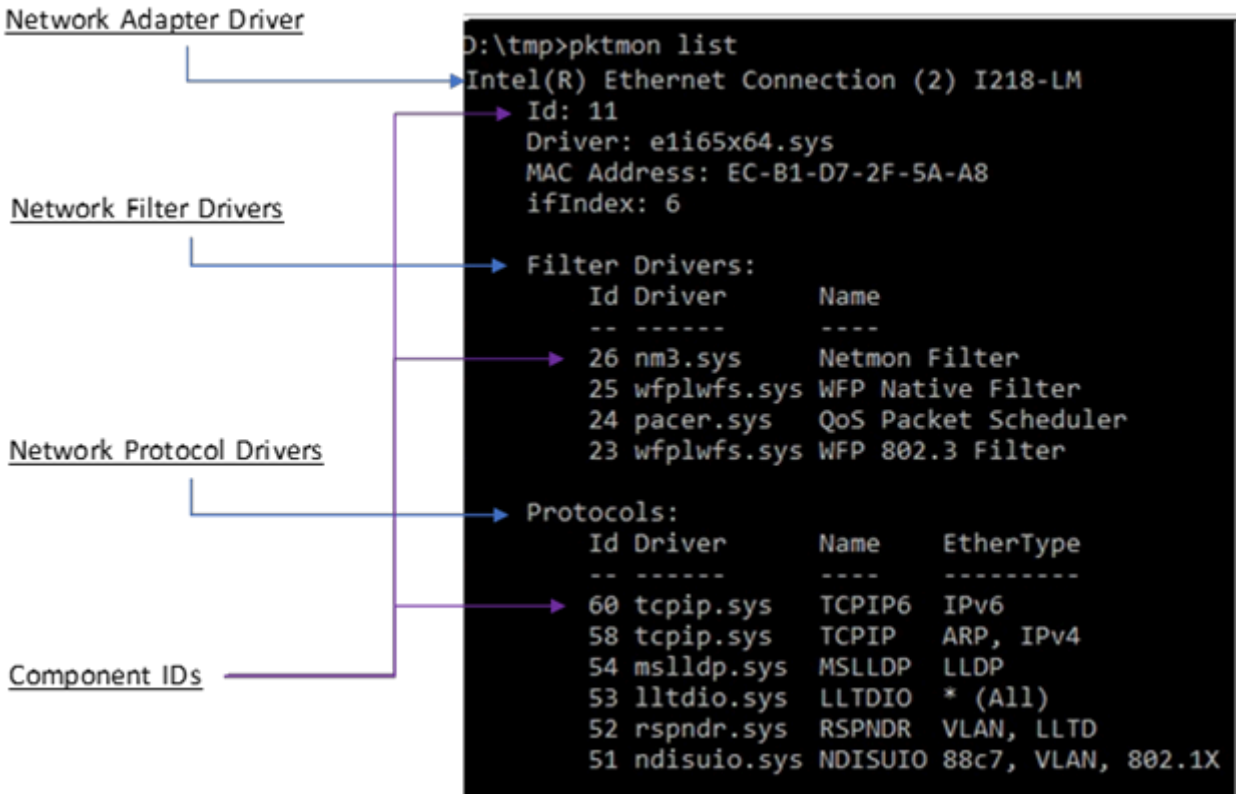
```
D:\tmp>pktmon counter

Intel(R) Ethernet Connection (2) I218-LM
 Id Name                    Counter  Direction  Packets     Bytes | Direction  Packets     Bytes
 -- ----                    -------  ---------  -------     ----- | ---------  -------     -----
 11 Intel(R) Ethernet Con... Drops    Rx              17     1,020 | Tx               0         0
                             Upper    Rx           1,409   646,763 | Tx             543   144,556
                                                                   |
 26 Netmon Filter            Lower    Rx           1,409   646,763 | Tx             543   144,556
                             Upper    Rx           1,409   646,763 | Tx             543   144,556
 25 WFP Native Filter        Lower    Rx           1,409   646,763 | Tx             543   144,556
                             Upper    Rx           1,409   646,763 | Tx             543   144,556
 24 QoS Packet Scheduler     Lower    Rx               0         0 | Tx             543   144,556
                             Upper    Rx               0         0 | Tx             543   144,556
                                                                   |
 60 TCPIP6 (NDIS)            Lower    Rx             254   156,829 | Tx             105    35,615
 58 TCPIP (NDIS)             Lower    Rx           1,137   488,410 | Tx             438   108,941
 54 MSLLDP                   Lower    Rx               1       504 | Tx               0         0
 51 NDISUIO                  Lower    Rx           1,409   646,763 | Tx               0         0
```

Comme indiqué dans ces exemples, les compteurs peuvent fournir beaucoup d'informations par le biais d'un diagramme qui peut être analysé en un simple coup d'œil.

Pour plus d'informations, consultez la syntaxe des compteurs pktmon.

Disposition de la pile réseau

Examinez la disposition de la pile réseau à l'aide de la commande **pktmon list**.



La commande affiche les composants réseau (pilotes) organisés par liaisons d'adaptateurs.

Une liaison classique se compose des éléments suivants :

- Une carte d'interface réseau unique (NIC)
- Quelques pilotes de filtre (peut-être zéro)
- Un ou plusieurs pilotes de protocole (TCP/IP ou autres)

Chaque composant est identifié de manière unique par un ID de composant Packet Monitor, qui est utilisé pour cibler des composants individuels à des fins de supervision.

> ⓘ **Notes**
>
> Les ID ne sont pas persistants et peuvent changer entre les redémarrages et le redémarrage du pilote du moniteur de paquets.
>
> Certains ID qui apparaissent dans la sortie du moniteur de paquets peuvent ne pas apparaître dans la liste des composants. Cela est dû à l'agrégation de certains composants en un ID unique pour faciliter leur sélection et leur affichage. Pour rechercher les ID d'origine pour ces composants, utilisez **pktmon list --json** et recherchez la propriété SecondaryId dans la sortie.

Pour plus d'informations, voir la syntaxe pktmon list.

Extension Packet Monitoring dans Windows Admin Center

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

L'extension du moniteur de paquets vous permet d'exploiter et d'utiliser le moniteur de paquets via Windows Admin Center. L'extension vous aide à diagnostiquer votre réseau en capturant et en affichant le trafic réseau via la pile réseau dans un journal facile à suivre et à manipuler.

Qu'est-ce que le moniteur de paquets (Pktmon) ?

Le moniteur de paquets (Pktmon) est un outil de diagnostic réseau multicomposants intégré pour Windows. Il peut être utilisé pour la capture de paquets, la détection des suppressions de paquets, le filtrage et le comptage des paquets. L'outil est particulièrement utile dans les scénarios de virtualisation, tels que la mise en réseau de conteneurs et le SDN, car il fournit une visibilité au sein de la pile de mise en réseau.

Qu'est-ce que Windows Admin Center ?

Windows Admin Center est un nouvel ensemble d'outils de gestion, basé sur un navigateur et déployé localement, qui vous permet d'administrer vos serveurs Windows, sans dépendance à Azure ni au cloud. Windows Admin Center vous donne un contrôle total sur tous les aspects de votre infrastructure de serveurs. Il s'avère particulièrement utile pour la gestion des serveurs sur les réseaux privés qui ne sont pas connectés à Internet. Windows Admin Center est l'évolution moderne des outils de gestion « intégrés » tels que le Gestionnaire de serveur et MMC.

Avant de commencer

- Pour utiliser l'outil, le serveur cible doit exécuter Windows Server 2019, version 1903 ou ultérieure.
- Installer Windows Admin Center.
- Ajoutez un serveur à Windows Admin Center :

    1. Cliquez **sur + Ajouter** sous **Toutes les connexions**.
    2. Choisissez d'ajouter une connexion serveur.

3. Tapez le nom du serveur et, si vous y êtes invité, les informations d'identification à utiliser.
4. Cliquez sur **Envoyer** pour terminer.

Le serveur sera ajouté à votre liste de connexions sur la page **Vue d'ensemble** .

Mise en route

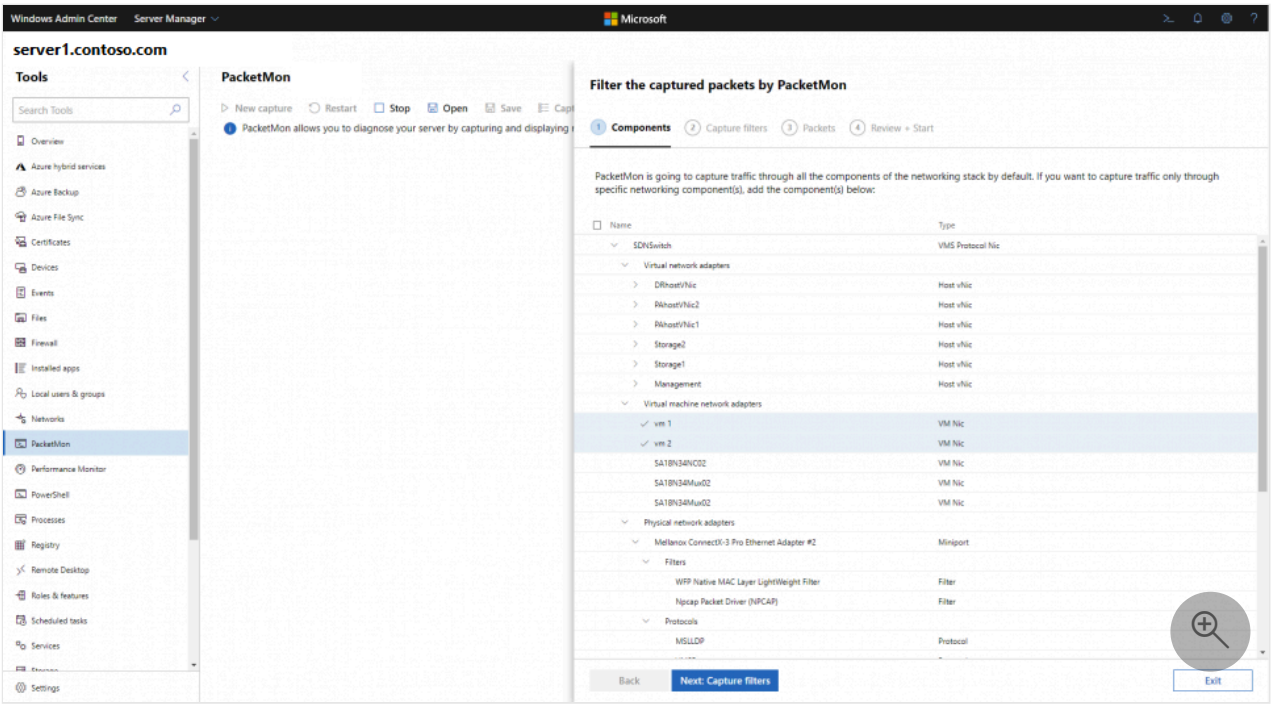
Pour accéder à l'outil, accédez au serveur que vous avez créé à l'étape précédente, puis accédez à l'extension « Analyse des paquets ».

Application de filtres

Il est vivement recommandé d'appliquer des filtres avant de démarrer une capture de paquets, car la résolution des problèmes de connectivité à une destination particulière est plus facile lorsque vous vous concentrez sur un seul flux de paquets. En revanche, la capture de l'ensemble du trafic réseau peut rendre la sortie trop bruyante pour être analysée. En conséquence, l'extension vous guide tout d'abord dans le volet filtres avant de démarrer la capture. Vous pouvez ignorer cette étape en cliquant sur **Suivant** pour démarrer la capture sans filtres. Le volet filtres vous guide pour ajouter des filtres en 3 étapes.

1. Filtrage par composants de pile réseau

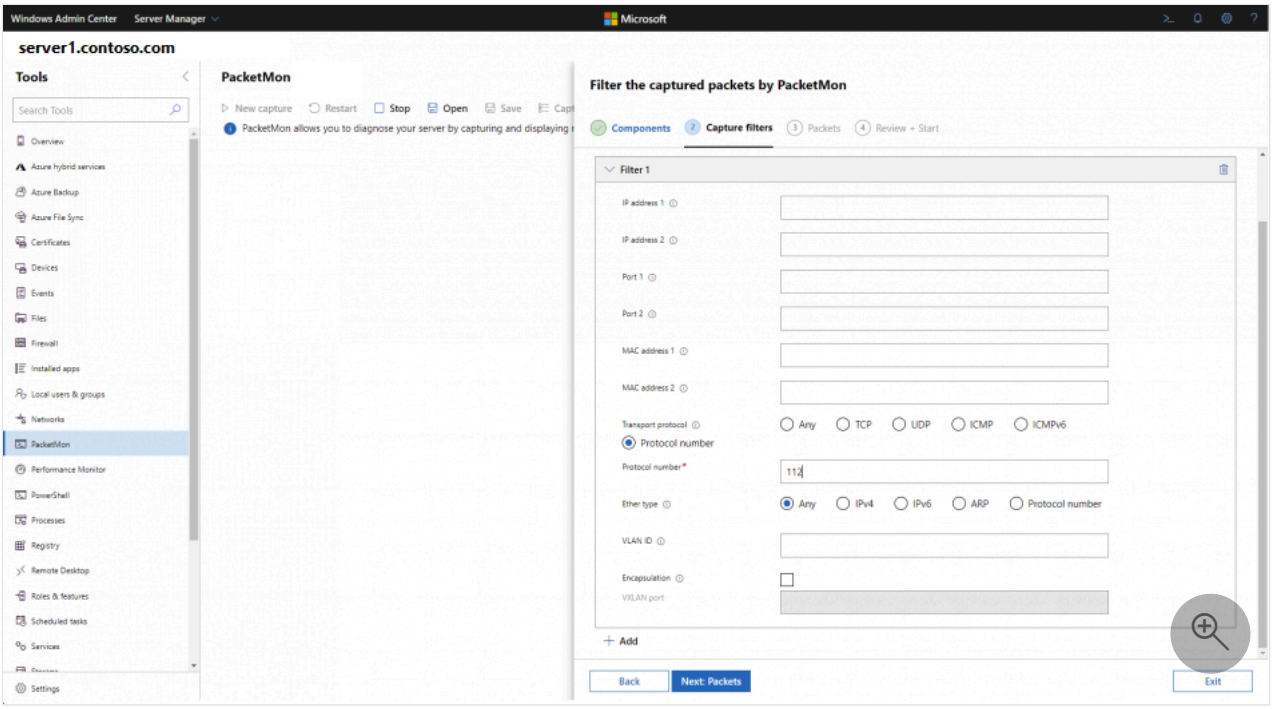
   Si vous souhaitez capturer le trafic qui passe uniquement par des composants spécifiques, la première étape du volet filtres affiche la disposition de la pile réseau afin de pouvoir sélectionner le ou les composants à filtrer. Il s'agit également d'un excellent endroit pour analyser et comprendre la disposition de la pile réseau de votre machine.



2. Filtrage par paramètres de paquets

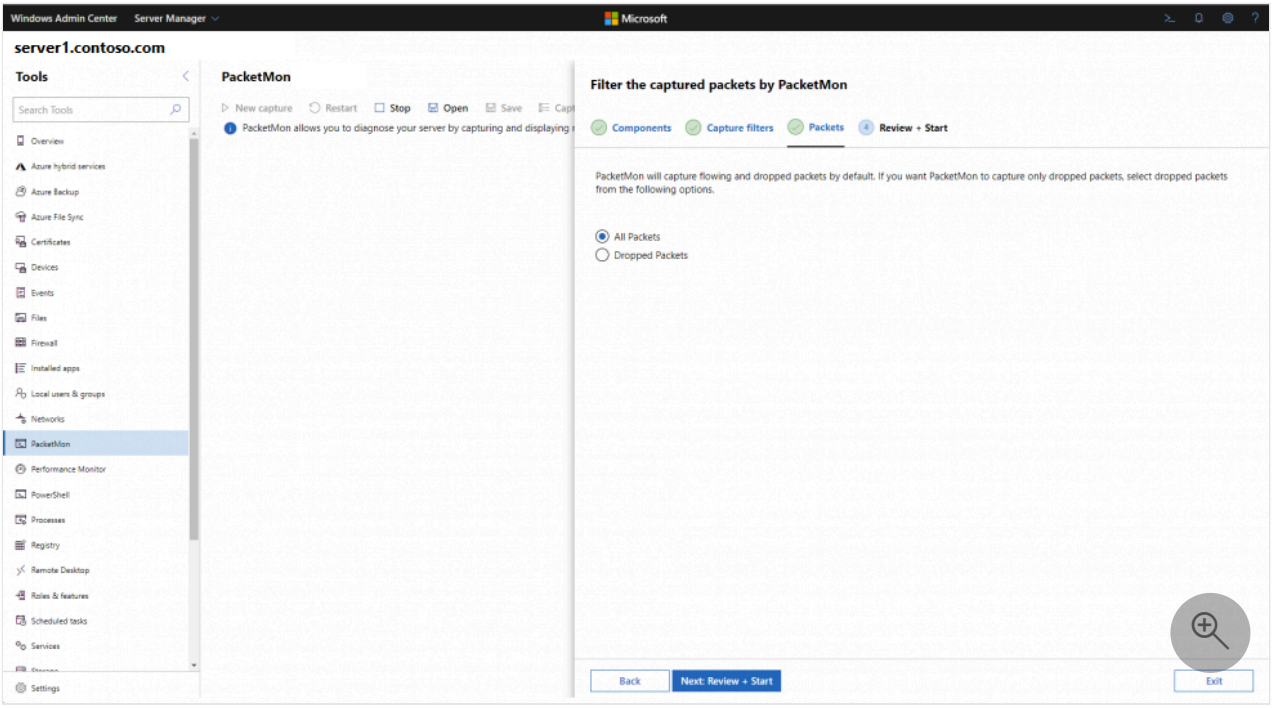
Pour la deuxième étape, le volet vous permet de filtrer les paquets par leurs paramètres. Pour qu'un paquet soit signalé, il doit correspondre à toutes les conditions spécifiées dans au moins un filtre ; jusqu'à 8 filtres sont pris en charge à la fois. Pour chaque filtre, vous pouvez spécifier des paramètres de paquet comme les adresses MAC, les adresses IP, les ports, l'ethertype, le protocole de transport, l'ID VLAN.

- Lorsque deux MAC, adresses IP ou ports sont spécifiés, l'outil ne fait pas la distinction entre la source ou la destination; il capture les paquets qui ont les deux valeurs, qu'il s'agisse d'une destination ou d'une source. Toutefois, les filtres d'affichage peuvent faire cette distinction ; consultez la section Filtres d'affichage ci-dessous.
- Pour filtrer davantage les paquets TCP, une liste facultative d'indicateurs TCP à correspondre peut être fournie. Les indicateurs pris en charge sont FIN, SYN, RST, PSH, ACK, URG, ECE et CWR.
- Si la case **encapsulation** est cochée, l'outil applique le filtre aux paquets internes encapsulés, en plus du paquet externe. Les méthodes d'encapsulation prises en charge sont VXLAN, GRE, NVGRE et IP-in-IP. Le port VXLAN personnalisé est facultatif et la valeur par défaut est 4789.

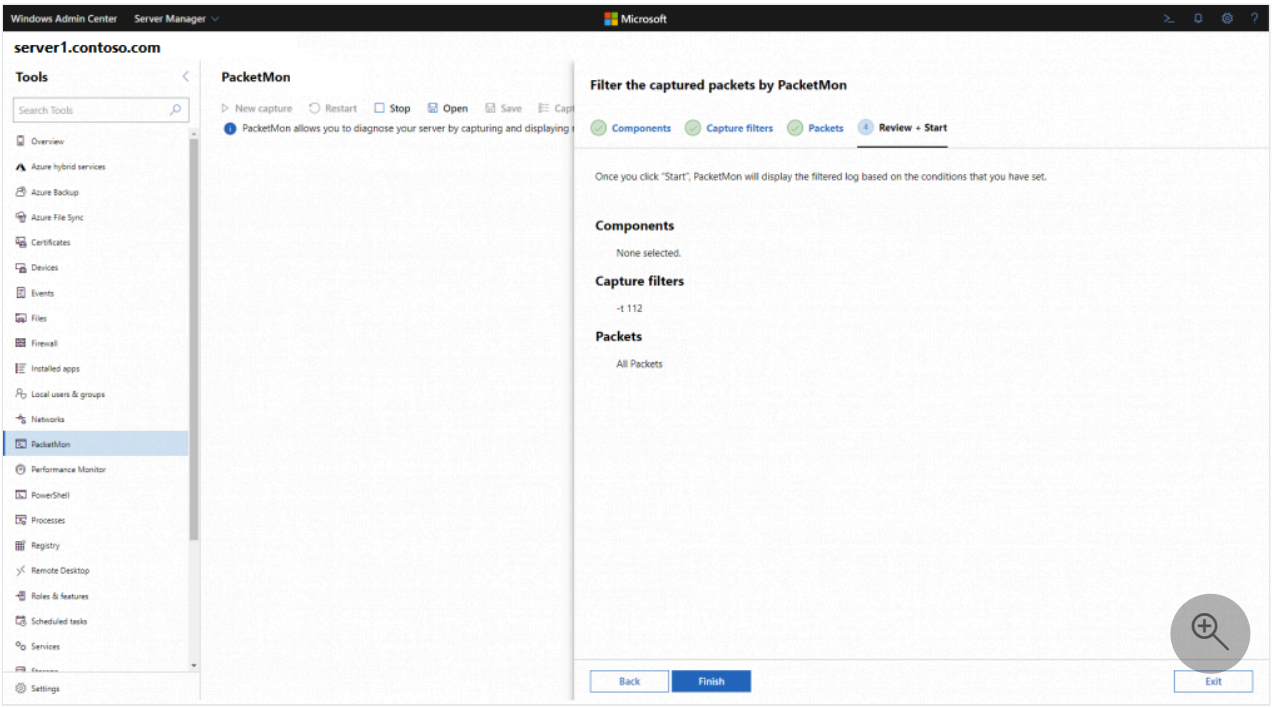


3. Filtrage par état de flux de paquets

Le moniteur de paquets capture les paquets qui circulent et suppriment les paquets par défaut. Pour capturer uniquement les paquets supprimés, sélectionnez **Paquets supprimés**.



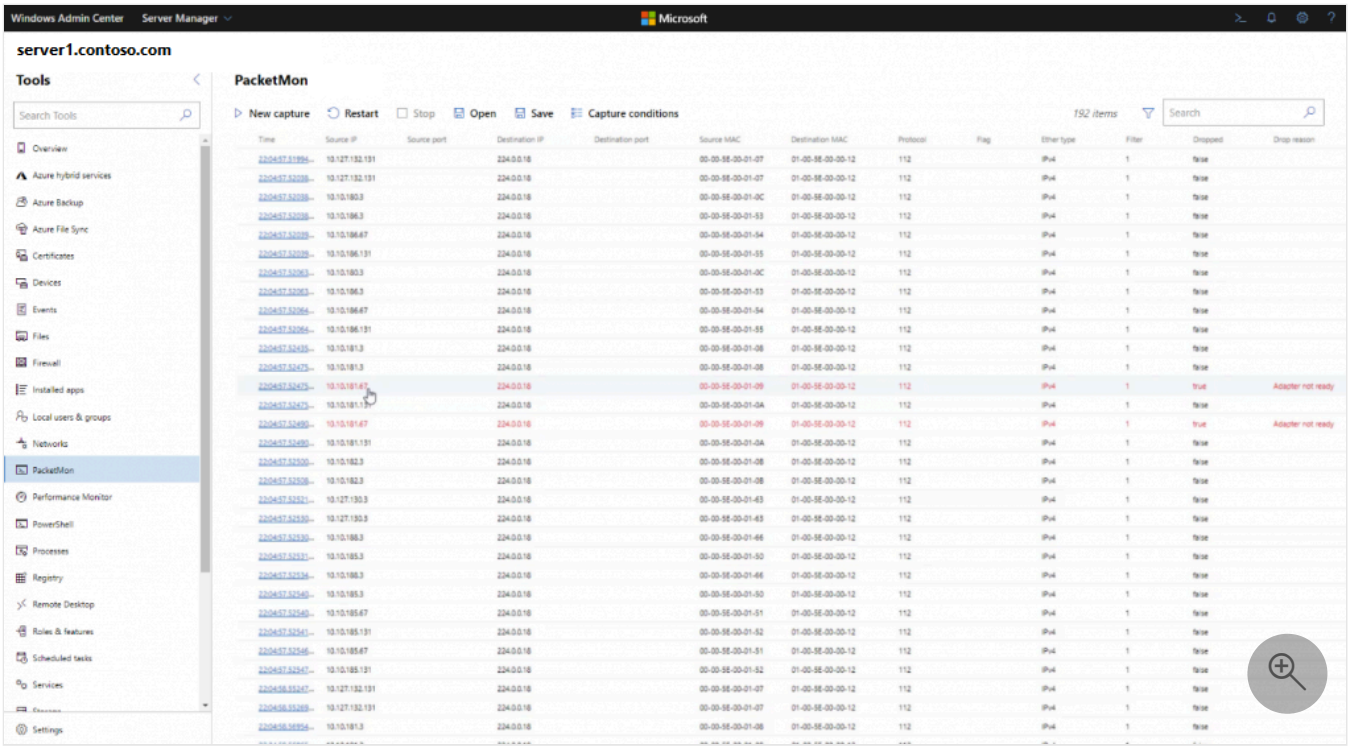
Par la suite, un résumé de toutes les conditions de filtre sélectionnées s'affiche pour révision. Vous pourrez récupérer cette vue après avoir démarré la capture via le bouton **Conditions de capture** .



Journal de capture

Les résultats sont affichés dans une table qui affiche les principaux paramètres des paquets capturés : Timestamp, Sources IP Address, Source Port, Destination IP Address, Destination Port, Ethertype, Protocol, TCP Flags, si le paquet a été supprimé et la raison de suppression.

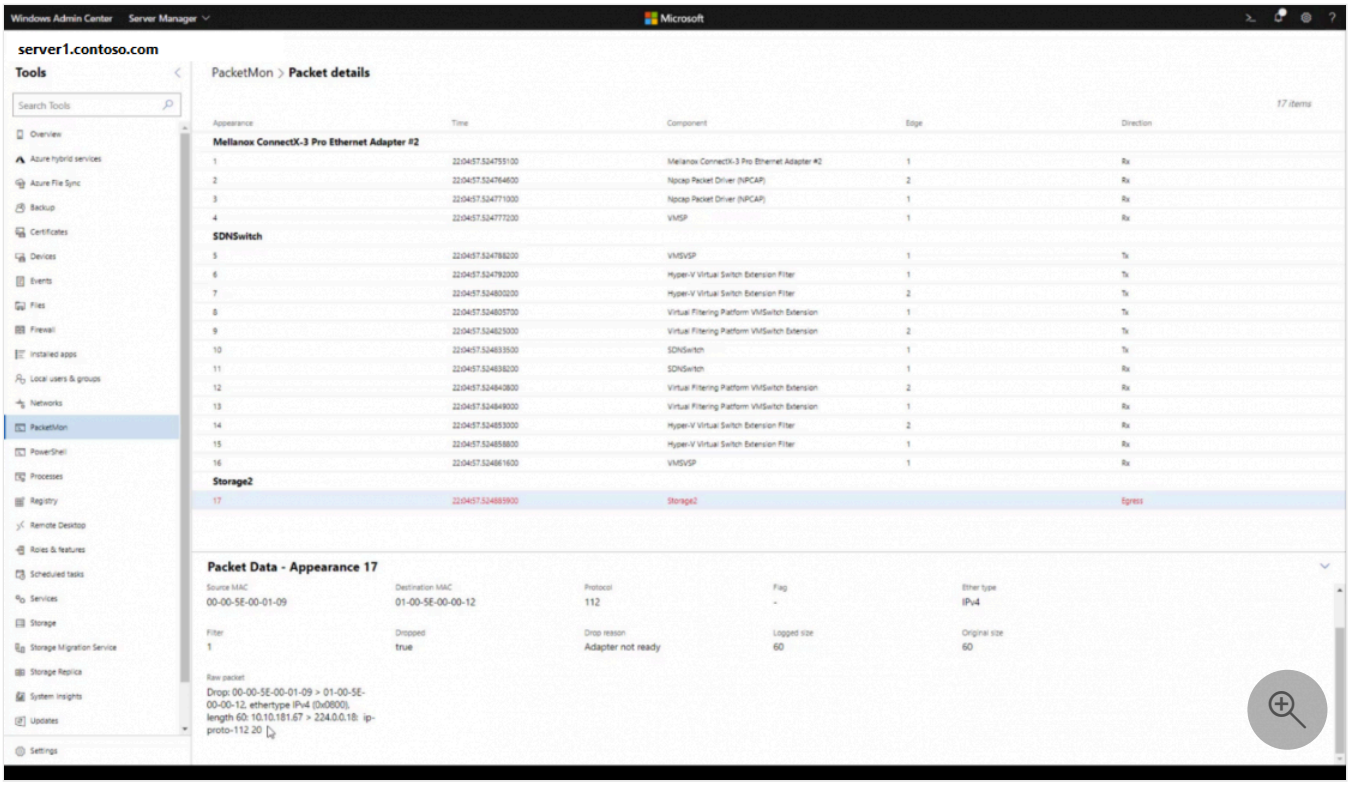
- L'horodatage de chacun de ces paquets est également un lien hypertexte qui vous redirige vers une autre page où vous trouverez plus d'informations sur le paquet sélectionné. Consultez la section Page de détails ci-dessous.
- Tous les paquets supprimés ont une valeur « True » dans l'onglet **Supprimé** , une raison de suppression et sont affichés en texte rouge pour les rendre plus faciles à identifier.
- Tous les onglets peuvent être triés croissants et décroissants.
- Vous pouvez rechercher une valeur dans n'importe quelle colonne du journal à l'aide de la barre de recherche.
- Vous pouvez redémarrer la capture avec les mêmes filtres choisis à l'aide du bouton **Redémarrer** .



Page Détails

Cette page présente un instantané du paquet lorsqu'il passe par chaque composant de la pile du réseau local. Cette vue vous montre le chemin du flux de paquets et vous permet d'examiner comment les paquets changent quand ils sont traités par chaque composant qu'ils passent.

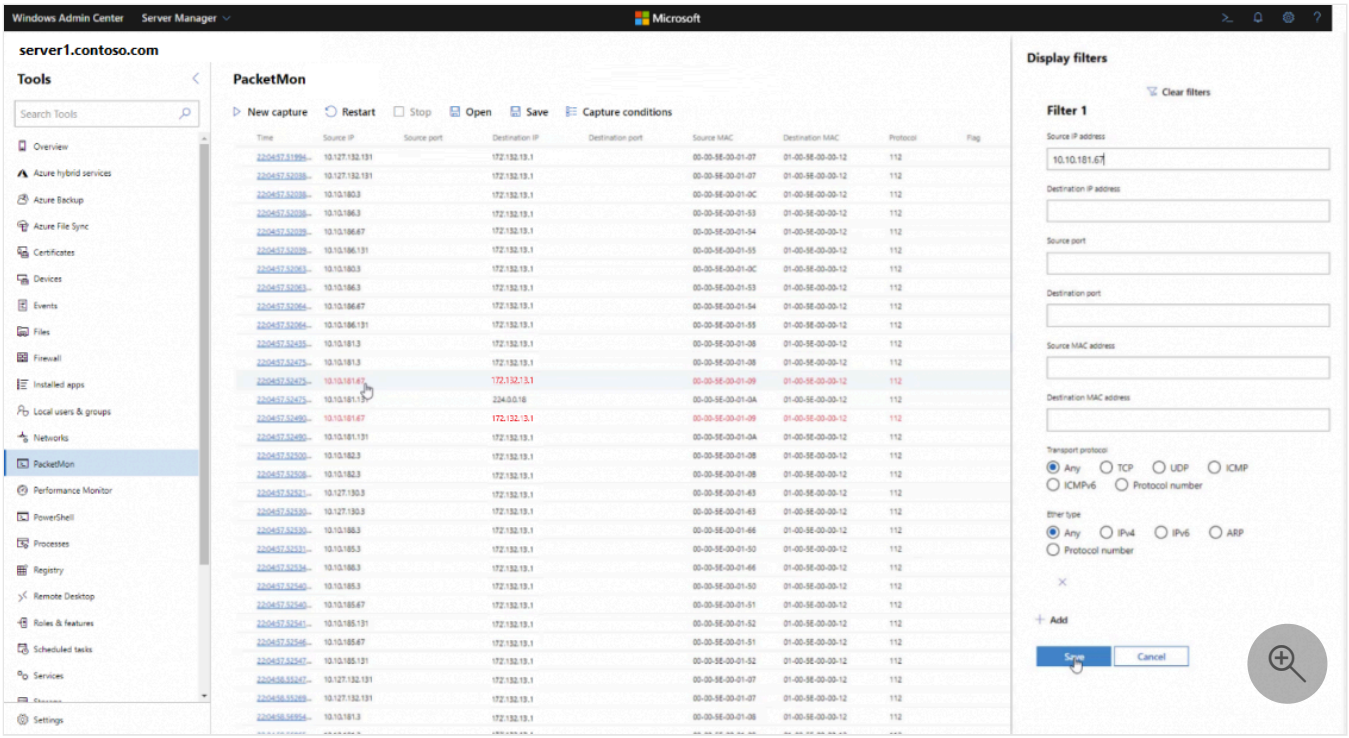
- Les instantanés de paquets sont regroupés par chaque pile adaptateur/commutateur ; par exemple, les instantanés de paquets capturés par un adaptateur/commutateur, ses pilotes de filtre et ses pilotes de protocole seront regroupés sous le nom de l'adaptateur/commutateur. Cela facilite le suivi du flux du paquet d'un adaptateur à l'autre.
- Lorsqu'un instantané est sélectionné, plus d'informations sur cet instantané spécifique sont affichés, y compris les en-têtes de paquets bruts.
- Tous les paquets supprimés ont une valeur « True » dans l'onglet **Supprimé** , une raison de suppression et sont affichés en texte rouge pour les rendre plus faciles à identifier.



Afficher les filtres

Les filtres d'affichage vous permettent de filtrer votre journal après avoir capturé les paquets. Pour chaque filtre, vous pouvez spécifier des paramètres de paquet comme les adresses MAC, les adresses IP, les ports, l'ethertype et le protocole de transport. Contrairement aux filtres de capture :

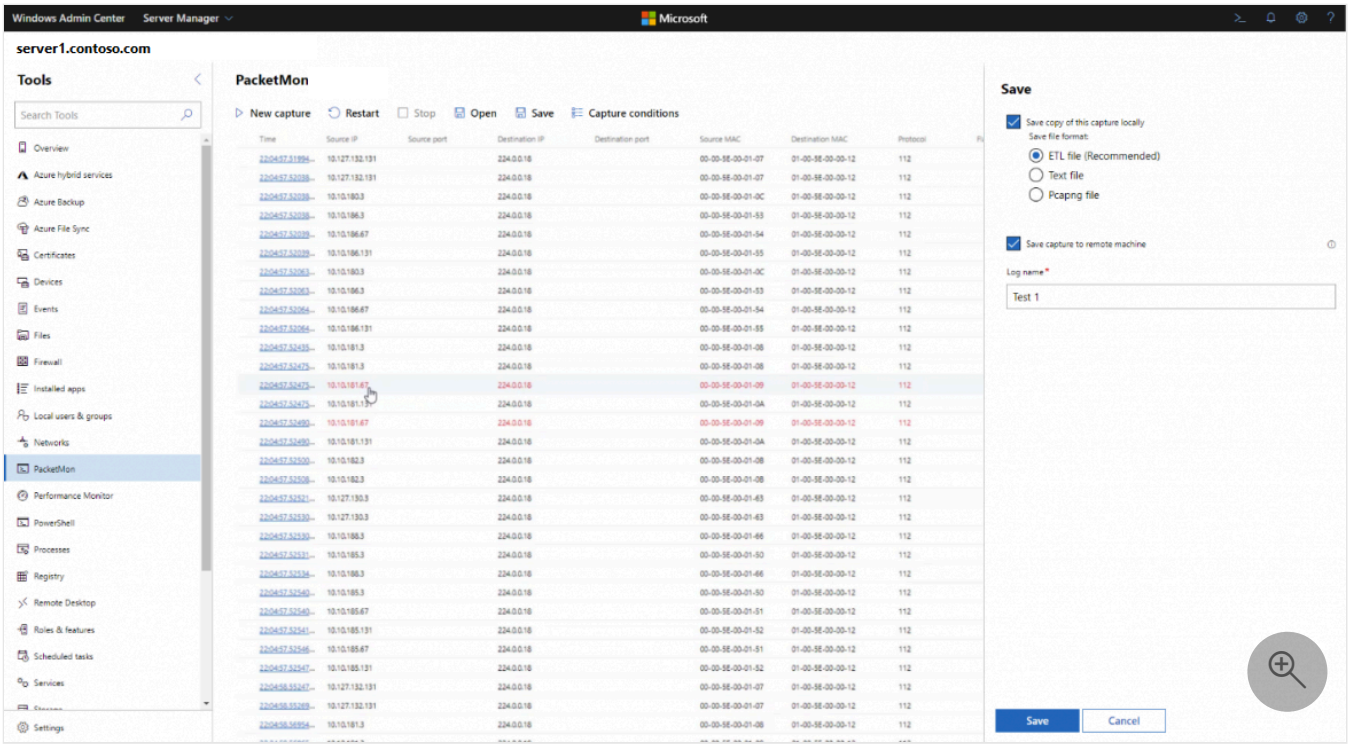
- Les filtres d'affichage peuvent faire la distinction entre la source et la destination des adresses IP, des adresses MAC et des ports.
- Les filtres d'affichage peuvent être supprimés et modifiés après les avoir appliqués pour modifier l'affichage du journal.
- Les filtres d'affichage sont inversés dans les journaux enregistrés.



Enregistrer la fonctionnalité

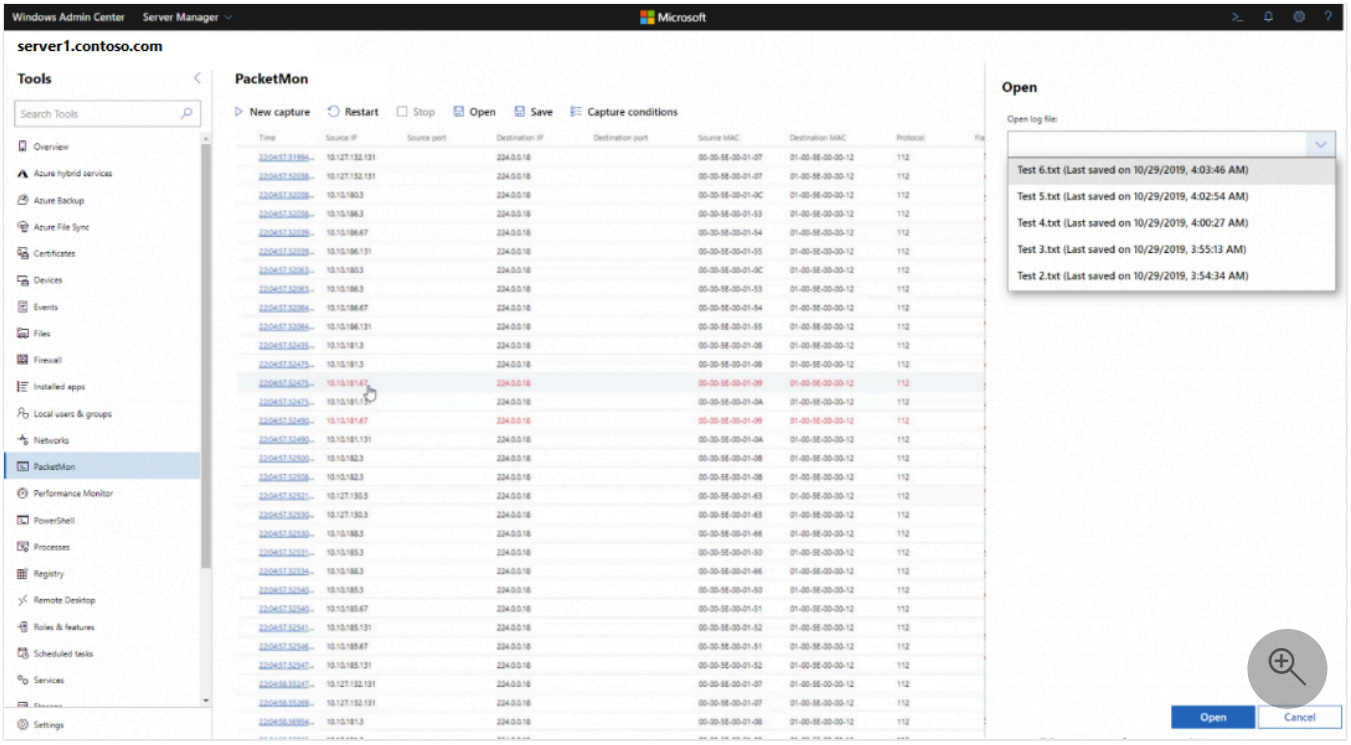
Le bouton Enregistrer vous permet d'enregistrer le journal sur votre ordinateur local, votre ordinateur distant ou les deux. Les filtres d'affichage sont inversés dans le journal enregistré.

- Si le journal est enregistré sur votre ordinateur local, vous pourrez l'enregistrer dans différents formats :
  - Format Etl qui peut être analysé à l'aide du Moniteur réseau Microsoft. Remarque : consultez cette page pour plus d'informations.
  - Format de texte qui peut être analysé à l'aide de n'importe quel éditeur de texte comme TextAnalysisTool.NET.
  - Format Pcapng qui peut être analysé à l'aide d'outils comme Wireshark.
  - La plupart des métadonnées du Moniteur de paquets seront perdues pendant cette conversion. Consultez cette page pour plus d'informations.



Ouvrir la fonctionnalité

La fonction d'ouverture vous permet de rouvrir n'importe lequel des cinq derniers journaux enregistrés afin de l'analyser à l'aide de l'outil.



Extension SDN Data Path Diagnostics dans Windows Admin Center

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

SDN Data Path Diagnostics est un outil au sein de l'extension de surveillance SDN de Windows Admin Center qui automatise les captures de paquets basées sur le moniteur de paquets en fonction de différents scénarios SDN et présente la sortie dans une vue unique facile à suivre et à manipuler.

Qu'est-ce que le moniteur de paquets (Pktmon) ?

Le moniteur de paquets (Pktmon) est un outil de diagnostic réseau multicomposants intégré pour Windows. Il peut être utilisé pour la capture de paquets, la détection de la suppression de paquets, le filtrage et le comptage de paquets. L'outil est particulièrement utile dans les scénarios de virtualisation, tels que la mise en réseau de conteneurs et le SDN, car il fournit une visibilité au sein de la pile de mise en réseau.

Qu'est-ce que Windows Admin Center ?

Windows Admin Center est un nouvel ensemble d'outils de gestion, basé sur un navigateur et déployé localement, qui vous permet d'administrer vos serveurs Windows, sans dépendance à Azure ni au cloud. Windows Admin Center vous donne un contrôle total sur tous les aspects de votre infrastructure de serveurs. Il s'avère particulièrement utile pour la gestion des serveurs sur les réseaux privés qui ne sont pas connectés à Internet. Windows Admin Center est l'évolution moderne des outils de gestion « intégrés » tels que le Gestionnaire de serveur et MMC.

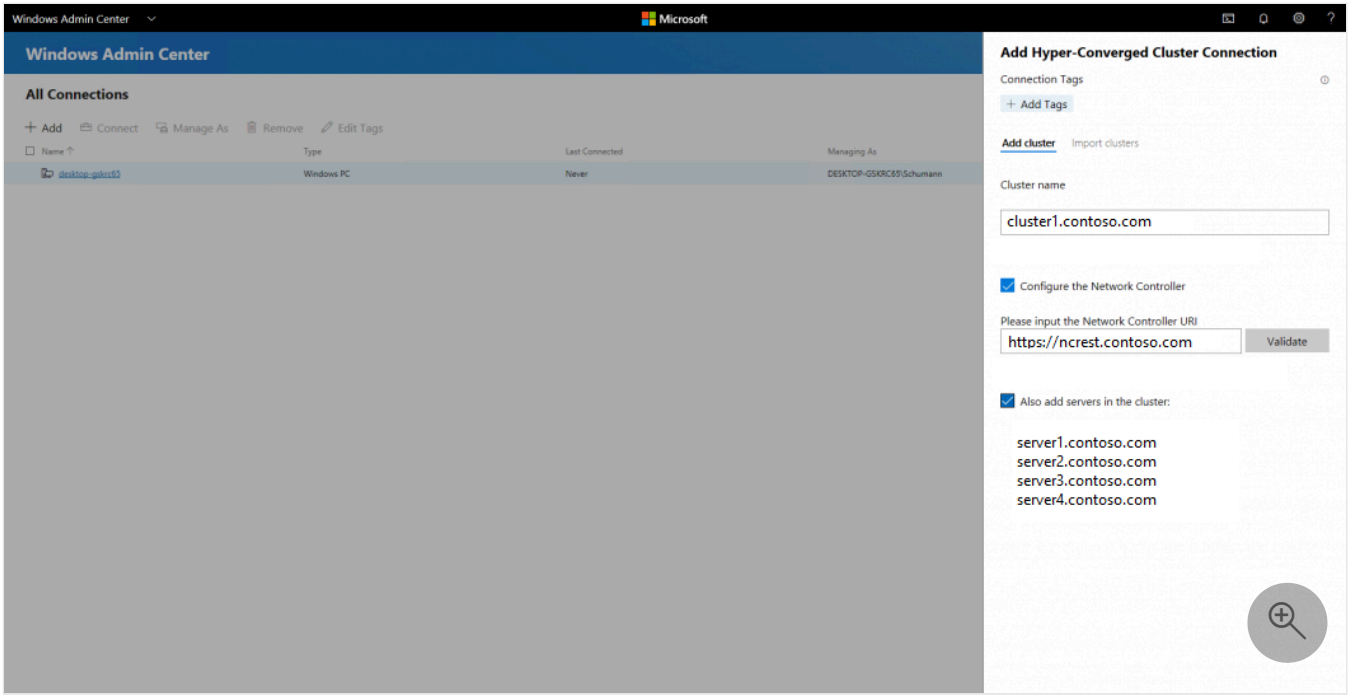
Avant de commencer

- Pour utiliser l'outil, le serveur cible doit exécuter Windows Server 2019 version 1903 (19H1) et versions ultérieures.
- Installer Windows Admin Center.
- Ajouter un cluster à Windows Admin Center :

    1. Cliquez **sur + Ajouter** sous **Toutes les connexions**.
    2. Choisissez d'ajouter une Connexion de cluster Hyper-Converged.

3. Tapez le nom du cluster et, si vous y êtes invité, les informations d'identification à utiliser.
4. Cochez **Configurer le contrôleur de réseau** pour qu'il continue.
5. Entrez l'URI du contrôleur de réseau, puis cliquez sur **Valider**.
6. Cliquez sur **Ajouter** pour terminer.

Le cluster sera ajouté à votre liste de connexions. Cliquez dessus pour lancer le tableau de bord.

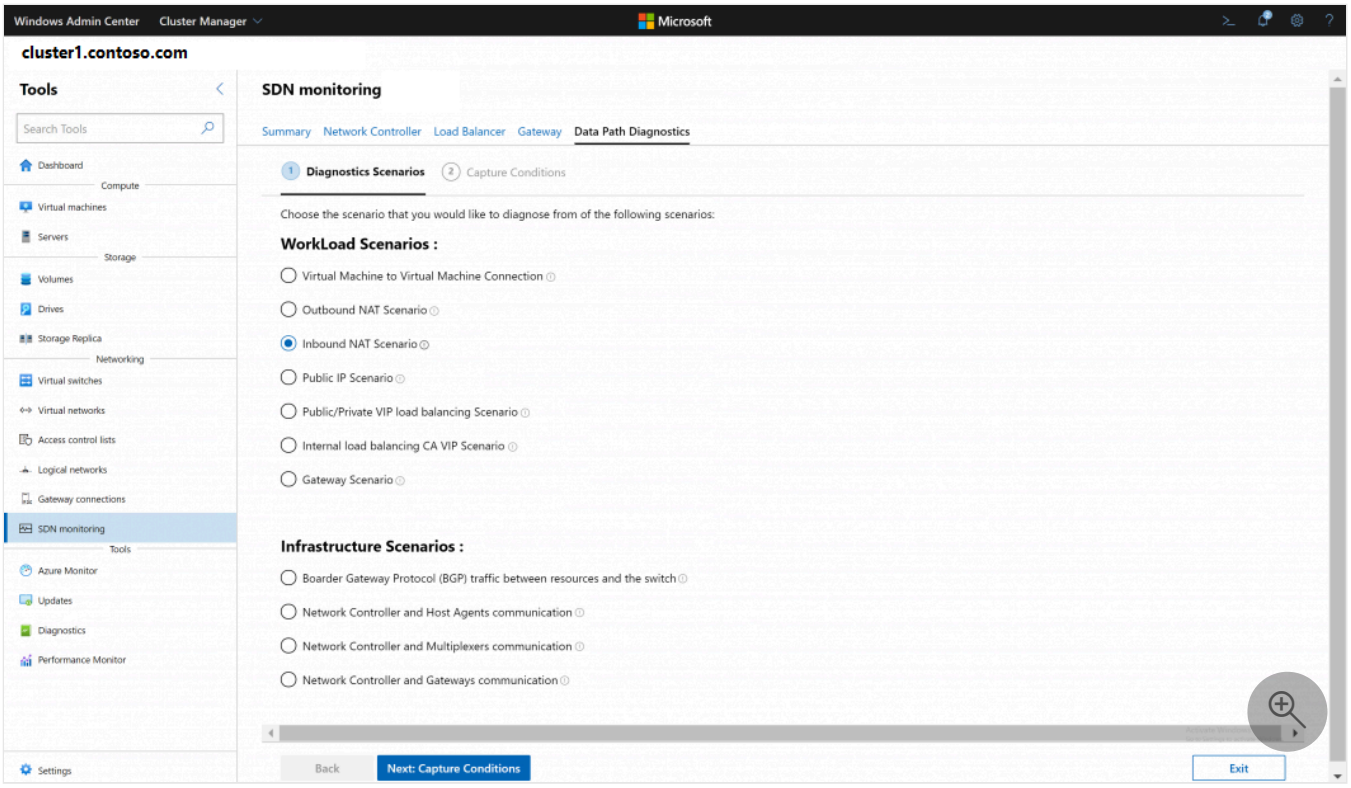


Mise en route

Pour accéder à l'outil, accédez au cluster que vous avez créé à l'étape précédente, puis à l'extension « Supervision SDN », puis à l'onglet « Diagnostics du chemin d'accès aux données ».

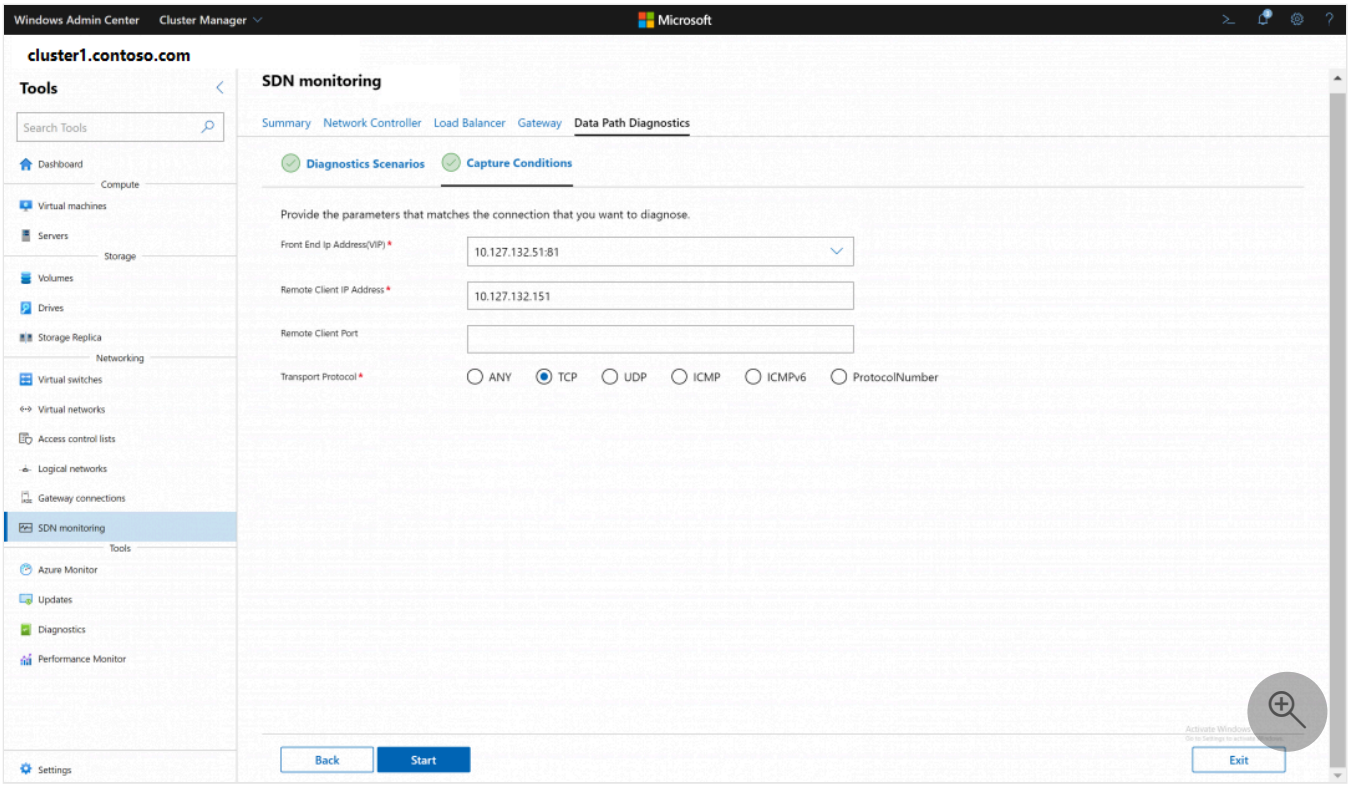
Sélection de scénarios

La première page répertorie tous les scénarios SDN classés comme scénarios de charge de travail et scénarios d'infrastructure, comme illustré dans l'image ci-dessous. Pour commencer, sélectionnez le scénario SDN qui doit être diagnostiqué.



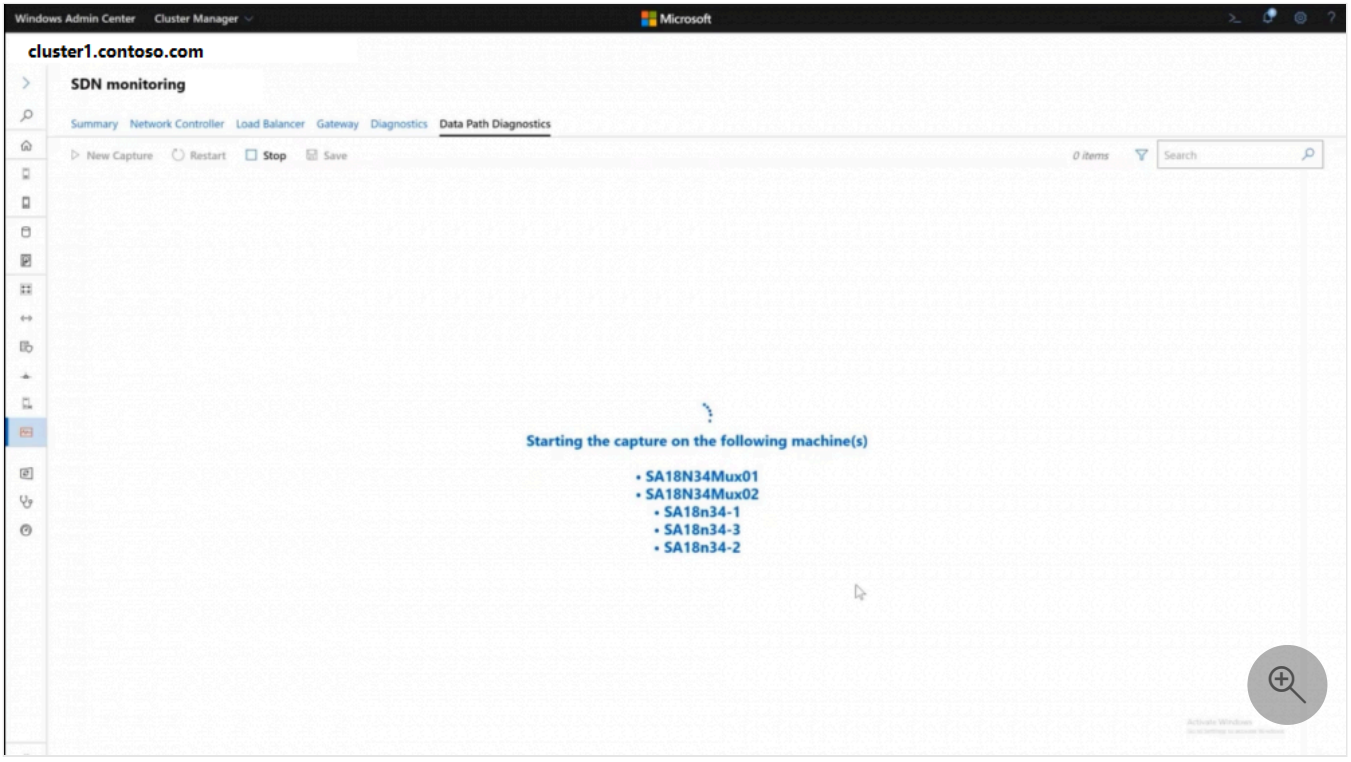
Paramètres de scénario

Après avoir choisi le scénario, remplissez une liste de paramètres obligatoires et facultatifs pour démarrer la capture. Ces paramètres de base pointent l'outil vers la connexion qui doit être diagnostiquée. L'outil utilise ensuite ces paramètres pour les requêtes afin d'exécuter une capture réussie, sans intervention de l'utilisateur pour déterminer le flux de paquets attendu, les machines impliquées dans le scénario, leur emplacement dans le cluster ou les filtres de capture à appliquer sur chaque ordinateur. Les paramètres obligatoires permettent à la capture de s'exécuter, et les paramètres facultatifs permettent de filtrer certains bruits.

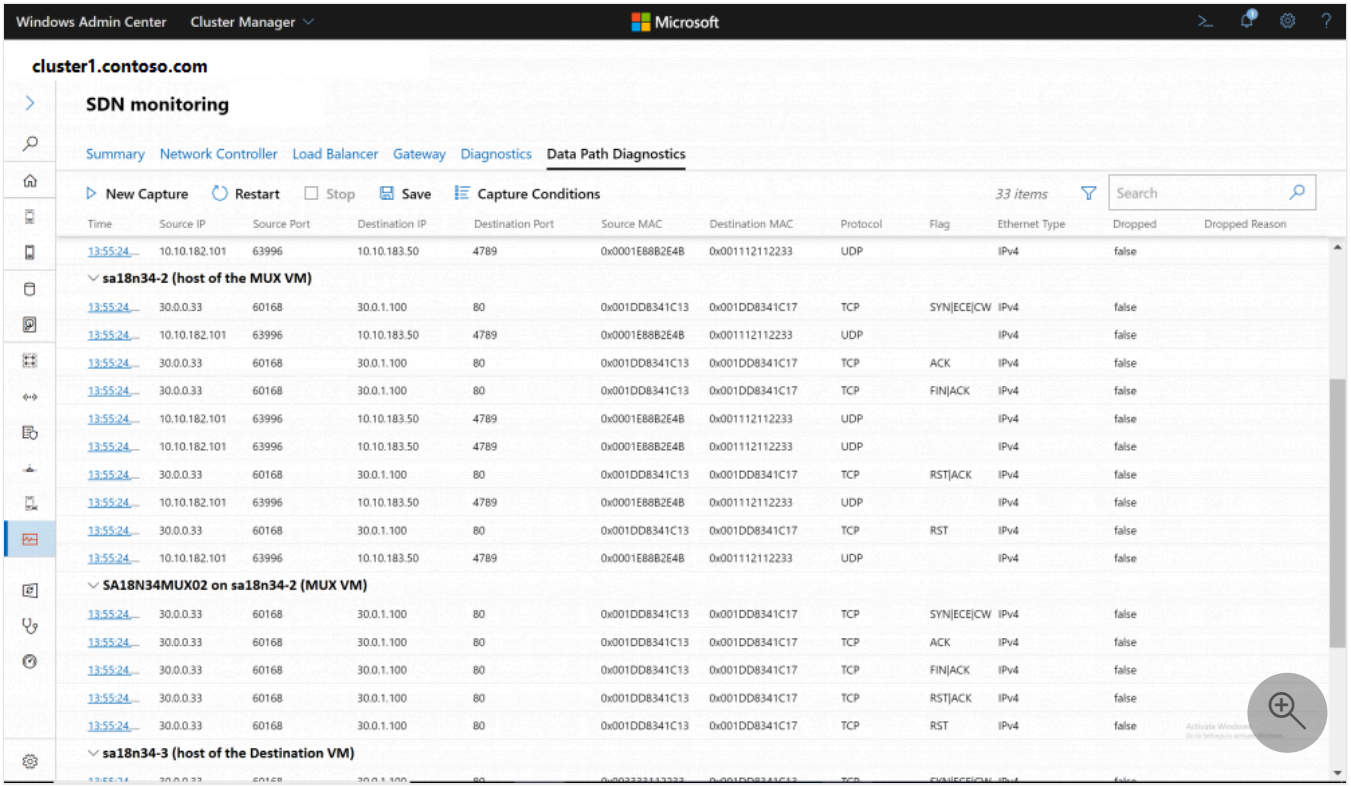


Journal de capture

Une fois la capture démarrée, l'extension affiche la liste des machines sur lesquelles la capture démarre. Vous pouvez être invité à vous connecter à ces ordinateurs si vos informations d'identification n'ont pas été enregistrées. Vous pouvez commencer à reproduire le ping ou le problème que vous essayez de diagnostiquer en capturant les paquets relatifs. Une fois les paquets capturés, l'extension affiche des marques en regard des ordinateurs sur lesquels les paquets ont été capturés.



Après l'arrêt de la capture, les journaux de toutes les machines sont affichés dans une seule page, divisée par le titre de la machine. Chaque titre inclut le nom de la machine, son rôle dans le scénario et son hôte dans le cas de machines virtuelles.



Les résultats sont affichés dans une table qui affiche les principaux paramètres des paquets capturés : Timestamp, Sources IP Address, Source Port, Destination IP Address, Destination Port, Ethertype, Protocol, TCP Flags, si le paquet a été supprimé et la raison de suppression.

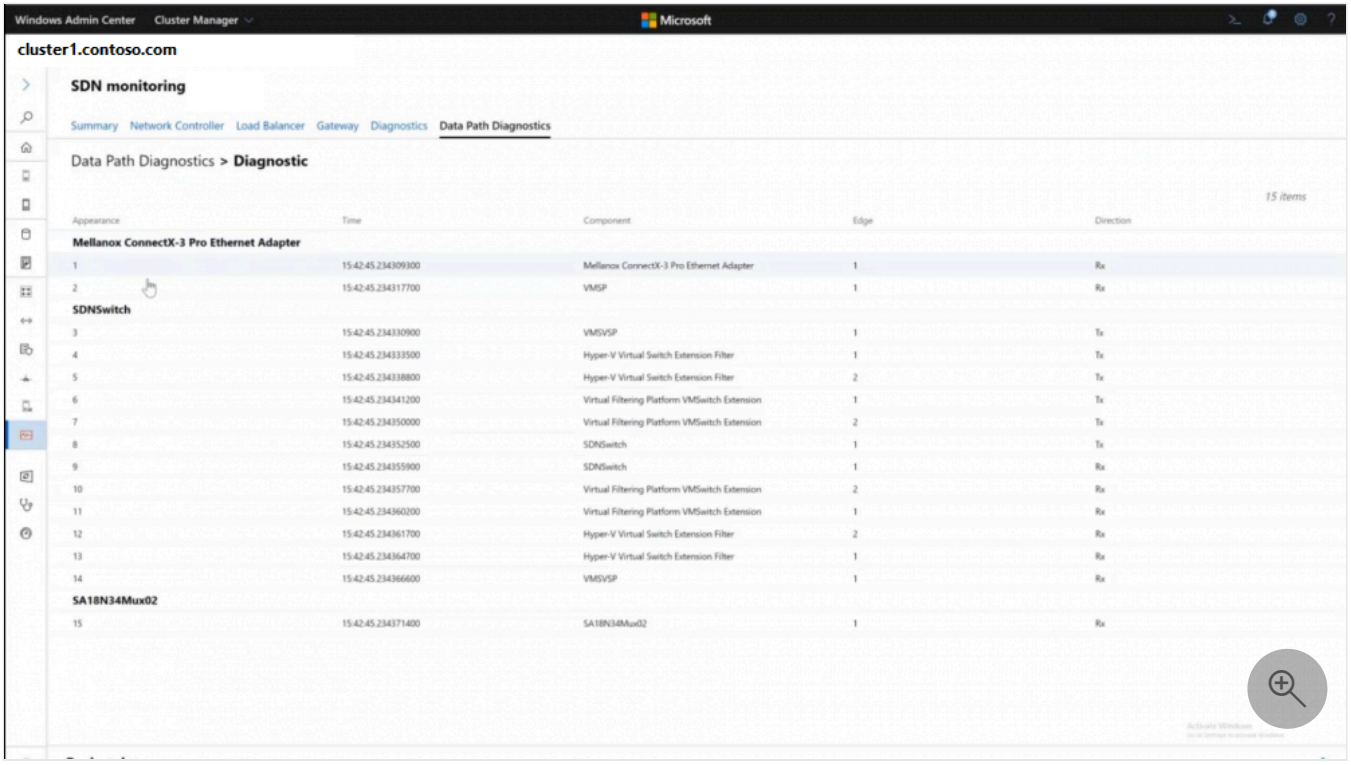
- L'horodatage de chacun de ces paquets est également un lien hypertexte qui vous redirige vers une autre page où vous trouverez plus d'informations sur le paquet sélectionné. Consultez la section Page de détails ci-dessous.
- Tous les paquets supprimés ont une valeur « True » dans l'onglet **Supprimé** , une raison de suppression et sont affichés en texte rouge pour faciliter l'identification.
- Tous les onglets peuvent être triés croissants et décroissants.
- Vous pouvez rechercher une valeur dans n'importe quelle colonne du journal à l'aide de la barre de recherche.
- Vous pouvez redémarrer la capture avec les mêmes filtres choisis à l'aide du bouton **Redémarrer** .

Page Détails

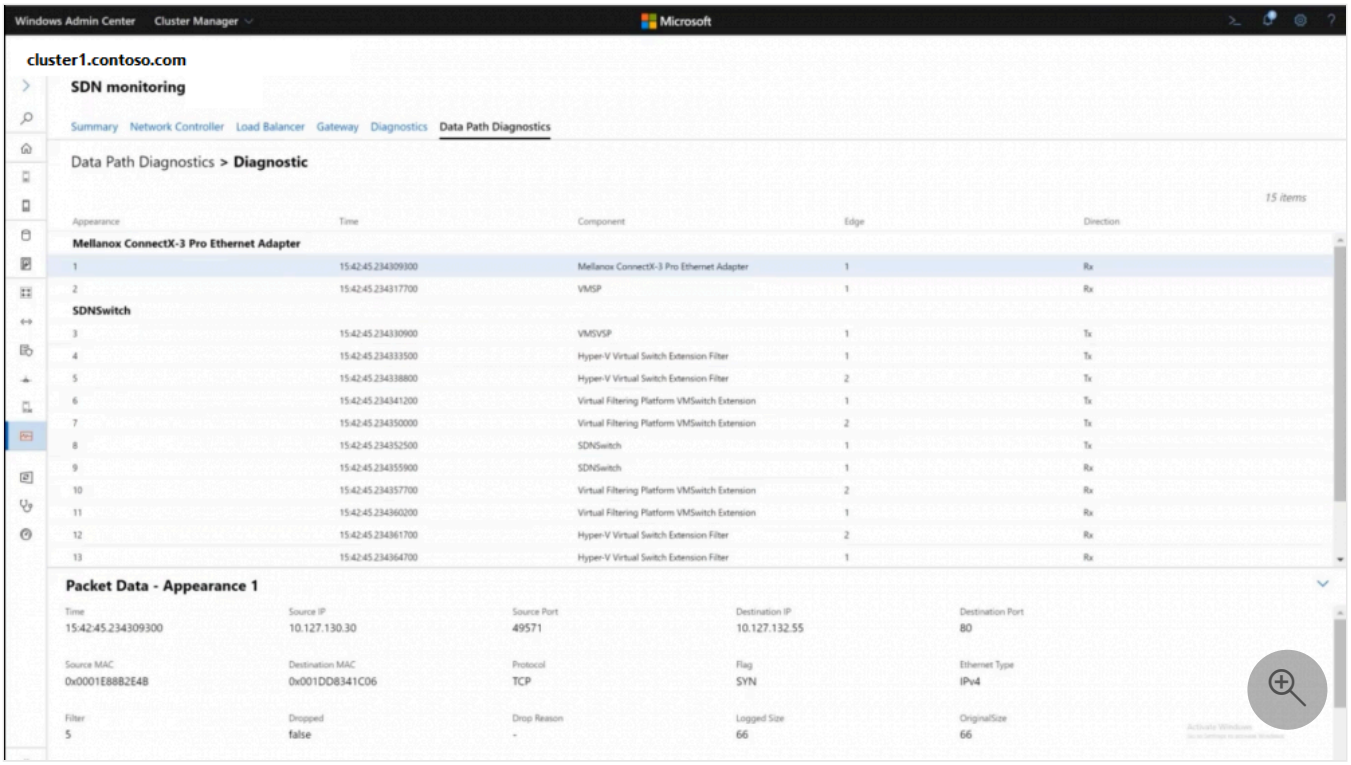
Les informations de cette page sont particulièrement utiles si vous rencontrez des problèmes de propagation de paquets incorrects ou des problèmes de configuration incorrecte, car vous pouvez examiner le flux du paquet via chaque composant de la pile réseau. Pour chaque

tronçon de paquets, il existe des détails qui incluent les paramètres de paquet ainsi que les détails du paquet brut.

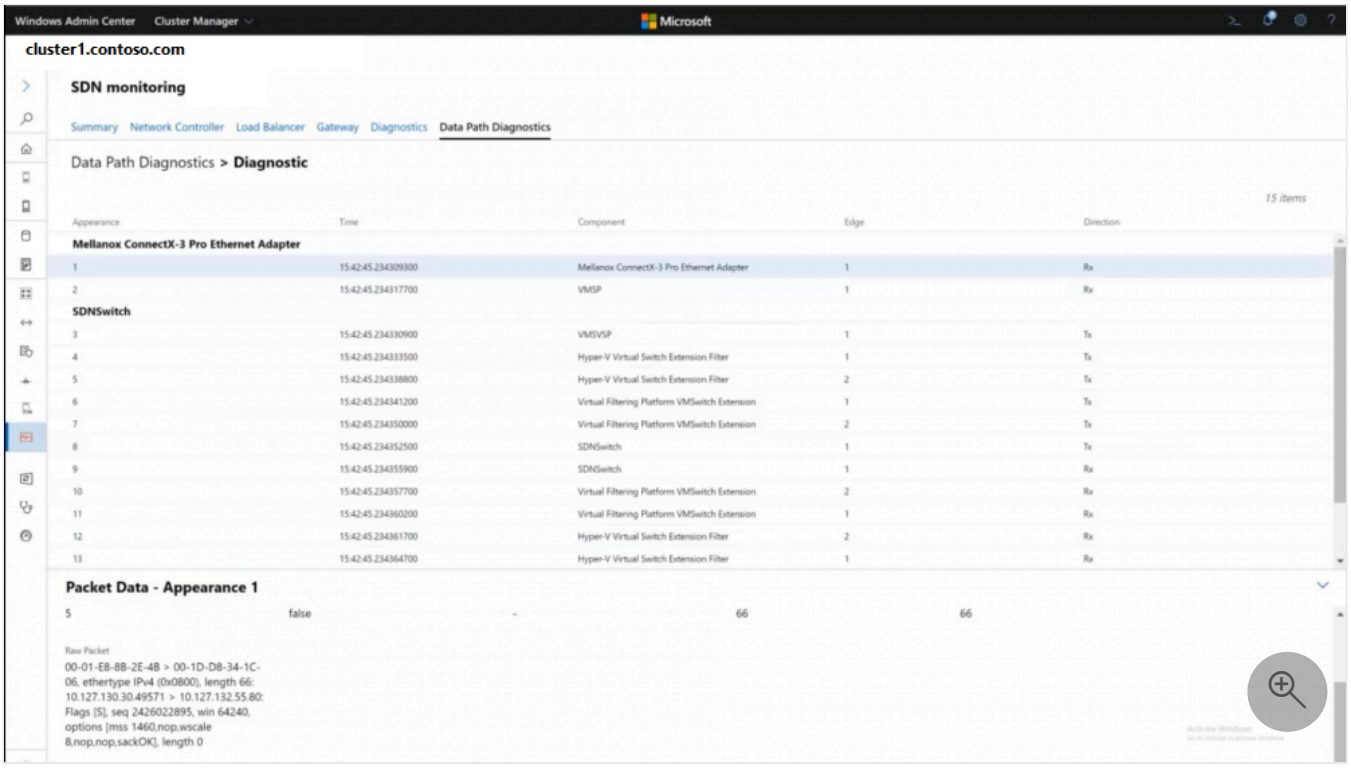
- Les tronçons sont regroupés en fonction des composants impliqués. Chaque adaptateur et les pilotes qui s'y trouvent sont regroupés par nom de l'adaptateur. Cela facilite le suivi du paquet à un niveau élevé par le biais de ces titres de groupe.
- Tous les paquets supprimés sont également affichés en texte rouge pour faciliter leur identification.



Sélectionner un tronçon pour voir plus de détails. Dans les scénarios d'encapsulation et NAT (traduction d'adresses réseau), cette fonctionnalité vous permet de voir le paquet changer à mesure qu'il passe dans la pile réseau et de vérifier les éventuels problèmes de configuration incorrecte.



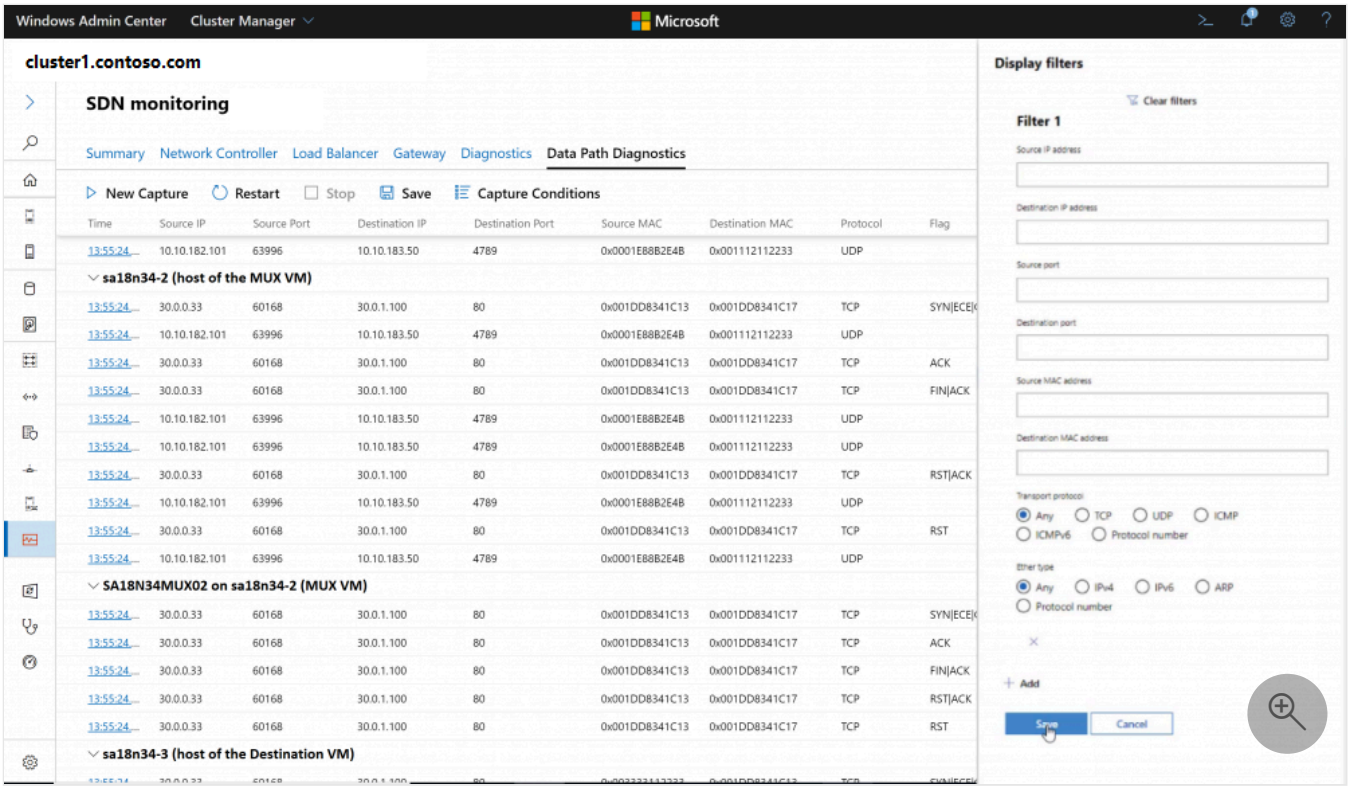
Faites défiler vers le bas pour afficher les détails des paquets bruts :



Afficher les filtres

Les filtres d'affichage vous permettent de filtrer le journal après la capture des paquets. Pour chaque filtre, vous pouvez spécifier des paramètres de paquet comme les adresses MAC, les adresses IP, les ports, l'ethertype et le protocole de transport.

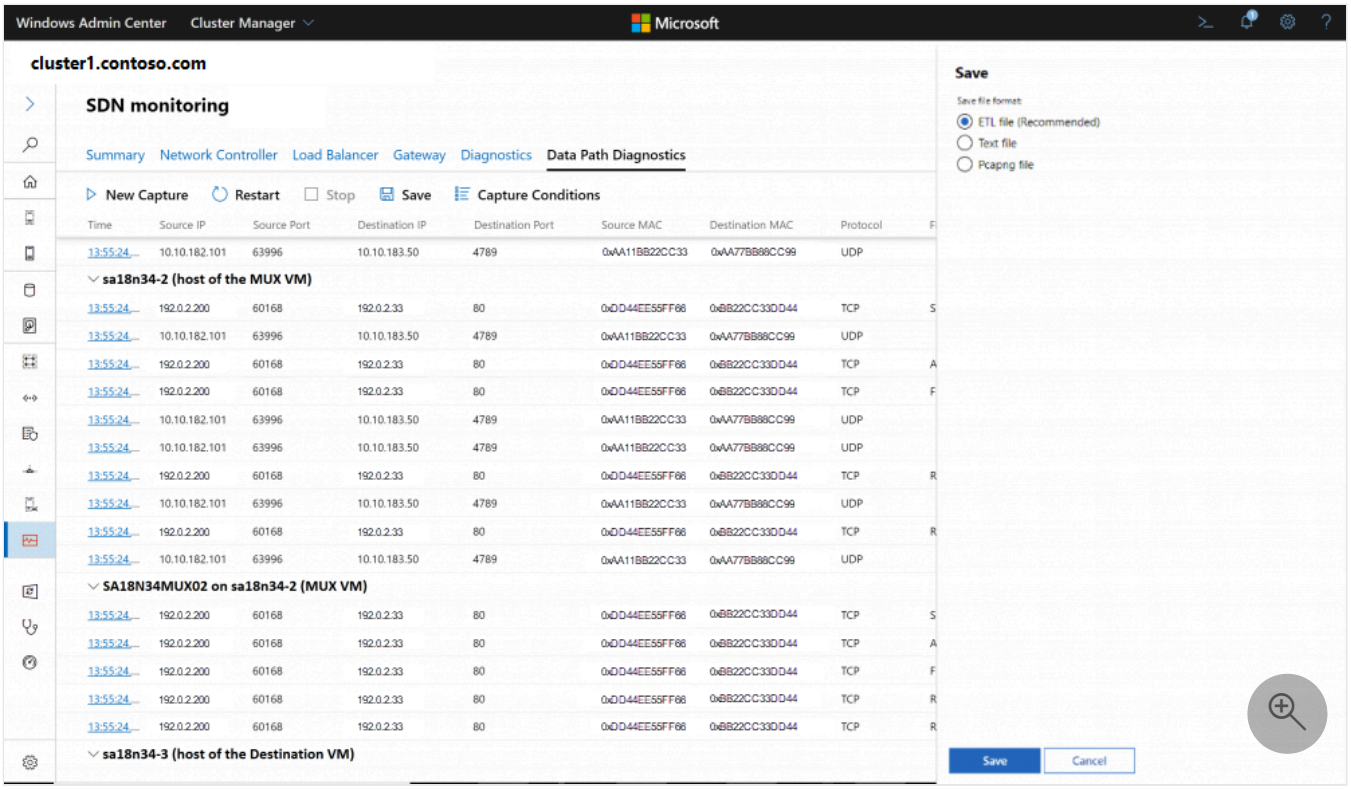
- Les filtres d'affichage peuvent faire la distinction entre la source et la destination des adresses IP, des adresses MAC et des ports.
- Les filtres d'affichage peuvent être supprimés et modifiés après les avoir appliqués pour modifier l'affichage du journal.
- Les filtres d'affichage sont inversés dans les journaux enregistrés.



Save

Le bouton Enregistrer vous permet d'enregistrer le journal sur votre ordinateur local pour une analyse plus approfondie via d'autres outils. Les filtres d'affichage sont inversés dans le journal enregistré. Les journaux peuvent être enregistrés dans différents formats :

- Format ETL qui peut être analysé à l'aide de Microsoft Network Monitor. Remarque : Pour plus d'informations, consultez cette page .
- Format de texte qui peut être analysé à l'aide de n'importe quel éditeur de texte comme TextAnalysisTool.NET.
- Format Pcapng qui peut être analysé à l'aide d'outils comme Wireshark.
  - La plupart des métadonnées du Moniteur de paquets seront perdues pendant cette conversion. Remarque : Pour plus d'informations, consultez cette page .


Windows Admin Center
Cluster Manager
Microsoft
cluster1.contoso.com
SDN monitoring
Summary
Network Controller
Load Balancer
Gateway
Diagnostics
Data Path Diagnostics
New Capture
Restart
Stop
Save
Capture Conditions
Time
Source IP
Source Port
Destination IP
Destination Port
Source MAC
Destination MAC
Protocol
13:55:24... 10.10.182.101 63996 10.10.183.50 4789 0xAA11BB22CC33 0xAA77BB88CC99 UDP
sa18n34-2 (host of the MUX VM)
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 10.10.182.101 63996 10.10.183.50 4789 0xAA11BB22CC33 0xAA77BB88CC99 UDP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 10.10.182.101 63996 10.10.183.50 4789 0xAA11BB22CC33 0xAA77BB88CC99 UDP
13:55:24... 10.10.182.101 63996 10.10.183.50 4789 0xAA11BB22CC33 0xAA77BB88CC99 UDP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 10.10.182.101 63996 10.10.183.50 4789 0xAA11BB22CC33 0xAA77BB88CC99 UDP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 10.10.182.101 63996 10.10.183.50 4789 0xAA11BB22CC33 0xAA77BB88CC99 UDP
SA18N34MUX02 on sa18n34-2 (MUX VM)
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
13:55:24... 192.0.2.200 60168 192.0.2:33 80 0xDD44EE55FF66 0xBB22CC33DD44 TCP
sa18n34-3 (host of the Destination VM)
Save
Save file format:
ETL file (Recommended)
Text file
Pcapng file
Save
Cancel

Pktmon prend en charge Microsoft Network Monitor (Netmon)

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Le moniteur de paquets (Pktmon) génère des journaux au format ETL. Ces journaux peuvent être analysés à l'aide du moniteur réseau Microsoft (Netmon) à l'aide d'analyseurs spéciaux. Cette rubrique explique comment analyser les fichiers ETL générés par le moniteur de paquets dans Netmon.

Configuration et configuration du moniteur réseau

Procédez comme suit pour installer et configurer Netmon pour analyser les fichiers ETL générés par Le moniteur de paquets :

1. Installez le moniteur réseau 3.4.
2. Démarrez le moniteur réseau avec élévation de privilèges et définissez Windows comme profil d'analyseur actif sur (Outils / Options / Profils d'analyseur).
3. Copiez etl_Microsoft-Windows-PktMon-Events.npl d'ici vers «%PROGRAMDATA%\Microsoft\Network Monitor 3\NPL\NetworkMonitor Parsers\Windows »
4. Copiez stub_etl_Microsoft-Windows-PktMon-Events.npl d'ici vers «%PROGRAMDATA%\Microsoft\Network Monitor 3\NPL\NetworkMonitor Parsers\Windows\Stubs »
5. Renommez stub_etl_Microsoft-Windows-PktMon-Events.npl en etl_Microsoft-Windows-PktMon-Events.npl
6. Incluez etl_Microsoft-Windows-PktMon-Events.npl dans NetworkMonitor_Parsers_sparser.npl à l'adresse « %PROGRAMDATA%\Microsoft\Network Monitor 3\NPL\NetworkMonitor Parsers »
7. Redémarrez le moniteur réseau avec élévation de privilèges pour la reconstruction des analyseurs.

Stratégie de qualité de service (QoS)

Article • 13/04/2023

> S’applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016

Vous pouvez utiliser la stratégie de QoS comme point central de gestion de la bande passante réseau sur l’ensemble de votre infrastructure Active Directory en créant des profils QoS, dont les paramètres sont distribués avec la stratégie de groupe.

Notes

Outre cette rubrique, la documentation de Stratégie de QoS suivante est également disponible.

- **Prise en main de la stratégie QoS**
- **Gérer une stratégie de QoS**
- **Questions fréquentes (FAQ) sur la stratégie de qualité de service (QoS)**

Les stratégies de QoS sont appliquées à une session de connexion utilisateur ou à un ordinateur dans le cadre d’un objet de stratégie de groupe (GPO) que vous avez lié à un conteneur Active Directory, tel qu’un domaine, un site ou une unité d’organisation (OU).

La gestion du trafic QoS se produit sous la couche application, ce qui signifie que vos applications existantes n’ont pas besoin d’être modifiées pour bénéficier des avantages fournis par les stratégies QoS.

Systèmes d’exploitation qui prennent en charge la stratégie de QoS

Vous pouvez utiliser la stratégie de QoS pour gérer la bande passante des ordinateurs ou des utilisateurs disposant des systèmes d’exploitation Microsoft suivants.

- Windows Server 2016
- Windows 10
- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2

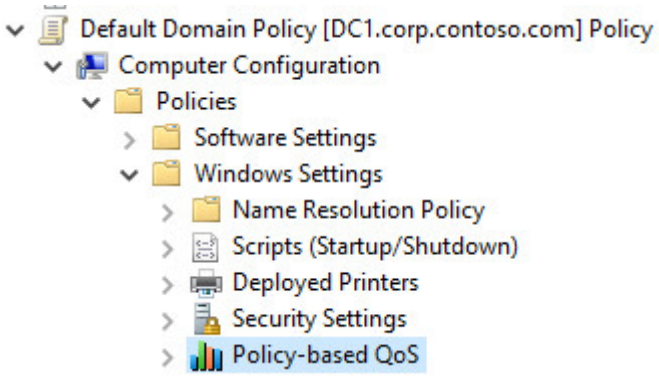
- Windows 7
- Windows Server 2008
- Windows Vista

Emplacement de la stratégie de QoS dans la stratégie de groupe

Dans Windows Server 2016 Stratégie de groupe Éditeur de gestion, le chemin d'accès à la stratégie de QoS pour la configuration de l'ordinateur est le suivant.

Stratégie de domaine par défaut | Configuration de l'ordinateur | Stratégies | Paramètres Windows | QoS basée sur une stratégie

Ce chemin est illustré dans l'image suivante.



Dans Windows Server 2016 Stratégie de groupe Éditeur de gestion, le chemin d'accès à la stratégie de QoS pour la configuration de l'utilisateur est le suivant.

Stratégie de domaine par défaut | Configuration de l'utilisateur | Stratégies | Paramètres Windows | QoS basée sur une stratégie

Par défaut, aucune stratégie de QoS n'est configurée.

Pourquoi utiliser la stratégie de QoS ?

À mesure que le trafic augmente sur votre réseau, il est de plus en plus important pour vous d'équilibrer les performances du réseau avec le coût du service, mais le trafic réseau n'est normalement pas facile à hiérarchiser et à gérer.

Sur votre réseau, les applications critiques et sensibles à la latence doivent concurrencer la bande passante réseau et le trafic de priorité inférieure. Dans le même temps, certains utilisateurs et ordinateurs ayant des exigences de performances réseau spécifiques peuvent nécessiter des niveaux de service différenciés.

Les défis liés à la fourniture de niveaux de performances réseau prévisibles et rentables apparaissent souvent d'abord sur des connexions de réseau étendu (WAN) ou avec des applications sensibles à la latence, telles que la voix sur IP (VoIP) et le streaming vidéo. Toutefois, l'objectif final de fournir des niveaux de service réseau prévisibles s'applique à n'importe quel environnement réseau (par exemple, un réseau local d'entreprise) et à plus d'applications VoIP, telles que les applications métier personnalisées de votre entreprise.

La QoS basée sur des stratégies est l'outil de gestion de la bande passante réseau qui vous fournit un contrôle réseau en fonction des applications, des utilisateurs et des ordinateurs.

Lorsque vous utilisez la stratégie de QoS, vos applications n'ont pas besoin d'être écrites pour des interfaces de programmation d'applications (API) spécifiques. Cela vous donne la possibilité d'utiliser la QoS avec des applications existantes. En outre, la qualité de service basée sur une stratégie tire parti de votre infrastructure de gestion existante, car la QoS basée sur une stratégie est intégrée à stratégie de groupe.

Définir la priorité de QoS par le biais d'un point de code de services différenciés (DSCP)

Vous pouvez créer des stratégies de QoS qui définissent la priorité du trafic réseau avec une valeur DSCP (Differentiated Services Code Point) que vous affectez à différents types de trafic réseau.

Le DSCP vous permet d'appliquer une valeur (0 à 63) dans le champ Type de service (TOS) dans l'en-tête d'un paquet IPv4 et dans le champ Classe de trafic dans IPv6.

La valeur DSCP fournit la classification du trafic réseau au niveau du protocole Internet (IP), que les routeurs utilisent pour décider du comportement de mise en file d'attente du trafic.

Par exemple, vous pouvez configurer des routeurs pour placer des paquets avec des valeurs DSCP spécifiques dans l'une des trois files d'attente suivantes : priorité élevée, effort maximum ou effort inférieur.

Le trafic réseau critique, qui se trouve dans la file d'attente de priorité élevée, a une préférence par rapport aux autres trafics.

Limiter l'utilisation de la bande passante réseau par application avec le taux de limitation

Vous pouvez également limiter le trafic réseau sortant RDP en spécifiant un taux de limitation dans la stratégie de QoS.

Une stratégie de QoS qui définit des taux de limitation détermine le taux de trafic réseau sortant. Par exemple, pour gérer les coûts WAN, un service informatique peut implémenter un contrat de niveau de service qui spécifie qu'un serveur de fichiers ne peut jamais fournir de téléchargements au-delà d'un tarif spécifique.

Utiliser la stratégie de QoS pour appliquer des valeurs DSCP et des taux de limitation

Vous pouvez également utiliser la stratégie de QoS pour appliquer des valeurs DSCP et des taux de limitation pour le trafic réseau sortant aux éléments suivants :

- Envoi du chemin d'accès de l'application et du répertoire
- Adresses ou préfixes d'adresse IPv4 ou IPv6 sources et de destination
- Protocole : Protocole TCP (Transmission Control Protocol) et UDP (User Datagram Protocol)
- Ports source et de destination et plages de ports (TCP ou UDP)
- Groupes spécifiques d'utilisateurs ou d'ordinateurs via le déploiement dans la stratégie de groupe

À l'aide de ces contrôles, vous pouvez spécifier une stratégie de QoS avec une valeur DSCP de 46 pour une application VoIP, ce qui permet aux routeurs de placer des paquets VoIP dans une file d'attente à faible latence, ou vous pouvez utiliser une stratégie de QoS pour limiter le trafic sortant d'un ensemble de serveurs à 512 kilo-octets par seconde (Kbits/s) lors de l'envoi à partir du port TCP 443.

Vous pouvez également appliquer la stratégie de QoS à une application particulière qui a des exigences particulières en bande passante. Pour plus d'informations, consultez les Scénarios de stratégie DNS.

Avantages de la stratégie de QoS

Avec la stratégie de QoS, vous pouvez configurer et appliquer des stratégies de QoS qui ne peuvent pas être configurées sur les routeurs et les commutateurs. La stratégie de QoS fournit les avantages suivants.

1. **Niveau de détail :** il est difficile de créer des stratégies de QoS au niveau de l'utilisateur sur des routeurs ou des commutateurs, en particulier si l'ordinateur de l'utilisateur est configuré à l'aide de l'attribution d'adresses IP dynamiques ou si l'ordinateur n'est pas connecté à des ports de commutateur ou de routeur fixes, comme c'est souvent le cas avec les ordinateurs portables. En revanche, la stratégie de QoS facilite la configuration d'une stratégie de QoS au niveau de l'utilisateur sur un contrôleur de domaine et la propage à l'ordinateur de l'utilisateur.

2. **Flexibilité**. Quel que soit l'emplacement ou la façon dont un ordinateur se connecte au réseau, la stratégie de QoS est appliquée : l'ordinateur peut se connecter à l'aide du Wi-Fi ou d'Ethernet à partir de n'importe quel emplacement. Pour les stratégies de QoS au niveau de l'utilisateur, la stratégie de QoS est appliquée à n'importe quel appareil compatible à n'importe quel emplacement où l'utilisateur se connecte.

3. **Sécurité :** si votre service informatique chiffre le trafic des utilisateurs de bout en bout à l'aide de la sécurité du protocole Internet (IPsec), vous ne pouvez pas classifier le trafic sur les routeurs en fonction des informations au-dessus de la couche IP dans le paquet (par exemple, un port TCP). Toutefois, à l'aide de la stratégie de QoS, vous pouvez classifier les paquets au niveau de l'appareil de fin pour indiquer la priorité des paquets dans l'en-tête IP avant que les charges utiles IP soient chiffrées et que les paquets soient envoyés.

4. **Performance :** certaines fonctions de QoS, telles que la limitation, sont mieux exécutées lorsqu'elles sont plus proches de la source. La stratégie de QoS déplace ces fonctions de QoS le plus près de la source.

5. **Gérabilité :** la stratégie de QoS améliore la gestion du réseau de deux manières :

   a. Étant donné qu'elle est basée sur la stratégie de groupe, vous pouvez utiliser la stratégie de QoS pour configurer et gérer un ensemble de stratégies de qualité de service utilisateur/ordinateur chaque fois que nécessaire, et sur un seul ordinateur de contrôleur de domaine central.

   b. La stratégie de QoS facilite la configuration utilisateur/ordinateur en fournissant un mécanisme permettant de spécifier des stratégies par URL (Uniform Resource Locator) au lieu de spécifier des stratégies basées sur les adresses IP de chacun des serveurs où les stratégies de QoS doivent être appliquées. Par exemple, supposons que votre réseau dispose d'un cluster de serveurs qui partagent une URL commune. En utilisant la stratégie de QoS, vous pouvez créer une stratégie basée sur l'URL commune, au lieu de créer une stratégie pour chaque serveur du cluster, avec chaque stratégie basée sur l'adresse IP de chaque serveur.

Pour la rubrique suivante de ce guide, consultez Prise en main avec la stratégie de QoS.

Prise en main de la stratégie QoS

Article • 30/04/2025 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser les rubriques suivantes pour commencer à utiliser la stratégie de qualité de service (QoS).

- Fonctionnement de la stratégie QoS
- Architecture de stratégie QoS
- Scénarios de stratégie QoS

Pour la première rubrique de ce guide, consultez la stratégie qualité de service (QoS).

Comment fonctionne la stratégie QoS

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Lors du démarrage ou de l'obtention des paramètres de configuration utilisateur ou ordinateur mis à jour stratégie de groupe pour QoS, le processus suivant se produit.

1. Le moteur stratégie de groupe récupère les paramètres de configuration utilisateur ou ordinateur stratégie de groupe à partir d'Active Directory.
2. Le moteur stratégie de groupe informe l'extension QoS Client-Side qu'il y a eu des modifications dans les stratégies QoS.
3. L'extension QoS Client-Side envoie une notification d'événement de stratégie QoS au module d'inspection QoS.
4. Le module d'inspection QoS récupère les stratégies QoS de l'utilisateur ou de l'ordinateur et les stocke.

Lorsqu'un nouveau point de terminaison de couche transport (connexion TCP ou trafic UDP) est créé, le processus suivant se produit.

1. Le composant Couche transport de l'assemblage TCP/IP informe le module d'inspection QoS.
2. Le module d'inspection QoS compare les paramètres du point de terminaison de la couche transport aux stratégies QoS stockées.
3. Si une correspondance est trouvée, le module d'inspection QoS contacte Pacer.sys pour créer un flux, une structure de données contenant la valeur DSCP et les paramètres de limitation du trafic de la stratégie QoS correspondante. S'il existe plusieurs stratégies QoS qui correspondent aux paramètres du point de terminaison de la couche transport, la stratégie QoS la plus spécifique est utilisée.
4. Pacer.sys stocke le flux et retourne un numéro de flux correspondant au flux dans le module d'inspection QoS.
5. Le module d'inspection QoS retourne le numéro de flux à la couche transport.
6. La couche transport stocke le numéro de flux avec le point de terminaison de la couche transport.

Lorsqu'un paquet correspondant à un point de terminaison de la couche transport marqué avec un numéro de flux est envoyé, le processus suivant se produit.

1. La couche transport marque en interne le paquet avec le numéro de flux.
2. Les requêtes de couche réseau Pacer.sys pour la valeur DSCP correspondant au numéro de flux du paquet.
3. Pacer.sys retourne la valeur DSCP à la couche réseau.
4. La couche réseau remplace le champ TOS IPv4 ou le champ Classe de trafic IPv6 par la valeur DSCP spécifiée par Pacer.sys et, pour les paquets IPv4, calcule la somme de contrôle d'en-tête IPv4 finale.
5. La couche réseau remet le paquet à la couche d'encadrement.
6. Étant donné que le paquet a été marqué avec un numéro de flux, la couche d'encadrement remet le paquet à Pacer.sys via NDIS 6.x.
7. Pacer.sys utilise le numéro de flux du paquet pour déterminer si le paquet doit être limité et, le cas échéant, planifie l'envoi du paquet.
8. Pacer.sys remet le paquet immédiatement (s'il n'y a pas de limitation du trafic) ou comme prévu (s'il y a limitation du trafic) à NDIS 6.x pour la transmission sur l'adaptateur réseau approprié.

Ces processus de QoS basée sur une stratégie offrent les avantages suivants.

- L'inspection du trafic pour déterminer si une stratégie QoS s'applique est effectuée par point de terminaison de couche transport, plutôt que par paquet.
- Il n'y a aucun impact sur les performances pour le trafic qui ne correspond pas à une stratégie QoS.
- Les applications n'ont pas besoin d'être modifiées pour tirer parti du service différencié basé sur DSCP ou de la limitation du trafic.
- Les stratégies QoS peuvent s'appliquer au trafic protégé par IPsec.

Pour la rubrique suivante de ce guide, consultez Architecture de la stratégie QoS.

Pour la première rubrique de ce guide, consultez Stratégie de qualité de service (QoS).

Commentaires

Cette page a-t-elle été utile ? Yes No

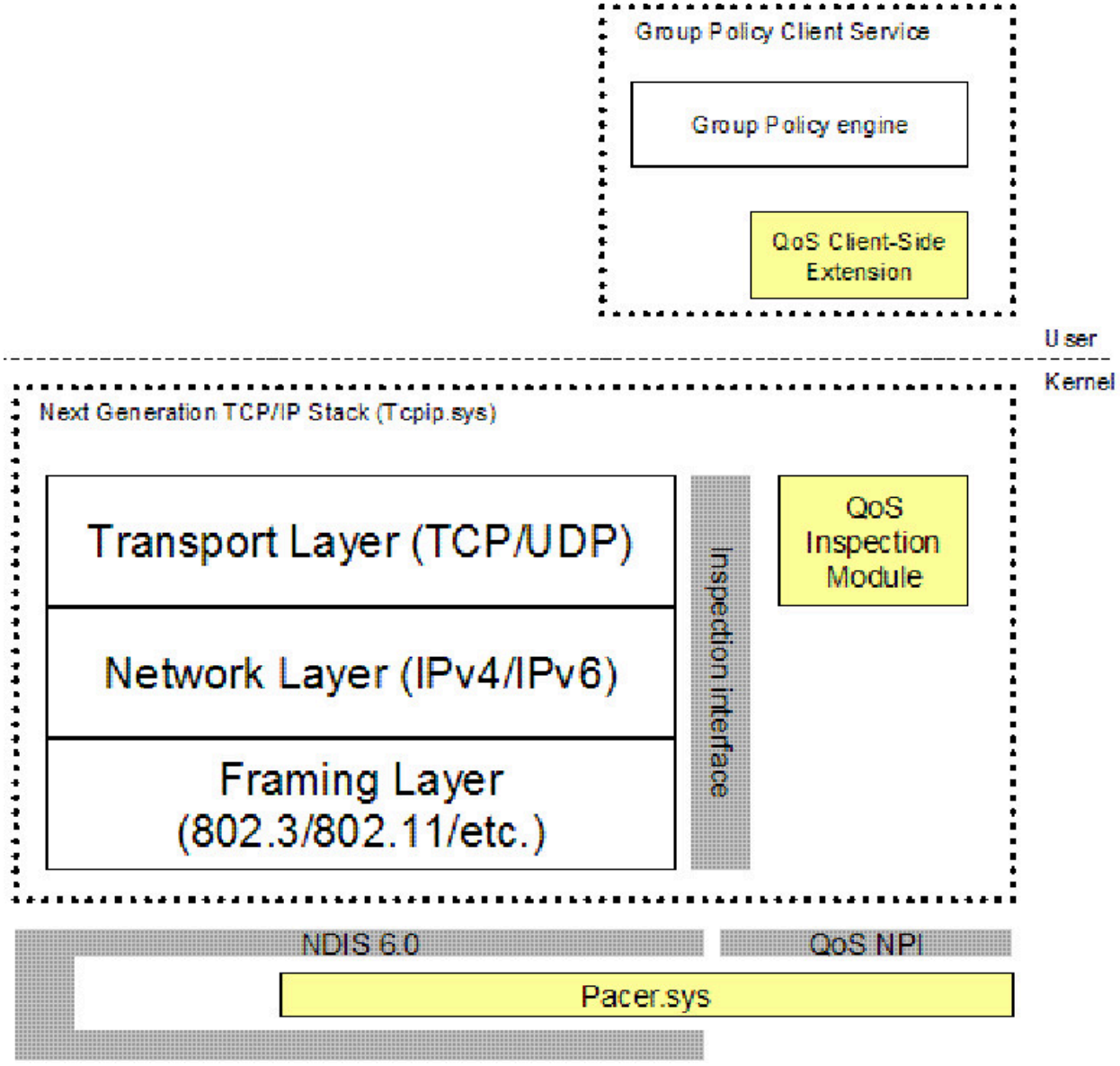
Architecture de la stratégie de qualité de service

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Vous pouvez utiliser cette rubrique pour en savoir plus sur l'architecture de la stratégie QoS.

La figure suivante illustre l'architecture de la QoS basée sur la stratégie.



L'architecture de la QoS basée sur la stratégie est constituée des composants suivants :

- **Service client de la stratégie de groupe**. Service Windows qui gère les paramètres de configuration des utilisateurs et des ordinateurs d'une stratégie de groupe.

- **Moteur de la stratégie de groupe**. Composant du service client d'une stratégie de groupe qui récupère les paramètres de configuration des utilisateurs et des ordinateurs d'une stratégie de groupe à partir d'Active Directory au démarrage et recherche régulièrement les modifications (par défaut, toutes les 90 minutes). Si des modifications sont détectées, le moteur de la stratégie de groupe récupère les nouveaux paramètres de la stratégie de groupe. Le moteur de la stratégie de groupe traite les GPO entrants et informe l'extension QoS côté client quand les stratégies QoS sont mises à jour.

- **Extension QoS côté client**. Composant du service client de la stratégie de groupe qui attend une indication du moteur de stratégie de groupe indiquant que les stratégies QoS ont été modifiées et informe le module d'inspection QoS.

- **Pile TCP/IP**. Pile TCP/IP qui inclut la prise en charge intégrée pour IPv4 et IPv6 et prend en charge la plateforme de filtrage Windows.

- **Module d'inspection QoS**. Composant dans la pile TCP/IP qui attend des indications de modification de la stratégie QoS à partir de l'extension QoS côté client, récupère les paramètres de stratégie QoS et interagit avec la couche transport et Pacer.sys pour marquer en interne le trafic correspondant aux stratégies QoS.

- **NDIS 6.x**. Interface standard entre les pilotes réseau en mode noyau et le système d'exploitation Windows Server et les systèmes d'exploitation Clients. NDIS 6.x prend en charge les filtres légers, qui est un modèle de pilote simplifié pour les pilotes intermédiaires NDIS et les pilotes miniport qui offre de meilleures performances.

- **Interface de fournisseur réseau (NPI) QoS**. Interface permettant aux pilotes en mode noyau d'interagir avec Pacer.sys.

- **Pacer.sys**. Pilote de filtre léger NDIS 6.x qui contrôle la planification des paquets pour la QoS basée sur une stratégie et pour le trafic des applications qui utilisent les API de QoS générique (GQoS) et de contrôle de trafic (TC). Pacer.sys a remplacé Psched.sys dans Windows Server 2003 et Windows XP. Pacer.sys est installé avec le composant Planificateur de paquets QoS à partir des propriétés d'une connexion ou d'une carte réseau.

Pour la rubrique suivante de ce guide, consultez Scénarios de la stratégie QoS.

Pour la première rubrique de ce guide, consultez Stratégie de qualité de service (QoS).

Commentaires

Cette page a-t-elle été utile ? Yes No

Scénarios de stratégie QoS

29/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour passer en revue les scénarios hypothétiques qui montrent comment, quand et pourquoi utiliser la stratégie QoS.

Les deux scénarios de cette rubrique sont les suivants :

1. hiérarchiser le trafic réseau pour une application de cœur de métier ;
2. hiérarchiser le trafic réseau pour une application de serveur HTTP.

> ⓘ **Notes**
>
> Certaines sections de cette rubrique détaillent des étapes générales qui permettent d'effectuer les actions décrites. Pour obtenir des instructions plus détaillées sur la gestion de la stratégie QoS, consultez Gérer la stratégie QoS.

Scénario 1 : hiérarchiser le trafic réseau pour une application de cœur de métier

Dans ce scénario, un service informatique peut atteindre plusieurs objectifs grâce à la stratégie QoS :

- améliorer les performances réseau des applications stratégiques ;
- améliorer les performances réseau d'un jeu clé d'utilisateurs lorsqu'ils utilisent une application spécifique ;
- garantir que l'application de sauvegarde de données à l'échelle de l'entreprise n'entrave pas les performances réseau en utilisant une bande passante trop importante.

Le service informatique décide de configurer la stratégie QoS pour hiérarchiser des applications spécifiques en utilisant des valeurs de point de code de service de différenciation (DSCP) aux fins d'une classification du trafic réseau, et de configurer ses routeurs pour exécuter un traitement préférentiel pour le trafic de priorité supérieure.

> ⓘ **Notes**
>
> Pour plus d'informations sur le service DSCP, consultez la section **Définir la priorité QoS à l'aide d'un point de code de services différenciés** dans la rubrique Stratégie de qualité

de service (QoS).

Outre les valeurs DSCP, les stratégies QoS peuvent spécifier un taux de limitation. La limitation a pour effet de limiter l'intégralité du trafic sortant qui correspond à la stratégie QoS selon un taux d'envoi spécifique.

Configuration de la stratégie QoS

L'administrateur informatique, qui doit accomplir trois objectifs distincts, décide de créer trois stratégies QoS différentes.

Stratégie QoS pour les serveurs d'applications de cœur de métier

La première application stratégique pour laquelle le service informatique crée une stratégie QoS est une application de planification des ressources d'entreprise (ERP) à l'échelle de l'entreprise. L'application ERP est hébergée sur plusieurs ordinateurs sous Windows Server 2016. Dans Active Directory Domain Services, ces ordinateurs sont membres d'une unité d'organisation (UO) créée pour les serveurs d'applications de cœur de métier (LOB). Le composant côté client de l'application ERP est installé sur les ordinateurs sous Windows 10 et Windows 8.1.

Dans la stratégie de groupe, un administrateur informatique sélectionne l'objet de stratégie de groupe (GPO) auquel la stratégie QoS sera appliquée. À l'aide de l'assistant de stratégie QoS, l'administrateur informatique crée une stratégie QoS appelée « Stratégie de cœur de métier de serveur ». Cette dernière spécifie une valeur DSCP de priorité élevée de 44 pour toutes les applications, les adresses IP, les protocoles TCP et UDP, et le numéro de port.

La stratégie QoS est appliquée uniquement aux serveurs de cœur de métier et associe l'objet de stratégie de groupe à l'unité d'organisation qui contient uniquement ces serveurs, et ce, par le biais de l'outil de la console de gestion des stratégies de groupe (GPMC). Cette stratégie de cœur de métier de serveur initiale applique la valeur DSCP de priorité élevée chaque fois que l'ordinateur envoie du trafic réseau. Cette stratégie QoS peut être modifiée ultérieurement (dans l'outil de l'éditeur d'objet de stratégie de groupe) pour inclure les numéros de port de l'application ERP. Cela garantit une application de la stratégie uniquement lorsque le numéro de port spécifié est utilisé.

Stratégie QoS pour le groupe responsable des finances

Bien que de nombreux groupes au sein de l'entreprise accèdent à l'application ERP, les activités et les rapports avec les clients du groupe responsable des finances reposent sur cette application ; cette dernière doit donc constamment garantir des performances élevées.

Pour garantir une relation optimale entre le groupe responsable des finances et ses clients, la stratégie QoS doit classer le trafic de ces utilisateurs en tant que hautement prioritaire. Toutefois, la stratégie ne doit pas s'appliquer lorsque les membres du groupe responsable des finances utilisent des applications autres que l'application ERP.

Pour cette raison, le service informatique définit une deuxième stratégie QoS appelée « Stratégie de cœur de métier de client » dans l'outil de l'éditeur d'objet de stratégie de groupe, qui applique une valeur DSCP de 60 lorsque le groupe d'utilisateurs responsables des finances exécute l'application ERP.

Stratégie QoS pour une application de sauvegarde

Une application de sauvegarde distincte s'exécute sur tous les ordinateurs. Pour s'assurer que le trafic de l'application de sauvegarde n'utilise pas toutes les ressources réseau disponibles, le service informatique crée une stratégie de données de sauvegarde. Cette stratégie de sauvegarde spécifie une valeur DSCP de 1 en fonction du nom exécutable de l'application de sauvegarde, qui est **backup.exe**.

Un troisième GPO est créé et déployé pour tous les ordinateurs des clients du domaine. Chaque fois que l'application de sauvegarde envoie des données, la valeur DSCP de faible priorité est appliquée, même si elle provient d'ordinateurs du service financier.

> **Notes**
>
> Le trafic réseau sans stratégie QoS est envoyé avec une valeur DSCP de 0.

Stratégies applicables au scénario

Le tableau suivant répertorie les stratégies QoS applicables à ce scénario.

Agrandir le tableau

Nom de stratégie	Valeur DSCP	Taux de limitation	Applicable aux unités d'organisation	Descriptif
[Aucune stratégie]	0	Aucun	[Aucun déploiement]	Traitement de meilleur effort (par défaut) pour le trafic non classé.
Données de sauvegarde	1	Aucun	Tous les clients	Applique une valeur DSCP de faible priorité pour ces données en bloc.

Nom de stratégie	Valeur DSCP	Taux de limitation	Applicable aux unités d'organisation	Descriptif
Cœur de métier de serveur	44	Aucun	Unité d'organisation d'ordinateur pour les serveurs ERP	Applique une valeur DSCP de priorité élevée pour le trafic serveur ERP
Cœur de métier de client	soixante	Aucun	Groupe d'utilisateurs responsables des finances	Applique une valeur DSCP de priorité élevée pour le trafic client ERP

> **Notes**
>
> Les valeurs DSCP présentent une forme décimale.

Lorsque les stratégies QoS sont définies et appliquées à l'aide de la stratégie de groupe, le trafic réseau sortant reçoit la valeur DSCP spécifiée par la stratégie. Les routeurs assurent ensuite un traitement différentiel basé sur ces valeurs DSCP grâce au processus de mise en file d'attente. Pour le service informatique, les routeurs sont configurés selon quatre files d'attente : priorité élevée, priorité moyenne, meilleur effort et priorité faible.

Lorsque le trafic arrive au niveau du routeur avec les valeurs DSCP de la « stratégie de cœur de métier de serveur » et de la « stratégie de cœur de métier de client », les données sont placées dans des files d'attente de priorité élevée. Le trafic dont la valeur DSCP est de 0 se voit attribuer un niveau de service de meilleur effort. Les paquets dont la valeur DSCP est 1 (en provenance de l'application de sauvegarde) se voient attribuer un traitement de faible priorité.

Conditions préalables à la hiérarchisation d'une application de cœur de métier

Pour effectuer cette tâche, assurez-vous de satisfaire aux exigences suivantes :

- Les ordinateurs impliqués exécutent des systèmes d'exploitation compatibles QoS.
- Les ordinateurs impliqués font partie d'un domaine Active Directory Domain Services (AD DS) afin de pouvoir être configurés à l'aide de la stratégie de groupe.
- Les réseaux TCP/IP sont configurés avec des routeurs configurés pour DSCP (RFC 2474). Pour plus d'informations, consultez RFC 2474.
- Les exigences inhérentes aux informations d'identification d'administration sont satisfaites.

Informations d'identification d'administration

Pour effectuer cette tâche, vous devez être en mesure de créer et de déployer des objets de stratégie de groupe.

Configuration de l'environnement de test pour hiérarchiser une application de cœur de métier

Pour configurer cet environnement de test, procédez comme suit :

- Créez un domaine AD DS avec des clients et des utilisateurs regroupés en unités d'organisation. Pour obtenir des instructions sur le déploiement du service AD DS, consultez le Guide de réseau central.
- Configurez les routeurs pour qu'ils assurent un processus de mise en file d'attente différentielle en fonction des valeurs DSCP. Par exemple, la valeur DSCP 44 est placée dans une file d'attente « Platinum », et toutes les autres valeurs sont placées dans une file d'attente équitable et pondérée.

> **Notes**
>
> Vous pouvez afficher les valeurs DSCP à l'aide de captures réseau et d'outils tels que le moniteur réseau. Après avoir effectué une capture réseau, vous pouvez observer le champ TOS dans les données capturées.

Étapes de hiérarchisation d'une application de cœur de métier

Pour hiérarchiser une application de cœur de métier, procédez comme suit :

1. Créez un objet de stratégie de groupe (GPO) et associez-le à une stratégie QoS.
2. Configurez les routeurs pour qu'ils traitent de manière différentielle une application de cœur de métier (selon un processus de mise en file d'attente) en fonction des valeurs DSCP sélectionnées. Les procédures de cette tâche varient en fonction du type de routeurs dont vous disposez.

Scénario 2 : hiérarchiser le trafic réseau pour une application de serveur HTTP

Dans Windows Server 2016, la stratégie QoS basée sur une stratégie inclut les stratégies basées sur les URL de fonctionnalité. Les stratégies d'URL vous permettent de gérer la bande passante

des serveurs HTTP.

De nombreuses applications d'entreprise sont développées et hébergées sur des serveurs Web Internet Information Services (IIS), et les applications Web sont accessibles depuis les navigateurs sur les ordinateurs client.

Dans ce scénario, supposons que vous gériez un jeu de serveurs IIS qui hébergent des vidéos de formation pour tous les employés de votre organisation. Votre objectif est de veiller à ce que le trafic provenant de ces serveurs vidéo ne surcharge pas votre réseau et de vous assurer que le trafic vidéo est différencié du trafic vocal et de données sur le réseau.

La tâche est semblable à celle du scénario 1. Vous allez concevoir et configurer les paramètres de gestion du trafic, tels que la valeur DSCP du trafic vidéo et le taux de limitation, de la même manière que vous le feriez pour les applications de cœur de métier. Toutefois, pour spécifier le trafic, au lieu de fournir le nom de l'application, entrez uniquement l'URL à laquelle votre application serveur HTTP répondra : par exemple, https://hrweb/training..

> **Notes**
>
> Vous ne pouvez pas utiliser de stratégies QoS basées sur une URL pour hiérarchiser le trafic réseau des ordinateurs exécutant des systèmes d'exploitation Windows antérieurs à Windows 7 et à Windows Server 2008 R2.

Règles de priorité pour les stratégies basées sur des URL

Les URL suivantes sont toutes valides ; elles peuvent donc être spécifiées dans la stratégie QoS et être appliquées simultanément à un ordinateur ou à un utilisateur :

- https://video
- `https://training.hr.mycompany.com`
- https://10.1.10.249:8080/tech
- https ://*/ebooks

Mais laquelle sera prioritaire ? Les règles sont simples. Les stratégies basées sur des URL sont hiérarchisées selon un ordre de lecture de gauche à droite. Ainsi, de la priorité la plus élevée à la priorité la plus faible, les champs d'URL sont les suivants :

1. Modèle d'URL

2. Hôte d'URL

3. Port d'URL

4. Chemin d'URL

Les détails sont les suivants :

1. Modèle d'URL

La priorité de `https://` est plus élevée que celle de `https://`.

2. Hôte d'URL

De la priorité la plus élevée à la plus faible :

1. HostName
2. Adresse IPv6
3. Adresse IPv4
4. Caractère générique

Dans le cas d'un nom d'hôte, un nom d'hôte comportant plus d'éléments séparés par un point (plus de profondeur) a une priorité plus élevée qu'un nom d'hôte avec moins d'éléments séparés par un point. Par exemple, parmi les noms d'hôte suivants :

- video.internal.training.hr.mycompany.com (profondeur = 6)
- selfguide.training.mycompany.com (profondeur = 4)
- training (profondeur = 1)
- library (profondeur = 1)

  La priorité de **video.internal.training.hr.mycompany.com** est la plus élevée. La priorité de **selfguide.training.mycompany.com** est la deuxième plus élevée. **Training** et **library** ont la même priorité, qui est la plus faible.

3. Port d'URL

Un numéro de port spécifique ou implicite a une priorité plus élevée qu'un port générique.

4. Chemin d'URL

À l'instar d'un nom d'hôte, un chemin d'URL peut se composer de plusieurs éléments. Le chemin qui comporte plus d'éléments a toujours une priorité plus élevée qu'un chemin qui en comporte moins. Par exemple, les chemins suivants sont répertoriés par priorité :

1. /ebooks/tech/windows/networking/qos
2. /ebooks/tech/windows/
3. /livres numériques
4. /

Si un utilisateur choisit d'inclure tous les sous-répertoires et fichiers suivant un chemin d'URL, ce chemin d'URL aura une priorité inférieure à celle qu'il aurait si l'utilisateur n'avait pas fait de choix.

Un utilisateur peut également choisir de spécifier une adresse IP de destination dans une stratégie basée sur une URL. L'adresse IP de destination présente une priorité inférieure à l'un des quatre champs d'URL décrits précédemment.

Stratégie quintuple

Une stratégie quintuple est spécifiée par l'ID de protocole, l'adresse IP source, le port source, l'adresse IP de destination et le port de destination. Une stratégie quintuple a toujours une priorité plus élevée que n'importe quelle stratégie basée sur une URL.

Si une stratégie quintuple est déjà appliquée à un utilisateur, une nouvelle stratégie basée sur une URL n'entraîne aucun conflit sur les ordinateurs client de cet utilisateur.

Pour la rubrique suivante de ce guide, consultez Gérer la stratégie QoS.

Pour la première rubrique de ce guide, consultez Stratégie de qualité de service (QoS).

Gérer une stratégie de QoS

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Vous pouvez utiliser cette rubrique pour en savoir plus sur l'utilisation de l'Assistant Stratégie de QoS pour créer, modifier ou supprimer une stratégie de QoS.

> ⓘ **Notes**
>
> Outre cette rubrique, la documentation de gestion de stratégie de QoS suivante est également disponible.
>
> - Erreurs et événements de stratégie QoS

Dans les systèmes d'exploitation Windows, la stratégie de QoS combine les fonctionnalités de la QoS basée sur les normes avec la facilité de gestion de la stratégie de groupe. La configuration de cette combinaison simplifie l'application des stratégies de QoS aux objets de stratégie de groupe. Windows inclut un Assistant de Stratégie de QoS pour vous aider à effectuer les tâches suivantes.

- Créer une stratégie QoS
- Afficher, modifier ou supprimer une stratégie QoS

Créer une stratégie QoS

Avant de créer une stratégie de QoS, il est important de comprendre les deux principaux contrôles de QoS utilisés pour gérer le trafic réseau :

- Valeur DSCP
- Taux de limitation

Hiérarchisation du trafic avec DSCP

Comme indiqué dans l'exemple d'application métier précédent, vous pouvez définir la priorité du trafic réseau sortant à l'aide de **Spécifier la valeur DSCP** pour configurer une stratégie QoS avec une valeur DSCP spécifique.

Comme décrit dans RFC 2474, DSCP permet de spécifier des valeurs comprises entre 0 et 63 dans le champ TOS d'un paquet IPv4 et dans le champ Classe de trafic dans IPv6. Les routeurs réseau utilisent la valeur DSCP pour classer les paquets réseau et les mettre dans la file d'attente de manière appropriée.

> ⓘ **Notes**
>
> Par défaut, le trafic Windows a une valeur DSCP de 0.

Le nombre de files d'attente et la définition de leur priorité doivent être décidés dans le cadre de la stratégie de QoS de votre organisation. Par exemple, votre organisation peut choisir d'avoir cinq files d'attente : trafic sensible à la latence, contrôle du trafic, trafic critique pour l'entreprise, trafic du meilleur effort et trafic de transfert de données en bloc.

Limitation du trafic

Avec les valeurs DSCP, la limitation est un autre contrôle clé pour la gestion de la bande passante réseau. Comme mentionné auparavant, vous pouvez utiliser le paramètre **Spécifier le taux d'accélération** pour configurer une stratégie de QoS avec un taux d'accélération spécifique pour le trafic sortant. En utilisant la limitation de bande passante, une stratégie de QoS limite le trafic réseau sortant à un taux d'accélération spécifique. Le marquage DSCP et la limitation de bande passante peuvent être utilisés conjointement pour gérer efficacement le trafic.

> ⓘ **Notes**
>
> Par défaut, la case à cocher **Spécifier le taux d'accélération** n'est pas activée.

Pour créer une stratégie de QoS, modifiez les paramètres d'un objet de stratégie de groupe dans l'outil de Console de gestion des stratégies de groupe (GPMC, Group Policy Management Console). GpMC ouvre ensuite l'Éditeur d'objet stratégie de groupe.

Les noms des stratégies de QoS doivent être uniques. La façon dont les stratégies sont appliquées aux serveurs et aux utilisateurs finaux dépend de l'emplacement où la stratégie QoS est stockée dans l'éditeur d'objets stratégie de groupe :

- Une stratégie de QoS dans Configuration ordinateur\Paramètres Windows\Stratégie de QoS s'applique aux ordinateurs, quel que soit l'utilisateur actuellement connecté. Les stratégies de QoS basées sur un ordinateur sont généralement utilisées pour les ordinateurs serveurs.

- Une stratégie de QoS dans Configuration utilisateur\Paramètres Windows\stratégie de QoS s'applique aux utilisateurs une fois qu'ils se sont connectés, quel que soit l'ordinateur auquel ils se sont connectés.

Pour créer une stratégie de QoS avec l'Assistant de stratégie de QoS

- Dans l'éditeur d'objets de stratégie de groupe, cliquez à droite sur les nœuds **QoS Policy**, puis cliquez sur **Créer une nouvelle stratégie**.

Assistant page 1 - Profil de stratégie

Sur la première page de l'Assistant de stratégie de QoS, vous pouvez spécifier un nom de stratégie et configurer la manière dont la QoS contrôle le trafic réseau sortant.

Pour configurer la page Profil de stratégie de l'Assistant QoS basée sur la stratégie

1. Dans **Nom de la stratégie**, tapez le nom de la stratégie de QoS. Le nom doit identifier la stratégie de manière unique.
2. Vous pouvez éventuellement utiliser **Spécifier la valeur DSCP** pour activer le marquage DSCP, puis configurer une valeur DSCP comprise entre 0 et 63.
3. Vous pouvez éventuellement utiliser **Spécifier le taux d'accélération** pour activer le limitation du trafic et configurer le taux d'accélération. La valeur du taux d'accélération doit être supérieure à 1 et vous pouvez spécifier des unités de kilo-octets par seconde (Ko/s) ou de mégaoctets par seconde (Mo/s).
4. Cliquez sur **Suivant**.

Assistant page 2 - Nom de l'application

Dans la deuxième page de l'Assistant de Stratégie de QoS, vous pouvez appliquer la stratégie à toutes les applications, à une application spécifique, comme identifiée par son nom exécutable, à un chemin d'accès et un nom d'application, ou aux applications serveur HTTP qui gèrent les demandes pour une URL spécifique.

- L'option **Toutes les applications** spécifie que les paramètres de gestion du trafic définis sur le première page de l'Assistant de stratégie QoS s'appliquent à toutes les applications.
- L'option **Uniquement les applications possédant ce nom exécutable** spécifie que les paramètres de gestion du trafic définis sur la première page de l'Assistant de stratégie

QoS s'appliquent à une application spécifique. Le nom du fichier exécutable doit se terminer par l'extension de nom de fichier .exe.

- L'option **Seules les applications de serveur HTTP répondant aux demandes de cette URL** spécifie que les paramètres de gestion du trafic sur la première page de l'Assistant de stratégie QoS s'appliquent uniquement à certaines applications serveur HTTP.

Vous pouvez éventuellement entrer le chemin d'accès de l'application. Pour spécifier le chemin d'accès à une application, indiquez le chemin d'accès en plus du nom de l'application. Le chemin d'accès peut inclure des variables d'environnement. Par exemple, %ProgramFiles%\Chemin_De_Mon_Application\MonApp.exe, ou c:\program files\chemin_de_mon_application\monapp.exe.

> **Notes**
>
> Le chemin d'accès de l'application ne peut pas inclure de chemin d'accès qui se résout en lien symbolique.

L'URL doit être conforme à RFC 1738, sous la forme `http[s]://<hostname\>:<port\>/<url-path>`. Vous pouvez utiliser un caractère générique, `'*'`, pour `<hostname>` et/ou `<port>`, par exemple `https://training.\*/, https://\*.\*`, mais le caractère générique ne peut pas désigner une sous-chaîne de `<hostname>` ou `<port>`.

En d'autres termes, ni `https://my\*site/`, ni `https://\*training\*/` n'est valide.

Si vous le souhaitez, vous pouvez cocher **Inclure des sous-répertoires et des fichiers** pour effectuer une correspondance sur tous les sous-répertoires et fichiers qui suivent une URL. Par exemple, si cette option est cochée et que l'URL est `https://training`, la stratégie de QoS prend en compte les demandes pour `https://training/video` une bonne correspondance.

Pour configurer la page Nom de l'application de l'Assistant de stratégie de QoS

1. Dans **Cette stratégie de QoS s'applique à**, sélectionnez soit **Toutes les applications**, soit **Uniquement les applications possédant ce nom d'exécutable**.
2. Si vous sélectionnez **Uniquement les applications possédant ce nom d'exécutable**, spécifiez un nom d'exécutable se terminant par l'extension de nom de fichier .exe.
3. Cliquez sur **Suivant**.

Assistant page 3 - Adresses IP

Dans la troisième page de l'Assistant de Stratégie de QoS, vous pouvez spécifier des conditions d'adresse IP pour la stratégie de QoS, notamment les suivantes :

- Toutes les adresses IPv4 ou IPv6 sources ou des adresses IPv4 ou IPv6 sources spécifiques.
- Toutes les adresses IPv4 ou IPv6 de destination ou des adresses IPv4 ou IPv6 de destination spécifiques

Si vous sélectionnez **Uniquement pour l'adresse ou le préfixe IP source suivant** ou **Uniquement pour l'adresse ou le préfixe IP de destination suivant**, vous devez taper l'un des éléments suivants :

- une adresse IPv4, telle que `192.168.1.1`
- Un préfixe d'adresse IPv4 utilisant la notation de préfixe réseau, tel que `192.168.1.0/24`
- Une adresse IPv6, telle que `3ffe:ffff::1`
- Un préfixe d'adresse IPv6, tel que `3ffe:ffff::/48`

Si vous sélectionnez **Uniquement pour l'adresse ou le préfixe IP source suivant** et **Uniquement pour l'adresse ou le préfixe IP de destination suivant**, les adresses et les préfixes d'adresses doivent être des adresses/préfixes IPv4 ou IPv6.

Si vous avez spécifié l'URL des applications serveur HTTP dans la page précédente de l'Assistant, vous remarquerez que l'adresse IP source de la stratégie de QoS sur cette page de l'Assistant est grisée.

Cela est vrai, car l'adresse IP source est l'adresse du serveur HTTP et elle n'est pas configurable ici. En revanche, vous pouvez toujours personnaliser la stratégie en spécifiant l'adresse IP de destination. Cela vous permet de créer différentes stratégies pour différents clients à l'aide des mêmes applications serveur HTTP.

Pour configurer la page Adresses IP de l'assistant de politique de QoS

1. Dans **Cette stratégie de QoS s'applique à** (source), sélectionnez **Toute adresse IP source** ou **Uniquement pour l'adresse ou le préfixe IP source suivant**.
2. Si vous sélectionnez **Uniquement pour l'adresse ou le préfixe IP source suivant**, spécifiez une adresse ou un préfixe IPv4 ou IPv6.
3. Dans **Cette stratégie de QoS s'applique à** (destination), sélectionnez **Toute adresse IP de destination** ou **Uniquement pour l'adresse ou le préfixe IP de destination suivant.**

4. Si vous sélectionnez **Uniquement pour l'adresse ou le préfixe IP de destination suivant**, spécifiez une adresse ou un préfixe IPv4 ou IPv6 qui correspond au type d'adresse ou de préfixe spécifié pour l'adresse source.

5. Cliquez sur **Suivant**.

Assistant page 4 - Protocoles et ports

Sur la quatrième page de l'Assistant de stratégie de QoS, vous pouvez spécifier les types de trafic et les ports qui sont contrôlés par les paramètres définis sur la première page de l'Assistant. Vous pouvez spécifier les valeurs suivantes :

- trafic TCP, trafic UDP ou les deux ;
- tous les ports sources, une plage de ports sources ou un port source spécifique ;
- Tous les ports de destination, une plage de ports de destination ou un port de destination spécifique

Pour configurer la page Protocoles et ports de l'Assistant de stratégie de QoS

1. Dans **Sélectionnez le protocole auquel s'applique cette stratégie de QoS**, sélectionnez **TCP**, **UDP** ou **TCP et UDP**.

2. Dans **Spécifiez le numéro de port source**, sélectionnez **À partir d'un port source quelconque** ou **À partir de ce numéro de port ou plage source**.

3. Si vous avez sélectionné **À partir de ce numéro de port source**, tapez un numéro de port compris entre 1 et 65535.

   Vous pouvez éventuellement spécifier une plage de ports, au format « *Bas*:*Haut*,» où *Bas* et *Haut* représentent les limites inférieures et supérieures de la plage de ports. *Faible* et *Élevé* doivent être des nombres compris entre 1 et 65535. Aucun espace n'est autorisé entre les deux-points (:) et les nombres.

4. Dans **Spécifiez le numéro de port de destination**, sélectionnez **Vers un port de destination quelconque** ou **Vers ce numéro de port ou plage de destination**.

5. Si vous avez sélectionné **Vers ce numéro de port ou plage de destination** à l'étape précédente, tapez un numéro de port compris entre 1 et 65535.

Pour terminer la création de la nouvelle stratégie de QoS, cliquez sur **Terminer** dans la page **Protocoles et Ports** de l'Assistant de stratégie de QoS. Une fois terminée, la nouvelle stratégie

QoS est répertoriée dans le volet Détails de l'éditeur d'objets de stratégie de groupe.

Pour appliquer les paramètres de stratégie QoS aux utilisateurs ou à des ordinateurs, liez l'objet de stratégie de groupe dans lequel se trouvent les stratégies de QoS à un conteneur Active Directory Domain Services, comme un domaine, un site ou une unité d'organisation.

Afficher, modifier ou supprimer une stratégie QoS

Les pages de l'Assistant de stratégie de QoS décrites précédemment correspondent aux pages de propriétés qui apparaissent lorsque vous affichez ou modifiez les propriétés d'une stratégie.

Pour afficher les propriétés d'une stratégie de QoS

- Cliquez avec le bouton droit sur le nom de la stratégie dans le volet de l'Éditeur d'objet de stratégie de groupe, puis cliquez sur **Propriétés**.

  L'éditeur d'objets de stratégie de groupe affiche la page des propriétés avec les onglets suivants :

  - Profil de stratégie
  - Nom de l'application
  - Adresses IP
  - Protocoles et ports

Pour modifier une stratégie de QoS

- Cliquez avec le bouton droit sur le nom de la stratégie dans le volet de l'Éditeur d'objet de stratégie de groupe, puis cliquez sur **Modifier la stratégie existante**.

  L'éditeur d'objet de stratégie de groupe affiche la boîte de dialogue **Modifier une stratégie de QoS existante**.

Pour supprimer une stratégie de QoS

- Cliquez avec le bouton droit sur le nom de la stratégie dans le volet de l'Éditeur d'objet de stratégie de groupe, puis cliquez sur **Supprimer la stratégie**.

Création de rapports sur la console de gestion des stratégies de groupe QoS

Une fois que vous avez appliqué un certain nombre de stratégies de QoS au sein de votre organisation, il peut être utile ou nécessaire d'examiner régulièrement la façon dont les stratégies sont appliquées. Un résumé des stratégies de QoS pour un utilisateur ou un ordinateur spécifique peut être affiché à l'aide de la création de rapports GPMC.

Pour exécuter l'Assistant de résultats de stratégie de groupe pour un rapport de stratégies de QoS

- Dans GPMC, cliquez avec le bouton droit sur le nœud **Résultats de stratégie de groupe**, puis sélectionnez l'option de menu pour l'**Assistant de résultats de stratégie de groupe.**

Une fois les résultats de stratégie de groupe générés, cliquez sur l'onglet **Paramètres**. Sous l'onglet **Paramètres**, les stratégies de QoS se trouvent sous les nœuds « Configuration ordinateur\Paramètres Windows\Stratégie de QoS » et « Configuration utilisateur\Paramètres Windows\Stratégie de QoS ».

Sous l'onglet **Paramètres**, les stratégies de QoS sont répertoriées par leur nom de stratégie de QoS avec leur valeur DSCP, leur taux de limitation, leurs conditions de stratégie et les GPO gagnants répertoriés sur la même ligne.

La vue des résultats de stratégie de groupe identifie de manière unique le GPO gagnant. Lorsque plusieurs GPO ont des stratégies DE QoS avec le même nom de stratégie DE QoS, le GPO avec la priorité de GPO la plus élevée est appliqué. Il s'agit du GPO gagnant. Les stratégies de QoS en conflit (identifiées par le nom de la stratégie) qui sont attachées à un GPO de priorité inférieure ne sont pas appliquées. Notez que les priorités des GPO définissent les stratégies de QoS déployées dans le site, le domaine ou l'unité d'organisation, le cas échéant. Après le déploiement, au niveau de l'utilisateur ou de l'ordinateur, les règles de priorité de la stratégie de QoS déterminent quel trafic est autorisé et bloqué.

La valeur DSCP, le taux de limitation et les conditions de stratégie de la stratégie de QoS sont également visibles dans l'éditeur d'objet de stratégie de groupe (GPOE)

Paramètres avancés pour les utilisateurs itinérants et distants

Avec la stratégie de QoS, l'objectif est de gérer le trafic sur le réseau d'une entreprise. Dans les scénarios mobiles, les utilisateurs peuvent envoyer du trafic sur ou hors du réseau d'entreprise. Étant donné que les stratégies de QoS ne sont pas pertinentes en dehors du réseau de l'entreprise, les stratégies de QoS sont activées uniquement sur les interfaces réseau connectées à l'entreprise pour Windows 8, Windows 7 ou Windows Vista.

Par exemple, un utilisateur peut connecter son ordinateur portable au réseau de son entreprise via un réseau privé virtuel (VPN) à partir d'un café. Pour le VPN, les stratégies de QoS ne seront

pas appliquées à l'interface réseau physique (par exemple, sans fil). Toutefois, des stratégies de QoS seront appliquées à l'interface VPN, car elle se connecte à l'entreprise. Si l'utilisateur entre ultérieurement dans le réseau d'une autre entreprise qui n'a pas de relation d'approbation AD DS, les stratégies de QoS ne sont pas activées.

Notez que ces scénarios mobiles ne s'appliquent pas aux charges de travail du serveur. Par exemple, un serveur avec plusieurs cartes réseau peut se trouver à la périphérie du réseau d'une entreprise. Le service informatique peut choisir d'avoir des stratégies de QoS qui limitent le trafic affectant l'entreprise ; toutefois, cette carte réseau qui envoie ce trafic de sortie ne se connecte pas nécessairement au réseau d'entreprise. Pour cette raison, les stratégies de QoS sont toujours activées sur toutes les interfaces réseau d'un ordinateur exécutant Windows Server 2012.

> ⓘ **Notes**
>
> L'activation sélective s'applique uniquement aux stratégies de QoS et non aux paramètres de QoS avancés abordés ensuite dans ce document.

Paramètres avancés de QoS

Les paramètres de QoS avancés fournissent des contrôles supplémentaires pour les administrateurs informatiques, afin de gérer la consommation du réseau des ordinateurs et les marquages DSCP. Les paramètres de QoS avancés s'appliquent uniquement au niveau de l'ordinateur, tandis que les stratégies de QoS peuvent être appliquées au niveau de l'ordinateur et de l'utilisateur.

Pour configurer les paramètres de QoS avancés

1. Cliquez sur **Configuration de l'ordinateur**, puis sur **Paramètres Windows dans stratégie de groupe**.

2. Cliquez avec le bouton droit sur **Stratégie de QoS**, puis cliquez sur **Paramètres de QoS avancés**.

   La figure suivante montre les deux onglets de paramètres de QoS avancés : **Trafic TCP entrant** et **Remplacement du marquage DSCP**.

> ⓘ **Notes**

Les paramètres de QoS avancés sont des paramètres de stratégie de groupe au niveau de l'ordinateur.

Paramètres de QoS avancés : trafic TCP entrant

Le **trafic TCP entrant** contrôle la consommation de bande passante TCP côté récepteur, tandis que les stratégies QoS affectent le trafic TCP et UDP sortant.

En définissant un niveau de débit inférieur sous l'onglet **Trafic TCP entrant**, TCP limite la taille de sa fenêtre de réception TCP annoncée. L'effet de ce paramètre sera l'augmentation des débits et l'utilisation des liaisons pour les connexions TCP avec des bandes passantes ou des latences plus élevées (produit de délai de bande passante). Par défaut, les ordinateurs exécutant Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows Server 2008 et Windows Vista sont définis sur le niveau de débit maximal.

La fenêtre de réception TCP a changé dans Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows Server 2008 et Windows Vista à partir des versions précédentes de Windows. Les versions précédentes de Windows limitait la fenêtre TCP côté réception à un maximum de 64 ko, tandis que Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows Server 2008 et Windows Vista dimensionnent dynamiquement la fenêtre côté réception jusqu'à 16 mégaoctets (Mo). Dans le contrôle Trafic TCP entrant, vous pouvez contrôler le niveau de débit entrant en définissant la valeur maximale à laquelle la fenêtre de réception TCP peut croître. Les niveaux correspondent aux valeurs maximales suivantes.

Agrandir le tableau

Niveau de débit entrant	Maximale
0	64 Ko
1	256 kB
2	1 Mo
3	16 Mo

La taille réelle de la fenêtre peut être d'une valeur égale ou inférieure à la valeur maximale, en fonction des conditions réseau.

Pour définir la fenêtre côté réception TCP

1. Dans l'éditeur d'objet de stratégie de groupe, cliquez sur **Stratégie d'ordinateur local**, sur **Paramètres Windows**, sur **Stratégie de QoS** avec le bouton droit, puis sur **Paramètres de**

QoS avancés.

2. Dans **Débit de réception TCP**, sélectionnez **Configurer le débit de réception TCP**, puis sélectionnez le niveau de débit souhaité.

3. Liez le GPO à l'unité d'organisation.

Paramètres de QoS avancés : Remplacement du marquage DSCP

La substitution de marquage DSCP limite la capacité des applications à spécifier, ou à « marquer » des valeurs DSCP autres que celles spécifiées dans les stratégies de QoS. En spécifiant que les applications sont autorisées à définir des valeurs DSCP, les applications peuvent définir des valeurs DSCP non nulles.

En spécifiant **Ignorer**, les applications qui utilisent des API de QoS ont leurs valeurs DSCP définies sur zéro, et seules les stratégies de QoS peuvent définir des valeurs DSCP.

Par défaut, les ordinateurs exécutant Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8 , Windows Server 2008 R2, Windows Server 2008 et Windows Vista permettent aux applications de spécifier des valeurs DSCP ; les applications et les appareils qui n'utilisent pas les API de QoS ne sont pas remplacés.

Valeurs multimédia sans fil et DSCP

Wi-Fi Alliance a établi une certification pour le multimédia sans fil (WMM) qui définit quatre catégories d'accès (WMM_AC) pour hiérarchiser le trafic réseau transmis sur un réseau sans fil Wi-Fi. Les catégories d'accès incluent (par ordre de priorité la plus élevée à la priorité la plus basse) : voix, vidéo, meilleur effort et arrière-plan ; respectivement abrégé vo, VI, BE et BK. La spécification WMM définit les valeurs DSCP qui correspondent à chacune des quatre catégories d'accès :

Agrandir le tableau

Valeur DSCP	Catégorie d'accès WMM
48-63	Voix (VO)
32-47	Vidéo (VI)
24-31, 0-7	Meilleur effort (BE)
8-23	Arrière-plan (BK)

Vous pouvez créer des stratégies de QoS qui utilisent ces valeurs DSCP pour vous assurer que les ordinateurs portables dotés d'adaptateurs sans fil Wi-Fi certifiés™ pour WMM reçoivent une gestion prioritaire lorsqu'ils sont associés à Wi-Fi Certified pour les points d'accès WMM.

Règles de précédence de la stratégie de QoS

Comme les priorités des GPO, les stratégies de QoS ont des règles de priorité pour résoudre les conflits lorsque plusieurs stratégies de QoS s'appliquent à un ensemble spécifique de trafic. Pour le trafic TCP ou UDP sortant, une seule stratégie de QoS peut être appliquée à la fois, ce qui signifie que les stratégies de QoS n'ont pas d'effet cumulatif, comme l'emplacement où les taux de limitation seraient additionnés.

En général, la stratégie de QoS avec les conditions les plus correspondantes est gagnante. Lorsque plusieurs stratégies de QoS s'appliquent, les règles se répartissent en trois catégories : au niveau de l'utilisateur et au niveau de l'ordinateur ; application par rapport au quintuple réseau ; et parmi le quintuple réseau.

Par *quintuple réseau*, nous entendons l'adresse IP source, l'adresse IP de destination, le port source, le port de destination et le protocole (TCP/UDP).

La stratégie QoS au niveau de l'utilisateur est prioritaire sur la stratégie QoS au niveau de l'ordinateur

Cette règle facilite considérablement la gestion par les administrateurs réseau des objets de stratégie de groupe QoS, en particulier pour les stratégies basées sur des groupes d'utilisateurs. Par exemple, si l'administrateur réseau souhaite définir une stratégie de QoS pour un groupe d'utilisateurs, il peut simplement créer et distribuer un GPO à ce groupe. Ils n'ont pas à se soucier des ordinateurs sur lesquels ces utilisateurs sont connectés et si ces ordinateurs auront des stratégies de qualité de service en conflit définies, car, en cas de conflit, la stratégie au niveau de l'utilisateur est toujours prioritaire.

> ⓘ **Notes**
>
> Une stratégie de QoS au niveau de l'utilisateur s'applique uniquement au trafic généré par cet utilisateur. Les autres utilisateurs d'un ordinateur spécifique, et l'ordinateur lui-même, ne seront soumis à aucune stratégie de QoS définie pour cet utilisateur.

Spécificité de l'application et priorité sur le quintuple réseau

Lorsque plusieurs stratégies de QoS correspondent au trafic spécifique, la stratégie plus spécifique est appliquée. Parmi les stratégies qui identifient les applications, une stratégie qui inclut le chemin du fichier de l'application d'envoi est considérée comme plus spécifique

qu’une autre stratégie qui identifie uniquement le nom de l’application (aucun chemin). Si plusieurs stratégies avec des applications s’appliquent toujours, les règles de priorité utilisent le quintuple réseau pour trouver la meilleure correspondance.

Vous pouvez également appliquer plusieurs stratégies de QoS au même trafic en spécifiant des conditions qui ne se chevauchent pas. Entre les conditions des applications et le quintuple réseau, la stratégie qui spécifie l’application est considérée comme plus spécifique et elle est appliquée.

Par exemple, policy_A spécifie uniquement un nom d’application (app.exe), et policy_B spécifie l’adresse IP de destination 192.168.1.0/24. Lorsque ces stratégies de QoS sont en conflit (app.exe envoie le trafic à une adresse IP dans la plage 192.168.4.0/24), policy_A est appliquée.

Plus de spécificité est prioritaire dans le quintuple réseau

Pour les conflits de stratégie au sein du quintuple réseau, la stratégie avec les conditions les plus correspondantes est prioritaire. Par exemple, supposons que policy_C spécifie l’adresse IP source « any », l’adresse IP de destination 10.0.0.1, le port source « any », le port de destination « any » et le protocole « TCP ».

Ensuite, supposons que policy_D spécifie l’adresse IP source « any », l’adresse IP de destination 10.0.0.1, le port source « any », le port de destination 80 et le protocole « TCP ». Ensuite, policy_C et policy_D les deux correspondances avec les connexions à destination 10.0.0.1:80. Étant donné que la stratégie de QoS applique la stratégie avec les conditions de correspondance les plus spécifiques, policy_D est prioritaire dans cet exemple.

Toutefois, les stratégies de QoS peuvent avoir un nombre égal de conditions. Par exemple, plusieurs stratégies peuvent chacune spécifier une seule partie (mais pas la même) du quintuple réseau. Parmi le quintuple réseau, l’ordre suivant est de priorité supérieure à inférieure :

- Adresse IP source
- Adresse IP de destination
- Port source
- Port de destination
- Protocole (TCP ou UDP)

Dans une condition spécifique, telle que l’adresse IP, une adresse IP plus spécifique est traitée avec une priorité plus élevée ; par exemple, une adresse IP 192.168.4.1 est plus spécifique que 192.168.4.0/24.

Concevez vos stratégies de QoS aussi spécifiquement que possible pour simplifier la capacité de votre organisation à comprendre quelles stratégies sont en vigueur.

Pour la rubrique suivante de ce guide, consultez Événements et erreurs de la stratégie de QoS.

Pour la première rubrique de ce guide, consultez Stratégie de qualité de service (QoS).

Messages d'erreur et d'événement de la stratégie QoS

31/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Voici les messages d'erreur et d'événement associés à la stratégie QoS.

Informational Messages

Voici une liste des messages d'information de la stratégie QoS.

Agrandir le tableau

Attribute	Value
MessageId	16500
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_MACHINE_POLICY_REFRESH_NO_CHANGE
Language	English
Message	Les stratégies QoS de l'ordinateur ont été actualisées avec succès. Aucune modification n' a été détectée.

Agrandir le tableau

Attribute	Value
MessageId	16501
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_MACHINE_POLICY_REFRESH_WITH_CHANGE
Language	English
Message	Les stratégies QoS de l'ordinateur ont été actualisées avec succès. Des modifications de stratégie ont été détectées.

Agrandir le tableau

Attribute	Value
MessageId	16502
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_USER_POLICY_REFRESH_NO_CHANGE
Language	English
Message	Les stratégies QoS de l'utilisateur ont été actualisées avec succès. Aucune modification n' a été détectée.

Agrandir le tableau

Attribute	Value
MessageId	16503
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_USER_POLICY_REFRESH_WITH_CHANGE
Language	English
Message	Les stratégies QoS de l'utilisateur ont été actualisées avec succès. Des modifications de stratégie ont été détectées.

Agrandir le tableau

Attribute	Value
MessageId	16504
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_TCP_AUTOTUNING_NOT_CONFIGURED
Language	English
Message	Le paramètre QoS avancé pour le niveau de débit TCP entrant a été actualisé avec succès. La valeur de paramètre n'est spécifiée par aucune stratégie QoS. La valeur par défaut de l'ordinateur local sera appliquée.

Agrandir le tableau

Attribute	Value
MessageId	16505

Attribute	Value
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_TCP_AUTOTUNING_OFF
Language	English
Message	Le paramètre QoS avancé pour le niveau de débit TCP entrant a été actualisé avec succès. La valeur de paramètre est Niveau 0 (débit minimal).

Agrandir le tableau

Attribute	Value
MessageId	16506
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_TCP_AUTOTUNING_HIGHLY_RESTRICTED
Language	English
Message	Le paramètre QoS avancé pour le niveau de débit TCP entrant a été actualisé avec succès. La valeur de paramètre est niveau 1.

Agrandir le tableau

Attribute	Value
MessageId	16507
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_TCP_AUTOTUNING_RESTRICTED
Language	English
Message	Le paramètre QoS avancé pour le niveau de débit TCP entrant a été actualisé avec succès. La valeur de paramètre est niveau 2.

Agrandir le tableau

Attribute	Value
MessageId	16508
Severity	Informational

Attribute	Value
SymbolicName	EVENT_EQOS_INFO_TCP_AUTOTUNING_NORMAL
Language	English
Message	Le paramètre QoS avancé pour le niveau de débit TCP entrant a été actualisé avec succès. La valeur de paramètre est Niveau 3 (débit maximal).

Agrandir le tableau

Attribute	Value
MessageId	16509
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_APP_MARKING_NOT_CONFIGURED
Language	English
Message	Le paramètre QoS avancé pour les remplacements de marquage DSCP a été actualisée avec succès. La valeur de paramètre n'est pas spécifiée. Les applications peuvent définir des valeurs DSCP indépendamment des stratégies QoS.

Agrandir le tableau

Attribute	Value
MessageId	16510
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_APP_MARKING_IGNORED
Language	English
Message	Le paramètre QoS avancé pour les remplacements de marquage DSCP a été actualisée avec succès. Les demandes de marquage DSCP de l'application seront ignorées. Seules les stratégies QoS peuvent définir des valeurs DSCP.

Agrandir le tableau

Attribute	Value
MessageId	16511
Severity	Informational

Attribute	Value
SymbolicName	EVENT_EQOS_INFO_APP_MARKING_ALLOWED
Language	English
Message	Le paramètre QoS avancé pour les remplacements de marquage DSCP a été actualisée avec succès. Les applications peuvent définir des valeurs DSCP indépendamment des stratégies QoS.

Agrandir le tableau

Attribute	Value
MessageId	16512
Severity	Informational
SymbolicName	EVENT_EQOS_INFO_LOCAL_SETTING_DONT_USE_NLA
Language	English
Message	L'application sélective des stratégies QoS en fonction de la catégorie de réseau de domaine a été désactivée. Les stratégies QoS seront appliquées à toutes les interfaces réseau.

Warning Messages

Voici une liste des messages d'avertissement de la stratégie QoS.

Agrandir le tableau

Attribute	Value
MessageId	16600
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_TEST_1
Language	English
Message	EQOS: ***Testing***[, avec une chaîne] "%2".

Agrandir le tableau

Attribute	Value
MessageId	16601
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_TEST_2
Language	English
Message	EQOS: ***Testing***[, avec deux chaînes, chaîne1 est] "%2"[, chaîne2 est] "%3".

Agrandir le tableau

Attribute	Value
MessageId	16602
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_MACHINE_POLICY_VERSION
Language	English
Message	La stratégie QoS de l'ordinateur « %2 » a un numéro de version non valide. Cette stratégie ne sera pas appliquée.

Agrandir le tableau

Attribute	Value
MessageId	16603
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_USER_POLICY_VERSION
Language	English
Message	La stratégie QoS de l'utilisateur « %2 » a un numéro de version non valide. Cette stratégie ne sera pas appliquée.

Agrandir le tableau

Attribute	Value
MessageId	16604
Severity	Warning

Attribute	Value
SymbolicName	EVENT_EQOS_WARNING_MACHINE_POLICY_PROFILE_NOT_SPECIFIED
Language	English
Message	La stratégie QoS de l'ordinateur « %2 » ne spécifie pas de valeur DSCP ou de taux de limitation. Cette stratégie ne sera pas appliquée.

Agrandir le tableau

Attribute	Value
MessageId	16605
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_USER_POLICY_PROFILE_NOT_SPECIFIED
Language	English
Message	La stratégie QoS de l'utilisateur « %2 » ne spécifie pas de valeur DSCP ou de taux de limitation. Cette stratégie ne sera pas appliquée.

Agrandir le tableau

Attribute	Value
MessageId	16606
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_MACHINE_POLICY_QUOTA_EXCEEDED
Language	English
Message	Dépassement du nombre maximal de stratégies QoS de l'ordinateur. La stratégie QoS « %2 » et les stratégies QoS de l'ordinateur suivantes ne seront pas appliquées.

Agrandir le tableau

Attribute	Value
MessageId	16607
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_USER_POLICY_QUOTA_EXCEEDED

Attribute	Value
Language	English
Message	Dépassement du nombre maximal de stratégies QoS de l'utilisateur. La stratégie QoS « %2 » et les stratégies QoS de l'utilisateur suivantes ne seront pas appliquées.

Agrandir le tableau

Attribute	Value
MessageId	16608
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_MACHINE_POLICY_CONFLICT
Language	English
Message	La stratégie QoS de l'ordinateur « %2 » est potentiellement en conflit avec d'autres stratégies QoS. Consultez la documentation pour connaître les règles relatives à la stratégie à appliquer.

Agrandir le tableau

Attribute	Value
MessageId	16609
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_USER_POLICY_CONFLICT
Language	English
Message	La stratégie QoS de l'utilisateur « %2 » est potentiellement en conflit avec d'autres stratégies QoS. Consultez la documentation pour connaître les règles relatives à la stratégie à appliquer.

Agrandir le tableau

Attribute	Value
MessageId	16610
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_MACHINE_POLICY_NO_FULLPATH_APPNAME

Attribute	Value
Language	English
Message	La stratégie QoS de l'ordinateur « %2 » a été ignorée, car le chemin d'accès de l'application ne peut pas être traité. Le chemin d'accès de l'application peut être non valide, contenir une lettre de lecteur non valide ou contenir un lecteur mappé réseau.

Agrandir le tableau

Attribute	Value
MessageId	16611
Severity	Warning
SymbolicName	EVENT_EQOS_WARNING_USER_POLICY_NO_FULLPATH_APPNAME
Language	English
Message	La stratégie QoS de l'utilisateur « %2 » a été ignorée, car le chemin d'accès de l'application ne peut pas être traité. Le chemin d'accès de l'application peut être non valide, contenir une lettre de lecteur non valide ou contenir un lecteur mappé réseau.

Error Messages

Voici une liste des messages d'avertissement de la stratégie QoS.

Agrandir le tableau

Attribute	Value
MessageId	16700
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_MACHINE_POLICY_REFERESH
Language	English
Message	Échec de l'actualisation des stratégies QoS de l'ordinateur. Code d'erreur : « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16701

Attribute	Value
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_USER_POLICY_REFERESH
Language	English
Message	Échec de l'actualisation des stratégies QoS de l'utilisateur. Code d'erreur : « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16702
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_OPENING_MACHINE_POLICY_ROOT_KEY
Language	English
Message	La QoS n'a pas pu ouvrir la clé racine au niveau de l'ordinateur pour les stratégies QoS. Code d'erreur : « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16703
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_OPENING_USER_POLICY_ROOT_KEY
Language	English
Message	La QoS n'a pas pu ouvrir la clé racine au niveau de l'utilisateur pour les stratégies QoS. Code d'erreur : « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16704
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_MACHINE_POLICY_KEYNAME_TOO_LONG

Attribute	Value
Language	English
Message	Une stratégie QoS d'ordinateur dépasse la longueur maximale autorisée du nom. La stratégie incriminée est répertoriée sous la clé racine de la stratégie QoS au niveau de l'ordinateur, avec l'index « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16705
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_USER_POLICY_KEYNAME_TOO_LONG
Language	English
Message	Une stratégie QoS d'utilisateur dépasse la longueur maximale autorisée du nom. La stratégie incriminée est répertoriée sous la clé racine de la stratégie QoS au niveau de l'utilisateur, avec l'index « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16706
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_MACHINE_POLICY_KEYNAME_SIZE_ZERO
Language	English
Message	Une stratégie QoS d'ordinateur a un nom de longueur zéro. La stratégie incriminée est répertoriée sous la clé racine de la stratégie QoS au niveau de l'ordinateur, avec l'index « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16707
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_USER_POLICY_KEYNAME_SIZE_ZERO

Attribute	Value
Language	English
Message	Une stratégie QoS d'utilisateur a un nom de longueur zéro. La stratégie incriminée est répertoriée sous la clé racine de la stratégie QoS au niveau de l'utilisateur, avec l'index « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16708
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_OPENING_MACHINE_POLICY_SUBKEY
Language	English
Message	QoS n'a pas pu ouvrir la sous-clé de Registre pour une stratégie QoS d'ordinateur. La stratégie est répertoriée sous la clé racine de la stratégie QoS au niveau de l'ordinateur, avec l'index « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16709
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_OPENING_USER_POLICY_SUBKEY
Language	English
Message	QoS n'a pas pu ouvrir la sous-clé de Registre pour une stratégie QoS d'utilisateur. La stratégie est répertoriée sous la clé racine de la stratégie QoS au niveau de l'utilisateur, avec l'index « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16710
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_PROCESSING_MACHINE_POLICY_FIELD

Attribute	Value
Language	English
Message	QoS n'a pas pu lire ou valider le champ « %2 » pour la stratégie QoS de l'ordinateur « %3 ».

Agrandir le tableau

Attribute	Value
MessageId	16711
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_PROCESSING_USER_POLICY_FIELD
Language	English
Message	QoS n'a pas pu lire ou valider le champ « %2 » pour la stratégie QoS de l'ordinateur « %3 ».

Agrandir le tableau

Attribute	Value
MessageId	16712
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_SETTING_TCP_AUTOTUNING
Language	English
Message	QoS n'a pas pu lire ou définir le niveau de débit TCP entrant, code d'erreur : « %2 ».

Agrandir le tableau

Attribute	Value
MessageId	16713
Severity	Error
SymbolicName	EVENT_EQOS_ERROR_SETTING_APP_MARKING
Language	English
Message	QoS n'a pas pu lire ou définir le paramètre de remplacement du marquage DSCP, code

Attribute	Value
	d’erreur : « %2 ».

Pour la rubrique suivante de ce guide, consultez le Forum aux questions sur la stratégie QoS.

Pour la première rubrique de ce guide, consultez Stratégie de qualité de service (QoS).

Forum aux questions sur la stratégie QoS

Voici les questions fréquemment posées et les réponses à ces questions pour la stratégie QoS.

Quel système d'exploitation mon contrôleur de domaine doit-il exécuter pour utiliser la stratégie QoS ?

Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 ou Windows Server 2008

Quels systèmes d'exploitation prennent en charge l'application de la stratégie QoS à l'utilisateur ou à l'ordinateur ?

Vous pouvez appliquer des stratégies QoS aux utilisateurs ou aux ordinateurs exécutant Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows Server 2008 et Windows Vista.

Les stratégies QoS s'appliquent-elles à l'expéditeur ou au destinataire du trafic ?

Les stratégies QoS doivent être appliquées sur l'ordinateur d'envoi pour affecter son trafic sortant. Pour affecter le trafic bidirectionnel de deux ordinateurs, les stratégies QoS doivent être appliquées aux deux ordinateurs.

Que se passe-t-il si des stratégies QoS en conflit sont déployées sur le même ordinateur ?

Si plusieurs stratégies s'appliquent, la stratégie QoS plus spécifique est prioritaire. Par exemple, une stratégie qui indique une adresse hôte (192.168.4.12) est appliquée au lieu d'une adresse réseau moins spécifique (192.168.0.0/16). Si une stratégie au niveau de l'ordinateur et au

niveau de l'utilisateur présente la même spécificité, la stratégie QoS au niveau de l'utilisateur est appliquée au lieu de la stratégie QoS au niveau de l'ordinateur.

La stratégie QoS est-elle activée par défaut ?

Non, la stratégie QoS n'est pas activée par défaut. Vous devez créer manuellement des stratégies QoS pour activer QoS. Pour plus d'informations, consultez Gérer la stratégie qoS.

Pour la première rubrique de ce guide, consultez stratégie de qualité de service (QoS).

Configuration réseau requise pour Azure Local

> S'applique à : déploiements hyperconvergés d'Azure Local

Cette rubrique décrit les considérations et exigences relatives à la mise en réseau de l'hôte pour Azure Local. Pour plus d'informations sur les architectures de centre de données et les connexions physiques entre les machines, consultez configuration réseau physique requise.

Pour plus d'informations sur la simplification de la mise en réseau hôte à l'aide de Network ATC, consultez Simplifier la mise en réseau de l'hôte avec Network ATC.

Types de trafic réseau

Le trafic réseau local Azure peut être classifié par son objectif prévu :

- **Trafic de gestion :** Trafic vers ou depuis l'extérieur du système local. Par exemple, le trafic utilisé par l'administrateur pour la gestion du système comme le Bureau à distance, Windows Admin Center, Active Directory, etc.
- **Trafic de calcul :** Trafic provenant ou destiné à une machine virtuelle.
- **Trafic de stockage :** Trafic à l'aide de SMB (Server Message Block), par exemple des espaces de stockage direct ou une migration dynamique basée sur SMB. Ce trafic est de couche 2 et n'est pas routable.

Sélectionner une carte réseau

Les cartes réseau sont qualifiées par les **types de trafic réseau** (voir ci-dessus) avec lesquels elles sont compatibles. Lorsque vous passez en revue le catalogue Windows Server, la certification Windows Server 2022 indique désormais un ou plusieurs des rôles suivants. Avant d'acheter une machine pour Azure Local, vous devez disposer *minimalement d'au moins* un adaptateur qualifié pour la gestion, le calcul et le stockage, car les trois types de trafic sont requis sur Azure Local. Vous pouvez ensuite utiliser Network ATC pour configurer vos adaptateurs pour les types de trafic appropriés.

Pour découvrir plus d'informations sur cette qualification de carte réseau axée sur les rôles, consultez ce billet de blog Windows Server.

> **Important**

L'utilisation d'un adaptateur en dehors de son type de trafic qualifié n'est pas prise en charge.

Agrandir le tableau

Niveau	Rôle de gestion	Rôle de calcul	Rôle de stockage
Distinction basée sur les rôles	Gestion	Standard de calcul	Norme de stockage
Prix maximal	Non applicable	Calcul Premium	Stockage Premium

Remarque

La qualification la plus élevée pour n'importe quel adaptateur de notre écosystème contiendra les qualifications **Management**, **Compute Premium** et **Storage Premium** .

Exigences des pilotes

Les pilotes de boîte de réception ne sont pas pris en charge pour une utilisation avec Azure Local. Pour identifier si votre adaptateur utilise un pilote de boîte de réception, exécutez l'applet de commande suivante. Un adaptateur utilise un pilote de boîte de réception si la propriété **DriverProvider** est **Microsoft.**

Powershell

```
Get-NetAdapter -Name <AdapterName> | Select *Driver*
```

Si le pilote de boîte de réception est utilisé, téléchargez et installez le dernier pilote à partir du site web de votre partenaire OEM.

Vue d'ensemble des principales fonctionnalités des adaptateurs réseau

Les principales fonctionnalités de l'adaptateur réseau utilisées par Azure Local sont les suivantes :

- File d'attente multiple de machines virtuelles dynamique (Dynamic VMMQ, ou d.VMMQ)

- Accès direct à la mémoire à distance (RDMA, Remote Direct Memory Access)
- RDMA invité
- SET (Switch Embedded Teaming)

VMMQ dynamique

Toutes les cartes réseau dotées de la qualification Compute (Premium) prennent en charge Dynamic VMMQ. Dynamic VMMQ nécessite l'utilisation de la fonctionnalité Switch Embedded Teaming.

Types de trafic applicables : calcul

Certifications requises : Informatique (Premium)

Dynamic VMMQ est une technologie intelligente côté réception. Il s'appuie sur ses prédécesseurs, File d'attente d'ordinateurs virtuels (VMQ), Mise à l'échelle côté réception virtuelle (vRSS) et VMMQ, pour offrir trois améliorations principales :

- optimisation de l'efficacité des hôtes en utilisant moins de cœurs de processeur ;
- réglage automatique du traitement du trafic réseau sur les cœurs de processeur, permettant ainsi aux machines virtuelles de respecter et de maintenir le débit attendu ;
- Permet aux charges de travail « en rafale » de recevoir la quantité de trafic attendue.

Pour plus d'informations sur Dynamic VMMQ, consultez le billet de blog Accélérations synthétiques .

RDMA

RDMA est un déchargement de la pile réseau vers la carte réseau. Cela permet au trafic de stockage SMB de contourner le système d'exploitation pour traitement.

La fonctionnalité RDMA permet une mise en réseau à débit élevé et faible latence avec une utilisation minimale des ressources de processeur hôte. Ces ressources peuvent alors servir à exécuter des machines virtuelles ou des conteneurs supplémentaires.

Types de trafic applicables : stockage hôte

Certifications requises : Stockage (standard)

Tous les adaptateurs avec la qualification Storage (Standard) ou Storage (Premium) prennent en charge le RDMA côté hôte. Pour plus d'informations sur l'utilisation de RDMA avec des charges de travail invitées, consultez la section « RdMA invité » plus loin dans cet article.

Azure Local prend en charge RDMA avec les implémentations des protocoles Internet Wide Area RDMA Protocol (iWARP) ou RDMA over Converged Ethernet (RoCE).

> **Important**
>
> Les adaptateurs RDMA fonctionnent uniquement avec d'autres adaptateurs RDMA qui implémentent le même protocole RDMA (iWARP ou RoCE).

Toutes les cartes réseau des fournisseurs ne prennent pas en charge la fonctionnalité RDMA. Le tableau suivant répertorie les fournisseurs (par ordre alphabétique) qui offrent des adaptateurs RDMA certifiés. Toutefois, il existe des fabricants de matériel qui ne figurent pas dans cette liste et prennent également en charge la fonctionnalité RDMA. Consultez le catalogue Windows Server pour rechercher des adaptateurs avec la qualification Stockage (Standard) ou Stockage (Premium) qui nécessitent le support RDMA.

> **Remarque**
>
> InfiniBand (IB) n'est pas pris en charge avec Azure Local.

Agrandir le tableau

Fournisseur de cartes réseau	iWARP	RoCE
Broadcom	Non	Oui
Intel	Oui	Oui (certains modèles)
Marvell (Qlogic)	Oui	Oui
Nvidia	Non	Oui

Pour plus d'informations sur le déploiement de RDMA pour l'hôte, nous vous recommandons vivement d'utiliser Network ATC. Pour plus d'informations sur le déploiement manuel, consultez le référentiel GitHub SDN.

iWARP

iWARP utilise le protocole TCP (Transmission Control Protocol) et peut éventuellement être amélioré avec les standards PFC (Priority-based Flow Control) et ETS (Enhanced Transmission Service).

Utilisez iWARP si :

- Vous n'avez pas d'expérience de gestion des réseaux RDMA.
- Vous ne gérez pas vos commutateurs ToR (top-of-rack) ou n'êtes pas à l'aise avec leur gestion.
- Vous n'êtes pas la personne qui gère la solution après le déploiement.

- Vous avez déjà effectué des déploiements utilisant iWARP.
- Vous ne savez pas quelle option choisir.

RoCE

RoCE utilise le protocole UDP (User Datagram Protocol) et demande à PFC et ETS d'assurer sa fiabilité.

Utilisez RoCE si :

- Votre centre de données comporte déjà des déploiements avec RoCE.
- Vous êtes à l'aise avec la gestion des exigences du réseau DCB.

RDMA invité

Guest RDMA n'est pas pris en charge sur Azure Local.

SET (Switch Embedded Teaming)

SET (Switch Embedded Teaming) est une technologie d'association basée sur des logiciels qui a été intégrée dans le système d'exploitation Windows Server depuis la version Windows Server 2016. SET est la seule technologie d'association prise en charge par Azure Local et fonctionne bien avec le trafic de calcul, de stockage et de gestion. SET prend en charge jusqu'à huit adaptateurs dans une seule équipe. Les autres méthodes d'agrégation de cartes réseau, comme l'équilibrage de charge/basculement (LBFO), ne sont pas prises en charge.

Dans l'Azure Local, Network ATC configure automatiquement à la fois le SET et le vswitch. Vous ne devez pas déployer manuellement SET à l'aide de PowerShell, par exemple avec l'applet de commande New-VMSwitch . Bien que cette commande active l'association incorporée par défaut lorsque plusieurs adaptateurs sont répertoriés, l'approche recommandée consiste à utiliser Network ATC avec des intentions.

Types de trafic applicables : calcul, stockage et gestion

Certifications requises : Calcul (Standard) ou Calcul (Premium)

SET est important pour Azure Local, car il s'agit de la seule technologie d'association qui permet :

- Association d'adaptateurs RDMA (si nécessaire).
- RDMA invité.
- VMMQ dynamique.
- Autres fonctionnalités clés d'Azure Local (consultez Teaming dans Azure Local).

SET nécessite l'utilisation d'adaptateurs symétriques (identiques). Les cartes réseau symétriques sont celles qui présentent les mêmes caractéristiques :

- Marque (fournisseur)
- Modèle (version)
- Vitesse (débit)
- d'origine

Network ATC détecte et vous informe automatiquement si les adaptateurs que vous choisissez sont asymétriques. Le moyen le plus simple d'identifier manuellement si les adaptateurs sont symétriques est que les vitesses et les descriptions d'interface correspondent **exactement** . Ils ne peuvent différer que par le chiffre indiqué dans la description. Utilisez la cmdlet Get-NetAdapterAdvancedProperty pour vérifier que la configuration signalée présente les mêmes valeurs de propriété.

Dans le tableau suivant figure un exemple de descriptions d'interface qui ne diffèrent que par le chiffre :

Agrandir le tableau

Nom	Description de l'interface	Vitesse de liaison
NIC1	Carte réseau 1	25 Gbits/s
NIC2	Carte réseau 2	25 Gbits/s
NIC3	Carte réseau 3	25 Gbits/s
NIC4	Carte réseau 4	25 Gbits/s

> **Remarque**
>
> SET prend uniquement en charge la configuration indépendante du commutateur à l'aide des algorithmes d'équilibrage de charge Port Hyper-V ou Dynamic. Pour bénéficier de performances optimales, nous vous recommandons d'utiliser Port Hyper-V sur toutes les cartes réseau qui opèrent à 10 Gbits/s ou plus. Network ATC effectue toutes les configurations requises pour SET.

Considérations relatives au trafic RDMA

Si vous implémentez DCB, vous devez vous assurer que la configuration PFC et ETS est correctement implémentée sur chacun des ports réseau, notamment les commutateurs réseau. Les standards DCB sont obligatoires pour le protocole RoCE et facultatifs pour le protocole iWARP.

Pour plus d'informations sur le déploiement de RDMA, téléchargez le document à partir du dépôt GitHub SDN .

Les implémentations locales Azure basées sur RoCE nécessitent la configuration de trois classes de trafic PFC, y compris la classe de trafic par défaut, dans l'infrastructure et tous les hôtes.

Classe de trafic système

Cette classe de trafic garantit que la bande passante réservée aux pulsations système est suffisante :

- Obligatoire : Oui
- Compatible avec PFC : non
- Priorité de trafic recommandée : priorité 7
- Réservation de bande passante recommandée :
  - Réseaux RDMA de 10 GbE ou moins = 2 pour cent
  - Réseaux RDMA de 25 GbE ou moins = 1 pour cent

Classe de trafic RDMA

Cette classe de trafic garantit une bande passante réservée suffisante pour les communications RDMA sans perte en utilisant SMB Direct :

- Obligatoire : Oui
- PFC activé : oui
- Priorité de trafic recommandée : priorité 3 ou 4
- Réservation de bande passante recommandée : 50 pour cent

Classe de trafic par défaut

Cette classe de trafic transporte tout autre trafic non défini dans les classes de trafic système ou RDMA, notamment le trafic de machine virtuelle et le trafic de gestion :

- Obligatoire : par défaut (aucune configuration nécessaire sur l'hôte)
- Contrôle de flux (PFC) activé : non
- Classe de trafic recommandée : par défaut (Priorité 0)
- Réservation de bande passante recommandée : par défaut (aucune configuration hôte requise)

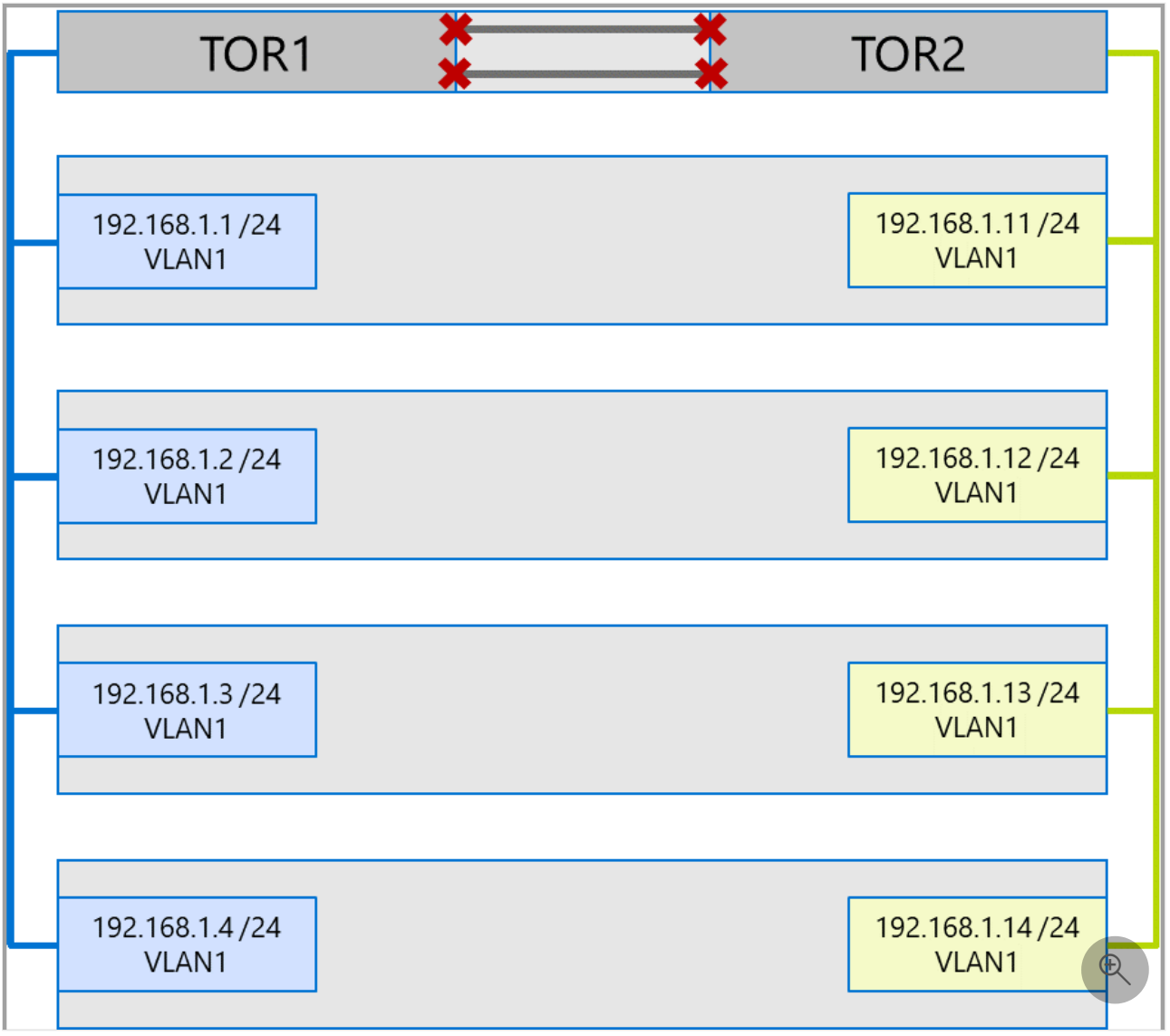
Modèles de trafic de stockage

SMB offre de nombreux avantages en tant que protocole de stockage pour Azure Local, notamment SMB Multichannel. SMB Multichannel n'est pas discuté dans cette rubrique. Cependant, il est important de comprendre que le trafic est multiplexé sur chacune des liaisons possibles utilisées par SMB Multichannel.

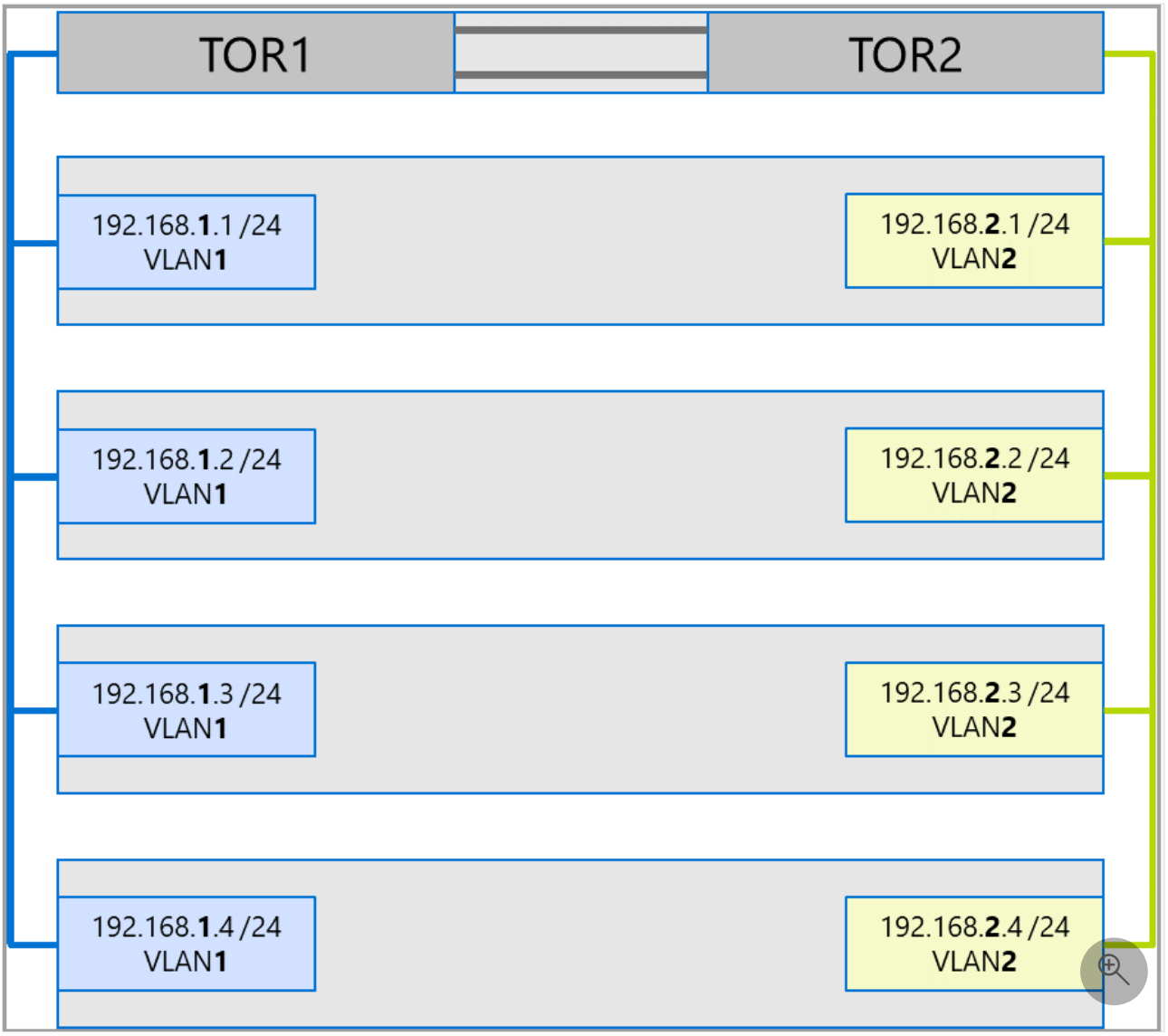
> **Remarque**
>
> Nous vous recommandons d'utiliser plusieurs sous-réseaux et réseaux locaux virtuels pour séparer le trafic de stockage dans Azure Local.

Prenons l'exemple suivant d'un système à quatre nœuds. Chaque machine a deux ports de stockage (gauche et droite). Étant donné que chaque adaptateur se trouve sur le même sous-réseau et le même réseau VLAN, SMB Multichannel répartit les connexions entre toutes les liaisons disponibles. Par conséquent, le port gauche sur la première machine (192.168.1.1)) établira une connexion au port de gauche sur la deuxième machine (192.168.1.2). Le port de droite sur la première machine (192.168.1.12) se connecte au port de droite sur la deuxième machine. Des connexions similaires sont établies pour les troisième et quatrième machines.

Cela crée toutefois des connexions inutiles et provoque une congestion au niveau de l'interlien (groupe d'agrégation de liens à plusieurs châssis ou MC-LAG) qui connecte les commutateurs ToR (marqués par des X). Consultez le diagramme suivant :



L'approche recommandée consiste à utiliser des sous-réseaux et des réseaux VLAN distincts pour chaque ensemble d'adaptateurs. Dans le diagramme suivant, les ports de droite utilisent désormais le sous-réseau 192.168.2.x /24 et VLAN2. Cela permet au trafic des ports de gauche de rester sur TOR1 et à celui des ports de droite de rester sur TOR2.



Allocation de bande passante au trafic

Le tableau suivant montre des exemples d'allocations de bande passante de différents types de trafic, à l'aide de vitesses d'adaptateur courantes, dans Azure Local. Notez qu'il s'agit d'un exemple de *solution convergée*, où tous les types de trafic (calcul, stockage et gestion) s'exécutent sur les mêmes adaptateurs physiques et sont en équipe à l'aide de SET.

Puisque ce cas d'usage est celui qui impose le plus de contraintes, il constitue une bonne ligne de base. Toutefois, en prenant en compte les permutations du nombre d'adaptateurs et des vitesses, il doit être considéré comme un exemple et non comme une configuration requise pour la prise en charge.

Cet exemple repose sur les hypothèses suivantes :

- Il existe deux adaptateurs par équipe.
- Le trafic SBL (Storage Bus Layer), le trafic de Volume partagé de cluster (CSV) et le trafic Hyper-V (Migration dynamique) :
  - utilisent les mêmes adaptateurs physiques ;
  - utilisent le protocole SMB.
- SMB reçoit une allocation de bande passante de 50 % en utilisant DCB.
  - SBL/CSV est le trafic avec la priorité la plus élevée et reçoit 70 % d'une réservation de bande passante SMB.
  - La Migration dynamique (LM) est limitée en utilisant la cmdlet `Set-SMBBandwidthLimit` et reçoit 29 % de la bande passante restante.
    - Si la bande passante disponible pour la Migration dynamique est >= 5 Gbits/s et que les cartes réseau sont compatibles, optez pour la fonctionnalité RDMA. Utilisez pour cela la cmdlet suivante :

      Powershell
      ```
      Set-VMHost -VirtualMachineMigrationPerformanceOption SMB
      ```

    - Si la bande passante disponible pour la Migration dynamique est < 5 Gbits/s, appliquez une compression pour réduire les durées d'indisponibilité. Utilisez pour cela la cmdlet suivante :

      Powershell
      ```
      Set-VMHost -VirtualMachineMigrationPerformanceOption Compression
      ```

- Si vous utilisez la fonctionnalité RDMA avec la trafic de Migration dynamique, assurez-vous que le trafic de Migration dynamique ne peut pas utiliser toute la bande passante allouée à la classe de trafic RDMA grâce à une limite de bande passante SMB. Soyez prudent, car cette cmdlet prend une entrée en octets par seconde (octets/s), tandis que les cartes réseau sont répertoriées en bits par seconde (bits/s). Utilisez la cmdlet suivante pour définir une limite de bande passante de 6 Gbit/s, par exemple :

  Powershell
  ```
  Set-SMBBandwidthLimit -Category LiveMigration -BytesPerSecond 750MB
  ```

  > ⓘ **Remarque**
  >
  > 750 Mbits/s dans cet exemple équivaut à 6 Gbit/s.

Voici le tableau d'allocation des exemples de bande passante :

Agrandir le tableau

Vitesse de la carte réseau	Bande passante agrégée	Réservation de bande passante SMB**	% SBL/CSV	Bande passante SBL/CSV	Migration en direct %	Bande passante maximale de migration en direct	% pulsations	Bande passante de fréquenc cardiaqu
10 Gbits/s	20 Gbits/s	10 Gbits/s	70 %	7 Gbits/s	*	200 Mbits/s		
25 Gbits/s	50 Gbit/s	25 Gbits/s	70 %	17,5 Gbit/s	29 %	7,25 Gbit/s	1 %	250 Mbit,
40 Gbits/s	80 Gbit/s	40 Gbits/s	70 %	28 Gbit/s	29 %	11,6 Gbit/s	1 %	400 Mbit,
50 Gbit/s	100 Gbits/s	50 Gbit/s	70 %	35 Gbit/s	29 %	14,5 Gbit/s	1 %	500 Mbit
100 Gbits/s	200 Gbits/s	100 Gbits/s	70 %	70 Gbit/s	29 %	29 Gbit/s	1 %	1 Gbit/s
200 Gbits/s	400 Gbit/s	200 Gbits/s	70 %	140 Gbit/s	29 %	58 Gbit/s	1 %	2 Gbit/s

Utilisez la compression plutôt que la fonctionnalité RDMA, car l'allocation de bande passante pour le trafic de Migration dynamique est < 5 Gbits/s.

** 50 % est un exemple de réservation de bande passante.

Clustering conscient de la disposition des racks

Le clustering prenant en charge le rack améliore la tolérance de panne et la distribution des données dans une instance locale Azure. Cette architecture vous permet de mettre en cluster des nœuds qui sont stratégiquement placés sur deux racks physiques dans des salles ou des bâtiments distincts, connectés par une bande passante élevée et un réseau à faible latence. Pour obtenir une vue d'ensemble de cette fonctionnalité, consultez la vue d'ensemble du clustering prenant en charge le rack Azure Local.

Pour connaître la configuration réseau requise et l'architecture, consultez l'architecture de référence du cluster prenant en charge le rack Azure.

Étapes suivantes

- Pour plus d'informations sur les exigences liées aux commutateurs réseau et aux réseaux physiques, Consultez la configuration réseau physique requise.

- Apprenez à simplifier la mise en réseau des hôtes à l'aide de Network ATC. Consultez Simplifier la mise en réseau de l'hôte avec Network ATC.
- Rafraîchissez vos connaissances sur les Informations de base sur les réseaux de clustering de basculement.
- Consultez Déployer à l'aide du portail Azure.
- Consultez Déployer à l'aide du modèle Azure Resource Manager.

Dernière mise à jour : 15/09/2026

Réseau privé virtuel (VPN)

15/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10

Passerelle RAS en tant que serveur VPN à abonné unique

Dans Windows Server 2016, le rôle serveur Accès à distance est un regroupement logique des technologies d'accès réseau associées suivantes.

- Service d'accès à distance
- Routing
- Proxy d'application web

Ces technologies sont les services de rôle du rôle serveur Accès à distance.

Lorsque vous installez le rôle serveur Accès à distance avec l'Assistant Ajouter des rôles et des fonctionnalités ou Windows PowerShell, vous pouvez choisir d'installer un ou plusieurs des trois services de rôle suivants :

Lorsque vous installez le service de rôle **DirectAccess et VPN (RAS),** vous déployez la passerelle de service d'accès à distance (**Passerelle RAS**). Vous pouvez déployer la passerelle RAS en tant que serveur de réseau privé virtuel (VPN) de passerelle RAS à abonné unique qui fournit de nombreuses fonctionnalités avancées et des fonctionnalités améliorées.

> ⓘ **Notes**
>
> Vous pouvez également déployer la passerelle RAS en tant que serveur VPN multi-abonné à utiliser avec SDN (Software Defined Networking) ou en tant que serveur DirectAccess. Pour plus d'informations, consultez passerelle RAS, Mise en réseau définie par logiciel (SDN) et DirectAccess.

Rubriques connexes

- Fonctions et fonctionnalités Always On VPN : dans cette rubrique, vous allez découvrir les fonctions et fonctionnalités de Always On VPN.
- Configurer des tunnels de périphérique VPN dans Windows 10 : Always On VPN vous permet de créer un profil VPN dédié pour l'appareil ou la machine. Les connexions VPN

Always On incluent deux types de tunnels : *tunnel d'appareil* et *tunnel utilisateur*. Le tunnel d'appareil est utilisé pour les scénarios de connectivité préalables à l'ouverture de session et à des fins de gestion des appareils. Le tunnel d'utilisateur permet aux utilisateurs d'accéder aux ressources de l'organisation via les serveurs VPN.

- Déploiement Always On VPN pour Windows Server 2016 et Windows 10 : fournit des instructions sur le déploiement de l'accès à distance en tant que passerelle RAS VPN à abonné unique pour les connexions VPN point à site qui permettent à vos employés distants de se connecter au réseau de votre organisation à l'aide de connexions Always On VPN. Il est recommandé de consulter les guides de conception et de déploiement pour chacune des technologies utilisées dans ce déploiement.

- Guide technique du VPN Windows 10 : il vous aide à prendre des décisions concernant les clients Windows 10 dans votre solution VPN d'entreprise et à configurer votre déploiement. Vous pouvez trouver des références quant au fournisseur de services de configuration (CSP) VPNv2. Il fournit des instructions de configuration relatives à la gestion des périphériques mobiles (GPM) à l'aide de Microsoft Intune et du modèle de profil VPN pour Windows 10.

- Comment créer des profils VPN dans le Gestionnaire de configurations : cette rubrique explique comment créer des profils VPN dans le Gestionnaire de configurations.

- Configurer les connexions clientes Windows 10 Always On VPN : cette rubrique décrit les options et le schéma ProfileXML et comment créer le VPN ProfileXML. Après avoir configuré l'infrastructure du serveur, vous devez configurer les ordinateurs clients Windows 10 pour communiquer avec cette infrastructure avec une connexion VPN.

- Options de profil VPN : cette rubrique décrit les paramètres de profil VPN dans Windows 10. Vous découvrez comment configurer des profils VPN à l'aide de Intune ou du Gestionnaire de configurations. Vous pouvez configurer tous les paramètres VPN dans Windows 10 à l'aide du nœud ProfileXML dans le CSP VPNv2.

Service WINS (Windows Internet Name Service)

Article • 02/11/2024 •

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Stack HCI, versions 23H2 and 22H2

Le service WINS (Windows Internet Name Service) représente un service hérité d'inscription et de résolution de noms d'ordinateurs qui mappe les noms NetBIOS d'ordinateurs à des adresses IP.

Si vous n'avez pas encore déployé WINS sur votre réseau, ne déployez pas WINS. À la place, déployez le système DNS (Domain Name System). DNS fournit également des services d'inscription et de résolution de noms d'ordinateur, et offre de nombreux avantages supplémentaires par rapport à WINS, tels que l'intégration à domaine Active Directory Domain Services.

Pour plus d'informations, consultez Domain Name System (DNS)

Si vous avez déjà déployé WINS sur votre réseau, il est recommandé de déployer DNS, puis de désactiver WINS.

Commentaires

Cette page a-t-elle été utile ? Yes No

Service de temps Windows (W32Time)

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Le service de temps Windows (W32Time) synchronise la date et l'heure de tous les ordinateurs s'exécutant dans Active Directory Domain Services (AD DS). La synchronisation de l'heure est essentielle au bon fonctionnement de nombreux services Windows et applications métier. Le service de temps Windows utilise le protocole NTP (Network Time Protocol) pour synchroniser les horloges des ordinateurs sur le réseau. NTP garantit qu'une valeur d'horloge exacte, ou horodatage, peut être affectée aux demandes de validation réseau et d'accès aux ressources.

La rubrique Service de temps Windows (W32Time) met à votre disposition le contenu suivant :

- **Heure exacte Windows Server 2016.** La précision de la synchronisation du temps dans Windows Server 2016 a été considérablement améliorée, tout en conservant une compatibilité NTP complète avec les anciennes versions de Windows. Dans des conditions de fonctionnement raisonnables, vous pouvez maintenir une précision de 1 ms par rapport à l'heure UTC, ou une meilleure précision pour les membres de domaine Mise à jour anniversaire de Windows 10 et Windows Server 2016.
- **Limite de prise en charge pour les environnements haute précision.** Cet article décrit les limites de prise en charge pour le service de temps Windows (W32Time) dans les environnements qui nécessitent une heure système extrêmement précise et stable.
- **Configuration de systèmes de haute précision.** La synchronisation de l'heure dans Windows 10 et Windows Server 2016 a été considérablement améliorée. Dans des conditions de fonctionnement raisonnables, les systèmes peuvent être configurés pour maintenir une précision de 1 ms (milliseconde), ou une meilleure précision (par rapport à l'heure UTC).
- **Temps Windows pour la traçabilité.** Dans de nombreux secteurs, les réglementations exigent que les systèmes soient traçables au format UTC. Cela signifie que le décalage d'un système peut être attesté par rapport au temps universel coordonné (UTC). Pour permettre des scénarios de conformité réglementaire, Windows 10 et Windows Server 2016 fournissent de nouveaux journaux des événements afin de proposer une image du point de vue du système d'exploitation permettant de comprendre les actions effectuées sur l'horloge système. Ces journaux des événements sont générés en continu pour le service de temps Windows et peuvent être examinés ou archivés en vue de les analyser ultérieurement.
- **Informations techniques de référence sur le service de temps Windows.** Le service W32Time assure la synchronisation de l'horloge réseau pour les ordinateurs sans nécessiter de configuration étendue. Le service W32Time est essentiel au bon fonctionnement de l'authentification Kerberos V5 et donc de l'authentification AD DS.

- **Fonctionnement du service de temps Windows.** Bien que le service de temps Windows ne soit pas une implémentation exacte du protocole NTP (Network Time Protocol), il utilise la suite complexe d'algorithmes définie dans les spécifications NTP pour faire en sorte que les horloges des ordinateurs d'un réseau soient aussi précises que possible.
- **Paramètres et outils du service de temps Windows.** La plupart des ordinateurs membres du domaine ont un type de client de temps NT5DS, ce qui signifie qu'ils synchronisent l'heure à partir de la hiérarchie de domaine. La seule exception classique est le contrôleur de domaine qui fonctionne en tant que maître d'opérations de l'émulateur du contrôleur de domaine principal du domaine racine de la forêt, qui est généralement configuré pour synchroniser l'heure avec une source de temps externe.

Rubriques connexes

Pour plus d'informations sur la hiérarchie de domaine et le système de scoring, consultez le billet de blog « What is Windows Time Service? ».

Le modèle de plug-in du fournisseur de temps Windows est documenté sur TechNet.

Un addenda référencé par l'article Sur le temps précis de Windows 2016 peut être téléchargé ici

Pour une présentation rapide du service d'heure de Windows, regardez cette vidéo de présentation globale.

Préversion Insider

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Prise en charge des secondes intercalaires

Une seconde intercalaire est un ajustement occasionnel de 1 seconde du temps UTC. Comme la rotation de la terre ralentit, UTC (une échelle de temps atomique) diffère du temps solaire moyen ou de l'heure astronomique. Une fois UTC a divergé d'au plus 0,9 secondes, une seconde bissextile est insérée pour maintenir la synchronisation de l'UTC avec le temps solaire moyen.

Les secondes intercalaires sont devenues importantes pour répondre aux exigences réglementaires de précision et de traçabilité à la fois aux États-Unis et dans l'Union européenne.

Pour plus d'informations, voir :

- Notre blog d'annonce
- Guide de validation pour les développeurs
- Guide de validation pour le professionnel de l'informatique

Protocole PTP (Precision Time Protocol)

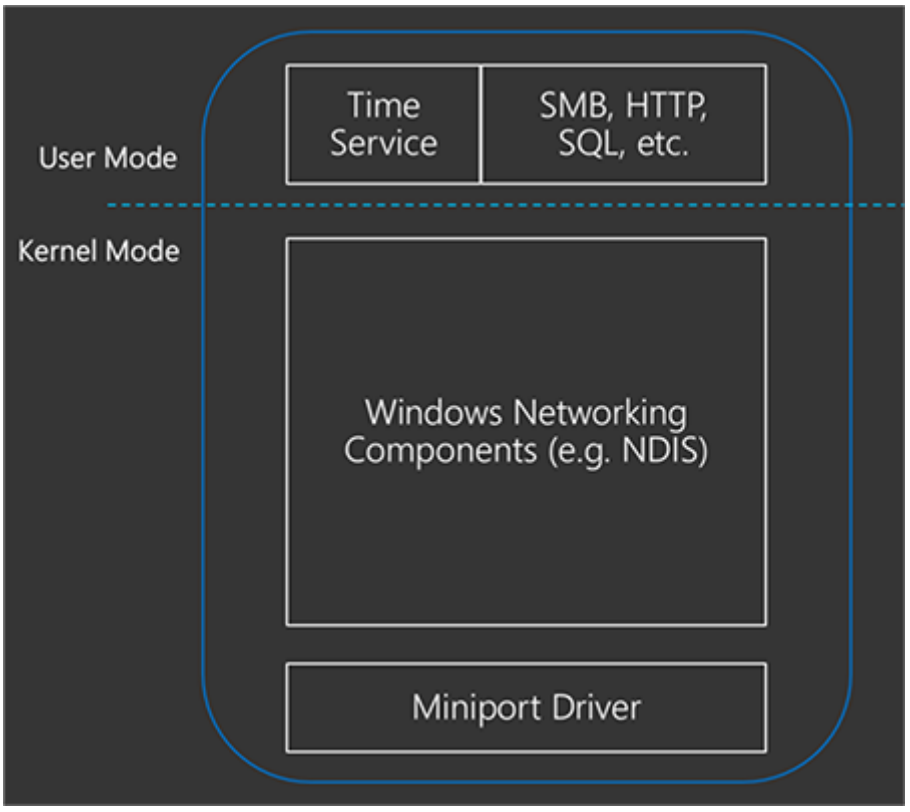
Un nouveau fournisseur de temps inclus dans Windows Server 2019 et Windows 10 (version 1809) vous permet de synchroniser l'heure à l'aide du protocole PTP (Precision Time Protocol). Quand l'heure est distribuée sur un réseau, elle rencontre un délai (latence) qui, s'il n'est pas pris en compte ou n'est pas symétrique, complique la compréhension de l'horodatage envoyé du serveur de temps. Le protocole PTP permet aux appareils réseau d'ajouter la latence introduite par chacun d'eux dans les mesures de synchronisation, fournissant ainsi au client Windows un échantillon de temps beaucoup plus précis.

Pour plus d'informations, voir :

- Notre blog d'annonce
- Guide de validation pour le professionnel de l'informatique

Horodatage logiciel

Quand un paquet de synchronisation est reçu sur le réseau à partir d'un serveur de temps, il doit être traité par la pile réseau du système d'exploitation avant d'être consommé dans le service de temps. Chaque composant de la pile réseau introduit une quantité variable de latence qui affecte la précision de la mesure de synchronisation.



Pour résoudre ce problème, l'horodatage logiciel nous permet d'horodater les paquets avant et après les « composants réseau Windows » indiqués ci-dessus pour tenir compte du délai dans le système d'exploitation.

Pour plus d'informations, voir :

- Notre blog d'annonce
- Guides de validation pour les développeurs et les professionnels de l'informatique

Heure exacte pour Windows Server 2016

29/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Le service de temps Windows est un composant qui utilise un modèle de plug-in pour les fournisseurs de synchronisation de l'heure du client et du serveur. Il existe deux fournisseurs clients intégrés sur Windows et des plug-ins tiers sont disponibles. L'un des fournisseurs utilise NTP (RFC 1305) ou MS-NTP pour synchroniser l'heure système locale sur un serveur de référence compatible avec NTP et/ou MS-NTP. L'autre fournisseur, destiné à Hyper-V, synchronise les machines virtuelles avec l'hôte Hyper-V. Si plusieurs fournisseurs existent, Windows choisit le meilleur fournisseur en fonction, successivement, du niveau de couche, du délai racine, de la dispersion racine et du décalage de temps.

> **Notes**
>
> Pour une présentation rapide du service d'heure de Windows, regardez cette vidéo de présentation globale.

Dans cette rubrique, nous aborderons les sujets ci-après, liés à l'activation du temps précis :

- Improvements
- Measurements
- Best Practices

> **Important**
>
> An addendum referenced by the Windows 2016 Accurate Time article can be downloaded here. Ce document fournit plus de détails sur nos méthodologies de test et de mesure.

> **Notes**
>
> Le modèle de plug-in du fournisseur de temps Windows est documenté sur TechNet.

Domain Hierarchy

Les configurations de domaine et autonomes fonctionnent différemment.

- Les membres de domaine utilisent un protocole NTP sécurisé, qui se sert de l'authentification pour garantir la sécurité et l'authenticité de la référence d'heure. Les membres de domaine se synchronisent avec une horloge maître déterminée par la hiérarchie de domaine et un système d'évaluation. Dans un domaine, il existe une couche hiérarchique de strates temporelles, selon laquelle chaque contrôleur de domaine pointe vers un contrôleur de domaine parent avec une strate temporelle plus précise. La hiérarchie correspond au contrôleur de domaine principal ou à un contrôleur de domaine dans la forêt racine, ou à un contrôleur de domaine avec l'indicateur de domaine GTIMESERV, qui désigne un serveur de temps approprié pour le domaine. Consultez la section Spécifier un service de temps fiable local à l'aide de GTIMESERV ci-dessous.

- Les ordinateurs autonomes sont configurés pour utiliser time.windows.com par défaut. Ce nom est résolu par votre serveur DNS, qui doit pointer vers une ressource appartenant à Microsoft. Comme toutes les références d'heure à distance, les pannes de réseau peuvent empêcher la synchronisation. Les charges de trafic réseau et les chemins réseau asymétriques peuvent réduire la précision de la synchronisation du temps. Pour une précision de 1 ms, vous ne pouvez pas dépendre d'une source de temps distante.

Étant donné que les invités Hyper-V ont le choix entre au moins deux fournisseurs de temps Windows, l'heure de l'hôte et NTP, vous risquez de voir des comportements différents avec la configuration de type domaine ou autonome lors de l'exécution en tant qu'invité.

> ⓘ **Notes**
>
> Pour plus d'informations sur la hiérarchie de domaine et le système de scoring, consultez le billet de blog « What is Windows Time Service? ».

> ⓘ **Notes**
>
> La couche est un concept utilisé à la fois dans les fournisseurs NTP et Hyper-V, et sa valeur indique l'emplacement des horloges dans la hiérarchie. La couche 1 est réservée à l'horloge de niveau supérieur, tandis que la couche 0 est réservée au matériel censé être précis et auquel est associé un délai infime ou nul. La couche 2 communique avec les serveurs de couche 1, la couche 3 avec la couche 2, et ainsi de suite. Bien qu'une couche inférieure indique souvent une horloge plus précise, il est possible de trouver des différences. De plus, W32time accepte uniquement l'heure des couches 15 ou inférieures. Pour voir la couche d'un client, utilisez *w32tm /query /status*.

Facteurs critiques pour une heure précise

Pour une heure précise, il existe systématiquement trois facteurs critiques :

1. **Horloge source solide** : l'horloge source dans votre domaine doit être stable et précise. Cela signifie généralement l'installation d'un appareil GPS ou le pointage vers une source de couche 1, en tenant compte du point 3. Par analogie, si vous avez deux bateaux sur l'eau et que vous essayez de mesurer l'altitude de l'un par rapport à l'autre, la précision est meilleure si le bateau source est très stable et ne bouge pas. Il en va de même pour l'heure, et si votre horloge source n'est pas stable, la chaîne entière des horloges synchronisées est affectée et agrandie à chaque étape. Elle doit également être accessible, car les interruptions de la connexion interfèrent avec la synchronisation de l'heure. Enfin, elle doit être sécurisée. Si la référence d'heure n'est pas correctement gérée ou qu'elle est gérée par un tiers potentiellement malveillant, vous risquez d'exposer votre domaine à des attaques basées sur l'heure.
2. **Horloge cliente stable** : les horloges clientes stables garantissent que la dérive naturelle de l'oscillateur est maîtrisable. NTP utilise plusieurs échantillons à partir d'un voire plusieurs serveurs NTP pour conditionner et discipliner l'horloge de vos ordinateurs locaux. Il n'arrête pas les changements de temps, mais ralentit ou accélère plutôt l'horloge locale, afin que vous puissiez vous approcher rapidement de l'heure précise et conserver cette précision entre les demandes NTP. Toutefois, si l'oscillateur de l'horloge de l'ordinateur client n'est pas stable, des fluctuations entre les ajustements peuvent se produire et les algorithmes que Windows utilise pour conditionner l'horloge ne fonctionnent pas correctement. Dans certains cas, des mises à jour du microprogramme peuvent être nécessaires pour avoir une heure précise.
3. **Communication NTP symétrique** : il est essentiel que la connexion pour la communication NTP soit symétrique. Pour ajuster l'heure, le protocole NTP utilise des calculs qui partent du principe que le chemin réseau est symétrique. Si le temps que met le paquet NTP pour atteindre le serveur diffère du temps du chemin inverse, la précision est affectée. Par exemple, le chemin peut changer en raison de modifications apportées à la topologie du réseau ou du fait que les paquets sont routés par le biais d'appareils qui ont des vitesses d'interface différentes.

Pour les appareils fonctionnant sur batterie, à la fois mobiles et portables, vous devez envisager différentes stratégies. Conformément à notre recommandation, le fait de conserver une heure précise exige que l'horloge soit disciplinée une fois par seconde, soit la fréquence de mise à jour de l'horloge. Ces paramètres consomment plus de batterie que prévu et peuvent interférer avec les modes d'économie d'énergie disponibles dans Windows pour ces appareils. Les appareils alimentés par batterie disposent également de certains modes de gestion de l'alimentation qui empêchent l'exécution de toutes les applications, ce qui interfère avec la capacité de W32time à discipliner l'horloge et à conserver une heure précise. De plus, les horloges des appareils mobiles peuvent ne pas être très précises au départ. Les conditions environnementales affectent la précision de l'horloge et un appareil mobile peut passer d'une

condition à une autre, ce qui peut interférer avec sa capacité à conserver un temps précis. Ainsi, Microsoft ne vous recommande pas de configurer des appareils portables alimentés par batterie avec des paramètres de haute précision.

Pourquoi l'heure est importante ?

Il existe de nombreuses raisons pour lesquelles vous pouvez avoir besoin d'une heure précise. Le cas typique pour Windows est Kerberos, qui nécessite une précision de 5 minutes entre le client et le serveur. Toutefois, il existe de nombreux autres domaines qui peuvent être affectés par la précision du temps, notamment :

- Lois gouvernementales telles que :
  - Précision de 50 ms pour FINRA aux États-Unis
  - 1 ms : ESMA (MiFID II) dans l'Union européenne.
- Cryptography Algorithms
- Systèmes distribués tels que cluster/SQL/Exchange et les bases de données de documents
- Framework de blockchain pour les transactions en bitcoins
- Journaux distribués et analyse des menaces
- AD Replication
- PCI (Payment Card Industry) : précision de 1 seconde

Additional references

- Améliorations apportées à la précision de l'heure dans Windows Server 2016

Configuration de systèmes de haute précision

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

La synchronisation de temps dans Windows 10 et Windows Server 2016 est améliorée. Dans des conditions optimales, ces systèmes peuvent être configurés pour atteindre et maintenir une précision de 1 milliseconde (ms) ou mieux par rapport à UTC.

> ⚠ **Avertissement**
>
> Windows Server 2012 R2 et les versions précédentes ne répondent pas aux mêmes objectifs de précision élevé. Ces systèmes d'exploitation ne sont pas pris en charge pour une précision élevée. Dans ces versions, le service de temps Windows respectait les exigences suivantes :
>
> - Il fournissait la précision de temps nécessaire pour répondre aux exigences d'authentification Kerberos version 5.
> - Il fournissait un temps moyennement précis pour les clients et les serveurs Windows joints à une forêt Active Directory commune.
>
> Les tolérances accrues sur 2012 R2 et les versions précédentes sont hors de la spécification de conception du service de temps de Windows.

Configuration par défaut sur Windows 10 et Windows Server 2016

Bien que nous prenions en charge une précision allant jusqu'à 1 ms sur Windows 10 ou Windows Server 2016, la plupart des clients n'ont pas besoin d'un temps haute précision.

Ainsi, la **configuration par défaut** est destinée à répondre aux mêmes exigences que les systèmes d'exploitation antérieurs, à savoir :

- Fournir la précision nécessaire pour répondre aux exigences d'authentification Kerberos version 5.
- Fournir une heure moyennement précise pour les clients et les serveurs Windows joints à une forêt Active Directory commune.

Comment configurer des systèmes haute précision

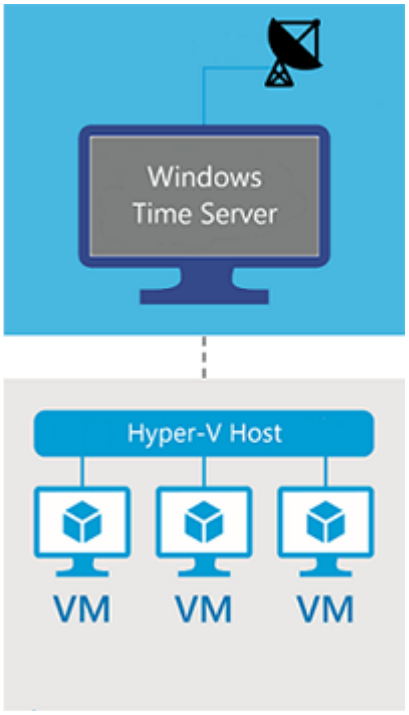
La précision de l'heure implique la distribution de bout en bout d'une heure précise depuis une source de temps de référence vers l'appareil final. Tout ce qui ajoute des asymétries dans les mesures le long de ce chemin influence négativement la précision réalisable sur vos appareils.

Pour cette raison, la limite de support permettant de configurer le service de temps Windows pour les environnements à haute précision est documentée en décrivant les exigences environnementales qui doivent également être satisfaites pour atteindre des cibles de précision élevées.

Système d'exploitation requis

Les configurations de haute précision nécessitent Windows 10 ou Windows Server 2016. Tous les appareils Windows dans la topologie du temps doivent répondre à cette exigence, y compris les serveurs de temps Windows de couche supérieure et, dans les scénarios virtualisés, les hôtes Hyper-V qui exécutent les machines virtuelles sensibles au facteur temps. Tous ces appareils doivent exécuter au moins Windows 10 ou Windows Server 2016.

Dans l'illustration suivante, les machines virtuelles nécessitant une précision élevée exécutent Windows 10 ou Windows Server 2016. De même, l'hôte Hyper-V sur lequel résident les machines virtuelles et le serveur de temps Windows en amont doivent également exécuter Windows Server 2016.



Conseil

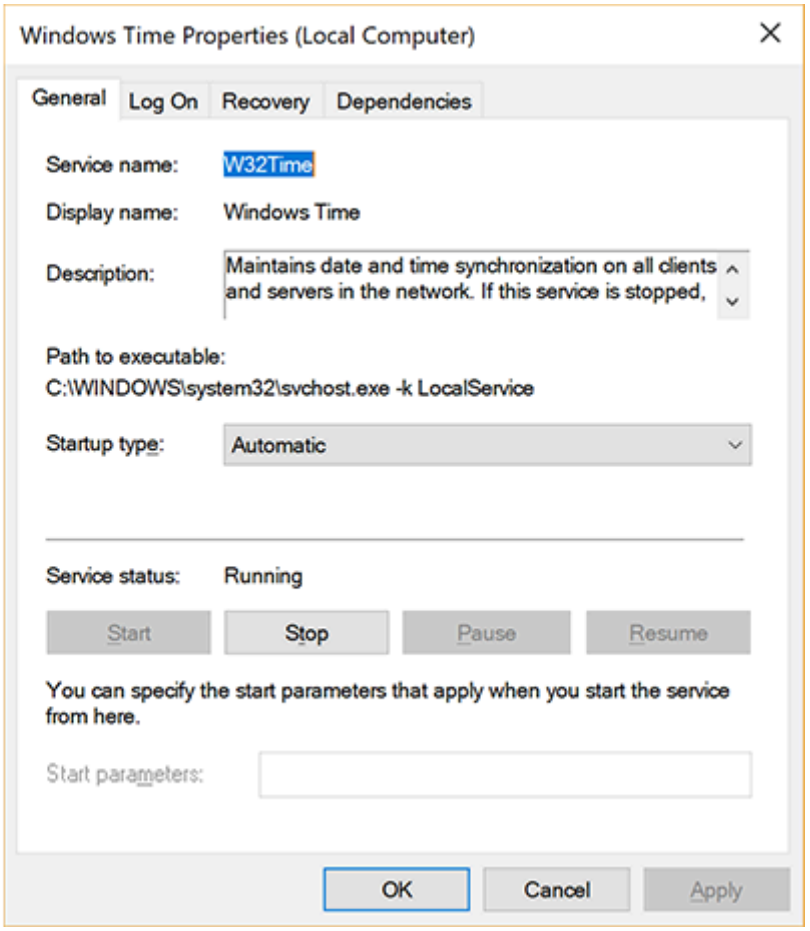
Vous pouvez exécuter la `winver` commande dans une invite de commandes ou via PowerShell pour afficher la version du système d'exploitation et le numéro de build :

Configuration système

Pour atteindre des objectifs de haute précision, vous devez configurer le système. Il existe plusieurs façons d'effectuer cette configuration, notamment directement dans le Registre ou par le biais de la stratégie de groupe. Pour plus d'informations sur chacun de ces paramètres, consultez les Informations techniques de référence sur le service de temps Windows : Outils du service de temps Windows.

Type de démarrage du service de temps Windows

Pour vous assurer que le service de temps Windows (W32Time) s'exécute en continu, définissez son type de démarrage sur **Automatique**.



Latence réseau unidirectionnelle cumulée

L'incertitude des mesures et le « bruit » augmentent la latence réseau. Il est donc impératif que la latence réseau se situe dans une limite raisonnable. Les exigences spécifiques dépendent de la précision cible et sont présentées dans l'article Limites de prise en charge pour configurer le service de temps Windows pour les environnements de haute précision.

Pour calculer la latence réseau unidirectionnelle cumulative, ajoutez les délais unidirectionnels individuels entre les paires de nœuds client-serveur NTP (Network Time Protocol) dans la topologie de temps, en commençant par la cible et en se terminant par la source de temps de stratum 1 à haute précision.

Par exemple : Considérez une hiérarchie de synchronisation horaire comportant une source extrêmement précise, deux serveurs NTP intermédiaires A et B et la machine cible, dans cet ordre. Pour obtenir la latence réseau cumulée entre la cible et la source, mesurez les temps d'aller-retour (RTT) NTP individuels moyens entre :

- Le serveur cible et le serveur de temps B
- Le serveur de temps B et le serveur de temps A
- Le serveur de temps A et la source

Cette mesure peut être obtenue à l'aide de l'outil boîte de réception `w32tm.exe` en effectuant les étapes suivantes :

1. Effectuez le calcul à partir de la cible et du serveur de temps B.

   Invite de commandes Windows

   ```
   w32tm /stripchart /computer:TimeServerB /rdtsc /samples:450 >
   c:\temp\Target_TsB.csv
   ```

2. Effectuez le calcul à partir du serveur de temps B par rapport au serveur de temps A (avec pointage vers ce dernier).

   Invite de commandes Windows

   ```
   w32tm /stripchart /computer:TimeServerA /rdtsc /samples:450 >
   c:\temp\Target_TsA.csv
   ```

3. Effectuez le calcul à partir du serveur de temps A par rapport à la source.

4. Ajoutez ensuite les temps d'aller-retour moyens mesurés à l'étape précédente et divisez le résultat par 2 pour obtenir le délai réseau cumulé entre la cible et la source.

Paramètres du Registre

MinPollInterval

Configure le plus petit intervalle en secondes log2 autorisé pour l'interrogation du système.

Agrandir le tableau

Descriptif	Valeur
Emplacement de la clé	HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config
Setting	6
Résultat	L'intervalle d'interrogation minimal est maintenant de 64 secondes.

MaxPollInterval

Configure le plus grand intervalle en secondes log2 autorisé pour l'interrogation du système.

Agrandir le tableau

Descriptif	Valeur
Emplacement de la clé	HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config
Setting	6
Résultat	L'intervalle d'interrogation maximal est maintenant de 64 secondes.

Intervalle de mise à jour

Nombre de cycles d'horloge entre les ajustements de correction de phase.

Agrandir le tableau

Descriptif	Valeur
Emplacement de la clé	HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config
Setting	100
Résultat	Le nombre de cycles d'horloge entre les ajustements de correction de phase s'élève maintenant à 100.

SpecialPollInterval

Configure l'intervalle d'interrogation en secondes quand l'indicateur SpecialInterval 0x1 est activé.

Agrandir le tableau

Descriptif	Valeur
Emplacement de la clé	HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient
Setting	64
Résultat	L'intervalle d'interrogation est maintenant de 64 secondes.

FrequencyCorrectRate

Agrandir le tableau

Descriptif	Valeur
Emplacement de la clé	HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config
Setting	2

UtiliserSslTimeData

Agrandir le tableau

Descriptif	Valeur
Emplacement de la clé	HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config
Setting	0
Résultat	La fonctionnalité d'amorçage du temps sécurisé est désactivée.

Application des paramètres de Registre modifiés

La commande suivante indique au service de temps Windows de récupérer les paramètres mis à jour :

Invite de commandes Windows

```
w32tm /config /update
```

La commande suivante redémarre le service de temps Windows pour récupérer les paramètres mis à jour :

Invite de commandes Windows

```
net stop w32time && net start w32time
```

L'application de la modification du paramètre UtiliserSslTimeData nécessite le redémarrage du système.

Notes

Pour en savoir plus sur les paramètres du Registre W32Time, consultez la référence du registre W32Time

Temps Windows pour la traçabilité

14/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Dans de nombreux secteurs, les réglementations exigent que les systèmes soient traçables au format UTC. Cela signifie que le décalage d'un système peut être attesté par rapport au temps universel coordonné (UTC). Pour autoriser les scénarios de conformité réglementaire, Windows 10 (version 1703 ou ultérieure) et Windows Server 2016 (version 1709 ou ultérieure) fournissent de nouveaux journaux des événements afin de proposer une image du point de vue du système d'exploitation permettant de comprendre les actions effectuées sur l'horloge système. Ces journaux des événements sont générés en continu pour le service de temps Windows et peuvent être examinés ou archivés en vue de les analyser ultérieurement.

Ces nouveaux événements permettent de répondre aux questions suivantes :

- L'horloge système a-t-elle été modifiée ?
- La fréquence d'horloge a-t-elle été modifiée ?
- La configuration du service de temps Windows a-t-elle été modifiée ?

Availability

Ces améliorations sont incluses dans Windows 10 version 1703 ou ultérieure et Windows Server 2016 version 1709 ou ultérieure.

Configuration

Aucune configuration n'est nécessaire pour réaliser cette fonctionnalité. Ces journaux des événements sont activés par défaut et se trouvent dans l'observateur d'événements sous le canal **Applications and Services Log\Microsoft\Windows\Time-Service\Operational**.

Liste des journaux des événements

La section suivante présente les événements journalisés en vue d'une utilisation dans les scénarios de traçabilité.

Cet événement est journalisé lors du démarrage du service de temps Windows (W32Time) et journalise les informations relatives à l'heure actuelle, au nombre de cycles actuel, à la configuration du runtime, aux fournisseurs de temps et à la fréquence d'horloge actuelle.

Agrandir le tableau

Description de l'événement	**Démarrage du service**
Details	Se produit au démarrage de W32time
Données journalisées	• Heure actuelle UTC • Nombre de cycles actuel • Configuration de W32Time • Configuration du fournisseur de temps • Fréquence d'horloge
Mécanisme de régulation	None. Cet événement se déclenche chaque fois que le service démarre.

Example:

```
W32time service has started at 2018-02-27T04:25:17.156Z (UTC), System Tick
Count 3132937.
```

Command:

Vous pouvez également interroger ces informations à l'aide des commandes suivantes :

Configuration du fournisseur de temps et de W32Time

```
w32tm.exe /query /configuration
```

Fréquence d'horloge

```
w32tm.exe /query /status /verbose
```

Informations techniques de référence sur le service de temps Windows

31/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Le service W32Time assure la synchronisation de l'horloge réseau pour les ordinateurs sans nécessiter de configuration étendue. Le service W32Time est essentiel au bon fonctionnement de l'authentification Kerberos V5 et donc de l'authentification AD DS. Toute application prenant en charge Kerberos, ce qui inclut la plupart des services de sécurité, repose sur la synchronisation de l'heure entre les ordinateurs qui participent à la demande d'authentification. Les horloges des contrôleurs de domaine AD DS doivent aussi être synchronisées pour garantir la réplication correcte des données.

> ⓘ **Notes**
>
> Dans Windows Server 2003 et Microsoft Windows 2000 Server, le service d'annuaire se nomme service d'annuaire Active Directory. Dans Windows Server 2008 R2 et Windows Server 2008, le service d'annuaire se nomme Active Directory Domain Services (AD DS). Le reste de cette rubrique fait référence aux services AD DS, mais les informations sont également applicables à Active Directory Domain Services dans Windows Server 2016.

The W32Time service is implemented in a dynamic link library called W32Time.dll, which is installed by default in **%Systemroot%\System32**. W32Time.dll a été développé à l'origine pour Windows 2000 Server de façon à prendre en charge une spécification du protocole d'authentification Kerberos V5 qui exigeait la synchronisation des horloges d'un réseau. Dès Windows Server 2003, W32Time.dll proposait une synchronisation des horloges réseau plus précise par rapport au système d'exploitation Windows Server 2000. De plus, dans Windows Server 2003, W32Time.dll prenait en charge une grande diversité d'appareils et de protocoles de temps réseau en utilisant des fournisseurs de temps.

Même s'il a été conçu à l'origine pour assurer la synchronisation des horloges pour l'authentification Kerberos, de nombreuses applications actuelles utilisent des horodatages pour garantir la cohérence transactionnelle, enregistrer l'heure des événements importants et d'autres informations critiques pour l'entreprise et sensibles au facteur temps. Ces applications bénéficient de la synchronisation de l'heure entre les ordinateurs assurée par le service de temps Windows.

Importance des protocoles de temps

Les protocoles de temps établissent une communication entre deux ordinateurs pour échanger les informations d'heure dont ils se servent pour synchroniser leurs horloges. Avec le protocole de temps du service de temps Windows, un client demande les informations d'heure à un serveur et synchronise son horloge en fonction des informations qu'il reçoit.

Le service de temps Windows utilise NTP pour permettre la synchronisation de l'heure sur un réseau. NTP est un protocole de temps Internet qui comprend les algorithmes de discipline nécessaires à la synchronisation des horloges. Ce protocole de temps est plus précis que SNTP (Simple Network Time Protocol) qui est utilisé dans certaines versions de Windows. Cependant, W32Time continue de prendre en charge SNTP pour permettre une compatibilité descendante avec les ordinateurs qui exécutent des services de temps SNTP, comme Windows 2000.

Sources d'information traitant de la configuration du service de temps Windows

This guide does **not** discuss configuring the Windows Time service. Il existe sur Microsoft TechNet et dans la Base de connaissances Microsoft plusieurs rubriques qui décrivent les procédures de configuration du service de temps Windows. Si vous avez besoin d'informations sur la configuration, les rubriques suivantes devraient vous aider à trouver les informations nécessaires.

- Pour configurer le service de temps Windows pour l'émulateur de contrôleur de domaine principal (PDC) racine de forêt, consultez :
  - Configurer le service de temps Windows sur l'émulateur PDC du domaine racine de forêt
  - Configuration d'une source de temps pour la forêt
  - L'article 816042 de la Base de connaissances Microsoft, Configuration d'un serveur de temps de référence dans Windows Server, qui décrit les paramètres de configuration pour les ordinateurs exécutant Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 et Windows Server 2003 R2.
- Pour configurer le service de temps Windows sur un client ou un serveur membre de domaine, ou même sur des contrôleurs de domaine qui ne sont pas configurés en tant qu'émulateur PDC de racine de forêt, consultez Configurer un ordinateur client pour la synchronisation automatique de l'heure du domaine.

> ⚠ **Avertissement**

Certaines applications peuvent exiger l'utilisation de services de temps de grande précision sur l'ordinateur. Dans ce cas, vous pouvez choisir de configurer une source de temps manuelle, tout en sachant que le service de temps Windows n'a pas été conçu pour fonctionner comme une source de temps hautement précise. Veillez à prendre connaissance des limitations de prise en charge pour les environnements exigeant une grande précision d'heure, comme décrit dans l'article 939322 de la Base de connaissances Microsoft, **Limite de prise en charge pour configurer le service de temps Windows pour les environnements à haute précision**.

- Pour configurer le service de temps Windows sur des ordinateurs clients ou serveurs Windows configurés comme membres de groupe de travail et non comme membres de domaine, consultez Configurer une source de temps manuelle pour un ordinateur client sélectionné.

- Pour configurer le service de temps Windows sur un ordinateur hôte qui exécute un environnement virtuel, consultez l'article 816042 de la Base de connaissances Microsoft, Configuration d'un serveur de temps de référence dans Windows Server. Si vous utilisez un produit de virtualisation non-Microsoft, veillez à consulter la documentation de l'éditeur de ce produit.

- Pour configurer le service de temps Windows sur un contrôleur de domaine qui s'exécute dans une machine virtuelle, il est recommandé de désactiver partiellement la synchronisation de l'heure entre le système hôte et le système d'exploitation invité jouant le rôle de contrôleur de domaine. Cela permet à votre contrôleur de domaine invité de synchroniser l'heure pour la hiérarchie de domaines, mais cela lui évite de subir un décalage horaire s'il est restauré à partir d'un état enregistré. Pour plus d'informations, consultez l'article 976924 de la Base de connaissances Microsoft, Vous recevez les ID d'événement 24, 29 et 38 du service de temps Windows sur un contrôleur de domaine virtualisé qui s'exécute sur un serveur hôte basé sur Windows Server 2008 avec Hyper-V et Considérations sur le déploiement pour les contrôleurs de domaine virtualisés.

- Pour configurer le service de temps Windows sur un contrôleur de domaine jouant le rôle d'émulateur PDC de racine de forêt qui s'exécute également dans un ordinateur virtuel, suivez les mêmes instructions que pour un ordinateur physique décrites dans Configurer le service de temps Windows sur l'émulateur PDC du domaine racine de forêt.

- Pour configurer le service de temps Windows sur un serveur membre qui s'exécute en tant qu'ordinateur virtuel, utilisez la hiérarchie temporelle de domaines comme décrit dans Configurer un ordinateur client pour la synchronisation automatique de l'heure du domaine.

> **Important**
>
> Avant Windows Server 2016, le service W32Time n'était pas conçu pour répondre aux besoins des applications sensibles au facteur temps. Cependant, les mises à jour apportées à Windows Server 2016 vous permettent désormais d'implémenter une solution pour une précision de 1 ms dans votre domaine. Pour plus d'informations, consultez **Précision de l'heure dans Windows Server 2016** et **Limites de prise en charge pour configurer le service de temps Windows pour les environnements de haute précision**.

Related topics

- Précision de l'heure dans Windows Server 2016
- Améliorations apportées à la précision de l'heure dans Windows Server 2016
- Fonctionnement du service de temps Windows
- Paramètres et outils du service de temps Windows
- Limites de prise en charge pour configurer le service de temps Windows pour les environnements de haute-précision

Fonctionnement du service de temps Windows

28/07/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Bien que le service de temps Windows ne soit pas une implémentation exacte du protocole NTP (Network Time Protocol), il utilise la suite complexe d'algorithmes définis dans les spécifications NTP pour garantir que les horloges sur les ordinateurs d'un réseau sont aussi précises que possible. Idéalement, toutes les horloges d'ordinateurs d'un domaine AD DS doivent être synchronisées avec l'heure d'un ordinateur de référence. De nombreux facteurs peuvent affecter la synchronisation de l'heure sur un réseau. Voici les facteurs qui sont souvent préjudiciables à la précision de la synchronisation dans AD DS :

- Network conditions
- Précision de l'horloge matérielle de l'ordinateur
- Quantité de ressources processeur et réseau disponibles pour le service de temps Windows

> **Notes**
>
> Cette rubrique explique uniquement le fonctionnement du service de temps Windows (W32Time). Pour savoir comment configurer le service de temps Windows, consultez Configuration de systèmes de haute précision.

> **Important**
>
> Avant Windows Server 2016, le service W32Time n'était pas conçu pour répondre aux besoins des applications sensibles au facteur temps. Cependant, les mises à jour apportées à Windows Server 2016 vous permettent désormais d'implémenter une solution pour une précision de 1 ms dans votre domaine. Pour plus d'informations, consultez Précision de l'heure dans Windows Server 2016 et Limites de prise en charge pour configurer le service de temps Windows pour les environnements de haute précision.

Par défaut, les ordinateurs qui synchronisent leur heure avec moins fréquence ou qui ne sont pas joints à un domaine sont configurés pour se synchroniser avec time.windows.com. Par conséquent, il est impossible de garantir la précision de l'heure sur les ordinateurs qui ont des connexions réseau intermittentes ou inexistantes.

Une forêt AD DS a une hiérarchie de synchronisation d'heure prédéterminée. Le service de temps Windows synchronise l'heure entre les ordinateurs de la hiérarchie, au sommet de laquelle se trouvent les horloges de référence les plus précises. Si plusieurs sources de temps sont configurées sur un ordinateur, le service de temps Windows utilise les algorithmes NTP pour sélectionner la meilleure source de temps parmi celles configurées en tenant compte de la capacité de l'ordinateur à se synchroniser avec celles-ci. Le service de temps Windows ne prend pas en charge la synchronisation réseau à partir d'homologues de diffusion ou de multidiffusion. Pour plus d'informations sur ces fonctionnalités NTP, consultez la RFC 1305 dans la base de données IETF RFC.

L'objectif pour chaque ordinateur exécutant le service de temps Windows est de maintenir la précision de l'heure. Sachant que les ordinateurs membres d'un domaine jouent par défaut le rôle de client temps, dans la plupart des cas, il n'est pas nécessaire de configurer le service de temps Windows. Cependant, le service de temps Windows peut être configuré pour demander l'heure à une source de temps de référence désignée et peut aussi fournir l'heure aux clients.

Le degré de précision de l'heure d'un ordinateur s'appelle une strate. La source de temps la plus précise sur un réseau (par exemple une horloge matérielle) occupe la strate la plus basse, à savoir la strate 1. Cette source de temps précise s'appelle une horloge de référence. Un serveur NTP qui obtient son heure directement auprès d'une horloge de référence occupe la strate juste au-dessus de celle de l'horloge de référence. Les ressources qui obtiennent l'heure auprès du serveur NTP sont distantes de l'horloge de référence de deux niveaux. Par conséquent, elles occupent une strate située à deux niveaux au-dessus de la source de temps la plus précise, et ainsi de suite. Plus le numéro de strate d'un ordinateur est élevé, plus la précision de son heure système est susceptible de diminuer. Par conséquent, le niveau de strate d'un ordinateur est une indication de sa proximité vis-à-vis de la source de temps la plus précise.

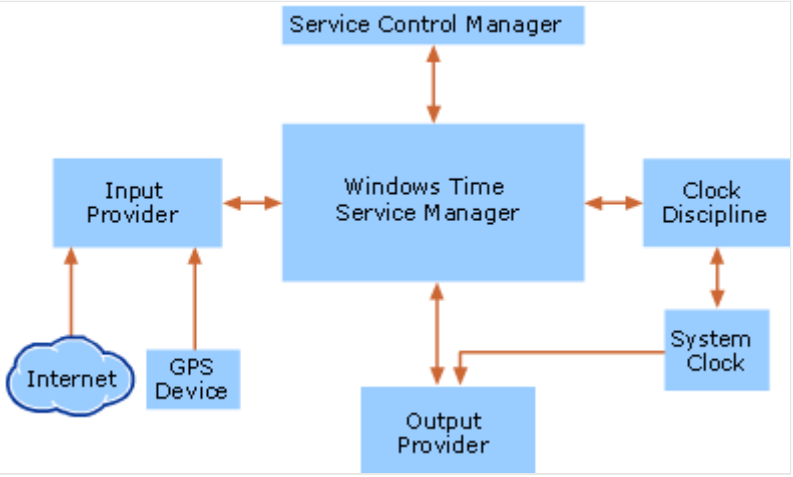
Quand le gestionnaire W32Time reçoit des échantillons d'heure, il utilise des algorithmes spéciaux NTP pour déterminer ceux qu'il est préférable d'utiliser. Le service de temps utilise par ailleurs un autre jeu d'algorithmes pour identifier la source de temps la plus précise parmi celles configurées. Une fois que le service de temps a identifié le meilleur échantillon d'heure, sur la base des critères précédents, il ajuste la fréquence d'horloge locale pour la faire converger vers l'heure exacte. Si la différence d'heure entre l'horloge locale et l'échantillon d'heure précis sélectionné (ce qui s'appelle aussi une asymétrie temporelle) est trop importante pour être corrigée par l'ajustement de la fréquence d'horloge locale, le service de temps met l'horloge locale à la bonne heure. Cet ajustement de la fréquence d'horloge ou le réglage direct de l'heure est ce que l'on appelle la « discipline d'horloge ».

Architecture du service de temps Windows

Le service de temps Windows se compose des éléments suivants :

- Gestionnaire de contrôle des services
- Gestionnaire du service de temps Windows
- Clock Discipline
- Time providers

Le schéma suivant illustre l'architecture du service de temps Windows.



Le gestionnaire de contrôle des services est chargé de démarrer et d'arrêter le service de temps Windows. Le gestionnaire du service de temps Windows est chargé de lancer l'action des fournisseurs de temps NTP intégrés au système d'exploitation. Le gestionnaire du service de temps Windows contrôle toutes les fonctions du service de temps Windows et assure le regroupement de tous les échantillons d'heure. En plus de fournir des informations sur l'état actuel du système, notamment la source de temps actuelle ou la date de la dernière mise à jour de l'horloge système, le gestionnaire du service de temps Windows est aussi chargé de créer des événements dans le journal des événements.

Le processus de synchronisation de l'heure comprend les étapes suivantes :

1. Les fournisseurs en entrée demandent des échantillons d'heure aux sources de temps NTP configurées et les réceptionnent.
2. Ces échantillons d'heure sont transmis au gestionnaire du service de temps Windows, qui collecte tous les échantillons et les transmet au sous-composant Discipline d'horloge.
3. Le sous-composant Discipline d'horloge applique les algorithmes NTP, ce qui se traduit par la sélection du meilleur l'échantillon d'heure.
4. Le sous-composant Discipline d'horloge ajuste l'heure de l'horloge système avec la plus grande précision possible en ajustant la fréquence d'horloge ou en réglant directement l'heure.

Si un ordinateur a été désigné serveur de temps, il peut envoyer l'heure à un ordinateur qui demande une synchronisation de l'heure à n'importe quel stade du processus.

Protocoles de temps du service de temps Windows

Les protocoles de temps déterminent le niveau de synchronisation entre les horloges de deux ordinateurs. Un protocole de temps est chargé d'identifier les meilleures informations d'heure disponibles et de faire converger les horloges de sorte que les différents systèmes restent à la même heure.

Le service de temps Windows utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure sur un réseau. NTP est un protocole de temps Internet qui comprend les algorithmes de discipline nécessaires à la synchronisation des horloges. NTP est un protocole de temps plus précis que le protocole SNTP (Simple Network Time Protocol) utilisé dans certaines versions de Windows ; Toutefois, W32Time continue de prendre en charge SNTP pour permettre la compatibilité descendante avec les ordinateurs exécutant des services de temps basés sur SNTP.

Protocole NTP

Le protocole NTP (Network Time Protocol) est le protocole de synchronisation d'heure que le service de temps Windows utilise par défaut dans le système d'exploitation. NTP est un protocole de temps tolérant aux pannes et hautement scalable qui est le plus souvent utilisé pour synchroniser les horloges d'ordinateurs à partir d'une référence de temps désignée.

La synchronisation d'heure NTP se produit au cours d'une période donnée et implique le transfert de paquets NTP sur un réseau. Les paquets NTP contiennent des horodatages constitués d'un échantillon d'heure du client et du serveur participant à la synchronisation de l'heure.

NTP se fie à une horloge de référence pour définir l'heure la plus précise possible et synchronise toutes les horloges d'un réseau avec cette horloge de référence. L'heure fournie par NTP est basée sur le standard universel UTC (temps universel coordonné). L'heure UTC étant indépendante des fuseaux horaires, NTP peut être utilisé partout dans le monde, quels que soient les paramètres de fuseau horaire.

NTP Algorithms

Pour identifier le meilleur échantillon d'heure, le service de temps Windows s'appuie sur les deux algorithmes NTP que sont l'algorithme de filtrage d'horloge et l'algorithme de sélection d'horloge. L'algorithme de filtrage d'horloge a pour fonction d'analyser les échantillons de temps reçus des sources de temps interrogées et d'identifier les meilleurs échantillons d'heure en provenance de chaque source. L'algorithme de sélection d'horloge identifie ensuite le serveur de temps le plus précis sur le réseau. Ces informations sont ensuite transmises à

l'algorithme de discipline d'horloge, qui se sert des informations collectées pour corriger l'horloge locale de l'ordinateur, tout en compensant les erreurs dues à la latence du réseau et à l'imprécision de l'horloge de l'ordinateur.

Les algorithmes NTP sont les plus précis dans les conditions de charges réseau et serveur légères à modérées. Comme pour tout algorithme qui prend en compte le temps de transit réseau, il peut arriver que les algorithmes NTP fonctionnent mal dans des conditions d'encombrement réseau extrême. Pour plus d'informations sur les algorithmes NTP, consultez la RFC 1305 dans la base de données IETF RFC.

Fournisseur de temps NTP

Le service de temps Windows est un package de synchronisation d'heure complet qui peut prendre en charge une grande variété d'appareils et de protocoles de temps. Pour permettre cette prise en charge, le service utilise des fournisseurs de temps enfichables. Un fournisseur de temps est chargé d'obtenir des horodatages précis (auprès du réseau ou du matériel) ou de fournir ces horodatages à d'autres ordinateurs via le réseau.

Le fournisseur NTP est le fournisseur de temps standard intégré au système d'exploitation. Le fournisseur NTP suit les normes spécifiées par NTP version 3 pour un client et un serveur, et peut interagir avec les clients et serveurs SNTP pour la compatibilité descendante. Le fournisseur NTP du service de temps Windows se compose des éléments suivants :

- **Fournisseur NtpServer en sortie.** Il s'agit d'un serveur de temps qui répond aux demandes d'heure clientes sur le réseau.
- **Fournisseur NtpClient en entrée.** Il s'agit d'un client de temps qui obtient les informations d'heure auprès d'une autre source (soit un appareil, soit un serveur NTP) qui peut ensuite retourner les échantillons d'heure utiles à la synchronisation de l'horloge locale.

Bien que les opérations réelles de ces deux fournisseurs soient étroitement liées, elles sont indépendantes pour le service de temps. Lorsqu'un ordinateur Windows est connecté à un réseau, il est configuré en tant que client NTP. De même, les ordinateurs exécutant le service de temps Windows tentent par défaut de synchroniser l'heure avec uniquement un contrôleur de domaine ou une source de temps spécifiée manuellement. Il s'agit des fournisseurs de temps préférés, car ce sont des sources de temps automatiquement disponibles et sécurisées.

NTP Security

Dans une forêt AD DS, le service de temps Windows s'appuie sur des fonctionnalités de sécurité de domaine standard pour imposer l'authentification des données de temps. La sécurité des paquets NTP échangés entre un ordinateur membre de domaine et un contrôleur

de domaine local qui joue le rôle de serveur de temps est basée sur l'authentification par clé partagée. Le service de temps Windows utilise la clé de session Kerberos de l'ordinateur pour créer des signatures authentifiées sur les paquets NTP qui transitent par le réseau. Les paquets NTP ne sont pas transmis dans le canal sécurisé du service Net Logon. Au lieu de cela, quand un ordinateur demande l'heure à un contrôleur de domaine situé dans la hiérarchie de domaines, le service de temps Windows exige une authentification de l'heure. Le contrôleur de domaine retourne alors les informations demandées sous la forme d'une valeur de 64 bits qui a été authentifiée avec la clé de session à partir du service Net Logon. Si le paquet NTP retourné n'est pas signé avec la clé de session de l'ordinateur ou s'il l'est de manière incorrecte, l'heure est rejetée. Tous ces échecs d'authentification sont consignés dans le journal des événements. C'est ainsi que le service de temps Windows assure la sécurité des données NTP au sein d'une forêt AD DS.

En général, les clients du service de temps Windows obtiennent automatiquement une heure précise pour la synchronisation auprès des contrôleurs de domaine d'un même domaine. Dans une forêt, les contrôleurs de domaine d'un domaine enfant synchronisent l'heure avec les contrôleurs de domaine de leurs domaines parents. Quand un serveur de temps retourne un paquet NTP authentifié à un client qui demande l'heure, le paquet est signé au moyen d'une clé de session Kerberos définie par un compte de confiance interdomaine. Ce compte est créé au moment où un nouveau domaine AD DS est joint à une forêt, et le service Net Logon gère la clé de session. De cette façon, le contrôleur de domaine qui est configuré comme étant fiable dans le domaine racine de la forêt devient la source de temps authentifiée de tous les contrôleurs de domaine des domaines parent et enfants, et indirectement de tous les ordinateurs situés dans l'arborescence de domaines.

Le service de temps Windows peut être configuré pour fonctionner entre différentes forêts, mais il est important de noter que cette configuration n'est pas sécurisée. Par exemple, un serveur NTP peut être disponible dans une forêt différente. Cependant, comme cet ordinateur se trouve dans autre forêt différente, il n'existe pas de clé de session Kerberos permettant de signer et authentifier les paquets NTP. Pour obtenir une synchronisation d'heure précise à partir d'un ordinateur situé dans une forêt différente, le client a besoin d'un accès réseau à cet ordinateur et le service de temps doit être configuré pour utiliser une source de temps spécifique située dans l'autre forêt. Si un client est configuré manuellement pour accéder à l'heure d'un serveur NTP situé en dehors de sa propre hiérarchie de domaines, les paquets NTP échangés entre le client et le serveur de temps ne sont pas authentifiés et donc pas sécurisés. Même avec l'implémentation des approbations de forêt, le service de temps Windows n'est pas sécurisé entre les forêts. Bien que le canal sécurisé Net Logon soit le mécanisme d'authentification du service de temps Windows, l'authentification entre les forêts n'est pas prise en charge.

Appareils pris en charge par le service de temps Windows

Les horloges matérielles que sont les horloges GPS ou radio sont souvent utilisées comme horloges de référence de haute précision. Par défaut, le fournisseur de temps NTP du service de temps Windows ne prend pas en charge la connexion directe d'un appareil à un ordinateur, même s'il est possible de créer un fournisseur de temps logiciel indépendant qui prend en charge ce type de connexion. Ce type de fournisseur, en liaison avec le service de temps Windows, peut fournir une référence de temps fiable et stable.

Les appareils, tels qu'une horloge au césium ou un récepteur GPS (Global Positioning System), fournissent une heure précise en suivant un standard pour obtenir une définition d'heure précise. Si les horloges au césium sont extrêmement stables et ne sont pas affectées par des facteurs comme la température, la pression ou l'humidité, elles sont aussi très coûteuses. Un récepteur GPS est beaucoup moins onéreux à exploiter et constitue également une horloge de référence précise. Les récepteurs GPS obtiennent leur heure auprès de satellites qui eux-mêmes obtiennent leur heure auprès d'une horloge au césium. Sans passer par un fournisseur de temps indépendant, les serveurs de temps Windows peuvent obtenir leur heure en se connectant à un serveur NTP externe, lui-même connecté à un appareil par téléphone ou Internet. Des organismes comme l'observatoire naval des États-Unis disposent de serveurs NTP qui sont connectés à des horloges de référence extrêmement fiables.

De nombreux récepteurs GPS et autres appareils de temps peuvent fonctionner comme serveurs NTP sur un réseau. Vous pouvez configurer votre forêt AD DS de sorte qu'elle synchroniser l'heure avec ces appareils externes à condition qu'ils jouent aussi le rôle de serveurs NTP sur votre réseau. Pour ce faire, configurez le contrôleur de domaine faisant office d'émulateur de contrôleur de domaine principal (PDC) dans la racine de votre forêt de sorte qu'il se synchronise avec le serveur NTP fourni par l'appareil GPS.

Protocole SNTP

Le protocole SNTP (simple Network Time Protocol) est un protocole de temps simplifié qui s'adresse aux serveurs et clients qui n'exigent pas le degré de précision offert par NTP. SNTP, une version plus rudimentaire de NTP, est le protocole de temps principal utilisé dans Windows. Comme le format des paquets réseau SNTP et NTP est identique, les deux protocoles sont interopérables. La principale différence entre les deux est que le protocole SNTP ne dispose pas des systèmes de filtrage complexes et de gestion d'erreurs proposés par NTP. Pour plus d'informations sur le protocole SNTP, consultez la RFC 1769 dans la base de données IETF RFC.

Interopérabilité des protocoles de temps

Le service de temps Windows peut fonctionner dans un environnement mixte d'ordinateurs exécutant Windows et Windows Server.

Le service de temps de Windows NT Server 4.0, appelé TimeServ, synchronise l'heure sur un réseau Windows NT 4.0. TimeServ est une fonctionnalité complémentaire disponible dans le cadre du Kit de *ressources Microsoft Windows NT 4.0* et ne fournit pas le degré de fiabilité de la synchronisation de temps requise par Windows Server.

Windows NT 4.0 utilise un mécanisme de synchronisation d'heure plus simple que celui du service de temps Windows. Par conséquent, pour garantir une synchronisation de temps précise sur votre réseau, il est recommandé de mettre à niveau tous les contrôleurs de domaine Windows NT 4.0 vers une version ultérieure de Windows ou Windows Server.

Processus et interactions du service de temps Windows

Le service de temps Windows est conçu pour synchroniser les horloges des ordinateurs d'un réseau. Le processus de synchronisation d'heure de réseau, également appelé « convergence horaire », intervient sur un réseau chaque fois que les ordinateurs accèdent à l'heure d'un serveur de temps plus précis. La convergence horaire implique un processus par lequel un serveur de référence fournit l'heure du moment aux ordinateurs clients sous forme de paquets NTP. Les informations contenues dans un paquet indiquent si l'heure actuelle de l'ordinateur doit être ajustée de façon à être synchronisée avec le serveur plus précis.

Dans le cadre du processus de convergence, les membres d'un domaine essaient de synchroniser l'heure avec un contrôleur de domaine situé dans le même domaine. Si l'ordinateur est un contrôleur de domaine, il tente de se synchroniser avec un contrôleur de domaine qui fait davantage autorité.

Les ordinateurs qui ne sont pas joints à un domaine ne tentent pas de se synchroniser avec la hiérarchie de domaine, mais sont configurés par défaut pour obtenir du temps à partir de time.windows.com.

Pour établir un ordinateur exécutant Windows Server comme faisant autorité, l'ordinateur doit être configuré pour être une source de temps fiable. Par défaut, le premier contrôleur de domaine installé sur un domaine Windows Server est automatiquement configuré pour être une source de temps fiable. S'agissant de l'ordinateur de référence du domaine, il doit être configuré pour se synchroniser avec une source de temps externe et non avec la hiérarchie de domaines. Par défaut, tous les autres membres du domaine Windows Server sont configurés pour se synchroniser avec la hiérarchie de domaine.

Une fois que vous avez établi un réseau Windows Server, vous pouvez configurer le service de temps Windows pour utiliser l'une des options suivantes pour la synchronisation :

- Synchronisation basée sur la hiérarchie de domaines

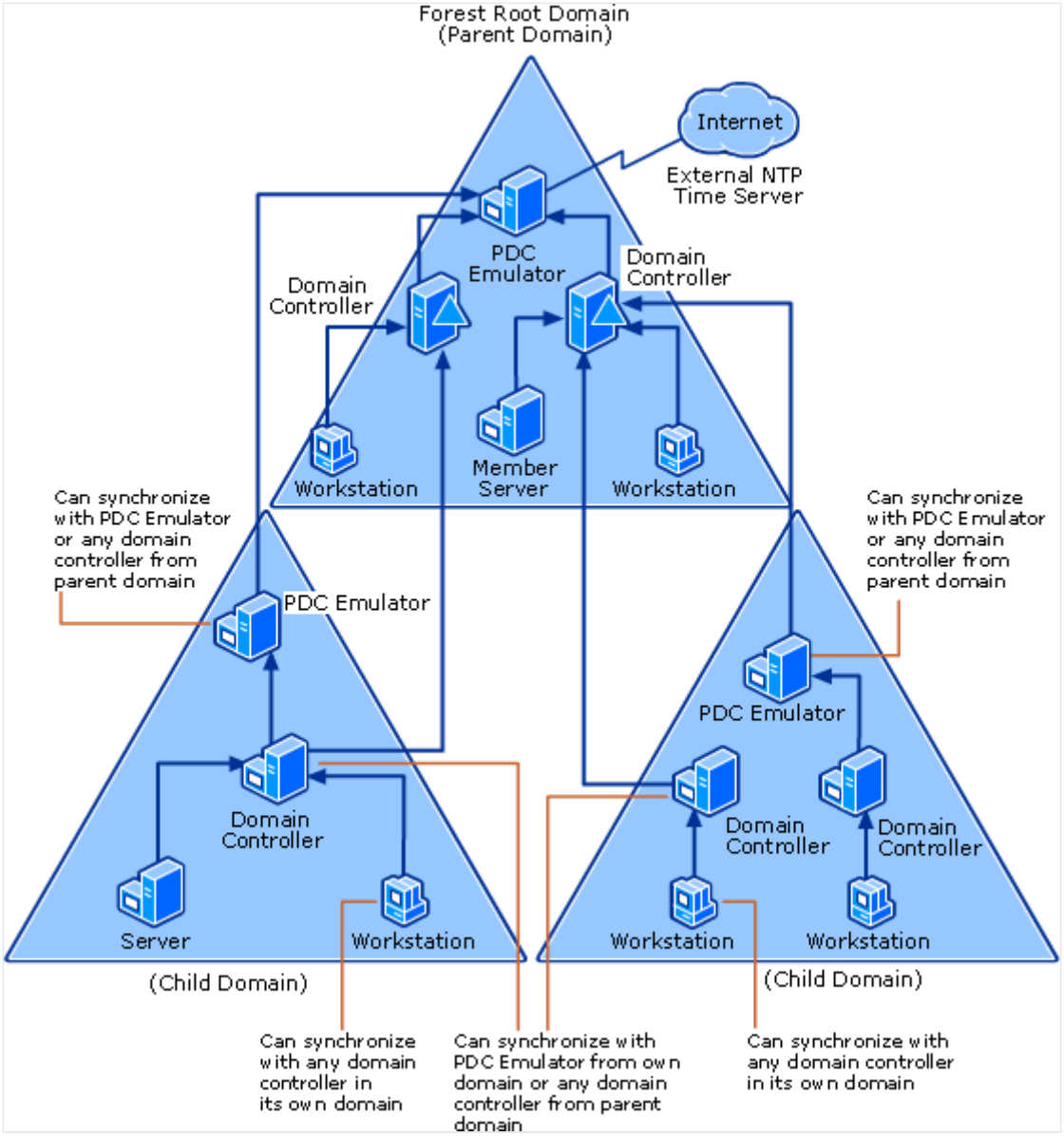
- Source de synchronisation spécifiée manuellement
- Tous les mécanismes de synchronisation disponibles
- No synchronization.

Chacun de ces types de synchronisation est décrit dans la section suivante.

Synchronisation basée sur la hiérarchie de domaines

La synchronisation basée sur une hiérarchie de domaines recherche une source fiable avec laquelle synchroniser l'heure dans la hiérarchie de domaines AD DS. Le service de temps Windows détermine la précision de chaque serveur de temps en fonction de la hiérarchie de domaines. Dans une forêt Windows Server, l'ordinateur qui détient le rôle d'émulateur de contrôleur de domaine principal (PDC) maître d'opérations, situé dans le domaine racine de la forêt, est considéré comme la meilleure source de temps, sauf si une autre source de temps fiable a été configurée. Le schéma suivant illustre un chemin de synchronisation d'heure entre les ordinateurs d'une hiérarchie de domaines.

Synchronisation de temps dans une hiérarchie AD DS



Configuration d’une source de temps fiable

Un ordinateur configuré en tant que source de temps fiable est identifié comme étant la racine du service de temps. Celle-ci correspond au serveur de référence du domaine et est généralement configurée pour récupérer l’heure auprès d’un serveur NTP externe ou d’un appareil. Un serveur de temps peut être configuré comme source de temps fiable pour optimiser la façon dont l’heure est transférée dans la hiérarchie de domaines. Si un contrôleur de domaine est configuré comme étant une source de temps fiable, le service Net Logon présente ce contrôleur de domaine comme étant une source de temps fiable au moment de se connecter au réseau. Quand d’autres contrôleurs de domaine recherchent une source de temps avec laquelle se synchroniser, ils choisissent d’abord une source fiable s’il en existe une.

Sélection de la source de temps

Le processus de sélection de la source de temps peut créer deux problèmes sur un réseau :

- Cycles de synchronisation supplémentaires.
- Volume accru du trafic réseau.

Un cycle dans le réseau de synchronisation se produit quand l'heure reste cohérente entre un groupe de contrôleurs de domaine et que la même heure est partagée entre eux en continu sans resynchronisation avec une autre source de temps fiable. L'algorithme de sélection de la source de temps du service de temps Windows est conçu pour éviter ces types de problèmes.

Un ordinateur utilise l'une des méthodes suivantes pour identifier une source de temps avec laquelle se synchroniser :

- Si l'ordinateur n'est pas membre d'un domaine, il doit être configuré pour se synchroniser avec une source de temps spécifiée.
- Si l'ordinateur est un serveur ou une station de travail membre au sein d'un domaine, par défaut, il suit la hiérarchie AD DS et synchronise son heure avec un contrôleur de domaine de son domaine local qui exécute actuellement le service de temps Windows.

Si l'ordinateur est un contrôleur de domaine, il effectue jusqu'à six requêtes pour trouver un autre contrôleur de domaine avec lequel se synchroniser. Chaque requête vise à identifier une source de temps présentant certains attributs, par exemple un type de contrôleur de domaine, un emplacement particulier et s'il s'agit ou non d'une source de temps fiable. La source de temps doit aussi respecter les contraintes suivantes :

- Une source de temps fiable ne peut se synchroniser qu'avec un contrôleur de domaine du domaine parent.
- Un émulateur PDC peut se synchroniser avec une source de temps fiable de son propre domaine ou avec un contrôleur de domaine du domaine parent.

Si le contrôleur de domaine n'est pas en mesure de se synchroniser avec le type de contrôleur de domaine qu'il interroge, la requête n'est pas exécutée. Avant d'effectuer la requête, le contrôleur de domaine sait auprès de quel type d'ordinateur il peut obtenir l'heure. Par exemple, un émulateur PDC local ne tente pas d'interroger les numéros trois ou six, car un contrôleur de domaine ne tente pas de se synchroniser avec lui-même.

Le tableau suivant liste les requêtes qu'effectue un contrôleur de domaine pour trouver une source de temps ainsi que l'ordre d'exécution des requêtes.

Requêtes de source de temps du contrôleur de domaine

Agrandir le tableau

Query Number	Domain Controller	Location	Fiabilité de la source de temps
1	Contrôleur de domaine parent	In-site	Préfère une source de temps fiable, mais peut se synchroniser avec une source de temps non fiable si c'est la seule à être disponible.
2	Contrôleur de domaine local	In-site	Se synchronise uniquement avec une source de temps fiable.
3	Émulateur PDC local	In-site	Non applicable. Un contrôleur de domaine ne tente pas de se synchroniser avec lui-même.
4	Contrôleur de domaine parent	Out-of-site	Préfère une source de temps fiable, mais peut se synchroniser avec une source de temps non fiable si c'est la seule à être disponible.
5	Contrôleur de domaine local	Out-of-site	Se synchronise uniquement avec une source de temps fiable.
6	Émulateur PDC local	Out-of-site	Non applicable. Un contrôleur de domaine ne tente pas de se synchroniser avec lui-même.

Notes

Un ordinateur ne se synchronise jamais avec lui-même. Si l'ordinateur qui tente la synchronisation est l'émulateur PDC local, il ne tente pas les requêtes 3 ou 6.

Chaque requête retourne la liste des contrôleurs de domaine qui peuvent être utilisés comme source de temps. Le service de temps Windows attribue à chaque contrôleur de domaine interrogé un score basé sur la fiabilité et l'emplacement du contrôleur de domaine. Le tableau suivant liste les scores attribués par le service de temps Windows à chaque type de contrôleur de domaine.

Score Determination

Agrandir le tableau

État du contrôleur de domaine	Score
Contrôleur de domaine situé sur le même site	8
Contrôleur de domaine marqué comme source de temps fiable	4
Contrôleur de domaine situé dans le domaine parent	2
Contrôleur de domaine correspondant à un émulateur PDC	1

Une fois que le service de temps Windows a déterminé qu'il a identifié le contrôleur de domaine ayant le meilleur score possible, aucune autre requête n'est effectuée. Les scores attribués par le service de temps sont cumulatifs, ce qui signifie qu'un émulateur PDC situé sur le même site reçoit un score de neuf.

Si la racine du service de temps n'est pas configurée pour se synchroniser avec une source externe, l'horloge matérielle interne de l'ordinateur régit l'heure.

Synchronisation spécifiée manuellement

La synchronisation spécifiée manuellement vous permet de désigner un homologue unique ou une liste d'homologues à partir duquel un ordinateur obtient du temps. Si l'ordinateur n'est pas membre d'un domaine, il doit être configuré manuellement pour se synchroniser avec une source de temps spécifiée. Un ordinateur membre d'un domaine est configuré par défaut pour se synchroniser à partir de la hiérarchie de domaine, la synchronisation spécifiée manuellement est la plus utile pour la racine de forêt du domaine ou pour les ordinateurs qui ne sont pas joints à un domaine. Le fait de spécifier manuellement qu'un serveur NTP externe se synchronise avec l'ordinateur de référence de votre domaine fournit une heure fiable. Cependant, configurer l'ordinateur de référence pour que votre domaine se synchronise avec une horloge matérielle est en fait une meilleure solution et est le gage de l'heure la plus précise et la plus sûre pour votre domaine.

Les sources de temps spécifiées manuellement ne sont pas authentifiées, sauf si un fournisseur de temps spécifique est écrit pour eux, et ils sont donc vulnérables aux attaquants. En outre, si un ordinateur se synchronise avec une source spécifiée manuellement plutôt que son contrôleur de domaine d'authentification, les deux ordinateurs peuvent ne pas être synchronisés, ce qui entraîne l'échec de l'authentification Kerberos. Cela peut entraîner l'échec d'autres actions nécessitant une authentification réseau, comme l'impression ou le partage de fichiers. Si seule la racine de la forêt est configurée pour se synchroniser avec une source externe, tous les autres ordinateurs de la forêt restent synchronisés entre eux, ce qui contrarie les attaques par relecture.

Tous les mécanismes de synchronisation disponibles

L'option « all available synchronization mechanisms » (tous les mécanismes de synchronisation disponibles) est la méthode de synchronisation la plus intéressante pour les utilisateurs d'un réseau. Cette méthode permet une synchronisation avec la hiérarchie de domaines et peut aussi fournir une autre source de temps si la hiérarchie de domaines devient indisponible, selon la configuration. Si le client ne parvient pas à synchroniser l'heure avec la hiérarchie de domaines, la source de temps revient automatiquement à la source de temps spécifiée par le

paramètre **NtpServer**. Cette méthode de synchronisation est la plus encline à fournir une heure précise aux clients.

Arrêt de la synchronisation de l'heure

Dans certaines situations, vous souhaiterez peut-être empêcher un ordinateur de synchroniser son heure. Par exemple, si un ordinateur tente de se synchroniser auprès d'une source de temps basée sur Internet ou sur un autre site en empruntant un réseau étendu (WAN) au moyen d'une connexion d'accès à distance, cela peut occasionner des frais téléphoniques coûteux. Si vous désactivez la synchronisation sur cet ordinateur, vous l'empêcherez d'accéder à une source de temps via une connexion d'accès à distance.

Vous pouvez aussi désactiver la synchronisation pour empêcher la génération d'erreurs dans le journal des événements. Chaque fois qu'un ordinateur tente de se synchroniser avec une source de temps qui n'est pas disponible, il génère une erreur dans le journal des événements. Si une source de temps est déconnectée du réseau pour des raisons de maintenance planifiée et que vous n'envisagez pas de reconfigurer le client afin qu'il se synchronise auprès d'une autre source, vous pouvez désactiver la synchronisation sur le client pour l'empêcher de tenter une synchronisation pendant que le serveur de temps est indisponible.

Il est utile de désactiver la synchronisation sur l'ordinateur désigné comme racine du réseau de synchronisation. Cela indique que l'ordinateur racine fait confiance à son horloge locale. Si la racine de la hiérarchie de synchronisation n'est pas définie sur **NoSync** et qu'elle ne peut pas se synchroniser avec une autre source de temps, les clients n'acceptent pas le paquet envoyé par cet ordinateur, car la confiance ne peut pas être accordée à son heure.

Les seuls serveurs de temps à être considérés comme fiables par les clients, même s'ils n'ont pas été synchronisés avec une autre source de temps, sont ceux qui ont été identifiés par le client comme étant des serveurs de temps fiables.

Désactivation du service de temps Windows

Le service de temps Windows (W32Time) peut être complètement désactivé. Si vous choisissez d'implémenter un produit de synchronisation d'heure tiers qui utilise NTP, vous devez désactiver le service de temps Windows. Cela est dû au fait que tous les serveurs NTP ont besoin d'accéder au port UDP (User Datagram Protocol) 123 et tant que le service de temps Windows s'exécute sur le système d'exploitation Windows Server, le port 123 reste réservé par l'heure Windows.

Ports réseau utilisés par le service de temps Windows

Le service de temps Windows communique sur un réseau pour identifier les sources de temps fiables, obtenir les informations d'heure et les fournir à d'autres ordinateurs. Il établit cette communication selon les normes RFC NTP et SNTP.

Affectations de port pour le service de temps Windows

Agrandir le tableau

Service name	UDP	TCP
NTP	123	N/A
SNTP	123	N/A

Related content

Informations techniques de référence sur le service de temps WindowsParamètres et outils du service de temps WindowsService de temps Windows (W32Time)

Paramètres et outils du service de temps Windows

18/09/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Le service de temps Windows (W32Time) synchronise la date et l'heure de tous les ordinateurs gérés par Active Directory Domain Services (AD DS). Cet article décrit les différents outils et paramètres utilisés pour gérer W32Time.

Par défaut, un ordinateur joint à un domaine synchronise l'heure via une hiérarchie de domaines de sources de temps. Toutefois, parfois, un ordinateur est configuré manuellement pour se synchroniser à partir d'une source de temps spécifique, peut-être parce qu'il n'a pas été précédemment joint à un domaine. Dans ce cas, vous pouvez reconfigurer l'ordinateur pour commencer à approvisionner automatiquement son temps à partir de la hiérarchie de domaine.

La plupart des ordinateurs joints à un domaine ont un type de client de temps du service d'annuaire NT5DS (Net Time 5DS), ce qui signifie qu'ils synchronisent l'heure à partir de la hiérarchie de domaine. Une exception est le contrôleur de domaine, qui fonctionne comme maître d'opérations d'émulateur de contrôleur de domaine principal (PDC) pour le domaine de forêt racine. Le maître d'opérations de l'émulateur du contrôleur de domaine principal est configuré à son tour pour synchroniser l'heure avec une source de temps externe.

Vous pouvez atteindre une précision d'une milliseconde dans votre domaine. Pour plus d'informations, consultez Limite de prise en charge pour un temps haute précision et Heure exacte pour Windows Server 2016.

Port réseau

W32Time suit la spécification NTP (Network Time Protocol), qui nécessite l'utilisation du port UDP (User Datagram Protocol) 123 pour toute synchronisation de temps. Chaque fois que l'ordinateur synchronise son horloge ou fournit l'heure à un autre ordinateur, cette communication se produit sur le port UDP 123. W32Time réserve ce port comme port de destination.

> ⓘ **Notes**
>
> - Les serveurs NTP écoutent généralement sur le port UDP 123 pour les requêtes et répondent à partir du même port, ce qui est également vrai pour le serveur NTP

W32Time intégré.

- Vous pouvez activer ou désactiver le client NTP W32Time intégré et le serveur NTP indépendamment. Les deux partagent le port UDP 123 pour leurs fonctions.
- Le client NTP W32Time intégré ne peut utiliser UDP 123 que comme port source.
- Si votre ordinateur a plusieurs cartes réseau (il est multi-accueil), vous ne pouvez pas activer W32Time en fonction d'une carte réseau.

Paramètres de ligne de commande pour W32Time

Vous pouvez utiliser la `w32tm` commande pour configurer les paramètres W32Time et diagnostiquer les problèmes de temps de l'ordinateur. La `w32tm` commande est l'outil en ligne de commande préféré pour la configuration, la surveillance et la résolution des problèmes W32Time. L'appartenance au groupe Administrateurs local est requise pour exécuter cet outil localement, et l'appartenance au groupe Administrateurs de domaine est requise pour exécuter cet outil à distance.

Pour utiliser `w32tm`, procédez comme suit :

1. Sélectionnez **Démarrer**, puis entrez **cmd**. Cliquez avec le bouton droit sur **Invite de commandes**, puis sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commandes, entrez **w32tm** suivi des paramètres applicables.

Agrandir le tableau

Paramètre	Descriptif
/?	Affiche l'aide de `w32tm` la ligne de commande.
/config [/computer :<*target*>] [/update] [/manualpeerlist : <*peer*>] [/syncfromflags :<] [/LocalClockDispersion :> <] [/reliable :(YES|NO)] [/largephaseoffset :> <*millisecondes*>]	**/computer:<*target*>** : modifie la configuration de la <*cible*>. S'il n'est pas spécifié, la cible par défaut est l'ordinateur local. **/update** : avertit W32Time que la configuration change, ce qui entraîne l'effet des modifications. **/manualpeerlist :<*peers*>** : définit la liste d'homologues manuelle sur <*des homologues*>, qui est une liste délimitée par un espace d'adresses DNS (Domain Name System) ou IP. Lorsque vous spécifiez plusieurs homologues, cette option doit être placée entre guillemets. **/syncfromflags :<*source*>** : définit les sources à partir de laquelle le client NTP doit se synchroniser. La < valeur *source*> doit être une liste séparée par des virgules des mots clés suivants (pas sensibles à la casse) :

Paramètre	Descriptif
	• **MANUAL** : inclut les pairs de la liste de pairs manuels. • **DOMHIER** : synchronise à partir d'un contrôleur de domaine de la hiérarchie de domaines. **/LocalClockDispersion :**<***seconds***> : configure la précision de l'horloge interne utilisée par W32Time lorsqu'il ne peut pas acquérir de temps à partir de ses sources configurées. **/reliable :(YES|NO)** : définit si cet ordinateur est une source de temps fiable. Ce paramètre est uniquement significatif sur les contrôleurs de domaine. • **YES** : cet ordinateur est un service de temps fiable. • **NO** : cet ordinateur n'est pas un service de temps fiable. **/largephaseoffset :**<***millisecondes***>: définit la différence de temps entre l'heure locale et l'heure réseau que W32Time considère comme un pic.
/debug {/disable | {/enable /file :<*nom*> /size :/<*bytes*> /entries :<*value*> [/truncate]}}	Active ou désactive le journal privé W32Time de l'ordinateur local. **/disable** : désactive le journal privé. **/enable** : active le journal privé. • **file:**<***name***> : spécifie le nom de fichier absolu. • **size:**<***bytes***> : spécifie la taille maximale de la journalisation circulaire. • **entrées :**<***value***> : contient une liste d'indicateurs, spécifiés par nombre et séparés par des virgules, qui spécifie les types d'informations à journaliser. La valeur indiquée doit être comprise entre **0** et **300**. Une plage de nombres est valide, car il s'agit de nombres uniques, tels que **0-100 103 106**. La valeur **0-300** est destinée à journaliser toutes les informations. **/truncate : tronque** le fichier s'il existe.
/dumpreg [/subkey :<*key*>] [/computer :<*target*>]	Affiche les valeurs associées à une clé de Registre donnée. La clé par défaut est **HKLM\System\CurrentControlSet\Services\W32Time** (la clé racine pour W32Time). **/subkey:**<***key***> : affiche les valeurs associées à la sous-clé <key> de la clé par défaut. **/computer:**<***target***> : interroge les paramètres du registre pour l'ordinateur <*cible*>.
/monitor [/domain :<*domain name*>] [/computers :<*name*>[,	Surveille W32Time. **/domain** : spécifie le domaine à superviser. Si aucun nom de domaine n'est donné et que les options **/domain** et **/computers** ne sont pas

Paramètre	Descriptif
<*name*>[,<*name*>...]]] [/threads : <*num*>]	spécifiées, le domaine par défaut est utilisé. Cette option peut être utilisée plusieurs fois. **/computers** : supervise la liste donnée d'ordinateurs. Les noms d'ordinateur sont séparés par des virgules, sans espace. Si un nom est précédé d'un astérisque (*), l'ordinateur est traité comme un contrôleur de domaine principal. Cette option peut être utilisée plusieurs fois. **/threads** : spécifie le nombre d'ordinateurs à analyser simultanément. La valeur par défaut est **3**. La plage autorisée est **de 1 à 50**.
/ntpte<NTP *période de temps*>	Convertit une heure NTP (mesurée tous les 2^{-7} de seconde à partir du 1er janvier 1900 à 0h) dans un format lisible.
/ntte<NT *période de temps*>	Convertit une heure du système Windows NT (mesurée tous les 10^{-7} de seconde à partir du 1er janvier 1601 à 0h) dans un format lisible.
/query [/computer :<*target*>] {/source | /configuration | /peer | /status} [/verbose]	Affiche les informations W32Time de l'ordinateur. **/computer:<*target*>** : interroge les informations de la <*cible*>. Si ce paramètre n'est pas spécifié, la valeur par défaut est l'ordinateur local. **/source** : affiche la source de temps. **/configuration** : affiche la configuration du runtime et la source des paramètres. En mode détaillé, ce paramètre affiche également les paramètres non définis ou inutilisés. **/peers** : affiche la liste de pairs et leur état. **/status** : affiche l'état W32Time. **/verbose** : active le mode détaillé pour afficher plus d'informations.
/registre	Inscrit W32Time pour s'exécuter en tant que service et ajoute ses informations de configuration par défaut au Registre.
/resync [/computer : <*computer*>] [/nowait] [/redécouvrir] [/soft]	Indique à un ordinateur qu'il doit resynchroniser son horloge dès que possible, en éliminant toutes les statistiques d'erreurs accumulées. Le client NTP nécessite UDP 123 comme port source. **/computer:<*computer*>** : spécifie l'ordinateur qui doit être resynchronisé. Si aucun ordinateur n'est spécifié, l'ordinateur local resynchronise. **/nowait** : n'attend pas que la resynchronisation se produise. Au lieu de cela, elle retourne immédiatement. Si cette option n'est pas présente, la commande attend la resynchronisation avant de retourner. **/redécouvrir** : Redécouvre la configuration du réseau, redécouvre les sources réseau, puis resynchronise.

Paramètre	Descriptif
	/soft : resynchronise en utilisant les statistiques d'erreur existantes. Cette option est utilisée à des fins de compatibilité.
/stripchart /computer :<*target*> [/period :<*refresh*>] [/dataonly] [/samples :<*count*>] [/rdtsc]	Affiche un graphique à bandes du décalage entre cet ordinateur et un autre. Le client NTP utilise un port source UDP éphémère pour communiquer avec le serveur afin d'éviter les conflits avec le client NTP intégré. **/computer :<*target*>** : spécifie l'ordinateur sur lequel mesurer le décalage. **/period :<*refresh*>** : spécifie le temps entre les échantillons, en secondes. La valeur par défaut est **2**. **/dataonly** : affiche les données uniquement, sans graphiques. **/samples :<*count* : collecte des exemples de nombre>** <, puis s'arrête.> S'il n'est pas spécifié, les exemples sont collectés tant que **Ctrl+C** n'est pas sélectionné. **/rdtsc** : pour chaque exemple, imprime des valeurs séparées par des virgules, ainsi que les en-têtes **RdtscStart**, **RdtscEnd**, **FileTime**, **RoundtripDelay** et **NtpOffset** au lieu du graphique de texte. • **RdtscStart** : valeur rdtsc (Read Time Stamp Counter) collectée juste avant la génération de la requête NTP. • **RdtscEnd** : valeur RDTSC collectée juste après la réception et le traitement de la réponse NTP. • **FileTime** : valeur locale `FILETIME` utilisée dans la requête NTP. • **RoundtripDelay** : temps écoulé en secondes entre la génération de la demande NTP et le traitement de la réponse NTP reçue, calculée en fonction des calculs d'aller-retour NTP. • **NTPOffset** : décalage de temps en secondes entre l'ordinateur local et le serveur NTP, calculé en fonction des calculs de décalage NTP.
/tz	Affiche les paramètres du fuseau horaire actuel.
/désinscrire	Annule l'inscription de W32Time et supprime toutes ses informations de configuration du Registre.

Configurer le client pour qu'il utilise deux serveurs de temps

Pour configurer un ordinateur client pour se connecter à deux serveurs de temps différents, l'un nommé `ntpserver.contoso.com` et l'autre nommé `clock.adatum.com`, exécutez la commande suivante :

Invite de commandes Windows

```
w32tm /config /manualpeerlist:"ntpserver.contoso.com clock.adatum.com"
/syncfromflags:manual /update
```

Configurer le client pour qu'il synchronise automatiquement l'heure à partir d'une source de domaine

Supposons que vous disposez d'un ordinateur client qui synchronise actuellement le temps à l'aide d'un ordinateur spécifié manuellement. Pour configurer l'ordinateur client pour synchroniser automatiquement l'heure à partir de la hiérarchie de domaine Active Directory, exécutez la commande suivante :

Invite de commandes Windows

```
w32tm /config /syncfromflags:domhier /update

net stop w32time

net start w32time
```

Vérifier la configuration de l'heure du client

Pour vérifier la configuration client d'un ordinateur client Windows ayant pour nom d'hôte `contosoW1`, exécutez la commande suivante :

Invite de commandes Windows

```
w32tm /query /computer:contosoW1 /configuration
```

La sortie de cette commande répertorie les paramètres de configuration W32Time définis pour le client.

Depuis Windows Server 2016, les améliorations apportées aux algorithmes de synchronisation de temps prennent en charge l'alignement avec les spécifications RFC (Request for Comments). Par conséquent, si vous souhaitez définir le client de temps local pour qu'il pointe vers plusieurs homologues, nous vous recommandons de préparer trois serveurs de temps ou plus.

Si vous n'avez que deux serveurs de temps, vous devez spécifier l'indicateur **NtpServer**`UseAsFallbackOnly` (0x2) pour supprimer la priorité de l'un d'eux. Par exemple, si vous souhaitez donner la priorité à `ntpserver.contoso.com` plutôt qu'à `clock.adatum.com`, exécutez la commande suivante :

Invite de commandes Windows

```
w32tm /config /manualpeerlist:"ntpserver.contoso.com,0x8 clock.adatum.com,0x2"
/syncfromflags:manual /update
```

Vous pouvez également exécuter la commande suivante et lire la valeur de `NtpServer` la sortie :

Invite de commandes Windows

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
```

Configurer une réinitialisation de l'horloge de l'ordinateur

Pour que `w32tm` réinitialise une horloge d'ordinateur, il vérifie d'abord le décalage `CurrentTimeOffset`, également appelé `Phase Offset`, entre l'heure actuelle et l'heure de l'horloge d'ordinateur pour déterminer si le décalage est inférieur à la valeur `MaxAllowedPhaseOffset`.

- `CurrentTimeOffset` ≤ `MaxAllowedPhaseOffset` : permet de régler progressivement l'horloge de l'ordinateur à l'aide de la fréquence d'horloge.
- `CurrentTimeOffset` > `MaxAllowedPhaseOffset` : définit immédiatement l'horloge de l'ordinateur.

Pour ajuster l'horloge de l'ordinateur à l'aide du taux d'horloge, `w32tm` calcule une `PhaseCorrection` valeur. Cet algorithme varie en fonction de la version de Windows :

- Windows Server 2016 et versions ultérieures :

  `PhaseCorrection_raw` = (`CurrentTimeOffset`) ÷ (16 × `PhaseCorrectRate` × `pollIntervalInSeconds`)

  `MaximumCorrection` = (`CurrentTimeOffset`) ÷ (`UpdateInterval` ÷ 100)

  `PhaseCorrection` = min(`PhaseCorrection_raw`, `MaximumCorrection`)

- Windows Server 2012 R2 et versions antérieures :

  `PhaseCorrection` = (`CurrentTimeOffset`) ÷ (`PhaseCorrectRate` × `UpdateInterval`)

Toutes les versions de Windows utilisent la même équation finale pour vérifier `PhaseCorrection` :

`PhaseCorrection` `SystemClockRate` ≤ ÷ 2

Notes

Les systèmes d'exploitation suivants appliquent des mises à jour cumulatives à partir de KB5006744, de sorte qu'ils utilisent la formule pour Windows Server 2016 et versions ultérieures :

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019 version 1809
- Windows 11
- Windows 10 version 1809

Dans ces équations, , `PhaseCorrectRate`, `UpdateInterval` `MaxAllowedPhaseOffset` et `SystemClockRate` sont mesurées en unités de cycles d'horloge. Sur les systèmes Windows, une milliseconde est égale à 10 000 cycles d'horloge.

Vous pouvez configurer la `MaxAllowedPhaseOffset` valeur dans le Registre. Toutefois, le paramètre du Registre est mesuré en secondes et non en battements d'horloge.

Pour afficher les `SystemClockRate` valeurs (`pollIntervalInSeconds` mesurées en secondes), ouvrez une fenêtre d'invite de commandes, puis exécutez la commande suivante : `w32tm /query /status /verbose`. Cette commande produit une sortie semblable aux lignes suivantes :

Sortie

```
Leap Indicator: 0(no warning)
Stratum: 1 (primary reference - syncd by radio clock)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0003538s
Root Dispersion: 0.0100002s
ReferenceId: 0x00000000 (unspecified)
Last Successful Sync Time: 5/23/2023 7:51:39 PM
Source: VM IC Time Synchronization Provider
Poll Interval: 6 (64s)

Phase Offset: -0.0000013s
ClockRate: 0.0156250s
State Machine: 2 (Sync)
Time Source Flags: 3 (Authenticated Hardware )
Server Role: 0 (None)
Last Sync Error: 0 (The command completed successfully.)
Time since Last Good Sync Time: 15.7344985s
```

Dans la sortie, l'intervalle d'interrogation est répertorié en cycles d'horloge et en secondes. Les équations utilisent la valeur mesurée en secondes (la valeur entre parenthèses).

La sortie répertorie le taux d'horloge en secondes. Pour calculer la valeur en cycles d'horloge `SystemClockRate` , utilisez la formule suivante :

() = (`value in clock ticks` `value in seconds`) × 1 000 × 10 000

Cette formule utilise les facteurs de conversion suivants :

- Une seconde est égale à 1 000 millisecondes.
- Une milliseconde est égale à 10 000 cycles d'horloge sur un système Windows, comme décrit dans La propriété DateTime.Ticks.

Par exemple:

- Si `SystemClockRate` la valeur est de 0,0156250 secondes, la valeur produite par l'équation est de 156 250 cycles d'horloge.
- Par extension, cinq minutes deviennent 5 × 60 × 1000 × 10000 = 3 000 000 000 cycles d'horloge.

Les exemples suivants montrent comment appliquer les calculs de correction de phase pour Windows Server 2012 R2 et les versions antérieures.

Exemple : le taux d'horloge système est désactivé de quatre minutes

Si l'heure de l'horloge de votre ordinateur est 11:05 et que l'heure actuelle réelle est 11:09, `w32tm` utilise les valeurs suivantes :

- `PhaseCorrectRate` = 1
- `UpdateInterval` = 30 000 battements d'horloge
- `SystemClockRate` = 156 000 battements d'horloge
- `MaxAllowedPhaseOffset` = 10 min = 600 secondes = 600 × 1 000 × 10 000 = 6 000 000 000 de battements d'horloge
- `CurrentTimeOffset` = 4 min = 4 × 60 × 1 000 × 10 000 = 2 400 000 000 battements d'horloge

Pour réinitialiser l'horloge, `w32tm` vérifie la condition suivante :

Est-ce que `CurrentTimeOffset` ≤ `MaxAllowedPhaseOffset` ?

Dans ce cas, la condition a les valeurs suivantes. Elle prend donc la valeur true :

2 400 000 000 ≤ 6 000 000 000 000

Ensuite, `w32tm` vérifie la condition suivante :

Est-ce que (CurrentTimeOffset) ÷ (PhaseCorrectRate × UpdateInterval) ≤ SystemClockRate ÷ 2 ?

Dans ce cas, la condition a les valeurs suivantes :

2 400 000 000 ÷ (30 000 × 1) ≤ 156 000 ÷ 2 ou 80 000 ≤ 78 000

Cette condition est false. Par conséquent, `w32tm` définit immédiatement l'horloge.

> ⓘ **Notes**
>
> Dans cet exemple, si vous souhaitez restaurer l'horloge lentement, vous devez également ajuster les valeurs du registre ou `PhaseCorrectRate` dans le Registre pour vous assurer que le résultat de `UpdateInterval` l'équation est vrai.

Exemple : le taux d'horloge système est désactivé de trois minutes

Si l'heure de l'horloge de votre ordinateur est 11:05 et que l'heure actuelle réelle est 11:08, `w32tm` utilise les valeurs suivantes :

- `PhaseCorrectRate` = 1
- `UpdateInterval` = 30 000 battements d'horloge
- `SystemClockRate` = 156 000 battements d'horloge
- `MaxAllowedPhaseOffset` = 10 min = 600 secondes = 600 × 1 000 × 10 000 = 6 000 000 000 de battements d'horloge
- `CurrentTimeOffset` = 3 min = 3 × 60 × 1 000 × 10 000 = 1 800 000 000 battements d'horloge

Pour réinitialiser l'horloge, `w32tm` vérifie la condition suivante :

Est-ce que `CurrentTimeOffset` ≤ `MaxAllowedPhaseOffset` ?

Dans ce cas, la condition a les valeurs suivantes. Elle prend donc la valeur true :

1 800 000 000 ≤ 6 000 000 000 000

Ensuite, `w32tm` vérifie la condition suivante :

Est-ce que (CurrentTimeOffset) ÷ (PhaseCorrectRate × UpdateInterval) ≤ SystemClockRate ÷ 2 ?

Dans ce cas, la condition a les valeurs suivantes :

(1 800 000 000) ÷ (1 × 30 000) ≤ 156 000 ÷ 2 ou 60 000 ≤ 78 000

Cette condition est vraie. L'horloge est rétablie lentement.

Utiliser l'éditeur de stratégie de groupe local

W32Time stocke plusieurs propriétés de configuration en tant qu'entrées de Registre. Vous pouvez utiliser des objets de stratégie de groupe (GPO) dans l'Éditeur d'objets de stratégie de groupe afin de configurer la plupart de ces informations. Par exemple, vous pouvez utiliser des objets de stratégie de groupe pour configurer un ordinateur en tant que serveur NTP ou client NTP, configurer le mécanisme de synchronisation de l'heure ou configurer un ordinateur pour qu'il soit une source de temps fiable. Vous pouvez également appliquer des paramètres de stratégie de groupe pour W32Time aux contrôleurs de domaine.

Windows stocke les informations de stratégie W32Time dans l'Éditeur de stratégie de groupe local sous **Configuration ordinateur\Modèles d'administration\System\Service de temps Windows**. Il stocke les informations de configuration définies par les stratégies dans le Registre Windows, puis utilise ces entrées de Registre pour configurer les entrées de Registre spécifiques à W32Time. Par conséquent, les valeurs définies par la stratégie de groupe remplacent toutes les valeurs préexistantes dans la section W32Time du Registre. Certains paramètres d'objet de stratégie de groupe prédéfinis diffèrent des entrées de Registre W32Time par défaut correspondantes.

Le tableau suivant répertorie les stratégies que vous pouvez configurer pour les sous-clés W32Time et registre équivalentes que ces stratégies affectent.

Agrandir le tableau

Stratégie de groupe	Emplacements dans le Registre[1,2]
Paramètres de configuration globale	W32Time W32Time\Config W32Time\Parameters
Fournisseurs de temps\Configurer le client NTP Windows	W32Time\TimeProviders\NtpClient
Fournisseurs de temps\Activer le client NTP Windows	W32Time\TimeProviders\NtpClient
Fournisseurs de temps\Activer le serveur NTP Windows	W32Time\TimeProviders\NtpServer

[1] Sous-clé : `HKLM\SOFTWARE\Policies\Microsoft`

[2] Sous-clé : `HKLM\SYSTEM\CurrentControlSet\Services\W32Time`

> **Notes**
>
> Quand vous supprimez un paramètre de stratégie de groupe, Windows supprime l'entrée correspondante de la zone stratégie du Registre.

Paramètres par défaut des objets de stratégie de groupe pour W32Time

Le tableau suivant répertorie les valeurs par défaut des **paramètres de configuration globaux** lorsqu'ils sont activés :

Agrandir le tableau

Paramètre de stratégie de groupe	Valeur par défaut
AnnounceFlags	10
ChainDisable	0
ChainEntryTimeout	16
ChainLoggingRate	30
ChainMaxEntries	128
ChainMaxHostEntries	4
ClockAdjustmentAuditLimit	800
ClockHoldoverPeriod	7,800
EventLogFlags	2
FrequencyCorrectRate	4
HoldPeriod	5
LargePhaseOffset	50 000 000
LocalClockDispersion	10
MaxAllowedPhaseOffset	3:00
MaxNegPhaseCorrection	172 800 (48 heures)
MaxPollInterval	10
MaxPosPhaseCorrection	172 800 (48 heures)

Paramètre de stratégie de groupe	Valeur par défaut
MinPollInterval	6
PhaseCorrectRate	1
PollAdjustFactor	5
Exiger des demandes de synchronisation sécurisée du temps	0
SpikeWatchPeriod	900
Intervalle de mise à jour	100 (1 seconde)
UtilizeSslTimeData	1

Paramètres d'objet de stratégie de groupe pour un client NTP

Le tableau suivant répertorie les paramètres client Windows NTP par défaut contenus dans **Configuration ordinateur\Modèles d'administration\System\Service de temps Windows\Fournisseurs de temps\Configurer le client NTP Windows**.

Agrandir le tableau

Paramètre de stratégie de groupe	Valeur par défaut
Serveur NTP	`time.windows.com`, 0x9
Type	**NT5DS** : utilisé pour les ordinateurs joints à un domaine **NTP** : utilisé pour les ordinateurs non joints à un domaine
CrossSiteSyncFlags	2
ResolvePeerBackoffMinutes	15
ResolvePeerBackoffMaxTimes	7
SpecialPollInterval	1 024
EventLogFlags	0

Notes

Si vous utilisez la stratégie de groupe pour définir la `NtpServer` valeur dans le cadre de la stratégie **configurer le client NTP Windows** et l'appliquer à un membre de domaine, W32Time n'utilise pas la valeur de `NtpServer` Registre. Pour afficher votre configuration

NTP, ouvrez l'invite de commandes et exécutez la commande suivante : `w32tm /query /configuration`.

Informations de référence sur le registre W32Time

W32Time stocke les informations sous les chemins d'accès au Registre suivants :

registry

```
HKLM\SYSTEM\CurrentControlSet\Services\W32Time
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer
```

⚠ Avertissement

Ces informations sont fournies sous forme de référence à utiliser pour la résolution des problèmes et la validation. Les clés de Registre Windows sont utilisées par W32Time pour stocker des informations critiques. Ne changez pas ces valeurs. Les modifications apportées au Registre ne sont pas validées par l'éditeur de Registre ou par Windows avant qu'elles ne soient appliquées. Si le Registre contient des valeurs non valides, Windows peut rencontrer des erreurs irrécupérables.

Certains paramètres du Registre sont mesurés en cycles d'horloge et d'autres en secondes. Pour effectuer une conversion entre les deux unités, consultez l'explication précédente dans Configurer une réinitialisation de l'horloge de l'ordinateur.

Dans le tableau suivant, *toutes les versions* font référence à toutes les versions prises en charge de Windows et Windows Server.

Configuration

Agrandir le tableau

Entrée de Registre	Versions	Descriptif
AnnounceFlags	Toutes les versions	Détermine si cet ordinateur est marqué comme étant un serveur de temps fiable. Un ordinateur n'est pas marqué comme fiable, sauf s'il est également marqué comme serveur de temps.

Entrée de Registre	Versions	Descriptif
		• **0x00** : Serveur pas d'heure • **0x01** : serveur toujours à temps • **0x02** : serveur de temps automatique • **0x04** : serveur de temps toujours fiable • **0x08** : serveur de temps fiable automatique La valeur par défaut pour les membres du domaine est **10**. La valeur par défaut pour les serveurs et les clients autonomes est **10**.
ClockAdjustmentAuditLimit	Windows Server 2016 version 1709 et versions ultérieures ; Windows 10 version 1709 et versions ultérieures	Spécifie les plus petits ajustements d'horloge locale qui peuvent être enregistrés dans le journal des événements W32Time sur l'ordinateur cible. La valeur par défaut est **de 800** parties par million (ppm).
ClockHoldoverPeriod	Windows Server 2016 version 1709 et versions ultérieures ; Windows 10 version 1709 et versions ultérieures	Indique le nombre maximal de secondes pendant lesquelles une horloge système peut théoriquement conserver sa précision sans se synchroniser avec une source de temps. Si, à l'issue de cette période, W32Time n'obtient pas de nouveaux échantillons de ses fournisseurs d'entrée, W32Time lance une nouvelle découverte des sources de temps. La valeur par défaut est **de 7 800** secondes.
EventLogFlags	Toutes les versions	Contrôle les événements des journaux du service de temps. • **0x1** : saut de temps • **0x2** : Modification de la source La valeur par défaut sur les membres du domaine est **2**. La valeur par défaut sur les serveurs et les clients autonomes est **2**.
FrequencyCorrectRate	Toutes les versions	Détermine la fréquence de correction de l'horloge. Si cette valeur est trop petite, l'horloge est instable et fait l'objet d'une correction excessive. Si la valeur est trop grande, la synchronisation de l'horloge prend beaucoup de temps. La valeur par défaut sur les membres du domaine est **4**. La valeur par défaut sur les serveurs et les clients autonomes est **4**.

Entrée de Registre	Versions	Descriptif
		La valeur zéro n'est pas valide pour l'entrée de Registre **FrequencyCorrectRate**.
HoldPeriod	Toutes les versions	Détermine la durée pendant laquelle la détection des pics est désactivée afin de mettre rapidement l'horloge locale en mode synchronisation. Un pic est un échantillon de temps indiquant que l'heure est décalée de plusieurs secondes, et est reçu après que les bons échantillons de temps reviennent de manière cohérente. La valeur par défaut sur les membres du domaine est **5**. La valeur par défaut sur les serveurs et les clients autonomes est **5**.
LargePhaseOffset	Toutes les versions	Indique qu'un décalage de temps supérieur ou égal à cette valeur en 10^{-7} de seconde est considéré comme un pic. Une interruption du réseau, telle qu'une grande quantité de trafic, peut entraîner un pic. Un pic est ignoré sauf s'il persiste pendant une longue période de temps. La valeur par défaut sur les membres du domaine est **de 50 000 000**. La valeur par défaut sur les clients et serveurs autonomes est **de 50 000 000**.
LocalClockDispersion	Toutes les versions	Détermine la dispersion (en secondes) que vous devez supposer quand la seule source de temps est l'horloge CMOS intégrée. La valeur par défaut sur les membres du domaine est **10**. La valeur par défaut sur les serveurs et les clients autonomes est **10**.
Décalage de Phase Maximum Autorisé	Toutes les versions	Spécifie le décalage maximal (en secondes) pendant lequel W32Time tente d'ajuster l'horloge de l'ordinateur en utilisant la fréquence d'horloge. Quand le décalage dépasse cette fréquence, W32Time définit l'horloge de l'ordinateur directement. La valeur par défaut pour les membres du domaine est **300**. La valeur par défaut pour les serveurs et les clients autonomes est **1**.
MaxClockRate	Toutes les versions	Géré par W32Time. Il contient des données réservées utilisées par le système d'exploitation Windows, et toutes les modifications apportées à ce paramètre peuvent entraîner des résultats imprévisibles. La valeur par défaut pour les membres du domaine est **de 155 860**. La valeur

Entrée de Registre	Versions	Descriptif
		par défaut pour les clients et serveurs autonomes est **de 155 860**.
MaxNegPhaseCorrection	Toutes les versions	Spécifie la plus grande correction de temps négative en secondes qu'effectue le service. Si le service détermine qu'une modification supérieure à cette valeur est requise, elle journalise un événement à la place. La valeur **0xFFFFFFFF** est un cas spécial. Cette valeur signifie que le service corrige toujours l'heure. La valeur par défaut pour les membres de domaine est **0xFFFFFFFF** (hexadécimal). La valeur par défaut pour les contrôleurs de domaine est **172 800** (48 heures). La valeur par défaut pour les serveurs et les clients autonomes est **54 000** (15 heures).
MaxPollInterval	Toutes les versions	Spécifie le plus grand intervalle (soit 2 secondes en base logarithmique) à être autorisé pour l'intervalle d'interrogation du système. Un système doit interroger selon l'intervalle planifié. Un fournisseur peut refuser de produire des échantillons lorsqu'il est demandé de le faire. La valeur par défaut pour les contrôleurs de domaine est **10**. La valeur par défaut pour les membres du domaine est **15**. La valeur par défaut pour les serveurs et les clients autonomes est **15**.
MaxPosPhaseCorrection	Toutes les versions	Spécifie la plus grande correction de temps positive en secondes qu'effectue le service. Si le service détermine qu'une modification supérieure à cette valeur est requise, elle journalise un événement à la place. La valeur **0xFFFFFFFF** est un cas spécial. Cette valeur signifie que le service corrige toujours l'heure. La valeur par défaut pour les membres de domaine est **0xFFFFFFFF** (hexadécimal). La valeur par défaut pour les contrôleurs de domaine est **172 800** (48 heures). La valeur par défaut pour les serveurs et les clients autonomes est **54 000** (15 heures).
MinClockRate	Toutes les versions	Géré par W32Time. Il contient des données réservées utilisées par le système d'exploitation

Entrée de Registre	Versions	Descriptif
		Windows, et toutes les modifications apportées à ce paramètre peuvent entraîner des résultats imprévisibles. La valeur par défaut pour les membres du domaine est **de 155 860**. La valeur par défaut pour les clients et serveurs autonomes est **de 155 860**.
MinPollInterval	Toutes les versions	Spécifie le plus petit intervalle (soit 2 secondes en base logarithmique) à être autorisé pour l'intervalle d'interrogation du système. Un système ne demande pas d'échantillons plus fréquemment que cette valeur. Un fournisseur peut produire des échantillons parfois autres que l'intervalle planifié. La valeur par défaut pour les contrôleurs de domaine est **6**. La valeur par défaut pour les membres du domaine est **10**. La valeur par défaut pour les serveurs et les clients autonomes est **10**.
PhaseCorrectRate	Toutes les versions	Détermine la fréquence de correction de l'erreur de phase. La spécification d'une petite valeur corrige rapidement l'erreur de phase, mais peut entraîner l'instabilité de l'horloge. Si la valeur est trop grande, il faut plus de temps pour corriger l'erreur de phase. La valeur par défaut sur les membres du domaine est **1**. La valeur par défaut sur les serveurs et les clients autonomes est **7**. La valeur zéro n'est pas valide pour l'entrée de Registre **PhaseCorrectRate**.
PollAdjustFactor	Toutes les versions	Détermine la décision d'augmenter ou de diminuer l'intervalle d'interrogation pour le système. Plus la valeur est élevée, plus la quantité d'erreur qui entraîne la diminution de l'intervalle d'interrogation est faible. La valeur par défaut sur les membres du domaine est **5**. La valeur par défaut sur les serveurs et les clients autonomes est **5**.
SpikeWatchPeriod	Toutes les versions	Spécifie la durée pendant laquelle un décalage suspect doit persister avant qu'il soit accepté comme correct (en secondes). La valeur par défaut sur les membres du domaine est **900**. La valeur par défaut sur les stations de travail et les clients autonomes est **900**.

Entrée de Registre	Versions	Descriptif
TimeJumpAuditOffset	Toutes les versions	Indique le seuil d'audit de saut de temps, en secondes. Le décalage est stocké en tant qu'entier non signé. Si le service de temps ajuste l'horloge locale en définissant l'horloge directement et que la correction de l'heure est supérieure à cette valeur, le service de temps journalise un événement d'audit.
UpdateInterval	Toutes les versions	Spécifie l'intervalle (en unités de 10 ms) entre les ajustements de correction de phase. La valeur 0 a le même effet que 1. Les valeurs par défaut sont : • Contrôleurs de domaine : **100** • Membres du domaine : **30 000** • Clients et serveurs autonomes : **360 000**
UtiliserSslTimeData	Versions de Windows postérieures à Windows 10 build 1511	Indique si W32Time utilise plusieurs horodatages SSL pour amorçage d'une horloge qui est grossièrement inexacte. La valeur **1** indique que plusieurs horodatages SSL sont utilisés. La valeur de Registre **UtiliserSslTimeData** fait référence à la fonctionnalité d'amorçage du temps sécurisé. Pour plus d'informations, consultez Amorçage du temps sécurisé : amélioration de la conservation du temps dans Windows. La valeur prête à l'emploi par défaut pour toutes les versions de Windows avec cette fonctionnalité est **1** , à l'exception de Windows Server 2025, où la valeur par défaut est **0**. L'appartenance au domaine n'affecte pas ce paramètre.

Journalisation améliorée

Les entrées de Registre suivantes ne font pas partie de la configuration par défaut W32Time, mais vous pouvez les ajouter au Registre pour obtenir des fonctionnalités de journalisation améliorées. Vous pouvez modifier les informations journalisées dans le journal des événements système en ajustant les paramètres **EventLogFlags** dans l'Éditeur d'objets de stratégie de groupe. Par défaut, W32Time journalise un événement chaque fois qu'il bascule vers une nouvelle source de temps.

Pour activer la journalisation W32Time améliorée, ajoutez les entrées de Registre suivantes dans le chemin d'accès `HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config` .

Agrandir le tableau

Entrée	Versions	Descriptif
FileLogEntries	Toutes les versions	Contrôle le nombre d'entrées créées dans le fichier journal W32Time. La valeur par défaut n'est **aucune**, ce qui entraîne l'absence de journaux d'activité W32Time. La valeur indiquée doit être comprise entre **0** et **300**. Cette valeur n'affecte pas les entrées du journal des événements que W32Time crée normalement.
FileLogName	Toutes les versions	Contrôle l'emplacement et le nom de fichier du journal W32Time. La valeur par défaut est vide. Il ne doit pas être modifié, sauf si **FileLogEntries** est modifié. Une valeur valide est un chemin d'accès complet et un nom de fichier que W32Time utilise pour créer le fichier journal. Cette valeur n'affecte pas les entrées du journal des événements que W32Time crée normalement.
FileLogSize	Toutes les versions	Contrôle le comportement de journalisation circulaire des fichiers journaux W32Time. Lorsque **FileLogEntries** et **FileLogName** sont définis, cette valeur est également définie. Il contient la taille en octets que le fichier journal peut atteindre avant de remplacer les entrées de journal les plus anciennes avec de nouvelles entrées. Utilisez **1 000 000** ou une valeur supérieure pour ce paramètre. Cette valeur n'affecte pas les entrées du journal des événements que W32Time crée normalement.

Contenu connexe

- RFC 1305 - Protocole de temps réseau, version 3
- RFC 5905 - Protocole de temps réseau, version 4

Aperçu du réseau local sans fil

16/08/2025

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

Le service LAN sans fil (WLAN) est une fonctionnalité de Windows Server qui vous permet de configurer, de découvrir et de vous connecter à des réseaux sans fil. Lorsqu'il est activé, le service WLAN AutoConfig analyse et sélectionne dynamiquement les réseaux sans fil auxquels votre appareil peut se connecter automatiquement à l'aide d'un adaptateur réseau sans fil. Le service AutoConfig se connecte automatiquement à un réseau sans fil préféré lorsqu'il est disponible.

Le Wi-Fi offre également diverses mesures de sécurité pour protéger les transmissions de données sur les réseaux sans fil à l'aide de protocoles d'authentification et de chiffrement. Pour plus d'informations, consultez la section Protocole d'authentification extensible (EAP) pour l'accès au réseau.

Prerequisites

- Un système d'exploitation Windows Server 2012 ou supérieur.
- Des pilotes pour les adaptateurs sans fil supportés.

Installation du réseau sans fil pour Windows Server

Le réseau local sans fil n'est pas installé par défaut dans Windows Server. Pour installer le réseau sans fil et le service associé, procédez comme suit :

1. Ouvrez **le Gestionnaire de serveur**, sélectionnez **Ajouter des rôles et des fonctionnalités**, sélectionnez **Suivant**, puis à nouveau.
2. Sur la page **Sélectionner des rôles de serveur**, sélectionnez **Suivant**, sélectionnez **Service LAN sans fil**, puis sélectionnez **Suivant**.
3. Sur la page **Confirmer les sélections d'installation**, sélectionnez **Installer**, puis **Fermer**.
4. Redémarrez votre appareil pour que les modifications soient prises en compte.

Vous pouvez également installer la fonctionnalité LAN sans fil en l'exécutant dans PowerShell :

PowerShell

```
Install-WindowsFeature -Name Wireless-Networking
```

> ⓘ **Notes**
>
> Dans Windows Server 2025, la fonctionnalité WLAN est installée par défaut et vous devez activer ce service pour utiliser les capacités sans fil.

Activer le service WLAN

Une fois votre appareil redémarré, le service **wlansvc** doit être activé dans l'application **Services** en procédant comme suit :

1. Sélectionnez **Démarrer le**> type **services.msc**> , sélectionnez **Services**.
2. Dans le volet droit, faites défiler vers le bas jusqu'à ce que vous **voyiez la configuration automatique DU RÉSEAU LOCAL**.
3. Cliquez avec le bouton droit sur **LA configuration automatique DU RÉSEAU LOCAL** , puis sélectionnez **Démarrer**.

Vous pouvez également utiliser l'invite de commande ou PowerShell pour démarrer le service WLAN en cliquant sur Exécuter :

Invite de commandes Windows

```
net start wlansvc
```

PowerShell

```
Start-Service -Name wlansvc
```

Installer WLAN pour le client Windows

Ce service est déjà installé et activé par défaut sur les appareils clients Windows.

Voir aussi

- Vue d'ensemble de NCSI
- Vue d'ensemble du déploiement de l'accès sans fil
- Guide de dépannage de la technologie sans fil