Documentation de prise en main de Windows Server

Windows Server crée une infrastructure d'applications connectées, de réseau et de services web, du groupe de travail au centre de données, en faisant le lien local avec Azure.

Overview

VUE D'ENSEMBLE

Qu'est-ce que Windows Server ?

Nouveautés de Windows Server 2025

Windows Server Insiders Preview

CONCEPT

Comparaison des fonctionnalités des éditions

Configuration matérielle requise

Fonctionnalités supprimées ou non développées dans Windows Server

Plan

CONCEPT

Installer, mettre à niveau ou migrer

Choix entre Server Core et Serveur avec Expérience utilisateur

Comparaison des canaux de maintenance

CONCEPT

Compatibilité des applications serveur Microsoft

Azure Hybrid Benefit pour Windows Server

Installation et mise à niveau

DÉPLOYER

Installer Windows Server à partir du support d'installation

Planifier votre mise à niveau de Windows Server

Réalisation d'une mise à niveau sur place

GUIDE PRATIQUE

Convertir des éditions et des types de licences

Installer la fonctionnalité de compatibilité des applications dans Server Core

Activation

CONCEPT

Activation automatique de machine virtuelle

Planification de l'activation de KMS

GUIDE PRATIQUE

Créer un hôte KMS

Activation de client KMS

Résolution des problèmes d'activation en volume Windows

Serveurs avec Azure Arc

CONCEPT

Options de déploiement de l'agent Azure Connected Machine

GUIDE PRATIQUE

Connecter Windows Server à Azure Arc

Obtenir des mises à jour de sécurité étendue

Fournir des mises à jour de sécurité étendues avec Azure Arc

Activer Hotpatch pour les serveurs avec Azure Arc

Qu’est-ce que Windows Server ?

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

> **Conseil**
>
> Déjà familiarisé avec Windows Server ? Accédez aux **nouveautés de Windows Server 2025** pour en savoir plus sur les dernières fonctionnalités et améliorations.

Windows Server est la plateforme de serveur d’entreprise de Microsoft qui permet aux organisations d’exécuter et de sécuriser des applications, des services et des charges de travail sur des environnements locaux, hybrides et cloud.

Que vous exécutiez une petite entreprise ou que vous gériez une infrastructure d’entreprise, Windows Server constitue la base de l’informatique sécurisée, évolutive et hautes performances qui augmente avec votre organisation. Basé sur des décennies d’innovation Windows, il sert de principal principal pour des millions d’organisations dans le monde entier, ce qui alimente tout ce qui se passe des serveurs de fichiers et des applications web aux charges de travail d’entreprise complexes et aux solutions basées sur l’IA.

https://learn-video.azurefd.net/vod/player?id=715f723f-0644-4b9d-b7df-6e708da43242&locale=fr-fr&embedUrl=%2Fwindows-server%2Fget-started%2Foverview

Pourquoi choisir Windows Server ?

Windows Server offre des fonctionnalités complètes qui aident les organisations à moderniser leur infrastructure tout en conservant la sécurité, les performances et la fiabilité.

Utilisez Windows Server pour :

- **Environnements mixtes** : gestion unifiée des charges de travail Windows, Linux et conteneur.
- **Intégration d’entreprise** : intégration transparente à SQL Server, System Center, Exchange, SharePoint, Project et infrastructure Windows existante.
- **Support commercial** : support de niveau entreprise avec une communauté technologique active.
- **Scénarios de conformité : fonctionnalités intégrées** pour les secteurs réglementés (soins de santé, finances, gouvernement).

- **Licence flexible** : choisissez entre les licences de paiement à l'utilisation, perpétuelles ou basées sur un abonnement.

Windows Server s'appuie sur cette base avec de nouvelles fonctionnalités qui améliorent la sécurité, les performances et l'intégration cloud. Les sections suivantes mettent en évidence certains des principaux avantages et fonctionnalités de Windows Server.

Sécurité avancée multicouche

Amélioration des protections contre les menaces en constante évolution, les protections multicouches et la résilience améliorée.

- **Protection avancée des identités** : services d'annuaire d'entreprise (Active Directory) qui fournissent une authentification centralisée, une autorisation et une gestion des stratégies sur les systèmes Windows, Linux et Mac.
- **Sécurité basée sur la virtualisation** : sécurité améliorée Hyper-V avec enclaves VBS et protection de clé pour l'informatique confidentielle.
- **Mise en réseau sécurisée** : chiffrement TLS 1.3, SMB sur QUIC et micro-segmentation avancée pour empêcher la propagation des attaques latérales.

Agilité du cloud n'importe où

Bénéficiez de la puissance d'Azure fournie à votre environnement cloud edge et hybride avec Azure Arc. Déployez avec une flexibilité complète : dans le cloud, dans votre centre de données ou hybride à la périphérie.

- **Flexibilité du déploiement** : Expérience Windows Server cohérente que vous déployiez localement, hybride ou dans Azure avec une gestion unifiée.
- **Hotpatching** : appliquez des mises à jour de sécurité sans redémarrages : réduction de 12 redémarrages requis par an à seulement 4 pour une productivité améliorée.
- **Intégration d'Azure Arc** : Azure Arc étend les fonctionnalités de gestion d'Azure à vos serveurs locaux, ce qui vous donne une gouvernance, des stratégies de sécurité et une surveillance de style cloud sans déplacer vos données, qu'elles se trouvent dans Azure, votre centre de données ou d'autres clouds.
- **Licences de paiement à l'utilisation** : tarification flexible basée sur l'abonnement avec Azure Arc.

Infrastructure haute performance et prête à l'avenir

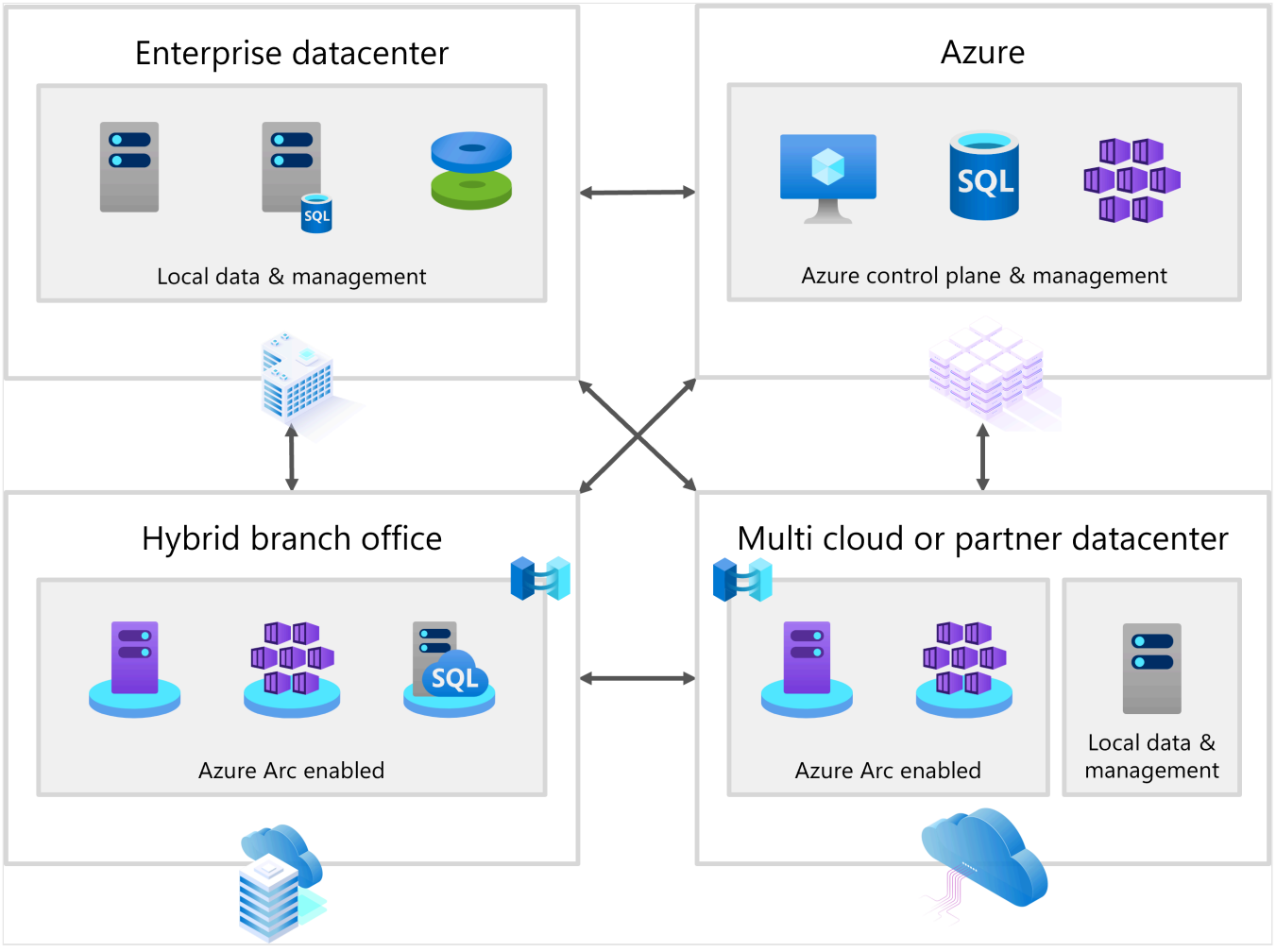
Avance dans la scalabilité, les performances, le stockage et les fonctionnalités pour prendre en charge l'IA et le ML.

- **IA et ML prêts** : partitionnement GPU sur les machines virtuelles avec prise en charge de la migration dynamique et performances améliorées pour les charges de travail IA et l'inférence de périphérie.
- **Grande échelle** : utilisez Hyper-V pour virtualiser vos charges de travail avec prise en charge de jusqu'à 240 To de RAM et de 2 048 processeurs virtuels par machine virtuelle pour les charges de travail les plus exigeantes.
- **Optimisation du stockage** : ReFS amélioré avec une déduplication et une compression optimisées pour le stockage défini par logiciel.

Pour plus d'informations sur les nouvelles fonctionnalités, consultez Nouveautés de Windows Server 2025.

Où pouvez-vous déployer Windows Server ?

Windows Server vous offre la possibilité de choisir l'emplacement de vos applications et données en fonction des besoins de votre entreprise. Chaque option de déploiement offre des avantages uniques pour aider à alimenter la croissance et l'innovation de votre organisation. Vous pouvez déployer Windows Server dans le cloud, dans votre centre de données ou en tant que solution hybride à la périphérie dans différents environnements.



Déployer Windows Server :

- ☁ **Dans le cloud**

  Déployez des machines virtuelles Windows Server dans Azure pour une scalabilité maximale et une portée globale. Parfait pour les nouvelles applications, les environnements de développement ou quand vous devez effectuer une mise à l'échelle rapide.

  Idéal pour : nouveaux projets, charges de travail variables, applications globales et scénarios de récupération d'urgence.

- 🏢 **Dans votre centre de données**

  Mettez à niveau votre infrastructure existante vers Windows Server pour contrôler complètement votre environnement. Idéal lorsque vous avez des exigences de conformité spécifiques, des investissements matériels existants ou besoin d'environnements air-gapped.

  Idéal pour : industries réglementées, infrastructure existante, exigences matérielles spécialisées et contrôle complet des données.

- 🌐 **Hybride à la périphérie**

  Étendez votre centre de données à Azure avec Azure Arc tout en conservant les charges de travail en cours d'exécution localement. Obtenez le meilleur des deux mondes : performances locales avec la gestion et les services cloud.

  Conservez des charges de travail sensibles localement pour des raisons de conformité, de performances ou de coût tout en obtenant la gestion, la supervision et les services cloud via Azure Arc. Parfait pour les organisations qui ont besoin d'avantages cloud sans engagement cloud complet ou problèmes de résidence des données.

  Idéal pour : adoption progressive du cloud, emplacements distribués, scénarios d'informatique en périphérie et utilisation d'investissements existants tout en obtenant des fonctionnalités cloud.

Éditions

Windows Server propose deux éditions conçues pour différentes échelles et besoins de virtualisation :

⛶ **Agrandir le tableau**

Edition	Norme	Datacenter
Environnements	Serveurs physiques ou environnements avec des besoins de virtualisation limités	Environnements hautement virtualisés et scénarios cloud
Droits de virtualisation	2 machines virtuelles plus un hôte Hyper-V par licence	Machines virtuelles illimitées plus un hôte Hyper-V par licence
Meilleur pour	Déploiements de petite à moyenne taille, charges de travail spécifiques, environnements conscients des coûts	Grands centres de données, déploiements cloud, virtualisation étendue

Les deux éditions incluent plusieurs des mêmes fonctionnalités et capabilites. Pour obtenir une comparaison détaillée, consultez :

- Comparaison des éditions de Windows Server
- Comparaison des verrous et des limites dans Windows Server

Approches de déploiement

Choisissez la bonne approche pour implémenter Windows Server en fonction de votre environnement actuel et de vos exigences :

Agrandir le tableau

Approche	Descriptif	Idéal pour
Nettoyer l'installation	Installer sur un nouveau matériel ou remplacer complètement le système d'exploitation existant	Nouveaux déploiements, performances maximales, configurations complexes
Mise à niveau sur place	Mettre à niveau tout en conservant les paramètres, les rôles et les données	Machines virtuelles, configurations stables, temps d'arrêt minimal
Migration	Déplacer progressivement des rôles et des fonctionnalités vers de nouvelles installations	Environnements complexes, systèmes stratégiques
Mise à niveau propagée du cluster	Mettre à niveau des nœuds de cluster un à la fois	clusters Hyper-V, serveur de fichiers Scale-Out, sla stricts

Pour obtenir des instructions détaillées sur chaque approche, consultez Les options d'installation, de mise à niveau et de migration.

Options d'installation

Lors de l'installation de Windows Server, choisissez entre deux options en fonction de la façon dont vous envisagez de gérer votre serveur :

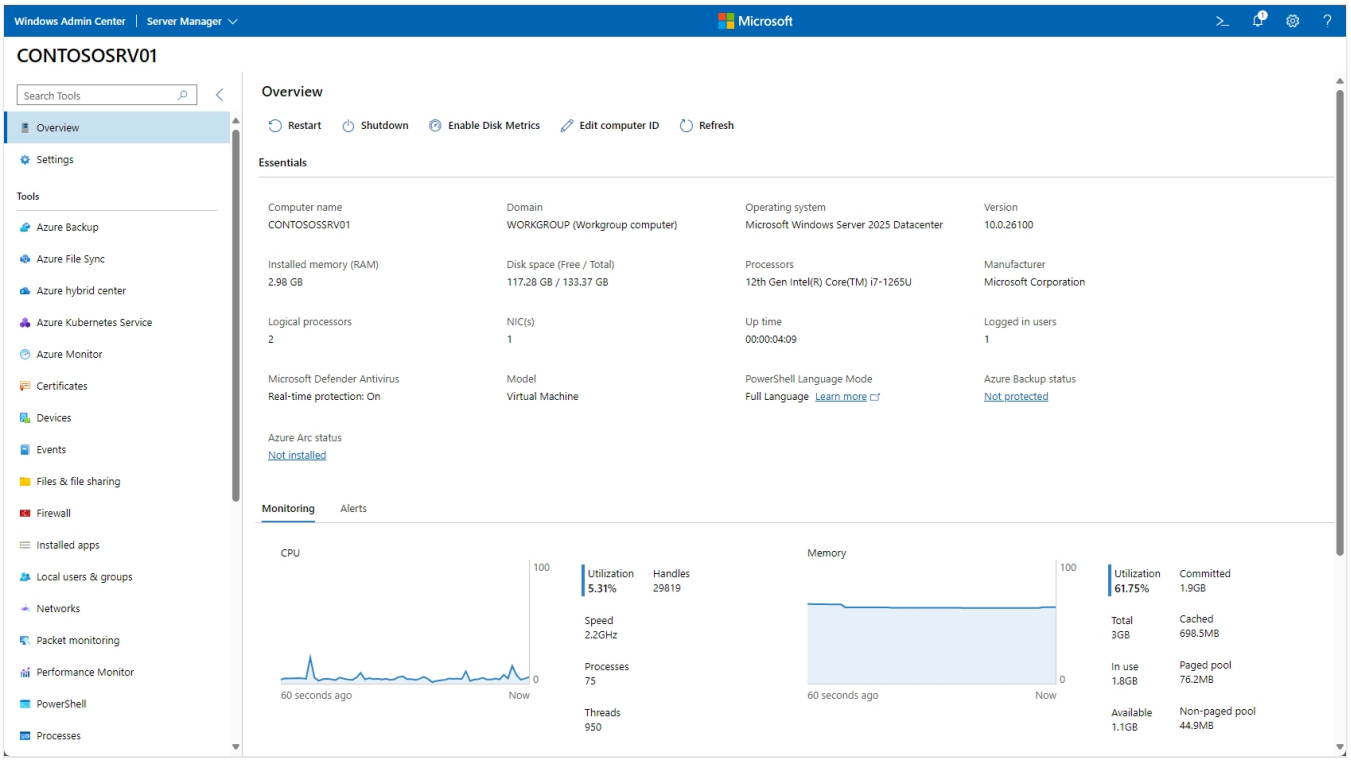
Agrandir le tableau

Option d'installation	Server Core	Server avec Expérience utilisateur
Description	Installation minimale sans interface graphique. Géré via PowerShell, SConfig ou des outils à distance. Offre une empreinte réduite, une surface d'attaque réduite et de meilleures performances.	Installation complète avec le bureau Windows standard et tous les outils de gestion de l'interface graphique utilisateur. Fournit une interface familière et une gestion graphique locale.
Idéal pour	La plupart des charges de travail serveur, en particulier lors de l'utilisation de la gestion à distance	Serveurs nécessitant un accès à l'interface graphique utilisateur local ou des applications dépendantes du bureau

En savoir plus sur les différences et les instructions détaillées sur Server Core et Server avec expérience de bureau.

Gérer Windows Server

Windows Server fournit plusieurs outils de gestion qui s'étendent d'un serveur unique à des centres de données d'entreprise.



Vous pouvez gérer Windows Server à l'aide d'une ou plusieurs des approches suivantes :

🌐 **Windows Admin Center** : gestion moderne basée sur un navigateur pour l'administration quotidienne des serveurs. Fonctionne localement ou s'intègre au portail Azure pour les scénarios hybrides.

☁ **Azure Arc** : gestion basée sur le cloud qui étend la gouvernance, la sécurité et la surveillance Azure aux serveurs n'importe où - dans votre centre de données, d'autres clouds ou emplacements de périphérie.

🔧 **Outils locaux** : gestion traditionnelle, y compris le Gestionnaire de serveur (administration de l'interface graphique utilisateur), PowerShell (interpréteur de commandes orienté objet et langage de script) et les outils d'administration de serveur distant pour l'accès direct au serveur et l'automatisation.

🏢 **System Center** : gestion à l'échelle de l'entreprise pour les grands centres de données nécessitant une surveillance, un déploiement et une gestion de configuration complètes.

Choisissez votre approche de gestion en fonction de la taille de votre environnement et de votre stratégie cloud. Pour obtenir des instructions détaillées, consultez la vue d'ensemble de la gestion de Windows Server.

Programme Windows Insider

Le programme Windows Insider pour Windows Server fournit une préversion de Windows Server, ce qui vous permet d'accéder rapidement à l'apprentissage, au test et à la mise en forme de l'avenir de Windows Server. Pour en savoir plus, vous pouvez commencer à utiliser le programme Windows Insider pour Windows Server et participer à la communauté Windows Server Insiders.

Bien démarrer avec Windows Server

Prêt à commencer votre parcours Windows Server ? Commencez par une évaluation gratuite pour tester dans votre environnement :

- Télécharger l'évaluation de Windows Server 2025
- Afficher la configuration requise
- Obtenir des conseils sur la mise à niveau
- Parcourez les parcours d'apprentissage de Windows Server pour vous aider à apprendre de nouvelles compétences et à accélérer votre déploiement avec des instructions pas à pas.

Pour obtenir les dernières actualités sur Windows Server, visitez le blog Windows Server pour rester à jour sur les annonces, fonctionnalités, événements et autres informations des équipes

d’ingénierie Windows Server. Vous pouvez également visiter la communauté Windows Server pour partager les meilleures pratiques, obtenir les dernières actualités et découvrir des experts sur Windows Server.

ⓘ **Remarque :** Cet article contient du contenu créé avec l'IA. En savoir plus

---

Last updated on 16/08/2025

Nouveautés de Windows Server 2025

S'applique à: ✅ Windows Server 2025

Cet article décrit certaines des évolutions récentes de Windows Server 2025, qui propose des fonctionnalités avancées améliorant la sécurité, les performances et la flexibilité. Grâce à des options de stockage plus rapides et la possibilité de s'intégrer à des environnements de cloud hybride, la gestion de votre infrastructure est désormais plus simplifiée. Windows Server 2025 repose sur la base solide de son prédécesseur et introduit une gamme d'améliorations innovantes pour s'adapter à vos besoins.

Expérience de bureau et mise à niveau

Explorez les options de mise à niveau et l'expérience de bureau.

Mise à niveau sur place à partir de Windows Server 2012 R2

Avec Windows Server 2025, vous pouvez mettre à niveau jusqu'à quatre versions à la fois. Vous pouvez effectuer une mise à niveau directe vers Windows Server 2025 à partir de Windows Server 2012 R2 et versions ultérieures.

Environnement de Bureau

Lors de votre première connexion, l'environnement de Bureau offre une expérience conforme au style et à l'apparence de Windows 11.

Bluetooth

Vous pouvez maintenant connecter des souris, des claviers, des casques, des appareils audio et bien plus encore via Bluetooth dans Windows Server 2025.

DTrace

Windows Server 2025 est équipé de `dtrace` en tant qu'outil natif. DTrace est un utilitaire en ligne de commande qui permet aux utilisateurs de surveiller et de résoudre les problèmes de performances de leur système en temps réel. Avec DTrace, vous pouvez instrumenter dynamiquement le noyau et le code d'espace utilisateur sans avoir à modifier le code lui-même. Cet outil polyvalent prend en charge une gamme de techniques de collecte et d'analyse de données, telles que les agrégations, les histogrammes et le traçage des événements au

niveau utilisateur. Pour plus d'informations, consultez DTrace pour obtenir de l'aide en ligne de commande et DTrace sur Windows pour d'autres fonctionnalités.

E-mail et comptes

Vous pouvez maintenant ajouter les types de comptes suivants dans Windows **Paramètres** sous **Comptes**>**comptes de messagerie &** pour Windows Server 2025 :

- ID d'entrée Microsoft
- Compte Microsoft
- Compte professionnel ou scolaire

La jonction de domaine est toujours requise pour la plupart des situations.

Hub de commentaires

Pour envoyer des commentaires ou signaler des problèmes que vous rencontrez lorsque vous utilisez Windows Server 2025, utilisez le Hub de commentaires Windows. Incluez des captures d'écran ou des enregistrements du processus qui ont provoqué le problème pour nous aider à comprendre votre situation et à partager des suggestions pour améliorer votre expérience Windows. Pour en savoir plus, consultez la section Explorer le Hub de commentaires.

Compression de fichier

Windows Server 2025 a une nouvelle fonctionnalité de compression. Pour compresser un élément, cliquez avec le bouton droit et sélectionnez **Compresser sur**. Cette fonctionnalité prend en charge ZIP, **7z**et **formats de compression TAR** avec des méthodes de compression spécifiques pour chacune d'elles.

Applications épinglées

Vous pouvez désormais épingler vos applications les plus utilisées via le menu **Démarrer** et personnaliser selon vos besoins. Les applications épinglées par défaut sont actuellement les suivantes :

- Installation d'Azure Arc
- Hub de commentaires
- Explorateur de fichiers
- Microsoft Edge
- Gestionnaire de serveur
- Paramètres

- Terminal
- Windows PowerShell

Gestionnaire des tâches

Windows Server 2025 intègre une version moderne du Gestionnaire des tâches, harmonisée au style Windows 11 grâce à l'utilisation du matériau Mica.

Wi-Fi

Il est désormais plus facile d'activer les fonctionnalités sans fil, car la fonctionnalité service LAN sans fil est désormais installée par défaut. Le service de démarrage sans fil est défini sur manuel. Pour l'activer, exécutez `net start wlansvc` dans l'invite de commandes, le terminal Windows ou PowerShell.

Windows Terminal

Le Terminal Windows, une application multishell puissante et efficace pour les utilisateurs en ligne de commande, est disponible dans Windows Server 2025. Recherchez le Terminal dans la barre de recherche.

WinGet

WinGet est installé par défaut, qui est un outil du Gestionnaire de package Windows en ligne de commande qui fournit des solutions complètes de gestionnaire de package pour l'installation d'applications sur des appareils Windows. Pour plus d'informations, consultez Utiliser l'outil WinGet pour installer et gérer des applications.

Sécurité multicouche avancée

Découvrez la sécurité dans Windows 2025.

Patch à chaud (préversion)

Hotpatch est désormais disponible pour les machines Windows Server 2025 connectées à Azure Arc après l'activation de Hotpatch dans le portail Azure Arc. Vous pouvez utiliser Hotpatch pour appliquer les mises à jour de sécurité du système d'exploitation sans redémarrer votre ordinateur. Pour en savoir plus, consultez Hotpatch.

> **Important**
>
> Hotpatch avec Azure Arc est actuellement en préversion. Pour connaître les conditions juridiques qui s'appliquent aux fonctionnalités Azure en version bêta, en préversion ou plus généralement non encore en disponibilité générale, consultez l'Avenant aux conditions d'utilisation des préversions de Microsoft Azure.

Protection des informations d'identification

À partir de Windows Server 2025, Credential Guard est désormais activé par défaut sur les appareils qui remplissent les conditions requises. Pour plus d'informations sur Credential Guard, voir Configurer Credential Guard.

Services de domaine Active Directory

Les dernières améliorations apportées aux services de domaine Active Directory (AD DS) et aux services de domaine Active Directory légers (AD LDS) proposent une série de nouvelles fonctionnalités et capacités visant à optimiser votre expérience de gestion de domaine.

- **fonctionnalité facultative de taille de page de base de données 32k**: Active Directory utilise une base de données ESE (Extensible Storage Engine) depuis son introduction dans Windows 2000 qui utilise une taille de page de base de données 8k. L'option architecturale 8k a imposé des limitations dans Active Directory, détaillées dans la documentation sur les limites maximales d'Active Directory : Évolutivité. Un exemple de cette limitation est un seul objet Active Directory d'enregistrement, qui ne peut pas dépasser la taille de 8 ko d'octets. Le passage à un format de page de base de données de 32k offre une amélioration considérable dans les domaines affectés par les anciennes restrictions. Les attributs à valeurs multiples peuvent maintenant contenir jusqu'à environ 3 200 valeurs, ce qui est une augmentation par un facteur de 2,6.

  Il est possible d'installer de nouveaux contrôleurs de domaine (DC) utilisant une base de données à pages de 32k et exploitant des Long Value ID (LID) de 64 bits, tout en fonctionnant en mode 8k-pages pour assurer la compatibilité avec les versions antérieures. Un DC mis à niveau continue d'utiliser son format de base de données actuel et ses pages de 8k. Le passage à une base de données de 32 000 pages est effectué à l'échelle de la forêt et nécessite que tous les contrôleurs de domaine (CD) de la forêt disposent d'une base de données capable de gérer 32 000 pages.

- **Mise à jour du schéma Active Directory** : Trois nouveaux fichiers de base de données de journaux sont introduits et étendent le schéma Active Directory : `sch89.ldf`, `sch90.ldf` et

`sch91.ldf`. Les mises à jour de schéma équivalentes AD LDS se trouvent dans `MS-ADAM-Upgrade3.ldf`. Pour en savoir plus sur les mises à jour de schéma précédentes, consultez mises à jour de schéma Windows Server Active Directory.

- Réparation d'objets Active Directory : les administrateurs d'entreprise peuvent désormais réparer des objets ayant des attributs noyaux manquants, notamment `SamAccountType` et `ObjectCategory`. Les administrateurs d'entreprise peuvent réinitialiser l'attribut `LastLogonTimeStamp` d'un objet à l'heure courante. Ces opérations sont effectuées grâce à une nouvelle fonctionnalité de modification d'opération RootDSE sur l'objet concerné appelé `fixupObjectState`.

- **Prise en charge de l'audit de la liaison de chaînes :** Vous pouvez désormais activer les événements 3074 et 3075 pour la liaison de chaînes LDAP (Lightweight Directory Access Protocol). Lorsque la stratégie de liaison de canal est modifiée en un paramètre plus sécurisé, un administrateur peut identifier les appareils dans l'environnement qui ne prennent pas en charge ou échouent la liaison de canal. Ces événements d'audit sont également disponibles dans Windows Server 2022 et versions ultérieures via KB4520412.

- **améliorations apportées à l'algorithme d'emplacement DC**: L'algorithme de découverte des DC fournit de nouvelles fonctionnalités avec des améliorations du mappage des noms de domaine courts de style NetBIOS aux noms de domaine de style DNS. Pour plus d'informations, consultez Localisation des contrôleurs de domaine dans Windows et Windows Server.

  > **Remarque**
  >
  > Windows n'utilise pas les mailslots pendant les opérations de découverte de DC car Microsoft a annoncé l'abandon de WINS et des mailslots pour ces technologies héritées.

- **Niveaux fonctionnels de la forêt et du domaine** - Le nouveau niveau fonctionnel est utilisé pour le support général et est requis pour la nouvelle fonctionnalité de taille de page de base de données de 32K. Le nouveau niveau fonctionnel mappe la valeur de `DomainLevel 10` et `ForestLevel 10` pour les installations sans surveillance. Microsoft n'a pas l'intention de modifier les niveaux fonctionnels pour Windows Server 2019 et Windows Server 2022. Pour réaliser une promotion ou une rétrogradation sans intervention manuelle d'un DC, référez-vous à la syntaxe du fichier de réponse DCPROMO destinée à cet usage.

L'API DsGetDcName prend également en charge le nouvel indicateur `DS_DIRECTORY_SERVICE_13_REQUIRED` qui permet l'emplacement des contrôleurs de domaine exécutant Windows Server 2025. Vous trouverez plus d'informations sur les niveaux fonctionnels dans les articles suivants :

- Niveaux fonctionnels de AD DS
- augmenter le niveau fonctionnel du domaine
- augmenter le niveau fonctionnel de la forêt

> **Remarque**
>
> De nouvelles forêts Active Directory ou ensembles de configuration AD LDS sont nécessaires pour avoir un niveau fonctionnel de Windows Server 2016 ou version ultérieure. La promotion d'un réplica d'Active Directory ou d'AD LDS nécessite que le domaine ou le jeu de configuration existant s'exécute déjà avec un niveau fonctionnel de Windows Server 2016 ou une version ultérieure.
>
> Microsoft recommande à tous les clients de commencer à planifier la mise à niveau de leurs serveurs Active Directory et AD LDS vers Windows Server 2022 en préparation de la prochaine version.

- **Algorithmes améliorés pour les recherches de nom et de numéro d'identification :** Le transfert de la recherche de nom et de SID de l'autorité de sécurité locale (LSA) entre les comptes de machine n'utilise plus la chaîne sécurisée Netlogon. L'authentification Kerberos et l'algorithme dc Locator sont utilisés à la place. Pour maintenir la compatibilité avec les systèmes d'exploitation hérités, il est toujours possible d'utiliser le canal sécurisé Netlogon comme option de secours.

- **Sécurité améliorée pour les attributs confidentiels**: les instances DCS et AD LDS autorisent uniquement LDAP à ajouter, rechercher et modifier des opérations qui impliquent des attributs confidentiels lorsque la connexion est chiffrée.

- **Sécurité améliorée pour les mots de passe de compte d'ordinateur par défaut**: Active Directory utilise désormais les mots de passe de compte d'ordinateur par défaut générés de manière aléatoire. Les contrôleurs de domaine Windows 2025 empêchent de définir les mots de passe des comptes ordinateur comme mots de passe par défaut du nom du compte ordinateur.

  Pour contrôler ce comportement, activez le paramètre objet de stratégie de groupe (GPO) **contrôleur de domaine : refuser de définir le mot de passe du compte d'ordinateur par défaut** situé dans *Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité*.

Les utilitaires tels que le Centre d'administration Active Directory (ADAC), les utilisateurs et les ordinateurs Active Directory (ADUC), `net computer` et `dsmod` respectent également ce nouveau comportement. ADAC et ADUC n'autorisent plus la création d'un compte pré-Windows 2000.

- **Prise en charge de PKINIT Kerberos pour une flexibilité cryptographique**: L'implémentation du protocole PKINIT (Cryptographie à clé publique pour l'authentification initiale dans Kerberos) est mise à jour pour permettre une flexibilité cryptographique, en prenant en charge davantage d'algorithmes et en supprimant des algorithmes codés en dur.

- **Modifications de Kerberos pour les algorithmes utilisés pour les tickets de délivrance de tickets**: le Centre de distribution Kerberos n'émettra plus de tickets de délivrance de tickets à l'aide du chiffrement RC4, tel que RC4-HMAC(NT).

- **Modifications Kerberos pour la configuration de type de chiffrement prise en charge : Kerberos** ne respecte plus la clé de Registre héritée REG_DWORD `SupportedEncryptionTypes` trouvée dans le chemin d'accès `HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Kerberos\Parameters`, Microsoft recommande d'utiliser la stratégie de groupe à la place. Pour en savoir plus sur les paramètres de stratégie de groupe, consultez Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos.

- **Paramètre GPO Gestionnaire de réseau local - Paramètre GPO Sécurité du réseau : Ne pas stocker la valeur de hachage du gestionnaire de réseau local lors du prochain changement de mot de passe** n'est plus présent ni applicable aux nouvelles versions de Windows.

- **Chiffrement LDAP par défaut** : tous les nouveaux déploiements Active Directory nécessitent la signature LDAP (sealing) par défaut pour toutes les communications client LDAP après une liaison SASL (Simple Authentication and Security Layer). Pour en savoir plus sur le comportement de signature, consultez signature LDAP pour les services de domaine Active Directory.

- **prise en charge LDAP du protocole TLS (Transport Layer Security) 1.3**: LDAP utilise la dernière implémentation SCHANNEL et prend en charge TLS 1.3 pour LDAP via des connexions TLS. L'utilisation de TLS 1.3 élimine les algorithmes de chiffrement obsolètes et améliore la sécurité par rapport aux versions antérieures. TLS 1.3 a pour objectif de chiffrer au maximum la liaison. Pour en savoir plus, consultez la section Protocoles TLS/SSL (Schannel SSP) et Suites de chiffrement TLS dans Windows Server 2022.

- **Comportement de changement de mot de passe de l'ancien Security Account Manager (SAM) par appel de procédure à distance (RPC)** : Les protocoles sécurisés tels que

Kerberos sont le meilleur moyen de modifier les mots de passe des utilisateurs du domaine. Sur les DC, la méthode récente de changement de mot de passe SAM RPC, SamrUnicodeChangePasswordUser4, utilisant le standard Advanced Encryption Standard (AES), est activée par défaut pour les appels distants. Les méthodes RPC SAM héritées suivantes sont bloquées par défaut lorsqu'elles sont appelées à distance :

- SamrChangePasswordUser
- SamrOemChangePasswordUser2
- SamrUnicodeChangePasswordUser2

Pour les utilisateurs de domaine membres du groupe utilisateurs protégés et pour les comptes locaux sur les ordinateurs membres du domaine, toutes les modifications de mot de passe à distance par le biais de l'interface RPC SAM héritée sont bloquées par défaut, y compris `SamrUnicodeChangePasswordUser4`.

Ce comportement peut être ajusté en configurant l'objet de stratégie de groupe suivant :

fr-FR: **Configuration ordinateur>Modèles d'administration>Système>Gestionnaire de comptes de sécurité>Configurer la politique des méthodes RPC de changement de mot de passe de SAM**

- **Prise en charge de l'accès non uniforme à la mémoire (NUMA)** : AD DS tire désormais parti du matériel compatible NUMA en utilisant des CPU dans tous les groupes de processeurs. Auparavant, Active Directory n'utiliserait que des processeurs dans le groupe 0. Active Directory peut s'étendre au-delà de 64 cœurs.

- **Compteurs de performance**: La surveillance et le dépannage des performances des compteurs suivants est désormais disponible :
  - **Localisateur de DC :** Des compteurs spécifiques aux clients et aux DC sont disponibles.
  - **Consultations LSA** : Recherches de noms et de SID par l'intermédiaire des API `LsaLookupNames`, `LsaLookupSids` et équivalentes. Ces compteurs sont disponibles sur les versions client et serveur.
  - **client LDAP**: disponible dans Windows Server 2022 et versions ultérieures via la mise à jour KB 5029250.

- **Ordre de priorité de réplication** : Les administrateurs peuvent désormais augmenter la priorité de réplication calculée par le système avec un partenaire de réplication particulier pour un contexte de nommage particulier. Cette fonctionnalité permet une plus grande flexibilité dans la configuration de l'ordre de réplication pour répondre à des scénarios spécifiques.

Compte de Service Managé Délégué

Ce nouveau type de compte permet la migration d'un compte de service vers un Compte de Service Managé délégué (dMSA). Ce type de compte est fourni avec des clés managées et entièrement aléatoires pour garantir une modification minimale de l'application pendant que les mots de passe du compte de service d'origine sont désactivés. Pour en savoir plus, consultez Vue d'ensemble des Comptes de Service Managé Délégué.

Solution de mot de passe d'administrateur local Windows

Windows Local Administrator Password Solution (LAPS) aide les organisations à gérer les mots de passe d'administrateur local sur leurs ordinateurs joints à un domaine. Il génère automatiquement des mots de passe uniques pour le compte d'administrateur local de chaque ordinateur. Il les stocke ensuite en toute sécurité dans Active Directory et les met à jour régulièrement. Les mots de passe générés automatiquement permettent d'améliorer la sécurité. Ils réduisent le risque que les attaquants accèdent à des systèmes sensibles à l'aide de mots de passe compromis ou faciles à deviner.

Plusieurs fonctionnalités nouvelles de Microsoft LAPS présentent les améliorations suivantes :

- **nouvelle fonctionnalité de gestion automatique des comptes**: les administrateurs informatiques peuvent désormais créer facilement un compte local sous gestion. Avec cette fonctionnalité, vous pouvez personnaliser le nom du compte et activer ou désactiver le compte. Vous pouvez même aléatoirer le nom du compte pour renforcer la sécurité. La mise à jour inclut également une intégration améliorée aux stratégies de gestion des comptes locaux existantes de Microsoft. Pour en savoir plus sur cette fonctionnalité, consultez les modes de gestion des comptes Windows LAPS.

- **nouvelle détection de restauration d'image**: Windows LAPS détecte désormais lorsqu'une restauration d'image se produit. Si une restauration se produit, le mot de passe stocké dans Active Directory peut ne plus correspondre au mot de passe stocké localement sur l'appareil. Les retours en arrière peuvent provoquer un *état fragmenté*. Dans ce cas, l'administrateur informatique ne peut pas se connecter à l'appareil à l'aide du mot de passe Windows LAPS persistant.

  Pour résoudre ce problème, une nouvelle fonctionnalité a été ajoutée qui inclut un attribut Active Directory appelé `msLAPS-CurrentPasswordVersion`. Cet attribut contient un identificateur global global aléatoire (GUID) écrit par Windows LAPS chaque fois qu'un nouveau mot de passe est conservé dans Active Directory et enregistré localement. Pendant chaque cycle de traitement, le GUID stocké dans `msLAPS-CurrentPasswordVersion` est interrogé et comparé à la copie persistante localement. S'ils sont différents, le mot de passe est immédiatement modifié.

Pour activer cette fonctionnalité, exécutez la dernière version de l'applet de commande `Update-LapsADSchema`. Windows LAPS reconnaît ensuite le nouvel attribut et commence à l'utiliser. Si vous n'exécutez pas la version mise à jour de l'applet de commande `Update-LapsADSchema`, Windows LAPS enregistre un événement d'avertissement 10108 dans le journal des événements, mais continue de fonctionner normalement à tous les autres égards.

Aucun paramètre de stratégie n'est utilisé pour activer ou configurer cette fonctionnalité. La fonctionnalité est toujours activée une fois le nouvel attribut de schéma ajouté.

- **Nouvelle phrase secrète**: les administrateurs informatiques peuvent désormais utiliser une nouvelle fonctionnalité dans Windows LAPS qui permet la génération de phrases secrètes moins complexes. Un exemple de phrase de passe pourrait être **EatYummyCaramelCandy**. Cette expression est plus facile à lire, mémoriser et taper par rapport à un mot de passe traditionnel comme **V3r_b4tim#963 ?**.

  Avec cette nouvelle fonctionnalité, vous pouvez configurer le paramètre de stratégie `PasswordComplexity` pour sélectionner l'une des trois listes de mots différents pour les phrases secrètes. Toutes les listes sont incluses dans Windows et ne nécessitent pas de téléchargement distinct. Un nouveau paramètre de stratégie appelé `PassphraseLength` contrôle le nombre de mots utilisés dans la phrase secrète.

  Lorsque vous créez une phrase secrète, le nombre spécifié de mots est sélectionné de manière aléatoire dans la liste de mots choisie et concaténés. La première lettre de chaque mot est mise en majuscule pour améliorer la lisibilité. Cette fonctionnalité prend également entièrement en charge la sauvegarde des mots de passe dans Active Directory ou Microsoft Entra ID.

  Les listes de mots de passe utilisées dans les trois nouveaux paramètres de phrase secrète `PasswordComplexity` proviennent de l'article de la Electronic Frontier Foundation Deep Dive : les nouvelles listes de mots de l'EFF pour des phrases secrètes aléatoires. Les listes de mots de passe Windows LAPS, régies par la licence CC-BY-3.0, sont disponibles en téléchargement.

  > **Remarque**
  >
  > Windows LAPS n'autorise pas la personnalisation des listes de mots intégrées ou l'utilisation de listes de mots configurées par le client.

- **dictionnaire de mots de passe de lisibilité améliorée**: Windows LAPS introduit un nouveau paramètre de `PasswordComplexity` qui permet aux administrateurs informatiques de créer des mots de passe moins complexes. Vous pouvez utiliser cette fonctionnalité

pour personnaliser LAPS pour utiliser les quatre catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) comme le paramètre de complexité existant de `4`. Avec le nouveau paramètre de `5`, les caractères les plus complexes sont exclus pour améliorer la lisibilité du mot de passe et réduire la confusion. Par exemple, le numéral **1** et la lettre **I** ne sont jamais utilisés avec le nouveau paramètre.

Lorsque `PasswordComplexity` est configuré pour `5`, les modifications suivantes sont apportées au jeu de caractères du dictionnaire de mots de passe par défaut :

- **N'utilisez pas :** les lettres **I**, **O**, **Q**, **l**, **o**
- **N'utilisez pas :** Les nombres **0**, **1**
- **N'utilisez pas :** Les caractères spéciaux **,**, **.**, **&**, **{**, **}**, **[**, **]**, **(**, **)**, **;**
- **Utiliser :** Les caractères spéciaux **:**, **=**, **?**, *****

Le composant logiciel enfichable ADUC (via Microsoft Management Console) propose désormais un onglet Windows LAPS amélioré. Le mot de passe Windows LAPS apparaît désormais dans une nouvelle police qui améliore sa lisibilité lorsqu'elle apparaît en texte brut.

- **Prise en charge des actions de post-authentification pour l'arrêt de processus individuels** : Une nouvelle option est ajoutée au paramètre de stratégie de groupe **Actions de post-authentification** (PAA), `Reset the password, sign out the managed account, and terminate any remaining processes`, qui se trouve dans **Configuration de l'ordinateur**>**Modèles administratifs**>**Système**>**LAPSP**> **Actions de post-authentification**.

  Cette nouvelle option est une extension de l'option précédente, `Reset the password and log off the managed account`. Après la configuration, le PAA prévient, puis termine toutes les sessions de connexion interactives. Il énumère et met fin aux processus restants qui s'exécutent toujours sous l'identité de compte local gérée par Windows LAPS. Aucune notification n'précède cette terminaison.

  L'extension des événements de journal pendant l'exécution de l'AAP offre une meilleure visibilité sur les opérations.

Pour en savoir plus sur Windows LAPS, consultez Qu'est-ce que Windows LAPS?

OpenSSH

Dans les versions antérieures de Windows Server, l'outil de connectivité OpenSSH a requis l'installation manuelle avant d'utiliser. Le composant côté serveur OpenSSH est installé par défaut dans Windows Server 2025. L'interface utilisateur du Gestionnaire de Serveur inclut également une option en une étape sous **Accès SSH distant** qui active ou désactive le service

`sshd.exe`. En outre, vous pouvez ajouter des utilisateurs au groupe **Utilisateurs OpenSSH** pour autoriser ou restreindre l'accès à vos appareils. Pour en savoir plus, consultez Vue d'ensemble d'OpenSSH pour Windows.

Base de référence de sécurité

En appliquant une base de référence de sécurité personnalisée, vous pouvez établir des mesures de sécurité dès le départ pour le rôle de votre appareil ou machine virtuelle en fonction de la posture de sécurité recommandée. Cette base de référence est équipée de plus de 350 paramètres de sécurité Windows préconfigurés. Vous pouvez utiliser les paramètres pour appliquer et mettre en œuvre des paramètres de sécurité spécifiques qui s'alignent sur les meilleures pratiques recommandées par Microsoft et les normes du secteur. Pour plus d'informations, consultez Présentation d'OSConfig.

Enclaves de sécurité basées sur la virtualisation

Une enclave de sécurité basée sur la virtualisation (VBS) est un environnement d'exécution approuvé basé sur le logiciel à l'intérieur de l'espace d'adressage d'une application hôte. Les enclaves VBS utilisent la technologie VBS sous-jacente pour isoler la partie sensible d'une application dans une partition sécurisée de la mémoire. Les enclaves VBS permettent d'isoler les charges de travail sensibles à la fois de l'application hôte et du reste du système.

Les enclaves VBS permettent aux applications de protéger leurs secrets en supprimant le besoin de faire confiance aux administrateurs et en renforçant la protection contre les attaquants malveillants. Pour plus d'informations, lisez la référence Win32 des enclaves VBS.

Protection des clés de sécurité basée sur la virtualisation

La protection des clés VBS permet aux développeurs Windows de sécuriser les clés de chiffrement à l'aide de VBS. VBS utilise la capacité d'extension de virtualisation du processeur pour créer un temps d'exécution isolé en dehors du système d'exploitation normal.

Quand elles sont utilisées, les clés VBS sont isolées dans un processus sécurisé. Les opérations clés peuvent se produire sans exposer le matériel de clé privée à l'extérieur de cet espace. À l'état de repos, une clé TPM chiffre les données de clé privée, ce qui lie les clés VBS à l'appareil. Les clés protégées de cette façon ne peuvent pas être vidées de la mémoire du processus ou exportées en texte brut à partir de l'ordinateur d'un utilisateur.

La protection par clé VBS permet d'empêcher les attaques d'exfiltration par n'importe quel attaquant au niveau de l'administrateur. VBS doit être activé pour utiliser la protection par clé. Pour plus d'informations sur l'activation de VBS, consultez Activer l'intégrité de la mémoire.

Connectivité sécurisée

Les sections suivantes décrivent la sécurité des connexions.

Gestion sécurisée des certificats

La recherche ou la récupération de certificats sur Windows prend désormais en charge les hachages SHA-256, comme décrit dans les fonctions CertFindCertificateInStore et CertGetCertificateContextProperty. L'authentification du serveur TLS est plus sécurisée sur Windows et nécessite désormais une longueur minimale de clé RSA de 2 048 bits. Pour en savoir plus, lisez Authentification de serveur TLS : obsolescence des certificats RSA faibles.

SMB sur QUIC

La fonctionnalité SMB sur QUIC du serveur, qui n'était disponible que dans l'édition Azure de Windows Server, est désormais disponible dans les versions Windows Server Standard et Windows Server Datacenter. SMB sur QUIC ajoute les avantages de QUIC, qui fournit des connexions chiffrées à faible latence sur Internet.

Stratégie d'activation de SMB sur QUIC

Les administrateurs peuvent désactiver SMB sur le client QUIC via la stratégie de groupe et PowerShell. Pour désactiver SMB sur QUIC via une stratégie de groupe, réglez la stratégie **Activer SMB** sur QUIC sur **Désactivé** dans les chemins spécifiés.

- configuration ordinateur *Modèles d'administration\Network\Station de travail Lanman*
- configuration ordinateur *Modèles d'administration\Network\Lanman Server*

Pour désactiver SMB sur QUIC à l'aide de PowerShell, exécutez cette commande dans une invite PowerShell avec élévation de privilèges :

PowerShell

```
Set-SmbClientConfiguration -EnableSMBQUIC $false
```

Audit de la signature et du chiffrement SMB

Les administrateurs peuvent activer l'audit du serveur et du client SMB pour la prise en charge de la signature et du chiffrement SMB. Si un client ou un serveur non-Microsoft ne prend pas en charge le chiffrement ou la signature SMB, il peut être détecté. Lorsqu'un appareil ou un

logiciel non-Microsoft indique qu'il prend en charge SMB 3.1.1, mais ne prend pas en charge la signature SMB, il enfreint l'exigence du protocole d'intégrité de pré-authentification SMB 3.1.1.

Vous pouvez configurer les paramètres d'audit de signature et de chiffrement SMB à l'aide de la stratégie de groupe ou de PowerShell. Ces stratégies peuvent être modifiées dans les emplacements correspondants des stratégies de groupe.

- *Configuration de l'ordinateur\Modèles d'administration\Réseau\Serveur Lanman\Le client d'audit ne prend pas en charge le chiffrement*
- *Configuration de l'ordinateur\Modèles d'administration\Réseau\Serveur Lanman\Le client d'audit ne prend pas en charge la signature*
- *Configuration de l'ordinateur\Modèles d'administration\Réseau\Station de travail Lanman\Le serveur d'audit ne prend pas en charge le chiffrement*
- *Configuration de l'ordinateur\Modèles d'administration\Réseau\Station de travail Lanman\Le serveur d'audit ne prend pas en charge la signature*

Pour effectuer ces modifications à l'aide de PowerShell, exécutez ces commandes dans une invite avec élévation de privilèges où `$true` active et `$false` désactive ces paramètres :

PowerShell

```
Set-SmbServerConfiguration -AuditClientDoesNotSupportEncryption $true
Set-SmbServerConfiguration -AuditClientDoesNotSupportSigning $true

Set-SmbClientConfiguration -AuditServerDoesNotSupportEncryption $true
Set-SmbClientConfiguration -AuditServerDoesNotSupportSigning $true
```

Les journaux d'événements associés à ces modifications se trouvent dans les emplacements indiqués dans l'Observateur d'événements, avec leurs ID spécifiques.

Agrandir le tableau

Chemin	ID de l'événement
Journal des applications et des services\Microsoft\Windows\SMBClient\Audit	31998 31999
Journaux des applications et des services\Microsoft\Windows\SMBServer\Audit	3021 3022

Audit de SMB sur QUIC

L'audit de la connexion client SMB sur QUIC capture des événements qui sont écrits dans un journal d'événements pour inclure le transport QUIC dans l'observateur d'événements. Ces

journaux d'événements sont stockés dans les chemins d'accès suivants avec leur ID d'événement spécifique.

Agrandir le tableau

Chemin	ID de l'événement
Journaux des applications et des services\Microsoft\Windows\SMBClient\Connectivité	30832
Journaux des applications et des services\Microsoft\Windows\SMBServer\Connectivité	1913

Contrôle d'accès du client SMB via QUIC

Windows Server 2025 inclut le contrôle d'accès client pour SMB sur QUIC. SMB sur QUIC est une alternative à TCP et RDMA qui fournit une connectivité sécurisée aux serveurs de fichiers edge sur des réseaux non approuvés. Le contrôle d'accès client introduit davantage de contrôles pour restreindre l'accès à vos données à l'aide de certificats. Pour en savoir plus, veuillez consulter la section Fonctionnement du contrôle d'accès client.

Ports alternatifs SMB

Vous pouvez utiliser le client SMB pour vous connecter à d'autres ports TCP, QUIC et RDMA au lieu de leurs valeurs par défaut IANA/IETF de 445, 5445 et 443. Vous pouvez configurer d'autres ports via une stratégie de groupe ou PowerShell. Auparavant, le serveur SMB dans Windows a mandaté les connexions entrantes pour utiliser le port IANA inscrit TCP/445 alors que le client TCP SMB n'a autorisé que les connexions sortantes vers ce même port TCP. À présent, SMB sur QUIC permet d'utiliser d'autres ports SMB là où les ports UDP/443 mandatés par QUIC sont disponibles pour le serveur et les appareils clients. Pour en savoir plus, veuillez consulter la section Configurer des ports SMB alternatifs.

Renforcement de la règle de pare-feu SMB

Auparavant, lorsqu'un partage a été créé, les règles de pare-feu SMB ont été configurées automatiquement pour activer le groupe **partage de fichiers et d'imprimantes** pour les profils de pare-feu appropriés. Maintenant, la création d'un partage SMB dans Windows entraîne la configuration automatique du nouveau groupe de partage de fichiers et d'imprimantes (restrictif) , qui n'autorise plus les ports NetBIOS entrants 137-139. Pour en savoir plus, veuillez consulter la section Règles de pare-feu mises à jour.

Chiffrement SMB

Faire respecter le chiffrement SMB est activé pour toutes les connexions clientes SMB sortantes. Grâce à cette mise à jour, les administrateurs peuvent définir un mandat que tous les serveurs de destination prennent en charge SMB 3.x et le chiffrement. Si un serveur ne dispose pas de ces fonctionnalités, le client ne peut pas établir de connexion.

Limiteur de débit d'authentification SMB

Le limiteur de taux d'authentification SMB limite le nombre de tentatives d'authentification dans un certain délai. Le limiteur de taux d'authentification SMB permet de combattre les attaques d'authentification par force brute. Le service du serveur SMB utilise le limiteur de débit d'authentification pour implémenter un délai entre chaque tentative d'authentification basée sur NTLM ou PKU2U ayant échoué. Le service est activé par défaut. Pour en savoir plus, consultez le fonctionnement du limiteur de débit d'authentification SMB.

Désactiver SMB NTLM

À compter de Windows Server 2025, le client SMB prend en charge le blocage NTLM pour les connexions sortantes distantes. Auparavant, le mécanisme de négociation GSSAPI simple et protégé (SPNEGO) a négocié Kerberos, NTLM et d'autres mécanismes avec le serveur de destination pour déterminer un package de sécurité pris en charge. Pour en savoir plus, consultez Bloquer les connexions NTLM sur SMB.

Contrôle de dialecte SMB

Vous pouvez maintenant gérer les dialectes SMB dans Windows. Lorsqu'il est configuré, le serveur SMB détermine les dialectes SMB 2 et SMB 3 qu'il négocie par rapport au comportement précédent et correspond uniquement au dialecte le plus élevé.

Signature SMB

La signature SMB est désormais requise par défaut pour toutes les connexions sortantes SMB. Auparavant, il n'était nécessaire que lorsque vous vous connectiez à des partages nommés **SYSVOL** et **NETLOGON** sur des contrôleurs de domaine Active Directory. Pour en savoir plus, veuillez consulter la section Fonctionnement de la signature.

Boîte aux lettres distante

Le protocole Remote Mailslot est désactivé par défaut pour SMB et pour le protocole DC Locator à utiliser avec Active Directory. Remote Mailslot pourrait être supprimé dans une

version ultérieure. Pour plus d'informations, consultez Fonctionnalités supprimées ou non développées dans Windows Server.

Renforcement du routage et des services d'accès à distance

Par défaut, les nouvelles installations de services de routage et d'accès à distance (RRAS) n'acceptent pas les connexions VPN basées sur PPTP et L2TP. Vous pouvez toujours activer ces protocoles, si nécessaire. Les connexions VPN basées sur SSTP et IKEv2 sont toujours acceptées sans aucune modification.

Les configurations existantes conservent leur comportement. Par exemple, si vous exécutez Windows Server 2019 et acceptez les connexions PPTP et L2TP, et que vous effectuez une mise à niveau vers Windows Server 2025 à l'aide d'une mise à niveau sur place, les connexions basées sur L2TP et PPTP sont toujours acceptées. Cette modification n'affecte pas les systèmes d'exploitation clients Windows. Pour en savoir plus sur la façon de réactiver PPTP et L2TP, consultez Configurer des protocoles VPN.

Modification du protocole de clé par défaut IPsec

Les modules de clé par défaut ont été modifiés en IKEv1 et IKEv2 pour les connexions IPsec authentifiées avec des certificats d'ordinateur. Pour les autres méthodes d'authentification, les protocoles AuthIP et IKEv1 par défaut restent. Cela s'applique aux clients Windows Server 2025 et Windows 11 24H2. Dans le chemin du Registre `HKLM:\SYSTEM\CurrentControlSet\Services\MpsSvc\Parameters`, l'entrée `IpsecRestoreLegacyKeyMod` avec une valeur de **0** utilise la nouvelle séquence, IKEv2 et IKEv1. Une valeur de **1** utilise la séquence précédente, AuthIP et IKEv1. Pour revenir au comportement précédent, ajoutez la clé de Registre suivante sur les systèmes utilisant la nouvelle séquence de protocoles de chiffrement par défaut. Un redémarrage est nécessaire pour que les modifications prennent effet.

PowerShell

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\MpsSvc\Parameters"
-Name "IpsecRestoreLegacyKeyMod" -PropertyType "DWORD" -Value 1
```

Hyper-V, IA et performances

Les sections suivantes décrivent Hyper-V, l'IA et les performances.

Mise en réseau accélérée (aperçu)

La mise en réseau accélérée (AccelNet) simplifie la gestion de la virtualisation d'E/S racine unique (SR-IOV) pour les machines virtuelles hébergées sur des clusters Windows Server 2025. Cette fonctionnalité utilise le chemin de données haute performance SR-IOV pour réduire la latence, l'instabilité et l'utilisation du processeur. AccelNet inclut également une couche de gestion qui gère la vérification des prérequis, la configuration de l'hôte et les paramètres de performances des machines virtuelles. Pour plus d'informations, consultez Réseau accéléré (version préliminaire).

Compatibilité du processeur dynamique

Le mode de compatibilité du processeur dynamique est mis à jour pour tirer parti des nouvelles fonctionnalités du processeur dans un environnement cluster. La compatibilité du processeur dynamique utilise le nombre maximal de fonctionnalités de processeur disponibles sur tous les serveurs d'un cluster. Le mode améliore les performances par rapport à la version précédente de la compatibilité du processeur.

Vous pouvez également utiliser la compatibilité dynamique du processeur pour enregistrer son état entre les hôtes de virtualisation qui utilisent différentes générations de processeurs. Le mode de compatibilité du processeur fournit désormais des fonctionnalités dynamiques améliorées sur les processeurs capables de traduction d'adresses de deuxième niveau. Pour en savoir plus sur le mode de compatibilité mis à jour, consultez compatibilité du processeur pour Hyper-V machines virtuelles.

Gestionnaire Hyper-V

Lors de la **création d'une machine virtuelle via Hyper-V Manager**, l'option par défaut dans l'assistant est désormais **Génération 2**.

Traduction de la pagination renforcée par l'hyperviseur

La traduction de pagination contrôlée par l'hyperviseur (HVPT) est une amélioration de la sécurité pour garantir l'intégrité des traductions d'adresses linéaires. HVPT protège les données système critiques contre les attaques de type write-what-where, où l'attaquant écrit une valeur arbitraire à un emplacement arbitraire, souvent à la suite d'un dépassement de mémoire tampon. HVPT protège les tables de pages qui configurent les structures de données système critiques. HVPT inclut tout ce qui est déjà sécurisé avec l'intégrité du code protégé par l'hyperviseur (HVCI). HVPT est activé par défaut, où la prise en charge matérielle est disponible. HVPT n'est pas activé lorsque Windows Server s'exécute en tant qu'invité dans une machine virtuelle.

Partitionnement GPU

Vous pouvez partager un appareil GPU physique avec plusieurs machines virtuelles à l'aide du partitionnement GPU. Au lieu d'allouer l'intégralité du GPU à une seule machine virtuelle, le partitionnement GPU (GPU-P) affecte des fractions dédiées du GPU à chaque machine virtuelle. Avec Hyper-V GPU-P haute disponibilité, une machine virtuelle GPU-P est automatiquement activée sur un autre nœud de cluster en cas de temps d'arrêt non planifié.

La migration dynamique GPU-P offre une solution pour déplacer une machine virtuelle (pour un temps d'arrêt planifié ou un équilibrage de charge) avec GPU-P vers un autre nœud, qu'elle soit autonome ou en cluster. Pour en savoir plus sur le partitionnement GPU, consultez le partitionnement GPU.

Réseau ATC

Network ATC simplifie le déploiement et la gestion des configurations réseau pour les clusters Windows Server 2025. Network ATC utilise une approche basée sur les objectifs, où les utilisateurs spécifient leurs objectifs souhaités, tels que la gestion, le calcul ou le stockage pour un adaptateur réseau. Le déploiement est automatisé en fonction de la configuration prévue.

Cette approche réduit le temps, la complexité et les erreurs associées au déploiement de mise en réseau hôte. Elle garantit la cohérence de la configuration sur le cluster et élimine également la dérive de configuration. Pour plus d'informations, consultez Déployer la mise en réseau de l'hôte avec Network ATC.

Extensibilité

Avec Windows Server 2025, Hyper-V prend désormais en charge jusqu'à 4 pétaoctets de mémoire et 2 048 processeurs logiques par hôte. Cette augmentation permet une plus grande scalabilité et des performances pour les charges de travail virtualisées.

Windows Server 2025 prend également en charge jusqu'à 240 To de mémoire et 2 048 processeurs virtuels pour les machines virtuelles de génération 2, ce qui offre une flexibilité accrue pour l'exécution de charges de travail volumineuses. Pour plus d'informations, consultez Planifier l'extensibilité Hyper-V dans Windows Server.

Clusters de groupe de travail

Les clusters de groupe de travail Hyper-V représentent une catégorie particulière de clusters de basculement Windows Server, dans lesquels les nœuds Hyper-V ne sont pas affiliés à un

domaine Active Directory, mais permettent la migration en direct des machines virtuelles au sein du cluster.

Stockage

Les sections suivantes décrivent les mises à jour de stockage.

Prise en charge du clonage de blocs

Dev Drive prend désormais en charge le clonage de bloc à partir de Windows 11 24H2 et Windows Server 2025. Étant donné que dev Drive utilise le format ReFS (Resilient File System), la prise en charge du clonage de bloc offre des avantages significatifs en matière de performances lorsque vous copiez des fichiers. Avec le clonage de bloc, le système de fichiers peut copier une plage d'octets de fichier pour une application en tant qu'opération de métadonnées à faible coût au lieu d'effectuer des opérations de lecture et d'écriture coûteuses dans les données physiques sous-jacentes.

Le résultat est l'achèvement plus rapide de la copie de fichiers, la réduction des E/S vers le stockage sous-jacent et une capacité de stockage améliorée en permettant à plusieurs fichiers de partager les mêmes clusters logiques. Pour en savoir plus, consultez la section Clonage de blocs sur ReFS.

Lecteur de développement

Dev Drive est un volume de stockage qui vise à améliorer les performances des charges de travail cruciales des développeurs. Dev Drive utilise la technologie ReFS et intègre des optimisations spécifiques du système de fichiers pour offrir un meilleur contrôle sur les paramètres et la sécurité du volume de stockage. Les administrateurs ont désormais la possibilité de désigner l'approbation, de configurer les paramètres antivirus et d'exercer un contrôle administratif sur les filtres attachés. Pour en savoir plus, consultez la section Configurer un lecteur de développement sous Windows 11.

NVMe

NVMe est une nouvelle norme pour les lecteurs SSD rapides. Les performances de stockage NVMe sont optimisées dans Windows Server 2025. Le résultat est une amélioration des performances avec une augmentation des E/S par seconde et une diminution de l'utilisation du processeur.

Réplica de stockage

La compression de la réplication de stockage réduit la quantité de données transférées sur le réseau pendant la réplication. Pour en savoir plus sur la compression dans Storage Replica, consultez aperçu de Storage Replica.

Journal amélioré de réplica de stockage

Storage Replica Enhanced Log optimise la gestion des journaux pour réduire les coûts de performance liés aux abstractions des systèmes de fichiers. Les performances de réplication de bloc sont améliorées. Pour en savoir plus, veuillez consulter la section Journal amélioré de Storage Replica.

Déduplication et compression du stockage natif ReFS

La déduplication et la compression du stockage natif ReFS sont des techniques utilisées pour optimiser l'efficacité du stockage pour les charges de travail statiques et actives, telles que les serveurs de fichiers ou les bureaux virtuels. Pour en savoir plus sur la déduplication et la compression ReFS, consultez Optimiser le stockage avec la déduplication et la compression ReFS dans Azure Local.

Volumes à provisionnement fin

Les volumes à provisionnement léger avec Storage Spaces Direct sont un moyen d'allouer des ressources de stockage plus efficacement et d'éviter une surallocation coûteuse en allouant des ressources depuis le pool uniquement lorsqu'elles sont nécessaires au sein d'un cluster. Vous pouvez également convertir des volumes fixes en volumes à provisionnement fin. La conversion de volumes fixes en volumes à provisionnement fin renvoie tout le stockage inutilisé dans le pool pour que d'autres volumes puissent l'utiliser. Pour en savoir plus sur les volumes à provisionnement fin, consultez Provisionnement fin de stockage.

Protocole SMB

Server Message Block (SMB) est l'un des protocoles les plus couramment utilisés dans la mise en réseau. SMB offre un moyen fiable de partager des fichiers et d'autres ressources entre des appareils sur votre réseau. Windows Server 2025 inclut la prise en charge de la compression SMB pour l'algorithme de compression LZ4 standard du secteur. LZ4 vient s'ajouter à la prise en charge existante de SMB pour XPRESS (LZ77), XPRESS Huffman (LZ77+Huffman), LZNT1 et PATTERN_V1.

Azure Arc et hybride

Les sections suivantes décrivent les configurations Azure Arc et hybrides.

Configuration simplifiée d'Azure Arc

Le programme d'installation d'Azure Arc est une fonctionnalité à la demande. Elle est donc installée par défaut. Une interface d'Assistant conviviale et une icône de barre d'état système dans la barre des tâches permettent de faciliter le processus d'ajout de serveurs à Azure Arc. Azure Arc étend les fonctionnalités de la plateforme Azure afin de pouvoir créer des applications et des services qui peuvent fonctionner dans différents environnements. Ces environnements incluent les centres de données, la périphérie et les environnements multiclouds et offrent une flexibilité accrue. Pour plus d'informations, consultez Connecter des machines Windows Server à Azure via le programme d'installation d'Azure Arc.

Licence pay-as-you-go

L'option de licence d'abonnement avec paiement à l'utilisation Azure Arc est une alternative aux licences perpétuelles conventionnelles pour Windows Server 2025. Avec l'option de paiement à l'utilisation, vous pouvez déployer un appareil Windows Server, le licencer et payer uniquement autant que vous l'utilisez. Cette fonctionnalité est facilitée via Azure Arc et facturée via votre abonnement Azure. Pour plus d'informations, consultez les licences de paiement à l'utilisation d'Azure Arc.

Gestion de Windows Server activée par Azure Arc

Windows Server Management activé par Azure Arc offre de nouveaux avantages aux clients disposant de licences Windows Server qui ont des licences Software Assurance ou Windows Server actives qui sont des licences d'abonnement actives. Windows Server 2025 présente les principaux avantages suivants :

- **Windows Admin Center dans Azure Arc**: intègre Azure Arc à Windows Admin Center afin de pouvoir gérer vos instances Windows Server à partir du portail Azure Arc. Cette intégration offre une expérience de gestion unifiée pour vos instances Windows Server, qu'elles s'exécutent localement, dans le cloud ou en périphérie.
- **support à distance**: offre aux clients bénéficiant d'un support professionnel la possibilité d'accorder un accès en temps opportun avec des transcriptions d'exécution détaillées et des droits de révocation.
- **Best Practices Assessment**: la collecte et l'analyse des données du serveur génèrent des problèmes et des conseils de correction et des améliorations des performances.
- **configuration Azure Site Recovery**: la configuration d'Azure Site Recovery garantit la continuité de l'activité et assure la réplication et la résilience des données pour les charges de travail critiques.

Pour en savoir plus sur windows Server Management activé par Azure Arc et les avantages disponibles, consultez Gestion de Windows Server activée par Azure Arc.

Software-Defined Mise en réseau

Software-Defined Networking (SDN) est une approche de mise en réseau que les administrateurs réseau peuvent utiliser pour gérer les services réseau via l'abstraction des fonctionnalités de bas niveau. SDN permet la séparation du plan de contrôle réseau, qui gère le réseau, du plan de données, qui gère le trafic. Cette séparation permet une flexibilité et une programmabilité accrues dans la gestion du réseau. SDN offre les avantages suivants dans Windows Server 2025 :

- **Contrôleur de réseau** : Ce plan de contrôle pour le SDN est désormais hébergé directement en tant que services de cluster de basculement sur les machines hôtes physiques. L'utilisation d'un rôle de cluster élimine la nécessité de déployer des machines virtuelles, ce qui simplifie le déploiement et la gestion et conserve les ressources.
- **segmentation basée sur des balises**: les administrateurs peuvent utiliser des balises de service personnalisées pour associer des groupes de sécurité réseau (NSG) et des machines virtuelles pour le contrôle d'accès. Au lieu de spécifier des plages d'adresses IP, les administrateurs peuvent désormais utiliser des étiquettes simples et explicites pour baliser des machines virtuelles de charge de travail et appliquer des stratégies de sécurité basées sur ces balises. Les balises simplifient le processus de gestion de la sécurité réseau et éliminent la nécessité de mémoriser et de retyper des plages d'adresses IP. Pour plus d'informations, consultez Configurer des groupes de sécurité réseau avec des balises dans Windows Admin Center.
- **stratégies réseau par défaut dans Windows Server 2025**: ces stratégies apportent des options de protection de type Azure aux groupes de sécurité réseau pour les charges de travail déployées via Windows Admin Center. La stratégie par défaut refuse tout accès entrant, ce qui autorise l'ouverture sélective de ports entrants connus tout en autorisant l'accès sortant complet à partir de machines virtuelles de charge de travail. Les stratégies réseau par défaut garantissent que les machines virtuelles de charge de travail sont sécurisées à partir du point de création. Pour plus d'informations, consultez Utiliser les stratégies d'accès réseau par défaut sur les machines virtuelles sur Azure Local.
- **SDN Multisite**: cette fonctionnalité fournit une connectivité native de couche 2 et 3 entre les applications entre deux emplacements sans composants supplémentaires. Avec SDN Multisite, les applications peuvent se déplacer en toute transparence sans avoir à reconfigurer l'application ou les réseaux. Il offre également une gestion unifiée des stratégies réseau pour les charges de travail afin que vous n'ayez pas besoin de mettre à jour les stratégies lorsqu'une machine virtuelle de charge de travail passe d'un emplacement à un autre. Pour en savoir plus, consultez Qu'est-ce que SDN Multisite ?.

- **performances améliorées des passerelles SDN couche 3**: les passerelles de couche 3 obtiennent un débit plus élevé et des cycles de processeur réduits. Ces améliorations sont activées par défaut. Les utilisateurs rencontrent automatiquement de meilleures performances lorsqu'une connexion de passerelle SDN 3 est configurée via PowerShell ou Windows Admin Center.

Portabilité des conteneurs Windows

La portabilité constitue un aspect crucial de la gestion des conteneurs et permet de simplifier les mises à niveau en améliorant la flexibilité et la compatibilité des conteneurs dans Windows.

La portabilité est une fonctionnalité Windows Server que les utilisateurs peuvent utiliser pour déplacer des images conteneur et leurs données associées, entre différents hôtes ou environnements sans nécessiter de modifications. Les utilisateurs peuvent créer une image conteneur sur un hôte, puis la déployer sur un autre hôte sans se soucier des problèmes de compatibilité. Pour en savoir plus, consultez Portabilité pour les conteneurs.

Programme Windows Server Insider

Le programme Windows Server Insider fournit un accès anticipé aux dernières versions du système d'exploitation Windows pour une communauté de passionnés. En tant que membre, vous êtes parmi les premiers à essayer de nouvelles idées et concepts que Microsoft développe. Après vous être inscrit en tant que membre, vous pouvez participer à différents canaux de distribution. Accédez à **Démarrer**>**Paramètres**>**Mise à jour de Windows**>**Programme Windows Insider**.

Contenu connexe

discussions de la communauté Windows Server Insider

Last updated on 15/01/2026

Nouveautés de Windows Server 2022

28/07/2025S'applique à: ✅ Windows Server 2022

Cet article décrit certaines des nouvelles fonctionnalités de Windows Server 2022. Windows Server 2022 repose sur la base solide de Windows Server 2019 et apporte de nombreuses innovations sur trois thèmes clés : la sécurité, l'intégration et la gestion hybrides Azure et la plateforme d'applications.

Édition Azure

Windows Server 2022 Datacenter : Azure Edition vous aide à utiliser les avantages du cloud pour maintenir vos machines virtuelles à jour tout en réduisant les temps d'arrêt. Cette section décrit certaines des nouvelles fonctionnalités de Windows Server 2022 Datacenter: Azure Edition. En savoir plus sur la façon dont Azure Automanage pour Windows Server intègre ces nouvelles fonctionnalités à Windows Server Azure Edition dans l'article Azure Automanage pour les services Windows Server.

Windows Server 2022 Datacenter : Azure Edition s'appuie sur Datacenter Edition pour fournir un système d'exploitation de machine virtuelle uniquement qui permet d'utiliser les avantages du cloud, avec des fonctionnalités avancées telles que SMB sur QUIC, Hotpatch et La mise en réseau étendue Azure. Cette section décrit certaines de ces nouvelles fonctionnalités.

Comparez les différentes éditions de Windows Server 2022. Vous pouvez également en savoir plus sur la façon dont Azure Automanage pour Windows Server intègre ces nouvelles fonctionnalités à Windows Server Azure Edition dans l'article Azure Automanage pour les services Windows Server.

Avril 2023

Hotpatch

Windows Server 2022 Datacenter : Azure Edition Hotpatch est désormais disponible en préversion publique pour l'expérience de bureau dans Azure et en tant que machine virtuelle invitée prise en charge sur Azure Local version 22H2.

Septembre 2022

Cette section répertorie les fonctionnalités et améliorations qui sont désormais disponibles dans Windows Server Datacenter: Azure Edition à compter de la mise à jour cumulative 2022-09 pour le système d'exploitation serveur Microsoft version 21H2 pour les systèmes x64

(KB5017381). Une fois la mise à jour cumulative installée, le numéro de build du système d'exploitation sera 20348.1070 ou une version ultérieure.

Compression du réplica de stockage pour le transfert de données

Cette mise à jour inclut la compression de Storage Replica pour les données transférées entre les serveurs source et destination. Cette nouvelle fonctionnalité compresse les données de réplication à partir du système source, qui sont envoyées sur le réseau, décompressées et enregistrées sur la destination. La compression entraîne moins de paquets réseau pour transférer la même quantité de données, ce qui permet d'obtenir plus de débit et moins d'utilisation du réseau. Un débit de données plus élevé doit également entraîner une réduction du temps de synchronisation lorsque vous en avez besoin, par exemple dans un scénario de récupération d'urgence.

De nouveaux paramètres PowerShell de réplica de stockage sont disponibles pour les commandes existantes. Pour en savoir plus, consultez la référence PowerShell StorageReplica . Pour plus d'informations sur Storage Replica, consultez la Vue d'ensemble de Storage Replica.

Prise en charge d'Azure Local

Avec cette version, vous pouvez exécuter Windows Server 2022 Datacenter : Azure Edition en tant que machine virtuelle invitée prise en charge sur Azure Local, version 22H2. Avec Azure Edition s'exécutant sur Azure Local, vous serez en mesure d'utiliser toutes les fonctionnalités existantes, notamment Hotpatch pour Server Core et SMB sur QUIC à vos emplacements de centre de données et de périphérie.

Commencez à déployer Windows Server 2022 Datacenter : Édition Azure à l'aide du déploiement à partir de l'Azure Marketplace sur Azure Local (aperçu) ou à l'aide d'un fichier ISO. Vous pouvez télécharger l'ISO ici :

- ISO Windows Server 2022 Datacenter: Azure Edition (EN-US)
- ISO Windows Server 2022 Datacenter: Azure Edition (ZH-CN)

Votre abonnement Azure vous permet d'utiliser Windows Server Datacenter : Azure Edition sur toutes les instances de machine virtuelle s'exécutant sur Azure Local. Pour plus d'informations, consultez les conditions de votre produit .

En savoir plus sur les dernières fonctionnalités locales d'Azure dans Les nouveautés d'Azure Local version 22H2.

Déploiement à partir d'Azure Marketplace sur Azure Local compatible avec Arc (prévisualisation)

Les images Windows Server 2022 Datacenter: Azure Edition sont disponibles dans la Place de marché Azure pour Azure Local avec Arc, ce qui facilite l'essai, l'achat et le déploiement à l'aide d'images certifiées Azure.

Apprenez-en davantage sur l'intégration de la Place de marché Azure pour les fonctionnalités locales Azure Arc dans l'article Nouveautés d'Azure Local .

Azure Edition (version initiale)

Cette section répertorie les fonctionnalités et améliorations disponibles dans Windows Server Datacenter: Azure Edition avec la version de septembre 2021.

Azure Automanage – Hotpatch

Hotpatch, qui fait partie d'Azure Automanage, est une nouvelle façon d'installer des mises à jour sur de nouvelles machines virtuelles Windows Server Azure Edition qui ne nécessitent pas de redémarrage après l'installation. Pour plus d'informations, consultez Hotpatch pour Windows Server.

SMB sur QUIC

SMB sur QUIC met à jour le protocole SMB 3.1.1 pour utiliser le protocole QUIC au lieu de TCP dans Windows Server 2022 Datacenter : Azure Edition, Windows 11 et versions ultérieures et les clients tiers s'ils le prennent en charge. Lorsqu'ils utilisent SMB sur QUIC avec TLS 1.3, les utilisateurs et les applications disposent d'un accès sécurisé et fiable aux données des serveurs de fichiers Edge exécutés dans Azure. Les utilisateurs mobiles et les télétravailleurs n'ont plus besoin d'un VPN pour accéder à leurs serveurs de fichiers via SMB sous Windows. Pour plus d'informations, consultez SMB sur QUIC et SMB sur la gestion de QUIC avec les meilleures pratiques de gestion des machines Automanage.

Pour en savoir plus sur QUIC, consultez RFC 9000 .

Réseau étendu pour Azure

Le réseau étendu Azure vous permet d'étendre un sous-réseau local dans Azure pour permettre aux machines virtuelles locales de conserver leurs adresses IP privées locales d'origine lorsque vous migrez vers Azure. Pour en savoir plus, consultez Réseau étendu Azure.

Toutes les éditions

Cette section décrit certaines des nouvelles fonctionnalités de Windows Server 2022 dans toutes les éditions. Pour en savoir plus sur les différentes éditions, consultez Comparaison des éditions de Windows Server.

Sécurité

Les nouvelles fonctionnalités de sécurité de Windows Server 2022 combinent d'autres fonctionnalités de sécurité de Windows Server dans différents domaines afin de fournir une défense en profondeur contre les menaces avancées. La sécurité multicouche avancée de Windows Server 2022 offre la protection complète dont les serveurs ont actuellement besoin.

Serveur à cœur sécurisé

Un matériel de serveur à noyau sécurisé certifié provenant d'un partenaire OEM fournit des protections de sécurité supplémentaires qui sont utiles contre les attaques sophistiquées. Le matériel serveur sécurisé certifié peut fournir une assurance accrue lors de la gestion des données stratégiques dans certaines des industries les plus sensibles aux données. Un serveur à noyau sécurisé utilise des fonctions de matériel, de microprogramme et de pilote pour activer les fonctionnalités avancées de sécurité Windows Server. La plupart de ces fonctionnalités sont disponibles dans les PC à noyau sécurisé Windows et sont désormais également disponibles avec le matériel de serveur à noyau sécurisé et Windows Server 2022. Pour plus d'informations, consultez Serveur principal sécurisé.

Racine de confiance matérielle

Utilisées par des fonctionnalités comme le chiffrement de lecteur BitLocker, les puces de processeur de chiffrement sécurisé du module de plateforme sécurisée 2.0 (TPM 2.0) fournissent un magasin matériel sécurisé pour les clés de chiffrement et les données sensibles, y compris des mesures de l'intégrité des systèmes. TPM 2.0 peut vérifier que le serveur commence par du code légitime et est approuvé par l'exécution de code suivante, appelée racine de confiance matérielle.

Protection des microprogrammes

Les microprogrammes s'exécutent avec des privilèges élevés et sont souvent invisibles pour les solutions antivirus traditionnelles. Cela a entraîné une augmentation du nombre d'attaques basées sur le microprogramme. Les serveurs à cœurs sécurisés mesurent et vérifient les processus de démarrage avec la Technologie DRTM (Dynamic Root of Trust for Measurement). Les serveurs de cœur sécurisé peuvent également isoler l'accès des pilotes à la mémoire grâce à la protection d'accès direct à la mémoire (DMA).

Démarrage sécurisé UEFI

Le démarrage sécurisé UEFI est une norme de sécurité qui protège vos serveurs contre les rootkits malveillants. Le démarrage sécurisé garantit que le serveur démarre uniquement le microprogramme et les logiciels approuvés par le fabricant du matériel. Lorsque le serveur est démarré, le microprogramme vérifie la signature de chaque composant de démarrage, y compris les pilotes de microprogramme et le système d'exploitation. Si les signatures sont valides, le serveur démarre et le microprogramme donne le contrôle au système d'exploitation.

Sécurité basée sur la virtualisation (VBS)

Les serveurs à noyau sécurisé prennent en charge la sécurité basée sur la virtualisation (VBS) et l'intégrité du code appliquée par l'hyperviseur (HVCI). VBS utilise des fonctionnalités de virtualisation matérielle pour créer et isoler une région sécurisée de mémoire du système d'exploitation normal, en assurant une protection contre toute une classe de vulnérabilités utilisée dans les attaques d'exploration de la cryptomonnaie. VBS permet également l'utilisation de Credential Guard, où les informations d'identification de l'utilisateur et les secrets sont stockés dans un conteneur virtuel auquel le système d'exploitation ne peut pas accéder directement.

HVCI utilise VBS pour renforcer considérablement l'application de la stratégie d'intégrité du code. L'intégrité du mode noyau empêche le chargement de pilotes ou de fichiers système en mode noyau non signés dans la mémoire système.

La protection des données du noyau (KDP, kernel data protection) fournit une protection en lecture seule de la mémoire du noyau contenant des données non exécutables où les pages mémoire sont protégées par l'hyperviseur. KDP protège les structures clés au sein de l'environnement d'exécution de Windows Defender System Guard contre l'altération.

Connectivité sécurisée

Transport : HTTPS et TLS 1.3 activés par défaut sur Windows Server 2022

Les connexions sécurisées sont au cœur des systèmes interconnectés d'aujourd'hui. Transport Layer Security (TLS) 1.3 est la dernière version du protocole de sécurité le plus déployé sur Internet, qui chiffre les données pour fournir un canal de communication sécurisé entre deux points de terminaison. HTTPS et TLS 1.3 sont désormais activés par défaut sur Windows Server 2022, protégeant ainsi les données des clients qui se connectent au serveur. Ils éliminent les algorithmes de chiffrement obsolètes, améliorent la sécurité par rapport aux anciennes

versions, et visent à chiffrer la plus grande partie possible de la négociation. Découvrez-en plus sur les versions prises en charge de TLS ainsi que sur les suites de chiffrement prises en charge.

Même si TLS 1.3 dans la couche de protocole est maintenant activé par défaut, les applications et services doivent également le prendre en charge activement. Le blog sur la Sécurité Microsoft est plus détaillé dans le billet Taking Transport Layer Security (TLS) to the next level with TLS 1.3 .

DNS sécurisé : demandes de résolution de noms DNS chiffrées avec DNS-over-HTTPS

Le client DNS dans Windows Server 2022 prend désormais en charge DNS-over-HTTPS (DoH), qui chiffre les requêtes DNS à l'aide du protocole HTTPS. DoH permet de garder votre trafic aussi privé que possible en empêchant l'écoute et vos données DNS d'être manipulées. Pour plus d'informations, consultez Configurer le client DNS pour utiliser DoH.

Server Message Block (SMB) : chiffrement SMB AES-256 pour les plus soucieux de la sécurité

Windows Server prend désormais en charge les suites de chiffrement AES-256-GCM et AES-256-CCM pour le chiffrement SMB. Windows négocie automatiquement une méthode de chiffrement plus avancée lors de la connexion à un autre ordinateur qui le prend également en charge, et peut également être mandatée par le biais de la stratégie de groupe. Windows Server prend toujours en charge AES-128 pour la compatibilité descendante. La signature AES-128-GMAC accélère désormais aussi les performances de signature.

SMB : contrôles de chiffrement SMB est-ouest pour les communications de cluster internes

Les clusters de basculement Windows Server prennent désormais en charge le contrôle précis du chiffrement et de la signature des communications de stockage intra-nœud pour les volumes partagés de cluster (CSV) et la couche de bus de stockage (SBL). Lors de l'utilisation des espaces de stockage direct, vous pouvez maintenant décider de chiffrer ou de signer les communications est-ouest au sein du cluster lui-même pour une sécurité accrue.

Chiffrement SMB Direct et RDMA

SMB Direct et RDMA fournissent une bande passante élevée, une infrastructure réseau à faible latence pour les charges de travail telles que Storage Spaces Direct, Storage Replica, Hyper-V, Serveur de fichiers Scale-Out et SQL Server. SMB Direct dans Windows Server 2022 prend en charge le chiffrement. Auparavant, l'activation du chiffrement SMB a désactivé le placement

direct des données. C'était intentionnel, mais il a sérieusement affecté les performances. Désormais, les données sont chiffrées avant leur placement, ce qui entraîne une dégradation bien moins importante des performances, tout en ajoutant la confidentialité des paquets protégés par AES-128 et AES-256.

Pour plus d'informations sur le chiffrement SMB, l'accélération de signature, la prise en charge sécurisée de RDMA et du cluster, consultez améliorations de la sécurité SMB.

Fonctionnalités hybrides Azure

Vous pouvez augmenter votre efficacité et votre agilité avec des fonctionnalités hybrides intégrées dans Windows Server 2022 qui vous permettent d'étendre vos centres de données à Azure plus facilement que jamais.

Serveurs Windows habilités par Azure Arc

Les serveurs avec Azure Arc avec Windows Server 2022 apportent des serveurs Windows locaux et multiclouds à Azure avec Azure Arc. Cette expérience de gestion est conçue pour être cohérente avec la façon dont vous gérez des machines virtuelles Azure natives. Quand une machine hybride est connectée à Azure, elle devient une machine connectée et est traitée comme une ressource dans Azure. Vous trouverez plus d'informations dans la documentation sur les serveurs avec Azure Arc.

Ajouter des machines Windows Server

À partir de la mise à jour KB5031364 , vous pouvez ajouter des machines Windows Server avec un processus facile.

Pour ajouter de nouvelles machines Windows Server, accédez à l'icône Azure Arc dans le coin inférieur droit de la barre des tâches et lancez le programme d'installation d'Azure Arc pour installer et configurer un agent De machine connectée Azure. Une fois l'installation terminée, vous pouvez utiliser Azure Connected Machine Agent sans frais supplémentaires pour votre compte Azure. Après avoir activé Azure Arc sur votre serveur, vous pouvez voir les informations d'état dans l'icône de barre des tâches.

Pour plus d'informations, consultez Connecter des machines Windows Server à Azure via le programme d'installation d'Azure Arc.

Windows Admin Center (Centre d'administration Windows)

Les améliorations apportées à Windows Admin Center pour gérer Windows Server 2022 incluent des fonctionnalités permettant de signaler l'état actuel des fonctionnalités principales sécurisées mentionnées et, le cas échéant, pour vous permettre d'activer les fonctionnalités. Pour plus d'informations sur ces améliorations et bien d'autres améliorations apportées à Windows Admin Center, consultez la documentation de Windows Admin Center.

Plateforme d'application

Il existe plusieurs améliorations de plateforme pour les conteneurs Windows, notamment la compatibilité des applications et l'expérience de conteneur Windows avec Kubernetes.

Voici certaines des nouvelles fonctionnalités :

- Réduction de la taille de l'image conteneur Windows de jusqu'à 40 %, ce qui permet un démarrage 30 % plus rapide et offre de meilleures performances.
- Les applications peuvent désormais utiliser l'ID Microsoft Entra avec le compte de service administré de groupe (gMSA) sans joindre le domaine à l'hôte de conteneur. Les conteneurs Windows prennent désormais également en charge Microsoft Distributed Transaction Coordinator (DTC) et Microsoft Message Queuing (MSMQ).
- Des bus simples peuvent désormais être affectés à conteneurs Windows Server isolés des processus. Les applications s'exécutant dans des conteneurs qui doivent communiquer via SPI, I2C, GPIO et UART/COM sont désormais en mesure de le faire.
- Nous avons activé la prise en charge de l'accélération matérielle des API DirectX dans les conteneurs Windows pour prendre en charge des scénarios tels que l'inférence machine learning à l'aide du matériel d'unité de traitement graphique (GPU) locale. Pour plus d'informations, consultez le billet de blog Intégration de l'accélération GPU dans les conteneurs Windows.
- Il existe plusieurs autres améliorations qui simplifient l'expérience de conteneur Windows avec Kubernetes. Parmi ces améliorations figurent la prise en charge des conteneurs hôte-processus pour la configuration des nœuds, IPv6, et l'implémentation cohérente de la stratégie réseau avec Calico.
- Windows Admin Center est mis à jour pour faciliter la conteneurisation des applications .NET. Une fois que l'application se trouve dans un conteneur, vous pouvez l'héberger sur Azure Container Registry pour la déployer sur d'autres services Azure, y compris Azure Kubernetes Service.
- Grâce à la prise en charge des processeurs Intel Ice Lake, Windows Server 2022 prend en charge les applications critiques et à grande échelle qui nécessitent jusqu'à 48 To de

mémoire et 2 048 cœurs logiques exécutés sur 64 sockets physiques. L'informatique confidentielle avec Intel Secured Guard Extension (SGX) sur Intel Ice Lake améliore la sécurité des applications en les isolant les unes des autres avec une mémoire protégée.

Autres fonctionnalités clés

Virtualisation IP des services Bureau à distance

À partir de la mise à jour KB5030216 , vous pouvez utiliser la virtualisation IP bureau à distance.

La virtualisation IP des services Bureau à distance simule un bureau à utilisateur unique en prenant en charge la virtualisation IP des services Bureau à distance par session et par programme pour les applications Winsock. Pour plus d'informations, consultez Virtualisation IP du Bureau à distance dans Windows Server.

Planificateur de tâches et Gestionnaire Hyper-V pour les installations Server Core

Nous avons ajouté deux outils de gestion au package de fonctionnalités de compatibilité des applications à la demande dans cette version : planificateur de tâches (taskschd.msc) et Hyper-V Manager (virtmgmt.msc). Pour plus d'informations, consultez Fonctionnalité à la demande de compatibilité des applications Server Core.

Virtualisation imbriquée pour les processeurs AMD

La virtualisation imbriquée est une fonctionnalité qui vous permet d'exécuter Hyper-V à l'intérieur d'une machine virtuelle (VM) Hyper-V. Windows Server 2022 prend en charge la virtualisation imbriquée à l'aide de processeurs AMD, offrant ainsi plus de choix de matériel pour vos environnements. Pour plus d'informations, consultez la documentation sur la virtualisation imbriquée.

Navigateur Microsoft Edge

Microsoft Edge est inclus dans Windows Server 2022, en remplacement d'Internet Explorer. Il repose sur Chromium open source et s'appuie sur la sécurité et l'innovation de Microsoft. Il peut être utilisé avec les options d'installation Serveur avec Expérience utilisateur. Pour plus d'informations, consultez la documentation Microsoft Edge Enterprise. Le support de Microsoft Edge, contrairement au reste de Windows Server, suit le cycle de vie moderne. Pour plus d'informations, consultez la documentation relative au cycle de vie de Microsoft Edge.

Performances réseau

Améliorations des performances UDP

UDP devient un protocole de plus en plus courant transportant davantage de trafic réseau, grâce à la popularité croissante des protocoles RTP et des protocoles de streaming et de jeu personnalisés (UDP). Le protocole QUIC, basé sur UDP, mets les performances d'UDP au même niveau que TCP. Point important : Windows Server 2022 comprend le déchargement segmentation UDP (USO). Le déchargement segmentation UDP transfère la majeure partie du travail nécessaire pour envoyer des paquets UDP du processeur vers le matériel spécialisé de la carte réseau. La fonctionnalité UDP RSC (Receive Side Coalescing) vient en complément du déchargement segmentation UDP. Celle-ci permet de fusionner les paquets et de réduire l'utilisation du processeur pour le traitement UDP. En outre, des centaines d'améliorations ont été apportées au chemin de données UDP afin d'améliorer l'émission et la réception. Windows Server 2022 et Windows 11 disposent tous les deux de cette nouvelle fonctionnalité.

Améliorations des performances de TCP

Windows Server 2022 utilise TCP HyStart++ pour réduire la perte de paquets pendant le démarrage de la connexion (surtout dans les réseaux à haut débit), et RACK pour réduire les délais d'attente de retransmission (RTO). Ces fonctionnalités sont activées par défaut dans la pile de transport, et elles fournissent un flux de données réseau plus régulier, avec de meilleures performances à des débits élevés. Windows Server 2022 et Windows 11 disposent tous les deux de cette nouvelle fonctionnalité.

Améliorations apportées au commutateur virtuel Hyper-V

Dans Hyper-V, les commutateurs virtuels sont améliorés à l'aide d'une nouvelle fonctionnalité RSC (Receive Segment Coalescing). RSC permet au réseau de l'hyperviseur de fusionner les paquets et de les traiter comme un seul segment plus grand. Les cycles de processeur sont réduits et les segments restent coalescés sur l'ensemble du chemin de données jusqu'à ce que l'application prévue soit traitée. RSC améliore les performances du trafic réseau envoyé par un hôte externe et reçu par une carte réseau virtuelle ainsi que le trafic envoyé par une carte réseau virtuelle et reçu par une autre carte réseau virtuelle présente sur le même hôte.

Dans vSwitch, RSC peut également regrouper plusieurs segments TCP en un segment plus important avant que les données ne traversent le vSwitch. Cette modification améliore également les performances de mise en réseau pour les charges de travail virtuelles. RSC est activé par défaut sur les commutateurs virtuels externes.

Détection des anomalies de disque d’Insights système

System Insights dispose d’une autre fonctionnalité via Windows Admin Center : détection des anomalies de disque.

La détection des anomalies de disque est une nouvelle fonctionnalité qui signale quand les disques se comportent de manière *inhabituelle*. Bien que le fait d'être différent ne soit pas forcément une mauvaise chose, il peut être utile de voir ces moments anormaux lorsque vous dépannez des problèmes sur vos systèmes. Cette fonctionnalité est également disponible pour les serveurs exécutant Windows Server 2019.

Améliorations de la restauration des mises à jour Windows

Les serveurs peuvent désormais reprendre automatiquement leur activité après des échecs du démarrage en supprimant les mises à jour si ces échecs se sont manifestés après l'installation récente de mises à jour qualité de Windows ou de pilotes. Lorsqu'un appareil ne parvient pas à démarrer correctement après l'installation récente de mises à jour de pilote, Windows désinstalle automatiquement les mises à jour pour que l'appareil fonctionne normalement.

Cette fonctionnalité nécessite que le serveur utilise l’option d’installation Server Core avec une partition d’environnement de récupération Windows .

Stockage

Windows Server 2022 inclut les mises à jour de stockage suivantes. Le stockage est également concerné par les mises à jour de la détection d'anomalies des disques System Insights et de Windows Admin Center.

Service de migration de stockage

Les améliorations apportées au service de migration de stockage dans Windows Server 2022 facilitent la migration du stockage vers Windows Server ou Vers Azure à partir d’emplacements sources supplémentaires. Les fonctionnalités disponibles lors de l'exécution de l'orchestrateur du serveur de migration du stockage sur Windows Server 2022 sont les suivantes :

- Migrer des groupes et utilisateurs locaux vers le nouveau serveur
- Migrer le stockage depuis des clusters de basculement, migrer vers des clusters de basculement, et migrer entre des serveurs autonomes et des clusters de basculement.
- Migrer le stockage à partir d'un serveur Linux qui utilise Samba
- Synchroniser plus facilement des partages migrés dans Azure à l’aide d’Azure File Sync
- Migrer vers de nouveaux réseaux comme Azure

- Migrer des serveurs CIFS NetApp entre des groupes NetApp FAS et des serveurs et clusters Windows

Vitesse de réparation du stockage réglable

La vitesse de réparation de stockage réglable par l'utilisateur est une nouvelle fonctionnalité des espaces de stockage direct qui offre un meilleur contrôle sur le processus de resynchronisation des données. La vitesse de réparation du stockage ajustable vous permet d'allouer des ressources pour réparer des copies de données (résilience) ou pour exécuter des charges de travail actives (performances). Le contrôle de la vitesse de réparation contribue à améliorer la disponibilité et vous permet de gérer vos clusters d'une façon plus flexible et plus efficace.

Réparation et resynchronisation plus rapides

La réparation et la resynchronisation du stockage après des événements tels que les redémarrages de nœuds et les défaillances de disque sont maintenant deux fois plus rapides. Les réparations ont moins de variation dans le temps écoulé afin de pouvoir être plus sûr du temps nécessaire aux réparations. Cette amélioration est obtenue en ajoutant plus de granularité au suivi des données. Les réparations déplacent désormais uniquement les données qui doivent être déplacées, ce qui réduit les ressources système utilisées et le temps nécessaire pour effectuer des réparations.

Cache de bus de stockage avec espaces de stockage sur des serveurs autonomes

Le cache de bus de stockage est désormais disponible pour les serveurs autonomes. Il peut améliorer considérablement les performances de lecture et d'écriture, tout en conservant l'efficacité du stockage et en conservant les coûts opérationnels faibles. À l'instar de son implémentation pour espaces de stockage direct, cette fonctionnalité associe des supports plus rapides (par exemple, NVMe ou SSD) à des supports plus lents (par exemple, HDD) pour créer des niveaux. Une partie de la couche de stockage la plus rapide est réservée au cache. Pour plus d'informations, consultez Activer le cache de bus de stockage avec espaces de stockage sur des serveurs autonomes.

Instantanés au niveau du fichier ReFS

Le système de fichiers résilients Microsoft (ReFS) inclut désormais la possibilité d'instantanér des fichiers à l'aide d'une opération de métadonnées rapide. Les instantanés sont différents du clonage de blocs ReFS en cela que les clones sont accessibles en écriture, tandis que les

instantanés sont en lecture seule. Cette fonctionnalité est particulièrement utile dans les scénarios de sauvegarde de machines virtuelles avec les fichiers VHD/VHDX. Les instantanés ReFS sont uniques parce qu'ils prennent le même temps, quelle que soit la taille des fichiers. La prise en charge des instantanés est disponible dans ReFSUtil ou en tant qu'API.

Compression SMB

L'amélioration de SMB sur Windows Server 2022 et Windows 11 permet à un utilisateur ou à une application de compresser les fichiers lors de leur transfert sur le réseau. Vous n'avez plus besoin de compresser manuellement les fichiers afin de transférer plus rapidement sur des réseaux plus lents ou plus ingérés. Pour plus d'informations, consultez compression SMB.

conteneurs

Windows Server 2022 comprend les modifications suivantes apportées aux conteneurs Windows.

Réduction de la taille de l'image Server Core

Nous avons réduit la taille des images Server Core. La plus petite taille d'image vous permet de déployer des applications conteneurisées plus rapidement. Dans Windows Server 2022, la couche d'image de base Server Core au moment du lancement général (GA) atteint 2,76 Go non compressés sur le disque. Comparé à la couche Windows Server 2019 RTM au moment du lancement général (GA), qui atteint 3,47 Go non compressés sur le disque, cela représente une réduction de 33 % de l'empreinte sur disque pour cette couche. Bien que vous ne deviez pas attendre que la taille totale de l'image soit réduite de 33%, une taille de couche RTM plus petite réduit généralement la taille globale de l'image.

> **Notes**
>
> Les images de base de conteneurs Windows sont fournies sous la forme de deux couches : une couche RTM et une couche de correctifs contenant les derniers correctifs de sécurité pour les bibliothèques de système d'exploitation et les fichiers binaires superposés sur la couche RTM. La taille de la couche corrective change au fil de la durée du cycle de prise en charge de l'image conteneur, en fonction du nombre de modifications dans les fichiers binaires. Lorsque vous récupérez une image de base de conteneur sur un nouvel hôte, vous devez récupérer les deux couches.

Cycle de prise en charge plus long pour toutes les images conteneurs Windows

Les images Windows Server 2022, notamment Server Core, Nano Server et Server, ont cinq ans de support standard et cinq ans de support étendu. Ce cycle de support plus long garantit que vous avez le temps d'implémenter, d'utiliser et de mettre à niveau ou de migrer le cas échéant pour votre organisation. Pour plus d'informations, consultez Cycles de vie de la maintenance des images de base Windows et Cycles de vie Windows Server 2022.

Fuseau horaire virtualisé

Avec Windows Server 2022, les conteneurs Windows peuvent gérer une configuration de fuseau horaire virtualisée distincte de l'hôte. Toutes les configurations généralement utilisées par le fuseau horaire de l'hôte sont maintenant virtualisées et instanciées pour chaque conteneur. Pour configurer le fuseau horaire du conteneur, vous pouvez utiliser l'utilitaire de commande tzutil ou la cmdlet PowerShell Set-TimeZone. Pour en savoir plus, consultez le fuseau horaire virtualisé.

Améliorations de la scalabilité pour la prise en charge de la superposition de réseaux

Windows Server 2022 intègre plusieurs améliorations de performances et d'évolutivité qui étaient déjà présentes dans quatre versions précédentes en canal semi-annuel (SAC) de Windows Server et qui n'avaient pas été rétroportées dans Windows Server 2019 :

- Résolution du problème de saturation des ports lors de l'utilisation de centaines de services et de pods Kubernetes sur le même nœud.
- Amélioration des performances du transfert de paquets dans le commutateur virtuel Hyper-V (vSwitch).
- Amélioration de la fiabilité des redémarrages de l'interface CNI dans Kubernetes.
- Améliorations au niveau du plan de contrôle HNS (Host Networking Service) et du plan de données utilisé par les conteneurs Windows Server et les réseaux Kubernetes.

Pour en savoir plus sur les améliorations des performances et de la scalabilité au niveau de la prise en charge de la superposition des réseaux, consultez Kubernetes Overlay Networking for Windows.

Routage de retour direct au serveur pour les réseaux overlay et L2Bridge

Direct Server Return (DSR) est une distribution de charge réseau asymétrique dans les systèmes de répartition de charge qui fait que le trafic de demande et de réponse utilise des chemins

réseau différents. L'utilisation de chemins réseau différents aide à éviter les sauts supplémentaires et réduit la latence, accélérant le temps de réponse entre le client et le service et retirant la charge supplémentaire du répartiteur de charge. La technologie DSR améliore de manière transparente les performances du réseau pour les applications, avec peu voire aucune modification de l'infrastructure requise.

Pour plus d'informations, consultez DSR in Introduction to Windows support in Kubernetes.

Améliorations gMSA

Vous pouvez utiliser des comptes de service administré de groupe (gMSA) avec des conteneurs Windows pour faciliter l'authentification Active Directory. Lorsqu'il a été introduit dans Windows Server 2019, gMSA nécessitait de joindre l'hôte de conteneur à un domaine pour récupérer les informations d'identification gMSA à partir d'Active Directory. Dans Windows Server 2022, gMSA pour les conteneurs avec un hôte non rejoint à un domaine utilise une identité utilisateur portable au lieu d'une identité d'hôte pour récupérer les informations d'identification gMSA. Ainsi, la jonction manuelle des nœuds Worker Windows à un domaine n'est plus nécessaire. Après l'authentification, Kubernetes enregistre l'identité utilisateur en tant que secret. Un gMSA pour conteneurs avec un hôte qui n'est pas joint à un domaine offre la flexibilité de créer des conteneurs avec gMSA sans joindre le nœud hôte au domaine.

Pour en savoir plus sur les améliorations apportées aux comptes gMSA, consultez Créer des comptes de service administré de groupe pour des conteneurs Windows.

Prise en charge d'IPv6

Kubernetes sous Windows prend désormais en charge la pile double IPv6 dans les réseaux basés sur L2bridge sous Windows Server. IPv6 dépend du CNI utilisé par Kubernetes, et nécessite également la version Kubernetes 1.20 ou ultérieure pour activer la prise en charge IPv6 de bout en bout. Pour plus d'informations, consultez IPv4/IPv6 - Introduction à la prise en charge de Windows dans Kubernetes.

Prise en charge de plusieurs sous-réseaux pour les nœuds Worker Windows avec Calico pour Windows

Le service réseau hôte (HNS) permet désormais d'utiliser des sous-réseaux plus restrictifs, tels que des sous-réseaux avec une longueur de préfixe plus longue, et également plusieurs sous-réseaux pour chaque nœud de travail Windows. Auparavant, HNS restreignait les configurations de point de terminaison de conteneur Kubernetes à utiliser uniquement la longueur de préfixe du sous-réseau sous-jacent. La première interface CNI qui utilise cette

fonctionnalité est Calico pour Windows. Pour plus d'informations, consultez Prise en charge de plusieurs sous-réseaux dans Host Networking Service.

Conteneurs HostProcess pour la gestion des nœuds

Les conteneurs HostProcess sont un nouveau type de conteneur qui s'exécute directement sur l'hôte et étend le modèle de conteneur Windows pour permettre une plus large gamme de scénarios de gestion pour les clusters Kubernetes. Avec les conteneurs HostProcess, vous pouvez empaqueter et distribuer des opérations de gestion qui nécessitent un accès hôte tout en conservant les méthodes de contrôle de version et de déploiement fournies par les conteneurs. Vous pouvez utiliser des conteneurs Windows pour différents scénarios de gestion de périphériques, de stockage et de gestion réseau dans Kubernetes.

Les conteneurs HostProcess présentent les avantages suivants :

- Les utilisateurs du cluster n'ont plus besoin de se connecter et de configurer individuellement chaque nœud Windows pour les tâches administratives et la gestion des services Windows.
- Vous pouvez utiliser le modèle de conteneur pour déployer la logique de gestion sur autant de clusters que nécessaire.
- Vous pouvez créer des conteneurs HostProcess au-dessus des images de base Windows Server 2019 ou ultérieures existantes, les gérer à l'aide du runtime de conteneur Windows et s'exécuter en tant qu'utilisateur disponible dans le domaine de l'ordinateur hôte.
- Les conteneurs HostProcess constituent le meilleur moyen de gérer des nœuds Windows dans Kubernetes.

Pour plus d'informations, consultez Conteneurs de processus hôte Windows.

Améliorations de Windows Admin Center

Windows Server 2022 développe l'extension Containers ajoutée à Windows Admin Center pour conteneuriser les applications Web existantes basées sur ASP.NET de .NET Framework. Vous pouvez utiliser des dossiers statiques ou des solutions Visual Studio provenant de votre développeur.

Windows Admin Center comprend les améliorations suivantes :

- L'extension Containers prend désormais en charge les fichiers de déploiement Web, ce qui vous permet d'extraire l'application et sa configuration à partir d'un serveur en cours d'exécution, puis de conteneuriser l'application.
- Vous pouvez valider l'image localement, puis envoyer (push) cette image à Azure Container Registry.

- Azure Container Registry et Azure Container Instances disposent désormais de fonctionnalités de gestion de base. Vous pouvez désormais utiliser l'interface utilisateur du Centre d'administration Windows pour créer et supprimer des registres, gérer des images, et démarrer et arrêter de nouvelles instances de conteneurs.

Azure Migrate : Outil conteneurisation d'applications

Application Azure Migrate : La conteneurisation est une solution de bout en bout qui conteneurise et déplace les applications web existantes vers Azure Kubernetes Service. Vous pouvez évaluer les serveurs web existants, créer une image de conteneur, pousser l'image vers le Registre de conteneurs Azure, créer un déploiement Kubernetes, et enfin le déployer vers le service Azure Kubernetes.

Pour plus d'informations sur l'outil Azure Migrate App : Containerization, consultez ASP.NET conteneurisation et migration d'applications vers Azure Kubernetes Service et java web containerization et migration vers Azure Kubernetes Service.

Nouveautés de Windows Server 2019

25/07/2025S'applique à: ✅ Windows Server 2019

Cet article décrit certaines des nouvelles fonctionnalités de Windows Server 2019. Windows Server 2019 repose sur les bases solides de Windows Server 2016 et apporte de nombreuses innovations dans quatre thèmes clés : cloud hybride, sécurité, plateforme d'applications et infrastructure hyperconvergée (HCL).

General

Windows Admin Center (Centre d'administration Windows)

Windows Admin Center est une application basée sur navigateur, déployée localement pour la gestion des serveurs, des clusters, de l'infrastructure hyperconvergée et des PC Windows 10. Il est fourni sans coût supplémentaire avec Windows et est prêt à être utilisé en production.

Vous pouvez installer Windows Admin Center sur Windows Server 2019 et Windows 10 et 11, et l'utiliser pour gérer les serveurs et les clusters exécutant Windows Server 2012 et versions ultérieures.

Pour plus d'informations, consultez Windows Admin Center.

Desktop experience

Étant donné que Windows Server 2019 est une version de canal de maintenance à long terme (LTSC), il inclut l'**expérience utilisateur**. Les versions SAC (Semi-Annual Channel) n'incluent pas l'expérience de bureau par conception ; il s'agit strictement de versions d'images de conteneurs Server Core et Nano Server. Comme avec Windows Server 2016, pendant l'installation du système d'exploitation, vous pouvez choisir entre les installations Server Core ou Server avec Expérience utilisateur.

System Insights

Insights système est une nouvelle fonctionnalité disponible dans Windows Server 2019 qui apporte des fonctionnalités analytiques prédictives locales en mode natif de Windows Server. Ces fonctionnalités prédictives, chacune basées sur un modèle Machine Learning, analysent localement les données système de Windows Server, comme les compteurs de performances et les événements. Les Insights système vous permet de comprendre le fonctionnement de vos serveurs et vous aide à réduire les dépenses opérationnelles associées à la gestion réactive des problèmes dans vos déploiements Windows Server.

Hybrid Cloud

Fonctionnalité de compatibilité des applications Server Core à la demande

La fonctionnalité de compatibilité des applications Server Core à la demande (FOD) améliore considérablement la compatibilité des applications en incluant un sous-ensemble des fichiers binaires et des composants de Windows Server avec l'Expérience utilisateur. Server Core est maintenu aussi simple que possible et n'ajoute pas l'environnement graphique de l'Expérience utilisateur de Windows Server lui-même, ce qui augmente les fonctionnalités et la compatibilité.

Cette fonctionnalité facultative à la demande est disponible sur un fichier ISO distinct et peut être ajoutée à des installations et des images Windows Server Core uniquement, à l'aide de DISM.

Rôle serveur de transport des Services de déploiement Windows (WDS) ajouté à Server Core

Le Serveur de transport contient uniquement les composants de mise en réseau principaux de WDS. Vous pouvez désormais utiliser Server Core avec le rôle Serveur de transport pour créer des espaces de noms de multidiffusion qui transmettent les données (y compris des images du système d'exploitation) depuis un serveur autonome. Vous pouvez également l'utiliser si vous souhaitez disposer d'un serveur PXE qui permette aux clients d'utiliser un démarrage PXE et de télécharger votre propre application d'installation personnalisée.

Intégration des services Bureau à distance à Azure AD

Avec l'intégration d'Azure AD, vous pouvez utiliser les stratégies d'accès conditionnel, l'authentification multifacteur, l'authentification intégrée avec d'autres applications SaaS en utilisant Azure Active Directory, etc. Pour plus d'informations, consultez Intégrer Azure AD Domain Services à votre déploiement RDS.

Networking

Nous avons apporté plusieurs améliorations à la pile réseau principale, comme TCP Fast Open (TFO), Receive Window Autotuning, IPv6, etc. Pour plus d'informations, consultez le billet Amélioration des fonctionnalités de la pile réseau principale.

vRSS dynamique et VMMQ

Dans le passé, les files d'attente de machines virtuelles et les files d'attente multiples de machines virtuelles (VMMQ) ont permis d'augmenter considérablement le débit des machines virtuelles individuelles lorsque les débits du réseau ont atteint la barre des 10 GbE et au-delà. Malheureusement, la planification, la définition des bases, le réglage et la surveillance nécessaires pour réussir sont devenus une entreprise beaucoup plus importante que les administrateurs informatiques ne l'avaient prévu.

Windows Server 2019 améliore ces optimisations en répartissant et en réglant dynamiquement le traitement des charges de travail réseau en fonction des besoins. Windows Server 2019 garantit une efficacité maximale et supprime la charge de configuration imposée aux administrateurs informatiques. Pour en savoir plus, voir Configuration requise du réseau hôte pour Azure Local.

Security

Protection avancée contre les menaces Windows Defender

Les capteurs profonds de plate-forme et les actions de réponse d'ATP exposent des attaques au niveau de la mémoire et du noyau et y répondent par la suppression des fichiers malveillants et l'arrêt des processus malveillants.

- Pour plus d'informations sur Windows Defender ATP, consultez Présentation des capacités de Windows Defender ATP.
- Pour plus d'informations sur l'intégration des serveurs, consultez Intégrer des serveurs au service Windows Defender ATP.

Windows Defender ATP Exploit Guard est un nouvel ensemble de fonctionnalités de prévention des intrusions des hôtes qui vous permettent d'équilibrer les risques de sécurité et les exigences de productivité. Windows Defender Exploit Guard est conçu pour protéger l'appareil contre un grand nombre de vecteurs d'attaque et pour bloquer les comportements couramment utilisés dans les attaques par programmes malveillants. Les composants sont :

- La réduction de la surface d'attaque (ASR) est un ensemble de contrôles que les entreprises peuvent activer pour empêcher les logiciels malveillants de s'installer sur la machine en bloquant les fichiers malveillants suspects. Par exemple, les fichiers Office, les scripts, les mouvements latéraux, le comportement des ransomwares et les menaces basées sur les e-mails.

- Protection réseau protège le point de terminaison contre les menaces web en bloquant n'importe quel processus sortant sur l'appareil vers des adresses d'hôtes/IP non approuvées à travers Windows Defender SmartScreen.
- L'accès contrôlé aux dossiers protège les données sensibles contre les rançongiciels en empêchant les processus non approuvés d'accéder à vos dossiers protégés.
- Exploit Protection est un ensemble de mesures d'atténuation des attaques de vulnérabilité (remplaçant EMET) qui peuvent être facilement configurées pour protéger votre système et vos applications.
- Contrôle d'application Windows Defender (également connu sous le nom de stratégie d'intégrité du code [CI]) a été publié dans Windows Server 2016. Nous avons simplifié le déploiement en incluant des stratégies d'intégrité du code par défaut. La stratégie par défaut autorise tous les fichiers intégrés dans Windows ainsi que les applications Microsoft comme SQL Server, et bloque les fichiers exécutables connus qui peuvent contourner l'intégrité du code.

Sécurité avec SDN (Software Defined Networking)

Sécurité avec SDN offre de nombreuses fonctionnalités destinées à renforcer la confiance des clients exécutant des charges de travail, soit en local, soit comme fournisseurs de services dans le cloud.

Ces améliorations de sécurité sont intégrées dans la plateforme SDN complète introduite dans Windows Server 2016.

Pour connaître la liste complète des nouveautés de SDN, consultez Nouveautés SDN pour Windows Server 2019.

Améliorations apportées aux machines virtuelles dotées d'une protection maximale

Nous avons apporté les améliorations suivantes aux machines virtuelles blindées.

Améliorations pour les filiales

Vous pouvez maintenant exécuter des machines virtuelles dotées d'une protection maximale sur des ordinateurs ayant une connectivité intermittente au Service Guardian hôte à l'aide du nouveau SGH de secours et des fonctionnalités du mode hors connexion. Le SGH de secours vous permet de configurer un deuxième ensemble d'URL qu'Hyper-V peut essayer s'il ne peut pas atteindre votre serveur SGH principal.

Même si vous ne pouvez pas atteindre le HGS, le mode hors ligne vous permet de continuer à démarrer vos machines virtuelles protégées. Le mode hors ligne vous permet également de démarrer vos machines virtuelles tant que la machine virtuelle a démarré avec succès une fois et que la configuration de sécurité de l'hôte n'a pas changé.

Troubleshooting improvements

Nous avons également facilité le dépannage de vos machines virtuelles protégées en activant la prise en charge de VMConnect Enhanced Session Mode et de PowerShell Direct. Ces outils sont utiles lorsque vous perdez la connectivité réseau avec votre VM et que vous devez mettre à jour sa configuration pour rétablir l'accès. Pour en savoir plus, voir Guarded fabric et shielded VMs.

Vous n'avez pas besoin de configurer ces fonctionnalités car elles deviennent automatiquement disponibles lorsque vous placez une VM blindée sur un hôte Hyper-V exécutant Windows Server version 1803 ou ultérieure.

Linux support

Si vous exécutez des environnements à systèmes d'exploitation mixtes, Windows Server 2019 prend désormais en charge l'exécution d'Ubuntu, Red Hat Enterprise Linux et SUSE Linux Enterprise Server dans les machines virtuelles.

HTTP/2 pour un Internet plus rapide et plus sûr

- Amélioration de la fusion de connexions pour offrir une expérience de navigation ininterrompue et correctement chiffrée.
- Mise à niveau de la négociation de suite de chiffrement côté serveur HTTP/2 pour l'atténuation automatique des échecs de connexion et la simplicité de déploiement.
- Modification de notre fournisseur de congestion TCP par défaut en faveur de Cubic pour vous offrir davantage de débit !

Encrypted networks

Le chiffrement du réseau virtuel crypte le trafic du réseau virtuel entre les machines virtuelles au sein des sous-réseaux portant l'étiquette **Chiffrement activé**. Les réseaux chiffrés utilisent également Datagram Transport Layer Security (DTLS) sur le sous-réseau virtuel pour chiffrer les paquets. DTLS protège vos données contre l'écoute, la manipulation et la contrefaçon par toute personne ayant accès au réseau physique.

Pour plus d'informations, veuillez consulter la rubrique Réseaux chiffrés.

Firewall auditing

L'audit des pare-feu est une nouvelle fonctionnalité pour le pare-feu SDN qui enregistre tout flux traité par les règles de pare-feu SDN et les listes de contrôle d'accès (ACL) qui ont le journalisation activée.

Peering de réseau virtuel

Le peering de réseaux virtuels vous permet de connecter deux réseaux virtuels de manière transparente. Une fois appairés, les réseaux virtuels apparaissent dans la surveillance comme un seul réseau.

Egress metering

La mesure de sortie offre des compteurs d'utilisation pour les transferts de données sortants. Network Controller utilise cette fonctionnalité pour conserver une liste d'autorisation de toutes les plages IP utilisées dans SDN par réseau virtuel. Ces listes considèrent que tout paquet se dirigeant vers une destination non incluse dans les plages IP répertoriées est facturé comme des transferts de données sortants.

Storage

Voici quelques-unes des modifications que nous avons apportées au stockage dans Windows Server 2019. Le stockage est également affecté par les mises à jour de la déduplication des données, en particulier sa mise à jour de l'API DataPort pour une entrée ou une sortie optimisée vers les volumes dédupliqués.

Gestionnaire de Ressources du Serveur de Fichiers

Il est maintenant possible d'empêcher le service Outils de gestion de ressources pour serveur de fichiers de créer un journal des modifications (également appelé journal USN) sur tous les volumes au démarrage du service. Empêcher la création du parcours de modification peut économiser de l'espace sur chaque volume, mais va désactiver la classification des fichiers en temps réel. Pour plus d'informations, consultez Vue d'ensemble du Gestionnaire de ressources du serveur de fichiers.

SMB

- Windows Server n'installe plus le client et le serveur SMB1 par défaut. En outre, la possibilité d'authentification en tant qu'invité dans SMB2 et versions ultérieures est désactivée par défaut. Pour plus d'informations, consultez SMBv1 n'est pas installé par défaut dans Windows 10 version 1709, Windows Server version 1709 et les versions ultérieures.

- Vous pouvez désormais désactiver les oplocks dans SMB2+ pour les applications héritées. Vous pouvez également exiger d'un client une signature ou un chiffrement par connexion. Pour plus d'informations, consultez l'aide du module PowerShell de SMBShare.

Service de migration de stockage

Le Service de migration du stockage facilite la migration des serveurs vers une version plus récente de Windows Server. Cet outil graphique répertorie les données sur les serveurs, puis transfère les données et configurations vers de nouveaux serveurs. Le Service de migration de stockage peut également transférer les identités des anciens serveurs vers les nouveaux serveurs afin que les utilisateurs n'aient pas à reconfigurer leurs profils et applications. Pour plus d'informations, veuillez consulter la rubrique Service de migration de stockage.

Windows Admin Center version 1910 a ajouté la possibilité de déployer des machines virtuelles Azure. Cette mise à jour intègre le déploiement de machines virtuelles Azure dans le service de migration de stockage. Pour plus d'informations, consultez Migration de machines virtuelles Azure.

Vous pouvez également accéder aux fonctionnalités suivantes après la mise en production (RTM) en exécutant l'orchestrateur du Serveur de migration de stockage sous Windows Server 2019 avec KB5001384 installé ou sous Windows Server 2022 :

- Migrer des groupes et utilisateurs locaux vers le nouveau serveur
- Migrer le stockage à partir de clusters de basculement, migrer vers des clusters de basculement, et migrer entre des serveurs autonomes et des clusters de basculement
- Migrer le stockage à partir d'un serveur Linux qui utilise Samba
- Synchroniser plus facilement des partages migrés dans Azure en utilisant Azure File Sync
- Migrer vers de nouveaux réseaux comme Azure
- Migrer les serveurs NetApp Common Internet File System (CIFS) des matrices NetApp Federated Authentication Service (FAS) vers des serveurs et clusters Windows.

Espaces de stockage direct

Voici les nouveautés de Storage Spaces Direct. Pour plus d'informations sur l'acquisition de systèmes Espaces de Stockage Direct validés, consultez vue d'ensemble de la solution locale Azure.

- Déduplication et compression des volumes ReFS Le stockage de morceaux de taille variable avec compression optionnelle maximise les taux d'économie, tandis que l'architecture de post-traitement multithread minimise l'impact sur les performances. Cette fonctionnalité prend en charge des volumes allant jusqu'à 64 To et déduplique les 4 premiers Mo de chaque fichier.

- Prise en charge native de la mémoire persistante, qui vous permet de gérer la mémoire persistante comme n'importe quel autre disque dans PowerShell ou Windows Admin Center. Cette fonctionnalité prend en charge les modules de mémoire persistante Intel Optane DC PM et NVDIMM-N.

- Résilience imbriquée pour une infrastructure hyperconvergée à deux nœuds en périphérie. Grâce à une nouvelle option de résilience logicielle basée sur RAID 5+1, vous pouvez désormais survivre simultanément à deux pannes matérielles. Un cluster Storage Spaces Direct à deux nœuds fournit un stockage accessible en continu pour les applications et les machines virtuelles, même si un nœud de serveur tombe en panne et qu'un autre nœud de serveur subit une défaillance de disque.

- Les clusters à deux serveurs peuvent désormais utiliser une clé USB comme témoin. Si un serveur tombe en panne, puis effectue une sauvegarde, le cluster de lecteur USB sait quel serveur possède les données les plus récentes. Pour plus d'informations, consultez notre article de blog sur l'annonce de Storage Spaces Direct et Configurez un témoin de partage de fichiers pour le clustering de basculement.

- Le Centre d'administration Windows prend en charge un tableau de bord qui vous permet de gérer et de surveiller Storage Spaces Direct. Vous pouvez surveiller l'IOPS et la latence IO du niveau global du cluster jusqu'aux disques SSD ou HDD individuels, sans frais supplémentaires. Pour plus d'informations, consultez Gérer une infrastructure hyperconvergée à l'aide de Windows Admin Center.

- L'historique des performances est une nouvelle fonctionnalité qui offre une visibilité sans effort sur l'utilisation des ressources et les mesures. Pour en savoir plus, consultez la rubrique Historique des performances pour Storage Spaces Direct.

- Évoluez jusqu'à 4 Po par cluster en utilisant une capacité de 64 volumes de 64 To maximum. Vous pouvez également assembler plusieurs clusters en un ensemble de clusters pour une montée en charge encore plus importante au sein d'un même espace de noms de stockage.

- En utilisant la parité accélérée par miroir, il est possible de construire des volumes Storage Spaces Direct qui intègrent à la fois des stratégies de miroir et de parité, comme un mélange de RAID-1 et de RAID-5/6. La parité accélérée par le miroir est désormais deux fois plus rapide que celle de Windows Server 2016.

- La détection des valeurs aberrantes de latence des lecteurs identifie automatiquement les lecteurs lents dans PowerShell et Windows Admin Center avec un état « Latence anormale ».
- Délimitez manuellement l'allocation des volumes pour augmenter la tolérance aux pannes. Pour plus d'informations, consultez Délimiter l'allocation de volumes dans Storage Spaces Direct.

Storage Replica

Voici les nouveautés du réplica de stockage.

- Storage Replica est désormais disponible dans Windows Server 2019 Standard Edition et Windows Server 2019 Datacenter Edition. Cependant, avec l'édition standard, vous ne pouvez répliquer qu'un seul volume, et ce volume ne peut atteindre une taille de 2 To.
- Le basculement de test est une nouvelle fonctionnalité qui vous permet de monter temporairement un instantané du stockage répliqué sur un serveur de destination à des fins de test ou de sauvegarde. Pour plus d'informations, consultez la rubrique Questions fréquemment posées sur le réplica de stockage.
- Améliorations des performances des logs Storage Replica, telles que l'amélioration du débit et de la latence de la réplication sur le stockage all-flash et les clusters Storage Spaces Direct qui se répliquent les uns les autres.
- Prise en charge de Windows Admin Center, y compris la gestion graphique de la réplication à l'aide de Server Manager pour la réplication de serveur à serveur, de cluster à cluster et de stretch cluster.

Data deduplication

Windows Server 2019 prend désormais en charge le système de fichiers résilient (ReFS). ReFS vous permet de stocker jusqu'à dix fois plus de données sur le même volume avec la déduplication et la compression pour le système de fichiers ReFS. Le magasin de morceaux de taille variable s'accompagne d'une fonction de compression optionnelle qui peut maximiser les taux d'économie, tandis que l'architecture de post-traitement multithread maintient l'impact sur les performances à un niveau minimal. ReFS prend en charge des volumes allant jusqu'à 64 To et déduplique les 4 premiers To de chaque fichier. Pour en savoir plus, consultez Comment activer la déduplication et la compression dans Windows Admin Center pour une démonstration vidéo rapide.

Failover Clustering

Nous avons ajouté les fonctionnalités suivantes au clustering de basculement dans Windows Server 2019 :

- Les ensembles de clusters regroupent plusieurs clusters en un regroupement faiblement couplé de plusieurs clusters de basculement qui se déclinent en trois types : calcul, stockage et hyperconvergé. Ce regroupement augmente le nombre de serveurs dans une seule solution de centre de données défini par logiciel (SDDC) au-delà des limites actuelles d'un cluster. Avec les ensembles de clusters, vous pouvez déplacer des machines virtuelles en ligne entre les clusters de l'ensemble de clusters. Pour plus d'informations, voir Déployer un ensemble de clusters.

- Les clusters sont désormais compatibles avec Azure par défaut. Les clusters Azure-aware détectent automatiquement lorsqu'ils s'exécutent dans des machines virtuelles Azure IaaS, puis optimisent leur configuration pour atteindre les niveaux de disponibilité les plus élevés. Ces optimisations incluent le basculement proactif et la journalisation des événements de maintenance planifiée Azure. L'optimisation automatisée simplifie le déploiement en supprimant la nécessité de configurer l'équilibreur de charge avec le nom de réseau distribué pour le nom du cluster.

- La migration de clusters inter-domaines permet aux clusters de basculement de passer dynamiquement d'un domaine Active Directory à un autre, ce qui simplifie la consolidation des domaines et permet aux partenaires matériels de créer des clusters et de les joindre ultérieurement au domaine du client.

- La fonction USB witness vous permet d'utiliser une clé USB connectée à un commutateur réseau comme témoin pour déterminer le quorum d'une grappe. Cette fonction inclut une prise en charge étendue des témoins de partage de fichiers pour tout périphérique compatible SMB2.

- Le cache CSV est désormais activé par défaut pour améliorer les performances de la machine virtuelle. MSDTC prend désormais en charge les volumes partagés de cluster pour permettre le déploiement des charges de travail MSDTC sur Storage Spaces Direct, comme avec SQL Server. Amélioration de la logique pour détecter les nœuds partitionnés avec auto-adaptation afin de renvoyer les nœuds à l’appartenance au cluster. Amélioration de l’auto-adaptation et de la détection des routes de réseau de cluster.

- La mise à jour adaptée aux clusters (CAU) est désormais intégrée et prend en compte les espaces de stockage direct, validant et garantissant la resynchronisation des données sur chaque nœud. La mise à jour adaptée aux clusters inspecte les mises à jour pour redémarrer intelligemment uniquement si nécessaire. Cette fonctionnalité vous permet de redémarrer tous les serveurs du cluster en cas de maintenance planifiée.

- Vous pouvez désormais utiliser des témoins de partage de fichiers dans les scénarios suivants :
    - Accès Internet absent ou médiocre en raison d'un emplacement distant, empêchant l'utilisation d'un témoin de cloud.
    - Absence de lecteurs partagés pour un témoin de disque. Par exemple, une configuration qui n'utilise pas de disques partagés, telle qu'une configuration hyperconvergée Storage Spaces Direct, un groupe de disponibilité (AG) SQL Server Always On ou un groupe de disponibilité de base de données (DAG) Exchange.
    - Absence de connexion au contrôleur de domaine parce que le cluster se trouve derrière une zone démilitarisée.
    - Un groupe de travail ou un cluster inter-domaines qui n'a pas d'objet de nom de cluster Active Directory (CNO). Windows Server bloque désormais également l'utilisation d'un partage DFS Namespaces en tant qu'emplacement. L'ajout d'un témoin de partage de fichiers à un partage DFS peut entraîner des problèmes de stabilité sur votre cluster, et cette configuration n'a jamais été prise en charge. Nous avons ajouté une logique pour détecter si un partage utilise des espaces de noms DFS, et quand des espaces de noms DFS sont détectés, le Gestionnaire du cluster de basculement bloque la création du témoin et affiche un message d'erreur indiquant qu'il n'est pas pris en charge.
- Une fonctionnalité de renforcement des clusters a été mise en œuvre pour améliorer la sécurité des communications intra-cluster via Server Message Block (SMB) pour les volumes partagés de cluster et Storage Spaces Direct. Cette fonctionnalité s'appuie sur des certificats pour fournir la plateforme la plus sécurisée possible. Ce faisant, les Clusters de basculement peuvent désormais fonctionner sans aucune dépendance à NTLM, ce qui permet d'établir des lignes de base de sécurité.
- Les clusters de basculement n'utilisent plus l'authentification NTLM. Au lieu de cela, les clusters Windows Server 2019 utilisent désormais exclusivement Kerberos et l'authentification basée sur les certificats. Les utilisateurs n'ont pas besoin d'effectuer des modifications ou de déployer quoi que ce soit pour profiter de cette amélioration de la sécurité. Cette modification vous permet également de déployer des clusters de basculement dans des environnements où NTLM est désactivé.

Application Platform

Conteneurs Linux sur Windows

Il est désormais possible d'exécuter des conteneurs Windows et Linux sur le même hôte de conteneurs en utilisant le même démon Docker. Vous pouvez maintenant avoir un environnement d'hôte de conteneurs hétérogène offrant davantage de flexibilité aux développeurs d'applications.

Prise en charge intégrée de Kubernetes

Windows Server 2019 poursuit les améliorations apportées aux capacités de calcul, de réseau et de stockage à partir des versions de canal semi-annuel nécessaires pour prendre en charge Kubernetes sur Windows. Plus de détails sont disponibles dans les prochaines versions de Kubernetes.

- Les réseaux de conteneurs dans Windows Server 2019 améliorent considérablement la facilité d'utilisation de Kubernetes sur Windows. Nous avons amélioré la résilience réseau des plateformes et la prise en charge des plug-ins réseau des conteneurs.
- Les charges de travail déployées sur Kubernetes peuvent utiliser la sécurité du réseau pour protéger les services Windows et Linux à l'aide d'outils intégrés.

Container improvements

- **Identité intégrée améliorée**

  Nous avons simplifié l'authentification Windows intégrée dans les conteneurs et l'avons rendue plus fiable en résolvant plusieurs limitations des versions antérieures de Windows Server.

- **Meilleure compatibilité des applications**

  La mise en conteneur des applications basées sur Windows est plus facile que jamais : La compatibilité des applications pour l'image **windowsservercore** existante a été augmentée. Pour les applications avec des dépendances d'API supplémentaires, il existe désormais une image de base de tiers : **windows**.

- **Taille réduite et performances supérieures**

  La taille du téléchargement, la taille sur disque et le temps de démarrage des images de conteneur de base ont été améliorés de façon à accélérer les workflows des conteneurs.

- **Expérience de gestion à l'aide de Windows Admin Center (préversion)**

  Il est maintenant plus facile que jamais de voir quels conteneurs sont en cours d'exécution sur votre ordinateur et de gérer des conteneurs individuels avec une nouvelle

extension pour Windows Admin Center. Recherchez l'extension « Conteneurs » dans le flux public du Windows Admin Center.

Compute improvements

- **Ordre de démarrage des machines virtuelles** La fonctionnalité Ordre de démarrage des machines virtuelles est également améliorée avec la reconnaissance des applications et du système d'exploitation. Elle apporte des déclencheurs améliorés pour déterminer si une machine virtuelle est considérée comme démarrée avant le démarrage de la suivante.

- La **prise en charge de la mémoire de classe stockage pour les machines virtuelles** permet la création de volumes NTFS à accès direct sur des éléments DIMM non volatiles et leur exposition à des machines virtuelles Hyper-V. Les machines virtuelles Hyper-V peuvent maintenant tirer parti des avantages des performances à faible latence des périphériques mémoire de classe stockage.

- **Prise en charge de la mémoire persistante pour les machines virtuelles Hyper-V** Pour utiliser le débit élevé et la faible latence de la mémoire persistante (également connue sous le nom de « mémoire de classe de stockage ») dans les machines virtuelles, elle peut désormais être projetée directement dans les machines virtuelles. La mémoire persistante peut aider à réduire considérablement la latence des transactions de base de données ou à réduire les temps de récupération de bases de données à faible latence en mémoire en cas d'échec.

- **Stockage des conteneurs : volumes de données persistants** Les conteneurs d'application disposent désormais d'un accès persistant aux volumes. Pour plus d'informations, consultez le billet de blog Container Storage Support with Cluster Shared Volumes (CSV), Storage Spaces Direct (S2D), SMB Global Mapping.

- **Format de fichier de configuration de machine virtuelle (mis à jour)** Le fichier d'état d'invité de la machine virtuelle (`.vmgs`) a été ajouté pour les machines virtuelles avec une version de configuration 8.2 et ultérieure. Le fichier d'état d'invité de la machine virtuelle inclut des informations sur l'état de l'appareil, qui faisaient auparavant partie du fichier d'état du runtime de la machine virtuelle.

Encrypted Networks

Réseaux chiffrés - Le chiffrement des réseaux virtuels permet de chiffrer le trafic de réseau virtuel entre des machines virtuelles qui communiquent entre eux 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.

Améliorations des performances réseau pour les charges de travail virtuelles

Améliorations des performances réseau pour les charges de travail virtuelles optimise le débit du réseau pour les machines virtuelles sans avoir à constamment ajuster ou surdimensionner votre hôte. Les performances améliorées réduisent les coûts d'exploitation et de maintenance tout en augmentant la densité disponible de vos hôtes. Ces nouvelles fonctionnalités sont les suivantes :

- Machine virtuelle dynamique multi-file d'attente (d.VMMQ)
- Receive Segment Coalescing dans le commutateur virtuel

Transport d'arrière-plan à faible délai supplémentaire

Low Extra Delay Background Transport (LEDBAT) est un fournisseur de contrôle de congestion du réseau à latence optimisée, conçu pour allouer automatiquement de la bande passante aux utilisateurs et aux applications. LEDBAT consomme la bande passante disponible quand le réseau n'est pas en cours d'utilisation. La technologie est destinée à être utilisée lors de déploiement de mises à jour volumineuses et critiques dans un environnement informatique, sans impact sur les services côté client ni sur la bande passante associée.

Service de temps Windows

Le Service de temps Windows comprend une véritable prise en charge de la de seconde intercalaire conforme à l'UTC, un nouveau protocole d'horaire appelé Precision Time Protocol et une traçabilité de bout en bout.

Passerelles SDN hautes performances

Les passerelles SDN hautes performances dans Windows Server 2019 améliorent considérablement les performances pour les connexions IPsec et GRE, fournissant un débit ultra hautes performances en utilisant beaucoup moins l'UC.

Nouvelle interface utilisateur de déploiement et extension du Windows Admin Center pour SDN

Désormais, avec Windows Server 2019, il est facile de déployer et de gérer par le biais d'une nouvelle interface utilisateur de déploiement et l'extension Windows Admin Center qui permettra à tout le monde de tirer parti de la puissance du SDN.

Sous-système Windows pour Linux (WSL)

WSL permet aux administrateurs de serveur d'utiliser les outils et les scripts existants de Linux sur Windows Server. De nombreuses améliorations présentées dans le blog de la ligne de commande font désormais partie de Windows Server, y compris les tâches en arrière-plan, DriveFS, WSLPath et bien plus encore.

Services de fédération Active Directory (AD FS)

Active Directory Federation Services (AD FS) pour Windows Server 2019 inclut les modifications suivantes .

Connexions protégées

Les ouvertures de session protégées avec AD FS incluent désormais les mises à jour suivantes :

- Les utilisateurs peuvent désormais utiliser des produits d'authentification tiers comme premier facteur sans exposer les mots de passe. Dans les cas où le fournisseur d'authentification externe peut prouver deux facteurs, il peut utiliser l'authentification multifactorielle (MFA).
- Les utilisateurs peuvent désormais utiliser des mots de passe comme facteur supplémentaire après avoir utilisé une option sans mot de passe comme premier facteur. Cette prise en charge intégrée améliore l'expérience globale par rapport à AD FS 2016, qui nécessitait le téléchargement d'un adaptateur GitHub.
- Les utilisateurs peuvent désormais construire leurs propres modules enfichables d'évaluation des risques pour bloquer certains types de demandes pendant l'étape de préauthentification. Cette fonctionnalité facilite l'utilisation de l'intelligence du cloud, comme la protection de l'identité, pour bloquer les utilisateurs ou les transactions à risque. Pour plus d'informations, consultez Créer des plug-ins avec un modèle d'évaluation des risques AD FS 2019.
- Amélioration de l'ingénierie de réparation rapide Extranet Smart Lockout (ESL) par l'ajout des fonctionnalités suivantes :
    - Vous pouvez désormais utiliser le mode audit tout en étant protégé par la fonctionnalité de verrouillage extranet classique.

- Les utilisateurs peuvent désormais utiliser des seuils de verrouillage indépendants pour des sites familiers. Cette fonctionnalité vous permet d'exécuter plusieurs instances d'applications au sein d'un compte de service commun afin de reconduire les mots de passe avec un minimum d'interruption.

Autres améliorations apportées à la sécurité

AD FS 2019 inclut les améliorations de sécurité suivantes :

- PowerShell à distance à l'aide de la connexion par carte à puce permet aux utilisateurs de se connecter à distance à AD FS avec des cartes à puce en exécutant des commandes PowerShell. Les utilisateurs peuvent également utiliser cette méthode pour gérer toutes les fonctions PowerShell, y compris les cmdlets multi-nœuds.

- La personnalisation des en-têtes HTTP permet aux utilisateurs de personnaliser les en-têtes HTTP créés lors des réponses à AD FS. La personnalisation des en-têtes saisit les types d'en-têtes suivants :

  - HSTS, qui vous permet uniquement d'utiliser les points d'extrémité AD FS sur des points d'extrémité HTTPS pour qu'un navigateur compatible les applique.

  - X-frame-options, qui permet aux administrateurs AD FS d'autoriser des parties utilisatrices spécifiques à intégrer des iFrames dans les pages d'ouverture de session interactive AD FS. Vous ne devez utiliser cet en-tête que sur les hôtes HTTPS.

  - Future header. Vous pouvez également configurer plusieurs en-têtes futurs.

  Pour plus d’informations, consultez Personnaliser des en-têtes de réponse de sécurité HTTP avec AD FS 2019.

Fonctions d'authentification et de stratégie

AD FS 2019 inclut les fonctionnalités d'authentification et de stratégie suivantes :

- Les utilisateurs peuvent désormais créer des règles pour spécifier le fournisseur d'authentification que leur déploiement invoque pour l'authentification supplémentaire. Cette fonctionnalité facilite la transition entre les fournisseurs d'authentification et la sécurisation d'apps spécifiques qui ont des exigences particulières pour les fournisseurs d'authentification supplémentaires.

- Restrictions facultatives pour les authentifications de périphériques basées sur Transport Layer Security (TLS) afin que seules les applications nécessitant TLS puissent les utiliser. Les utilisateurs peuvent restreindre les authentifications de périphériques basées sur TLS

pour que seules les applications effectuant un accès conditionnel basé sur le périphérique puissent les utiliser. Cette fonctionnalité permet d'éviter les invites indésirables d'authentification de périphérique pour les applications qui ne nécessitent pas d'authentification de périphérique basée sur TLS.

- AD FS prend désormais en charge le rétablissement des informations d'identification à deuxième facteur en fonction de la fraîcheur des informations d'identification à deuxième facteur. Cette fonctionnalité permet aux utilisateurs de n'exiger l'authentification TFA que pour la première transaction, puis de n'exiger le deuxième facteur que périodiquement. Vous ne pouvez utiliser cette fonctionnalité que sur des applications qui peuvent fournir un paramètre supplémentaire dans la demande, car il ne s'agit pas d'un paramètre configurable dans AD FS. Microsoft Entra ID prend en charge ce paramètre si vous configurez le paramètre **Se souvenir de mon AMF pendant X jours** pour que *supportsMFA* soit défini sur **True** dans les paramètres de confiance du domaine fédéré de Microsoft Entra ID.

Améliorations apportées à l'authentification unique

AD FS 2019 comprend également les améliorations suivantes en matière d'authentification unique (SSO) :

- AD FS utilise désormais un flux UX paginé et une interface utilisateur (UI) centrée qui offre une expérience de connexion plus fluide aux utilisateurs. Ce changement reflète la fonctionnalité offerte dans Azure AD. Il se peut que vous deviez mettre à jour le logo et les images d'arrière-plan de votre organisation pour les adapter à la nouvelle interface utilisateur.

- Nous avons corrigé un problème qui faisait que l'état MFA ne persistait pas lors de l'utilisation de l'authentification par jeton de rafraîchissement primaire (PRT) sur les appareils Windows 10. Les utilisateurs devraient désormais être invités moins souvent à fournir des informations d'identification de second facteur. L'expérience devrait maintenant être cohérente lorsque l'authentification du périphérique est réussie sur l'authentification TLS et PRT du client.

Prise en charge de la création d'applications métier modernes

AD FS 2019 inclut les fonctionnalités suivantes pour prendre en charge la création d'applications modernes de ligne de métier (LOB) :

- AD FS inclut désormais la prise en charge du profil de flux de périphériques OAuth pour la connexion à l'aide de périphériques sans surface d'interface utilisateur afin de prendre en charge des expériences de connexion riches. Cette fonctionnalité permet aux

utilisateurs de terminer la connexion sur un autre appareil. L'interface de ligne de commande Azure (CLI) dans Azure Stack nécessite cette fonctionnalité, mais vous pouvez également l'utiliser dans d'autres scénarios.

- Vous n'avez plus besoin du paramètre *Resource* pour utiliser AD FS, ce qui est conforme aux spécifications actuelles de l'OAUth. Les clients n'ont plus qu'à fournir l'identifiant de confiance de la partie se fiant à eux en tant que paramètre d'étendue avec les autorisations demandées.

- Vous pouvez utiliser des en-têtes CORS (cross-origin resource sharing) dans les réponses AD FS. Ces nouveaux en-têtes permettent aux utilisateurs de créer des applications à page unique qui autorisent les bibliothèques JavaScript côté client à valider la signature *id_token* en demandant les clés de signature du document de découverte Open ID Connect (OIDC) sur AD FS.

- AD FS inclut la prise en charge de la clé de preuve pour l'échange de code (PKCE) pour un flux de code d'authentification sécurisé dans le cadre d'OAuth. Cette couche de sécurité supplémentaire empêche les acteurs malveillants de détourner le code et de le rejouer à partir d'un autre client.

- Nous avons corrigé un problème mineur qui faisait que AD FS n'envoyait que la réclamation x5t. Désormais, AD FS envoie également une réclamation kid pour indiquer l'indice d'identification de la clé pour la vérification de la signature.

Supportability improvements

Les administrateurs peuvent désormais configurer AD FS pour permettre aux utilisateurs de leur envoyer des rapports d'erreur et des journaux de débogage sous la forme d'un fichier ZIP à des fins de dépannage. Les administrateurs peuvent également configurer une connexion SMTP (Simple Mail Transfer Protocol) pour envoyer automatiquement le fichier ZIP à un compte de messagerie de triage. Un autre paramètre permet aux administrateurs de créer automatiquement un ticket pour leur système d'assistance sur la base de ce courrier électronique.

Deployment updates

Les mises à jour de déploiement suivantes sont maintenant incluses dans AD FS 2019 :

- AD FS dispose d'une fonction similaire à sa version Windows Server 2016 qui facilite la mise à niveau des fermes de serveurs Windows Server 2016 en fermes de serveurs Windows Server 2019. Un serveur Windows Server 2019 ajouté à une batterie de serveurs Windows Server 2016 se comportera uniquement comme un serveur Windows Server

2016 jusqu'à ce que vous soyez prêt à le mettre à niveau. Pour plus d'informations, consultez Mise à niveau vers AD FS dans Windows Server 2016.

SAML updates

AD FS 2019 inclut les mises à jour SAML (Security Assertion Markup Language) suivantes :

- Nous avons corrigé des problèmes dans la prise en charge des fédérations agrégées, telles que InCommon, dans ces domaines :
  - Amélioration de la mise à l'échelle pour de nombreuses entités dans le document de métadonnées de la fédération agrégée. Auparavant, la mise à l'échelle de ces entités échouait et renvoyait un message d'erreur ADMIN0017.
  - Vous pouvez désormais effectuer des requêtes à l'aide du paramètre *ScopeGroupID* en exécutant la `Get-AdfsRelyingPartyTrustsGroup` cmdlet PowerShell.
  - Amélioration de la gestion des conditions d'erreur en cas de duplication des valeurs de *entityID*.

Spécification de ressource de style Azure AD dans le paramètre d'étendue

Auparavant, AD FS exigeait que la ressource et l'étendue souhaitées se trouvent dans un paramètre distinct dans toute requête d'authentification. Par exemple, la requête OAuth suivante contient un paramètre scope :

```HTTP
https://fs.contoso.com/adfs/oauth2/authorize?
response_type=code&client_id=claimsxrayclient&resource=urn:microsoft:adfs:claimsxr
ay&scope=oauth&redirect_uri=https://adfshelp.microsoft.com/
ClaimsXray/TokenResponse&prompt=login
```

Avec AD FS sur Windows Server 2019, vous pouvez désormais passer la valeur de la ressource incorporée dans le paramètre d'étendue. Ce changement est cohérent avec l'authentification contre Microsoft Entra ID.

Le paramètre scope peut maintenant être organisé comme une liste séparée par des espaces qui structure chaque entité comme une ressource ou un scope.

> ⓘ **Notes**

Vous ne pouvez spécifier qu'une seule ressource dans la demande d'authentification. Si vous incluez plus d'une ressource dans la demande, AD FS renvoie une erreur et l'authentification n'aboutit pas.

Nouveautés de Windows Server 2016

08/04/2025S’applique à: ✅ Windows Server 2016

Cet article décrit les nouvelles fonctionnalités de Windows Server 2016 qui sont susceptibles d'avoir l'impact le plus important lorsque vous utilisez cette version.

Calcul

La zone Virtualisation contient des fonctionnalités et produits de virtualisation que les professionnels de l’informatique peuvent utiliser pour la conception, le déploiement et la maintenance de Windows Server.

Général

Les machines physiques et virtuelles bénéficient d’une plus grande précision du temps en raison des améliorations apportées aux services Synchronisation date/heure de Hyper-V et de Win32. Windows Server peut désormais héberger des services qui sont conformes aux réglementations à venir qui exigent une précision égale à 1 ms en ce qui concerne l’heure UTC.

Hyper-V

La virtualisation du réseau Hyper-V (HNV) est un élément fondamental de la nouvelle solution SDN (Software Defined Networking) de Microsoft et est entièrement intégrée dans la pile SDN. Windows Server 2016 inclut les changements suivants pour Hyper-V :

- Windows Server 2016 inclut désormais un commutateur Hyper-V programmable. Le contrôleur de réseau de Microsoft pousse les stratégies HNV vers le bas jusqu'à un agent d'hôte qui s'exécute sur chaque hôte en utilisant le protocole de gestion de base de données Open vSwitch (OVSDB) en tant qu'interface SouthBound (SBI). L’agent hôte stocke cette stratégie à l’aide d’une personnalisation du schéma VTEP et programme des règles de flux complexes dans un moteur de flux performant dans le commutateur Hyper-V. Le moteur de flux du commutateur Hyper-V est le même que celui utilisé par Azure. L'ensemble de la pile SDN, jusqu'au contrôleur réseau et au fournisseur de ressources réseau, est également conforme à Azure, ce qui rend ses performances comparables à celles du cloud public Azure. Dans le moteur de flux de Microsoft, le commutateur Hyper-V est équipé pour gérer les règles de flux avec et sans état par le biais d'un simple mécanisme de correspondance qui définit comment les paquets doivent être traités dans le commutateur.

- HNV prend désormais en charge l'encapsulation du protocole Virtual eXtensible Local Area Network (VXLAN). HNV utilise le protocole VXLAN en mode de distribution MAC par l'intermédiaire du contrôleur de réseau Microsoft pour mapper les adresses IP du réseau global du locataire aux adresses IP du réseau physique sous-jacent. Les décharges de tâches NVGRE et VXLAN prennent en charge des pilotes tiers pour améliorer les performances.

- Windows Server 2016 inclut un équilibreur de charge logiciel (SLB) avec une prise en charge complète du trafic de réseau virtuel et une interaction transparente avec HNV. Le moteur de flux performant met en œuvre le SLB dans le v-Switch du plan de données, puis le contrôleur de réseau le contrôle pour les mappages IP virtuels (VIP) ou IP dynamiques (DIP).

- HNV implémente des en-têtes Ethernet L2 corrects pour garantir l'interopérabilité avec des appliances virtuelles et physiques tierces qui dépendent de protocoles standard du secteur. Microsoft s'assure que tous les paquets transmis ont des valeurs conformes dans tous les champs pour garantir l'interopérabilité. HNV nécessite la prise en charge des trames Jumbo (MTU > 1780) dans le réseau physique L2 pour tenir compte de la surcharge des paquets introduite par les protocoles d'encapsulation tels que NVGRE et VXLAN. La prise en charge des trames Jumbo garantit que les machines virtuelles invitées attachées à un réseau virtuel HNV conservent une MTU de 1514.

- La prise en charge des conteneurs Windows ajoute des améliorations de performance, une gestion simplifiée du réseau et une prise en charge des conteneurs Windows sur Windows 10. Pour plus d'informations, consultez notre documentation sur les conteneurs Windows et les conteneurs : Docker, Windows et les tendances.

- Hyper-V est désormais compatible avec Connected Standby. Lorsque vous installez le rôle Hyper-V sur un ordinateur qui utilise le modèle d'alimentation Always On/Always Connected (AOAC), vous pouvez désormais le configurer pour qu'il utilise l'état d'alimentation Connected Standby.

- L'attribution de périphériques discrets vous permet de donner à une machine virtuelle (VM) un accès direct et exclusif à certains périphériques matériels PCIe. Cette fonctionnalité contourne la pile de virtualisation Hyper-V, ce qui permet un accès plus rapide. Pour plus d'informations, voir Affectation de périphériques discrets et Affectation de périphériques discrets - Description et contexte.

- Hyper-V prend désormais en charge le chiffrement de lecteur BitLocker pour les disques de système d'exploitation dans les machines virtuelles de génération 1. Cette méthode de protection remplace les modules TPM (Trusted Platform Modules) virtuels, qui ne sont disponibles que dans les machines virtuelles de génération 2. Pour décrypter le disque et démarrer la VM, l'hôte Hyper-V doit soit faire partie d'une structure surveillée autorisée,

soit disposer de la clé privée de l'un des gardiens de la VM. Le stockage des clés nécessite une VM version 8. Pour plus d'informations, reportez-vous à la section Mise à niveau de la version de la machine virtuelle dans Hyper-V sur Windows ou Windows Server.

- La protection des ressources de l'hôte empêche les machines virtuelles d'utiliser trop de ressources système en surveillant les niveaux d'activité excessifs. Lorsque la surveillance détecte un niveau d'activité anormalement élevé dans une VM, elle limite la quantité de ressources consommées par la VM. Vous pouvez activer cette fonctionnalité en exécutant la cmdlet Set-VMProcessor dans PowerShell.

- Vous pouvez maintenant utiliser l'ajout ou la suppression à chaud pour ajouter ou supprimer des cartes réseau pendant l'exécution de la machine virtuelle sans temps d'arrêt dans les machines virtuelles de génération 2 exécutant Linux ou Windows OS. Vous pouvez également ajuster la quantité de mémoire affectée à une machine virtuelle pendant son exécution même si la mémoire dynamique n'est pas activée sur les machines virtuelles de génération 1 et 2 exécutant Windows Server 2016 et versions ultérieures ou Windows 10 et ultérieures.

- Hyper-V Manager prend désormais en charge les fonctionnalités suivantes :

  - Les informations d'identification alternatives, qui vous permettent d'utiliser un ensemble différent d'informations d'identification dans Hyper-V Manager lors de la connexion à un autre hôte distant Windows Server 2016 ou Windows 10. Vous pouvez également enregistrer ces informations d'identification pour faciliter la connexion.

  - Vous pouvez désormais gérer Hyper-V sur des machines exécutant Windows Server 2012 R2, Windows Server 2012, Windows 8.1 et Windows 8.

  - Hyper-V Manager communique désormais avec les hôtes Hyper-V distants à l'aide du protocole WS-MAN, qui permet l'authentification CredSSP, Kerberos et NTLM. Lorsque vous utilisez CredSSP pour vous connecter à un hôte Hyper-V distant, vous pouvez effectuer une migration en direct sans activer la délégation restreinte dans Active Directory. WS-MAN facilite également l'activation des hôtes pour la gestion à distance. WS-MAN se connecte par le biais du port 80 qui est ouvert par défaut.

- Les mises à jour des services d'intégration pour les invités Windows sont désormais distribuées via Windows Update. Les fournisseurs de services et les hôtes de nuages privés peuvent donner aux locataires qui possèdent les machines virtuelles le contrôle de l'application des mises à jour. Les locataires Windows peuvent désormais mettre à jour leurs machines virtuelles avec toutes les dernières mises à jour par le biais d'une méthode unique. Pour plus d'informations sur la façon dont les locataires Linux peuvent utiliser les services d'intégration, consultez Machines virtuelles Linux et FreeBSD prises en charge pour Hyper-V sur Windows Server et Windows.

> **ⓘ Important**
>
> Hyper-V pour Windows Server 2016 n'inclut plus le fichier image vmguest.iso car il n'est plus nécessaire.

- Les systèmes d'exploitation Linux s'exécutant sur des machines virtuelles de génération 2 peuvent désormais démarrer avec l'option Démarrage sécurisé activée. Les systèmes d'exploitation qui prennent en charge le démarrage sécurisé sur les hôtes Windows Server 2016 incluent Ubuntu 14.04 et versions ultérieures, SUSE Linux Enterprise Server 12 et versions ultérieures, Red Hat Enterprise Linux 7.0 et versions ultérieures, et CentOS 7.0 et versions ultérieures. Avant de démarrer la VM pour la première fois, vous devez la configurer pour qu'elle utilise l'autorité de certification Microsoft UEFI dans Hyper-V Manager, Virtual Machine Manager ou en exécutant la cmdlet Set-VMFirmware dans PowerShell.

- Les machines virtuelles de génération 2 et les hôtes Hyper-V peuvent désormais utiliser plus de mémoire et de processeurs virtuels. Vous pouvez également configurer les hôtes avec plus de mémoire et de processeurs virtuels que les versions précédentes. Ces modifications prennent en charge des scénarios tels que l'exécution de grandes bases de données en mémoire pour le traitement des transactions en ligne (OLTP) et l'entreposage de données (DW) pour le commerce électronique. Pour plus d'informations, consultez les performances des VM Windows Server 2016 Hyper-V à grande échelle pour le traitement des transactions en mémoire. Pour en savoir plus sur la compatibilité des versions et les configurations maximales prises en charge, consultez Mettre à niveau la version de machine virtuelle dans Hyper-V sur Windows ou Windows Server et planifier l'évolutivité Hyper-V dans Windows Server.

- La fonction de virtualisation imbriquée vous permet d'utiliser une VM comme hôte Hyper-V et de créer des VM au sein de l'hôte virtualisé. Vous pouvez utiliser cette fonctionnalité pour créer des environnements de développement et de test exécutant au moins Windows Server 2016 ou Windows 10 avec un processeur compatible Intel VT-x. Pour plus d'informations, consultez la section Qu'est-ce que la virtualisation imbriquée ?

- Vous pouvez désormais configurer des points de contrôle de production pour vous conformer aux politiques de support des VM exécutant des charges de travail de production. Ces points de contrôle s'exécutent sur la technologie de sauvegarde à l'intérieur du périphérique invité au lieu d'un état sauvegardé. Les machines virtuelles Windows utilisent le service de cliché instantané de volume (VSS), tandis que les machines virtuelles Linux rincent les tampons du système de fichiers pour créer des points de contrôle cohérents avec le système de fichiers. Vous pouvez toujours utiliser des points de contrôle basés sur des états sauvegardés en utilisant des points de contrôle standard à

la place. Pour plus d'informations, voir Choisir entre les points de contrôle standard ou de production dans Hyper-V.

> ⓘ **Important**
>
> Les nouvelles machines virtuelles utilisent les points de contrôle de production par défaut.

- Vous pouvez désormais redimensionner les disques durs virtuels partagés (fichiers `.vhdx`) pour le clustering invité sans temps d'arrêt. Vous pouvez également utiliser les clusters invités pour protéger les disques durs virtuels partagés en utilisant Hyper-V Replica pour la reprise après sinistre. Vous ne pouvez utiliser cette fonctionnalité que sur les collections d'un cluster invité pour lequel vous avez activé la réplication via Windows Management Instrumentation (WMI). Pour plus d'informations, voir la classe Msvm_CollectionReplicationService et la présentation du partage des disques durs virtuels.

  > ⓘ **Notes**
  >
  > La gestion de la réplication d'une collection n'est pas possible via des applets de commande PowerShell ou à l'aide de l'interface WMI.

- Lors de la sauvegarde d'une seule machine virtuelle, nous ne recommandons pas l'utilisation d'un groupe de VM ou d'une collection d'instantanés, que l'hôte soit en cluster ou non. Ces options sont destinées à la sauvegarde de clusters d'invités qui utilisent un vhdx partagé. Nous vous recommandons plutôt de prendre un instantané à l'aide du fournisseur Hyper-V WMI (V2).

- Vous pouvez désormais créer des machines virtuelles Hyper-V protégées qui incluent des fonctionnalités pour empêcher Hyper-V administrateurs sur l'hôte ou les programmes malveillants d'inspecter ou de falsifier l'état de la machine virtuelle protégée. Ces fonctionnalités protègent également contre le vol de données à partir de l'état de machine virtuelle protégée. Les données et l'état sont cryptés afin que les administrateurs Hyper-V ne puissent pas voir la sortie vidéo et les disques disponibles. Vous pouvez également limiter les machines virtuelles à s'exécuter uniquement sur les hôtes qu'un serveur Guardian de l'hôte détermine comme sains et fiables. Pour plus d'informations, consultez Présentation de l'infrastructure protégée et des machines virtuelles dotées d'une protection maximale.

  > ⓘ **Notes**

Les machines virtuelles blindées sont compatibles avec Hyper-V Replica. Pour répliquer une machine virtuelle blindée, vous devez autoriser l'hôte que vous souhaitez répliquer à exécuter cette VM blindée.

- La fonction de priorité de l'ordre de démarrage des machines virtuelles en grappe vous permet de mieux contrôler les VM en grappe qui démarrent ou redémarrent en premier. La priorité de l'ordre de démarrage vous permet de démarrer les machines virtuelles qui fournissent des services avant les machines virtuelles qui utilisent ces services. Vous pouvez définir des ensembles, ajouter des machines virtuelles aux ensembles et spécifier des dépendances à l'aide de cmdlets PowerShell telles que New-ClusterGroupSet, Get-ClusterGroupSet et Add-ClusterGroupSetDependency.

- Les fichiers de configuration de la machine virtuelle utilisent désormais le format d'extension de fichier `.vmcx` tandis que les fichiers de données d'état d'exécution utilisent le format d'extension de fichier `.vmrs`. Ces nouveaux formats de fichiers sont conçus pour permettre une lecture et une écriture plus efficaces. Ils réduisent également la probabilité de corruption des données en cas de défaillance du stockage.

  > **ⓘ Important**
  >
  > L'extension du nom de fichier `.vmcx` indique qu'il s'agit d'un fichier binaire. Hyper-V pour Windows Server 2016 ne prend pas en charge la modification des fichiers `.vmcx` ou `.vmrs`.

- Nous avons mis à jour la compatibilité de la version avec les VM de la version 5. Ces VM sont compatibles avec Windows Server 2012 R2 et Windows Server 2016. Cependant, les VM de la version 5 compatibles avec Windows Server 2019 ne peuvent s'exécuter que sur Windows Server 2016, et non sur Windows Server 2012 R2. Si vous déplacez ou importez une VM Windows Server 2012 R2 vers un serveur exécutant une version ultérieure de Windows Server, vous devez mettre à jour manuellement la configuration de la VM pour utiliser les fonctionnalités des versions ultérieures de Windows Server. Pour plus d'informations sur la compatibilité des versions et les fonctionnalités mises à jour, voir Mise à niveau de la version de la machine virtuelle dans Hyper-V sur Windows ou Windows Server.

- Vous pouvez désormais utiliser les fonctions de sécurité basées sur la virtualisation pour les machines virtuelles de génération 2, telles que Device Guard et Credential Guard, afin de protéger votre système d'exploitation contre les exploits de logiciels malveillants. Ces fonctionnalités sont disponibles dans les machines virtuelles exécutant la version 8 ou

une version ultérieure. Pour plus d'informations, reportez-vous à la section Mise à niveau de la version de la machine virtuelle dans Hyper-V sur Windows ou Windows Server.

- Vous pouvez désormais exécuter des cmdlets à l'aide de Windows PowerShell Direct pour configurer votre VM à partir de la machine hôte, ce qui constitue une alternative à VMConnect ou Remote PowerShell. Vous n'avez pas besoin de répondre à des exigences en matière de réseau ou de pare-feu, ni de disposer d'une configuration spéciale de gestion à distance pour commencer à l'utiliser. Pour plus d'informations, voir Gérer les machines virtuelles Windows avec PowerShell Direct.

Nano Server

Nano Server inclut désormais un module mis à jour pour la création d'images Nano Server. Cette mise à jour offre une séparation des fonctionnalités de machine virtuelle hôte physique et invité et ajoute la prise en charge des différentes éditions de Windows Server. Pour plus d'informations, voir Installer Nano Server.

Des améliorations ont également été apportées à la console de récupération, notamment la séparation des règles de pare-feu entrantes et sortantes ainsi que la possibilité de réparer la configuration de WinRM.

Machines virtuelles dotées d'une protection maximale

Windows Server 2016 fournit une nouvelle machine virtuelle Hyper-V dotée d'une protection maximale, pour protéger une machine virtuelle de deuxième génération contre une structure compromise. Voici quelques-unes des principales fonctionnalités introduites dans Windows Server 2016 :

- Un nouveau mode **Chiffrement pris en charge** qui offre plus de protections que pour une machine virtuelle ordinaire, mais moins que le mode **Protection maximale**, tout en prenant toujours en charge le module de plateforme sécurisée (TPM) virtuel, le chiffrement de disque, le chiffrement de trafic de migration dynamique et d'autres fonctionnalités, notamment les avantages d'administration de structure directe tels que les connexions de console de machine virtuelle et PowerShell Direct.

- Prise en charge complète de la conversion de machines virtuelles de génération 2 non protégées existantes en machines virtuelles dotées d'une protection maximale, dont le chiffrement automatique du disque.

- Hyper-V Virtual Machine Manager peut désormais afficher les structures sur lesquelles une machine virtuelle dotée d'une protection maximale peut s'exécuter, ce qui permet à l'administrateur de la structure d'ouvrir le protecteur de clé d'une machine virtuelle dotée

d’une protection maximale et d’afficher les structures sur lesquelles l’exécution est autorisée.

- Vous pouvez changer les modes d’attestation sur un Host Guardian Service en fonctionnement. Vous pouvez maintenant basculer sur-le-champ entre l’attestation Active Directory moins sécurisée, mais plus simple, et l’attestation basée sur le module de plateforme sécurisée.

- Des outils de diagnostic de bout en bout basés sur Windows PowerShell qui sont en mesure de détecter des problèmes de configuration ou des erreurs à la fois dans les hôtes Hyper-V protégés et le service Guardian hôte.

- Un environnement de récupération qui offre un moyen de résoudre les problèmes des machines virtuelles dotées d’une protection maximale et de les réparer en toute sécurité au sein de la structure dans laquelle elles s’exécutent normalement tout en offrant le même niveau de protection que la machine virtuelle dotée d’une protection maximale elle-même.

- Le service Guardian de l'hôte prend en charge un Active Directory existant et sécurisé : vous pouvez demander au service Guardian de l'hôte d’utiliser une forêt Active Directory existante comme son propre Active Directory, au lieu de créer sa propre instance Active Directory.

Pour plus d’informations et d’instructions sur l’utilisation des machines virtuelles dotées d’une protection maximale, consultez Structure protégée et machines virtuelles dotées d’une protection maximale.

Identité et accès

De nouvelles fonctionnalités d'identité améliorent la capacité des organisations à sécuriser les environnements Active Directory et leur permettent de migrer vers les déploiements de cloud uniquement et les déploiements hybrides, où certains services et applications sont hébergés dans le cloud et d'autres en local.

Services de certificats Active Directory

Les services de certificats Active Directory (AD CS) dans Windows Server 2016 améliorent la prise en charge de l’attestation de clé de module de plateforme sécurisée (TPM) : vous pouvez maintenant utiliser le fournisseur de stockage de clés de carte à puce pour l’attestation de clé, et les appareils qui ne sont pas joints au domaine peuvent maintenant utiliser l’inscription NDES pour obtenir des certificats qui peuvent être attestés pour des clés présentes dans un module de plateforme sécurisée (TPM).

Gestion des accès privilégiés

La gestion des accès privilégiés (PAM) permet d'atténuer les problèmes de sécurité dans les environnements Active Directory qui sont causés par des techniques de vol d'informations d'identification telles que le hachage, le hameçonnage de lance, etc. Vous pouvez configurer cette nouvelle solution d'accès administratif à l'aide de Microsoft Identity Manager (MIM). Elle présente les fonctionnalités suivantes :

- La forêt bastion Active Directory, approvisionnée par MIM, a une relation d'approbation spéciale PAM avec une forêt existante. Les forêts bastion constituent un nouveau type d'environnement Active Directory, à l'abri de toute activité malveillante, car elles sont isolées des forêts existantes et n'autorisent l'accès qu'aux comptes privilégiés.

- Nouveaux processus dans MIM pour demander des privilèges administratifs, y compris de nouveaux flux de travail pour l'approbation des requêtes.

- Nouveaux principaux de sécurité d'ombre (ou groupes) approvisionnés dans la forêt bastion par MIM en réponse aux demandes de privilèges d'administration. Les groupes de sécurité fantôme ont un attribut qui fait référence au SID d'un groupe d'administration dans une forêt existante. Cela permet au groupe d'ombres d'accéder aux ressources dans des forêts existantes sans modifier les listes de contrôle d'accès.

- Fonctionnalité de liens arrivant à expiration qui permet aux utilisateurs de rejoindre temporairement un groupe d'ombres pendant une durée spécifiée, ce qui leur permet d'effectuer des tâches administratives. La durée d'appartenance est contrôlée par une valeur de durée de vie (TTL), qui détermine également la période de validité du ticket Kerberos.

  > ⓘ **Notes**
  >
  > Les liens arrivant à expiration sont disponibles sur tous les attributs liés. Toutefois, seule la relation d'attribut lié *member/memberOF* entre un groupe et un utilisateur est préconfigurée avec PAM pour utiliser la fonctionnalité de liens arrivant à expiration.

- Les améliorations intégrées des contrôleurs de domaine Kerberos (KDC) dans les contrôleurs de domaine Active Directory permettent de restreindre la durée de vie des tickets Kerberos à la valeur TTL la plus basse possible lorsque les utilisateurs ont plusieurs adhésions temporaires à des groupes d'administration. Par exemple, si vous appartenez à un groupe **A** limité dans le temps, lorsque vous vous authentifiez, la durée de vie du ticket TGT (Ticket-granting ticket) Kerberos est égale au temps qu'il vous reste dans le groupe **A**. Si vous rejoignez également un autre groupe **B** limité dans le temps, dont la

durée de vie est inférieure à celle du groupe **A**, la durée de vie du TGT est égale au temps qu'il vous reste dans le groupe **B**.

- De nouvelles fonctionnalités de surveillance vous permettent d'identifier les utilisateurs qui ont demandé un accès, les accès que les administrateurs leur ont accordés et les activités qu'ils ont effectuées lorsqu'ils étaient connectés.

Pour en savoir plus sur les PAM, consultez Privileged Access Management for Active Directory Domain Services.

Jonction Microsoft Entra

La jonction Microsoft Entra améliore les expériences d'identité pour les clients de l'entreprise, du commerce et de l'éducation, et inclut des fonctionnalités améliorées pour les appareils professionnels et personnels.

- Les paramètres modernes sont désormais disponibles sur les appareils Windows appartenant à l'entreprise. Les fonctionnalités de Core Windows ne nécessitent plus de compte Microsoft personnel : elles s'exécutent désormais à partir des comptes professionnels existants des utilisateurs pour garantir la conformité. Ces services fonctionnent sur les PC qui sont joints à un domaine Windows local, ainsi que les appareils qui sont « joints » à Microsoft Entra. Il s'agit notamment des paramètres suivants :
  - Itinérance ou personnalisation, paramètres d'accessibilité et informations d'identification
  - Sauvegarde et restauration
  - Accès au Microsoft Store avec votre compte professionnel
  - Vignettes dynamiques et notifications
- Accès aux ressources organisationnelles sur des appareils mobiles, notamment des téléphones et des tablettes, qui ne peuvent pas être joints à un domaine Windows, qu'ils appartiennent à une entreprise ou qu'ils soient BYOD.
- Utilisez une authentification unique (SSO) pour Office 365 et d'autres applications, sites web et ressources de l'organisation.
- Sur les appareils BYOD, ajoutez un compte professionnel à partir d'un domaine local ou d'Azure AD à un appareil appartenant à un utilisateur. Vous pouvez utiliser le SSO pour accéder aux ressources professionnelles, via les applications et sur le Web, de manière à

garantir la conformité avec les nouvelles fonctionnalités telles que le contrôle de compte conditionnel et l'attestation d'intégrité de l'appareil.

- L'intégration de la gestion des appareils mobiles (MDM) vous permet d'inscrire automatiquement des appareils à votre outil de gestion des appareils mobiles (MDM) (Microsoft Intune ou tiers).
- Configurer le mode « kiosque » et les appareils partagés pour plusieurs utilisateurs de votre organisation.
- L'expérience des développeurs vous permet de créer des applications qui s'adressent aux contextes d'entreprise et personnels avec une pile de programmation partagée.
- L'option d'acquisition d'images vous permet de choisir entre la création d'images et permettre à vos utilisateurs de configurer des appareils appartenant à l'entreprise directement pendant l'expérience de première exécution.

Windows Hello Entreprise

Windows Hello Entreprise est une approche d'authentification basée sur la clé pour les organisations et les consommateurs qui ne nécessite pas de passer par un mot de passe. Cette forme d'authentification repose sur des informations d'identification qui sont résistantes aux violations, au vol et au hameçonnage.

L'utilisateur se connecte à l'appareil à l'aide d'un identifiant biométrique ou d'un code PIN lié à un certificat ou à une paire de clés asymétriques. Les fournisseurs d'identité valident l'utilisateur en mappant la clé publique de l'utilisateur à IDLocker et fournit des informations de connexion via un mot de passe à usage unique (OTP), par téléphone ou un autre mécanisme de notification.

Pour plus d'informations, voir Windows Hello for Business.

Dépréciation des niveaux fonctionnels du service de réplication de fichiers (FRS) et de Windows Server 2003

Bien que le service de réplication de fichiers et les niveaux fonctionnels de Windows Server 2003 soient déconseillés dans les versions précédentes de Windows Server, nous souhaitons vous rappeler qu'AD DS ne prend plus en charge le système d'exploitation Windows Server 2003. Vous devez donc supprimer du domaine tous les contrôleurs de domaine qui exécutent Windows Server 2003. Vous devez également élever le niveau fonctionnel du domaine et de la forêt au moins à Windows Server 2008.

Aux niveaux fonctionnels de domaine Windows Server 2008 et supérieurs, AD DS utilise la réplication DFS (Distributed File Service) pour répliquer le contenu du dossier SYSVOL entre les contrôleurs de domaine. Si vous créez un domaine au niveau fonctionnel de domaine Windows Server 2008 ou supérieur, la réplication DFS réplique automatiquement le dossier SYSVOL. Si vous avez créé le domaine à un niveau fonctionnel inférieur, vous devez passer de l'utilisation de FRS à la réplication DFS pour le fichier SYSVOL. Pour obtenir des étapes de migration plus détaillées, consultez Installer, mettre à niveau ou migrer vers Windows Server.

Pour plus d'informations, consultez les ressources suivantes :

- Présentation des niveaux fonctionnels des services de domaine Active Directory (AD DS)
- Comment élever les niveaux fonctionnels du domaine et de la forêt Active Directory

Services de fédération Active Directory (AD FS)

Les services AD FS de Windows Server 2016 incluent de nouvelles fonctionnalités qui vous permettent de configurer AD FS pour authentifier les utilisateurs stockés dans les annuaires LDAP (Lightweight Directory Access Protocol).

Proxy d'application web

La dernière version du Proxy d'application Web se concentre sur les nouvelles fonctionnalités qui permettent la publication et la préauthentification d'applications supplémentaires et améliorent l'expérience utilisateur. Consultez la liste complète des nouvelles fonctionnalités qui incluent la pré-authentification pour les applications clientes enrichies telles qu'Exchange ActiveSync et les domaines génériques pour faciliter la publication d'applications SharePoint. Pour plus d'informations, consultez Proxy d'application web dans Windows Server 2016.

Administration

La section Gestion et automatisation fournit des informations sur les outils et références pour les professionnels de l'informatique qui souhaitent exécuter et gérer Windows Server 2016, dont Windows PowerShell.

Windows PowerShell 5.1 contient de nouvelles fonctionnalités importantes, notamment la prise en charge du développement avec les classes, et de nouvelles fonctionnalités de sécurité, qui étendent son utilisation, améliorent sa convivialité, et vous permettent de contrôler et de gérer des environnements Windows de façon plus simple et plus complète. Pour plus d'informations, consultez Nouveaux scénarios et nouvelles fonctionnalités dans WMF 5.1.

Les nouvelles fonctionnalités de Windows Server 2016 incluent la capacité d'exécuter PowerShell.exe localement sur Nano Server (et non plus seulement à distance), de nouvelles

applets de commande pour les utilisateurs et groupes locaux pour remplacer l'interface graphique, la prise en charge du débogage dans PowerShell, et dans Nano Server, la transcription et la journalisation de la sécurité, ainsi que la prise en charge de JEA.

Voici d'autres nouvelles fonctionnalités d'administration :

Configuration d'état souhaité Windows PowerShell (DSC) dans Windows Management Framework (WMF) 5

Windows Management Framework 5 inclut des mises à jour de configuration d'état souhaité Windows PowerShell (DSC), Windows Remote Management (WinRM) et Windows Management Instrumentation (WMI).

Pour plus d'informations sur le test des fonctionnalités DSC de Windows Management Framework 5, consultez la série de billets de blog mentionnés dans Valider les fonctionnalités de PowerShell DSC. Pour effectuer le téléchargement, consultez Windows Management Framework 5.1.

Gestion unifiée des packages PackageManagement pour la détection, l'installation et l'inventaire des logiciels

Windows Server 2016 et Windows 10 incluent une nouvelle fonctionnalité PackageManagement (auparavant appelée OneGet) qui permet aux professionnels de l'informatique ou développeurs d'automatiser la détection, l'installation et l'inventaire des logiciels, localement ou à distance, quels que soient la technologie d'installation utilisée et l'emplacement des logiciels.

Pour en savoir plus, voir https://github.com/OneGet/oneget/wiki.

Améliorations de PowerShell pour faciliter la forensique numérique et aider à réduire les violations de sécurité

Pour aider l'équipe responsable de l'examen des systèmes compromis, parfois appelée « l'équipe bleue », nous avons ajouté des fonctionnalités d'investigation numérique et de journalisation PowerShell supplémentaires ainsi que des fonctionnalités destinées à réduire les vulnérabilités dans les scripts, comme PowerShell limité et à sécuriser les API CodeGeneration.

Pour plus d'informations, consultez le billet de blog PowerShell ♥ the Blue Team.

Réseau

La section Mise en réseau décrit les fonctionnalités et produits de mise en réseau que les professionnels de l'informatique peuvent utiliser pour la conception, le déploiement et la maintenance de Windows Server 2016.

Mise en réseau définie par logiciel

La mise en réseau définie par logiciel (SDN) est une nouvelle solution SDDC (Centre de données définis par logiciel) qui inclut les fonctionnalités suivantes :

- Contrôleur de réseau, qui vous permet d'automatiser la configuration de l'infrastructure réseau au lieu d'effectuer une configuration manuelle des services et appareils réseau. Le contrôleur de réseau utilise Representational State Transfer (REST) sur son interface direction nord avec des charges utiles JavaScript Object Notation (JSON). L'interface direction sud du contrôleur de réseau utilise le protocole OVSDB (Open vSwitch Database Management).

- Nouvelles fonctionnalités pour Hyper-V :

  - Commutateur virtuel Hyper-V, qui vous permet de créer une commutation et un routage distribués, ainsi qu'une couche d'application de stratégie alignée et compatible avec Microsoft Azure. Pour en savoir plus, consultez Commutateur virtuel Hyper-V.

  - Accès direct à la mémoire à distance (RDMA) et switch-embedded teaming (SET) lorsque vous créez des commutateurs virtuels. Vous pouvez configurer RDMA sur les adaptateurs réseau liés à un commutateur virtuel Hyper-V, que vous utilisiez ou non SET. SET peut donner à vos commutateurs virtuels des capacités similaires à celles de l'agrégation de cartes réseau. Pour plus d'informations, consultez Configuration réseau requise pour Azure Local.

  - Les files d'attente multiples de machines virtuelles (VMMQ) améliorent le rendement des VMQ en allouant plusieurs files d'attente matérielles par VM. La file d'attente par défaut devient un ensemble de files d'attente pour une VM et répartit le trafic entre les files d'attente.

  - La qualité de service (QoS) pour les réseaux définis par logiciel gère la classe de trafic par défaut via le commutateur virtuel dans la bande passante de la classe par défaut.

- La virtualisation des fonctions réseau (NFV), qui vous permet de mettre en miroir ou d'acheminer des fonctions réseau exécutées par des appareils matériels vers des appareils virtuels, tels que des équilibreurs de charge, des pare-feu, des routeurs, des commutateurs, etc. Vous pouvez également déployer et gérer toute votre pile SDN à l'aide de System Center Virtual Machine Manager. Vous pouvez utiliser Docker pour gérer

la mise en réseau de conteneurs Windows Server et associer des stratégies de mise en réseau SDN à des machines virtuelles et à des conteneurs.

- Un pare-feu de centre de données qui fournit des listes de contrôle d'accès (ACL) granulaires, ce qui vous permet d'appliquer des stratégies de pare-feu au niveau de l'interface de la machine virtuelle ou du sous-réseau. Pour en savoir plus, consultez Qu'est-ce que le pare-feu de centre de données ?

- Passerelle RAS, qui vous permet d'acheminer le trafic entre des réseaux virtuels et des réseaux physiques, y compris les connexions VPN de site à site entre votre centre de données dans le cloud et les sites distants de vos locataires. Le protocole Border Gateway Protocol (BGP) vous permet de déployer et de fournir un routage dynamique entre les réseaux pour tous les scénarios de passerelles, y compris les réseaux privés virtuels (VPN) de site à site IKEv2 (Internet Key Exchange version 2), les VPN de couche 3 (L3) et les passerelles GRE (Generic Routing Encapsulation). Les passerelles prennent désormais également en charge les pools de passerelles et la redondance M+N. Pour en savoir plus, consultez Qu'est-ce qu'une passerelle de service d'accès à distance (RAS) pour une mise en réseau définie par logiciel ?

- L'équilibreur de charge logicielle (SLB) et la traduction d'adresses réseau (NAT) améliorent le débit en prenant en charge le retour direct du serveur. Ainsi, le trafic de retour du réseau peut contourner le multiplexeur d'équilibrage de charge et peut être réalisé à l'aide d'un équilibreur de charge de couche 4 nord-sud et est-ouest, et d'une NAT. Pour en savoir plus, consultez Qu'est-ce qu'un équilibreur de charge logicielle (SLB) pour SDN ? et la virtualisation de fonction réseau.

- Des technologies d'encapsulation flexibles qui fonctionnent au niveau du plan de données et prennent en charge à la fois Virtual Extensible LAN (VxLAN) et Network Virtualization Generic Routing Encapsulation (NVGRE).

Pour plus d'informations, consultez Planifier une mise en réseau SDN (Software Defined Networking).

Principes fondamentaux de la mise à l'échelle du cloud

Windows Server 2016 inclut les éléments fondamentaux suivants à l'échelle du cloud :

- Carte d'interface réseau (NIC) convergée, qui vous permet d'utiliser une seule carte réseau pour la gestion, le stockage compatible RDMA (Remote Direct Memory Access) et le trafic de locataires. Une carte d'interface réseau convergée réduit le coût de chaque serveur de votre centre de données, car elle nécessite moins de cartes réseau pour gérer différents types de trafic par serveur.

- Packet Direct fournit une infrastructure de traitement des paquets à faible latence et à débit de trafic réseau élevé.
- Switch Embedded Teaming (SET) est une solution d'association de cartes réseau intégrée au commutateur virtuel Hyper-V. SET permet d'associer jusqu'à huit cartes d'interface réseau physiques en une seule équipe SET, ce qui améliore la disponibilité et permet le basculement. Dans Windows Server 2016, vous pouvez créer des associations SET qui sont limitées à l'utilisation de Server Message Block (SMB) et RDMA. Vous pouvez également utiliser des équipes SET pour répartir le trafic réseau dans le cadre de la virtualisation de réseau Hyper-V. Pour plus d'informations, consultez Configuration réseau requise pour Azure Local.

Améliorations des performances de TCP

La fenêtre de congestion initiale par défaut (ICW) a augmenté de 4 à 10 et TCP Fast Open (TFO) est implémentée. TFO réduit le temps nécessaire pour établir une connexion TCP et la nouvelle fenêtre de congestion initiale permet de transférer des objets plus volumineux dans la rafale initiale. Cette combinaison réduit considérablement le temps nécessaire pour transférer un objet Internet entre le client et le cloud.

Pour améliorer le comportement de TCP en cas de récupération suite à une perte de paquets, TCP TLP (Tail Loss Probe) et RACK (Recent Acknowledgment) ont été implémentés. TLP permet de convertir des délais de retransmission en récupérations rapides, et RACK réduit le temps nécessaire à une récupération rapide pour retransmettre un paquet perdu.

Protocole DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP (Dynamic Host Configuration Protocol) présente les changements suivants dans Windows Server 2016 :

- À partir d Windows 10, version 2004, lorsque vous exécutez un client Windows et que vous vous connectez à Internet à l'aide d'un appareil Android en partage de connexion, les connexions sont désormais étiquetées comme mesurées. Le nom du fournisseur client traditionnel qui s'affichait comme MSFT 5.0 sur certains appareils Windows est maintenant MSFT 5.0 XBOX.
- À compter de Windows 10, version 1803, le client DHCP peut désormais lire et appliquer l'option 119, l'option de recherche de domaine, à partir du serveur DHCP auquel votre système se connecte. L'option de recherche de domaine fournit également des suffixes DNS (Domain Name Services) pour les recherches DNS de noms courts. Pour plus d'informations, consultez RFC 3397 .

- DHCP prend désormais en charge l'option 82 (sous-option 5). Vous pouvez utiliser cette option pour autoriser les clients proxy DHCP et les agents de relais à demander une adresse IP pour un sous-réseau spécifique. 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. Pour plus d'informations, consultez Options de sélection de sous-réseau DHCP.

- Nouveaux événements de journalisation pour les cas où les inscriptions d'enregistrements DNS échouent sur le serveur DNS. Pour en savoir plus, consultez Événements de journalisation DHCP pour les inscriptions DNS.

- Le rôle de serveur DHCP ne prend plus en charge la protection d'accès réseau (NAP). Les serveurs DHCP n'appliquent pas de stratégies NAP et les étendues DHCP ne peuvent pas être activées pour NAP. Les ordinateurs clients DHCP qui sont également des clients NAP envoient une instruction d'intégrité (SoH) avec la requête DHCP. Si le serveur DHCP exécute Windows Server 2016, ces requêtes sont traitées comme si aucun SoH n'était présent. Le serveur DHCP accorde un bail DHCP normal au client. Si les serveurs qui exécutent Windows Server 2016 sont des proxys RADIUS (Remote Authentication Dial-In User Service) qui transmettent les demandes d'authentification à un serveur de stratégie réseau (NPS) qui prend en charge NAP, le NPS évalue ces clients comme n'étant pas compatibles NAP, ce qui entraîne l'échec du traitement NAP. Pour en savoir plus sur NAP et son obsolescence, consultez Fonctionnalités supprimées ou obsolètes dans Windows Server 2012 R2.

Tunneling GRE

La passerelle RAS prend désormais en charge les tunnels GRE (Generic Routing Encapsulation) à haute disponibilité, pour les connexions de site à site, ainsi que la redondance M+N des passerelles. GRE est un protocole de tunneling léger qui encapsule une grande variété de protocoles de la couche réseau dans les liaisons point à point virtuelles sur un réseau d'interconnexion IP. Pour plus d'informations, consultez Tunneling GRE dans Windows Server 2016.

Gestion des adresses IP (IPAM)

L'IPAM présente les mises à jour suivantes :

- Gestion des adresses IP améliorée Les fonctionnalités IPAM sont améliorées pour les scénarios tels que la gestion des sous-réseaux IPv4 /32 /32 et IPv6 /128 et la recherche de sous-réseaux et plages d'adresses IP libres dans un bloc d'adresses IP.

- Vous pouvez maintenant exécuter l'applet de commande `Find-IpamFreeSubnet` pour rechercher les sous-réseaux disponibles pour l'allocation. Cette fonction n'alloue pas les sous-réseaux et signale uniquement leur disponibilité. Toutefois, vous pouvez diriger la sortie de l'applet de commande vers l'applet de commande `Add-IpamSubnet` pour créer un sous-réseau. Pour plus d'informations, consultez Find-IpamFreeSubnet.

- Vous pouvez maintenant exécuter l'applet de commande `Find-IpamFreeRange` pour rechercher les plages d'adresses IP disponibles dans un bloc IP, une longueur de préfixe et un nombre de sous-réseaux demandés. Cette applet de commande n'alloue pas la plage d'adresses IP, signale uniquement leur disponibilité. Toutefois, vous pouvez diriger la sortie vers l'applet de commande `AddIpamRange` pour créer la plage. Pour plus d'informations, consultez Find-IpamFreeRange.

- Gestion des services DNS améliorée :

  - Collection d'enregistrements de ressources DNS pour les serveurs DNS non DNSSEC.

  - Configuration des propriétés et des opérations sur tous les types d'enregistrements de ressources non DNSSEC.

  - Gestion des zones DNS pour les serveurs DNS intégrés dans Active Directory et les serveurs DNS adossés à des fichiers. Vous pouvez gérer tous les types de zones DNS, notamment les zones principales, secondaires et de stub.

  - Déclenchez des tâches sur les zones secondaires et les zones de stub, qu'il s'agisse de zones de recherche directe ou inversée.

  - Contrôle d'accès basé sur les rôles pour les configurations DNS prises en charge pour les enregistrements et les zones.

  - Redirecteurs conditionnels

- Gestion intégrée du service DNS, du protocole DHCP et des adresses IP (DDI). Vous pouvez maintenant afficher tous les enregistrements de ressources DNS associés à une adresse IP dans l'inventaire des adresses IP. Vous pouvez également conserver automatiquement les enregistrements de pointeurs (PTR) des adresses IP et gérer les cycles de vie des adresses IP pour les opérations DNS et DHCP.

- Support pour plusieurs forêts Active Directory. Vous pouvez utiliser l'IPAM pour gérer les serveurs DNS et DHCP de plusieurs forêts Active Directory lorsqu'il existe une relation d'approbation bidirectionnelle entre la forêt dans laquelle vous avez installé l'IPAM et chacune des forêts distantes. Pour en savoir plus, consultez Gérer les ressources dans plusieurs forêts Active Directory.

- La fonctionnalité « Supprimer définitivement les données d'utilisation » vous permet de réduire la taille de la base de données IPAM en supprimant les anciennes données d'utilisation IP. Spécifiez simplement une date et l'IPAM supprime toutes les entrées de base de données antérieures ou égales à la date que vous avez entrée. Pour plus d'informations, consultez Purge Utilization Data.

- Vous pouvez désormais utiliser le contrôle d'accès en fonction du rôle (RBAC) pour définir des étendues d'accès pour les objets IPAM dans PowerShell. Pour plus d'informations, consultez Gérer le contrôle d'accès basé sur les rôles avec Windows PowerShell et des applets de commande de serveur de gestion des adresses IP (IPAM) dans Windows PowerShell.

Pour plus d'informations, consultez Gérer IPAM.

Sécurité et assurance

La section Sécurité et assurance contient des fonctionnalités et solutions de sécurité pour professionnels de l'informatique à déployer dans votre environnement de centre de données et cloud. Pour plus d'informations générales sur la sécurité dans Windows Server 2016, consultez Sécurité et assurance.

Just Enough Administration (JEA)

JEA dans Windows Server 2016 est une technologie de sécurité qui permet l'administration déléguée pour tout ce qui peut être géré avec Windows PowerShell. Les fonctionnalités disponibles incluent la prise en charge de l'exécution sous une identité réseau, la connexion par le biais PowerShell Direct, la copie de manière sécurisée de fichiers vers/depuis des points de terminaison JEA (Just Enough Administration) et la configuration de la console PowerShell pour un lancement dans un contexte JEA par défaut. Pour en savoir plus, consultez JEA sur GitHub.

Protection des informations d'identification

La protection des informations d'identification utilise une sécurité basée sur la virtualisation pour isoler les secrets, afin que seuls les logiciels système privilégiés puissent y accéder. Pour plus d'informations, consultez la section Protéger les informations d'identification de domaine dérivées avec Credential Guard.

Credential Guard pour Windows Server 2016 inclut les mises à jour suivantes pour les sessions utilisateur connectées :

- Kerberos et New Technology LAN Manager (NTLM) utilisent la sécurité basée sur la virtualisation pour protéger les secrets Kerberos et NTLM pour les sessions utilisateur connectées.
- Credential Manager protège les identifiants de domaine enregistrés à l'aide d'une sécurité basée sur la virtualisation. Les informations d'identification signées et les informations d'identification de domaine enregistrées ne sont pas transmises aux hôtes distants utilisant Remote Desktop.
- Vous pouvez activer Credential Guard sans verrou UEFI (Unified Extensible Firmware Interface).

Protection des informations d'identification à distance

Protection des informations d'identification prend en charge les sessions RDP afin que les informations d'identification de l'utilisateur restent côté client et ne soient pas exposées côté serveur. Il fournit également l'authentification unique pour Bureau à distance. Pour plus d'informations, consultez Protéger les informations d'identification de domaine dérivées avec Windows Defender Credential Guard.

Remote Credential Guard pour Windows Server 2016 inclut les mises à jour suivantes pour les utilisateurs connectés :

- Remote Credential Guard conserve les secrets des informations d'identification Kerberos et NTLM des utilisateurs connectés sur l'appareil client. Toute requête d'authentification de l'hôte distant pour évaluer les ressources du réseau en tant qu'utilisateur nécessite que l'appareil client utilise les secrets.
- Remote Credential Guard protège les informations d'identification fournies par l'utilisateur lors de l'utilisation du bureau à distance.

Protections de domaine

Les protections de domaine nécessitent désormais un domaine Active Directory.

Prise en charge de l'extension PKInit Freshness

Les clients Kerberos tentent désormais d'utiliser l'extension de fraîcheur PKInit pour les signatures basées sur les clés publiques.

Les KDC prennent désormais en charge l'extension de fraîcheur PKInit. Cependant, ils ne proposent pas l'extension de fraîcheur PKInit par défaut.

Pour plus d'informations, consultez Prise en charge du client Kerberos et du centre de distribution de clés pour l'extension RFC 8070 PKInit Freshness.

Clés publiques propagées uniquement les secrets NTLM de l'utilisateur

À partir du niveau fonctionnel de domaine (DFL) de Windows Server 2016, les DC prennent désormais en charge le roulement des secrets NTLM d'un utilisateur à clé publique uniquement. Cette fonctionnalité n'est pas disponible dans les niveaux de fonctionnement des domaines inférieurs (DFL).

> ⚠ **Avertissement**
>
> L'ajout d'un DC activé avant la mise à jour du 8 novembre 2016 à un domaine qui prend en charge les secrets NTLM roulants peut entraîner le plantage du DC.

Pour les nouveaux domaines, cette fonctionnalité est activée par défaut. Pour les domaines existants, vous devez le configurer dans le Centre administratif Active Directory.

Dans le Centre administratif Active Directory, cliquez avec le bouton droit de la souris sur le domaine dans le volet gauche et sélectionnez **Propriétés**. Cochez la case **Activer le renouvellement des secrets NTLM expirés lors de l'ouverture de session pour les utilisateurs qui doivent utiliser Windows Hello for Business ou une carte à puce pour l'ouverture de session interactive**. Ensuite, sélectionnez **OK** pour appliquer cette modification.

L'autorisation de réseau NTLM lorsqu'un utilisateur est limité à certains appareils associés à un domaine

Les DC peuvent désormais prendre en charge l'autorisation de NTLM réseau lorsqu'un utilisateur est limité à des appareils spécifiques joints à un domaine dans la LDF Windows Server 2016 et les versions ultérieures. Cette fonctionnalité n'est pas disponible dans les Niveaux Fonctionnels de Domaine exécutant un système d'exploitation antérieur à Windows Server 2016.

Pour configurer ce paramètre, dans la stratégie d'authentification, sélectionnez **Autoriser l'authentification réseau NTLM lorsque l'utilisateur est limité aux appareils sélectionnés**.

Pour plus d'informations, voir Stratégies d'authentification et silos de stratégies d'authentification.

Protection de périphérique (intégrité du code)

Protection de périphérique assure l'intégrité du code en mode noyau (KMCI) et en mode utilisateur (UMCI), en créant des stratégies qui spécifient le code exécutable sur le serveur. Consultez Introduction à Windows Defender Device Guard : Stratégies d'intégrité du code et de sécurité basée sur la virtualisation.

Windows Defender

Windows Defender Overview for Windows Server 2016 (Présentation de Windows Defender pour Windows Server 2016. Windows Server Anti-malware est installé et activé par défaut dans Windows Server 2016, mais l'interface utilisateur de Windows Server Anti-malware n'est pas installée. Toutefois, Windows Server Anti-malware met à jour les définitions anti-programmes malveillants et protège l'ordinateur sans l'interface utilisateur. Si vous avez besoin de l'interface utilisateur pour Windows Server Anti-malware, vous pouvez l'installer après l'installation du système d'exploitation à l'aide de l'Assistant Ajout de rôles et de fonctionnalités.

Control Flow Guard

Protection de flux de contrôle est une fonctionnalité de sécurité de plateforme qui a été créée pour lutter contre les risques de corruption de mémoire. Pour plus d'informations, consultez Control Flow Guard (Protection du flux de contrôle).

Stockage

Le stockage dans Windows Server 2016 comprend de nouvelles fonctionnalités et améliorations pour le stockage défini par logiciel et les serveurs de fichiers traditionnels.

Espaces de stockage directs

Les espaces de stockage direct permettent de créer un stockage à haute disponibilité et scalable en utilisant des serveurs avec un stockage local. Il simplifie le déploiement et la gestion des systèmes de stockage définis par logiciel et vous permet d'utiliser de nouvelles classes de périphériques de disque, telles que les disques SSD SATA et les périphériques de disque NVMe, qui n'étaient pas disponibles auparavant avec les espaces de stockage en cluster avec des disques partagés.

Pour plus d'informations, consultez Espaces de stockage direct.

Réplica de stockage

Storage Replica permet une réplication synchrone au niveau des blocs, indépendante du stockage, entre les serveurs ou les clusters pour la reprise après sinistre, et vous permet d'étendre un cluster de basculement entre les sites. La réplication synchrone permet la mise en miroir des données dans des sites physiques avec des volumes cohérents lors d'une panne, ce qui garantit aucune perte de données au niveau du système de fichiers. La réplication asynchrone permet l'extension de site au-delà des zones métropolitaines, tout en comportant un risque de perte de données.

Pour plus d'informations, consultez Storage Replica.

Qualité de service de stockage

Vous pouvez maintenant utiliser la qualité de service (QoS) de stockage pour analyser de manière centralisée les performances de stockage de bout en bout et créer des stratégies de gestion avec Hyper-V et des clusters CSV dans Windows Server 2016.

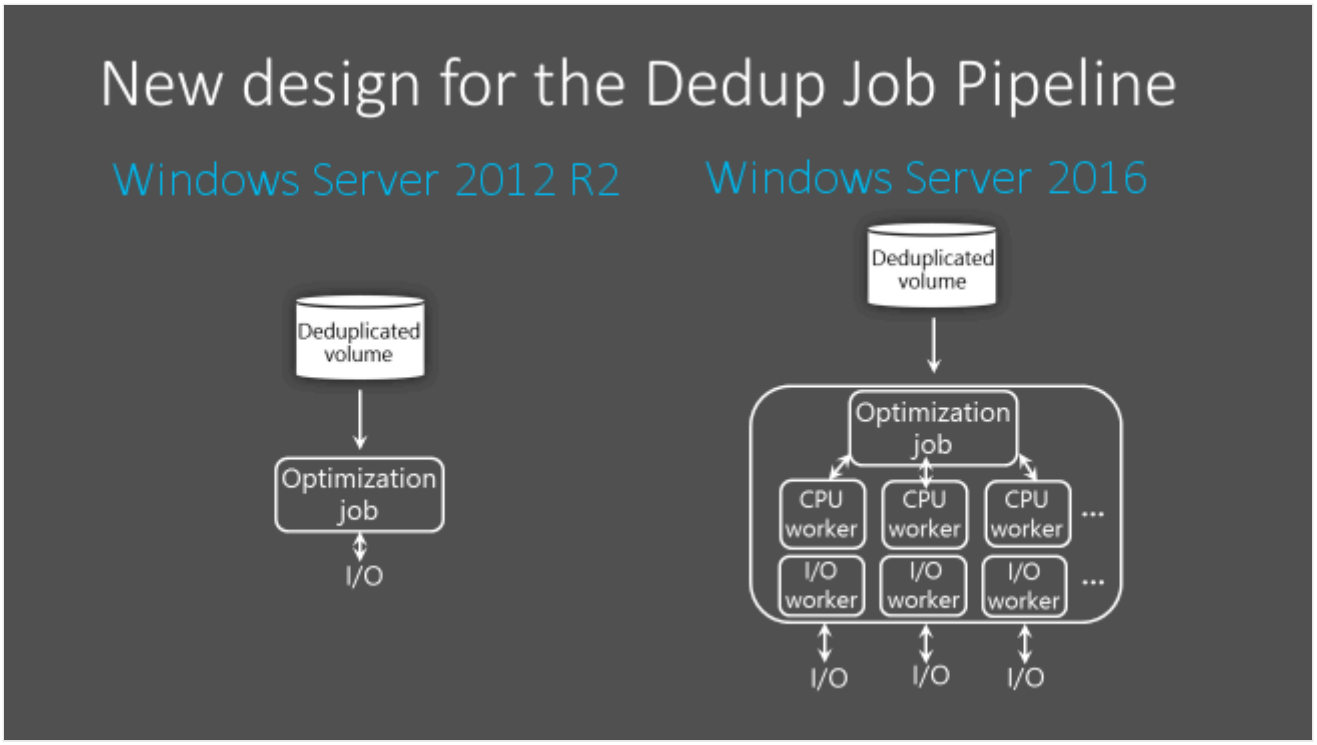
Pour plus d'informations, consultez Storage Quality of Service (Qualité de service de stockage).

Déduplication des données

Windows Server 2016 inclut les nouvelles fonctionnalités suivantes pour la déduplication des données.

Prise en charge de volumes importants

À compter de Windows Server 2016, le pipeline de la tâche de déduplication de données peut exécuter plusieurs threads en parallèle en utilisant plusieurs files d'attente d'E/S pour chaque volume. Cette modification permet d'atteindre des niveaux de performance auparavant uniquement possibles en divisant les données en plusieurs volumes de taille plus réduite. Ces optimisations s'appliquent à tous les travaux de déduplication des données, et non uniquement au travail d'optimisation. Le schéma suivant montre comment le pipeline a changé entre les versions de Windows Server.



Grâce à l'amélioration des performances, sur Windows Server 2016, la déduplication des données offre des performances élevées sur les volumes jusqu'à 64 To.

Prise en charge des fichiers de grande taille

À partir de Windows Server 2016, la déduplication des données utilise des structures de cartographie de flux et d'autres améliorations pour augmenter le débit d'optimisation et les performances d'accès. Le pipeline de traitement de déduplication peut également reprendre l'optimisation après Des scénarios de basculement au lieu de recommencer à partir du début. Cette modification améliore les performances des fichiers jusqu'à 1 To, ce qui permet aux administrateurs d'appliquer des économies de déduplication à un plus grand nombre de charges de travail, notamment les fichiers volumineux associés aux charges de travail de sauvegarde.

Prise en charge de Nano Server

Nano Server est une option de déploiement sans tête dans Windows Server 2016 qui nécessite une empreinte de ressource système beaucoup plus petite, démarre plus rapidement et nécessite moins de mises à jour et de redémarrages que l'option de déploiement Windows Server Core. De plus, Nano Server prend entièrement en charge la déduplication des données. Pour en savoir plus sur Nano Server, consultez Images de base de conteneur.

Configuration simplifiée pour les applications de sauvegarde virtualisées

À compter de Windows Server 2016, la déduplication des données pour les scénarios d'applications de sauvegarde virtualisées est largement simplifiée. Ce scénario est désormais une option de type d'utilisation prédéfinie. Vous n'avez plus besoin de paramétrer manuellement la déduplication, il vous suffit de l'activer pour un volume, comme vous le feriez pour le serveur de fichiers à usage général et l'infrastructure VDI (Virtual Desktop Infrastructure).

Prise en charge de la mise à niveau propagée du système d'exploitation de cluster

Les clusters de basculement Windows Server exécutant la déduplication des données peuvent comporter un mélange de nœuds qui exécutent des versions de Windows Server 2012 R2 et de Windows Server 2016 de la déduplication des données. Cette fonctionnalité de cluster en mode mixte offre un accès complet aux données de tous les volumes dédupliqués pendant les mises à niveau progressives de cluster. Vous pouvez désormais déployer progressivement des versions ultérieures des déduplications de données sur des clusters exécutant des versions antérieures de Windows Server sans temps d'arrêt.

Vous pouvez également utiliser les mises à jour en continu sur Hyper-V. Avec la mise à niveau continue d'un cluster Hyper-V, vous pouvez désormais ajouter un nœud exécutant Windows Server 2019 ou Windows Server 2016 à un cluster Hyper-V avec des nœuds exécutant Windows Server 2012 R2. Après avoir ajouté le nœud exécutant la version la plus récente de Windows Server, vous pouvez mettre à niveau le reste du cluster sans interruption de service. Le cluster s'exécute à un niveau de fonctionnalité Windows Server 2012 R2 jusqu'à ce que vous mettiez à niveau tous les nœuds du cluster et que vous exécutiez Update-ClusterFunctionalLevel dans PowerShell pour mettre à jour le niveau de fonctionnement du cluster. Pour des instructions plus détaillées sur le fonctionnement du processus de mise à niveau continue, voir Mise à niveau continue du système d'exploitation de cluster.

> ⓘ **Notes**
>
> Hyper-V sur Windows 10 ne prend pas en charge le clustering de basculement.

Améliorations de la sécurisation renforcée SMB pour les connexions SYSVOL et NETLOGON

Dans Windows 10 et Windows Server 2016, les connexions des clients aux services de domaine Active Directory utilisaient par défaut les partages SYSVOL et NETLOGON sur les contrôleurs de domaine. Désormais, ces connexions nécessitent une signature SMB et une authentification mutuelle à l'aide de services tels que Kerberos. Si la signature SMB et l'authentification

mutuelle ne sont pas disponibles, un ordinateur Windows 10 ou Windows Server 2016 ne traite pas la stratégie de groupe et les scripts basés sur un domaine. Cette modification protège les périphériques contre les attaques de type "adversary-in-the-middle".

> ⓘ **Notes**
>
> Les valeurs de registre pour ces paramètres ne sont pas présentes par défaut, mais les règles de durcissement s'appliquent toujours jusqu'à ce que vous les remplaciez en modifiant la stratégie de groupe ou d'autres valeurs de registre.

Pour plus d'informations sur ces améliorations de sécurité, voir MS15-011 : Vulnérabilité dans la stratégie de groupe et MS15-011 & MS15-014 : Durcissement de la stratégie de groupe.

Dossiers de travail

Windows Server 2016 propose une notification de changement améliorée lorsque le serveur Work Folders exécute Windows Server 2016 et que le client Work Folders est Windows 10. Lorsque des modifications de fichiers se synchronisent sur le serveur Work Folders, le serveur en informe désormais immédiatement les clients Windows 10, puis synchronise les modifications de fichiers.

Système de fichiers résilient (ReFS)

La nouvelle version de ReFS permet de réaliser des déploiements de stockage à grande échelle avec diverses charges de travail, offrant ainsi plus de fiabilité, de résilience et d'extensibilité pour vos données.

ReFS offre les améliorations suivantes :

- Nouvelle fonctionnalité de niveau de stockage, offrant des performances plus rapides et une capacité de stockage accrue, notamment :
  - Plusieurs types de résilience sur le même disque virtuel en utilisant la mise en miroir dans le niveau de performance et la parité dans le niveau de capacité.
  - Amélioration de la réactivité face aux ensembles de travail flottants.
- Introduit le clonage de blocs pour améliorer les performances des opérations de machines virtuelles, telles que les opérations de fusion de points de contrôle `.vhdx`.
- Un nouvel outil d'analyse ReFS qui peut vous aider à récupérer les espaces de stockage perdus et à sauver les données des corruptions critiques.

Clustering de basculement

Windows Server 2016 inclut de nombreuses nouvelles fonctionnalités et améliorations pour plusieurs serveurs regroupés dans un cluster à tolérance de panne, à l'aide de la fonctionnalité Clustering avec basculement.

Mise à niveau propagée de système d'exploitation de cluster

La mise à niveau propagée du système d'exploitation de cluster permet à un administrateur de mettre à niveau le système d'exploitation des nœuds de cluster de Windows Server 2012 R2 vers Windows Server 2016 sans arrêter les charges de travail Hyper-V ou Scale-Out serveur de fichiers. Vous pouvez utiliser cette fonctionnalité pour éviter les pénalités de temps d'arrêt sur les contrats de niveau de service (SLA).

Pour plus d'informations, consultez Mise à niveau propagée du système d'exploitation de cluster.

Témoin de cloud

Dans Windows Server 2016, le témoin cloud est un nouveau type de témoin de quorum de cluster avec basculement, qui utilise Microsoft Azure comme point d'arbitrage. Le témoin cloud, comme n'importe quel autre témoin de quorum, obtient un vote et peut participer aux calculs de quorum. Vous pouvez le configurer comme témoin de quorum à l'aide de l'Assistant Configuration de quorum du cluster.

Pour plus d'informations, consultez Déployer un témoin de quorum.

Résilience des machines virtuelles

Windows Server 2016 inclut une résilience de calcul accrue des machines virtuelles (VM) pour réduire les problèmes de communication intracluster dans votre cluster de calcul. Cette résilience accrue comprend les mises à jour suivantes :

- Vous pouvez désormais configurer les options suivantes pour définir la façon dont les machines virtuelles doivent se comporter pendant les défaillances temporaires :
    - Le **niveau de résilience** définit la façon dont votre déploiement doit gérer les défaillances temporaires.
    - La **période de résilience** définit la durée pendant laquelle toutes les machines virtuelles sont autorisées à s'exécuter de manière isolée.

- Les nœuds non sains sont mis en quarantaine et ne sont plus autorisés à rejoindre le cluster. Cette fonctionnalité empêche les nœuds non sains d'affecter négativement les autres nœuds et l'ensemble du cluster.

Pour en savoir plus sur les fonctionnalités de résilience de calcul, consultez Résilience de calcul des machines virtuelles dans Windows Server 2016.

Les machines virtuelles Windows Server 2016 incluent également de nouvelles fonctionnalités de résilience de stockage pour gérer les défaillances de stockage temporaires. Une résilience améliorée permet de préserver les états de session de machine virtuelle client si une interruption de stockage se produit. Lorsqu'une machine virtuelle se déconnecte de son stockage sous-jacent, elle se met en pause et attend le rétablissement du stockage. Pendant qu'elle est en pause, la machine virtuelle conserve le contexte des applications qui s'y exécutaient au moment de la défaillance du stockage. Lorsque la connexion entre la machine virtuelle et le stockage est restaurée, la machine virtuelle retourne à son état d'exécution. Par conséquent, l'état de session de la machine du locataire est conservé pendant la récupération.

Les nouvelles fonctionnalités de résilience du stockage s'appliquent également aux clusters invités.

Améliorations apportées au diagnostic

Pour vous aider à diagnostiquer les problèmes liés aux clusters de basculement, Windows Server 2016 comprend les éléments suivants :

- Plusieurs améliorations apportées aux fichiers journaux du cluster, comme les informations sur le fuseau horaire et le journal DiagnosticVerbose, facilitent la résolution des problèmes de clustering de basculement. Pour plus d'informations, consultez Windows Server 2016 Failover Cluster Troubleshooting Enhancements - Cluster Log.

- Un nouveau type de vidage de mémoire active filtre la plupart des pages de mémoire allouées aux machines virtuelles, ce qui facilite l'enregistrement ou la copie du fichier memory.dmp. Pour plus d'informations, consultez Windows Server 2016 Failover Cluster Troubleshooting Enhancements - Active Dump.

Clusters de basculement reconnaissant les sites

Windows Server 2016 inclut des clusters de basculement reconnaissant les sites qui activent les nœuds de groupe dans les clusters étendus en fonction de leur emplacement physique ou du site. La reconnaissance des sites par les clusters améliore les opérations clés pendant le cycle de vie du cluster, comme le comportement de basculement, les stratégies de placement, les

pulsations entre les nœuds et le comportement du quorum. Pour plus d'informations, consultez Site-aware Failover Clusters in Windows Server 2016.

Clusters de groupes de travail et à domaines multiples

Dans Windows Server 2012 R2 et les versions antérieures, un cluster peut uniquement être créé entre des nœuds membres joints au même domaine. Windows Server 2016 supprime ces barrières et introduit la possibilité de créer un cluster de basculement sans dépendre de l'Active Directory. Vous pouvez maintenant créer des clusters de basculement dans les configurations suivantes :

- Clusters à domaine unique, dont tous leurs nœuds sont rattachés au même domaine.
- Clusters à domaines multiples, dont les nœuds appartiennent à différents domaines.
- Clusters de groupe de travail, dont les nœuds sont des serveurs membres ou des groupes de travail qui ne sont pas rattachés à un domaine.

Pour plus d'informations, consultez Workgroup and Multi-domain clusters in Windows Server 2016

Équilibrage de charge des machines virtuelles

L'équilibrage de charge de machine virtuelle est une nouvelle fonctionnalité du clustering de basculement qui équilibre de manière transparente la charge des machines virtuelles sur les nœuds d'un cluster. La fonctionnalité identifie les nœuds trop sollicités en fonction de la mémoire de la machine virtuelle et de l'utilisation du processeur sur le nœud. Elle migre ensuite les machines virtuelles du nœud trop sollicité vers des nœuds avec une bande passante disponible. Vous pouvez ajuster le degré auquel la fonctionnalité équilibre les nœuds pour garantir des performances et une utilisation optimales du cluster. L'équilibrage de charge est activé par défaut dans la préversion technique de Windows Server 2016. Toutefois, l'équilibrage de charge est désactivé quand l'optimisation dynamique SCVMM est activée.

Ordre de démarrage des machines virtuelles

L'ordre de démarrage de la machine virtuelle est une nouvelle fonctionnalité du clustering de basculement qui introduit l'orchestration de l'ordre de démarrage pour les machines virtuelles et les autres groupes d'un cluster. Vous pouvez désormais regrouper des machines virtuelles en niveaux, puis créer des dépendances d'ordre de démarrage entre différents niveaux. Ces dépendances garantissent que les machines virtuelles les plus importantes, telles que les contrôleurs de domaine ou les machines virtuelles d'utilitaire, démarrent en premier. Les

machines virtuelles de niveau de priorité inférieur ne démarrent qu'après le démarrage des machines virtuelles dont elles dépendent.

Réseaux de clusters à plusieurs cartes réseau et SMB Multichannel simplifiés

Les réseaux de cluster de secours ne sont plus limités à une seule carte réseau (NIC) par réseau ou sous-réseau. Avec les réseaux de clusters simplifiés Server Message Block (SMB) multicanaux et multi-NIC, la configuration du réseau est automatique et chaque NIC du sous-réseau peut être utilisée pour le trafic des clusters et des charges de travail. Cette amélioration permet aux clients d'optimiser le débit réseau pour l'instance de cluster de basculement SQL Server, Hyper-V et d'autres charges de travail SMB.

Pour plus d'informations, consultez Réseaux de cluster SMB Multichannel et multi-NIC simplifiés.

Développement d'applications

Services d'informations Internet (IIS) 10.0

Les nouvelles fonctionnalités fournies par le serveur web IIS 10.0 dans Windows Server 2016 sont notamment les suivantes :

- Prise en charge du protocole HTTP/2 dans la pile Gestion de réseau et intégration à IIS 10.0, ce qui permet aux sites web IIS 10.0 de traiter automatiquement les requêtes HTTP/2 pour les configurations prises en charge. Cette évolution apporte de nombreuses améliorations comparé à HTTP/1.1, comme une réutilisation plus efficace des connexions et une moindre latence, ce qui améliore les temps de chargement des pages web.
- Possibilité d'exécuter et de gérer IIS 10.0 dans Nano Server. Consultez IIS sur Nano Server.
- Prise en charge des en-têtes d'hôte génériques, permettant aux administrateurs de configurer un serveur web pour un domaine de manière à ce qu'il traite les requêtes de tout sous-domaine.
- Un nouveau module PowerShell (IISAdministration) pour la gestion des services IIS.

Pour plus d'informations, consultez IIS.

Coordonnateur de Transaction Distribuée (MSDTC)

Trois nouvelles fonctionnalités ont été ajoutées dans Microsoft Windows 10 et Windows Server 2016 :

- Une nouvelle interface pour la méthode Rejoin de Resource Manager peut être utilisée par un gestionnaire de ressources pour déterminer le résultat d'une transaction incertaine après le redémarrage d'une base de données en raison d'une erreur. Pour plus d'informations, consultez IResourceManagerRejoinable::Rejoin.

- La limite des noms de source de données (DSN) a été étendue de 256 octets à 3 072 octets. Pour plus d'informations, consultez IDtcToXaHelperFactory::Create, IDtcToXaHelperSinglePipe::XARMCreate ou IDtcToXaMapper::RequestNewResourceManager.

- Suivi amélioré, qui vous permet de définir une clé de Registre de manière à inclure un chemin de fichier image dans le nom de fichier Tracelog pour simplifier l'identification du Tracelog à vérifier. Pour plus d'informations sur la configuration du suivi pour MSDTC, consultez Guide pratique pour activer le suivi de diagnostic pour MSDTC sur un ordinateur Windows.

Serveur DNS

Windows Server 2016 contient les mises à jour suivantes pour le serveur DNS (Domain Name System).

Stratégies DNS

Vous pouvez configurer des stratégies DNS pour spécifier la façon dont un serveur DNS répond aux requêtes DNS. Vous pouvez configurer les réponses DNS en fonction de l'adresse IP du client, de l'heure de la journée et de plusieurs autres paramètres. Les stratégies DNS peuvent activer le DNS qui prend en charge la géolocalisation, la gestion du trafic, l'équilibrage de charge, le DNS split-brain et d'autres scénarios. Pour plus d'informations, consultez le Guide de scénario de stratégie DNS.

RRL

Vous pouvez activer la limitation du taux de réponse (RRL) sur vos serveurs DNS pour empêcher les systèmes malveillants de les utiliser pour lancer une attaque par déni de service distribué (DDoS) sur un client DNS. La RRL empêche votre serveur DNS de répondre à trop de requêtes en même temps, ce qui le protège lors des scénarios où un botnet envoie plusieurs requêtes à la fois pour tenter d'interrompre les opérations du serveur.

Prise en charge de DANE

Vous pouvez utiliser l'authentification d'entités nommées basée sur le DNS (DANE) (RFC 6394 et RFC 6698) pour spécifier l'autorité de certification à partir de laquelle vos clients DNS doivent attendre des certificats pour les noms de domaine hébergés sur votre serveur DNS. Cela permet de prévenir une attaque de l'homme du milieu où un acteur malveillant corrompt un cache DNS et pointe un nom DNS vers sa propre adresse IP.

Prise en charge des enregistrements inconnus

Vous pouvez ajouter des enregistrements que le serveur DNS ne prend pas explicitement en charge à l'aide de la fonctionnalité d'enregistrement inconnu. Un enregistrement est inconnu lorsque le serveur DNS ne reconnaît pas son format RDATA. Windows Server 2016 prend en charge les types d'enregistrements inconnus (RFC 3597), ce qui vous permet d'ajouter des enregistrements inconnus aux zones de serveur DNS Windows au format filaire binaire. Le programme de résolution de mise en cache Windows peut déjà traiter des types d'enregistrements inconnus. Le serveur DNS Windows n'effectue pas de traitement spécifique à l'enregistrement pour les enregistrements inconnus, mais peut les envoyer en réponse aux requêtes qu'il reçoit.

Indicateurs racine IPv6

Le serveur DNS Windows inclut désormais des indications de racine IPv6 publiées par l'IANA (Internet Assigned Numbers Authority). La prise en charge des indications de racine IPv6 vous permet d'effectuer des requêtes Internet qui utilisent les serveurs racine IPv6 pour effectuer des résolutions de noms.

Prise en charge de Windows PowerShell

Windows Server 2016 inclut de nouvelles commandes que vous pouvez utiliser pour configurer DNS dans PowerShell. Pour plus d'informations, consultez le module DnsServer de Windows Server 2016 et le module DnsClient de Windows Server 2016.

Support Nano Server pour le service DNS basé sur les fichiers

Vous pouvez déployer des serveurs DNS dans Windows Server 2016 sur une image Nano Server. Cette option de déploiement est disponible si vous utilisez un DNS basé sur les fichiers. En exécutant un serveur DNS sur une image Nano Server, vous pouvez exécuter vos serveurs DNS avec une réduction de l'encombrement, un démarrage rapide et un minimum de correctifs.

> ⓘ **Notes**

Le DNS intégré Active Directory n’est pas pris en charge sur Nano Server.

Client DNS

Le service client DNS offre désormais une prise en charge améliorée des ordinateurs dotés de plusieurs interfaces réseau.

Les ordinateurs multirésidents peuvent également utiliser la liaison du service client DNS pour améliorer la résolution du serveur :

- Lorsque vous utilisez un serveur DNS configuré sur une interface spécifique pour résoudre une requête DNS, le client DNS se lie à l'interface avant d'envoyer la requête. Cette liaison permet au client DNS de spécifier l'interface où la résolution de nom doit avoir lieu, optimisant ainsi les communications entre les applications et le client DNS sur l'interface réseau.
- Si le serveur DNS que vous utilisez a été désigné par un paramètre de stratégie de groupe de la table de stratégie de résolution de noms (NRPT), le service client DNS ne se lie pas à l'interface spécifiée.

> ⓘ **Notes**
>
> Les modifications apportées au service client DNS dans Windows 10 sont également présentes dans les ordinateurs exécutant Windows Server 2016 et les versions ultérieures.

Services de Bureau à Distance

Services Bureau à distance (RDS) a apporté les modifications suivantes pour Windows Server 2016.

Compatibilité des applications

RDS et Windows Server 2016 sont compatibles avec de nombreuses applications Windows 10, créant une expérience utilisateur presque identique à celle d’un bureau physique.

Azure SQL Database

Le service Broker pour les connexions Bureau à distance (RD) peut désormais stocker toutes les informations de déploiement, telles que les états de connexion et les associations utilisateur-hôte, dans une base de données SQL Azure structurée partagée. Cette fonctionnalité vous

permet d'utiliser un environnement à haute disponibilité sans avoir à utiliser un groupe de disponibilité Always On de SQL Server. Pour plus d'informations, veuillez consulter la rubrique Utilisation d'Azure SQL DB pour votre environnement haute disponibilité du Service Broker pour les connexions Bureau à distance.

Améliorations graphiques

L'affectation de périphériques discrets pour Hyper-V vous permet de mapper directement les unités de traitement graphique (GPU) sur une machine hôte à une machine virtuelle (VM). Toutes les applications sur la machine virtuelle nécessitant plus de GPU que la machine virtuelle peuvent fournir peuvent utiliser le GPU mappé à la place. Nous avons également amélioré le vGPU RemoteFX, y compris la prise en charge d'OpenGL 4.4, d'OpenCL 1.1, de la résolution 4K et des VM Windows Server. Pour plus d'informations, veuillez consulter la rubrique Affectation de périphériques discrets.

Améliorations du Broker pour les connexions de Bureau à Distance

Nous avons amélioré la façon dont le Broker de connexion RD gère les connexions pendant les pics de connexion, qui sont des périodes de demandes de connexion élevées des utilisateurs. Le Broker pour les connexions RD peut désormais gérer plus de 10 000 demandes d'inscription simultanées ! Les améliorations de la maintenance facilitent également la réalisation de la maintenance sur votre déploiement en vous permettant de réintégrer rapidement les serveurs dans l'environnement une fois qu'ils sont prêts à être remis en ligne. Pour plus d'informations, veuillez consulter la section Amélioration des performances du Broker pour les connexions Bureau à distance.

Modifications du protocole RDP 10

Le protocole Bureau à distance (RDP) 10 utilise désormais le codec H.264/AVC 444, ce qui optimise à la fois la vidéo et le texte. Cette version inclut également la prise en charge de la saisie au stylet. Ces nouvelles fonctionnalités permettent à votre session à distance de se rapprocher davantage d'une session locale. Pour plus d'informations, veuillez consulter la section Améliorations RDP 10 AVC/H.264 dans Windows 10 et Windows Server 2016.

Ordinateurs de bureau pour sessions personnelles

Personal session desktops est une nouvelle fonctionnalité qui vous permet d'héberger votre propre bureau personnel dans le cloud. Les privilèges administratifs et les hôtes de session dédiés éliminent la complexité des environnements d'hébergement où les utilisateurs

souhaitent gérer un bureau à distance comme un bureau local. Pour plus d'informations, veuillez consulter la rubrique Personal Session Desktops.

Authentification Kerberos

Windows Server 2016 inclut les mises à jour suivantes pour l'authentification Kerberos.

Prise en charge du centre de distribution de clés (KDC) pour l'authentification cliente basée sur l'approbation de clé publique

Les centres de distribution de clés (KDC) prennent désormais en charge le mappage des clés publiques. Si vous provisionnez une clé publique pour un compte, le KDC prend en charge Kerberos PKInit explicitement à l'aide de cette clé. Étant donné qu'il n'y a pas de validation de certificat, Kerberos prend en charge les certificats auto-signés, mais pas la garantie du mécanisme d'authentification.

Les comptes que vous avez configurés pour utiliser l'approbation de clé utilisent uniquement l'approbation de clé, quelle que soit la façon dont vous avez configuré le paramètre UseSubjectAltName.

Prise en charge du client Kerberos et du KDC pour l'extension RFC 8070 PKInit Freshness

À partir de Windows 10, version 1607 et Windows Server 2016, les clients Kerberos peuvent utiliser l'extension RFC 8070 PKInit Freshness pour les connexions basées sur des clés publiques. Par défaut, l'extension PKInit Freshness est désactivée pour vous permettre de configurer la prise en charge du KDC pour la stratégie des modèles d'administration du KDC de l'extension PKInit Freshness sur tous les contrôleurs de domaine de votre domaine.

La stratégie a les paramètres suivants disponibles lorsque votre domaine se trouve dans le niveau fonctionnel du domaine (DFL) de Windows Server 2016 :

- **Désactivé** : le KDC n'offre jamais l'extension PKInit Freshness et accepte les demandes d'authentification valides sans vérifier l'actualisation. Les utilisateurs ne reçoivent pas le SID d'identité de clé publique actualisé.
- **Prise en charge** : Kerberos prend en charge l'extension PKInit Freshness sur demande. Les clients Kerberos qui sont authentifiés avec l'extension PKInit Freshness reçoivent le SID d'identité de clé publique actualisé.
- **Obligatoire** : l'extension PKInit Freshness est requise pour une authentification réussie. Les clients Kerberos qui ne prennent pas en charge l'extension PKInit Freshness

échoueront toujours lors de l'utilisation d'informations d'identification de clé publique.

Prise en charge des appareils joints à un domaine pour l'authentification à l'aide d'une clé publique

Si un appareil joint à un domaine peut enregistrer sa clé publique liée auprès d'un contrôleur de domaine (DC) Windows Server 2016, il peut alors s'authentifier avec la clé publique à l'aide de l'authentification Kerberos PKInit auprès d'un DC Windows Server 2016.

Les appareils joints à un domaine avec des clés publiques liées enregistrées auprès d'un contrôleur de domaine Windows Server 2016 peuvent désormais s'authentifier auprès d'un contrôleur de domaine Windows Server 2016 à l'aide des protocoles Kerberos de chiffrement à clé publique pour l'authentification initiale (PKInit). Pour plus d'informations, consultez Authentification par clé publique d'appareil joint au domaine.

Les centres de distribution de clés (KDC) prennent désormais en charge l'authentification à l'aide de la confiance de clé Kerberos.

Pour plus d'informations, consultez Prise en charge du centre de distribution de clés pour le mappage de comptes à approbation de clé.

Les clients Kerberos autorisent l'utilisation des noms d'hôte avec des adresses IPv4 et IPv6 dans les noms principaux de service (SPN).

À partir de Windows 10 version 1507 et Windows Server 2016, vous pouvez configurer les clients Kerberos pour qu'ils prennent en charge les noms d'hôte IPv4 et IPv6 dans les SPN. Pour plus d'informations, consultez Configuration de Kerberos pour les adresses IP.

Pour configurer la prise en charge des noms d'hôte d'adresses IP dans les SPN, créez une entrée TryIPSPN. Par défaut, cette entrée n'existe pas dans le Registre. Vous devez placer cette entrée sur le chemin suivant :

```text
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters
```

Après avoir créé l'entrée, remplacez sa valeur DWORD par 1. Si cette valeur n'est pas configurée, Kerberos ne fait pas de tentative de noms d'hôte d'adresses IP.

L'authentification Kerberos ne réussit que si le SPN est inscrit dans Active Directory.

Prise en charge du KDC pour le mappage de compte d'approbation de clé

Les contrôleurs de domaine prennent désormais en charge le mappage des comptes à approbation de clés et le remplacement vers AltSecID et UPN (User Principal Name) existants dans le comportement SAN. Vous pouvez configurer la variable UseSubjectAltName sur les paramètres suivants :

- Paramétrer la variable sur 0 rend le mappage explicite obligatoire. Les utilisateurs doivent utiliser une approbation de clé ou définir une variable ExplicitAltSecID.
- Paramétrer la variable sur 1, qui est la valeur par défaut, autorise le mappage implicite.
    - Si vous configurez une approbation de clé pour un compte dans Windows Server 2016 ou version ultérieure, le KDC utilise KeyTrust pour le mappage.
    - S'il n'y a pas d'UPN dans le SAN, le KDC tente d'utiliser AltSecID pour le mappage.
    - S'il y a un UPN dans le SAN, le KDC tente d'utiliser l'UPN pour le mappage.

Active Directory Federation Services (AD FS)

AD FS pour Windows Server 2016 contient les mises à jour suivantes.

Se connecter avec l'authentification multi-facteur Microsoft Entra

AD FS 2016 s'appuie sur les fonctionnalités d'authentification multifacteur (MFA) d'AD FS dans Windows Server 2012 R2. Vous pouvez désormais autoriser l'authentification qui nécessite uniquement un code d'authentification multifacteur Microsoft Entra au lieu d'un nom d'utilisateur ou d'un mot de passe.

- Lorsque vous configurez l'authentification multifacteur Microsoft Entra en tant que méthode d'authentification principale, AD FS invite l'utilisateur à saisir son nom d'utilisateur et le code de mot de passe à usage unique (OTP) de l'application Azure Authenticator.
- Lorsque vous configurez l'authentification multifacteur Microsoft Entra en tant que méthode d'authentification secondaire ou supplémentaire, l'utilisateur fournit des informations d'identification d'authentification principales. Les utilisateurs peuvent se connecter à l'aide de l'authentification intégrée Windows, qui peut leur demander leur nom d'utilisateur et leur mot de passe, leur carte à puce ou un certificat d'utilisateur ou

d’appareil. Ensuite, les utilisateurs sont invités à fournir leurs informations d’identification secondaires, telles que l’authentification multifacteur Microsoft Entra basée sur le texte, la voix ou l’OTP.

- L'adaptateur intégré d'authentification multifacteur Microsoft Entra offre un paramétrage et une configuration plus simples pour l'authentification multifacteur Microsoft Entra avec AD FS.
- Les organisations peuvent utiliser l’authentification multifacteur Microsoft Entra sans disposer d’un serveur d’authentification multifacteur Microsoft Entra local.
- Vous pouvez configurer l’authentification multifacteur Microsoft Entra pour un intranet, un extranet ou dans le cadre d’une stratégie de contrôle d’accès.

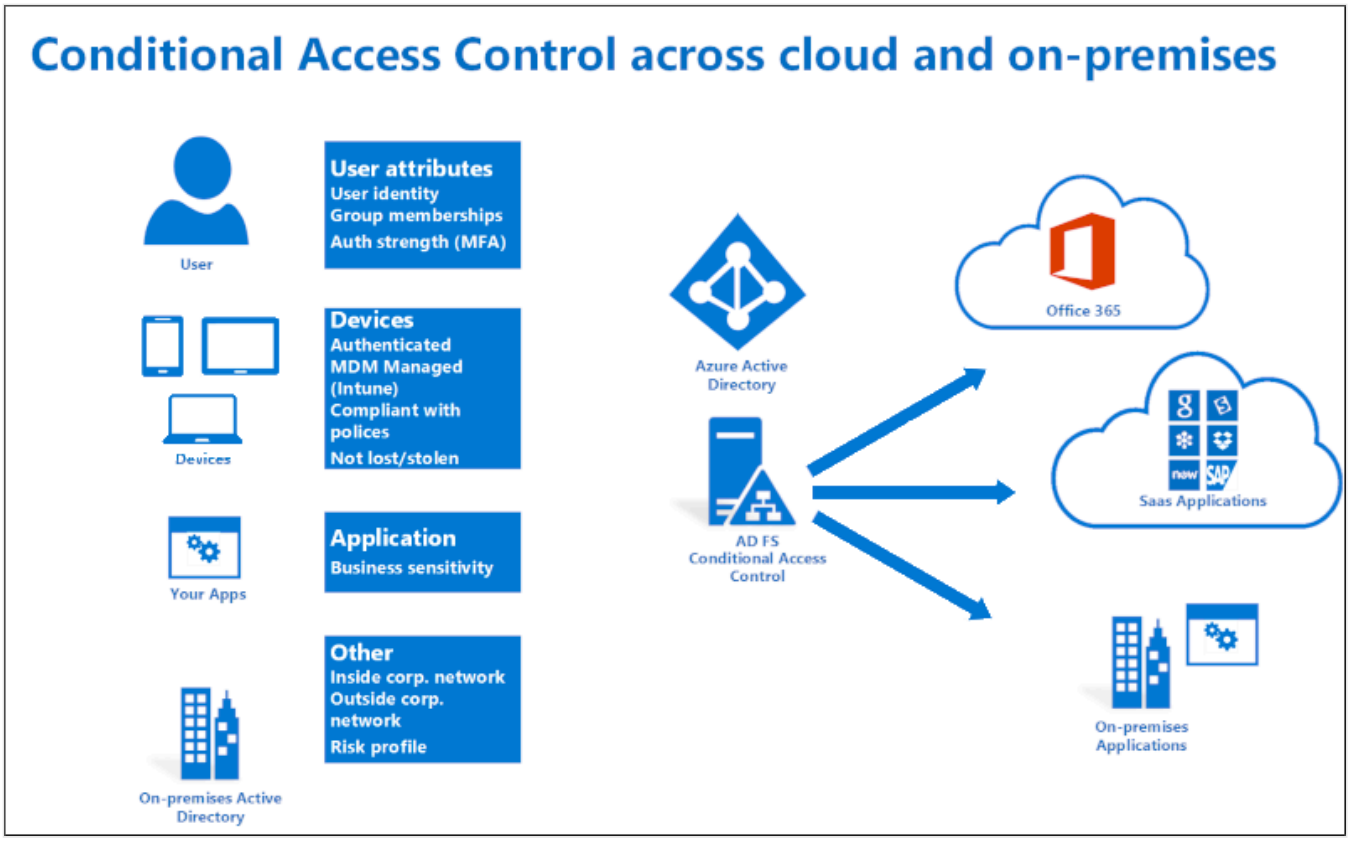
Pour en savoir plus sur l’authentification multifacteur Microsoft Entra avec AD FS, consultez Configurer AD FS 2016 et l’authentification multifacteur Microsoft Entra.

Accès sans mot de passe à partir des appareils conformes

AD FS 2016 s’appuie sur les fonctionnalités d’inscription d’appareils précédentes pour activer l’authentification et le contrôle d’accès en fonction de l’état de conformité des appareils. Les utilisateurs peuvent se connecter à l’aide des informations d’identification de l’appareil, et AD FS réévalue la conformité quand les attributs de l’appareil changent afin de garantir l’application des stratégies. Cette fonctionnalité active les stratégies suivantes :

- Activez l’accès uniquement à partir d’appareils managés et/ou conformes.
- Activez l’accès extranet uniquement à partir d’appareils managés et/ou conformes.
- Exiger l’authentification multifacteur pour les ordinateurs qui ne sont pas managés ou sont non conformes.

AD FS fournit le composant local des stratégies d’accès conditionnel dans un scénario hybride. Quand vous inscrivez des appareils auprès d’Azure AD pour l’accès conditionnel aux ressources cloud, vous pouvez aussi utiliser l’identité de l’appareil pour les stratégies AD FS.



Pour plus d'informations sur l'utilisation de l'accès conditionnel basé sur l'appareil dans le cloud, consultez Accès conditionnel Azure Active Directory.

Pour en savoir plus sur l'utilisation de l'accès conditionnel basé sur les appareils avec AD FS, consultez Planification de l'accès conditionnel basé sur l'appareil avec AD FS et Stratégies de contrôle d'accès dans AD FS.

Se connecter avec Windows Hello Entreprise

Les appareils Windows 10 contiennent Windows Hello et Windows Hello Entreprise, qui remplacent les mots de passe utilisateur par des informations d'identification de l'utilisateur puissantes, protégées par un mouvement de l'utilisateur (un code confidentiel, un mouvement biométrique comme une empreinte digitale ou une reconnaissance faciale). Avec Windows Hello, les utilisateurs peuvent se connecter à des applications AD FS à partir d'un intranet ou d'un extranet sans nécessiter de mot de passe.

Pour plus d'informations sur l'utilisation de Windows Hello Entreprise dans votre organisation, consultez Activer Windows Hello Entreprise dans votre organisation.

Authentification moderne

AD FS 2016 prend en charge les protocoles modernes les plus récents qui offrent une meilleure expérience utilisateur pour Windows 10 et les appareils et applications iOS et Android les plus récents.

Pour plus d'informations, consultez Scénarios AD FS pour les développeurs.

Configurer des stratégies de contrôle d'accès sans avoir à connaître le langage de règles de revendication

Avant, les administrateurs AD FS devaient configurer des stratégies en utilisant le langage de règles de revendication AD FS, ce qui compliquait la configuration et la maintenance des stratégies. Avec les stratégies de contrôle d'accès, les administrateurs peuvent utiliser des modèles intégrés pour appliquer des stratégies courantes. Par exemple, vous pouvez utiliser des modèles pour appliquer les stratégies suivantes :

- Autoriser l'accès intranet uniquement.
- Autoriser tout le monde et exiger l'authentification MFA à partir de l'extranet.
- Autoriser tout le monde et exiger l'authentification MFA pour un groupe spécifique.

Les modèles sont faciles à personnaliser. Vous pouvez appliquer des exceptions ou des règles de stratégie supplémentaires, et appliquer ces modifications à une ou plusieurs applications pour une mise en œuvre cohérente de la stratégie.

Pour plus d'informations, consultez Stratégies de contrôle d'accès dans AD FS.

Activer la connexion avec des répertoires LDAP non-AD

De nombreuses organisations combinent Active Directory et des annuaires tiers. Avec la prise en charge dans AD FS de l'authentification des utilisateurs stockés dans des annuaires compatibles Lightweight Directory Access Protocol (LDAP) v3, vous pouvez désormais utilisé AD FS dans les scénarios suivants :

- Les utilisateurs d'annuaires tiers compatibles LDAP v3.
- Les utilisateurs des forêts Active Directory pour lesquelles aucune approbation bidirectionnelle Active Directory n'est configurée.
- Les utilisateurs des services AD LDS (Active Directory Lightweight Directory Services).

Pour plus d'informations, voir Configurer AD FS pour authentifier les utilisateurs stockés dans les annuaires LDAP.

Personnaliser l'expérience de connexion pour les applications AD FS

Avant, AD FS dans Windows Server 2012 R2 offrait une expérience d'authentification commune pour toutes les applications par partie de confiance, avec la possibilité de personnaliser un sous-ensemble de contenu textuel par application. Avec Windows Server 2016, vous pouvez personnaliser non seulement les messages, mais aussi les images, le logo et le thème web par application. Vous pouvez aussi créer des thèmes web personnalisés et appliquer ces thèmes par partie de confiance.

Pour plus d'informations, consultez Personnalisation de la connexion utilisateur AD FS.

Audit rationalisé pour faciliter la gestion administrative

Dans les versions précédentes d'AD FS, une seule requête pouvait générer de nombreux événements d'audit. Les informations pertinentes sur les activités de connexion ou d'émission de jetons étaient souvent absentes ou réparties sur plusieurs événements d'audit, ce qui compliquait le diagnostic des problèmes. Ainsi, les événements d'audit étaient désactivés par défaut. Toutefois, dans AD FS 2016, le processus d'audit est plus rationalisé et les informations pertinentes sont plus faciles à trouver. Pour plus d'informations, consultez Améliorations de l'audit apportées à AD FS dans Windows Server 2016.

Amélioration de l'interopérabilité avec SAML 2.0 pour la participation aux confédérations

AD FS 2016 offre davantage de prise en charge du protocole SAML, notamment la prise en charge de l'importation des approbations basées sur des métadonnées contenant plusieurs entités. Ce changement vous permet de configurer AD FS pour participer à des confédérations telles que la fédération InCommon et d'autres implémentations conformes à la norme eGov 2.0.

Pour plus d'informations, consultez Interopérabilité améliorée avec SAML 2.0.

Gestion simplifiée des mots de passe pour les utilisateurs Microsoft 365 fédérés

Vous pouvez configurer AD FS pour envoyer des revendications d'expiration de mot de passe à toutes les approbations ou applications de partie de confiance qu'il protège. La façon dont ces revendications apparaissent varie selon les applications. Par exemple, avec Office 365 comme partie de confiance, des mises à jour sont implémentées dans Exchange et Outlook pour informer les utilisateurs fédérés de l'expiration prochaine de leurs mots de passe.

Pour plus d'informations, consultez Configurer AD FS pour envoyer les revendications d'expiration de mot de passe.

Simplification du passage d'AD FS dans Windows Server 2012 R2 à AD FS dans Windows Server 2016

Auparavant, la migration vers une nouvelle version d'AD FS nécessitait l'exportation des paramètres de configuration à partir de votre batterie Windows Server vers une nouvelle batterie de serveurs parallèle. AD FS sur Windows Server 2016 facilite le processus en supprimant l'obligation de disposer d'une batterie de serveurs parallèles. Lorsque vous ajoutez un serveur Windows Server 2016 à une batterie de serveurs Windows Server 2012 R2, le nouveau serveur se comporte comme un serveur Windows Server 2012 R2. Lorsque vous êtes prêt à effectuer une mise à niveau et que vous avez supprimé les serveurs plus anciens, vous pouvez changer le niveau opérationnel en Windows Server 2016. Pour plus d'informations, consultez Mise à niveau vers AD FS dans Windows Server 2016.

Bien démarrer avec Windows Server Insiders Preview

16/08/2025

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

Rejoignez le programme Windows Insider pour Windows Server et obtenez un accès exclusif aux prévisualisations de Windows Server Insider et aux outils d'administration de serveur à distance. En intégrant cette communauté, vous pourrez contribuer à façonner l'avenir de Windows Server et vous resterez à la pointe de l'innovation !

Où télécharger Windows Server Insiders Preview

Si vous êtes un membre Insider, vous pouvez accéder directement à la page téléchargements de Windows Insider Preview pour afficher les builds Windows Server Preview disponibles. Si vous souhaitez participer en tant qu'Insider, vous pouvez consulter la section Bien démarrer avec le programme Windows Insider pour Windows Server.

Les clés suivantes sont valides uniquement pour les versions de préversion :

Agrandir le tableau

Version de Windows Server	Key
Standard	MFY9F-XBN2F-TYFMP-CCV49-RMYVH
Datacenter	2KNJJ-33Y9H-2GXGX-KMQWH-G6H67
Édition Azure	Les clés ne sont pas acceptées

> **Notes**
>
> Les téléchargements peuvent être restreints dans certains pays/certaines régions. Pour en savoir plus, veuillez consulter la section Microsoft suspend ses ventes en Russie.

Problèmes connus avec Insiders Preview

- Pendant le processus d'installation OOBE, certains utilisateurs remarquent des fenêtres superposées ou des anomalies graphiques lorsqu'ils utilisent la souris pour passer à l'étape suivante.

- Les paramètres de confidentialité de l'utilisateur lors de la première connexion sont limités où toutes les fonctionnalités ne sont pas disponibles ni ne fonctionnent comme souhaité.
- L'installation du composant facultatif **WinPE-PowerShell** via n'importe quelle méthode ne fonctionne pas correctement et les applets de commande associées échouent. Cette version n'est pas pour les clients qui dépendent de PowerShell dans WinPE.
- Les nouvelles applications **du hub de commentaires** et du **terminal** ne fonctionnent pas correctement dans cette version.
- Nous déconseillons d'utiliser cette version pour valider les mises à niveau depuis Windows Server 2019 ou 2022 en raison de défaillances intermittentes de mise à niveau identifiées.
- L'utilisation de la commande `wevtutil al` pour archiver les journaux d'événements provoque un crash du service de journalisation des événements Windows et l'échec de l'opération d'archivage. Pour résoudre ce problème, le service doit être redémarré en exécutant ce qui suit dans une invite PowerShell élevée :

  ```PowerShell
  Start-Service EventLog
  ```

- Si vous avez activé le code de démarrage sécurisé ou Dynamic Root of Trust for Measurement (DRTM), nous recommandons d'éviter d'installer cette version.

Comment donner votre feedback pour Insiders Preview

Vos retours sont précieux pour nous car ils fournissent un aperçu de ce qui fonctionne à actuellement, nous aident à isoler les bugs, et nous transmettent des suggestions sur les améliorations possibles. Pour savoir comment donner votre feedback, veuillez consulter Un regard approfondi sur le feedback.

Utilisez votre appareil Windows 10 ou Windows 11 inscrit et ouvrez l'application Hub de commentaires . Dans l'application Feedback Hub, veuillez nous fournir :

1. Un titre pour le problème avec le numéro de la version de prévisualisation. Exemple, *Problème avec Server Manager dans Windows Server Standard 25997*.
2. Une explication détaillée de ce qui se passe.
3. Pour la **catégorie**, sélectionnez **Windows Server**.

4. Joindre une capture d’écran du problème est facultatif.
5. Terminez l’envoi de votre feedback.

Voir aussi

- Nouveautés de Windows Server 2025
- Explorer le Hub de commentaires

Comparaison des éditions de Windows Server

16/08/2025

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

Utilisez cet article pour comparer les éditions Standard, Datacenter et Datacenter : Azure Edition de Windows Server afin de déterminer celle qui répond le mieux à vos besoins.

> **Conseil**
>
> Si vous recherchez des informations sur les verrouillages et les limites dans Windows Server, consultez Comparaison des verrouillages et des limites dans Windows Server.

Rôles et fonctionnalités disponibles

Agrandir le tableau

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
Fonctionnalités de .NET Framework 3.5		✅	✅	✅
Fonctionnalités de .NET Framework 4.8		✅	✅	✅
Activation		✅	✅	✅
	Activation automatique de machine virtuelle	⚠[1]	✅	✅[2]
	Service de gestion de clés (KMS)	✅	✅	❌[3]
Services de certificats Active Directory		✅	✅	✅
	Service Web Stratégie d'inscription de certificats	✅	✅	✅
	Service Web Inscription de certificats	✅	✅	✅

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
	Autorité de certification	✅	✅	✅
	Inscription de l'autorité de certification via le Web	✅	✅	✅
	Service d'inscription de périphériques réseau	✅	✅	✅
	Répondeur en ligne	✅	✅	✅
Active Directory Domain Services		✅	✅	✅
Services de fédération d'Active Directory		✅	✅	✅
Services AD LDS (Active Directory Lightweight Directory Services)		✅	✅	✅
Services AD RMS (Active Directory Rights Management Services)		✅	✅	✅
Mise en réseau étendue Azure		❌	❌	✅
Service de transfert intelligent en arrière-plan (BITS)		✅	✅	✅
Chiffrement de lecteur BitLocker		✅	✅	✅
Déverrouillage réseau BitLocker		✅[4]	✅[4]	✅[4]
BranchCache		✅	✅	✅
Client pour NFS		✅	✅	✅
Data Center Bridging		✅	✅	✅
Attestation d'intégrité de l'appareil		✅	✅	✅
Serveur DHCP		✅	✅	✅
Lecture directe		✅[3]	✅[4]	✅[4]

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
DLNA – codecs et diffusion multimédia en continu sur le Web		✅[3]	✅[4]	✅[4]
Serveur DNS		✅	✅	✅
Stockage étendu		✅	✅	✅
Clustering de basculement		✅	✅	✅
Serveur de télécopie		✅	✅	✅
Services de fichiers et de stockage		✅	✅	✅
	BranchCache pour fichiers réseau	✅	✅	✅
	Déduplication des données	✅	✅	✅
	Espaces de noms DFS	✅	✅	✅
	Réplication DFS	✅	✅	✅
	Serveurs de fichiers	✅	✅	✅
	Gestionnaire de Ressources du Serveur de Fichiers	✅	✅	✅
	Service Agent VSS du serveur de fichiers	✅	✅	✅
	Serveur cible iSCSI	✅	✅	✅
	Fournisseur de stockage cible iSCSI (fournisseurs de matériel VDS et VSS)	✅	✅	✅
	Serveur pour NFS	✅	✅	✅
	Support de partage de fichiers SMB 1.0/CIFS	✅	✅	✅
	Limite de bande passante SMB	✅	✅	✅
	SMB sur QUIC	✅	✅	✅

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
	Dossiers de travail	✅	✅	✅
	Service de migration du stockage	✅	✅	✅
	Proxy du service de migration de stockage	✅	✅	✅
	Espaces de stockage	✅	✅	✅
	Espaces de stockage directs	❌	✅	✅
	Réplica de stockage	✅	✅	✅
Gestion des stratégies de groupe		✅	✅	✅
Support Hyper-V pour Guardian hôte		❌	✅	✅
Service Guardian hôte		✅	✅	✅
Hotpatching		✅[5]	✅[5]	✅
Qualité de service E/S		✅	✅	✅
Noyau Web hébergeable de IIS		✅	✅	✅
Serveur de gestion des adresses IP (IPAM)		✅	✅	✅
Extension ISS Management OData		✅	✅	✅
Media Foundation		✅	✅	✅
Message Queuing		✅	✅	✅
	Proxy DCOM Message Queuing	✅	✅	✅
	Services de file d'attente de messages	✅	✅	✅
Antivirus Microsoft Defender		✅	✅	✅

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
MPIO (Multipath I/O)		✅	✅	✅
MultiPoint Connector		✅	✅	✅
Réseau ATC		✅	✅	✅
Contrôleur de réseau		❌	✅	✅
Network Load Balancing		✅	✅	✅
Services de stratégie réseau et d'accès		✅[4]	✅[4]	✅[4]
Virtualisation du réseau		✅	✅	✅
Services d'impression et de numérisation de document		✅	✅	✅
	Impression Internet	✅[4]	✅[4]	✅[4]
	Service Line Printer Daemon (LPD)	✅[4]	✅[4]	✅[4]
	Serveur d'impression	✅[4]	✅[4]	✅[4]
Expérience audio-vidéo haute qualité Windows		✅	✅	✅
Kit d'administration du Gestionnaire des connexions (CMAK) RAS		✅	✅	✅
Accès à distance		✅	✅	✅
	DirectAccess et VPN (RAS)	✅	✅	✅
	Routing	✅	✅	✅
	Proxy d'application web	✅	✅	✅
Assistance à distance		✅[4]	✅[4]	✅[4]
Services Bureau à distance		✅[4]	✅[4]	✅[4]
Compression différentielle à distance		✅	✅	✅
Outils d'administration de serveur distant		✅	✅	✅

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
Proxy RPC sur HTTP		✅	✅	✅
Collection des événements de configuration et de démarrage		✅	✅	✅
Services TCP/IP simples		✅[4]	✅[4]	✅[4]
Service SNMP		✅	✅	✅
Équilibrage de la charge logicielle		✅	✅	✅
Programme d'archivage de données système		✅	✅	✅
System Insights		✅	✅	✅
Telnet Client		✅	✅	✅
TFTP Client		✅[4]	✅[4]	✅[4]
Virtualization		✅	✅	✅
	Containers	✅	✅	❌
	Hyper-V	✅	✅	✅
	Partitionnement GPU	✅[6]	✅	✅[6]
	Outils de protection d'ordinateur virtuel pour la gestion d'infrastructure	✅	✅	✅
Services d'activation en volume		✅	✅	✅
Serveur Web (IIS)		✅	✅	✅
	Serveur FTP	✅	✅	✅
	Serveur web	✅	✅	✅
Redirecteur WebDAV		✅	✅	✅
Windows Biométrique Framework		✅[4]	✅[4]	✅[4]

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
Services de déploiement de Windows		✅	✅	✅
Windows Identity Foundation 3.5		✅[4]	✅[4]	✅[4]
Base de données interne Windows		✅	✅	✅
Windows PowerShell		✅	✅	✅
	Moteur Windows PowerShell 2.0	✅	✅	✅
	Windows PowerShell 5.1	✅	✅	✅
	Service Desired State Configuration Windows PowerShell	✅	✅	✅
	Windows PowerShell Accès Web	✅	✅	✅
Service d'activation des processus Windows		✅	✅	✅
Gestion de Windows Server activée par Azure Arc		✅[7]	✅[7]	✅[7]
	Gestionnaire de mise à jour Azure	✅[7]	✅[7]	✅[7]
	Suivi des modifications et inventaire	✅[7]	✅[7]	✅[7]
	Configuration d'Azure Machine	✅[7]	✅[7]	✅[7]
	Windows Admin Center dans Azure pour Arc	✅[7]	✅[7]	✅[7]
	Support à distance	✅[7]	✅[7]	✅[7]
	HUD réseau	✅[7]	✅[7]	✅[7]
	Évaluation des bonnes pratiques	✅[7]	✅[7]	✅[7]

Feature	Subfeature	Édition standard	Édition datacenter	Centre de données : Édition Azure
	Configuration Azure Site Recovery	✅[7]	✅[7]	✅[7]
Service Windows Search		✅[4]	✅[4]	✅[4]
Sauvegarde Windows Server		✅	✅	✅
Outils de migration de Windows Server		✅	✅	✅
Windows Server Update Services		✅	✅	✅
Gestion du stockage basé sur les standards Windows		✅	✅	✅
Sous-système Windows pour Linux		✅	✅	✅
Windows TIFF IFilter		✅[4]	✅[4]	✅[4]
Extension WinRM IIS		✅	✅	✅
Serveur WINS		✅	✅	✅
Service de réseau local sans fil		✅	✅	✅
Prise en charge WoW64		✅	✅	✅
Visionneuse XPS		✅[4]	✅[4]	✅[4]

1. En tant qu'invité s'il est hébergé sur un hôte de virtualisation activé avec l'édition Datacenter
2. Datacenter : Azure Edition peut être utilisé comme hôte imbriqué ou invité
3. Il est activé par Azure et ne peut pas être configuré en tant qu'hôte KMS
4. Lorsqu'il est installé en tant que serveur avec Expérience utilisateur
5. Disponible en tant que service avec Azure Arc. Pour en savoir plus sur la tarification Azure Arc, consultez Calculateur de prix Azure.
6. Disponible avec Windows Server 2025 Standard, il est conçu pour les serveurs autonomes. Migrez en direct des machines virtuelles entre des nœuds autonomes en cas de temps

d'arrêt planifié. Si le clustering est nécessaire pour les temps d'arrêt non planifiés, Windows Server 2025 Datacenter doit être utilisé à la place.

7. Disponible pour les machines enregistrées sous Windows Server Management, activé par Azure Arc, avec des licences Windows Server comportant des assurances logicielles actives ou des licences d'abonnement actives. Pour en savoir plus sur les avantages, la facturation et les exigences Azure disponibles, consultez Gestion de Windows Server activée par Azure Arc.

Qu’est-ce qu’Azure Edition pour Windows Server ?

15/08/2025S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022

Windows Server Datacenter: Azure Edition est une édition de Windows Server axée sur l’innovation et la virtualisation optimisée pour s’exécuter sur Azure. Azure Edition propose un canal de maintenance à long terme (LTSC) et des mises à jour annuelles du produit, avec deux mises à jour majeures du produit au cours des 3 premières années. Azure Edition apporte également les nouvelles fonctionnalités aux utilisateurs de Windows Server plus rapidement que les éditions Standard et Datacenter de Windows Server.

Les mises à jour annuelles d’Azure Edition sont fournies à l’aide de Windows Update, plutôt que d’une mise à niveau complète du système d’exploitation. Dans le cadre de cette fréquence de mise à jour annuelle, le programme de préversion Insider d’Azure Edition offre la possibilité d’accéder aux versions préliminaires avant la disponibilité générale. Pour commencer à utiliser la préversion Insider d’Azure Edition, consultez l’offre Préversion Azure Edition sur la Place de marché Azure. Les détails relatifs à chaque préversion sont partagés dans les annonces de publication publiées dans l’espace Windows Server Insiders sur Microsoft Tech Community.

Principales différences

Le tableau suivant résume les principales différences :

Agrandir le tableau

Description	Windows Server Standard, Datacenter	Windows Server Datacenter : Azure Edition
Nouvelles versions	En général, 2-3 ans	En général, 2-3 ans
Mises à jour du produit	Avec une nouvelle version	Une fois par an, avec deux mises à jour majeures au cours des 3 premières années
Support	5 ans de support standard plus 5 ans de support étendu	5 ans de support standard plus 5 ans de support étendu
Canaux de maintenance	Canal de maintenance à long terme	Canal de maintenance à long terme
Qui peut l’utiliser ?	Tous les clients par le biais de tous les canaux	Software Assurance, abonnement Windows Server et clients cloud uniquement
Options d’installation	Server Core, Server avec Experience utilisateur, image de	Serveur Core et Serveur avec Desktop Experience uniquement. Les conteneurs

Description	Windows Server Standard, Datacenter	Windows Server Datacenter : Azure Edition
	conteneur Nano Server	Windows Server ne sont pas pris en charge.
Environnement de système d'exploitation (OSE)	Physique ou virtuel	Virtuelle uniquement
Droits de virtualisation associés	2 OSE virtuel pour les systèmes d'exploitation virtuels standard et illimités pour le centre de données	None

Les fonctionnalités varient selon l'image. Pour plus d'informations, consultez la section Prise en main de Windows Server Datacenter: Azure Edition.

> **Conseil**
>
> Pour plus d'informations, consultez les Termes du contrat de licence logiciel Microsoft. Les termes de licence peuvent varier en fonction du canal de distribution, par exemple, d'un programme de licences commerciales, de vente au détail, de fabricant d'équipement d'origine (OEM), etc.

Fonctionnalités clés

Hotpatch

Depuis Windows Server 2022 Datacenter: Azure Edition, Hotpatch vous permet d'appliquer des mises à jour de sécurité sur votre machine virtuelle sans redémarrer. Quand il est utilisé avec Azure, le service de mise à jour corrective d'invité Azure, ainsi que Automanage pour Windows Server, automatisent l'intégration, la configuration et l'orchestration de l'application des correctifs à chaud. Pour plus d'informations, consultez l'article Hotpatch pour les nouvelles machines virtuelles.

Plateformes prises en charge

Pour en savoir plus sur les systèmes d'exploitation qui prennent en charge Hotpatch pour les machines virtuelles s'exécutant sur Azure et Azure Stack HCI, consultez plateformes prises en charge.

> **Notes**

Hotpatch n'est pas pris en charge sur les images de base des conteneurs Windows Server.

SMB sur QUIC

Depuis Windows Server 2022 Datacenter: Azure Edition, SMB sur QUIC offre un « VPN SMB » pour les télétravailleurs, les utilisateurs d'appareils mobiles et les filiales. SMB sur QUIC offre une connectivité sécurisée et fiable aux serveurs de fichiers de périphérie sur des réseaux non approuvés comme Internet. QUIC est un protocole standard IETF utilisé dans HTTP/3, conçu pour une protection maximale des données avec TLS 1.3 et nécessite le chiffrement qui ne peut pas être désactivé. SMB se comporte normalement dans le tunnel QUIC, ce qui signifie que l'expérience utilisateur ne change pas. Les fonctionnalités SMB, telles que le multicanal, la signature, la compression, la disponibilité continue et le bail de répertoire, fonctionnent normalement.

SMB sur QUIC est également intégré aux meilleures pratiques d'Azure Automanage pour les machines Windows Server afin de simplifier la gestion de SMB sur QUIC. QUIC utilise des certificats pour fournir son chiffrement et les organisations ont souvent du mal à gérer des infrastructures de clés publiques complexes. Les bonnes pratiques des machines Azure Automanage garantissent que les certificats n'expirent pas sans avertissement et que SMB sur QUIC reste activé pour une continuité maximale du service.

Pour plus d'informations, consultez les articles SMB sur QUIC et Gestion de SMB sur QUIC avec les bonnes pratiques des machines Automanage.

Compression du réplica de stockage pour le transfert de données

Depuis la mise à jour 1 pour Windows Server 2022 Datacenter: Azure Edition, vous pouvez compresser les données répliquées du stockage entre les serveurs source et destination. La compression entraîne moins de paquets réseau pour transférer la même quantité de données, ce qui permet d'obtenir plus de débits et moins d'utilisation du réseau. Un débit de données plus élevé doit également réduire le temps de synchronisation pour le moment où vous en avez besoin, par exemple dans un scénario de récupération d'urgence.

Pour plus d'informations sur les fonctionnalités de réplication de stockage, consultez la section Fonctionnalités de réplication de stockage.

Réseau étendu pour Azure

Depuis Windows Server 2022 Datacenter: Azure Edition, le réseau étendu Azure vous permet d'étirer un sous-réseau local dans Azure pour permettre aux machines virtuelles locales de

conserver leurs adresses IP privées locales d'origine lors de la migration vers Azure. Pour plus d'informations, consultez l'article suivant :
Réseau étendu Azure.

Commencez avec Windows Server Datacenter : Édition Azure

Pour commencer à utiliser Azure Edition, utilisez votre méthode préférée pour créer une machine virtuelle azure ou locale Azure, puis sélectionnez l'image *Windows Server Datacenter : Azure Edition* que vous souhaitez utiliser.

> **ⓘ Important**
>
> Certaines fonctionnalités sont assorties d'étapes de configuration spécifiques à effectuer lors de la création d'une machine virtuelle, tandis que certaines fonctionnalités en préversion ont des exigences spécifiques relatives à l'acceptation et à l'affichage du portail. Consultez les articles sur les fonctionnalités individuelles pour en savoir plus sur l'utilisation de cette fonctionnalité avec votre machine virtuelle.

> **⊗ Attention**
>
> Une fois que Windows Server Datacenter : Azure Edition est installé, il n'est pas possible de revenir au système d'exploitation non-Azure Edition. Si vous n'avez pas voulu installer Azure Edition, la réinstallation du système d'exploitation précédent est nécessaire pour revenir en arrière.

Pour en savoir plus sur la création d'une machine virtuelle à l'aide d'Azure ou d'Azure Local, consultez Créer une machine virtuelle Windows dans le portail Azure et Déployer des machines virtuelles Windows Server Azure Edition dans Azure Local.

Étapes suivantes

- Comparatif des éditions Standard, Datacenter et Datacenter Azure Edition de Windows Server 2022
- Hotpatch pour les nouvelles machines virtuelles
- Activer Hotpatch pour les machines virtuelles Azure Edition générées à partir d'une image ISO
- SMB sur QUIC
- Étendre vos sous-réseaux locaux dans Azure à l'aide du réseau étendu pour Azure

Configurer le paiement à l'utilisation pour Windows Server avec Azure Arc

16/08/2025S'applique à: ✅ Windows Server 2025

Azure Arc propose une option de licence par abonnement pay-as-you-go en alternative à la licence perpétuelle traditionnelle de Windows Server 2025. Avec le paiement à l'utilisation, vous pouvez déployer un appareil Windows Server, le licencier, et ne payer que pour l'utilisation réelle. Cette fonctionnalité est rendue possible grâce à Azure Arc et facturée via votre abonnement Azure. Vous avez la possibilité de désactiver le paiement à l'utilisation à tout moment. De plus, l'utilisation du paiement à l'utilisation est gratuite pendant les sept premiers jours à titre d'essai. Le paiement à l'utilisation de Windows Server est un service Azure. Les droits d'utilisation détaillés figurent dans les Conditions générales des produits Microsoft.

> ⊗ **Attention**
>
> Si vous éteignez ou supprimez un appareil sans désactiver le paiement à l'utilisation, la facturation continue. Pour éviter toute facturation inattendue, désactivez le paiement à l'utilisation via le portail Azure, PowerShell, l'API, ou en retirant l'appareil d'Azure Arc.

Le paiement à l'utilisation de Windows Server utilise le même modèle tarifaire que celui des licences Windows Server sur Microsoft Azure, mais s'adresse aux appareils déployés en dehors d'Azure. Le paiement à l'utilisation de Windows Server avec Azure Arc n'est pas pris en charge sur Microsoft Azure, car d'autres méthodes de gestion des licences avec paiement à l'utilisation existent déjà dans ce cadre.

Les règles du paiement à l'utilisation diffèrent de celles des licences perpétuelles traditionnelles. Par exemple, avec le paiement à l'utilisation, le coût est identique pour les éditions Standard et Datacenter, et aucune licence d'accès client (CAL) n'est requise pour les fonctionnalités standard. Toutefois, les CAL des services Bureau à distance (RDS) sont toujours requises.

La licence de paiement à l'utilisation s'applique uniquement à l'appareil sur lequel la fonctionnalité est activée sur Microsoft Azure. Contrairement aux licences perpétuelles traditionnelles, elle ne fournit pas de droits supplémentaires pour les machines virtuelles s'exécutant sur le même serveur. Par conséquent, la fonctionnalité d'activation automatique de machine virtuelle (AVMA) n'est pas disponible. Chaque machine virtuelle doit disposer de sa propre licence, quel que soit le serveur hôte. L'hôte et les machines virtuelles peuvent exécuter différentes versions du système d'exploitation et mélanger différents types de licences.

Prerequisites

Avant de pouvoir configurer le paiement à l'utilisation de Windows Server, vérifiez que votre appareil répond aux conditions préalables suivantes :

- Votre appareil doit exécuter l'édition Standard ou Datacenter de Windows Server 2025. Si vous débutez avec Windows Server, familiarisez-vous avec Mise à jour des fonctionnalités, installation propre ou migration vers Windows Server pour plus d'informations.
- Votre appareil doit être connecté à Azure Arc et exécuter l'agent de machine connectée Microsoft Azure version 1.47 ou ultérieure. Pour en savoir plus sur l'intégration de votre appareil à Azure Arc, consultez Connecter des machines Windows Server à Azure via le programme d'installation d'Azure Arc.
- Aucune autre licence (OEM, Détail ou Licence en volume) n'est active sur votre appareil.
- Une connexion Internet active est requise.

Configurer le paiement à l'utilisation de Windows Server

Vous pouvez activer le paiement à l'utilisation Windows Server soit pendant l'installation de Windows Server, soit une fois l'installation terminée. Les sections suivantes expliquent les deux options étape par étape.

Choisir une méthode de gestion des licences

Pendant l'installation de Windows Server, vous pouvez choisir de configurer le paiement à l'utilisation. Cette option est disponible sur l'écran **Choisir une méthode de gestion des licences**, où vous entrez normalement une clé de produit. Une fois le paiement à l'utilisation sélectionné, vous n'avez pas besoin d'une clé de produit.

Si Windows Server est déjà installé et qu'il n'est pas activé, vous pouvez passer à la section Gérer le paiement Gérer le paiement à l'utilisation de Windows Server. Si vous débutez avec l'installation de Windows Server, vous pouvez suivre les étapes de la section Installer Windows Server à partir du support d'installation, puis revenir ici une fois arrivé à l'écran **Choisir une méthode de gestion des licences**.

> ⓘ **Notes**
>
> L'intégration du paiement à l'utilisation n'est disponible que pendant l'installation du système d'exploitation si vous exécutez Windows Setup à partir d'une copie commerciale du support Windows Server. Si vous utilisez une version Évaluation ou Licence en volume

(VL), la page de saisie de la clé produit est ignorée, ce qui signifie que vous ne pouvez pas activer le paiement à l'utilisation pendant l'installation du système. Néanmoins, vous pouvez activer le paiement à l'utilisation après l'installation, comme décrit dans la section Paiement à l'utilisation pour Windows Server.

Il existe deux méthodes pour configurer le paiement à l'utilisation : via l'Assistant graphique ou via la ligne de commande. Suivez ces étapes en fonction de l'édition de Windows que vous installez :

GUI

Une fois que vous êtes à l'écran **Choisir une méthode de gestion des licences**, procédez comme suit :

1. Sélectionnez **Paiement à l'utilisation** , puis sélectionnez **Suivant**.
2. Sélectionnez votre édition de Windows avec **expérience de bureau** , puis sélectionnez **Suivant**.
3. Acceptez les termes du contrat de licence en sélectionnant **Accepter** pour continuer.
4. Sous **Sélectionner l'emplacement d'installation Windows Server**, choisissez votre disque et votre partition en fonction de vos besoins. Ensuite, sélectionnez **Suivant**.
5. Sur l'écran **Prêt pour l'installation**, sélectionnez **Installer**.

Le processus d'installation redémarre automatiquement votre appareil si nécessaire. Vous êtes invité à créer un mot de passe pour poursuivre l'installation. Une fois l'installation terminée et après votre connexion, l'assistant **Installation d'Azure Arc** s'affiche. Suivez ces étapes pour continuer à configurer le paiement à l'utilisation :

1. Sur l'écran **Prise en main d'Azure Arc**, sélectionnez **Suivant**.
2. Sur l'écran **Installation d'Azure Arc** , votre appareil effectue plusieurs vérifications pour installer l'agent Azure Connected Machine (AzCM). Ensuite, sélectionnez **Configurer**.
3. Sur l'écran **Configurer Azure Arc**, sélectionnez **Suivant**.
4. Sur l'écran **Se connecter à Azure**, sélectionnez votre cloud Azure, connectez-vous, puis sélectionnez **Suivant**.
5. Dans l'écran **Détails de la ressource** , continuez à renseigner les informations requises, puis sélectionnez **Suivant**.
6. Sur l'écran **Choisir une méthode de gestion des licences pour Windows Server**, sélectionnez **Paiement à l'utilisation avec Azure**, puis **Suivant**.
7. Une fois que vous atteignez le dernier écran pendant le processus de configuration, sélectionnez **Terminer**.

> **Notes**
>
> Si vous sélectionnez **Utiliser une clé de produit** sur l'écran **Choisir une méthode de gestion des licences pour Windows Server** et continuez avec l'Assistant Installation, le paiement à l'utilisation n'est pas activé, même si vous aviez choisi cette option au début de l'installation.
>
> Si vous décidez de ne pas vous servir du paiement à l'utilisation, vous devez entrer manuellement une clé de produit à l'aide d'une méthode prise en charge. Toutefois, si vous souhaitez toujours utiliser le paiement à l'utilisation, même s'il n'a pas été activé via l'assistant de configuration d'Azure Arc, vous pouvez l'activer via le portail Azure.

Gérer le paiement à l'utilisation de Windows Server

Vous pouvez gérer le paiement à l'utilisation pour Windows Server via le portail Azure, PowerShell ou l'API. Même si vous n'avez pas activé le paiement à l'utilisation lors de l'installation initiale du système d'exploitation, vous pouvez toujours l'activer par la suite, à condition que les prérequis soient remplis.

Pour activer le paiement à l'utilisation pour Windows Server, procédez comme suit :

portail Azure

Pour activer le paiement à l'utilisation pour Windows Server via le portail Azure, procédez comme suit :

1. Accédez à votre portail Azure, puis recherchez et sélectionnez **Machines - Azure Arc**.
2. Sélectionnez la machine sur laquelle vous souhaitez activer le paiement à l'utilisation pour Windows Server.
3. Sélectionnez la vignette **Paiement à l'utilisation** .
4. Cochez la case en regard de **Paiement à l'utilisation avec Azure**, puis sélectionnez **Confirmer**.

Vous pouvez également, dans le menu du volet gauche, développer **des licences**, sélectionner **Windows Server** et suivre l'étape 4.

Pour désactiver le paiement à l'utilisation pour Windows Server, procédez comme suit :

portail Azure

Pour désactiver le paiement à l'utilisation pour Windows Server via le portail Azure, procédez comme suit :

1. Accédez à votre portail Azure, puis recherchez et sélectionnez **Machines - Azure Arc**.
2. Sélectionnez la machine sur laquelle vous souhaitez désactiver le paiement à l'utilisation pour Windows Server.
3. Sélectionnez la vignette **Paiement à l'utilisation** .
4. Décochez la case en regard de **Paiement à l'utilisation avec Azure**, puis sélectionnez **Confirmer**.
5. La notification **Désactiver le paiement à l'utilisation** s'affiche pour vous demander si vous souhaitez désactiver. Sélectionnez **Désactiver**.

Vous pouvez également, dans le menu du volet gauche, développer **des licences**, sélectionner **Windows Server** et suivre l'étape 4.

Voir aussi

- Serveurs avec Azure Arc
- Connecter des machines Windows Server à Azure via le programme d'installation d'Azure Arc

Qu’est-ce que Windows Server Annual Channel for Containers ?

15/08/2025S’applique à: ✅ Windows Server, version 23H2 and later

Le canal annuel Windows Server pour conteneurs est un système d’exploitation qui héberge des conteneurs Windows Server. Annual Channel permet aux clients qui innovent rapidement de profiter des nouvelles capacités du système d’exploitation à un rythme plus rapide, en se concentrant sur les conteneurs, les micro-services et la portabilité.

Windows Server Annual Channel for Containers est synonyme de nouvelles fonctionnalités et fonctionnalités publiées sur une base annuelle. Les sorties plus fréquentes de Annual Channel permettent aux clients de profiter plus rapidement de l’innovation, avec un accent sur les conteneurs et les micro-services. Pour en savoir plus sur le cycle de vie, consultez l’article sur le cycle de vie de Windows Server Annual Channel. Pour en savoir plus sur la différence entre les canaux de service, consultez la rubrique les canaux de service de Windows Server.

Plateformes prises en charge

Un hôte de conteneur Windows Server, version 23H2, ne prend en charge que l’image de conteneur du Canal de Service à Long Terme (LTSC) de Windows Server 2022.

Portability

La portabilité est une fonctionnalité importante introduite dans Windows Server Annual Channel for Containers qui permet aux utilisateurs d’exécuter des charges de travail avec différentes versions d’images de conteneur. La portabilité permet aux images de conteneurs basées sur Windows Server 2022 de fonctionner sur des hôtes de session exécutant des versions ultérieures de Windows Server. Ce support accru aide des services de conteneurs comme AKS à mettre à jour les systèmes d’exploitation sur les hôtes de conteneurs sur une base plus fréquente sans vous obliger à mettre à jour les conteneurs eux-mêmes. La portabilité ne facilite pas seulement le processus de mise à niveau, mais aide également les développeurs à tirer pleinement parti de la flexibilité et de la compatibilité améliorées que les conteneurs offrent. Pour plus d’informations sur la portabilité, veuillez consulter la rubrique la Portabilité dans Windows Server Annual Channel for Containers.

Prise en main de Windows Server Annual Channel for Containers

Pour bien démarrer avec Windows Server Annual Channel for Containers, utilisez votre méthode préférée pour installer Windows Server sur votre hôte de conteneur. Annual Channel est disponible pour les clients sous licence en volume avec Assurance Logicielle et programmes de fidélité tels que les abonnements Visual Studio. Vous pouvez obtenir les versions d'Annual Channel depuis :

- Centre de gestion des licences en volume (VLSC) : les clients sous licence en volume avec Software Assurance peuvent obtenir cette version en accédant au Centre de gestion des licences en volume et en sélectionnant **Se connecter**. Enfin, sélectionnez **Téléchargements et clés**, recherchez canal annuel, puis téléchargez le média.
- Abonnements Visual Studio : Les abonnés Visual Studio peuvent obtenir des versions de canal annuelles en les téléchargeant à partir de la page de téléchargement de l'Abonné Visual Studio. Si vous n'êtes pas déjà abonné, accédez à abonnements Visual Studio pour vous inscrire, puis visitez la page Téléchargements Abonné Visual Studio. Les versions obtenues via les abonnements Visual Studio sont destinées au développement et aux tests uniquement.

> ⚠ **Avertissement**
>
> Annual Channel ne peut être installé qu'avec l'option d'installation Server Core. Pour passer à une version d'Annual Channel depuis LTSC, ou pour mettre à niveau une installation existante du Canal Annuel, vous devez effectuer une installation propre.

Contenu connexe

- Portabilité dans Windows Server Annual Channel pour les conteneurs

Configuration matérielle requise pour Windows Server

02/07/2025

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

Pour installer correctement Windows Server, votre ordinateur doit répondre aux exigences matérielles minimales décrites dans cet article. Si votre ordinateur ne remplit pas ces conditions, le produit risque de ne pas s'installer correctement. Les exigences réelles varient en fonction de la configuration de votre système, des applications et des fonctionnalités installées.

Sauf indication contraire, ces exigences matérielles minimales s'appliquent à toutes les options d'installation (Server Core et Serveur avec interface de bureau) pour les éditions Windows Server Standard et Windows Server Datacenter.

> **ⓘ Important**
>
> L'étendue très diversifiée des déploiements potentiels rend irréaliste l'état des exigences matérielles recommandées qui seraient applicables. Consultez la documentation de chacun des rôles serveur que vous envisagez de déployer pour en savoir plus sur les besoins en ressources des rôles serveur particuliers. Pour obtenir les meilleurs résultats, procédez à des déploiements tests afin de déterminer la configuration matérielle appropriée pour vos propres scénarios de déploiement.

Components

CPU

Les performances du processeur dépendent non seulement de la fréquence d'horloge du processeur, mais également du nombre de cœurs de processeur et de la taille du cache de processeur. Les exigences relatives au processeur sont les suivantes.

Minimum:

- Processeur 1,4 GHz 64 bits
- Compatible avec le jeu d'instructions x64
- Prise en charge de NX et DEP

- Prise en charge des instructions CMPXCHG16b, LAHF/SAHF et PrefetchW
- Prise en charge de la traduction d'adresses de second niveau (EPT ou NPT)
- Prise en charge du jeu d'instructions SSE4.2 (Streaming SIMD Extensions 4.2)
- Support for SSE4.2 instruction set (Streaming SIMD Extensions 4.2)

Vous pouvez utiliser Coreinfo, qui est un outil inclus dans Windows Sysinternals, pour vérifier les fonctionnalités de votre processeur.

Configuration requise pour le serveur de base sécurisé

Le cœur sécurisé est un ensemble de fonctionnalités de sécurité intégrées du matériel, du microprogramme, du pilote et du système d'exploitation qui offrent une protection renforcée contre les menaces avancées. Les systèmes de base sécurisés offrent une sécurité qui démarre avant le démarrage du système d'exploitation et continue tout au long de l'opération du système. Les fonctionnalités de serveur de base sécurisée sont disponibles dans Windows Server 2022 et versions ultérieures. Pour déployer un serveur sécurisé, votre appareil doit répondre à ces exigences supplémentaires :

- **Remapping DMA (IOMMU)** : la prise en charge *d'Intel VT-d* ou *AMD-Vi* est nécessaire pour garantir une gestion sécurisée et efficace de l'accès direct à la mémoire (DMA) par les appareils, en protégeant contre l'accès à la mémoire non autorisé.
- **Protection DMA du noyau** : le système doit disposer d'une fonctionnalité d'opt-in pour la protection DMA du noyau, ce qui permet d'empêcher les attaques qui exploitent des périphériques externes pour obtenir un accès non autorisé.
- **DRTM (Racine dynamique de confiance pour la mesure)** : cette fonctionnalité est nécessaire pour garantir un processus de démarrage sécurisé en vérifiant l'intégrité de l'environnement de démarrage du système, en vous protégeant contre les attaques basées sur les microprogrammes.

> ⓘ **Notes**
>
> Outre les exigences spécifiques décrites pour le serveur de base sécurisé, les fonctionnalités suivantes doivent être activées sur votre matériel :
>
> - TPM 2.0
> - Démarrage sécurisé

- Prise en charge de la sécurité basée sur la virtualisation (VBS), y compris les extensions de virtualisation matérielle

Pour plus d'informations, consultez Qu'est-ce que le serveur de base sécurisé ?.

Autres exigences

Il existe d'autres exigences matérielles à prendre en compte, en fonction de votre scénario :

- Lecteur DVD (si vous envisagez d'installer le système d'exploitation à partir d'un support DVD)

Les éléments suivants sont obligatoires uniquement pour certaines fonctionnalités :

- Système et microprogramme basés sur UEFI 2.3.1c qui prennent en charge le démarrage sécurisé.
- Module de plateforme sécurisée (TPM).
- Graphiques intégrés ou dédiés et moniteurs capables de Super VGA (1024 x 768) ou d'une résolution supérieure.
- Clavier et souris (ou autre appareil de pointage compatible).
- Accès à internet. (Les frais peuvent s'appliquer.)

ⓘ Notes

Une puce TPM est nécessaire pour utiliser certaines fonctionnalités, telles que **le chiffrement de lecteur BitLocker**. Si votre ordinateur dispose d'un TPM, il doit répondre à ces exigences :

- Les modules de plateforme sécurisée matériels doivent implémenter la version 2.0 de la spécification de module de plateforme sécurisée.
- Les modules TPM qui implémentent la version 2.0 doivent disposer d'un certificat EK préprovisionné sur le module TPM par le fournisseur de matériel ou capables d'être récupérés par l'appareil pendant le premier démarrage.
- Les modules de plateforme sécurisée qui implémentent la version 2.0 doivent être livrés avec des banques de registre de configuration de plateforme (PCR) SHA-256 et implémenter les PCR 0 à 23 pour SHA-256. Il est acceptable d'expédier des TPM avec

une banque RPC modifiable unique qui peut être utilisée pour les mesures SHA-1 et SHA-256.

Comparaison des verrouillages et des limites dans Windows Server

14/08/2025

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

Le choix de l'édition appropriée de Windows Server est essentiel pour répondre aux exigences techniques et métier de votre organisation. Cet article fournit une comparaison en parallèle des verrous et limites clés du système d'exploitation sur les éditions de Windows Server prises en charge. Utilisez ces tableaux pour comparer les fonctionnalités clés des différentes éditions de Windows Server, telles que :

- Nombre maximal d'utilisateurs
- Limites de connexion
- Droits de virtualisation
- Prise en charge matérielle

Ces informations peuvent vous aider à choisir la version qui convient le mieux à vos besoins.

Sélectionnez une version de Windows Server pour afficher ses verrous et ses limites.

Verrouillages et limites

Pour afficher les verrous et les limites de Windows Server 2025, sélectionnez l'onglet de comparaison complète ou l'onglet des différences entre les versions.

Comparaison complète

Agrandir le tableau

Verrouillages et limites	Windows Server 2025 Standard	Windows Server 2025 Datacenter	Windows Server 2025 Datacenter : Azure Edition
Nombre maximal d'utilisateurs	Basé sur les licences d'accès client	Basé sur les licences d'accès client	Basé sur les licences d'accès client
Nombre maximal de connexions SMB	16,777,216	16,777,216	16,777,216

Verrouillages et limites	Windows Server 2025 Standard	Windows Server 2025 Datacenter	Windows Server 2025 Datacenter : Azure Edition
Nombre maximal de connexions RRAS	Unlimited	Unlimited	Unlimited
Nombre maximal de connexions IAS	2,147,483,647	2,147,483,647	2,147,483,647
Nombre maximal de connexions RDS	65,535	65,535	65,535
Nombre maximal de sockets 64 bits	64	64	64
Nombre maximal de cœurs	Unlimited	Unlimited	2048 processeurs logiques
Ram maximale	• 4 Po pour les hôtes prenant en charge la pagination à 5 niveaux • 256 To pour les hôtes prenant en charge la pagination à 4 niveaux.	• 4 Po pour les hôtes prenant en charge la pagination à 5 niveaux • 256 To pour les hôtes prenant en charge la pagination à 4 niveaux.	• 240 To pour une machine virtuelle de 2e génération • 1 To pour une machine virtuelle de 1re génération
Peut être utilisé comme invité de virtualisation	Oui, deux machines virtuelles plus un hôte Hyper-V par licence	Oui, **nombre illimité de machines virtuelles**, plus un hôte Hyper-V par licence	Oui, **nombre illimité de machines virtuelles**, plus un hôte Hyper-V par licence
Conteneurs Windows Server	Unlimited	Unlimited	Unlimited
Conteneurs isolés OSE/Hyper-V virtuels	2	Unlimited	Unlimited

Verrouillages et limites	Windows Server 2025 Standard	Windows Server 2025 Datacenter	Windows Server 2025 Datacenter : Azure Edition
Conteneurs Windows Server	Conteneurs Windows en nombre illimité et jusqu'à deux conteneurs Hyper-V	Conteneurs Windows et Hyper-V en nombre illimité	Conteneurs Windows et Hyper-V en nombre illimité
Réplica de stockage	1 partenariat et 1 groupe de ressources avec un seul volume de 2 To	**Unlimited**	**Unlimited**

Fonctionnalités supprimées ou non développées dans Windows Server

24/09/2025

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

Chaque version de Windows Server apporte de nouvelles fonctionnalités et améliorations. Parfois, les fonctionnalités plus anciennes sont supprimées pour rendre la place pour de meilleures alternatives. Cet article détaille les fonctionnalités et fonctionnalités supprimées ou déconseillées dans Windows Server.

> **Conseil**
>
> Vous pouvez obtenir un accès anticipé aux builds Windows Server en rejoignant le programme Windows Insider pour Entreprises, qui est un excellent moyen de tester les modifications des fonctionnalités.

> **Notes**
>
> Les versions de canal de maintenance à long terme (LTSC) de Windows Server ont une politique de cycle de vie fixe qui comprend 5 ans de support standard et 5 ans de support étendu pour un cycle de vie total de 10 ans. Pour en savoir plus, consultez :
>
> - Politique de cycle de vie fixe
> - Termes et définitions du cycle de vie

Cette liste est susceptible de changer et n'inclut peut-être pas toutes les fonctionnalités concernées.

Les fonctionnalités ne sont plus en cours de développement

Nous ne développons plus activement ces fonctionnalités et pourrions les supprimer d'une prochaine mise à jour. Certaines fonctionnalités ont été remplacées par d'autres fonctionnalités ou fonctionnalités. D'autres sont désormais disponibles à partir de différentes sources. *La dépréciation* signifie qu'une fonctionnalité, une fonctionnalité ou un service n'est plus en développement actif. Une fonctionnalité déconseillée peut être supprimée dans les versions ultérieures. Un composant déconseillé est toujours fourni dans Windows Server, est pris en

charge pour les déploiements de production et continue de recevoir des mises à jour de sécurité et de qualité par cycle de vie du produit.

Windows Server 2025

Agrandir le tableau

Feature	Explanation
Navigateur ordinateur	Le pilote et le service de l'Explorateur d'ordinateurs sont déconseillés. Le navigateur (protocole de navigateur et service) est un protocole d'emplacement d'appareil obsolète et non sécurisé. Ce protocole, service et pilote ont été désactivés par défaut dans Windows 10, avec la suppression du service SMB1. Pour plus d'informations sur le protocole CIFS Browser utilisé par le lecteur et le service Computer Browser, consultez MS-BRWS Common Internet File System.
Clustering de basculement Ensembles de clusters	La fonctionnalité Ensembles de clusters de cluster de basculement n'est plus en développement de fonctionnalités actives et est déconseillée.
Équilibrage de la charge réseau (NLB)	L'équilibrage de charge réseau ne fait plus l'objet d'un développement actif et est obsolète. Envisagez d'utiliser un équilibreur de charge logiciel (SLB) comme alternative. Pour en savoir plus sur SLB, consultez Qu'est-ce que l'équilibreur de charge logiciel (SLB) pour SDN ?
NTLM	NTLMv1 est supprimé. LANMAN et NTLMv2 ne sont plus en cours de développement de fonctionnalités actifs et sont déconseillés. NTLMv2 continuera de fonctionner, mais sera supprimé de Windows Server dans une prochaine version. Remplacez les appels à NTLM par les appels à Negotiate, qui essaie de s'authentifier auprès de Kerberos et de revenir uniquement à NTLM si nécessaire. Pour plus d'informations, consultez l'évolution de l'authentification Windows .
Mailslots distants	Les mailslots distants sont déconseillés. Le protocole Remote Mailslot, qui a été introduit initialement dans MS DOS, est une méthode IPC obsolète et simple qui n'est pas fiable et non sécurisée. Ce protocole a d'abord été désactivé par défaut dans windows 11 Insider Preview Build . Pour plus d'informations sur les mailslots distants, consultez About Mailslots and [MS-MAIL] : Remote Mailslot Protocol.
TLS 1.0 TLS 1.1	Les versions TLS 1.0 et 1.1 sont déconseillées par normes Internet et les organismes de réglementation en raison des préoccupations de sécurité mentionnées dans RFC 8996 . Ces versions sont désactivées par défaut dans Windows Server 2025. Pour plus d'informations sur l'abandon de TLS, consultez l'abandon de TLS 1.0 et TLS 1.1 dans Windows.

Feature	Explanation
Service redirecteur WebDAV	Le service redirecteur WebDAV est déconseillé. Le service n'est pas installé par défaut dans Windows Server. Pour plus d'informations sur le service redirecteur WebDAV, consultez WebDAV - Applications Win32.
Base de données interne Windows (WID)	WID est utilisé par plusieurs rôles, notamment AD FS, AD RMS, IPAM, RD Connection Broker et WSUS. Envisagez d'utiliser une version gratuite ou complète de SQL Server pour ces rôles. WID sera supprimé de Windows dans une prochaine version. Pour en savoir plus, consultez les éditions de SQL Server.
Ligne de commande Windows Management Instrumentation (WMIC)	À compter de Windows Server 2025, WMIC est disponible en tant que fonctionnalité à la demande (FOD). Elle peut être ajoutée avec la `DISM /Add-Capability` commande. Elle sera supprimée de Windows dans une prochaine version. PowerShell pour WMI remplace l'outil WMIC. Utilisez PowerShell ou interrogez par programmation WMI comme remplacement de WMIC. Pour en savoir plus sur l'amortissement WMIC, consultez dépréciation de l'utilitaire WMI (WMIC) : étapes suivantes .
VBScript	VBScript est disponible en tant qu'FOD et préinstallé dans Windows Server 2025, avant sa suppression du système d'exploitation dans une version ultérieure. Pour remplacer VBScript, utilisez PowerShell pour automatiser des tâches, des actions personnalisées ou des scripts. Pour en savoir plus sur la migration vers PowerShell, consultez le Guide de conversion VBScript-to-Windows PowerShell. Si vous utilisez VBScript dans votre page web, les fonctionnalités sont actuellement limitées aux navigateurs qui précèdent Internet Explorer 11. Nous vous recommandons de migrer vos pages web vers JavaScript, qui fournit une compatibilité entre navigateurs et une prise en charge moderne du navigateur.
Windows Server Update Services (WSUS)	WSUS n'est plus développé activement. Toutes les fonctionnalités et le contenu existants continuent d'être disponibles pour vos déploiements.

Fonctionnalités supprimées

Nous supprimons les fonctionnalités et fonctionnalités suivantes de l'image de produit installée dans Windows Server. Les applications ou le code qui dépendent de ces fonctionnalités ne fonctionnent pas dans les versions ultérieures, sauf si vous utilisez une autre méthode. La suppression se produit lorsqu'une fonctionnalité ou une fonctionnalité n'est plus disponible pour être utilisée et est éliminée d'un produit ou d'un service. La suppression des

fonctionnalités et fonctionnalités peut avoir lieu dans n'importe quelle version de Windows Server. Certaines fonctionnalités sont déconseillées, mais toujours fournies dans les versions actuelles de Windows Server. Les composants ne sont pas supprimés des versions généralement disponibles et prises en charge qui sont encore dans leur cycle de vie de produit.

Windows Server 2025

Agrandir le tableau

Feature	Explanation
Data Encryption Standard (DES)	DES, le chiffrement de chiffrement de bloc à clé symétrique n'est pas considéré comme sécurisé contre les attaques de chiffrement modernes. Il est remplacé par des algorithmes de chiffrement plus robustes. DES a été désactivé à partir de Windows Server 2008 R2 et est supprimé de Windows Server 2025 et versions ultérieures.
Console de gestion IIS 6 (Web-Lgcy-Mgmt-Console)	La console est supprimée car elle n'est plus développée dans Windows Server 2019. Vous devez également commencer à migrer à partir d'IIS 6.0 ou des versions antérieures vers la dernière version d'IIS, qui est toujours disponible dans la version la plus récente de Windows Server.
NTLMv1	Remplacez les appels à NTLM par les appels à Negotiate, qui essaie de s'authentifier auprès de Kerberos et revient uniquement à NTLM si nécessaire. Pour plus d'informations, consultez l'évolution de l'authentification Windows.
Windows PowerShell 2.0	À compter de la mise à jour de septembre 2025, Windows Server 2025 n'inclut plus Windows PowerShell 2.0. Si Windows PowerShell 2.0 a été installé avant la mise à jour de septembre, vous ne pouvez plus l'utiliser. Les applications et composants Windows PowerShell 2.0 doivent être migrés vers PowerShell 5.0 ou version ultérieure. Pour en savoir plus sur l'obsolescence, consultez Windows PowerShell 2.0 Obsolescence.
Serveur SMTP	Étant donné que les fonctionnalités smtp Server ont été supprimées de Windows Server 2025, il n'existe aucun remplacement dans le système d'exploitation. Envisagez d'utiliser Exchange Server ou un serveur SMTP non Microsoft comme alternative. Pour en savoir plus sur l'activation de la connexion SMTP dans Exchange Server, consultez Recevoir des connecteurs dans Exchange Server.
Wordpad	Nous vous recommandons Microsoft Word pour les documents de texte enrichi tels `.doc` que et `.rtf`, et le Bloc-notes Windows pour les documents en texte brut comme `.txt`.

Contenu connexe

- Obsolescence : signification dans le cycle de vie Windows

Informations de publication de Windows Server

Windows Server dispose de deux canaux de publication principaux : Le canal de maintenance à long terme et le canal annuel. Le canal de maintenance à long terme (LTSC) est une option à plus long terme axée sur un cycle de vie traditionnel de mises à jour de la sécurité et de la qualité. L canal annuel (AC) propose des versions plus fréquentes, axées sur les conteneurs et les microservices, afin que vous puissiez tirer parti de l'innovation plus rapidement.

La version actuelle du LTSC est Windows Server 2025. La dernière version du AC est la version 23H2 de Windows Server. L'accent est mis sur la virtualisation, les conteneurs et l'innovation des microservices avec Azure Stack HCI, les conteneurs Windows et AKS sur Azure Stack HCI.

Si vous êtes un administrateur informatique et que vous souhaitez obtenir des informations de manière programmatique à partir de cette page, utilisez la API de Mises à jour Windows dans Microsoft Graph.

Versions principales de Windows Server par option de maintenance

(Toutes les dates sont indiquées au format ISO 8601 : AAAA-MM-JJ)

Agrandir le tableau

Version Windows Server	Option de maintenance	Éditions	Date de disponibilité	Date de fin du support standard	Date de fin du support étendu	Dernière mise à jour pour ESU	Date de la dernière révision	D b
Windows Server 2025	Long-Term Servicing Channel (LTSC)	Datacenter, Standard	2024-11-01	2029-11-13	2034-11-14	2026-10 B	2026-10-13	2
Windows Server 2022	Long-Term Servicing Channel (LTSC)	Datacenter, Standard	2021-08-18	Fin des mises à jour	2031-10-14	2026-10 B	2026-10-13	2
Windows Server 2019 (version 1809)	Long-Term Servicing Channel (LTSC)	Datacenter, Standard	2018-11-13	Fin des mises à jour	2029-01-09	2026-10 B	2026-10-13	1
Windows Server 2016 (version 1607)	Long-Term Servicing Branch (LTSB)	Datacenter, Essentials, Standard	2016-08-02	Fin des mises à jour	2027-01-12	2026-10 B	2026-10-13	1

> **Remarque**
>
> Windows Server est régi par la politique de cycle de vie fixe. Pour plus d'informations sur les exigences de maintenance et d'autres informations importantes, consultez les FAQ sur le cycle de vie Windows et comparaison des canaux de maintenance. Pour en savoir plus sur la politique de cycle de vie de Windows Server, consultez Versions de Windows Server.

Historique des versions de Windows Server

Le tableau ci-dessous présente l'historique de toutes les mises à jour mensuelles de la préversion de sécurité et non relatives à la sécurité publiées pour les versions prises en charge de Windows Server dans le Canal de maintenance à long terme.

Notez que la colonne Type de mise à jour référence chaque mise à jour mensuelle par année et par mois de publication, suivie d'une lettre indiquant la semaine du mois (B correspond à la deuxième semaine du mois, D à la quatrième semaine du mois). Les mises à jour hors bande sont référencées sous l'abréviation OOB. Cette notation abrégée s'aligne sur ce que vous voyez dans Microsoft Intune. Pour plus d'informations, consultez Type de mises à jour publiées.

Les notes de publication pour Windows Server sont disponibles sur Historique des mises à jour Windows Server 2025, Historique des mises à jour de Windows Server 2022, Historique des mises à jour de Windows Server 2019 et Historique des mises à jour de Windows Server 2016.

Windows Server 2025 (OS build 26100)

Agrandir le tableau

Option de maintenance	Type de mise à jour	Date de disponibilité	Build	Article de la base de connaissances
LTSC	2026-10 B	2026-10-13	26100.33650	KB5126646
LTSC	2026-09 OOB	2026-09-14	26100.33451	KB5129235
LTSC	2026-09 B	2026-09-08	26100.33438	KB5122871
LTSC	2026-08 B	2026-08-11	26100.33296	KB5120233
LTSC	2026-07 B	2026-07-14	26100.33158	KB5099536
LTSC	2026-06 B	2026-06-09	26100.32995	KB5094125
LTSC	2026-05 B	2026-05-12	26100.32860	KB5087539
LTSC	2026-04 OOB	2026-04-19	26100.32698	KB5091157
LTSC	2026-04 B	2026-04-14	26100.32690	KB5082063
LTSC	2026-03 B	2026-03-10	26100.32522	KB5078740
LTSC	2026-02 B	2026-02-10	26100.32370	KB5075899

LTSC	2026-01 OOB	2026-01-24	26100.32236	KB5078135
LTSC	2026-01 OOB	2026-01-17	26100.32234	KB5077793
LTSC	2026-01 B	2026-01-13	26100.32230	KB5073379
LTSC	2025-12 B	2025-12-09	26100.7462	KB5072033
LTSC	2025-11 OOB	2025-11-18	26100.7178	KB5072359
LTSC	2025-11 B	2025-11-11	26100.7171	KB5068861
LTSC	2025-10 OOB	2025-10-23	26100.6905	KB5070881
LTSC	2025-10 OOB	2025-10-20	26100.6901	KB5070773
LTSC	2025-10 B	2025-10-14	26100.6899	KB5066835
LTSC	2025-09 OOB	2025-09-22	26100.6588	KB5068221
LTSC	2025-09 B	2025-09-09	26100.6584	KB5065426
LTSC	2025-08 B	2025-08-12	26100.4946	KB5063878
LTSC	2025-07 OOB	2025-07-13	26100.4656	KB5064489
LTSC	2025-07 B	2025-07-08	26100.4652	KB5062553
LTSC	2025-06 B	2025-06-10	26100.4349	KB5060842
LTSC	2025-05 OOB	2025-05-27	26100.4066	KB5061977
LTSC	2025-05 B	2025-05-13	26100.4061	KB5058411
LTSC	2025-04 OOB	2025-04-16	26100.3781	KB5059087
LTSC	2025-04 B	2025-04-08	26100.3775	KB5055523
LTSC	2025-03 B	2025-03-11	26100.3476	KB5053598
LTSC	2025-02 B	2025-02-11	26100.3194	KB5051987
LTSC	2025-01 B	2025-01-14	26100.2894	KB5050009
LTSC	2024-12 B	2024-12-10	26100.2605	KB5048667
LTSC	2024-11 B	2024-11-12	26100.2314	KB5046617
LTSC	2024-10 A	2024-11-01	26100.1742	

▼ Windows Server 2022 (OS build 20348)

Agrandir le tableau

Option de maintenance	Type de mise à jour	Date de disponibilité	Build	Article de la base de connaissances
LTSC	2026-10 B	2026-10-13	20348.5761	KB5126655
LTSC	2026-09 OOB	2026-09-14	20348.5631	KB5129237
LTSC	2026-09 B	2026-09-08	20348.5622	KB5122882
LTSC	2026-08 B	2026-08-11	20348.5499	KB5120242

LTSC	2026-07 B	2026-07-14	20348.5386	KB5099540
LTSC	2026-06 B	2026-06-09	20348.5256	KB5094128
LTSC	2026-05 B	2026-05-12	20348.5139	KB5087545
LTSC	2026-04 OOB	2026-04-19	20348.5024	KB5091575
LTSC	2026-04 B	2026-04-14	20348.5020	KB5082142
LTSC	2026-03 B	2026-03-10	20348.4893	KB5078766
LTSC	2026-02 OOB	2026-03-02	20348.4776	KB5082314
LTSC	2026-02 B	2026-02-10	20348.4773	KB5075906
LTSC	2026-01 OOB	2026-01-24	20348.4651	KB5078136
LTSC	2026-01 OOB	2026-01-17	20348.4650	KB5077800
LTSC	2026-01 B	2026-01-13	20348.4648	KB5073457
LTSC	2025-12 B	2025-12-09	20348.4529	KB5071547
LTSC	2025-11 B	2025-11-11	20348.4405	KB5068787
LTSC	2025-10 OOB	2025-10-23	20348.4297	KB5070884
LTSC	2025-10 B	2025-10-14	20348.4294	KB5066782
LTSC	2025-09 B	2025-09-09	20348.4171	KB5065432
LTSC	2025-08 B	2025-08-12	20348.4052	KB5063880
LTSC	2025-07 B	2025-07-08	20348.3932	KB5062572
LTSC	2025-06 B	2025-06-10	20348.3807	KB5060526
LTSC	2025-05 OOB	2025-05-23	20348.3695	KB5061906
LTSC	2025-05 B	2025-05-13	20348.3692	KB5058385
LTSC	2025-04 OOB	2025-04-16	20348.3566	KB5059092
LTSC	2025-04 OOB	2025-04-11	20348.3561	KB5058920
LTSC	2025-04 B	2025-04-08	20348.3453	KB5055526
LTSC	2025-03 B	2025-03-11	20348.3328	KB5053603
LTSC	2025-02 B	2025-02-11	20348.3207	KB5051979
LTSC	2025-01 OOB	2025-01-18	20348.3095	KB5052819
LTSC	2025-01 B	2025-01-14	20348.3091	KB5049983
LTSC	2024-12 B	2024-12-10	20348.2966	KB5048654
LTSC	2024-11 B	2024-11-12	20348.2849	KB5046616
LTSC	2024-10 B	2024-10-08	20348.2762	KB5044281
LTSC	2024-09 B	2024-09-10	20348.2700	KB5042881
LTSC	2024-08 B	2024-08-13	20348.2655	KB5041160

LTSC	2024-07 B	2024-07-09	20348.2582	KB5040437
LTSC	2024-06 OOB	2024-06-20	20348.2529	KB5041054
LTSC	2024-06 B	2024-06-11	20348.2527	KB5039227
LTSC	2024-05 B	2024-05-14	20348.2461	KB5037782
LTSC	2024-04 B	2024-04-09	20348.2402	KB5036909
LTSC	2024-03 OOB	2024-03-22	20348.2342	KB5037422
LTSC	2024-03 B	2024-03-12	20348.2340	KB5035857
LTSC	2024-02 B	2024-02-13	20348.2322	KB5034770
LTSC	2024-01 B	2024-01-09	20348.2227	KB5034129
LTSC	2023-12 B	2023-12-12	20348.2159	KB5033118
LTSC	2023-11 B	2023-11-14	20348.2113	KB5032198
LTSC	2023-10 B	2023-10-10	20348.2031	KB5031364
LTSC	2023-09 B	2023-09-12	20348.1970	KB5030216
LTSC	2023-08 B	2023-08-08	20348.1906	KB5029250
LTSC	2023-07 B	2023-07-11	20348.1850	KB5028171
LTSC	2023-06 B	2023-06-13	20348.1787	KB5027225
LTSC	2023-05 B	2023-05-09	20348.1726	KB5026370
LTSC	2023-04 B	2023-04-11	20348.1668	KB5025230
LTSC	2023-03 B	2023-03-14	20348.1607	KB5023705
LTSC	2023-02 B	2023-02-14	20348.1547	KB5022842
LTSC	2023-01 B	2023-01-10	20348.1487	KB5022291
LTSC	2022-12 OOB	2022-12-20	20348.1368	KB5022553
LTSC	2022-12 B	2022-12-13	20348.1366	KB5021249
LTSC	2022-11 C	2022-11-22	20348.1311	KB5020032
LTSC	2022-11 OOB	2022-11-17	20348.1251	KB5021656
LTSC	2022-11 B	2022-11-08	20348.1249	KB5019081
LTSC	2022-10 C	2022-10-25	20348.1194	KB5018485
LTSC	2022-10 OOB	2022-10-17	20348.1131	KB5020436
LTSC	2022-10 B	2022-10-11	20348.1129	KB5018421
LTSC	2022-09 C	2022-09-20	20348.1070	KB5017381
LTSC	2022-09 B	2022-09-13	20348.1006	KB5017316
LTSC	2022-08 C	2022-08-16	20348.946	KB5016693
LTSC	2022-08 B	2022-08-09	20348.887	KB5016627

LTSC	2022-07 C	2022-07-19	20348.859	KB5015879
LTSC	2022-07 B	2022-07-12	20348.825	KB5015827
LTSC	2022-06 C	2022-06-23	20348.803	KB5014665
LTSC	2022-06 B	2022-06-14	20348.768	KB5014678
LTSC	2022-05 C	2022-05-24	20348.740	KB5014021
LTSC	2022-05 OOB	2022-05-19	20348.709	KB5015013
LTSC	2022-05 B	2022-05-10	20348.707	KB5013944
LTSC	2022-04 C	2022-04-25	20348.681	KB5012637
LTSC	2022-04 B	2022-04-12	20348.643	KB5012604
LTSC	2022-03 C	2022-03-22	20348.617	KB5011558
LTSC	2022-03 B	2022-03-08	20348.587	KB5011497
LTSC	2022-02 C	2022-02-15	20348.558	KB5010421
LTSC	2022-02 B	2022-02-08	20348.524	KB5010354
LTSC	2022-01 C	2022-01-25	20348.502	KB5009608
LTSC	2022-01 OOB	2022-01-17	20348.473	KB5010796
LTSC	2022-01 B	2022-01-11	20348.469	KB5009555
LTSC	2022-01 OOB	2022-01-05	20348.407	KB5010197
LTSC	2021-12 B	2021-12-14	20348.405	KB5008223
LTSC	2021-11 C	2021-11-22	20348.380	KB5007254
LTSC	2021-11 B	2021-11-09	20348.350	KB5007205
LTSC	2021-10 C	2021-10-26	20348.320	KB5006745
LTSC	2021-10 B	2021-10-12	20348.288	KB5006699
LTSC	2021-09 C	2021-09-27	20348.261	KB5005619
LTSC	2021-09 B	2021-09-14	20348.230	KB5005575
LTSC	2021-08 C	2021-08-26	20348.202	KB5005104

▼ Windows Server 2019 (OS build 17763)

Agrandir le tableau

Option de maintenance	Type de mise à jour	Date de disponibilité	Build	Article de la base de connaissances
LTSC	2026-10 B	2026-10-13	17763.9376	KB5126651
LTSC	2026-09 OOB	2026-09-14	17763.9247	KB5129238
LTSC	2026-09 B	2026-09-08	17763.9245	KB5122876
LTSC	2026-08 B	2026-08-11	17763.9121	KB5120238

LTSC	2026-07 B	2026-07-14	17763.9020	KB5099538
LTSC	2026-06 B	2026-06-09	17763.8880	KB5094123
LTSC	2026-05 B	2026-05-12	17763.8755	KB5087538
LTSC	2026-04 OOB	2026-04-19	17763.8647	KB5091573
LTSC	2026-04 B	2026-04-14	17763.8644	KB5082123
LTSC	2026-03 B	2026-03-10	17763.8511	KB5078752
LTSC	2026-02 B	2026-02-10	17763.8389	KB5075904
LTSC	2026-01 OOB	2026-01-24	17763.8281	KB5078131
LTSC	2026-01 OOB	2026-01-17	17763.8280	KB5077795
LTSC	2026-01 B	2026-01-13	17763.8276	KB5073723
LTSC	2025-12 OOB	2025-12-18	17763.8148	KB5074975
LTSC	2025-12 B	2025-12-09	17763.8146	KB5071544
LTSC	2025-11 B	2025-11-11	17763.8027	KB5068791
LTSC	2025-10 OOB	2025-10-23	17763.7922	KB5070883
LTSC	2025-10 B	2025-10-14	17763.7919	KB5066586
LTSC	2025-09 B	2025-09-09	17763.7792	KB5065428
LTSC	2025-08 OOB	2025-08-19	17763.7683	KB5066187
LTSC	2025-08 B	2025-08-12	17763.7678	KB5063877
LTSC	2025-07 B	2025-07-08	17763.7558	KB5062557
LTSC	2025-06 B	2025-06-10	17763.7434	KB5060531
LTSC	2025-05 OOB	2025-05-27	17763.7322	KB5061978
LTSC	2025-05 B	2025-05-13	17763.7314	KB5058392
LTSC	2025-04 OOB	2025-04-16	17763.7249	KB5059091
LTSC	2025-04 OOB	2025-04-11	17763.7240	KB5058922
LTSC	2025-04 B	2025-04-08	17763.7136	KB5055519
LTSC	2025-03 B	2025-03-11	17763.7009	KB5053596
LTSC	2025-02 B	2025-02-11	17763.6893	KB5052000
LTSC	2025-01 B	2025-01-14	17763.6775	KB5050008
LTSC	2024-12 B	2024-12-10	17763.6659	KB5048661
LTSC	2024-11 B	2024-11-12	17763.6532	KB5046615
LTSC	2024-10 B	2024-10-08	17763.6414	KB5044277
LTSC	2024-09 B	2024-09-10	17763.6293	KB5043050
LTSC	2024-08 B	2024-08-13	17763.6189	KB5041578

LTSC	2024-07 B	2024-07-09	17763.6054	KB5040430
LTSC	2024-06 B	2024-06-11	17763.5936	KB5039217
LTSC	2024-05 OOB	2024-05-23	17763.5830	KB5039705
LTSC	2024-05 B	2024-05-14	17763.5820	KB5037765
LTSC	2024-04 B	2024-04-09	17763.5696	KB5036896
LTSC	2024-03 OOB	2024-03-25	17763.5579	KB5037425
LTSC	2024-03 B	2024-03-12	17763.5576	KB5035849
LTSC	2024-02 B	2024-02-13	17763.5458	KB5034768
LTSC	2024-01 B	2024-01-09	17763.5329	KB5034127
LTSC	2023-12 B	2023-12-12	17763.5206	KB5033371
LTSC	2023-11 B	2023-11-14	17763.5122	KB5032196
LTSC	2023-10 B	2023-10-10	17763.4974	KB5031361
LTSC	2023-09 B	2023-09-12	17763.4851	KB5030214
LTSC	2023-08 B	2023-08-08	17763.4737	KB5029247
LTSC	2023-07 B	2023-07-11	17763.4645	KB5028168
LTSC	2023-06 B	2023-06-13	17763.4499	KB5027222
LTSC	2023-05 B	2023-05-09	17763.4377	KB5026362
LTSC	2023-04 B	2023-04-11	17763.4252	KB5025229
LTSC	2023-03 B	2023-03-14	17763.4131	KB5023702
LTSC	2023-02 B	2023-02-14	17763.4010	KB5022840
LTSC	2023-01 B	2023-01-10	17763.3887	KB5022286
LTSC	2022-12 OOB	2022-12-20	17763.3772	KB5022554
LTSC	2022-12 B	2022-12-13	17763.3770	KB5021237
LTSC	2022-11 OOB	2022-11-17	17763.3653	KB5021655
LTSC	2022-11 B	2022-11-08	17763.3650	KB5019966
LTSC	2022-10 OOB	2022-10-17	17763.3534	KB5020438
LTSC	2022-10 B	2022-10-11	17763.3532	KB5018419
LTSC	2022-09 C	2022-09-20	17763.3469	KB5017379
LTSC	2022-09 B	2022-09-13	17763.3406	KB5017315
LTSC	2022-08 C	2022-08-23	17763.3346	KB5016690
LTSC	2022-08 B	2022-08-09	17763.3287	KB5016623
LTSC	2022-07 C	2022-07-21	17763.3232	KB5015880
LTSC	2022-07 B	2022-07-12	17763.3165	KB5015811

LTSC	2022-06 C	2022-06-23	17763.3113	KB5014669
LTSC	2022-06 B	2022-06-14	17763.3046	KB5014692
LTSC	2022-05 C	2022-05-24	17763.2989	KB5014022
LTSC	2022-05 OOB	2022-05-19	17763.2931	KB5015018
LTSC	2022-05 B	2022-05-10	17763.2928	KB5013941
LTSC	2022-04 C	2022-04-21	17763.2867	KB5012636
LTSC	2022-04 B	2022-04-12	17763.2803	KB5012647
LTSC	2022-03 C	2022-03-22	17763.2746	KB5011551
LTSC	2022-03 B	2022-03-08	17763.2686	KB5011503
LTSC	2022-02 C	2022-02-15	17763.2628	KB5010427
LTSC	2022-02 B	2022-02-08	17763.2565	KB5010351
LTSC	2022-01 C	2022-01-25	17763.2510	KB5009616
LTSC	2022-01 OOB	2022-01-18	17763.2458	KB5010791
LTSC	2022-01 B	2022-01-11	17763.2452	KB5009557
LTSC	2022-01 OOB	2022-01-04	17763.2369	KB5010196
LTSC	2021-12 B	2021-12-14	17763.2366	KB5008218
LTSC	2021-11 C	2021-11-22	17763.2330	KB5007266
LTSC	2021-11 OOB	2021-11-14	17763.2305	KB5008602
LTSC	2021-11 B	2021-11-09	17763.2300	KB5007206
LTSC	2021-10 C	2021-10-19	17763.2268	KB5006744
LTSC	2021-10 B	2021-10-12	17763.2237	KB5006672
LTSC	2021-09 C	2021-09-21	17763.2213	KB5005625
LTSC	2021-09 B	2021-09-14	17763.2183	KB5005568
LTSC	2021-08 C	2021-08-26	17763.2145	KB5005102
LTSC	2021-08 B	2021-08-10	17763.2114	KB5005030
LTSC	2021-07 OOB	2021-07-27	17763.2091	KB5005394
LTSC	2021-07 C	2021-07-20	17763.2090	KB5004308
LTSC	2021-07 B	2021-07-13	17763.2061	KB5004244
LTSC	2021-07 OOB	2021-07-06	17763.2029	KB5004947
LTSC	2021-06 C	2021-06-15	17763.2028	KB5003703
LTSC	2021-06 B	2021-06-08	17763.1999	KB5003646
LTSC	2021-05 C	2021-05-20	17763.1971	KB5003217
LTSC	2021-05 B	2021-05-11	17763.1935	KB5003171

LTSC	2021-04 C	2021-04-22	17763.1911	KB5001384
LTSC	2021-04 B	2021-04-13	17763.1879	KB5001342
LTSC	2021-03 C	2021-03-25	17763.1852	KB5000854
LTSC	2021-03 OOB	2021-03-18	17763.1823	KB5001638
LTSC	2021-03 OOB	2021-03-15	17763.1821	KB5001568
LTSC	2021-03 B	2021-03-09	17763.1817	KB5000822
LTSC	2021-02 C	2021-02-16	17763.1790	KB4601383
LTSC	2021-02 B	2021-02-09	17763.1757	KB4601345
LTSC	2021-01 C	2021-01-21	17763.1728	KB4598296
LTSC	2021-01 B	2021-01-12	17763.1697	KB4598230
LTSC	2020-12 B	2020-12-08	17763.1637	KB4592440
LTSC	2020-11 C	2020-11-19	17763.1613	KB4586839
LTSC	2020-11 OOB	2020-11-17	17763.1579	KB4594442
LTSC	2020-11 B	2020-11-10	17763.1577	KB4586793
LTSC	2020-10 C	2020-10-20	17763.1554	KB4580390
LTSC	2020-10 B	2020-10-13	17763.1518	KB4577668
LTSC	2020-09 C	2020-09-16	17763.1490	KB4577069
LTSC	2020-09 B	2020-09-08	17763.1457	KB4570333
LTSC	2020-08 C	2020-08-20	17763.1432	KB4571748
LTSC	2020-08 B	2020-08-11	17763.1397	KB4565349
LTSC	2020-07 C	2020-07-21	17763.1369	KB4559003
LTSC	2020-07 B	2020-07-14	17763.1339	KB4558998
LTSC	2020-06 OOB	2020-06-16	17763.1294	KB4567513
LTSC	2020-06 B	2020-06-09	17763.1282	KB4561608
LTSC	2020-05 B	2020-05-12	17763.1217	KB4551853
LTSC	2020-04 C	2020-04-21	17763.1192	KB4550969
LTSC	2020-04 B	2020-04-14	17763.1158	KB4549949
LTSC	2020-03 OOB	2020-03-30	17763.1132	KB4554354
LTSC	2020-03 C	2020-03-17	17763.1131	KB4541331
LTSC	2020-03 B	2020-03-10	17763.1098	KB4538461
LTSC	2020-02 C	2020-02-25	17763.1075	KB4537818
LTSC	2020-02 B	2020-02-11	17763.1039	KB4532691
LTSC	2020-01 C	2020-01-23	17763.1012	KB4534321

LTSC	2020-01 B	2020-01-14	17763.973	KB4534273
LTSC	2019-12 B	2019-12-10	17763.914	KB4530715
LTSC	2019-11 B	2019-11-12	17763.864	KB4523205
LTSC	2019-10 C	2019-10-15	17763.832	KB4520062
LTSC	2019-10 B	2019-10-08	17763.805	KB4519338
LTSC	2019-09 OOB	2019-10-03	17763.775	KB4524148
LTSC	2019-09 C	2019-09-24	17763.774	KB4516077
LTSC	2019-09 OOB	2019-09-23	17763.740	KB4522015
LTSC	2019-09 B	2019-09-10	17763.737	KB4512578
LTSC	2019-08 C	2019-08-17	17763.720	KB4512534
LTSC	2019-08 B	2019-08-13	17763.678	KB4511553
LTSC	2019-07 C	2019-07-22	17763.652	KB4505658
LTSC	2019-07 B	2019-07-09	17763.615	KB4507469
LTSC	2019-06 OOB	2019-06-26	17763.593	KB4509479
LTSC	2019-06 C	2019-06-18	17763.592	KB4501371
LTSC	2019-06 B	2019-06-11	17763.557	KB4503327
LTSC	2019-05 C	2019-05-21	17763.529	KB4497934
LTSC	2019-05 OOB	2019-05-19	17763.504	KB4505056
LTSC	2019-05 B	2019-05-14	17763.503	KB4494441
LTSC	2019-04 C	2019-05-03	17763.475	KB4495667
LTSC	2019-04 OOB	2019-05-01	17763.439	KB4501835
LTSC	2019-04 B	2019-04-09	17763.437	KB4493509
LTSC	2019-03 D	2019-04-02	17763.404	KB4490481
LTSC	2019-03 B	2019-03-12	17763.379	KB4489899
LTSC	2019-02 D	2019-03-01	17763.348	KB4482887
LTSC	2019-02 B	2019-02-12	17763.316	KB4487044
LTSC	2019-01 D	2019-01-22	17763.292	KB4476976
LTSC	2019-01 B	2019-01-08	17763.253	KB4480116
LTSC	2018-12 OOB	2018-12-19	17763.195	KB4483235
LTSC	2018-12 B	2018-12-11	17763.194	KB4471332
LTSC	2018-11 D	2018-12-05	17763.168	KB4469342
LTSC	2018-11 B	2018-11-13	17763.134	KB4467708
LTSC	2018-10 D	2018-11-13	17763.107	KB4464455

LTSC	2018-10 B	2018-10-09	17763.55	KB4464330
LTSC	2018-10 A	2018-10-02	17763.1	

▼ Windows Server 2016 (OS build 14393)

Agrandir le tableau

Option de maintenance	Type de mise à jour	Date de disponibilité	Build	Article de la base de connaissances
LTSB	2026-10 B	2026-10-13	14393.9612	KB5126868
LTSB	2026-09 OOB	2026-09-14	14393.9514	KB5129239
LTSB	2026-09 B	2026-09-08	14393.9512	KB5123099
LTSB	2026-08 B	2026-08-11	14393.9418	KB5120418
LTSB	2026-07 B	2026-07-14	14393.9339	KB5099535
LTSB	2026-06 B	2026-06-09	14393.9234	KB5094122
LTSB	2026-05 B	2026-05-12	14393.9140	KB5087537
LTSB	2026-04 OOB	2026-04-19	14393.9062	KB5091572
LTSB	2026-04 B	2026-04-14	14393.9060	KB5082198
LTSB	2026-03 B	2026-03-10	14393.8957	KB5078938
LTSB	2026-02 B	2026-02-10	14393.8868	KB5075999
LTSB	2026-01 B	2026-01-13	14393.8783	KB5073722
LTSB	2025-12 OOB	2025-12-18	14393.8692	KB5074974
LTSB	2025-12 B	2025-12-09	14393.8688	KB5071543
LTSB	2025-11 B	2025-11-11	14393.8594	KB5068864
LTSB	2025-10 OOB	2025-10-23	14393.8524	KB5070882
LTSB	2025-10 B	2025-10-14	14393.8519	KB5066836
LTSB	2025-09 B	2025-09-09	14393.8422	KB5065427
LTSB	2025-08 B	2025-08-12	14393.8330	KB5063871
LTSB	2025-07 B	2025-07-08	14393.8246	KB5062560
LTSB	2025-06 B	2025-06-10	14393.8148	KB5061010
LTSB	2025-05 B	2025-05-13	14393.8066	KB5058383
LTSB	2025-04 OOB	2025-04-11	14393.7973	KB5058921
LTSB	2025-04 B	2025-04-08	14393.7969	KB5055521
LTSB	2025-03 B	2025-03-11	14393.7876	KB5053594
LTSB	2025-02 B	2025-02-11	14393.7785	KB5052006
LTSB	2025-01 B	2025-01-14	14393.7699	KB5049993

LTSB	2024-12 B	2024-12-10	14393.7606	KB5048671
LTSB	2024-11 B	2024-11-12	14393.7515	KB5046612
LTSB	2024-10 B	2024-10-08	14393.7428	KB5044293
LTSB	2024-09 B	2024-09-10	14393.7336	KB5043051
LTSB	2024-08 B	2024-08-13	14393.7259	KB5041773
LTSB	2024-07 B	2024-07-09	14393.7159	KB5040434
LTSB	2024-06 B	2024-06-11	14393.7070	KB5039214
LTSB	2024-05 B	2024-05-14	14393.6981	KB5037763
LTSB	2024-04 B	2024-04-09	14393.6897	KB5036899
LTSB	2024-03 OOB	2024-03-22	14393.6800	KB5037423
LTSB	2024-03 B	2024-03-12	14393.6796	KB5035855
LTSB	2024-02 B	2024-02-13	14393.6709	KB5034767
LTSB	2024-01 B	2024-01-09	14393.6614	KB5034119
LTSB	2023-12 B	2023-12-12	14393.6529	KB5033373
LTSB	2023-11 B	2023-11-14	14393.6452	KB5032197
LTSB	2023-10 B	2023-10-10	14393.6351	KB5031362
LTSB	2023-09 B	2023-09-12	14393.6252	KB5030213
LTSB	2023-08 B	2023-08-08	14393.6167	KB5029242
LTSB	2023-07 B	2023-07-11	14393.6085	KB5028169
LTSB	2023-06 OOB	2023-06-23	14393.5996	KB5028623
LTSB	2023-06 B	2023-06-13	14393.5989	KB5027219
LTSB	2023-05 B	2023-05-09	14393.5921	KB5026363
LTSB	2023-04 B	2023-04-11	14393.5850	KB5025228
LTSB	2023-03 B	2023-03-14	14393.5786	KB5023697
LTSB	2023-02 B	2023-02-14	14393.5717	KB5022838
LTSB	2023-01 B	2023-01-10	14393.5648	KB5022289
LTSB	2022-12 B	2022-12-13	14393.5582	KB5021235
LTSB	2022-11 OOB	2022-11-17	14393.5502	KB5021654
LTSB	2022-11 B	2022-11-08	14393.5501	KB5019964
LTSB	2022-10 OOB	2022-10-18	14393.5429	KB5020439
LTSB	2022-10 B	2022-10-11	14393.5427	KB5018411
LTSB	2022-09 B	2022-09-13	14393.5356	KB5017305
LTSB	2022-08 B	2022-08-09	14393.5291	KB5016622

LTSB	2022-07 B	2022-07-12	14393.5246	KB5015808
LTSB	2022-06 B	2022-06-14	14393.5192	KB5014702
LTSB	2022-05 OOB	2022-05-19	14393.5127	KB5015019
LTSB	2022-05 B	2022-05-10	14393.5125	KB5013952
LTSB	2022-04 B	2022-04-12	14393.5066	KB5012596
LTSB	2022-03 B	2022-03-08	14393.5006	KB5011495
LTSB	2022-02 B	2022-02-08	14393.4946	KB5010359
LTSB	2022-01 OOB	2022-01-17	14393.4889	KB5010790
LTSB	2022-01 B	2022-01-11	14393.4886	KB5009546
LTSB	2022-01 OOB	2022-01-05	14393.4827	KB5010195
LTSB	2021-12 B	2021-12-14	14393.4825	KB5008207
LTSB	2021-11 OOB	2021-11-14	14393.4771	KB5008601
LTSB	2021-11 B	2021-11-09	14393.4770	KB5007192
LTSB	2021-10 B	2021-10-12	14393.4704	KB5006669
LTSB	2021-09 B	2021-09-14	14393.4651	KB5005573
LTSB	2021-08 B	2021-08-10	14393.4583	KB5005043
LTSB	2021-07 OOB	2021-07-29	14393.4532	KB5005393
LTSB	2021-07 B	2021-07-13	14393.4530	KB5004238
LTSB	2021-07 OOB	2021-07-07	14393.4470	KB5004948
LTSB	2021-06 B	2021-06-08	14393.4467	KB5003638
LTSB	2021-05 B	2021-05-11	14393.4402	KB5003197
LTSB	2021-04 B	2021-04-13	14393.4350	KB5001347
LTSB	2021-03 OOB	2021-03-18	14393.4288	KB5001633
LTSB	2021-03 B	2021-03-09	14393.4283	KB5000803
LTSB	2021-02 B	2021-02-09	14393.4225	KB4601318
LTSB	2021-01 B	2021-01-12	14393.4169	KB4598243
LTSB	2020-12 B	2020-12-08	14393.4104	KB4593226
LTSB	2020-11 OOB	2020-11-19	14393.4048	KB4594441
LTSB	2020-11 B	2020-11-10	14393.4046	KB4586830
LTSB	2020-10 B	2020-10-13	14393.3986	KB4580346
LTSB	2020-09 B	2020-09-08	14393.3930	KB4577015
LTSB	2020-08 B	2020-08-11	14393.3866	KB4571694
LTSB	2020-07 B	2020-07-14	14393.3808	KB4565511

LTSB	2020-06 OOB	2020-06-18	14393.3755	KB4567517
LTSB	2020-06 B	2020-06-09	14393.3750	KB4561616
LTSB	2020-05 B	2020-05-12	14393.3686	KB4556813
LTSB	2020-04 C	2020-04-21	14393.3659	KB4550947
LTSB	2020-04 B	2020-04-14	14393.3630	KB4550929
LTSB	2020-03 C	2020-03-17	14393.3595	KB4541329
LTSB	2020-03 B	2020-03-10	14393.3564	KB4540670
LTSB	2020-02 C	2020-02-25	14393.3542	KB4537806
LTSB	2020-02 B	2020-02-11	14393.3504	KB4537764
LTSB	2020-01 C	2020-01-23	14393.3474	KB4534307
LTSB	2020-01 B	2020-01-14	14393.3443	KB4534271
LTSB	2019-12 B	2019-12-10	14393.3384	KB4530689
LTSB	2019-11 B	2019-11-12	14393.3326	KB4525236
LTSB	2019-10 C	2019-10-15	14393.3300	KB4519979
LTSB	2019-10 B	2019-10-08	14393.3274	KB4519998
LTSB	2019-09 OOB	2019-10-03	14393.3243	KB4524152
LTSB	2019-09 C	2019-09-24	14393.3242	KB4516061
LTSB	2019-09 OOB	2019-09-23	14393.3206	KB4522010
LTSB	2019-09 B	2019-09-10	14393.3204	KB4516044
LTSB	2019-08 C	2019-08-17	14393.3181	KB4512495
LTSB	2019-08 B	2019-08-13	14393.3144	KB4512517
LTSB	2019-07 C	2019-07-16	14393.3115	KB4507459
LTSB	2019-07 B	2019-07-09	14393.3085	KB4507460
LTSB	2019-06 OOB	2019-06-27	14393.3056	KB4509475
LTSB	2019-06 C	2019-06-18	14393.3053	KB4503294
LTSB	2019-06 B	2019-06-11	14393.3025	KB4503267
LTSB	2019-05 C	2019-05-23	14393.2999	KB4499177
LTSB	2019-05 OOB	2019-05-19	14393.2972	KB4505052
LTSB	2019-05 B	2019-05-14	14393.2969	KB4494440
LTSB	2019-04 C	2019-04-25	14393.2941	KB4493473
LTSB	2019-04 OOB	2019-04-25	14393.2908	KB4499418
LTSB	2019-04 B	2019-04-09	14393.2906	KB4493470
LTSB	2019-03 C	2019-03-19	14393.2879	KB4489889

LTSB	2019-03 B	2019-03-12	14393.2848	KB4489882
LTSB	2019-02 C	2019-02-19	14393.2828	KB4487006
LTSB	2019-02 B	2019-02-12	14393.2791	KB4487026
LTSB	2019-01 C	2019-01-17	14393.2759	KB4480977
LTSB	2019-01 B	2019-01-08	14393.2724	KB4480961
LTSB	2018-12 OOB	2018-12-19	14393.2670	KB4483229
LTSB	2018-12 B	2018-12-11	14393.2665	KB4471321
LTSB	2018-11 OOB	2018-12-03	14393.2641	KB4478877
LTSB	2018-11 C	2018-11-27	14393.2639	KB4467684
LTSB	2018-11 B	2018-11-13	14393.2608	KB4467691
LTSB	2018-10 C	2018-10-18	14393.2580	KB4462928
LTSB	2018-10 B	2018-10-09	14393.2551	KB4462917
LTSB	2018-09 C	2018-09-20	14393.2515	KB4457127
LTSB	2018-09 B	2018-09-11	14393.2485	KB4457131
LTSB	2018-08 C	2018-08-30	14393.2457	KB4343884
LTSB	2018-08 B	2018-08-14	14393.2430	KB4343887
LTSB	2018-07 OOB	2018-07-30	14393.2396	KB4346877
LTSB	2018-07 C	2018-07-24	14393.2395	KB4338822
LTSB	2018-07 OOB	2018-07-16	14393.2368	KB4345418
LTSB	2018-07 B	2018-07-10	14393.2363	KB4338814
LTSB	2018-06 C	2018-06-21	14393.2339	KB4284833
LTSB	2018-06 B	2018-06-12	14393.2312	KB4284880
LTSB	2018-05 C	2018-05-17	14393.2273	KB4103720
LTSB	2018-05 B	2018-05-08	14393.2248	KB4103723
LTSB	2018-04 C	2018-04-17	14393.2214	KB4093120
LTSB	2018-04 B	2018-04-10	14393.2189	KB4093119
LTSB	2018-03 OOB	2018-03-29	14393.2156	KB4096309
LTSB	2018-03 C	2018-03-22	14393.2155	KB4088889
LTSB	2018-03 B	2018-03-13	14393.2125	KB4088787
LTSB	2018-02 C	2018-02-22	14393.2097	KB4077525
LTSB	2018-02 B	2018-02-13	14393.2068	KB4074590
LTSB	2018-01 C	2018-01-17	14393.2035	KB4057142
LTSB	2018-01 B	2018-01-03	14393.2007	KB4056890

LTSB	2017-12 B	2017-12-12	14393.1944	KB4053579
LTSB	2017-11 C	2017-11-27	14393.1914	KB4051033
LTSB	2017-11 B	2017-11-14	14393.1884	KB4048953
LTSB	2017-10 OOB	2017-11-02	14393.1797	KB4052231
LTSB	2017-10 C	2017-10-17	14393.1794	KB4041688
LTSB	2017-10 B	2017-10-10	14393.1770	KB4041691
LTSB	2017-09 C	2017-09-28	14393.1737	KB4038801
LTSB	2017-09 B	2017-09-12	14393.1715	KB4038782
LTSB	2017-08 OOB	2017-08-28	14393.1670	KB4039396
LTSB	2017-08 C	2017-08-16	14393.1613	KB4034661
LTSB	2017-08 B	2017-08-08	14393.1593	KB4034658
LTSB	2017-08 OOB	2017-08-07	14393.1537	KB4038220
LTSB	2017-07 C	2017-07-18	14393.1532	KB4025334
LTSB	2017-07 B	2017-07-11	14393.1480	KB4025339
LTSB	2017-06 C	2017-06-27	14393.1378	KB4022723
LTSB	2017-06 B	2017-06-13	14393.1358	KB4022715
LTSB	2017-05 B	2017-05-09	14393.1198	KB4019472
LTSB	2017-04 B	2017-04-11	14393.1066	KB4015217
LTSB	2017-03 OOB	2017-03-20	14393.969	KB4015438
LTSB	2017-03 B	2017-03-14	14393.953	KB4013429
LTSB	2017-01 B	2017-01-10	14393.693	KB3213986
LTSB	2016-12 B	2016-12-13	14393.576	KB3206632
LTSB	2016-11 C	2016-12-09	14393.479	KB3201845
LTSB	2016-11 B	2016-11-08	14393.447	KB3200970
LTSB	2016-10 D	2016-10-27	14393.351	KB3197954
LTSB	2016-10 B	2016-10-11	14393.321	KB3194798
LTSB	2016-09 D	2016-09-29	14393.222	KB3194496
LTSB	2016-09 B	2016-09-20	14393.187	KB3193494
LTSB	2016-09 B	2016-09-13	14393.187	KB3189866
LTSB	2016-08 E	2016-08-31	14393.105	KB3176938
LTSB	2016-08 D	2016-08-23	14393.82	KB3176934
LTSB	2016-08 B	2016-08-09	14393.51	KB3176495
LTSB	2016-08 A	2016-08-02	14393.10	KB3176929

Calendrier des mises à jour correctives à chaud pour Windows Server

Voir le calendrier des mises à jour correctives à chaud pour Windows Server 2025 et Windows Server 2022. Grâce aux mises à jour correctives à chaud, les appareils reçoivent une mise à jour cumulative de référence le premier mois de chaque trimestre de l'année civile. Un redémarrage est nécessaire pour installer cette mise à jour de base. Au cours des deux mois suivants, les appareils recevront une mise à jour corrective à chaud, qui ne comprend que des mises à jour de sécurité et peut être installée sans redémarrage.

Windows Server 2025 (OS build 26100)

Pour plus de détails sur ce qui est inclus dans chaque mise à jour, voir les Notes de version pour les mises à jour correctives à chaud destinées à Windows Server 2025 Datacenter Azure Edition.

Année civile 2026

Agrandir le tableau

Mois	Type de mise à jour	Type	Date de disponibilité	Build	Article de la base de connaissances
Janvier	2026.01 B	Baseline (Restart)	2026-01-13	26100.32230	KB5073379
Février	2026.02 B	Mise à jour corrective à chaud	2026-02-10	26100.32313	KB5075942
Mars	2026.03 B	Mise à jour corrective à chaud	2026-03-10	26100.32463	KB5078736
Avril	2026.04 B	Baseline (Restart)	2026-04-14	26100.32690	KB5082063
Mai	2026.05 B	Mise à jour corrective à chaud	2026-05-12	26100.32772	KB5087423
Juin	2026.06 B	Baseline (Restart)	2026-06-09	26100.32995	KB5094125
Juillet	2026.07 B	Baseline (Restart)	2026-07-14	26100.33158	KB5099536
Août	2026.08 B	Mise à jour corrective à chaud	2026-08-11	26100.33222	KB5120228
Septembre	2026.09 B	Baseline (Restart)	2026-09-08	26100.33438	KB5122871
Octobre	2026.10 B	Baseline (Restart)	2026-10-13	26100.33650	KB5126646
Novembre	2026.11 B	Mise à jour corrective à chaud			
Décembre	2026.12 B	Mise à jour corrective à chaud			

▼ Année civile 2025

Agrandir le tableau

Mois	Type de mise à jour	Type	Date de disponibilité	Build	Article de la base de connaissances
Janvier	2025.01 B	Baseline (Restart)	2025-01-14	26100.2894	KB5050009
Février	2025.02 B	Mise à jour corrective à chaud	2025-02-11	26100.3107	KB5052105
Mars	2025.03 B	Mise à jour corrective à chaud	2025-03-11	26100.3403	KB5053636
Avril	2025.04 B	Baseline (Restart)	2025-04-08	26100.3775	KB5055523
Mai	2025.05 B	Mise à jour corrective à chaud	2025-05-13	26100.3981	KB5058497
Juin	2025.06 B	Mise à jour corrective à chaud	2025-06-10	26100.4270	KB5060841
Juillet	2025.07 B	Baseline (Restart)	2025-07-08	26100.4652	KB5062553
Août	2025.08 B	Mise à jour corrective à chaud	2025-08-12	26100.4851	KB5064010
Septembre	2025.09 B	Mise à jour corrective à chaud	2025-09-09	26100.6508	KB5065474
Octobre	2025.10 B	Baseline (Restart)	2025-10-14	26100.6899	KB5066835
Novembre	2025.11 B	Mise à jour corrective à chaud	2025-11-11	26100.7092	KB5068966
Décembre	2025.12 B	Mise à jour corrective à chaud	2025-12-09	26100.7392	KB5072014

▼ Année civile 2024

Agrandir le tableau

Mois	Type de mise à jour	Type	Date de disponibilité	Build	Article de la base de connaissances
Novembre	2024.11 B	Mise à jour corrective à chaud	2024-11-12	26100.2240	KB5046696
Décembre	2024.12 B	Mise à jour corrective à chaud	2024-12-10	26100.2528	KB5048794

▼ Windows Server 2022 (OS build 20348)

Pour plus de détails sur ce qui est inclus dans chaque mise à jour, voir les Notes de version pour les mises à jour correctives à chaud destinées à Azure Automanage pour Windows Server 2022 .

Année civile 2026

Agrandir le tableau

Mois	Type de mise à jour	Type	Date de disponibilité	Build	Article de la base de connaissances
Janvier	2026.01 B	Baseline (Restart)	2026-01-13	20348.4648	KB5073457
Février	2026.02 B	Mise à jour corrective à chaud	2026-02-10	20348.4711	KB5075943
Mars	2026.03 B	Mise à jour corrective à chaud	2026-03-10	20348.4830	KB5078737
Avril	2026.04 B	Baseline (Restart)	2026-04-14	20348.5020	KB5082142
Mai	2026.05 B	Mise à jour corrective à chaud	2026-05-12	20348.5074	KB5087424
Juin	2026.06 B	Baseline (Restart)	2026-06-09	20348.5256	KB5094128
Juillet	2026.07 B	Baseline (Restart)	2026-07-14	20348.5386	KB5099540
Août	2026.08 B	Mise à jour corrective à chaud	2026-08-11	20348.5440	KB5120229
Septembre	2026.09 B	Baseline (Restart)	2026-09-08	20348.5622	KB5122882
Octobre	2026.10 B	Baseline (Restart)	2026-10-13	20348.5761	KB5126655
Novembre	2026.11 B	Mise à jour corrective à chaud			
Décembre	2026.12 B	Mise à jour corrective à chaud			

▼ Année civile 2025

Agrandir le tableau

Mois	Type de mise à jour	Type	Date de disponibilité	Build	Article de la base de connaissances
Janvier	2025.01 B	Baseline (Restart)	2025-01-14	20348.3091	KB5049983
Février	2025.02 B	Mise à jour corrective à chaud	2025-02-11	20348.3148	KB5052106
Mars	2025.03 B	Mise à jour corrective à chaud	2025-03-11	20348.3270	KB5053638
Avril	2025.04 B	Baseline (Restart)	2025-04-08	20348.3453	KB5055526
Mai	2025.05 B	Mise à jour corrective à chaud	2025-05-13	20348.3630	KB5058500
Juin	2025.06 B	Mise à jour corrective à chaud	2025-06-10	20348.3745	KB5060525

Juillet	2025.07 B	Baseline (Restart)	2025-07-08	20348.3932	KB5062572
Août	2025.08 B	Mise à jour corrective à chaud	2025-08-12	20348.3989	KB5063812
Septembre	2025.09 B	Mise à jour corrective à chaud	2025-09-09	20348.4106	KB5065306
Octobre	2025.10 B	Baseline (Restart)	2025-10-14	20348.4294	KB5066782
Novembre	2025.11 B	Mise à jour corrective à chaud	2025-11-11	20348.4346	KB5068840
Décembre	2025.12 B	Mise à jour corrective à chaud	2025-12-09	20348.4467	KB5071413

▼ **Année civile 2024**

Agrandir le tableau

Mois	Type de mise à jour	Type	Date de disponibilité	Build	Article de la base de connaissances
Janvier	2024.01 B	Baseline (Restart)	2024-01-09	20348.2227	KB5034129
Février	2024.02 B	Mise à jour corrective à chaud	2024-02-13	20348.2277	KB5034860
Mars	2024.03 B	Mise à jour corrective à chaud	2024-03-12	20348.2333	KB5035959
Avril	2024.04 B	Baseline (Restart)	2024-04-09	20348.2402	KB5036909
Mai	2024.05 B	Mise à jour corrective à chaud	2024-05-14	20348.2458	KB5037848
Juin	2024.06 B	Mise à jour corrective à chaud	2024-06-11	20348.2522	KB5039330
Juillet	2024.07 B	Baseline (Restart)	2024-07-09	20348.2582	KB5040437
Août	2024.08 B*	Baseline (Restart)	2024-08-13	20348.2655	KB5041160
Septembre	2024.09 B	Mise à jour corrective à chaud	2024-09-10	20348.2695	KB5042880
Octobre	2024.10 B	Baseline (Restart)	2024-10-08	20348.2762	KB5044281
Novembre	2024.11 B	Mise à jour corrective à chaud	2024-11-12	20348.2819	KB5046698
Décembre	2024.12 B	Mise à jour corrective à chaud	2024-12-10	20348.2908	KB5048800

Dernière mise à jour : 13/10/2026

Problèmes connus et notifications de Windows Server 2025

Trouvez des informations sur les problèmes connus et le status de maintenance pour Windows Server 2025. Pour obtenir une aide immédiate sur les problèmes de Windows Update, cliquez ici si vous utilisez un appareil Windows pour ouvrir l'application Aide ou accéder à support.microsoft.com. Suivez @WindowsUpdate sur X pour les mises à jour d'intégrité des versions Windows. Si vous êtes administrateur informatique et que vous souhaitez obtenir des informations par programme à partir de cette page, utilisez l'API des mises à jour Windows dans Microsoft Graph.

Statut actuel au 6 novembre 2024

Windows Server 2025 est désormais généralement disponible. Il offre des avancées en matière de sécurité et de nouvelles fonctionnalités de cloud hybride dans une plateforme haute performance et compatible avec l'IA. Windows Server 2025 est la dernière version du canal de maintenance Long-Term (LTSC) de Microsoft pour Windows Server. Pour télécharger une évaluation gratuite de 180 jours, visitez le Centre d'évaluation Microsoft.

Windows Server 2025 est proposé en tant que mise à jour **facultative** pour les appareils Windows Server 2022 et Windows Server 2019, si les organisations souhaitent effectuer une mise à niveau sur place. Nous vous recommandons d'utiliser ces méthodes pour déployer les mises à jour des fonctionnalités de Windows Server, car Windows Server 2025 n'est pas installé automatiquement.

Pour en savoir plus sur la politique de cycle de vie de Windows Server, consultez l'article sur le cycle de vie de Windows Server 2025 .

Nouveautés de Windows Server 2025

Découvrez ses fonctionnalités avancées et ses innovations

Obtenir les problèmes connus de Windows Server dans l'API Graph

Les données sont disponibles pour les versions de Windows Server prises en charge

Voir tous les messages >

Problèmes connus

Consultez les problèmes ouverts, le contenu mis à jour au cours des 30 derniers jours et les informations sur les dispositifs de protection. Pour rechercher un problème spécifique, utilisez la fonction de recherche de votre navigateur (CTRL + F pour Microsoft Edge).

Agrandir le tableau

Résumé	Mise à jour d'origine	Statut	Dernière mise à jour
Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé » L'antivirus Microsoft Defender reste actif et fonctionne correctement malgré les notifications suite à la dernière mise à jour.	Non applicable	Résolu	2026-09-30 16h42 PT
Les périphériques audio USB peuvent ne pas démarrer ou ne pas produire de son Certains appareils audio USB de classe 1.0 affichent le code 10 ou échouent en mode audio multicanal après l'installation de la mise à jour du 8 septembre	Build du système d'exploitation 26100.33438 KB5122871 2026-09-08	Atténué	2026-09-29 10h12 PT
Les services Bureau à distance pourraient cesser de répondre après la	Build du système d'exploitation 26100.33438 KB5122871 2026-09-08	Résolu KB5129235	2026-09-17 19h22 PT

Résumé	Mise à jour d'origine	Statut	Dernière mise à jour
mise à jour de sécurité de septembre 2026 Certains appareils Windows sur lesquels le Bureau à distance est activé peuvent rencontrer une instabilité des Services Bureau à distance (RDS).			

Détails du problème

Septembre 2026

Les périphériques audio USB peuvent ne pas démarrer ou ne pas produire de son

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Atténué	Build du système d'exploitation 26100.33438 KB5122871 2026-09-08	Dernière mise à jour : 2026-09-29, 10:12 PT Ouvert : 2026-09-25, 18:40 PT

Après l'installation de la mise à jour de sécurité Windows du 8 septembre 2026 (KB5122871), certains appareils USB audio classe 1.0 peuvent ne pas démarrer ou produire du son. Les appareils affectés peuvent rencontrer un ou plusieurs des symptômes suivants :

- L'appareil affiche une erreur dans le Gestionnaire de périphériques : « Ce périphérique ne peut pas démarrer (Code 10) ».
- Aucune sortie audio.
- Les contrôles de volume ne répondent pas ou restent à zéro.
- Les paramètres sonores ne répondent pas ou ne sont pas disponibles.
- Certains périphériques peuvent fonctionner dans des configurations stéréo standard, mais échouer lors de l'utilisation de fonctionnalités audio multicanaux, notamment les modes audio 8 canaux ou 3D. Certains clients ont signalé qu'ils sont en mesure de restaurer l'audio dans ces cas en passant en mode 2 canaux. *(*Remarque : ce comportement est résolu dans la mise à jour hors bande publiée le 14 septembre 2026. Voir la section Résolution ci-dessous.)*

Ce problème se limite aux périphériques audio USB de classe 1.0.

Support Microsoft : les administrateurs informatiques qui ont besoin d'une solution de contournement immédiate pour les symptômes qui n'ont pas encore été résolus par la mise à jour OOB doivent contacter le Support Microsoft pour les entreprises pour obtenir de l'aide.

Résolution : Ce problème est partiellement résolu dans la mise à jour hors cycle publiée le 14 septembre 2026 (KB5129235) et les mises à jour publiées après cette date. Cette mise à jour OOB corrige les symptômes rencontrés sur les appareils utilisant le mode audio 8 canaux ou 3D (dernier point de la liste de symptômes documentés dans cette entrée). Nous nous efforçons de traiter les autres symptômes et nous mettrons à jour cette documentation lorsque de plus amples informations seront disponibles.

Plateformes affectées :

- Client : Windows 11, version 26H2 ; Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Les services Bureau à distance pourraient cesser de répondre après la mise à jour de sécurité de septembre 2026

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5129235	Build du système d'exploitation 26100.33438 KB5122871 2026-09-08	Résolu : 2026-09-14, 10:00 PT Ouvert : 2026-09-11, 11:19 PT

Après l'installation de la mise à jour de sécurité Windows de septembre 2026 (KB5122871), certaines organisations peuvent rencontrer des problèmes avec les services Bureau à distance (RDS).

Dans certains environnements, les services Bureau à distance peuvent devenir instables, ce qui entraîne l'échec des connexions RDP après plusieurs minutes, des problèmes de connexion ou le blocage des serveurs sur l'écran « Veuillez attendre la configuration du Bureau à distance ». Les outils connexes, notamment Microsoft Management Console (MMC), RDS Licensing Diagnoser et l'Explorateur de fichiers peuvent également ne plus répondre. En outre, la page Windows Update peut cesser de répondre et afficher en permanence un indicateur de chargement.

Remarque : Ce problème n'affecte pas Windows 365 ou Azure Virtual Desktop.

Résolution : Ce problème est résolu par la mise à jour hors cycle publiée le 14 septembre 2026 (KB5129235), et par les mises à jour publiées après cette date.

Les administrateurs informatiques qui ont déployé une atténuation temporaire via la stratégie de groupe n'ont pas besoin de prendre de mesures avant d'installer cette mise à jour OOB.

Cette mise à jour OOB est cumulative et inclut toutes les améliorations et protections de sécurité contenues dans les mises à jour Windows précédentes. Nous vous recommandons d'installer la dernière mise à jour disponible pour vos appareils, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Août 2026

Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé »

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Non applicable	Résolu : 2026-09-30, 16:42 PT Ouvert : 2026-08-28, 15:34 PT

Après l'installation de Microsoft Defender mise à jour de l'antivirus (version 4.18.26070.9), publiée le 5 août 2026, des notifications peuvent apparaître indiquant que « l'antivirus Microsoft Defender est désactivé », même si l'antivirus fonctionne correctement et que tous les paramètres l'indiquent comme actif. Ces notifications peuvent apparaître au démarrage de Windows et par intermittence par la suite. Ils persistent même si les paramètres de notification sont désactivés.

Ce problème peut être observé dans n'importe quelle version de Windows ou de Windows Server avec l'antivirus Microsoft Defender exécuté avec les dernières mises à jour Defender.

Résolution : Ce problème a été résolu dans la mise à jour de l'antivirus Microsoft Defender (version 4.18.26080.4), publiée le 17 septembre 2026.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Signaler un problème avec les mises à jour Windows

Pour signaler un problème à Microsoft à tout moment, utilisez l'application Hub de commentaires . Pour plus d'informations, consultez Envoyer des commentaires à Microsoft avec l'application Hub de commentaires .

Besoin d'aide pour Windows Update ?

Recherchez, parcourez ou posez une question sur la communauté de Support Microsoft . Si vous êtes un professionnel de l'informatique soutenant une organisation, visitez l'état de publication de Windows sur le Centre d'administration Microsoft 365 pour plus de détails.

Pour obtenir de l'aide directe sur votre PC personnel, utilisez l'application Aide sur Windows ou contactez le Support Microsoft . Les organisations peuvent demander un support immédiat par le biais du Support pour les entreprises .

Afficher ce site dans votre langue

Ce site est disponible en 11 langues : anglais, chinois traditionnel, chinois simplifié, français (France), allemand, italien, japonais, coréen, portugais (Brésil), russe et espagnol (Espagne). Tout le texte s'affiche en anglais si la langue par défaut de votre navigateur n'est pas l'une des 11 langues prises en charge. Pour changer manuellement la langue d'affichage, faites défiler vers le bas de cette page, cliquez sur la langue actuelle affichée en bas à gauche de la page et sélectionnez l'une des 11 langues prises en charge dans la liste.

Dernière mise à jour : 16/10/2026

Problèmes résolus dans Windows Server 2025

Trouvez des informations sur les problèmes récemment résolus pour Windows Server 2025. Pour rechercher un problème spécifique, utilisez la fonction de recherche de votre navigateur (CTRL + F pour Microsoft Edge). Pour obtenir une aide immédiate sur les problèmes de Windows Update, cliquez ici si vous utilisez un appareil Windows pour ouvrir l'application Aide ou accéder à support.microsoft.com. Suivez @WindowsUpdate sur X pour les mises à jour d'intégrité des versions Windows. Si vous êtes administrateur informatique et que vous souhaitez obtenir des informations par programme à partir de cette page, utilisez l'API des mises à jour Windows dans Microsoft Graph.

Problèmes résolus

Agrandir le tableau

Résumé	Mise à jour d'origine	Statut	Date résolue
Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé » L'antivirus Microsoft Defender reste actif et fonctionne correctement malgré les notifications suite à la dernière mise à jour.	Non applicable	Résolu	2026-09-30 16h42 PT
Les services Bureau à distance pourraient cesser de répondre après la mise à jour de sécurité de septembre 2026 Certains appareils Windows sur lesquels le Bureau à distance est activé peuvent rencontrer une instabilité des Services Bureau à distance (RDS).	Build du système d'exploitation 26100.33438 KB5122871 2026-09-08	Résolu KB5129235	2026-09-14 10:00 PT

Résumé	Mise à jour d'origine	Statut	Date résolue
La fonctionnalité GIF dans le panneau Windows Emoji peut devenir indisponible Ce problème se produit, car le fournisseur GIF précédent (Tenor) a mis hors service son service le 30 juin 2026.	Non applicable	Résolu KB5120233	2026-08-11 10:00 PT
Les opérations de synchronisation de Windows Server Update Services peuvent rencontrer des problèmes ou expirer Des efforts d'assainissement sont en cours. Les temps de synchronisation devraient revenir à la normale à mesure que la récupération progresse.	Non applicable	Résolu	2026-07-20 13h22 PT
La suppression d'un fichier de la Corbeille affiche un nom de fichier interne dans la boîte de dialogue Ce problème se produit uniquement dans la boîte de dialogue de confirmation après l'installation de la mise à jour de sécurité Windows de juin.	Build du système d'exploitation 26100.32995 KB5094125 2026-06-09	Résolu KB5099536	2026-07-14 10:00 PT
Les mises à jour installées via WUSA peuvent échouer si elles sont installées à partir d'un dossier partagé Ce problème peut se produire lors de l'installation d'une mise à jour à partir d'un dossier réseau contenant plusieurs fichiers .msu.	Build du système d'exploitation 26100.4349 KB5060842 2025-06-10	Résolu KB5094125	2026-06-09 10:00 PT
Les contrôleurs de domaine peuvent redémarrer à plusieurs reprises après l'installation de la mise à jour de sécurité d'avril Les contrôleurs de domaine	Build du système d'exploitation 26100.32690 KB5082063 2026-04-14	Résolu KB5091157	2026-04-19 14:00 PT

Résumé	Mise à jour d'origine	Statut	Date résolue
affectés subiront des incidents LSASS. Une atténuation est disponible via le Support Microsoft.			
Windows Server 2022 et Server 2019 ont été mis à niveau de manière inattendue vers Windows Server 2025 Ce problème a été atténué. Il a été observé lorsque les mises à jour étaient gérées par certaines applications tierces.	Non applicable	Résolu KB5082063	2026-04-14 10:00 PT
Les applications peuvent cesser de répondre lors de l'enregistrement des fichiers dans un stockage sur le cloud Les applications concernées incluent Outlook, qui peut ne plus répondre lors de l'accès aux fichiers PST stockés sur Microsoft OneDrive.	Build du système d'exploitation 26100.32230 KB5073379 2026-01-13	Résolu KB5078135	2026-01-23 14:00 PT
Échecs de connexion et d'authentification dans Azure Virtual Desktop et Windows 365 Janvier 2026 La mise à jour Windows provoque des échecs d'invite d'informations d'identification de l'application application Windows sur Azure Virtual Desktop et Windows 365	Build du système d'exploitation 26100.32230 KB5073379 2026-01-13	Résolu KB5077793	2026-01-17 14:00 PT
Les sites web IIS peuvent ne pas se charger Les applications côté serveur qui s'appuient sur HTTP.sys peuvent rencontrer des problèmes avec les connexions entrantes.	Build du système d'exploitation 26100.6899 KB5066835 14-10-2025	Résolu KB5068861	2025-11-11 10:00 PT

Résumé	Mise à jour d'origine	Statut	Date résolue
Échec de la synchronisation d'annuaires pour les groupes AD de plus de 10 000 membres Le problème affecte la synchronisation des services de domaine Active Directory (AD DS), y compris la synchronisation de Microsoft Entra Connect	Build du système d'exploitation 26100.6584 KB5065426 2025-09-09	Résolu KB5068861	2025-11-11 10:00 PT
Des problèmes d'authentification par carte à puce peuvent se produire avec la mise à jour Windows d'octobre 2025 Ce problème est lié à une modification de sécurité introduite pour renforcer les services de chiffrement Windows.	Build du système d'exploitation 26100.6899 KB5066835 14-10-2025	Résolu	2025-10-22 17:31 PT
La souris et le clavier USB ne fonctionnent pas dans l'environnement de récupération Windows (WinRE) Ce problème affecte les périphériques USB uniquement dans WinRE après l'installation des mises à jour Windows publiées le 14 octobre 2025.	Build du système d'exploitation 26100.6899 KB5066835 14-10-2025	Résolu KB5070773	2025-10-20 14:00 PT

Détails du problème

Septembre 2026

Les services Bureau à distance pourraient cesser de répondre après la mise à jour de sécurité de septembre 2026

Agrandir le tableau

Statut	Mise à jour d'origine	Historique

Résolution KB5129235	Build du système d'exploitation 26100.33438 KB5122871 2026-09-08	Résolu : 2026-09-14, 10:00 PT Ouvert : 2026-09-11, 11:19 PT

Après l'installation de la mise à jour de sécurité Windows de septembre 2026 (KB5122871), certaines organisations peuvent rencontrer des problèmes avec les services Bureau à distance (RDS).

Dans certains environnements, les services Bureau à distance peuvent devenir instables, ce qui entraîne l'échec des connexions RDP après plusieurs minutes, des problèmes de connexion ou le blocage des serveurs sur l'écran « Veuillez attendre la configuration du Bureau à distance ». Les outils connexes, notamment Microsoft Management Console (MMC), RDS Licensing Diagnoser et l'Explorateur de fichiers peuvent également ne plus répondre. En outre, la page Windows Update peut cesser de répondre et afficher en permanence un indicateur de chargement.

Remarque : Ce problème n'affecte pas Windows 365 ou Azure Virtual Desktop.

Résolution : Ce problème est résolu par la mise à jour hors cycle publiée le 14 septembre 2026 (KB5129235), et par les mises à jour publiées après cette date.

Les administrateurs informatiques qui ont déployé une atténuation temporaire via la stratégie de groupe n'ont pas besoin de prendre de mesures avant d'installer cette mise à jour OOB.

Cette mise à jour OOB est cumulative et inclut toutes les améliorations et protections de sécurité contenues dans les mises à jour Windows précédentes. Nous vous recommandons d'installer la dernière mise à jour disponible pour vos appareils, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Août 2026

Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé »

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Non applicable	Résolu : 2026-09-30, 16:42 PT Ouvert : 2026-08-28, 15:34 PT

Après l'installation de Microsoft Defender mise à jour de l'antivirus (version 4.18.26070.9), publiée le 5 août 2026, des notifications peuvent apparaître indiquant que « l'antivirus Microsoft Defender est désactivé », même si l'antivirus fonctionne correctement et que tous les paramètres l'indiquent comme actif. Ces notifications peuvent apparaître au démarrage de Windows et par intermittence par la suite. Ils persistent même si les paramètres de notification sont désactivés.

Ce problème peut être observé dans n'importe quelle version de Windows ou de Windows Server avec l'antivirus Microsoft Defender exécuté avec les dernières mises à jour Defender.

Résolution : Ce problème a été résolu dans la mise à jour de l'antivirus Microsoft Defender (version 4.18.26080.4), publiée le 17 septembre 2026.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Juillet 2026

Les opérations de synchronisation de Windows Server Update Services peuvent rencontrer des problèmes ou expirer

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Non applicable	Résolu : 2026-07-20, 13:22 PT Ouvert : 2026-07-17, 18:18 PT

Microsoft a identifié une dégradation des services affectant Windows Server Update Services (WSUS). Les organisations peuvent constater une augmentation des temps de synchronisation ou des délais d'expiration des opérations de synchronisation sur les serveurs WSUS. Ce problème a commencé ces derniers jours, avec un impact accru observé à partir du 13 juillet 2026 et une atténuation côté service le samedi 18 juillet 2026. Après ce jour, les heures de synchronisation et les opérations de synchronisation devraient être rétablies à la normale.

Ce problème est lié à une accumulation de métadonnées de publication qui est présente sur les installations de serveur WSUS existantes ainsi que du côté service.

Résolution : La résolution de ce problème comporte deux parties.

- Les organisations avec des installations de serveur WSUS existantes qui connaissent de longs temps de synchronisation peuvent tirer parti d'étapes manuelles afin de propre des métadonnées inutiles. Ces métadonnées sont présentes dans les installations WSUS existantes, mais peuvent être supprimées en toute sécurité. Des instructions détaillées sont fournies dans l'article suivant de la Base de connaissances : https://support.microsoft.com/help/5121986
- Le 18 juillet 2026, Microsoft a déployé une atténuation côté service qui rétablit les temps de synchronisation et les opérations de synchronisation à la normale pour les nouvelles installations et reconstructions WSUS. Après cette date, les serveurs WSUS nouvellement installés ou recréés ne devraient pas rencontrer ce problème.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10, version 1809 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016 ; Windows 10, version 1607
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server, version 1809 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

juin 2026

La fonctionnalité GIF dans le panneau Windows Emoji peut devenir indisponible

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5120233	Non applicable	Résolu : 2026-08-11, 10:00 PT Ouvert : 2026-06-29, 20:45 PT

À partir du 30 juin 2026, il se peut que vous ne voyiez pas les options GIF dans le panneau Windows Emoji sur certains appareils, mais que vous voyiez à la place un message indiquant « Le service GIF n'est pas disponible ». Ce problème se produit, car le fournisseur GIF précédent (Tenor) a mis hors service son service à cette date.

Résolution : Ce problème a été résolu par les mises à jour Windows publiées le 11 août 2026 KB5120233 et versions ultérieures. Ces mises à jour incluent un nouveau fournisseur de fichiers GIF (GIPHY). Pour restaurer

la fonctionnalité GIF dans le panneau Windows Emoji, installez la dernière mise à jour Windows disponible.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2
- Serveur : Windows Server 2025

Retour au début

La suppression d'un fichier de la Corbeille affiche un nom de fichier interne dans la boîte de dialogue

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5099536	Build du système d'exploitation 26100.32995 KB5094125 2026-06-09	Résolu : 2026-07-14, 10:00 PT Ouvert : 2026-06-18, 12:03 PT

Lors de la suppression définitive d'un seul élément de la Corbeille, la boîte de dialogue de confirmation affiche le nom de fichier interne de la Corbeille (par exemple, $Rxxxxx.ext) au lieu du nom de fichier d'origine. La Corbeille elle-même affiche correctement le nom de fichier d'origine, et la restauration de l'élément le restaure également à l'aide du nom de fichier d'origine.

Ce problème se produit après l'installation du correctif de sécurité Windows publié le 9 juin 2026 (KB5094125).

Résolution : Ce problème a été résolu par les mises à jour Windows publiées le 14 juillet 2026 (KB5099536) et versions ultérieures. Nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci. Si votre organisation a installé une mise à jour publiée le 14 juillet 2026 ou une version ultérieure, vous n'avez pas besoin d'utiliser une restauration de problème connu ou une stratégie de groupe spéciale pour résoudre ce problème.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10, version 1607
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Avril 2026

Les contrôleurs de domaine peuvent redémarrer à plusieurs reprises après l'installation de la mise à jour de sécurité d'avril

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5091157	Build du système d'exploitation 26100.32690 KB5082063 2026-04-14	Résolu : 2026-04-19, 14:00 PT Ouvert : 2026-04-16, 18:50 PT

Après l'installation de la mise à jour de sécurité Windows (KB5082063) d'avril 2026 et le redémarrage, les contrôleurs de domaine (DC) dans les environnements avec plusieurs domaines dans la forêt qui utilisent Privileged Access Management (PAM) peuvent rencontrer des blocages LSASS au démarrage. Par conséquent, les contrôleurs de domaine affectés peuvent redémarrer à plusieurs reprises, empêchant l'authentification et les services d'annuaire de fonctionner, et potentiellement rendant le domaine indisponible.

Remarque : Ce problème affecte uniquement Windows Server. Il n'a pas d'impact sur les PC grand public ou les appareils personnels. Il est peu probable que le scénario soit observé sur des appareils à usage individuel qui ne sont pas gérés par un service informatique.

Résolution : Ce problème est résolu par les mises à jour hors cycle publiées le 19 avril 2026.

- La mise à jour standard de OOB est disponible en tant que KB5091157. Il peut être téléchargé à partir du catalogue Microsoft Update. Pour obtenir des conseils supplémentaires, consultez Comment télécharger des mises à jour à partir du catalogue Microsoft Update.
- Si votre appareil Windows Server 2025 est inscrit à la mise à jour corrective à chaud, vous devez plutôt installer le KB5091470 de mise à jour de mise à jour OOB hotpatch. Cette mise à jour hotpatch OOB est publiée via Windows Update et ne nécessite pas le redémarrage de l'appareil.

Versions concernées :

- Client : Aucun
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server, version 23H2 ; Windows Server 2019 ; Windows Server 2016

Retour au début

Janvier 2026

Les applications peuvent cesser de répondre lors de l'enregistrement des fichiers dans un stockage sur le cloud

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5078135	Build du système d'exploitation 26100.32230 KB5073379 2026-01-13	Résolu : 2026-01-23, 14:00 PT Ouvert : 2026-01-20, 22:10 PT

Après l'installation des mises à jour Windows publiées le 13 janvier 2026 (KB5073379), certaines applications peuvent ne plus répondre ou rencontrer des erreurs inattendues lors de l'ouverture ou de l'enregistrement de fichiers à partir d'un stockage cloud tel que OneDrive ou Dropbox.

Par exemple, dans certaines configurations d'Outlook qui stockent des fichiers PST sur OneDrive, Outlook peut ne plus répondre et ne pas pouvoir être rouvert , sauf si son processus est arrêté dans le Gestionnaire des tâches ou si le système est redémarré. En outre, les e-mails envoyés peuvent ne pas apparaître dans le dossier Éléments envoyés et les e-mails précédemment téléchargés peuvent être téléchargés à nouveau. Les configurations Outlook concernées impliquent principalement Outlook classique, qui est généralement lié aux licences d'entreprise et n'est pas inclus dans la plupart des installations à domicile de Windows. Pour vérifier votre configuration Outlook en case activée, consultez Comparaison des fonctionnalités entre le nouvel Outlook et Outlook classique.

Résolution :

Ce problème est résolu dans leKB5078135 de mise à jour hors cycle (OOB), publié le 24 janvier 2026 et disponible via lecatalogue Microsoft Update, ainsi que dans les mises à jour publiées après cette date. Nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Remarque : pour télécharger des mises à jour à partir du Catalogue Microsoft Update, suivez les étapes décrites dans cet article.

Pour les appareils qui n'ont pas encore installé la mise à jour OOB, il existe une solution de contournement facultative pour les scénarios spécifiques à Outlook. Le déplacement des fichiers Outlook PST hors de OneDrive devrait résoudre ce problème. Pour obtenir des conseils, consultez la documentation sur la suppression d'un fichier de données Outlook .pst de OneDrive. De plus, les comptes de messagerie sont toujours accessibles via le webmail, si votre fournisseur de messagerie le prend en charge.

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10 Entreprise LTSC 2021 ; Windows 10 Entreprise LTSC 2019
- Serveur : Windows Server 2025 ; Windows Server, version 23H2 ; Windows Server 2022 ; Windows Server 2019

Retour au début

Échecs de connexion et d'authentification dans Azure Virtual Desktop et Windows 365

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5077793	Build du système d'exploitation 26100.32230 KB5073379 2026-01-13	Résolu : 2026-01-17, 14:00 PT Ouvert : 14-01-2026, 00:52 PT

Après l'installation de la mise à jour de sécurité Windows de janvier 2026 (KB5073379), des échecs d'invite d'informations d'identification peuvent se produire dans certaines applications de connexion à distance. Cela inclut les connexions Bureau à distance à l'aide de l'application application Windows sur les appareils clients Windows, sur Azure Virtual Desktop et Windows 365. L'application application Windows est affectée par ce problème sur des builds Windows spécifiques et peut rencontrer des échecs de connexion.

D'autres connexions à distance et applications associées peuvent être touchées de la même manière.

Résolution : Pour résoudre ce problème, une mise à jour hors cycle (OOB) a été publiée le 17 janvier 2026 dans le Catalogue Microsoft Update. Il peut être trouvé sous la forme KB5077793.

Si vous n'avez pas encore déployé la mise à jour de sécurité Windows de janvier 2026 et que votre environnement informatique inclut les applications et fonctionnalités affectées, nous vous recommandons d'appliquer cette mise à jour OOB à la place. Pour obtenir des conseils supplémentaires, consultez Comment télécharger des mises à jour à partir du catalogue Microsoft Update. Comme toujours, nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Si l'OOB n'est pas installé, l'une des options de connexion suivantes peut être utilisée comme solution de contournement temporaire :

- Utiliser le client Bureau à distance pour Windows pour se connecter à Azure Virtual Desktop ici (/previous-versions/remote-desktop-client/whats-new-windows ?tabs=windows-msrdc-msi)
- Connectez-vous à l'aide du client web application Windows sur windows.cloud.microsoft

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2, Windows 10 Entreprise LTSC 2019
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019

Retour au début

Octobre 2025

Les sites web IIS peuvent ne pas se charger

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5068861	Build du système d'exploitation 26100.6899 KB5066835 14-10-2025	Résolu : 2025-11-11, 10:00 PT Ouvert : 2025-10-16, 16:06 PT

Après une enquête plus approfondie, nous avons conclu que ce problème ne s'appliquait pas à Windows Server 2025. Il affecte uniquement Windows 11, version 25H2 et 24H2.

Ce problème peut être ignoré par les utilisateurs de Windows Server.

Pour en savoir plus sur l'impact de ce problème sur Windows 11, sélectionnez l'un des liens ci-dessous :

- Windows 11, version 25H2
- Windows 11, version 24H2

Le problème mentionné ci-dessous a été publié avant cette découverte et les modifications du 14 novembre 2025 :

Suite à l'installation des mises à jour Windows publiées le 29 septembre ou après, les applications côté serveur qui s'appuient sur HTTP.sys peuvent rencontrer des problèmes avec les connexions entrantes. Par conséquent, les sites web IIS peuvent ne pas se charger, affichant un message tel que « Réinitialisation de connexion - erreur (ERR_CONNECTION_RESET) » ou une erreur similaire. Cela inclut les sites web hébergés sur http://localhost/et d'autres connexions IIS.

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2

Retour au début

Échec de la synchronisation d'annuaires pour les groupes AD de plus de 10 000 membres

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5068861	Build du système d'exploitation 26100.6584 KB5065426 2025-09-09	Résolu : 2025-11-11, 10:00 PT Ouvert : 2025-10-14, 17:49 PT

Les applications qui utilisent le contrôle de synchronisation d'annuaire Active Directory (DirSync) pour Active Directory local Domain Services (AD DS), par exemple lors de l'utilisation de Microsoft Entra Connect Sync, peuvent entraîner une synchronisation incomplète de groupes AD volumineux dépassant 10 000 membres. Ce problème se produit uniquement à Windows Server 2025 après l'installation de la mise à jour de sécurité Windows de septembre 2025 (KB5065426), ou des mises à jour ultérieures.

Résolution : Ce problème a été résolu par les mises à jour Windows publiées le 11 novembre 2025 KB5068861 et les mises à jour publiées après cette date. Nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Si vous avez installé des mises à jour publiées à partir du 11 novembre 2025 (KB5068861), vous n'avez pas besoin d'utiliser une restauration de problème connu (KIR) ou un stratégie de groupe spécial pour résoudre ce problème.

Si vous utilisez une mise à jour publiée avant le 11 novembre 2025 et que vous rencontrez ce problème, votre administrateur informatique peut le résoudre en installant et en configurant la stratégie de groupe spéciale répertoriée ci-dessous.

Téléchargements de la stratégie de groupe avec le nom de la stratégie de groupe :

- Télécharger pour Windows 11, versions 24H2 et 25H2 et Windows Server 2025 : Windows 11 24H2, Windows 11 25H2 et Windows Server 2025 KB5066835 251016_21401 Restauration du problème connu

Les stratégie de groupe spéciaux se trouvent dans**Configuration de l'ordinateur -> Modèles d'administration -> Windows 11 24H2, Windows 11 25H2 et Windows Server 2025 KB5066835 251016_21401 Restauration de problème connu.** Après avoir installé la stratégie de groupe, configurez la valeur **de restauration du problème connu KB5066835 251016_21401 sur Désactivé** et redémarrez Windows Server 2025 pour appliquer le paramètre de stratégie de groupe. (Windows 11 est hors du cadre de cette notification et de cette aide.) Pour plus d'informations sur le déploiement et la configuration de cette stratégie de groupe spéciale, consultez Comment utiliser une stratégie de groupe pour déployer une restauration de problème connu.

Les clients concernés peuvent également appliquer la clé de Registre suivante comme solution de contournement pour désactiver le changement de fonctionnalité.

Avertissement : des problèmes graves peuvent survenir si vous modifiez le Registre de façon incorrecte à l'aide de l'Éditeur du Registre ou d'une autre méthode. Ces problèmes peuvent nécessiter la réinstallation du système d'exploitation. Microsoft ne peut pas garantir que ces problèmes peuvent être résolus. Modifiez le Registre à vos propres risques. Pour plus d'informations, consultez Registre Windows pour utilisateurs avancés.

Chemin d’accès :
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\Microsoft\FeatureManagement\Overrides

Nom : 2362988687

Type : REG_DWORD

Valeur : 0

Plateformes affectées :

- Client : Aucun
- Serveur : Windows Server 2025

Retour au début

Des problèmes d’authentification par carte à puce peuvent se produire avec la mise à jour Windows d’octobre 2025

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Build du système d’exploitation 26100.6899 KB5066835 14-10-2025	Résolu : 2025-10-22, 17:31 PT Ouvert : 2025-10-17, 20:06 PT

L’authentification par carte intelligente et d’autres opérations de certificat peuvent échouer intentionnellement après l’installation de Windows Mises à jour publié à partir du 14 octobre 2025 (KB5066835) qui contient des protections contre la vulnérabilité de sécurité CVE-2024-30098 . Dans le cadre de cette amélioration du chiffrement, les certificats de carte à puce RSA sont requis pour utiliser KSP (fournisseur de stockage de clés) au lieu de CSP (fournisseur de services de chiffrement).

Voici quelques symptômes courants pour les certificats qui utilisent CSP :

- Les cartes à puce ne sont pas reconnues comme fournisseurs CSP (fournisseur de services de chiffrement) dans les applications 32 bits
- Incapacité à signer des documents
- Défaillances dans les applications reposant sur l’authentification basée sur les certificats
- Les utilisateurs peuvent observer des messages d’erreur tels que « Type de fournisseur spécifié non valide » et « Erreur CryptAcquireCertificatePrivateKey ».

Vous pouvez détecter si votre smart carte sera affecté par cette application de sécurité si, avant d’installer la mise à jour de sécurité Windows d’octobre 2025 (KB5066835), le journal système contient Smart Card Service

ou Microsoft-Windows-Smartcard-Server **Event ID : 624** avec le texte de message : « Audit : Ce système utilise CAPI pour les opérations de chiffrement RSA. Veuillez vous référer au lien suivant pour plus de détails : https://go.microsoft.com/fwlink/?linkid=2300823 ."

Résolution :

Pour une résolution permanente, les développeurs doivent mettre à jour leur application d'authentification pour effectuer une récupération du stockage de clés à l'aide de l'API de stockage de clés documentée dans Stockage et récupération de clés. Les développeurs doivent effectuer cette modification avant la publication des mises à jour Windows en avril 2026, date à laquelle la solution de contournement **DisableCapiOverrideForRSA** répertoriée ci-dessous devrait être supprimée.

Solution de contournement :

Si vous rencontrez ce problème, vous pouvez le résoudre temporairement en définissant la valeur de clé de Registre**DisableCapiOverrideForRSA** sur 0. Cela est documenté dans CVE-2024-30098 . Les étapes détaillées pour modifier la clé de Registre sont répertoriées ci-dessous. **Remarque** : cette option sera supprimée dans les mises à jour Windows, dont la sortie est prévue en avril 2026.

Étapes de modification du Registre

⚠ <**Important** : la modification incorrecte du Registre peut entraîner des problèmes système. Sauvegardez toujours le Registre avant d'apporter des modifications.

1. Ouvrez l'Éditeur du Registre.

- Appuyez sur Win + R, tapez regedit, puis appuyez sur Entrée.
- Si vous y êtes invité par le contrôle de compte d'utilisateur, cliquez sur Oui.

2. Accédez à la sous-clé.

- Accédez à : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais

3. Modifiez la clé et définissez la valeur.

- À l'intérieur de Calais, case activée si la clé DisableCapiOverrideForRSA existe
- Double-cliquez sur DisableCapiOverrideForRSA.
- Dans Date de la valeur, entrez : 0

Remarque : le paramètre de Registre DisableCapiOverrideForRSA n'est PAS ajouté par l'installation du système d'exploitation par défaut ou l'installation de Windows Mises à jour et doit être ajouté manuellement sur chaque appareil.

4. Fermez et redémarrez.

- Fermez l'Éditeur du Registre.
- Redémarrez l'ordinateur pour que les modifications prennent effet.

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 11, version 22H2 ; Windows 10, version 22H2
- Serveur : Windows Server 2025 ; Windows Server 23H2 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2

Retour au début

La souris et le clavier USB ne fonctionnent pas dans l'environnement de récupération Windows (WinRE)

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5070773	Build du système d'exploitation 26100.6899 KB5066835 14-10-2025	Résolu : 2025-10-20, 14:00 PT Ouvert : 2025-10-17, 22:18 PT

Après l'installation de la mise à jour de sécurité Windows publiée le 14 octobre 2025 (KB5066835), les périphériques USB, tels que les claviers et les souris, ne fonctionnent pas dans l'environnement de récupération Windows (WinRE). Ce problème empêche la navigation de l'une des options de récupération dans WinRE. Notez que les périphériques USB continuent de fonctionner normalement dans le système d'exploitation Windows.

Résolution : Ce problème a été résolu par la mise à jour hors bande Windows, publiée le 20 octobre 2025 (KB5070773), qui est disponible via le catalogue Microsoft Update, et les mises à jour publiées après cette date. Nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Solution de contournement : Si votre appareil est affecté par ce problème et ne parvient pas à démarrer à Windows pour installer la dernière mise à jour de Windows, vous pouvez contourner ce problème en utilisant l'une des méthodes suivantes :

- Si votre PC dispose d'un écran tactile, vous pouvez utiliser le clavier tactile de l'écran tactile pour naviguer dans WinRE.
- Si votre PC dispose d'un port PS/2, vous pouvez utiliser un clavier ou une souris PS/2 pour naviguer dans WinRE.
- Si vous avez déjà créé un lecteur de récupération USB, vous pouvez démarrer votre ordinateur à partir de ce lecteur. Cela vous mènera directement à WinRE avec la fonctionnalité USB restaurée.
- Les fabricants OEM et les entreprises peuvent utiliser l'environnement d'exécution préliminaire PXE (Preboot Execution Environment) dans Configuration Manager, ou peuvent déployer des fonctionnalités de réinitialisation rapide à l'aide du kit d'évaluation et de déploiement Windows (Windows ADK) et du

module complémentaire Windows Preinstallation Environment (WinPE) pour récupérer les appareils affectés.

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2
- Serveur : Windows Server 2025

Retour au début

Août 2025

Les mises à jour installées via WUSA peuvent échouer si elles sont installées à partir d'un dossier partagé

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5094125	Build du système d'exploitation 26100.4349 KB5060842 2025-06-10	Résolu : 2026-06-09, 10:00 PT Ouvert : 2025-08-15, 11:56 PT

Les mises à jour Windows installées à l'aide du programme d'installation autonome Windows Update (WUSA) peuvent échouer avec une erreur ERROR_BAD_PATHNAME, lorsque la mise à jour est installée à l'aide de WUSA ou lorsque vous double-cliquez sur un fichier .msu à partir d'un partage réseau qui contient plusieurs fichiers .msu. Ces problèmes peuvent se produire sur les appareils ayant installé les mises à jour publiées le 28 mai 2025 (KB5060842) et versions ultérieures.

WUSA est une méthode d'installation de mises à jour à l'aide de l'API de l'agent Windows Update qui est généralement utilisée uniquement dans les environnements d'entreprise. Il n'est pas courant dans les environnements personnels ou domestiques.

Notez que ce problème ne se produit pas lorsqu'il n'y a qu'un seul fichier .msu dans le partage réseau ou lorsque les fichiers .msu sont stockés localement sur l'appareil. En outre, après avoir installé un fichier .msu en double-cliquant ou en utilisant WUSA et en redémarrant Windows, vous remarquerez peut-être que la page Historique des mises à jour dans Paramètres continue d'indiquer qu'un redémarrage est nécessaire pour terminer la mise à jour. Ce problème est temporaire et doit être résolu par lui-même.

Résolution : ce problème a été résolu par les mises à jour Windows publiées le 9 juin 2026 (KB5094125) et versions ultérieures. Nous vous recommandons d'installer la dernière mise à jour de sécurité pour votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Si vous installez une mise à jour publiée le 9 juin 2026 (KB5094125) ou une version ultérieure, vous n'avez pas besoin d'utiliser une solution de contournement pour ce problème. Si vous utilisez une mise à jour publiée avant cette date et que vous rencontrez ce problème, vous pouvez la contourner en enregistrant les fichiers .msu localement sur l'appareil et en installant la mise à jour à partir de cet emplacement. En outre, si vous avez redémarré Windows après avoir installé un fichier .msu via WUSA, veuillez attendre au moins 15 minutes avant de vérifier la page Historique des mises à jour dans les Paramètres. Après ce court délai, l'application Paramètres doit indiquer correctement si la mise à jour a été correctement installée.

En outre, ce problème a été résolu à l'aide de la restauration des problèmes connus (KIR) à partir de septembre 2025 et a été résolu automatiquement pour la plupart des utilisateurs à domicile et des appareils professionnels non gérés. Le redémarrage de votre appareil Windows peut aider la résolution à s'appliquer à votre appareil plus rapidement. Les administrateurs informatiques peuvent résoudre ce problème pour les appareils gérés qui ont installé la mise à jour concernée et rencontré ce problème. Il peut être résolu en installant et en configurant la stratégie de groupe répertoriée ci-dessous. Pour plus d'informations sur le déploiement et la configuration de ces stratégies de groupe spéciales, consultez Comment utiliser une stratégie de groupe pour déployer une restauration de problème connu. La stratégie de groupe spéciale se trouve dans Modèles > **d'administration de configuration** > ordinateur [**nom de la stratégie de groupe**].

Téléchargements de la stratégie de groupe avec le nom de la stratégie de groupe :

- Télécharger pour Windows 11, version 24H2 et Windows Server, version 2025 - Windows 11 24H2 et Windows Server 2025 KB5062660 250806_17201 Problème connu Rollback.msi

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2
- Serveur : Windows Server 2025

Retour au début

Novembre 2024

Windows Server 2022 et Server 2019 ont été mis à niveau de manière inattendue vers Windows Server 2025

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5082063	Non applicable	Résolu : 2026-04-14, 10:00 PT Ouvert : 2024-11-09, 12:16 PT

Windows Server 2025 est destiné à être proposé en tant que mise à niveau **facultative** dans les paramètres de **Windows Update** pour les appareils exécutant Windows Server 2019 et Windows Server 2022. Deux scénarios

ont été observés dans certains environnements :

- Certains appareils ont été mis à niveau automatiquement vers Windows Server 2025 (KB5044284). Ce problème a été observé dans les environnements qui utilisent des produits tiers pour gérer la mise à jour des clients et des serveurs. Vérifiez si les logiciels de mise à jour tiers de votre environnement sont configurés pour ne pas déployer les mises à jour de fonctionnalités. Ce scénario a été atténué.

- Une mise à niveau vers Windows Server 2025 a été proposée via un message dans une bannière affichée sur la page **Windows Update** de l'appareil, sous **Paramètres**. Ce message est destiné aux organisations qui souhaitent exécuter une mise à niveau sur place. Ce scénario a déjà été résolu.

La mise à jour des fonctionnalités de Windows Server 2025 a été publiée en tant que mise à jour **facultative** sous la classification de mise à niveau : « DeploymentAction=OptionalInstallation ». Les métadonnées de mise à jour des fonctionnalités doivent être interprétées comme **facultatives** et non **recommandées** par les outils de gestion des correctifs.

Nous conseillons aux organisations d'utiliser les méthodes recommandées par Microsoft pour déployer les mises à jour des fonctionnalités de Windows Server.

Résolution : Ce problème est résolu et Microsoft a réactivé l'offre de mise à niveau via le panneau de configuration de **Windows Update** . Pour plus d'informations sur la mise à jour des fonctionnalités à partir de la boîte de dialogue de configuration de Windows Server, consultez Effectuer une mise à niveau sur place de Windows Server sur Microsoft Learn.

Plateformes affectées :

- Client : Aucun
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019

Retour au début

Signaler un problème avec les mises à jour Windows

Pour signaler un problème à Microsoft à tout moment, utilisez l'application Hub de commentaires . Pour plus d'informations, consultez Envoyer des commentaires à Microsoft avec l'application Hub de commentaires .

Besoin d'aide pour Windows Update ?

Recherchez, parcourez ou posez une question sur la communauté de Support Microsoft. Si vous êtes un professionnel de l'informatique soutenant une organisation, visitez l'état de publication de Windows sur le Centre d'administration Microsoft 365 pour plus de détails.

Pour obtenir de l'aide directe sur votre PC personnel, utilisez l'application Aide sur Windows ou contactez le Support Microsoft. Les organisations peuvent demander un support immédiat par le biais du Support pour les entreprises.

Afficher ce site dans votre langue

Ce site est disponible en 11 langues : anglais, chinois traditionnel, chinois simplifié, français (France), allemand, italien, japonais, coréen, portugais (Brésil), russe et espagnol (Espagne). Tout le texte s'affiche en anglais si la langue par défaut de votre navigateur n'est pas l'une des 11 langues prises en charge. Pour changer manuellement la langue d'affichage, faites défiler vers le bas de cette page, cliquez sur la langue actuelle affichée en bas à gauche de la page et sélectionnez l'une des 11 langues prises en charge dans la liste.

Dernière mise à jour : 16/10/2026

Windows Server 2022

Problèmes connus et notifications

Trouvez des informations sur les problèmes connus et le status de maintenance pour Windows Server 2022. Pour obtenir une aide immédiate sur les problèmes de Windows Update, cliquez ici si vous utilisez un appareil Windows pour ouvrir l'application Aide ou accéder à support.microsoft.com. Suivez @WindowsUpdate sur X (anciennement Twitter) les mises à jour d'intégrité des versions Windows. Si vous êtes administrateur informatique et que vous souhaitez obtenir des informations par programme à partir de cette page, utilisez l'API des mises à jour Windows dans Microsoft Graph.

Statut actuel au 13 octobre 2026

Depuis le 13 octobre 2026, Windows Server 2022 a atteint la fin du support standard et est passé au support étendu. Windows Server 2022 continuera à recevoir des mises à jour de sécurité mensuelles sans frais supplémentaires jusqu'au 14 octobre 2031. Pour plus d'informations, consultez la politique de cycle de vie fixe.

Prise en charge des mises à jour de patch à chaud pour Windows Server 2022 Datacenter : Azure Edition a été prolongée jusqu'en octobre 2027. Les appareils inscrits dans des mises à jour de patch à chaud continueront de recevoir des mises à jour de sécurité mensuelles sans nécessiter de redémarrage. Pour en savoir plus, consultez la page du cycle de vie de Windows Server 2022.

Windows Server 2025 est la dernière version du canal de maintenance Long-Term (LTSC) pour Windows Server. Pour télécharger une évaluation gratuite de 180 jours, visitez le Centre d'évaluation Microsoft.

Nouveautés de Windows Server 2025

Découvrez ses fonctionnalités avancées et ses innovations

Obtenir les problèmes connus de Windows Server dans l'API Graph

Les données sont disponibles pour les versions de Windows Server prises en charge

Voir tous les messages >

Problèmes connus

Consultez les problèmes ouverts, le contenu mis à jour au cours des 30 derniers jours et les informations sur les dispositifs de protection. Pour rechercher un problème spécifique, utilisez la fonction de recherche de votre navigateur (CTRL + F pour Microsoft Edge).

Agrandir le tableau

Résumé	Mise à jour d'origine	Statut	Dernière mise à jour
Les périphériques audio USB peuvent ne pas démarrer ou ne pas produire de son Certains appareils audio USB de classe 1.0 affichent le code 10 ou échouent en mode audio multicanal après l'installation de la mise à jour du 8 septembre	Os Build 20348.5622 KB5122882 2026-09-08	Résolu KB5129237	2026-10-13 11h02 PT
Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé » L'antivirus Microsoft Defender reste actif et fonctionne correctement malgré les notifications suite à la dernière mise à jour.	Non applicable	Résolu	2026-09-30 16h42 PT
Les services Bureau à distance pourraient cesser de répondre après la mise à jour de sécurité de septembre 2026 Certains appareils Windows sur lesquels le Bureau à distance est activé peuvent rencontrer une instabilité des Services Bureau à distance (RDS).	Os Build 20348.5622 KB5122882 2026-09-08	Résolu KB5129237	2026-09-17 19h22 PT

Détails du problème

Septembre 2026

Les périphériques audio USB peuvent ne pas démarrer ou ne pas produire de son

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5129237	Os Build 20348.5622 KB5122882 2026-09-08	Résolu : 2026-09-14, 10:00 PT Ouvert : 2026-09-11, 18:36 PT

Après l'installation de la mise à jour de sécurité Windows (KB5122882) du 8 septembre 2026, certains appareils USB audio classe 1.0 peuvent ne pas démarrer ou produire du son. Les appareils affectés peuvent rencontrer un ou plusieurs des symptômes suivants :

- L'appareil affiche une erreur dans le Gestionnaire de périphériques : « Ce périphérique ne peut pas démarrer (Code 10) ».
- Aucune sortie audio.
- Les contrôles de volume ne répondent pas ou restent à zéro.
- Les paramètres sonores ne répondent pas ou ne sont pas disponibles.
- Certains périphériques peuvent fonctionner dans des configurations stéréo standard, mais échouer lors de l'utilisation de fonctionnalités audio multicanaux, notamment les modes audio 8 canaux ou 3D. Certains clients ont signalé qu'ils sont en mesure de restaurer l'audio dans ces cas en passant en mode 2 canaux. *(*Remarque : ce comportement est résolu dans la mise à jour hors bande publiée le 14 septembre 2026. Voir la section Résolution ci-dessous.)*

Ce problème se limite aux périphériques audio USB de classe 1.0.

Résolution : Les symptômes rencontrés sur les appareils utilisant le mode audio 8 canaux ou 3D (dernier point de la liste de symptômes décrits dans cet article) sont résolus dans la mise à jour hors bande publiée le 14 septembre 2026 (KB5129237) et les mises à jour publiées après cette date. Les symptômes restants sont résolus dans le correctif de sécurité Windows publié le 13 octobre 2026 (KB5126655) et les mises à jour ultérieures. Nous vous recommandons d'installer la dernière mise à jour de sécurité pour votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Si vous êtes un administrateur informatique qui a contacté le Support Microsoft pour les entreprises pour obtenir une solution de contournement immédiate, vous n'avez pas besoin d'utiliser la restauration de problème connu ou une stratégie de groupe spéciale pour résoudre ce problème.

Plateformes affectées :

- Client : Windows 11, version 26H2 ; Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Les services Bureau à distance pourraient cesser de répondre après la mise à jour de sécurité de septembre 2026

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5129237	Os Build 20348.5622 KB5122882 2026-09-08	Résolu : 2026-09-14, 10:00 PT Ouvert : 2026-09-11, 11:19 PT

Après l'installation de la mise à jour de sécurité Windows de septembre 2026 (KB5122882), certaines organisations peuvent rencontrer des problèmes avec les services Bureau à distance (RDS).

Dans certains environnements, les services Bureau à distance peuvent devenir instables, ce qui entraîne l'échec des connexions RDP après plusieurs minutes, des problèmes de connexion ou le blocage des serveurs sur l'écran « Veuillez attendre la configuration du Bureau à distance ». Les outils connexes, notamment Microsoft Management Console (MMC), RDS Licensing Diagnoser et l'Explorateur de fichiers peuvent également ne plus répondre. En outre, la page Windows Update peut cesser de répondre et afficher en permanence un indicateur de chargement.

Remarque : Ce problème n'affecte pas Windows 365 ou Azure Virtual Desktop.

Résolution : Ce problème est résolu par la mise à jour hors cycle publiée le 14 septembre 2026 (KB5129237), et par les mises à jour publiées après cette date.

Les administrateurs informatiques qui ont déployé une atténuation temporaire via la stratégie de groupe n'ont pas besoin de prendre de mesures avant d'installer cette mise à jour OOB.

Cette mise à jour OOB est cumulative et inclut toutes les améliorations et protections de sécurité contenues dans les mises à jour Windows précédentes. Nous vous recommandons d'installer la dernière mise à jour disponible pour vos appareils, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Août 2026

Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé »

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Non applicable	Résolu : 2026-09-30, 16:42 PT Ouvert : 2026-08-28, 15:34 PT

Après l'installation de Microsoft Defender mise à jour de l'antivirus (version 4.18.26070.9), publiée le 5 août 2026, des notifications peuvent apparaître indiquant que « l'antivirus Microsoft Defender est désactivé », même si l'antivirus fonctionne correctement et que tous les paramètres l'indiquent comme actif. Ces notifications peuvent apparaître au démarrage de Windows et par intermittence par la suite. Ils persistent même si les paramètres de notification sont désactivés.

Ce problème peut être observé dans n'importe quelle version de Windows ou de Windows Server avec l'antivirus Microsoft Defender exécuté avec les dernières mises à jour Defender.

Résolution : Ce problème a été résolu dans la mise à jour de l'antivirus Microsoft Defender (version 4.18.26080.4), publiée le 17 septembre 2026.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Signaler un problème avec les mises à jour Windows

Pour signaler un problème à Microsoft à tout moment, utilisez l'application Hub de commentaires . Pour plus d'informations, consultez Envoyer des commentaires à Microsoft avec l'application Hub de commentaires.

Besoin d'aide pour Windows Update ?

Recherchez, parcourez ou posez une question sur la communauté de Support Microsoft. Si vous êtes un professionnel de l'informatique soutenant une organisation, visitez l'état de publication de Windows sur le Centre d'administration Microsoft 365 pour plus de détails.

Pour obtenir de l'aide directe sur votre PC personnel, utilisez l'application Aide sur Windows ou contactez le Support Microsoft. Les organisations peuvent demander un support immédiat par le biais du Support pour les entreprises.

Afficher ce site dans votre langue

Ce site est disponible en 11 langues : anglais, chinois traditionnel, chinois simplifié, français (France), allemand, italien, japonais, coréen, portugais (Brésil), russe et espagnol (Espagne). Tout le texte s'affiche en anglais si la langue par défaut de votre navigateur n'est pas l'une des 11 langues prises en charge. Pour changer manuellement la langue d'affichage, faites défiler vers le bas de cette page, cliquez sur la langue actuelle affichée en bas à gauche de la page et sélectionnez l'une des 11 langues prises en charge dans la liste.

Dernière mise à jour : 16/10/2026

Résolution des problèmes dans Windows Server 2022

Trouvez des informations sur les problèmes récemment résolus pour Windows Server 2022. Pour rechercher un problème spécifique, utilisez la fonction de recherche de votre navigateur (CTRL + F pour Microsoft Edge). Pour obtenir une aide immédiate sur les problèmes de Windows Update, cliquez ici si vous utilisez un appareil Windows pour ouvrir l'application Aide ou accéder à support.microsoft.com. Suivez @WindowsUpdate sur X (anciennement Twitter) les mises à jour d'intégrité des versions Windows. Si vous êtes administrateur informatique et que vous souhaitez obtenir des informations par programme à partir de cette page, utilisez l'API des mises à jour Windows dans Microsoft Graph.

Problèmes résolus

Agrandir le tableau

Résumé	Mise à jour d'origine	Statut	Date résolue
Les périphériques audio USB peuvent ne pas démarrer ou ne pas produire de son Certains appareils audio USB de classe 1.0 affichent le code 10 ou échouent en mode audio multicanal après l'installation de la mise à jour du 8 septembre	Os Build 20348.5622 KB5122882 2026-09-08	Résolu KB5129237	2026-09-14 10:00 PT
Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé » L'antivirus Microsoft Defender reste actif et fonctionne correctement malgré les notifications suite à la dernière mise à jour.	Non applicable	Résolu	2026-09-30 16h42 PT
Les services Bureau à distance pourraient cesser de répondre après la mise à jour de sécurité de septembre 2026 Certains appareils Windows sur lesquels le Bureau à distance est activé peuvent rencontrer une instabilité des Services Bureau à distance (RDS).	Os Build 20348.5622 KB5122882 2026-09-08	Résolu KB5129237	2026-09-14 10:00 PT
Les opérations de synchronisation de Windows Server Update Services peuvent rencontrer des	Non applicable	Résolu	2026-07-20 13h22 PT

Résumé	Mise à jour d'origine	Statut	Date résolue
problèmes ou expirer Des efforts d'assainissement sont en cours. Les temps de synchronisation devraient revenir à la normale à mesure que la récupération progresse.			
La suppression d'un fichier de la Corbeille affiche un nom de fichier interne dans la boîte de dialogue Ce problème se produit uniquement dans la boîte de dialogue de confirmation après l'installation de la mise à jour de sécurité Windows de juin.	Os Build 20348.5256 KB5094128 2026-06-09	Résolu KB5099540	2026-07-14 10:00 PT
Les contrôleurs de domaine peuvent redémarrer à plusieurs reprises après l'installation de la mise à jour de sécurité d'avril Les contrôleurs de domaine affectés subiront des incidents LSASS. Une atténuation est disponible via le Support Microsoft.	Os Build 20348.5020 KB5082142 2026-04-14	Résolu KB5091575	2026-04-19 14:00 PT
Windows Server 2022 et Server 2019 ont été mis à niveau de manière inattendue vers Windows Server 2025 Ce problème a été atténué. Il a été observé lorsque les mises à jour étaient gérées par certaines applications tierces.	Non applicable	Résolu KB5082142	2026-04-14 10:00 PT
Certains appareils peuvent ne pas s'arrêter ou rester en veille prolongée Ce problème affecte certains PC compatibles avec Secure Launch avec le mode sécurisé virtuel activé après l'installation des mises à jour du 26 janvier.	Os Build 20348.4648 KB5073457 2026-01-13	Résolu KB5075906	2026-02-10 10:00 PT
Les applications peuvent cesser de répondre lors de l'enregistrement des fichiers dans un stockage sur le cloud Les applications concernées incluent Outlook, qui peut ne plus répondre lors de l'accès aux fichiers PST stockés sur Microsoft OneDrive.	Os Build 20348.4648 KB5073457 2026-01-13	Résolu KB5078136	2026-01-23 14:00 PT
Échecs de connexion et d'authentification dans Azure Virtual Desktop et Windows 365 Janvier 2026 La mise à jour Windows provoque des échecs d'invite d'informations d'identification de l'application application Windows sur Azure Virtual Desktop et Windows 365	Os Build 20348.4648 KB5073457 2026-01-13	Résolu KB5077800	2026-01-17 14:00 PT
Des problèmes d'authentification par carte à puce peuvent se produire avec la mise à jour Windows d'octobre 2025	Os Build 20348.4294 KB5066782 14-10-2025	Résolu	2025-10-22 17:31 PT

Résumé	Mise à jour d'origine	Statut	Date résolue
Ce problème est lié à une modification de sécurité introduite pour renforcer les services de chiffrement Windows.			

Détails du problème

Septembre 2026

Les périphériques audio USB peuvent ne pas démarrer ou ne pas produire de son

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5129237	Os Build 20348.5622 KB5122882 2026-09-08	Résolu : 2026-09-14, 10:00 PT Ouvert : 2026-09-11, 18:36 PT

Après l'installation de la mise à jour de sécurité Windows (KB5122882) du 8 septembre 2026, certains appareils USB audio classe 1.0 peuvent ne pas démarrer ou produire du son. Les appareils affectés peuvent rencontrer un ou plusieurs des symptômes suivants :

- L'appareil affiche une erreur dans le Gestionnaire de périphériques : « Ce périphérique ne peut pas démarrer (Code 10) ».
- Aucune sortie audio.
- Les contrôles de volume ne répondent pas ou restent à zéro.
- Les paramètres sonores ne répondent pas ou ne sont pas disponibles.
- Certains périphériques peuvent fonctionner dans des configurations stéréo standard, mais échouer lors de l'utilisation de fonctionnalités audio multicanaux, notamment les modes audio 8 canaux ou 3D. Certains clients ont signalé qu'ils sont en mesure de restaurer l'audio dans ces cas en passant en mode 2 canaux. *(*Remarque : ce comportement est résolu dans la mise à jour hors bande publiée le 14 septembre 2026. Voir la section Résolution ci-dessous.)*

Ce problème se limite aux périphériques audio USB de classe 1.0.

Résolution : Les symptômes rencontrés sur les appareils utilisant le mode audio 8 canaux ou 3D (dernier point de la liste de symptômes décrits dans cet article) sont résolus dans la mise à jour hors bande publiée le 14 septembre 2026 (KB5129237) et les mises à jour publiées après cette date. Les symptômes restants sont résolus dans le correctif de sécurité Windows publié le 13 octobre 2026 (KB5126655) et les mises à jour ultérieures. Nous vous recommandons d'installer la dernière mise à jour de sécurité pour votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Si vous êtes un administrateur informatique qui a contacté le Support Microsoft pour les entreprises pour obtenir une solution de contournement immédiate, vous n'avez pas besoin d'utiliser la restauration de problème connu ou une stratégie de groupe spéciale pour résoudre ce problème.

Plateformes affectées :

- Client : Windows 11, version 26H2 ; Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Les services Bureau à distance pourraient cesser de répondre après la mise à jour de sécurité de septembre 2026

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5129237	Os Build 20348.5622 KB5122882 2026-09-08	Résolu : 2026-09-14, 10:00 PT Ouvert : 2026-09-11, 11:19 PT

Après l'installation de la mise à jour de sécurité Windows de septembre 2026 (KB5122882), certaines organisations peuvent rencontrer des problèmes avec les services Bureau à distance (RDS).

Dans certains environnements, les services Bureau à distance peuvent devenir instables, ce qui entraîne l'échec des connexions RDP après plusieurs minutes, des problèmes de connexion ou le blocage des serveurs sur l'écran « Veuillez attendre la configuration du Bureau à distance ». Les outils connexes, notamment Microsoft Management Console (MMC), RDS Licensing Diagnoser et l'Explorateur de fichiers peuvent également ne plus répondre. En outre, la page Windows Update peut cesser de répondre et afficher en permanence un indicateur de chargement.

Remarque : Ce problème n'affecte pas Windows 365 ou Azure Virtual Desktop.

Résolution : Ce problème est résolu par la mise à jour hors cycle publiée le 14 septembre 2026 (KB5129237), et par les mises à jour publiées après cette date.

Les administrateurs informatiques qui ont déployé une atténuation temporaire via la stratégie de groupe n'ont pas besoin de prendre de mesures avant d'installer cette mise à jour OOB.

Cette mise à jour OOB est cumulative et inclut toutes les améliorations et protections de sécurité contenues dans les mises à jour Windows précédentes. Nous vous recommandons d'installer la dernière mise à jour

disponible pour vos appareils, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Août 2026

Notifications incorrectes indiquant que « l'antivirus Microsoft Defender est désactivé »

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Non applicable	Résolu : 2026-09-30, 16:42 PT Ouvert : 2026-08-28, 15:34 PT

Après l'installation de Microsoft Defender mise à jour de l'antivirus (version 4.18.26070.9), publiée le 5 août 2026, des notifications peuvent apparaître indiquant que « l'antivirus Microsoft Defender est désactivé », même si l'antivirus fonctionne correctement et que tous les paramètres l'indiquent comme actif. Ces notifications peuvent apparaître au démarrage de Windows et par intermittence par la suite. Ils persistent même si les paramètres de notification sont désactivés.

Ce problème peut être observé dans n'importe quelle version de Windows ou de Windows Server avec l'antivirus Microsoft Defender exécuté avec les dernières mises à jour Defender.

Résolution : Ce problème a été résolu dans la mise à jour de l'antivirus Microsoft Defender (version 4.18.26080.4), publiée le 17 septembre 2026.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Juillet 2026

Les opérations de synchronisation de Windows Server Update Services peuvent rencontrer des problèmes ou expirer

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Non applicable	Résolu : 2026-07-20, 13:22 PT Ouvert : 2026-07-17, 18:18 PT

Microsoft a identifié une dégradation des services affectant Windows Server Update Services (WSUS). Les organisations peuvent constater une augmentation des temps de synchronisation ou des délais d'expiration des opérations de synchronisation sur les serveurs WSUS. Ce problème a commencé ces derniers jours, avec un impact accru observé à partir du 13 juillet 2026 et une atténuation côté service le samedi 18 juillet 2026. Après ce jour, les heures de synchronisation et les opérations de synchronisation devraient être rétablies à la normale.

Ce problème est lié à une accumulation de métadonnées de publication qui est présente sur les installations de serveur WSUS existantes ainsi que du côté service.

Résolution : La résolution de ce problème comporte deux parties.

- Les organisations avec des installations de serveur WSUS existantes qui connaissent de longs temps de synchronisation peuvent tirer parti d'étapes manuelles afin de propre des métadonnées inutiles. Ces métadonnées sont présentes dans les installations WSUS existantes, mais peuvent être supprimées en toute sécurité. Des instructions détaillées sont fournies dans l'article suivant de la Base de connaissances : https://support.microsoft.com/help/5121986
- Le 18 juillet 2026, Microsoft a déployé une atténuation côté service qui rétablit les temps de synchronisation et les opérations de synchronisation à la normale pour les nouvelles installations et reconstructions WSUS. Après cette date, les serveurs WSUS nouvellement installés ou recréés ne devraient pas rencontrer ce problème.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10, version 1809 ; Windows 10 Entreprise LTSC 2019 ; Windows 10 Entreprise LTSC 2016 ; Windows 10, version 1607
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server, version 1809 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

juin 2026

La suppression d’un fichier de la Corbeille affiche un nom de fichier interne dans la boîte de dialogue

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5099540	Os Build 20348.5256 KB5094128 2026-06-09	Résolu : 2026-07-14, 10:00 PT Ouvert : 2026-06-18, 12:03 PT

Lors de la suppression définitive d’un seul élément de la Corbeille, la boîte de dialogue de confirmation affiche le nom de fichier interne de la Corbeille (par exemple, $Rxxxxx.ext) au lieu du nom de fichier d’origine. La Corbeille elle-même affiche correctement le nom de fichier d’origine, et la restauration de l’élément le restaure également à l’aide du nom de fichier d’origine.

Ce problème se produit après l’installation du correctif de sécurité Windows publié le 9 juin 2026 (KB5094128).

Résolution : Ce problème a été résolu par les mises à jour Windows publiées le 14 juillet 2026 (KB5099540) et versions ultérieures. Nous vous recommandons d’installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci. Si votre organisation a installé une mise à jour publiée le 14 juillet 2026 ou une version ultérieure, vous n’avez pas besoin d’utiliser une restauration de problème connu ou une stratégie de groupe spéciale pour résoudre ce problème.

Plateformes affectées :

- Client : Windows 11, version 26H1 ; Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2 ; Windows 10 Entreprise LTSC 2019 ; Windows 10, version 1607
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2 ; Windows Server 2012

Retour au début

Avril 2026

Les contrôleurs de domaine peuvent redémarrer à plusieurs reprises après l'installation de la mise à jour de sécurité d'avril

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5091575	Os Build 20348.5020 KB5082142 2026-04-14	Résolu : 2026-04-19, 14:00 PT Ouvert : 2026-04-16, 18:50 PT

Après l'installation de la mise à jour de sécurité Windows (KB5082142) d'avril 2026 et le redémarrage, les contrôleurs de domaine (DC) dans les environnements avec plusieurs domaines dans la forêt qui utilisent Privileged Access Management (PAM) peuvent rencontrer des blocages LSASS au démarrage. Par conséquent, les contrôleurs de domaine affectés peuvent redémarrer à plusieurs reprises, empêchant l'authentification et les services d'annuaire de fonctionner, et potentiellement rendant le domaine indisponible.

Remarque : Ce problème affecte uniquement Windows Server. Il n'a pas d'impact sur les PC grand public ou les appareils personnels. Il est peu probable que le scénario soit observé sur des appareils à usage individuel qui ne sont pas gérés par un service informatique.

Résolution : Ce problème est résolu par les mises à jour hors cycle publiées le 19 avril 2026.

- La mise à jour standard de OOB est disponible en tant que KB5091575. Il peut être téléchargé à partir du catalogue Microsoft Update. Pour obtenir des conseils supplémentaires, consultez Comment télécharger des mises à jour à partir du catalogue Microsoft Update.
- Si votre appareil Windows Server 2022 est inscrit à la mise à jour corrective à chaud, vous devez plutôt installer la mise à jour de mise à jour OOB hotpatch KB5091576. Cette mise à jour hotpatch OOB est publiée via Windows Update et ne nécessite pas le redémarrage de l'appareil.

Versions concernées :

- Client : Aucun
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server, version 23H2 ; Windows Server 2019 ; Windows Server 2016

Retour au début

Janvier 2026

Certains appareils peuvent ne pas s'arrêter ou rester en veille prolongée

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5075906	Os Build 20348.4648 KB5073457 2026-01-13	Résolu : 2026-02-10, 10:00 PT Ouvert : 2026-01-15, 18:33 PT

Après l'installation des mises à jour Windows publiées le 13 janvier 2026 (KB5073457), certains PC compatibles avec Secure Launch avec le mode VSM (Virtual Secure Mode) activé ne peuvent pas s'arrêter ou entrer en mise en veille prolongée. Au lieu de cela, l'appareil redémarre. Ce problème n'affecte pas les appareils équipés de processeurs AMD ou ARM64 et se limite aux plateformes affectées répertoriées ci-dessous.

Résolution : Ce problème a été résolu par les mises à jour Windows publiées le 10 février 2026 (KB5075906) et les mises à jour publiées après cette date. Nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Plateformes affectées :

- Client : Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10 Entreprise LTSC 2021 ; Windows 10 Entreprise LTSC 2019
- Serveur : Windows Server 2022 ; Windows Server 2019

Retour au début

Les applications peuvent cesser de répondre lors de l'enregistrement des fichiers dans un stockage sur le cloud

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5078136	Os Build 20348.4648 KB5073457 2026-01-13	Résolu : 2026-01-23, 14:00 PT Ouvert : 2026-01-20, 22:10 PT

Après l'installation des mises à jour Windows publiées le 13 janvier 2026 (KB5073457), certaines applications peuvent ne plus répondre ou rencontrer des erreurs inattendues lors de l'ouverture ou de l'enregistrement de fichiers à partir d'un stockage cloud tel que OneDrive ou Dropbox.

Par exemple, dans certaines configurations d'Outlook qui stockent des fichiers PST sur OneDrive, Outlook peut ne plus répondre et ne pas pouvoir être rouvert , sauf si son processus est arrêté dans le Gestionnaire des tâches ou si le système est redémarré. En outre, les e-mails envoyés peuvent ne pas apparaître dans le dossier Éléments envoyés et les e-mails précédemment téléchargés peuvent être téléchargés à nouveau. Les configurations Outlook concernées impliquent principalement Outlook classique, qui est généralement lié aux

licences d'entreprise et n'est pas inclus dans la plupart des installations à domicile de Windows. Pour vérifier votre configuration Outlook en case activée, consultez Comparaison des fonctionnalités entre le nouvel Outlook et Outlook classique.

Résolution :

Ce problème est résolu dans leKB5078136 de mise à jour hors cycle (OOB), publié le 24 janvier 2026 et disponible via lecatalogue Microsoft Update, ainsi que dans les mises à jour publiées après cette date. Nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Remarque : pour télécharger des mises à jour à partir du Catalogue Microsoft Update, suivez les étapes décrites dans cet article.

Pour les appareils qui n'ont pas encore installé la mise à jour OOB, il existe une solution de contournement facultative pour les scénarios spécifiques à Outlook. Le déplacement des fichiers Outlook PST hors de OneDrive devrait résoudre ce problème. Pour obtenir des conseils, consultez la documentation sur la suppression d'un fichier de données Outlook .pst de OneDrive. De plus, les comptes de messagerie sont toujours accessibles via le webmail, si votre fournisseur de messagerie le prend en charge.

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10 Entreprise LTSC 2021 ; Windows 10 Entreprise LTSC 2019
- Serveur : Windows Server 2025 ; Windows Server, version 23H2 ; Windows Server 2022 ; Windows Server 2019

Retour au début

Échecs de connexion et d'authentification dans Azure Virtual Desktop et Windows 365

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu KB5077800	Os Build 20348.4648 KB5073457 2026-01-13	Résolu : 2026-01-17, 14:00 PT Ouvert : 14-01-2026, 00:52 PT

Après l'installation de la mise à jour de sécurité Windows de janvier 2026 (KB5073457), des échecs d'invite d'informations d'identification peuvent se produire dans certaines applications de connexion à distance. Cela inclut les connexions Bureau à distance à l'aide de l'application application Windows sur les appareils clients

Windows, sur Azure Virtual Desktop et Windows 365. L'application application Windows est affectée par ce problème sur des builds Windows spécifiques et peut rencontrer des échecs de connexion.

D'autres connexions à distance et applications associées peuvent être touchées de la même manière.

Résolution : Pour résoudre ce problème, une mise à jour hors cycle (OOB) a été publiée le 17 janvier 2026 dans le Catalogue Microsoft Update. Il peut être trouvé sous la forme KB5077800.

Si vous n'avez pas encore déployé la mise à jour de sécurité Windows de janvier 2026 et que votre environnement informatique inclut les applications et fonctionnalités affectées, nous vous recommandons d'appliquer cette mise à jour OOB à la place. Pour obtenir des conseils supplémentaires, consultez Comment télécharger des mises à jour à partir du catalogue Microsoft Update. Comme toujours, nous vous recommandons d'installer la dernière mise à jour de votre appareil, car elle contient des améliorations importantes et des résolutions de problèmes, y compris celle-ci.

Si l'OOB n'est pas installé, l'une des options de connexion suivantes peut être utilisée comme solution de contournement temporaire :

- Utiliser le client Bureau à distance pour Windows pour se connecter à Azure Virtual Desktop ici (/previous-versions/remote-desktop-client/whats-new-windows ?tabs=windows-msrdc-msi)
- Connectez-vous à l'aide du client web application Windows sur windows.cloud.microsoft

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 10, version 22H2 ; Windows 10, version 21H2, Windows 10 Entreprise LTSC 2019
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019

Retour au début

Octobre 2025

Des problèmes d'authentification par carte à puce peuvent se produire avec la mise à jour Windows d'octobre 2025

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolu	Os Build 20348.4294 KB5066782 14-10-2025	Résolu : 2025-10-22, 17:31 PT Ouvert : 2025-10-17, 20:06 PT

L'authentification carte intelligente et d'autres opérations de certificat peuvent échouer intentionnellement après l'installation de Windows Mises à jour publié à partir du 14 octobre 2025 (KB5066782) qui contient des

protections contre la vulnérabilité de sécurité CVE-2024-30098. Dans le cadre de cette amélioration du chiffrement, les certificats de carte à puce RSA sont requis pour utiliser KSP (fournisseur de stockage de clés) au lieu de CSP (fournisseur de services de chiffrement).

Voici quelques symptômes courants pour les certificats qui utilisent CSP :

- Les cartes à puce ne sont pas reconnues comme fournisseurs CSP (fournisseur de services de chiffrement) dans les applications 32 bits
- Incapacité à signer des documents
- Défaillances dans les applications reposant sur l'authentification basée sur les certificats
- Les utilisateurs peuvent observer des messages d'erreur tels que « Type de fournisseur spécifié non valide » et « Erreur CryptAcquireCertificatePrivateKey ».

Vous pouvez détecter si votre carte intelligente sera affectée par cette application de sécurité si, avant d'installer la mise à jour de sécurité Windows d'octobre 2025 (KB5066782), le journal système contient un ID d'événement de service de carte à puce ou de serveur Microsoft-Windows-Smartcard : **624** avec le texte du message : « Audit : Ce système utilise CAPI pour les opérations de chiffrement RSA. Veuillez vous référer au lien suivant pour plus de détails : https://go.microsoft.com/fwlink/?linkid=2300823."

Résolution :

Pour une résolution permanente, les développeurs doivent mettre à jour leur application d'authentification pour effectuer une récupération du stockage de clés à l'aide de l'API de stockage de clés documentée dans Stockage et récupération de clés. Les développeurs doivent effectuer cette modification avant la publication des mises à jour Windows en avril 2026, date à laquelle la solution de contournement **DisableCapiOverrideForRSA** répertoriée ci-dessous devrait être supprimée.

Solution de contournement :

Si vous rencontrez ce problème, vous pouvez le résoudre temporairement en définissant la valeur de clé de Registre**DisableCapiOverrideForRSA** sur 0. Cela est documenté dans CVE-2024-30098. Les étapes détaillées pour modifier la clé de Registre sont répertoriées ci-dessous. **Remarque** : cette option sera supprimée dans les mises à jour Windows, dont la sortie est prévue en avril 2026.

Étapes de modification du Registre

⚠ <**Important** : la modification incorrecte du Registre peut entraîner des problèmes système. Sauvegardez toujours le Registre avant d'apporter des modifications.

1. Ouvrez l'Éditeur du Registre.

- Appuyez sur Win + R, tapez regedit, puis appuyez sur Entrée.
- Si vous y êtes invité par le contrôle de compte d'utilisateur, cliquez sur Oui.

2. Accédez à la sous-clé.

- Accédez à : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais

3. Modifiez la clé et définissez la valeur.

- À l'intérieur de Calais, case activée si la clé DisableCapiOverrideForRSA existe
- Double-cliquez sur DisableCapiOverrideForRSA.
- Dans Date de la valeur, entrez : 0

Remarque : le paramètre de Registre DisableCapiOverrideForRSA n'est PAS ajouté par l'installation du système d'exploitation par défaut ou l'installation de Windows Mises à jour et doit être ajouté manuellement sur chaque appareil.

4. Fermez et redémarrez.

- Fermez l'Éditeur du Registre.
- Redémarrez l'ordinateur pour que les modifications prennent effet.

Plateformes affectées :

- Client : Windows 11, version 25H2 ; Windows 11, version 24H2 ; Windows 11, version 23H2 ; Windows 11, version 22H2 ; Windows 10, version 22H2
- Serveur : Windows Server 2025 ; Windows Server 23H2 ; Windows Server 2022 ; Windows Server 2019 ; Windows Server 2016 ; Windows Server 2012 R2

Retour au début

Novembre 2024

Windows Server 2022 et Server 2019 ont été mis à niveau de manière inattendue vers Windows Server 2025

Agrandir le tableau

Statut	Mise à jour d'origine	Historique
Résolution KB5082142	Non applicable	Résolu : 2026-04-14, 10:00 PT Ouvert : 2024-11-09, 12:16 PT

Windows Server 2025 est destiné à être proposé en tant que mise à niveau **facultative** dans les paramètres de **Windows Update** pour les appareils exécutant Windows Server 2019 et Windows Server 2022. Deux scénarios ont été observés dans certains environnements :

- Certains appareils ont été mis à niveau automatiquement vers Windows Server 2025 (KB5044284). Ce problème a été observé dans les environnements qui utilisent des produits tiers pour gérer la mise à jour des clients et des serveurs. Vérifiez si les logiciels de mise à jour tiers de votre environnement sont configurés pour ne pas déployer les mises à jour de fonctionnalités. Ce scénario a été atténué.

- Une mise à niveau vers Windows Server 2025 a été proposée via un message dans une bannière affichée sur la page **Windows Update** de l'appareil, sous **Paramètres**. Ce message est destiné aux organisations qui souhaitent exécuter une mise à niveau sur place. Ce scénario a déjà été résolu.

La mise à jour des fonctionnalités de Windows Server 2025 a été publiée en tant que mise à jour **facultative** sous la classification de mise à niveau : « DeploymentAction=OptionalInstallation ». Les métadonnées de mise à jour des fonctionnalités doivent être interprétées comme **facultatives** et non **recommandées** par les outils de gestion des correctifs.

Nous conseillons aux organisations d'utiliser les méthodes recommandées par Microsoft pour déployer les mises à jour des fonctionnalités de Windows Server.

Résolution : Ce problème est résolu et Microsoft a réactivé l'offre de mise à niveau via le panneau de configuration de **Windows Update** . Pour plus d'informations sur la mise à jour des fonctionnalités à partir de la boîte de dialogue de configuration de Windows Server, consultez Effectuer une mise à niveau sur place de Windows Server sur Microsoft Learn.

Plateformes affectées :

- Client : Aucun
- Serveur : Windows Server 2025 ; Windows Server 2022 ; Windows Server 2019

Retour au début

Signaler un problème avec les mises à jour Windows

Pour signaler un problème à Microsoft à tout moment, utilisez l'application Hub de commentaires . Pour plus d'informations, consultez Envoyer des commentaires à Microsoft avec l'application Hub de commentaires .

Besoin d'aide pour Windows Update ?

Recherchez, parcourez ou posez une question sur la communauté de Support Microsoft . Si vous êtes un professionnel de l'informatique soutenant une organisation, visitez l'état de publication de Windows sur le Centre d'administration Microsoft 365 pour plus de détails.

Pour obtenir de l'aide directe sur votre PC personnel, utilisez l'application Aide sur Windows ou contactez le Support Microsoft . Les organisations peuvent demander un support immédiat par le biais du Support pour les entreprises .

Afficher ce site dans votre langue

Ce site est disponible en 11 langues : anglais, chinois traditionnel, chinois simplifié, français (France), allemand, italien, japonais, coréen, portugais (Brésil), russe et espagnol (Espagne). Tout le texte s'affiche en anglais si la langue par défaut de votre navigateur n'est pas l'une des 11 langues prises en charge. Pour changer manuellement la langue d'affichage, faites défiler vers le bas de cette page, cliquez sur la langue actuelle affichée en bas à gauche de la page et sélectionnez l'une des 11 langues prises en charge dans la liste.

Dernière mise à jour : 16/10/2026

Planifier votre mise à niveau de Windows Server

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

Windows Server prend en charge plusieurs méthodes pour passer à une version plus récente, notamment la mise à niveau sur place, l'installation propre, la migration, la mise à niveau propagée du cluster et la conversion d'édition. Chaque méthode a des compromis différents pour les temps d'arrêt, la complexité et la configuration matérielle requise. La mise à niveau permet à vos serveurs de sécuriser, de prendre en charge et d'utiliser les dernières fonctionnalités et améliorations des performances.

Cet article explique les méthodes de mise à niveau disponibles, les chemins de mise à niveau sur place pris en charge par version et les restrictions qui s'appliquent.

Facteurs de choix d'une méthode de mise à niveau

La meilleure méthode dépend de votre environnement et de vos besoins. Tenez compte des facteurs suivants lors de la planification de votre mise à niveau :

- **Tolérance aux temps d'arrêt** : une mise à niveau sur place nécessite un redémarrage, mais vous conserve sur le même matériel. Une mise à niveau propagée de cluster maintient la disponibilité de la charge de travail tout au long du processus. Une installation ou une migration propre peut nécessiter davantage de temps d'arrêt, mais vous offre un nouvel environnement.
- **Contraintes matérielles** : si vous restez sur le même matériel, une mise à niveau sur place ou une installation propre est appropriée. Si vous passez à un nouveau matériel, la migration est le meilleur choix.
- **Rôles et fonctionnalités** : tous les rôles ne prennent pas en charge la mise à niveau sur place. Vérifiez le rôle et la matrice de migration des fonctionnalités pour vérifier la prise en charge de votre configuration.
- **Version gap** : À partir de Windows Server 2025, les systèmes non clusterisés peuvent effectuer une mise à niveau de jusqu'à quatre versions à la fois. Pour Windows Server 2022 et versions antérieures, les systèmes non cluster peuvent mettre à niveau jusqu'à deux versions à la fois. Les mises à niveau progressives des clusters ne peuvent

avancer que d'une version à la fois. Pour plus d'informations, consultez la table des chemins d'accès pris en charge .

- **Licences** : avant de procéder à la mise à niveau, vérifiez que vous disposez d'une clé de produit et d'une méthode d'activation valides pour la version cible. Contrairement à Windows client, chaque mise à niveau Windows Server nécessite une licence distincte.

méthodes de mise à niveau Windows Server

Utilisez le tableau suivant pour déterminer quelle méthode correspond à votre scénario.

> **Important**
>
> Sauvegardez toujours vos fichiers système et importants avant d'effectuer une mise à niveau sur place, une nouvelle installation ou une migration vers une version ultérieure de Windows Server.

Agrandir le tableau

Méthode	Qu'est-ce que cela fait ?	Quand l'utiliser ?	Plus d'informations
Mise à niveau sur place	Installe une version plus récente de Windows Server sur celle existante, en conservant vos paramètres, rôles serveur, fonctionnalités et données. Vous pouvez effectuer une mise à niveau sur place à l'aide d'un support d'installation ou la recevoir en tant que mise à jour de fonctionnalités via Windows Update.	Vous souhaitez obtenir le chemin le plus rapide vers une version plus récente sur le même matériel, et vos rôles et fonctionnalités prennent en charge la mise à niveau sur place.	Effectuer une mise à niveau sur place
Nouvelle installation	Installe Windows Server sur un nouveau serveur ou remplace le système d'exploitation existant.	Vous souhaitez un nouveau démarrage, votre matériel est nouveau ou une mise à niveau sur place n'est pas prise en charge pour votre configuration actuelle.	Installer Windows Server
Migration	Déplace des rôles ou des fonctionnalités d'un serveur source vers un autre serveur de destination exécutant Windows Server.	Vous passez au nouveau matériel, ou vous devez migrer un rôle ou une fonctionnalité à la fois	Mettre à niveau et migrer des rôles et des fonctionnalités

Méthode	Qu'est-ce que cela fait ?	Quand l'utiliser ?	Plus d'informations
		sans mettre à niveau le système d'exploitation sur place.	
Mise à niveau propagée du système d'exploitation de cluster	Met à niveau les systèmes d'exploitation de nœud de cluster un à la fois, sans arrêter les charges de travail Hyper-V ou Scale-Out File Server. Les clusters ne peuvent mettre à niveau qu'une seule version à la fois. Vous pouvez effectuer une mise à niveau propagée à l'aide d'un support d'installation ou la recevoir en tant que mise à jour de fonctionnalités via Windows Update. Pour les clusters de basculement s'exécutant sur Azure Local, utilisez le gestionnaire Lifecycle Manager (LCM) à la place.	Vous exécutez un cluster de basculement et devez maintenir la disponibilité pendant le processus de mise à niveau.	Mise à niveau propagée du système d'exploitation de cluster
Conversion de licence	Convertit une édition de Windows Server en une autre édition de la même version à l'aide d'une commande et d'une clé de produit (par exemple, Standard en Centre de données).	Vous devez modifier votre Windows Server édition ou basculer entre les licences de vente au détail, sous licence en volume et OEM.	Convertir Windows Server éditions et types de licences

Chemins de mise à niveau sur place pris en charge par version

Effectuez une mise à niveau vers la dernière version de Windows Server pour obtenir les fonctionnalités les plus récentes, les mises à jour de sécurité et les meilleures performances.

À compter de Windows Server 2025, les systèmes non cluster peuvent mettre à niveau jusqu'à quatre versions à la fois. Vous pouvez effectuer une mise à niveau directement vers Windows Server 2025 à partir de Windows Server 2012 R2 et versions ultérieures. Pour Windows Server 2022 et versions antérieures, les systèmes non cluster peuvent mettre à niveau jusqu'à deux versions à la fois. Si vous utilisez une mise à niveau propagée du système d'exploitation de cluster, vous ne pouvez mettre à niveau qu'une seule version à la fois.

Pour obtenir des instructions pas à pas sur la façon d'effectuer une mise à niveau sur place, consultez Performer une mise à niveau sur place de Windows Server.

Sélectionnez l'onglet de votre méthode de mise à niveau pour afficher les chemins d'accès pris en charge :

Support d'installation

Agrandir le tableau

Mise à niveau depuis / vers	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2025
Windows Server 2012	Oui	Oui	Non	Non	Non
Windows Server 2012 R2	Non	Oui	Oui	Non	Oui
Windows Server 2016	Non	Non	Oui	Oui	Oui
Windows Server 2019	Non	Non	Non	Oui	Oui
Windows Server 2022	Non	Non	Non	Non	Oui
Windows Server 2025	Non	Non	Non	Non	Oui

Restrictions de mise à niveau pour les versions sous licence de Windows Server

Les restrictions suivantes s'appliquent aux mises à niveau sur place où Windows Server est déjà sous licence (et non une version d'évaluation) :

- Les mises à niveau d'architectures 32 bits vers des architectures 64 bits ne sont pas prises en charge. Toutes les versions depuis Windows Server 2008 R2 sont 64 bits uniquement.
- Les mises à niveau d'une langue vers une autre ne sont pas prises en charge.
- Si le serveur est un contrôleur de domaine Active Directory, vous ne pouvez pas le convertir en version commerciale. Consultez Mettre à jour les contrôleurs de domaine vers Windows Server pour obtenir des informations importantes.
- Les mises à niveau des versions préliminaires (préversions) de Windows Server ne sont pas prises en charge. Effectuez une installation propre à la place.

- Le passage d'une installation Server Core à un serveur avec une installation d'expérience utilisateur (ou vice versa) pendant une mise à niveau sur place n'est pas pris en charge.
- Les mises à niveau d'une installation de Windows Server précédente vers une copie d'évaluation ne sont pas prises en charge. Installez les versions d'évaluation en tant qu'installations propres.
- Par défaut, une mise à niveau conserve l'édition existante. Par exemple, les mises à niveau Standard vers Standard et Datacenter vers Datacenter.
- Vous pouvez passer de Standard à Datacenter ou Datacenter : Azure Edition, ou de Datacenter à Datacenter : Azure Edition, lors d'une mise à niveau. Vous ne pouvez pas passer d'un centre de données à un centre de données standard ou d'un centre de données : Azure Edition vers Standard ou Datacenter.
- Si votre serveur utilise l'association de cartes réseau, désactivez l'association de cartes réseau avant la mise à niveau sur place. Vous pouvez le réactiver lorsque la mise à niveau sur place est terminée. Pour plus d'informations, consultez l'aperçu du teaming de cartes réseau.
- Les mises à niveau locales sur Windows Server configurées pour démarrer à partir d'un fichier VHD ne sont pas prises en charge.
- Les mises à niveau directement à partir des éditions de Windows Storage Server ne sont pas prises en charge.
- Certains fournisseurs de cloud public et privé prennent en charge les mises à niveau sur place. Pour plus d'informations, contactez votre fournisseur de cloud.

Versions de Windows Server de fin de prise en charge

La prise en charge de Windows Server 2012 et Windows Server 2012 R2 a pris fin le 10 octobre 2023. Les mises à jour de sécurité étendues (ESU) sont disponibles, avec une option permettant de migrer vos serveurs locaux vers Azure, où vous pouvez continuer à les exécuter sur des machines virtuelles. Pour plus d'informations, consultez la vue d'ensemble des mises à jour de sécurité étendues.

Contenu connexe

- Performer une mise à niveau sur place de Windows Server
- Convertir Windows Server éditions et types de licences
- Upgrader et migrer des rôles et des fonctionnalités dans Windows Server
- Mise à niveau propagée du système d'exploitation de cluster
- Vue d'ensemble de la mise à jour adaptée aux clusters

Last updated on 15/04/2026

Serveur Core vs Serveur avec Expérience de Bureau options d'installation

16/08/2025

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

Lorsque vous installez Windows Server à l'aide de l'assistant d'installation, vous pouvez choisir entre Server Core ou Serveur avec l'option d'installation Expérience de Bureau. Avec Server Core, l'interface utilisateur graphique standard (Expérience de bureau) n'est pas installée ; vous gérez le serveur à partir de la ligne de commande à l'aide de PowerShell, de l'outil de configuration du serveur (SConfig) ou des méthodes distantes. Server with Desktop Experience installe l'interface utilisateur graphique standard et tous les outils, y compris les fonctionnalités de l'expérience client.

Nous vous recommandons de choisir l'option d'installation server Core, sauf si vous avez besoin d'éléments d'interface utilisateur supplémentaires et d'outils de gestion graphique inclus dans l'option d'installation du serveur avec expérience utilisateur.

L'Assistant Installation répertorie les options d'installation. Dans cette liste, les éditions sans **Expérience utilisateur** sont les options d'installation server Core :

- Windows Server Standard
- Windows Server Standard avec expérience de bureau
- Windows Server Datacenter
- Windows Server Datacenter avec expérience de bureau

> **Notes**
>
> Contrairement à certaines versions précédentes de Windows Server, vous ne pouvez pas effectuer de conversion entre Server Core et Server avec Expérience de bureau après l'installation. Vous devrez effectuer une installation propre si vous installez ultérieurement décider d'utiliser une autre option.

Differences

Il existe quelques différences clés entre Server Core et Server avec Expérience de bureau :

Agrandir le tableau

Component	Server Core	Server avec Expérience utilisateur
Interface utilisateur	Minimal, piloté par la ligne de commande (PowerShell, SConfig, cmd)	Interface utilisateur graphique Windows standard
Espace disque	Exigences plus petites	Exigences plus importantes
Installer, configurer, désinstaller des rôles serveur localement	PowerShell	Gestionnaire de serveur ou PowerShell
Rôles et fonctionnalités	Certains rôles et fonctionnalités ne sont pas disponibles. Pour plus d'informations, consultez Rôles, Services de rôle et fonctionnalités non dans Windows Server - Server Core. Certaines des fonctionnalités de Server avec Expérience de bureau pour la compatibilité des applications peuvent être installées avec la fonctionnalité de compatibilité des applications à la demande (FOD).	Tous les rôles et fonctionnalités sont disponibles, y compris ceux pour la compatibilité des applications.
Gestion à distance	Oui, vous pouvez gérer à distance à l'aide d'outils GUI, tels que Windows Admin Center, les outils d'administration de serveur distant (RSAT) ou le Gestionnaire de serveur, ou par PowerShell.	Oui, vous pouvez gérer à distance à l'aide d'outils GUI, tels que Windows Admin Center, les outils d'administration de serveur distant (RSAT) ou le Gestionnaire de serveur, ou par PowerShell.
Surface d'attaque potentielle	Surface d'attaque considérablement réduite	Aucune réduction
Console MMC (Microsoft Management Console)	Non installé : peut être installé avec la fonctionnalité de compatibilité des applications à la demande (FOD).	Installed

> **Notes**
>
> Pour RSAT, vous devez utiliser la version incluse dans Windows 10 ou version ultérieure.

Canaux de maintenance Windows Server

16/08/2025

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

À compter de septembre 2023, Windows Server dispose de deux canaux de mise en production principaux disponibles, le canal de maintenance Long-Term et le canal annuel. Le canal de maintenance Long-Term (LTSC) offre une option à long terme axée sur la fourniture d'un cycle de vie traditionnel des mises à jour de qualité et de sécurité, tandis que le canal annuel (AC) fournit des versions plus fréquentes. Les versions plus fréquentes de l'AC entraînent une innovation plus rapide, en se concentrant sur les conteneurs et les microservices.

Canal de maintenance à long terme (LTSC)

Avec le canal de maintenance Long-Term, une nouvelle version majeure de Windows Server est généralement publiée toutes les 2 à 3 ans. Les utilisateurs ont droit à cinq ans de support standard et cinq ans de support étendu. Ce canal fournit aux systèmes une longue option de maintenance et une cohérence, et peut être installé avec Server Core ou Server avec les options d'installation de l'expérience utilisateur.

Canal annuel (AC)

Le canal annuel Windows Server pour conteneurs est un système d'exploitation qui héberge des conteneurs Windows Server. Le canal annuel permet aux clients qui innovent rapidement de tirer parti des nouvelles fonctionnalités du système d'exploitation à un rythme plus rapide, axés sur les conteneurs et les microservices. Pour en savoir plus sur le canal annuel Windows Server pour conteneurs, consultez notre annonce TechCommunity.

Chaque version de ce canal est prise en charge pendant 24 mois à partir de la version initiale. Ce canal ne peut être installé qu'avec l'option d'installation server Core. Le canal annuel est disponible pour les clients sous licence en volume avec Software Assurance et les programmes de fidélité tels que les abonnements Visual Studio.

Une version de canal annuel n'est pas une mise à jour, c'est la prochaine version de Windows Server dans le canal annuel. Pour passer à une version de canal annuel, vous devez effectuer une nouvelle installation.

Les versions de Windows Server dans le canal annuel se produisent généralement toutes les 12 mois. Le cycle de vie de support de 24 mois pour chaque version est de 18 mois de support

standard, plus 6 mois de support étendu. Pour en savoir plus sur le cycle de vie, consultez le cycle de vie de Windows Server 2022. Chaque version est nommée en fonction du cycle de publication ; par exemple, **la version 23H2** est une version au deuxième semestre de l'année 2023.

Principales différences

Le tableau suivant résume les principales différences entre les canaux :

Agrandir le tableau

Description	Canal de maintenance à long terme	Canal annuel
Scénarios recommandés	Serveurs de fichiers à usage général, charges de travail Microsoft et non-Microsoft, applications traditionnelles, rôles d'infrastructure, centre de données défini par logiciel et infrastructure hyperconvergée	Applications conteneurisées s'exécutant sur des hôtes de conteneur bénéficiant d'une innovation plus rapide
Nouvelles versions	En général, 2 à 3 ans	En général, 12 mois
Support	5 ans de support standard plus 5 ans de support étendu	18 mois de support standard, plus 6 mois de support étendu
Activation	Toutes les clés d'activation de Windows Server	Clés d'activation de Windows Server Datacenter
Licensing	Tous les programmes de licence	Clients Software Assurance uniquement
Obtenir un média	Tous les canaux de distribution	Centre de gestion des licences en volume (VLSC) et abonnements Visual Studio uniquement
Options d'installation	Server Core et Serveur avec Expérience utilisateur	Server Core pour un hôte de conteneur uniquement

Compatibilité des appareils

La configuration matérielle minimale requise pour exécuter les versions du canal annuel est la même que la version la plus récente du canal de maintenance de Windows Server Long-Term. La plupart des pilotes matériels continuent d'opérer dans ces versions.

Servicing

Le canal de maintenance Long-Term et les versions annuelles du canal sont pris en charge avec les mises à jour de sécurité et les mises à jour non de sécurité jusqu'aux dates répertoriées dans les pages de cycle de vie Microsoft . La différence est la durée pendant laquelle la version est prise en charge, comme décrit dans la section Canal annuel (AC) de cet article.

Outils de maintenance

Il existe de nombreux outils avec lesquels vous pouvez traiter Windows Server. Chaque option a ses avantages et ses inconvénients, allant des fonctionnalités et du contrôle aux faibles exigences en termes d'administration en passant par la simplicité. Voici des exemples d'outils de maintenance disponibles pour gérer les mises à jour :

- **Windows Update (autonome)** : cette option est disponible uniquement pour les serveurs connectés à Internet et pour utilisant Windows Update.
- **Windows Server Update Services (WSUS)** offre un contrôle étendu sur les mises à jour du client Windows Server et Windows et est disponible en mode natif dans le système d'exploitation Windows Server. Vous pouvez différer les mises à jour, ajouter une couche d'approbation et choisir de les déployer sur des ordinateurs ou groupes d'ordinateurs spécifiques chaque fois qu'ils sont prêts.
- **Microsoft Endpoint Configuration Manager** offre le meilleur contrôle sur la maintenance. Vous pouvez différer les mises à jour, les approuver et avoir plusieurs options pour cibler les déploiements et gérer l'utilisation de la bande passante et les temps de déploiement.

Vous pouvez continuer à utiliser le même processus pour les versions annuelles du canal ; par exemple, si vous utilisez déjà Configuration Manager pour gérer les mises à jour, vous pouvez continuer à l'utiliser. De même, si vous utilisez WSUS, vous pouvez continuer à l'utiliser.

Où obtenir le canal annuel

Vous pouvez obtenir des versions annuelles du canal à partir des emplacements suivants :

- Centre de gestion des licences en volume (VLSC) : les clients sous licence en volume avec Software Assurance peuvent obtenir cette version en accédant au Centre de gestion des licences en volume et en sélectionnant **Se connecter**. Enfin, sélectionnez **Téléchargements et clés**, recherchez canal annuel, puis téléchargez le média.

- Abonnements Visual Studio : Les abonnés Visual Studio peuvent obtenir des versions de canal annuelles en les téléchargeant à partir de la page de téléchargement de l'Abonné Visual Studio. Si vous n'êtes pas déjà abonné, accédez à abonnements Visual Studio pour vous inscrire, puis visitez la page Téléchargements Abonné Visual Studio. Les

versions obtenues via les abonnements Visual Studio sont destinées au développement et aux tests uniquement.

Activation des versions annuelles du canal

Vous devez activer votre installation à l'aide de vos clés d'activation obtenues à partir de la VLSC. Si vous utilisez KMS, les versions de canal annuel utilisent le même fichier CSVLK que celui de la dernière version LTSC avant leur publication. Par exemple, un canal annuel publié avec ou après Windows Server 2022 utiliserait le CSVLK de Windows Server 2022. Pour plus d'informations, consultez les clés de configuration du client KMS.

Comment savoir si un serveur exécute une version LTSC ou AC

Les versions du canal de maintenance à long terme peuvent être publiées en même temps qu'une nouvelle version du canal annuel. Pour déterminer si un serveur exécute la version du canal annuel, vous devez examiner la version du système d'exploitation. Le nom du produit ne reflète pas le canal de maintenance. Pour déterminer si un serveur exécute une version LTSC ou AC, vous pouvez exécuter la commande PowerShell Get-ComputerInfo . L'exemple suivant est un ordinateur exécutant Windows Server 2022 Datacenter Edition (LTSC).

Pour déterminer la version du système d'exploitation, exécutez la commande suivante :

PowerShell

```
Get-ComputerInfo  | fl WindowsProductName,OSDisplayVersion
```

Voici un exemple de sortie d'un ordinateur exécutant Windows Server LTSC.

Sortie

```
WindowsProductName : Windows Server 2022 Datacenter
OSDisplayVersion   : 21H2
```

Voici un exemple de sortie d'un ordinateur exécutant le canal annuel Windows Server pour conteneurs.

Sortie

```
WindowsProductName : Windows Server 2022 Datacenter
OSDisplayVersion   : 23H2
```

> **Conseil**
>
> `OSDisplayVersion` s'applique uniquement à Windows Server 2022 et versions ultérieures. Les versions annuelles du canal ne s'appliquent pas à Windows Server 2019 et versions antérieures. Si vous exécutez Windows Server 2019 ou une version antérieure, vous exécutez une version LTSC.

Le tableau suivant répertorie les versions windows Server LTSC et AC et leurs versions de système d'exploitation correspondantes.

Agrandir le tableau

Channel	Version d'affichage du système d'exploitation
LTSC	21H2
Canal annuel	23H2

L'aide est destinée à aider à identifier et différencier LTSC et AC à des fins de cycle de vie et d'inventaire général uniquement. Elle n'est pas destinée à la compatibilité des applications ou à représenter une surface d'API spécifique. Les développeurs d'applications doivent faire référence à d'autres conseils pour garantir la compatibilité. Les composants, LES API et les fonctionnalités peuvent être ajoutés pendant le cycle de vie d'un système ou peuvent ne pas encore être disponibles. Pour en savoir plus sur l'utilisation par programmation de la détermination de la version, consultez Version du système d'exploitation.

Compatibilité des applications serveur Microsoft pour Windows Server

28/07/2025

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

Nous comprenons que la compatibilité des applications est l'une des principales raisons pour lesquelles les clients choisissent Windows Server. Tout au long du cycle de développement de Windows Server, Microsoft teste régulièrement une grande suite d'applications Microsoft et non-Microsoft pour garantir que nos produits sont compatibles avec autant d'applications que possible. Ces tests couvrent un large éventail d'applications d'entreprise non-Microsoft, notamment les outils de développement, les outils graphiques, les outils de sécurité, les suites de bureau métier, la gestion du stockage, l'antivirus, la sauvegarde ou la récupération et les utilitaires.

Le tableau suivant répertorie les applications serveur Microsoft qui prennent en charge l'installation et les fonctionnalités sur Windows Server. Ces informations sont destinées à une référence rapide et ne sont pas destinées à remplacer les spécifications, exigences, annonces ou communications générales de chaque application serveur individuelle. Reportez-vous à la documentation officielle de chaque produit pour comprendre pleinement la compatibilité et les options.

> **Conseil**
>
> Si vous êtes un partenaire fournisseur de logiciels qui recherche plus d'informations sur la compatibilité de Windows Server avec les applications non-Microsoft, visitez le portail Certification des applications commerciales.

Agrandir le tableau

Produit	Pris en charge sur Server Core	Pris en charge sur Server avec Expérience utilisateur	Lien web du produit
Configuration Manager (version 2409)	✅[2]	✅	Prise en charge pour Windows Server 2025
Serveur Exchange	✅	✅	Matrice de supportabilité Exchange Server

Produit	Pris en charge sur Server Core	Pris en charge sur Server avec Expérience utilisateur	Lien web du produit
Les applications Microsoft 365	❌	✅	matrice de prise en charge de la configuration de Windows et d'Office
Édition Abonnement de Project Server	✅	✅	Exigences logicielles pour Project Server Subscription Edition
SharePoint Server Édition sous abonnement	✅	✅	configuration système requise pour l'édition d'abonnement SharePoint Server
SQL Server 2019	✅[1]	✅	configuration matérielle et logicielle requise pour l'installation de SQL Server 2019
SQL Server 2022	✅[1]	✅	configuration matérielle et logicielle requise pour l'installation de SQL Server 2022
Gestionnaire de Protection des Données System Center	✅[1]	✅	Préparation de votre environnement pour System Center Data Protection Manager
Gestionnaire des Opérations de System Center	✅[1]	✅	configuration système requise pour System Center Operations Manager
System Center Virtual Machine Manager	✅[1]	✅	Configuration système requise pour System Center Virtual Machine Manager

1. Peut présenter des limitations ou nécessiter la fonctionnalité à la demande de compatibilité des applications Server Core. Pour plus d'informations, consultez la documentation spécifique sur le produit ou la fonctionnalité à la demande.

2. Oui, en tant que client managé et point de distribution, mais pas en tant que serveur de site.

Azure Hybrid Benefit pour Windows Server

03/09/2025

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

Azure Hybrid Benefit permet aux clients commerciaux d'utiliser leurs licences locales éligibles pour obtenir des machines virtuelles Windows sur Azure à un coût réduit. Cet article se concentre sur les avantages de l'utilisation de licences Windows Server éligibles pour réaliser des économies pour les machines virtuelles Windows Server dans Azure, Azure Local et Azure Kubernetes Service (AKS) déploiements hybrides.

Pour d'autres avantages hybrides Azure (par exemple, Microsoft SQL Server), consultez Azure Hybrid Benefit.

Qu'est-ce qui vous qualifie pour Azure Hybrid Benefit ?

Pour être éligible à Azure Hybrid Benefit pour Windows Server, vous devez disposer de licences de base locales pour Windows Server à partir d'un programme applicable avec la Software Assurance active ou des licences d'abonnement éligibles. La Software Assurance et les licences d'abonnement éligibles sont uniquement disponibles dans le cadre de certains contrats de licence commerciale. Pour en savoir plus sur les licences commerciales, consultez Ressources de licence Microsoft. Pour en savoir plus sur les licences principales Windows Server, consultez Licences de produit Windows Server.

> **Important**
>
> - Les charges de travail utilisant Azure Hybrid Benefit ne peuvent s'exécuter que pendant la durée de Software Assurance ou des licences d'abonnement. Quand la Software Assurance ou une licence d'abonnement approche de sa date d'expiration, vous devez renouveler votre contrat avec la Software Assurance ou une licence d'abonnement, désactiver la fonctionnalité de l'avantage Hybrid Benefit ou déprovisionner les charges de travail qui utilisent Azure Hybrid Benefit.
> - Les conditions générales des produits Microsoft pour votre programme prévalent sur cet article. Pour plus d'informations, consultez Conditions générales des produits Microsoft Azure et sélectionnez votre programme pour les afficher.

Qu’est-ce qui est inclus dans Azure Hybrid Benefit ?

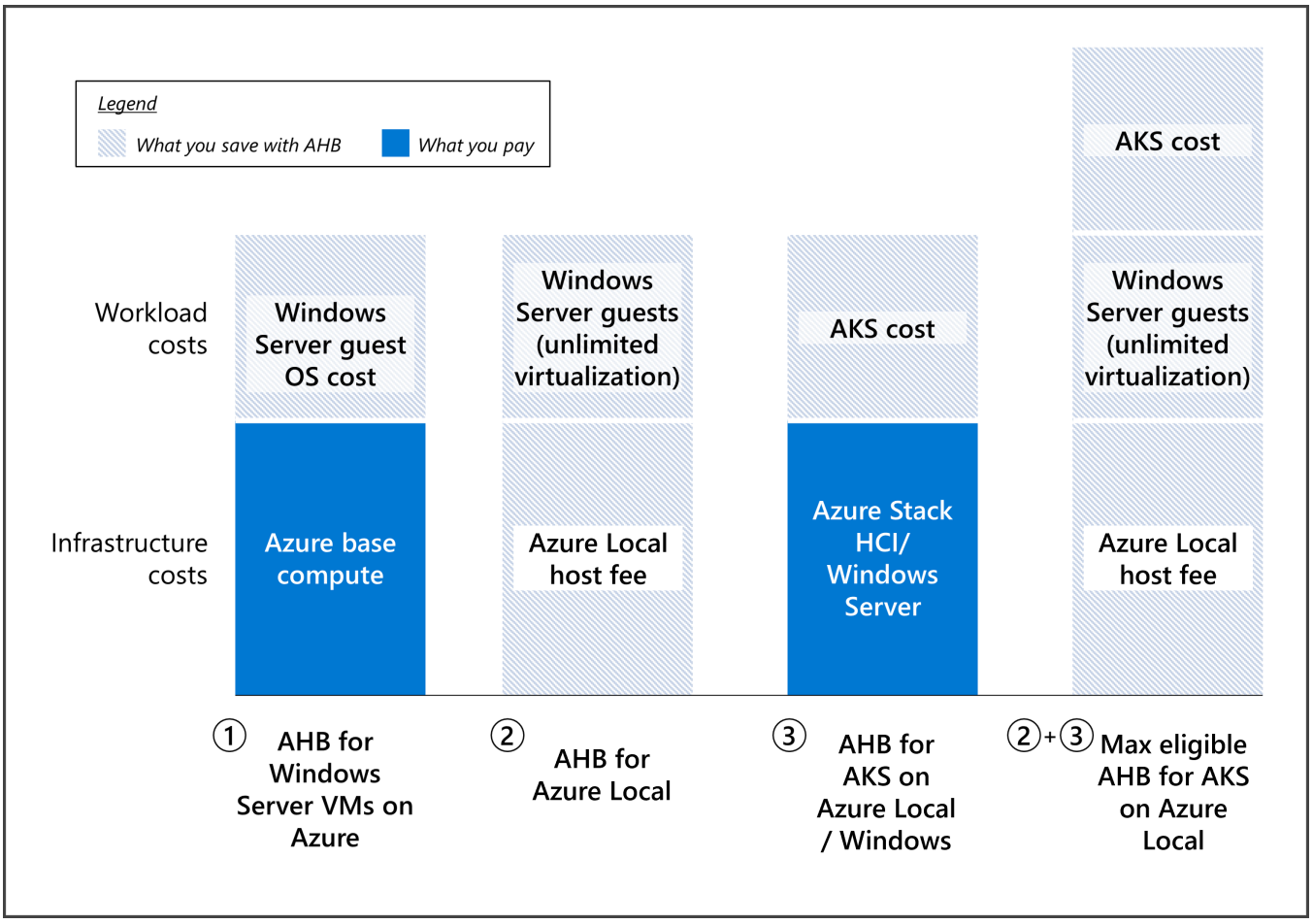
Les clients disposant d'une licence Windows Server dans le cadre d'un programme applicable avec une Software Assurance active ou des licences d'abonnement éligibles peuvent utiliser Azure Hybrid Benefit pour réduire davantage les coûts dans le cloud, les centres de données et les emplacements périphériques.

Azure Hybrid Benefit comprend les économies suivantes :

- **Machines virtuelles Windows Server sur Azure :** la licence pour Windows Server est couverte par Azure Hybrid Benefit. Vous ne devez donc payer que le taux de calcul de base de la machine virtuelle. Le taux de calcul de base est égal au taux Linux pour les machines virtuelles.

- **Azure Local :** Les frais d’hôte local Azure et les frais d’abonnement Windows Server sont annulés avec Azure Hybrid Benefit. Autrement dit, des droits de virtualisation illimités sont fournis sans coût supplémentaire. Vous payez toujours d’autres coûts associés à Azure Local (par exemple, matériel géré par le client, services Azure et charges de travail).

- **AKS :** Exécutez AKS sur Windows Server et Azure Local sans frais supplémentaires. Vous payez toujours pour l’infrastructure hôte sous-jacente et toutes les licences pour les conteneurs Windows, sauf si vous êtes également éligible à Azure Hybrid Benefit pour Azure Local. Avec Azure Hybrid Benefit pour Azure Local, vous pouvez renoncer aux frais pour l’hôte local Azure et l’abonnement Windows Server.



Tarification pour Azure Hybrid Benefit

Pour évaluer vos économies potentielles, vous pouvez utiliser ces ressources :

- **Machines virtuelles Windows sur Azure** :tarification des machines virtuelles Windows. Utilisez la calculatrice de prix Azure pour estimer les économies de coûts, ou comparer la tarification des machines virtuelles Windows avec et sans Azure Hybrid Benefit.
- **Tarification d'Azure Local** :Azure Local.
- **Azure Kubernetes Service (AKS)** :Tarification locale Azure pour AKS.

Obtenir Azure Hybrid Benefit

Sélectionnez l'onglet pour votre scénario.

Azure

Suivez les instructions de cette section pour obtenir et gérer Azure Hybrid Benefit pour vos machines virtuelles Windows dans Azure.

Conditions préalables aux licences

Pour bénéficier d'Azure Hybrid Benefit pour les machines virtuelles Windows dans Azure, vous devez respecter les conditions préalables de licence suivantes.

Types de licence

- Windows Server Standard Edition avec Software Assurance active ou abonnement.
- Windows Server Datacenter Edition avec Software Assurance ou abonnement.

Nombre de licences

Vous avez besoin d'un minimum de 8 licences par cœur (édition Datacenter ou Standard) par machine virtuelle. Par exemple, 8 licences par cœur sont toujours requises si vous exécutez une instance de 4 cœurs. Vous pouvez également exécuter des instances supérieures à 8 cœurs en allouant des licences égales à la taille de cœur de l'instance. Par exemple, 12 licences par cœur sont requises pour une instance de 12 cœurs. Pour les clients disposant de licences processeur, chaque licence de processeur équivaut à 16 licences par cœur.

Allocation de migration Azure

- **Édition Windows Server Standard :** les licences doivent être utilisées localement ou dans Azure, mais pas en même temps. La seule exception est lors d'une utilisation ponctuelle, pendant au maximum 180 jours, pour vous permettre de migrer les mêmes charges de travail vers Azure.
- **Édition Windows Server Datacenter :** Pour les licences de machine virtuelle, lors de la migration de charges de travail vers Azure, les licences autorisent l'utilisation simultanée locale et dans Azure indéfiniment. Pour les licences d'hôte dédié, lors de la migration de charges de travail vers Azure, les licences autorisent l'utilisation simultanée locale et dans Azure pendant une période de 180 jours à partir de laquelle les licences sont allouées à Azure.

Virtualisation illimitée

Les droits de virtualisation illimités font référence au droit d'utiliser n'importe quel nombre de machines virtuelles Windows Server sur un hôte.

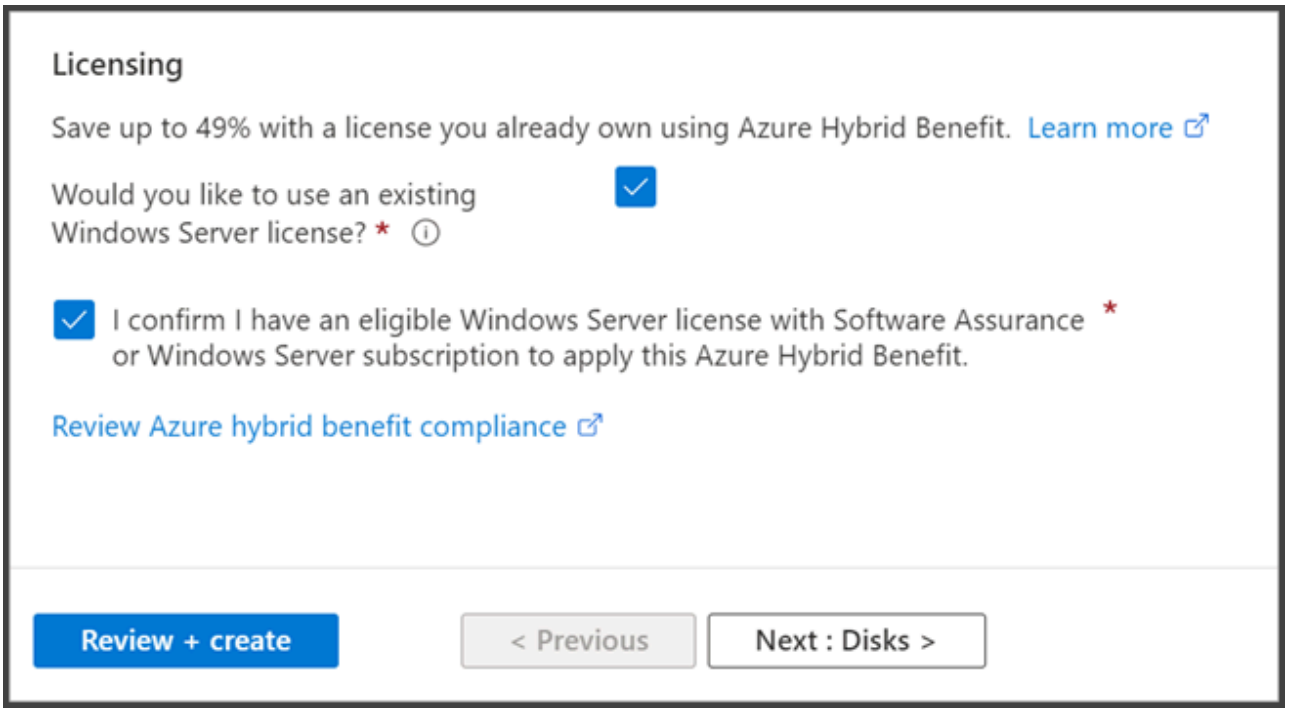
- **Édition Windows Server Datacenter :** Vous pouvez utiliser n'importe quel nombre de machines virtuelles Windows Server sur un hôte dédié Azure si vous allouez des

licences Windows Server Datacenter avec l'assurance logicielle active ou l'abonnement pour tous les cœurs physiques disponibles sur ce serveur Azure.

- **Édition Windows Server Standard :** les droits de virtualisation illimités ne sont pas disponibles.

Application d'Azure Hybrid Benefit aux machines virtuelles Windows dans Azure

Pour savoir comment déployer des machines virtuelles Windows Server dans Azure avec Azure Hybrid Benefit, suivez les étapes décrites dans Explorer Azure Hybrid Benefit pour les machines virtuelles Windows. L'une des façons d'activer Azure Hybrid Benefit pour une machine virtuelle Windows Server consiste à cocher la case sous **Licences** lors de la création de la machine virtuelle, comme illustré dans la capture d'écran suivante.



Comment rester en conformité

Si vous appliquez Azure Hybrid Benefit à vos machines virtuelles Windows Server, vérifiez le nombre de licences éligibles et la période de couverture de Software Assurance (ou de l'abonnement) avant d'activer cet avantage. Suivez les instructions précédentes pour veiller à déployer le nombre correct de machines virtuelles Windows Server avec cet avantage.

Si vous avez déjà des machines virtuelles Windows Server en cours d'exécution avec Azure Hybrid Benefit, faites l'inventaire pour connaître le nombre d'unités en cours d'exécution et comparez-le à vos licences Software Assurance ou d'abonnement. Vous pouvez

contacter votre spécialiste des licences Microsoft pour valider la situation de vos licences Software Assurance.

Pour afficher et compter toutes les machines virtuelles déployées avec Azure Hybrid Benefit dans un abonnement Azure, répertoriez toutes les machines virtuelles et groupes de machines virtuelles identiques.

Vous pouvez aussi regarder votre facture Microsoft Azure pour déterminer le nombre de machines virtuelles exécutées avec Azure Hybrid Benefit pour Windows Server. Vous trouverez des informations sur le nombre d'instances avec l'avantage sous **Informations supplémentaires** :

JSON


```
"
{"ImageType":"WindowsServerBYOL","ServiceType":"Standard_A1","VMName":"","Usag
eType":"ComputeHR"}"
```


La facturation n'est pas appliquée en temps réel. Attendez-vous à un délai de plusieurs heures après l'activation d'une machine virtuelle Windows Server avec Azure Hybrid Benefit avant que la machine virtuelle ne s'affiche sur votre facture.

Pour obtenir une vue complète de votre position de licence, effectuez un inventaire dans chacun de vos abonnements Azure. Vérifiez que vous disposez d'une licence complète pour les machines virtuelles Windows Server s'exécutant avec Azure Hybrid Benefit. Les utilisateurs n'ont pas besoin d'effectuer d'autres actions.

Effectuez régulièrement un inventaire pour vous assurer que vous utilisez tous les avantages de licence auxquels vous avez droit. Les inventaires réguliers peuvent vous aider à réduire les coûts et à vous assurer que vous disposez toujours de suffisamment de licences pour couvrir les machines virtuelles Windows Server que vous avez déployées avec Azure Hybrid Benefit.

Si vous n'avez pas suffisamment de licences Windows Server éligibles pour vos machines virtuelles déployées, vous avez trois options :

- Acheter des licences Windows Server supplémentaires couvertes par Software Assurance ou un abonnement via un contrat de licence commercial.
- Désactiver Azure Hybrid Benefit pour certaines de vos machines virtuelles et les acheter à des tarifs horaires Azure réguliers.
- Libérer certaines machines virtuelles.

ⓘ **Notes**

Microsoft se réserve le droit d'auditer les clients à tout moment pour vérifier son éligibilité à l'utilisation d'Azure Hybrid Benefit.

FAQ : Azure Hybrid Benefit

Quelles régions sont éligibles pour Azure Hybrid Benefit ?

Azure Hybrid Benefit est disponible dans toutes les régions Azure et dans les clouds souverains.

Qu'advient-il de mes avantages si ma Software Assurance ou mon abonnement expire ?

Pour utiliser ces avantages, votre Software Assurance ou votre abonnement éligible doivent être actifs. Si vous choisissez de ne pas renouveler votre Software Assurance ou votre abonnement à son expiration, vous devez supprimer vos avantages de vos ressources dans le Portail Azure.

Qu'est-ce que Software Assurance ?

La Software Assurance est un programme complet de licence en volume. La Software Assurance, disponible uniquement par le biais de licences en volume, est achetée lorsque vous souscrivez ou renouvelez un contrat de licence en volume. Elle est incluse avec certains contrats et est un achat facultatif avec d'autres. Les avantages de la Software Assurance incluent les nouveaux droits de version de produit, le support, les droits de mobilité de licence ainsi qu'un ensemble unique de technologies et de services afin d'optimiser vos investissements informatiques.

Pour plus d'informations sur la gestion des licences en volume, consultez Licences Microsoft. Pour en savoir plus sur les avantages de la Software Assurance et sur la façon dont chaque avantage peut vous aider à répondre à vos besoins métier, consultez Avantages de la Software Assurance.

Qu'est-ce qu'une licence d'abonnement ?

Les licences d'abonnement sont des licences permettant d'exécuter le logiciel uniquement pendant la durée de l'abonnement. Les licences d'abonnement n'incluent pas de droits perpétuels pour exécuter le logiciel.

Comment les clients peuvent-ils obtenir Software Assurance ?

Vous pouvez acheter Software Assurance par le biais de licences en volume. Vos avantages de la Software Assurance sont activés dans le Centre de gestion des licences en volume (VLSC). Si votre organisation dispose d'un Contrat de produits et de services Microsoft (MPSA), le Centre d'affaires est votre destination pour faciliter la gestion de vos avantages Software Assurance.

Voir aussi

- Page produit Azure Hybrid Benefit
- Explorer Azure Hybrid Benefit pour les machines virtuelles Windows
- Azure Hybrid Benefit pour Azure Stack HCI

Vue d’ensemble des mises à jour de sécurité étendues pour Windows Server

16/08/2025S’applique à: ✅ Windows Server 2012, ✅ Windows Server 2012 R2

Le programme de mise à jour de sécurité étendue (ESU) est une option de dernier recours pour les clients qui ont besoin d’exécuter certains produits Microsoft hérités après la fin de la prise en charge. Le canal de maintenance à long terme Windows Server (LTSC) a un minimum de 10 ans de support : cinq ans pour le support standard et cinq ans pour le support étendu, qui inclut des mises à jour de sécurité régulières.

Toutefois, une fois que les produits atteignent la fin du support, cela signifie également la fin des mises à jour et des bulletins de sécurité. Ce scénario peut entraîner des problèmes de sécurité ou de conformité et mettre en danger les applications métier. Microsoft vous recommande de mettre à niveau vers la version actuelle de Windows Server pour la sécurité, les performances et l’innovation les plus avancées.

La prise en charge étendue de Windows Server 2012 et Windows Server 2012 R2 a pris fin le 10 octobre 2023.

> **Conseil**
>
> Vous trouverez des informations sur les dates de support du **cycle de vie Microsoft**.

Que sont les correctifs de sécurité étendus ?

Les mises à jour de sécurité étendues pour Windows Server incluent les mises à jour de sécurité et les bulletins évalués *critiques* et *importants* pendant une période maximale à partir de la fin de la prise en charge étendue, en fonction de la version. Ils sont disponibles gratuitement pour les serveurs hébergés dans Azure et disponibles pour l’achat de serveurs non hébergés dans Azure. Les mises à jour de sécurité étendues n’incluent pas de nouvelles fonctionnalités, des correctifs logiciels non sécurisés demandés par le client ou des demandes de modification de conception. Pour plus d’informations, consultez faq sur le cycle de vie - Mises à jour de sécurité étendues.

Avec les mises à jour de sécurité étendues, les différentes phases de ces versions de Windows Server sont les suivantes :



Si vous n'avez pas encore mis à niveau vos serveurs, vous pouvez effectuer les opérations suivantes pour protéger vos applications et vos données pendant la transition :

- Migrez les charges de travail Windows Server existantes affectées as-is vers des machines virtuelles Azure. La migration vers Azure fournit automatiquement des mises à jour de sécurité étendues pour la période définie. Il n'existe aucun frais supplémentaire pour les mises à jour de sécurité étendues en plus du coût d'une machine virtuelle Azure, et vous n'avez pas besoin d'effectuer d'autres configurations.
- Achetez un abonnement de mise à jour de sécurité étendue pour vos serveurs et restez protégé jusqu'à ce que vous soyez prêt à effectuer une mise à niveau vers une version plus récente de Windows Server. Lorsque vous disposez d'un abonnement de mise à jour de sécurité étendue, Microsoft fournit des mises à jour pour la période définie. Une fois que vous avez acheté un abonnement, vous devez obtenir une clé de produit et l'installer sur chaque serveur applicable. Pour plus d'informations, consultez Comment obtenir les mises à jour de sécurité étendues.

Le tableau suivant répertorie la durée de mise à jour de sécurité étendue pour chaque version de Windows Server.

Agrandir le tableau

Version du produit	Hosted	Durée de l'ESU	Date de fin de l'ESU
Windows Server 2012 Windows Server 2012 R2	Azure*	Trois ans	13 octobre 2026
Windows Server 2012 Windows Server 2012 R2	Pas dans Azure	Trois ans	13 octobre 2026

* Inclut le portefeuille de produits Azure Stack qui étendent les services et fonctionnalités Azure à votre environnement de choix.

⚠ **Avertissement**

Une fois la période de mises à jour de sécurité étendues terminée, nous cesserons de fournir des mises à jour. Nous vous recommandons de mettre à jour dès que possible votre version de Windows Server vers une version plus récente.

Migrer vers Azure

Si vos serveurs locaux exécutent une version de Windows Server atteinte ou proche de la fin de la prise en charge étendue, vous pouvez les déplacer vers Azure. Dans Azure, vous pouvez continuer à exécuter ces serveurs en tant que machines virtuelles. Lorsque vous migrez vers Azure, vous restez non seulement conforme aux mises à jour de sécurité, mais vous ajoutez également l'innovation cloud à votre travail. Les avantages de la migration vers Azure sont les suivants :

- Mises à jour de sécurité dans Azure.
- Obtenez les mises à jour de sécurité critiques et importantes de Windows Server pendant une certaine période, incluses sans frais supplémentaires.
- Mises à niveau dans Azure gratuitement.
- Adoptez d'autres services cloud chaque fois que vous êtes prêt.
- En migrant SQL Server vers des machines virtuelles Azure, vous obtenez trois ans supplémentaires de mises à jour de sécurité critiques Windows Server, incluses sans frais supplémentaires. Vous pouvez également moderniser votre sql Server vers Azure SQL Managed Instance.
- Bénéficiez d'Azure Hybrid Benefit, qui vous permet d'utiliser des licences Windows Server existantes et des licences SQL Server pour les économies cloud uniques à Azure.

Pour commencer à migrer, découvrez comment charger un disque dur virtuel généralisé et l'utiliser pour créer de nouvelles machines virtuelles dans Azure ou utiliser des galeries d'images partagées dans Azure.

Vous pouvez également lire le Guide de migration pour Windows Server pour obtenir de l'aide sur les éléments suivants :

- Analysez vos ressources informatiques existantes.
- Évaluez l'état actuel de votre déploiement.
- Déterminez s'il faut déplacer certains services et applications vers le cloud. Vous pouvez également les conserver localement et les mettre à niveau vers la dernière version de Windows Server. Optez pour l'option la plus adaptée à votre organisation.

Mettre à niveau localement

Si vous devez conserver vos serveurs locaux au lieu de migrer vers Azure et le cloud, vous avez deux choix pour continuer :

- Créez de nouveaux serveurs avec une version prise en charge de Windows Server et migrez vos applications et données.
- Effectuez une mise à niveau sur place vers une version prise en charge de Windows Server.

Les mises à niveau sur place peuvent généralement mettre à niveau Windows Server via au moins une version, parfois même deux versions. Par exemple, Windows Server 2012 R2 peut effectuer une mise à niveau sur place vers Windows Server 2025. À mesure que vous effectuez une mise à niveau, vous pouvez également migrer vers Azure à tout moment. Pour plus d'informations sur vos options de mise à niveau locale, consultez les chemins de mise à niveau pris en charge pour Windows Server.

Mettre à niveau SQL Server en parallèle avec vos serveurs Windows

Si vous exécutez une version de SQL Server qui a atteint ou atteint la fin de sa prise en charge étendue, vous pouvez bénéficier également des mises à jour de sécurité étendues pour SQL Server. Pour plus d'informations, consultez Mises à jour de sécurité étendues pour SQL Server et Windows Server.

Contenu connexe

- Découvrez comment obtenir les mises à jour de sécurité étendues (ESU) pour Windows Server.
- Vue d'ensemble des mises à niveau de Windows Server

Qu’est-ce qu’un serveur à noyau sécurisé ?

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 concept de noyau sécurisé regroupe un ensemble de fonctionnalités de sécurité intégrées pour le matériel, les microprogrammes, les pilotes et les systèmes d’exploitation. La protection fournie par les systèmes à noyau sécurisé commence avant que ne démarre le système d’exploitation et se poursuit pendant l’exécution. Un serveur à noyau sécurisé est conçu pour fournir une plateforme sécurisée pour les données et les applications critiques.

Un serveur à noyau sécurisé repose sur trois piliers de sécurité clés :

- Création d’une racine de confiance matérielle.
- Défense contre les attaques au niveau des microprogrammes.
- Protection du système d’exploitation contre l’exécution de code non vérifié.

Comment reconnaître un serveur à noyau sécurisé

L’initiative du concept de noyau sécurisé a commencé avec les PC Windows grâce à une collaboration étroite entre Microsoft et des fabricants de PC partenaires visant à fournir une sécurité Windows encore jamais atteinte. Microsoft a étendu son partenariat à des fabricants de serveurs partenaires pour s’assurer que Windows Server fournit un environnement de système d’exploitation sécurisé.

Windows Server est étroitement intégré au matériel pour fournir des niveaux de sécurité croissants :

- Base de référence recommandée : valeur minimale recommandée pour tous les systèmes afin de fournir une intégrité système de base avec TPM 2.0 pour une racine matérielle de confiance et un démarrage sécurisé. TPM 2.0 et un démarrage sécurisé sont requis pour la certification matérielle de Windows Server. Pour en savoir plus, consultez Microsoft hausse les standards de sécurité dans la prochaine version majeure de Windows Server.
- Serveur à noyau sécurisé : recommandé pour les systèmes et les secteurs d’activité nécessitant des niveaux d’assurance plus élevés. Un serveur à noyau sécurisé s’appuie sur les fonctionnalités précédentes et utilise des fonctionnalités de processeur avancées pour fournir une protection contre les attaques de microprogramme.

Le tableau suivant montre comment chaque concept et chaque fonctionnalité de sécurité sont utilisés pour créer un serveur à noyau sécurisé.

Agrandir le tableau

Concept	Feature	Requirement	Base de référence recommandée	serveur Secured-Core
Créer une racine de confiance matérielle				
	Démarrage sécurisé	Le Démarrage sécurisé est activé par défaut dans le BIOS UEFI (Unified Extensible Firmware Interface).	✓	✓
	Trusted Platform Module (TPM) 2.0	Répond aux dernières exigences de Microsoft pour la spécification TCG (Trusted Computing Group).	✓	✓
	Certifié pour Windows Server	Indique qu'un système serveur atteint la barre technique la plus élevée de Microsoft en matière de sécurité, de fiabilité et de facilité de gestion.	✓	✓
	Protection DMA au démarrage	Prise en charge sur les appareils qui ont l'unité IOMMU (Input/Output Memory Management Unit). Par exemple, Intel VT-D ou AMD-Vi.		✓
Se défendre contre les attaques au niveau des microprogrammes				
	Lancement sécurisé de System Guard	Activé dans le système d'exploitation avec du matériel Intel et AMD compatible avec DRTM (Dynamic Root of Trust for Measurement).		✓
Protéger le système d'exploitation contre l'exécution de code non vérifié				

Concept	Feature	Requirement	Base de référence recommandée	serveur Secured-Core
	sécurité basée sur la virtualisation (VBS)	Nécessite l'hyperviseur Windows, qui est uniquement pris en charge sur les processeurs 64 bits avec des extensions de virtualisation, notamment Intel VT-X et AMD-v.	✓	✓
	HVCI (Hypervisor Enhanced Code Integrity)	Pilotes compatibles avec HVCI (Hypervisor Code Integrity) et exigences VBS.	✓	✓

Créer une racine de confiance matérielle

Le Démarrage sécurisé UEFI est un standard de sécurité qui protège vos serveurs contre les rootkits malveillants en vérifiant les composants de démarrage de vos systèmes. Le Démarrage sécurisé vérifie qu'un auteur approuvé a signé numériquement les pilotes et applications du microprogramme UEFI. Lorsque le serveur est démarré, le microprogramme vérifie la signature de chaque composant de démarrage, y compris les pilotes du microprogramme et le système d'exploitation. Si les signatures sont valides, le serveur démarre et le microprogramme donne le contrôle au système d'exploitation.

Pour en savoir plus sur le processus de démarrage, consultez Sécuriser le processus de démarrage Windows.

TPM 2.0 fournit un stockage sécurisé et basé sur le matériel pour les clés et données sensibles. Chaque composant chargé pendant le processus de démarrage est mesuré et les mesures sont stockées dans le module TPM. En vérifiant la racine de confiance matérielle, il élève la protection fournie par des fonctionnalités telles que BitLocker, qui utilise TPM 2.0 et facilite la création de workflows basés sur des attestations. Ces workflows basés sur les attestations peuvent être incorporés dans des stratégies de sécurité de Confiance Zéro.

Découvrez plus en détail les modules de plateforme sécurisée et l'utilisation du module TPM par Windows.

En plus du Démarrage sécurisé et de TPM 2.0, la fonctionnalité Noyau sécurisé de Windows Server utilise la protection DMA au démarrage sur les processeurs compatibles qui disposent de l'unité IOMMU (Input/Output Memory Management Unit). Par exemple, Intel VT-D ou AMD-Vi. Avec la protection DMA au démarrage, les systèmes sont protégés contre les attaques

d'accès direct à la mémoire (DMA) pendant le démarrage et pendant l'exécution du système d'exploitation.

Se défendre contre les attaques au niveau des microprogrammes

Les solutions de protection et de détection des points de terminaison ont généralement une visibilité limitée du microprogramme, étant donné que le microprogramme s'exécute derrière le système d'exploitation. Le microprogramme a un niveau d'accès et de privilège plus élevé que le système d'exploitation et le noyau de l'hyperviseur, ce qui en fait une cible intéressante pour les attaquants. Les attaques ciblant le microprogramme affaiblissent les autres mesures de sécurité implémentées par le système d'exploitation, ce qui rend plus difficile l'identification d'un système ou d'un utilisateur compromis.

À compter de Windows Server 2022, le lancement sécurisé de System Guard protège le processus de démarrage contre les attaques de microprogramme à l'aide des fonctionnalités matérielles d'AMD et d'Intel. Avec la prise en charge des processeurs par la technologie DRTM (Dynamic Root of Trust for Measurement), les serveurs à noyau sécurisé placent le microprogramme dans un bac à sable matériel afin de limiter les effets des vulnérabilités dans le code de microprogramme à privilèges élevés. System Guard utilise les fonctionnalités DRTM qui sont intégrées à des processeurs compatibles pour lancer le système d'exploitation, en veillant à ce que le système se lance dans un état approuvé en utilisant du code vérifié.

Protéger le système d'exploitation contre l'exécution de code non vérifié

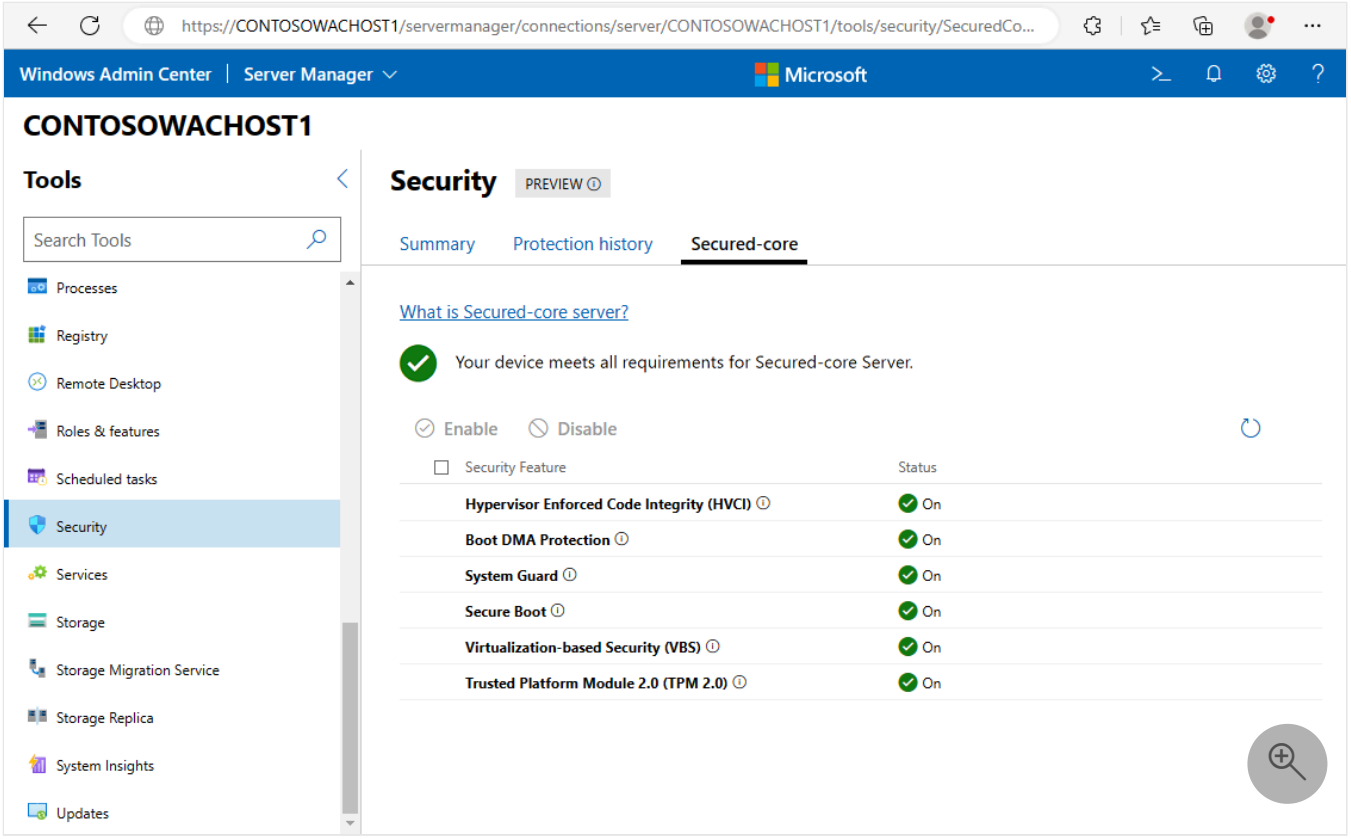
Un serveur à noyau sécurisé utilise la sécurité basée sur la virtualisation (VBS) et l'intégrité du code protégée par l'hyperviseur (HVCI) pour créer et isoler une région sécurisée de la mémoire du système d'exploitation normal. VBS utilise l'hyperviseur Windows pour créer un mode sécurisé virtuel (VSM, Virtual Secure Mode) afin d'offrir des barrières de sécurité au sein du système d'exploitation, qui peuvent être utilisées pour d'autres solutions de sécurité.

HVCI, communément appelé protection de l'intégrité de la mémoire, est une solution de sécurité qui permet de s'assurer que seul le code signé et approuvé est autorisé à s'exécuter dans le noyau. L'utilisation de code signé et approuvé uniquement empêche les attaques qui tentent de modifier le code en mode noyau. Par exemple, les attaques qui modifient les pilotes ou les programmes malveillants comme WannaCry qui tentent d'injecter du code malveillant dans le noyau.

Pour en savoir plus sur la configuration matérielle requise pour VBS, consultez La sécurité basée sur la virtualisation.

Gestion simplifiée

Vous pouvez afficher et configurer les fonctionnalités de sécurité de système d'exploitation des systèmes à noyau sécurisé avec Windows PowerShell ou l'extension de sécurité dans Windows Admin Center. Avec les systèmes intégrés Azure Local, les partenaires de fabrication ont encore simplifié l'expérience de configuration pour les clients afin que la meilleure sécurité serveur soit disponible dès la sortie de l'emballage grâce à Microsoft.



Explorez plus en détail Windows Admin Center.

Défense préventive

En activant la fonctionnalité de serveur à noyau sécurisé, vous pouvez vous défendre de manière proactive et bloquer la plupart des méthodes utilisées par les attaquants pour exploiter les failles de sécurité des systèmes. Un serveur à noyau sécurisé permet d'avoir des fonctionnalités de sécurité avancées dans les couches inférieures de la pile technologique qui protègent les zones les plus privilégiées du système avant que de nombreux outils de sécurité n'aient connaissance de programmes malveillants. Cette défense ne nécessite pas de tâches ou de surveillance supplémentaires de la part des équipes du service informatique et SecOps.

Commencer votre parcours vers un serveur à noyau sécurisé

Vous pouvez trouver du matériel certifié pour les serveurs à noyau sécurisé dans le catalogue Windows Server, et les serveurs locaux Azure dans le catalogue local Azure. Ces serveurs certifiés sont entièrement équipés avec des atténuations de sécurité de pointe intégrées au matériel, au microprogramme et au système d'exploitation pour aider à contrecarrer certains des vecteurs d'attaque les plus avancés.

Étapes suivantes

Maintenant que vous savez ce qu'est un serveur à noyau sécurisé, voici quelques ressources pour vous aider à démarrer. Découvrez comment :

- Configurer un serveur à noyau sécurisé.
- Microsoft apporte une sécurité matérielle avancée à Server et Edge avec les serveurs à noyau sécurisé dans le blog sur la sécurité Microsoft.
- De nouveaux serveurs à noyau sécurisé sont disponibles dans l'écosystème Microsoft pour vous aider à sécuriser votre infrastructure dans le blog sur la sécurité Microsoft.
- Créer des appareils, systèmes et pilotes de filtrage compatibles avec Windows sur toutes les plateformes Windows dans Spécifications et stratégies du programme de compatibilité matérielle Windows.

Configurer le serveur de base sécurisé

16/08/2025

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

Le cœur sécurisé est une collection de fonctionnalités qui offrent des fonctionnalités de sécurité intégrées du matériel, du microprogramme, du pilote et du système d'exploitation. Cet article explique comment configurer un serveur de base sécurisé à l'aide de Windows Admin Center, de l'expérience de bureau Windows Server et de la stratégie de groupe.

Le serveur de base sécurisé est conçu pour fournir une plateforme sécurisée pour les données et les applications critiques. Pour plus d'informations, consultez Qu'est-ce que le serveur de base sécurisé ?

Prerequisites

Avant de pouvoir configurer le serveur sécurisé, vous devez avoir les composants de sécurité suivants installés et activés dans le BIOS :

- Démarrage sécurisé.
- Module de plateforme sécurisée (TPM) 2.0.
- Le microprogramme système doit respecter les exigences de protection DMA de préboot et définir les indicateurs appropriés dans les tables ACPI pour choisir et activer la protection DMA du noyau. Pour en savoir plus sur la protection DMA du noyau, consultez protection DMA du noyau (protection de l'accès à la mémoire) pour les OEM.
- Processeur avec prise en charge activée dans le BIOS pour :
  - Extensions de virtualisation.
  - Unité de gestion de la mémoire d'entrée/sortie (IOMMU).
  - Mesure dynamique de la racine de confiance (DRTM).
  - Transparent Secure Memory Encryption est également nécessaire pour les systèmes AMD.

> **ⓘ Important**
>
> L'activation de chacune des fonctionnalités de sécurité dans le BIOS peut varier en fonction de votre fournisseur de matériel. Veillez à consulter le guide d'activation du serveur sécurisé de votre fabricant de matériel.

Vous pouvez trouver du matériel certifié pour le serveur avec cœur sécurisé dans le catalogue Windows Server, et des serveurs locaux Azure dans le catalogue local Azure.

Activer les fonctionnalités de sécurité

Pour configurer un serveur de base sécurisé, vous devez activer des fonctionnalités de sécurité Windows Server spécifiques, sélectionnez la méthode appropriée et suivez les étapes.

GUI

Voici comment activer le serveur sécurisé à l'aide de l'interface utilisateur.

1. Dans le bureau Windows, ouvrez le menu **Démarrer** , sélectionnez **Outils d'administration Windows**, ouvrez **Gestion des ordinateurs**.
2. Dans la gestion de l'ordinateur, sélectionnez **Gestionnaire** d'appareils, résolvez toute erreur d'appareil si nécessaire.
   a. Pour les systèmes AMD, vérifiez que le périphérique drTM Boot Driver est présent avant de continuer
3. Dans le bureau Windows, ouvrez le menu **Démarrer** , sélectionnez **Sécurité Windows**.
4. Sélectionnez **Sécurité de l'appareil** > **Détails de l'isolation du cœur**, puis activez **Intégrité de la mémoire** et **Protection du microprogramme**. Vous ne pourrez peut-être pas activer l'intégrité de la mémoire tant que vous n'avez pas activé la protection du microprogramme en premier et redémarré votre serveur.
5. Redémarrez votre serveur lorsque vous y êtes invité.

Une fois votre serveur redémarré, votre serveur est activé pour le serveur de base sécurisé.

Vérifier la configuration du serveur sécurisé

Maintenant que vous avez configuré le serveur de base sécurisé, sélectionnez la méthode appropriée pour vérifier votre configuration.

GUI

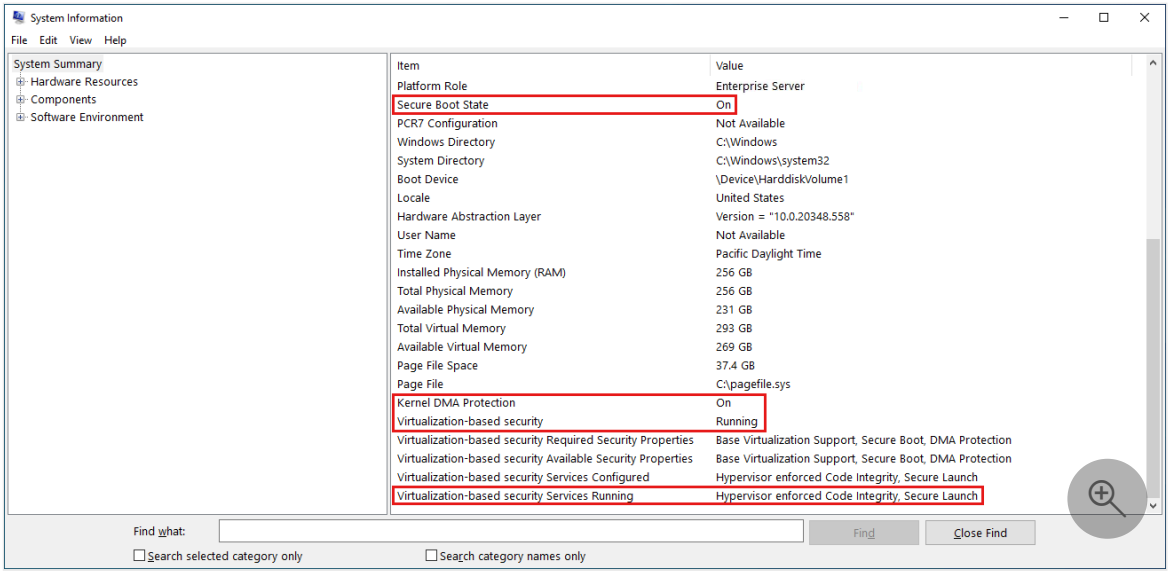
Voici comment vérifier que votre serveur de base sécurisé est configuré à l'aide de l'interface utilisateur.

1. Dans le bureau Windows, ouvrez le menu **Démarrer** , tapez `msinfo32.exe` pour ouvrir l'information système. Dans la page Résumé du système, confirmez :

   a. **État du démarrage sécurisé** et **Protection DMA du noyau** est activée.

   b. **La sécurité basée sur la virtualisation** est en cours d'exécution.

c. **Services de sécurité basés sur la virtualisation** En cours d'exécution affiche **Intégrité du code imposée par l'hyperviseur** et **lancement sécurisé**.



Étapes suivantes

Maintenant que vous avez configuré le serveur de base sécurisé, voici quelques ressources pour en savoir plus sur les points suivants :

- sécurité basée sur la virtualisation (VBS)
- L'intégrité de la mémoire et la mise en œuvre de VBS
- Lancement sécurisé System Guard

Hotpatch pour Windows Server

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

La mise à jour corrective à chaud (hotpatching) est un moyen d'installer les mises à jour de sécurité du système d'exploitation sur Windows Server sans avoir à redémarrer votre ordinateur. Elle procède à une mise à jour corrective du code en mémoire pour les processus en cours d'exécution sans qu'il soit nécessaire de les redémarrer. La mise à jour corrective à chaud offre également les avantages suivants :

- En diminuant le nombre de fichiers binaires, les mises à jour s'installent plus rapidement et consomment moins de ressources de disque et d'UC.
- En réduisant les redémarrages nécessaires de votre machine, vous réduisez l'impact sur la charge de travail.
- La protection est plus efficace, puisque les packages de mise à jour Hotpatch sont étendus aux mises à jour de sécurité Windows qui s'installent plus rapidement sans que vous deviez redémarrer votre machine.
- Réduction du temps d'exposition aux risques de sécurité et aux fenêtres de modification et simplification de l'orchestration des correctifs avec le Gestionnaire de mise à jour Azure.

Cet article décrit Hotpatch pour Windows Server, qui utilise le modèle de support et de gestion Windows Server sur Azure, Azure Local et les machines connectées à Azure Arc.

> ⓘ **Remarque**
>
> Cet article ne traite pas du client Hotpatch pour Windows, qui est distinct du modèle de support et de gestion de Windows Server décrit ici. Pour obtenir des conseils sur Hotpatch pour Windows 11 Enterprise, version 24H2 ou ultérieure, voir Mises à jour Hotpatch. Sur le client Windows, Windows Autopatch gère les mises à jour hotpatch via Microsoft Intune, et seuls les appareils éligibles remplissant les prérequis sur cette page les reçoivent.

Plateformes prises en charge

Machines virtuelles Azure et Azure Local

Le tableau suivant répertorie les combinaisons exactes d'éditeur, d'offre de système d'exploitation et de référence SKU qui prennent en charge la mise à jour corrective à chaud pour Windows Server 2022 et Windows Server 2025 sur Azure. Les machines virtuelles que vous créez sur Azure Local à l'aide de ces combinaisons prennent également en charge hotpatching.

> **Remarque**
>
> Les images de base de conteneurs Windows Server, les images personnalisées ou toute autre combinaison d'éditeur, d'offre et de référence SKU ne sont pas prises en charge.

Agrandir le tableau

Publisher	Offre de système d'exploitation	SKU
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core-smalldisk
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch-smalldisk
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition-smalldisk
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	WindowsServer	2025-Datacenter-Azure-Edition-Core-smalldisk

Pour plus d'informations sur les images disponibles, consultez Windows Server sur la Place de marché Azure.

Machines connectées à Azure Arc

> **Important**
>
> Le Hotpatch compatible avec Azure Arc pour Windows Server 2025 est désormais disponible sans frais supplémentaires. Pour plus d'informations, consultez Accès simplifié à la mise à jour corrective à chaud activée par Azure Arc pour Windows Server 2025.

Les machines Windows Server 2025 connectées à Azure Arc peuvent recevoir des mises à jour correctives à chaud si vous activez la fonctionnalité sur le portail Azure Arc. Pour commencer à utiliser les mises à jour correctives à chaud avec Azure Arc, connectez Azure Arc aux machines utilisant l'une des éditions suivantes :

- Windows Server 2025 Édition Datacenter
- Windows Server 2025 Édition Standard

Fonctionnement de Hotpatch

La mise à jour corrective à chaud établit d'abord une base de référence avec la mise à jour cumulative actuelle pour Windows Server. Toutes les trois mois, la base de référence s'actualise régulièrement avec la dernière mise à jour cumulative. Vous recevez ensuite les versions correctives à chaud pour les deux mois suivant la mise à jour cumulative. Par exemple, si janvier est une mise à jour cumulative, février et mars auront des versions Hotpatch. Pour plus d'informations sur la planification de la mise en production de Hotpatch, consultez le calendrier Hotpatch Windows Server.

Il existe deux types de lignes de base : les **lignes de base planifiées** et **les bases de référence non planifiées**.

- Les **bases de référence planifiées** sont publiées à intervalle régulier, avec entre-temps des mises à jour correctives à chaud. Les bases de référence planifiées incluent toutes les mises à jour dans une mise à jour cumulative comparable pour ce mois-ci et vous obligent à redémarrer votre machine.
  - Par exemple, une période de publication d'un an planifiée peut inclure quatre versions de base planifiées durant l'année civile et huit versions Hotpatch.
- **Les versions de référence non planifiées** sont publiées lors d'une mise à jour importante non planifiée, telle qu'un correctif zero-day, lorsque cette mise à jour ne peut pas être déployée sous forme de correctif à chaud. Quand des bases de référence non planifiées sont publiées, la publication d'une mise à jour corrective à chaud est remplacée par une base de référence non planifiée pour ce mois-là. Les bases de référence non planifiées incluent aussi toutes les mises à jour dans une mise à jour cumulative comparable pour ce mois-ci et vous obligent donc à redémarrer votre machine.
  - Ces événements étant non planifiés, les développeurs ne peuvent pas prédire les bases de référence non planifiées à l'avance.

Les mises à jour correctives à chaud ne vous obligent pas à redémarrer la machine. Les mises à jour correctives à chaud corrigeant le code en mémoire des processus en cours d'exécution sans avoir à les redémarrer, vos applications ne sont pas affectées. Cette absence de redémarrage n'affecte pas les performances ou les implications des fonctionnalités du correctif lui-même.

Mises à jour prises en charge

La mise à jour corrective à chaud couvre les mises à jour de sécurité Windows et maintient la parité avec le contenu des mises à jour de sécurité publiées dans le canal des mises à jour Windows standard hors mise à jour corrective à chaud.

Il existe quelques éléments importants à prendre en compte lors de l'activation des mises à jour correctives à chaud sur une version prise en charge de Windows Server. Vous devez quand même redémarrer votre machine pour installer les mises à jour qui ne sont pas incluses dans le programme de mises à jour correctives à chaud. Vous devez également redémarrer régulièrement après l'installation d'une nouvelle base de référence. Le redémarrage permet à votre machine virtuelle de se synchroniser avec les correctifs non liés à la sécurité inclus dans les dernières mises à jour cumulatives.

Les correctifs suivants ne sont actuellement pas inclus dans le programme de mises à jour correctives à chaud et vous obligent à mettre à jour votre machine pendant les mois de publication de mises à jour correctives à chaud :

- Mises à jour non liées à la sécurité pour Windows
- Mises à jour .NET
- Mises à jour non-Windows, par exemple les pilotes, les mises à jour du microprogramme, etc.

Processus d'orchestration des correctifs

La mise à jour corrective à chaud (Hotpatch) est une extension de Windows Update et des processus de gestion classiques. Toutefois, les outils de gestion des correctifs varient en fonction de la plateforme que vous utilisez.

Azure

- Les machines virtuelles que vous créez dans Azure à l'aide d'une image Windows Server prise en charge bénéficient par défaut de l'activation de la mise à jour corrective

automatisée des machines virtuelles invitées.

- La mise à jour corrective à chaud télécharge et applique automatiquement les correctifs classés comme critiques ou de sécurité à votre machine virtuelle.
- La mise à jour corrective à chaud applique les correctifs pendant les heures creuses dans le fuseau horaire de la machine virtuelle.
- Azure gère les correctifs pour vous, en appliquant des correctifs en fonction des principes de disponibilité.
- Azure surveille l'intégrité des machines virtuelles par le biais de signaux d'intégrité de la plateforme pour détecter les défaillances de mise à jour corrective.

> **Remarque**
>
> Vous ne pouvez pas créer de groupes de machines virtuelles identiques avec l'orchestration uniforme sur les images Azure Edition avec le patch à chaud. Pour en savoir plus sur les fonctionnalités prises en charge par l'orchestration Uniform pour les groupes identiques, consultez **Comparaison du mode d'orchestration Flexible, du mode d'orchestration Uniform et des groupes à haute disponibilité**.

Azure Local

Azure Local peut orchestrer les mises à jour Hotpatch pour les machines virtuelles à l'aide des outils suivants :

- La stratégie de groupe configure les paramètres du client Windows Update.
- SConfig configure Windows Update paramètres client pour Server Core.
- Solutions de gestion des correctifs non-Microsoft.

Machines connectées à Azure Arc

Les machines connectées à Azure Arc peuvent installer et gérer les mises à jour Hotpatch à l'aide des outils suivants :

- Gestionnaire de mise à jour Azure
- La stratégie de groupe configure les paramètres du client Windows Update.

- SConfig configure Windows Update paramètres client pour Server Core.
- Solutions de gestion des correctifs non-Microsoft.

Pour plus d'informations sur les outils utilisés par la mise à jour corrective à chaud, consultez notre documentation Gestionnaire de mise à jour Azure .

Comprendre l'état des correctifs pour votre machine virtuelle dans Azure

Pour afficher l'état du correctif de votre machine virtuelle, ouvrez la page Vue d'ensemble de votre machine virtuelle dans le Portail Azure. À partir de là, sous **Opérations**, sélectionnez **Mises à jour**. Vous devez voir l'état des correctifs et les derniers correctifs installés sous **mises à jour recommandées**.

Dans la page **Mises à jour recommandées** , vous pouvez voir l'état Hotpatch de votre machine virtuelle et s'il existe des correctifs disponibles pour votre machine virtuelle. Comme nous l'avons indiqué dans Fonctionnement de la mise à jour corrective à chaud, la mise à jour corrective automatique des invités de machine virtuelle installe automatiquement tous les correctifs critiques et de sécurité sur votre machine virtuelle.

Les correctifs en dehors de ces deux catégories ne sont pas installés automatiquement et sont affichés dans l'onglet **Conformité des mises à jour** sous la forme d'une liste de correctifs disponibles. Vous pouvez également consulter l'onglet **Historique** des mises à jour pour afficher les détails d'installation des correctifs pour les déploiements de mises à jour sur votre machine virtuelle au cours des 30 derniers jours.

La mise à jour corrective automatique des invités de machine virtuelle exécute régulièrement des évaluations des correctifs disponibles, que vous pouvez afficher sous l'onglet **Mises à jour** . Vous pouvez démarrer manuellement une évaluation en sélectionnant le bouton **Évaluer maintenant** . Vous pouvez également installer des correctifs à la demande en sélectionnant le bouton **Installer les mises à jour maintenant**. Cette option vous permet de choisir d'installer toutes les mises à jour sous des classifications de correctifs spécifiques. Vous pouvez également sélectionner des mises à jour individuelles à inclure ou exclure en fournissant une liste d'articles de base de connaissances. Gardez toutefois à l'esprit que les correctifs que vous installez manuellement ne suivent pas les principes de première disponibilité et peuvent nécessiter le redémarrage de votre machine virtuelle.

Vous pouvez également afficher les correctifs installés en exécutant l'applet de commande Get-HotFix dans PowerShell ou en affichant le menu **Paramètres** dans Expérience de bureau.

Prise en charge de la restauration pour les mises à jour correctives à chaud

Les mises à jour correctives à chaud ne prennent pas en charge la restauration automatique. Si vous rencontrez un problème pendant ou après une mise à jour, vous devez désinstaller la dernière mise à jour et installer la dernière mise à jour de base de référence fonctionnelle. Ce processus nécessite de redémarrer la machine virtuelle.

Étapes suivantes

- Activer Hotpatch pour les serveurs avec Azure Arc
- Mise à jour corrective automatique des invités pour les machines virtuelles
- Activer Hotpatch pour les machines virtuelles Azure Edition générées à partir d'une image ISO
- Gestion des mises à jour Azure

Dernière mise à jour : 10/09/2026

Installer Windows Server à partir du support d'installation

13/10/2025

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

Découvrez comment créer un lecteur USB ou un DVD de démarrage qui peut être utilisé pour installer Windows Server sur vos appareils. La création d'un support d'installation Windows Server est une étape cruciale de la configuration d'un nouveau serveur ou d'une mise à niveau à partir d'un support existant. Cet article vise à vous guider sur la création d'un support d'installation et l'installation de Windows Server à l'aide des options d'installation server Core ou Desktop Experience.

Conditions préalables

Le support d'installation pour la version cible de Windows Server peut être obtenu auprès du fabricant d'équipement d'origine (OEM), de la vente au détail, de l'abonnement Visual Studio et du centre de gestion des licences en volume (VLSC). Votre appareil ne doit pas non plus s'exécuter dans Azure. Si vous souhaitez installer Windows Server dans Azure, consultez démarrage rapide : Créer une machine virtuelle Windows dans le portail Azure. Les éléments suivants sont requis avant d'installer Windows Server :

- **Matériel**
  - Votre appareil doit respecter ou dépasser la configuration matérielle minimale requise. Pour plus d'informations, consultez Configuration matérielle requise pour Windows Server.
  - Un minimum d'un lecteur flash USB de 8 Go.
  - Lecteur optique capable de brûler un disque DVD+/-RW double couche.
  - Dvd double couche 8,5 Go.

- **Logiciel**
  - Déterminez la version de Windows Server appropriée pour votre environnement. Pour plus d'informations, consultez Comparaison des éditions de Windows Server.
  - Vérifiez que vous disposez d'une clé de produit ou d'une licence d'abonnement valide pour votre produit. Les clés de produit et les méthodes d'activation peuvent varier en fonction du canal de distribution à partir duquel vous avez reçu le support Windows Server, tel qu'un programme de licence commerciale, une vente au détail ou un OEM.

> ⓘ **Notes**

Pour les utilisateurs qui souhaitent installer Windows Server dans un environnement virtuel via Windows Hyper-V, les exigences minimales en matière de RAM diffèrent. Pour plus d'informations, consultez l'onglet **Exigences matérielles pour les composants de Windows Server**.

Créer un lecteur flash USB démarrable

En règle générale, la création d'un lecteur USB démarrable peut être effectuée à l'aide de l'utilitaire diskpart.exe. Une alternative à la préparation manuelle de votre lecteur USB, les utilisateurs peuvent exécuter le script PowerShell suivant pour rendre le lecteur USB démarrable. Le fichier ISO d'installation de Windows Server doit être monté avant d'exécuter ce script. Pour monter le fichier ISO, procédez comme suit :

1. Recherchez votre fichier ISO d'installation de Windows Server.
2. Cliquez avec le bouton droit sur votre fichier ISO, puis sélectionnez **montage**.

Le montage du fichier ISO crée un lecteur optique virtuel, avec sa propre lettre de lecteur, où les utilisateurs peuvent migrer le contenu ISO vers leur lecteur USB.

Une fois que vous avez branché votre lecteur USB, il devrait vous fournir une lettre de lecteur. Une fois que vous connaissez la lettre de lecteur du lecteur USB et de l'ISO monté, exécutez l'un des scripts suivants. Chaque script compte trois nouvelles tentatives avant de passer au jeu de fichiers suivant.

Formater en NTFS

Ce script permet à votre lecteur USB de démarrer au format NTFS.

PowerShell

```
# Select USB drive letter
$usbDriveLetter = Read-Host "Enter USB drive letter (Ex: E)"

# Format USB drive
Format-Volume -DriveLetter $usbDriveLetter -FileSystem NTFS -
NewFileSystemLabel "WinServerUSB" -Confirm:$false | Out-Null

# Select ISO file mount point
$isoMountPointDriveLetter = Read-Host "Enter ISO mount point drive letter (Ex:
F)"

# Copy ISO files to USB drive
$source = "$($isoMountPointDriveLetter):\"
$destination = "$($usbDriveLetter):\"
```

```
robocopy $source $destination /COPYALL /Z /E /SEC /R:3 /W:3

# Make USB drive bootable
$usbDriveNumber = (Get-WmiObject -Class Win32_DiskDrive | Where-Object
{$_.InterfaceType -eq "USB" -and $_.DeviceID -like "*$usbDriveLetter"}).Index
bootsect /nt60 $usbDriveLetter`:

# Task completion notification
Write-Host "USB Creation Complete!"
Start-Sleep -Seconds 2
```

Créer un DVD de démarrage

1. Insérez un DVD double couche 8,5 Go dans votre lecteur optique.
2. Recherchez votre fichier ISO d'installation de Windows Server.
3. Cliquez avec le bouton droit de la souris sur votre fichier ISO et sélectionnez **Graver une image disque**.
4. L'assistant **Windows Disc Image Burner** vous invite à sélectionner le **graveur** que vous souhaitez utiliser.
5. Sélectionnez le lecteur approprié, puis cliquez sur le bouton **Graver**.
6. Cette étape est facultative, mais recommandée pour s'assurer que l'intégrité des données est vérifiée par rapport aux erreurs ou différences entre le disque brûlé et l'image ISO d'origine. Cochez la case **Vérifier le disque après la gravure** pour détecter toute différence.

Configurer les paramètres du BIOS

Avant de pouvoir installer Windows Server via USB ou DVD, l'ordre de démarrage de l'ordinateur dans le BIOS doit être modifié pour vous assurer que le système démarre à partir de l'USB ou du DVD. L'accès au BIOS peut varier en fonction de votre matériel. Dans la plupart des cas, vous pouvez accéder au BIOS en appuyant sur une touche spécifique pendant le démarrage de votre appareil. En règle générale, la clé est F2, F10, **F12**ou **Supprimer**. Reportez-vous au manuel de l'utilisateur pour votre appareil. Sur certains matériels, une fois POST terminé, il existe une courte fenêtre autorisée pour accéder au BIOS. Vous devrez peut-être appuyer à plusieurs reprises sur l'une des touches dès que POST est terminé.

Une fois que vous êtes dans les paramètres du BIOS, parcourez les menus jusqu'à ce que vous voyiez l'option ordre de démarrage ou séquence de démarrage . Reportez-vous au manuel utilisateur de votre appareil pour localiser ce paramètre. Une fois que vous avez sélectionné le paramètre d'ordre de démarrage, vous pouvez modifier la priorité de l'ordre de démarrage en fonction de l'ordre de démarrage dans l'ordre supérieur. Déplacez le démarrage à partir du

lecteur USB ou optique en haut de la liste en fonction de la méthode d'installation du support que vous utilisez. Une fois les modifications appropriées effectuées, enregistrez et quittez le BIOS. Votre appareil redémarre automatiquement en appliquant ces modifications.

> ⓘ **Notes**
>
> Si votre système a deux disques et que vous tentez d'installer Windows Server 2025 sur le deuxième disque, l'installation peut échouer. Cela est dû au fait qu'un système BIOS hérité nécessite que le système d'exploitation soit installé sur le disque principal énuméré par le BIOS, généralement sur le disque BIOS 0. Si votre BIOS autorise la configuration explicite du disque énuméré BIOS principal, veillez à sélectionner le disque désigné pendant l'installation. Vous pouvez exécuter `SELECT DISK=SYSTEM` dans diskpart pour identifier le premier disque énuméré du BIOS.

Installer Windows Server

Une fois les modifications apportées à l'ordre de démarrage et que vous sélectionnez démarrer à partir du lecteur USB ou DVD, procédez comme suit pour installer Windows Server.

Expérience de bureau

1. Connectez votre lecteur USB ou dvd à votre lecteur optique, puis redémarrez votre appareil.
2. Une fois que votre appareil démarre, vous êtes invité à appuyer sur n'importe quelle touche pour démarrer à partir de votre support d'installation.
3. Sous **Sélectionner les paramètres de langue**, sélectionnez votre langue, votre heure et le format monétaire, puis sélectionnez suivant.
4. Sous **Sélectionner les paramètres du clavier**, sélectionnez la langue de votre clavier, puis suivant.
5. Sous **Sélectionner l'option d'installation**, sélectionnez **Installer Windows Server**, sélectionnez **je suis d'accord que tout sera supprimé, y compris les fichiers, les applications et les paramètres**, puis sélectionnez suivant.
6. Sous **Choisir une méthode de licence**, sélectionnez l'option qui convient le mieux à votre environnement, puis sélectionnez suivante :

a. **Utiliser une clé de produit** : cette option est destinée aux utilisateurs disposant d'une clé OEM, de vente au détail ou de licence en volume (VL). Si ce type de licence est sélectionné, procédez comme suit.

b. paiement à l'utilisation : cette option est destinée aux utilisateurs qui souhaitent utiliser leur licence d'abonnement Azure. Cette option est disponible uniquement pour Windows Server 2025 et possède son propre ensemble de conditions préalables . Si ce type de licence est sélectionné, reportez-vous à la section Configurer Windows Server Pay-as-you-go pour poursuivre le processus d'installation.

7. Sous **Sélectionner une image**, sélectionnez votre version de Windows Server, puis sélectionnez **Suivant**.

8. Sous **Avis applicables et conditions de licence**, passez en revue les termes du logiciel, puis sélectionnez **Accepter**.

9. Sous **Sélectionner l'emplacement d'installation de Windows Server**, sélectionnez le disque que vous souhaitez installer Windows Server, puis sélectionnez **Suivant**.

10. Dans la section **Prêt à installer**, sélectionnez **Installer**.

11. Une fois que votre appareil redémarre quelques fois, les termes du contrat de licence **s'affichent**. Sélectionnez **Accepter** pour continuer.

12. Sous **Personnaliser les paramètres**, fournissez un mot de passe complexe pour le compte Administrateur, puis sélectionnez **Terminer**.

13. Une fois que vous vous êtes connecté au compte Administrateur, passez en revue les informations **Envoyer les données de diagnostic à Microsoft**, puis sélectionnez **Accepter**.

> ⓘ **Notes**
>
> Pour gérer et configurer votre environnement Windows Server Core, vous avez la possibilité d'utiliser l'outil configuration du serveur (**SConfig**). Pour plus d'informations, consultez Administrer un serveur Server Core et Configurer une installation Server Core de Windows Server et Azure Local avec l'outil de configuration de serveur (SConfig).

Voir aussi

- Bien démarrer avec Windows Server
- Nouveautés de Windows Server 2025
- installer ou désinstaller des rôles, des services de rôle ou des fonctionnalités
- Vue d’ensemble de la technologie Hyper-V
- Vue d’ensemble du partage de fichiers à l’aide du protocole SMB 3 dans Windows Server

Installer la fonctionnalité de compatibilité des applications à la demande sur Server Core

18/07/2025S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

La fonctionnalité de compatibilité des applications à la demande (FOD) est un package de fonctionnalités facultatif conçu pour améliorer la compatibilité des installations Server Core dans Windows Server. À partir de Windows Server 2019, vous pouvez installer cette fonctionnalité à tout moment pour améliorer la compatibilité des applications avec les installations Server Core de Windows Server et fournir des outils supplémentaires pour les tâches quotidiennes. Cet article explique les avantages de la fonctionnalité de compatibilité des applications à la demande, décrit son processus d'installation et fournit des instructions pour l'ajouter à un serveur ou à une image Windows personnalisée.

Pour plus d'informations sur les autres fonctionnalités à la demande, consultez Fonctionnalités à la demande.

Pourquoi installer la fonctionnalité de compatibilité des applications à la demande

La fonctionnalité de compatibilité des applications à la demande pour Server Core inclut un sous-ensemble de fichiers binaires et de packages de l'option d'installation de Server with Desktop Experience. Ce package facultatif est disponible à partir de Windows Update ou sur une iso distincte, mais il ne peut être ajouté qu'aux installations et images Server Core.

Les deux principaux avantages de la fonctionnalité de compatibilité des applications à la demande sont les suivants :

- Compatibilité accrue de Server Core pour les applications serveur.
- L'ajout de composants du système d'exploitation n'est pas normalement inclus avec Server Core, ce qui peut vous aider à gérer les tâches d'administration et la compatibilité des outils logiciels utilisés dans les scénarios de résolution des problèmes et de débogage aigus.

Les composants du système d'exploitation disponibles dans le cadre de la fonctionnalité de compatibilité des applications à la demande sont les suivants :

Agrandir le tableau

Composant	Nom du fichier	Disponible pour la première fois
Gestionnaire de périphériques	`devmgmt.msc`	Windows Server 2019
Gestion des disques	`diskmgmt.msc`	Windows Server 2019
Observateur d'événements	`eventvwr.msc`	Windows Server 2019
Gestionnaire du cluster de basculement	`cluadmin.msc`	Windows Server 2019
Explorateur de fichiers	`explorer.exe`	Windows Server 2019
Gestionnaire Hyper-V	`virtmgmt.msc`	Windows Server 2022
Console MMC (Microsoft Management Console)	`mmc.exe`	Windows Server 2019
Analyseur de performances	`perfmon.exe`	Windows Server 2019
Moniteur de ressources	`resmon.exe`	Windows Server 2019
Planificateur de tâches	`taskschd.msc`	Windows Server 2022
Environnement de script intégré Windows PowerShell (ISE)	`powershell_ise.exe`	Windows Server 2019

Conditions préalables

Avant de commencer, vérifiez que vous remplissez les conditions préalables suivantes :

- La fonctionnalité de compatibilité des applications à la demande ne peut être installée que sur les installations minimales de Windows Server. N'essayez pas d'ajouter la fonctionnalité de compatibilité des applications à la demande aux serveurs avec l'option d'installation Expérience de Bureau.

- Vous devez être connecté avec un compte d'administrateur sur l'ordinateur Server Core auquel vous souhaitez ajouter la fonctionnalité de compatibilité des applications à la demande.

- Les fonctionnalités Windows Server suivantes nécessitent une configuration supplémentaire :
  - Le gestionnaire du cluster de basculement (`cluadmin.msc`) nécessite l'installation préalable de la fonctionnalité Clustering de basculement Windows Server.
  - La console de gestion IIS (`Web-Mgmt-Console`) s'appuie sur la fonctionnalité de compatibilité des applications à la demande pour être installée, car elle nécessite l'exécution de la console de gestion Microsoft (`mmc.exe`).

- Si vous souhaitez ajouter la fonctionnalité de compatibilité des applications à la demande à une image Windows personnalisée (WIM), vous avez besoin du fichier image ISO pour la version de Windows Server pour laquelle vous souhaitez créer une image personnalisée.

Installer la fonctionnalité de compatibilité des applications à la demande

L'installation de la fonctionnalité de compatibilité des applications à la demande implique l'ajout d'un package spécialisé à votre installation Server Core qui fournit des outils supplémentaires et des fonctionnalités de compatibilité normalement trouvés dans Server with Desktop Experience.

Le processus d'installation dépend de l'installation de la fonctionnalité de compatibilité des applications à la demande à partir de Windows Update ou d'une image ISO. Vous pouvez installer la fonctionnalité directement à partir de Windows Update en exécutant une commande PowerShell. Pour une image ISO, vous devez télécharger l'ISO des langues et des fonctionnalités facultatives pour Windows Server, la monter localement, et installer les fonctionnalités à partir de cette source.

Après avoir installé la fonctionnalité de compatibilité des applications à la demande et redémarré le serveur, la couleur du cadre de la fenêtre de console de commande passe à une autre nuance de bleu.

Sélectionnez l'onglet approprié pour votre méthode d'installation préférée.

Windows Update

Pour installer la fonctionnalité de compatibilité des applications à la demande sur une installation minimale de Windows Server à partir de Windows Update :

1. Connectez-vous au serveur avec un compte d'administrateur.
2. Dans `SConfig`, utilisez l'option **15** pour quitter `SConfig` PowerShell.
3. Installez la fonctionnalité de compatibilité des applications à la demande en exécutant la commande suivante. La commande prend plusieurs minutes.

```
PowerShell

Add-WindowsCapability -Online -Name
"ServerCore.AppCompatibility~~~~0.0.1.0"
```

Le résultat ressemble à l'exemple suivant :

Sortie

```
Path          :
Online        : True
RestartNeeded : True
```

4. Une fois la commande terminée, redémarrez le serveur pour appliquer les modifications, puis installez les dernières mises à jour du système d'exploitation.

> **Important**
>
> Si vous effectuez une mise à niveau sur place de Windows Server vers une version plus récente, la fonctionnalité de compatibilité des applications à la demande ne reste pas en place. Vous devez l'installer à nouveau après la mise à niveau. Vous pouvez également ajouter la fonctionnalité de compatibilité des applications à la demande à une image Windows personnalisée (WIM) que vous utilisez pour installer Windows Server. L'ajout de la fonctionnalité de compatibilité des applications à la demande à une image personnalisée garantit qu'elle est présente une fois la mise à niveau terminée. Pour plus d'informations, consultez Ajouter la fonctionnalité de compatibilité des applications à la demande à une section d'image WIM personnalisée .

Ajouter la fonctionnalité de compatibilité des applications à la demande à une image WIM personnalisée

Si vous ajoutez la fonctionnalité de compatibilité des applications à la demande à une image Windows personnalisée (WIM) et que vous utilisez cette image pour installer Windows Server, elle est automatiquement installée pendant le processus d'installation. Il reste en place après une mise à niveau sur place de Windows Server vers une version plus récente.

Pour ajouter la fonctionnalité de compatibilité des applications à la demande à une image WIM personnalisée, procédez comme suit. Veillez à remplacer `<values>` par le vôtre.

1. Téléchargez le fichier image ISO qui contient des fonctionnalités à la demande pour la version de Windows Server pour laquelle vous souhaitez créer une image personnalisée. Enregistrez l'image ISO dans un dossier dans le même dossier que celui où vous disposez

du fichier image ISO Windows Server. L'image ISO est disponible pour les versions suivantes de Windows Server :

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019

2. Montez à la fois les langages et les fonctionnalités facultatives ISO et windows Server ISO en exécutant les commandes suivantes dans une session PowerShell avec élévation de privilèges :

```PowerShell
$isoFolder = "<ISO folder path>"
$fodIsoFilename = "<FOD_ISO_filename.iso>"
$wsIsoFilename = "<Windows_Server_ISO_filename.iso>"

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
$wsIso = Mount-DiskImage -ImagePath "$isoFolder\$wsIsoFilename"
```

3. Exécutez la commande suivante pour obtenir les lettres de lecteur sur lesquelles les fichiers ISO FOD et ISO Windows Server sont montés :

```PowerShell
$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
$wsDriveLetter = ($wsIso | Get-Volume).DriveLetter
```

4. Copiez le contenu de l'image ISO Windows Server dans un dossier local, par exemple **C :\SetupFiles\WindowsServer\Files**, en exécutant les commandes suivantes. L'opération de copie peut prendre un certain temps.

```PowerShell
$wsFiles = "<Windows Server files path>"
New-Item -ItemType Directory -Path $wsFiles

Copy-Item -Path ${wsDriveLetter}:\* -Destination $wsFiles -Recurse
```

5. Obtenez le nom de l'image que vous souhaitez modifier dans le `install.wim` fichier en exécutant la commande suivante. Le `install.wim` fichier se trouve dans le dossier **sources** de l'image ISO Windows Server. Les noms des images disponibles dans ce `install.wim` fichier se trouvent dans la sortie.

```PowerShell
```

```
$installWimPath = "<Windows Server Files Path>\sources\install.wim"

Get-WindowsImage -ImagePath $installWimPath
```

6. Montez le `install.wim` fichier dans un nouveau dossier en exécutant la commande suivante :

   - `$wimImageName` - Entrez le nom de l'image à monter à partir de la sortie de la commande précédente. L'exemple ici utilise **Windows Server 2022 Datacenter**.
   - `$wimMountFolder` - Spécifiez un dossier vide à utiliser lors de l'accès au contenu du fichier install.wim.

PowerShell

```
$wimImageName = "<Image name, for example Windows Server 2022 Datacenter>"
$wimMountFolder = "<WIM folder path>"

New-Item -ItemType Directory -Path $wimMountFolder
Set-ItemProperty -Path $installWimPath -Name IsReadOnly -Value $false
Mount-WindowsImage -ImagePath $installWimPath -Name $wimImageName -Path
$wimMountFolder
```

7. Ajoutez les fonctionnalités et packages que vous souhaitez à l'image montée `install.wim` en exécutant les commandes suivantes (en fonction de la version), en remplaçant les valeurs d'exemple de variable par vos propres valeurs.

   - Pour Windows Server 2022 et versions ultérieures :

     PowerShell

     ```
     $capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"

     Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
     Source "${fodDriveLetter}:\LanguagesAndOptionalFeatures" -LimitAccess
     ```

   - Pour les versions précédentes de Windows Server :

     PowerShell

     ```
     $capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"

     Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
     Source "${fodDriveLetter}:\" -LimitAccess
     ```

8. Démontez et validez les modifications apportées au `install.wim` fichier en exécutant la commande suivante :

```powershell
Dismount-WindowsImage -Path $wimMountFolder -Save
```

Vous pouvez maintenant installer Windows Server à l'aide de l'image WIM personnalisée avec la fonctionnalité de compatibilité des applications à la demande incluse et reste en place après une mise à niveau sur place de Windows Server vers une version plus récente.

Installer Internet Explorer 11 sur Server Core

Vous pouvez installer Internet Explorer 11 sur une installation Server Core de Windows Server 2022 et des versions précédentes. Internet Explorer nécessite que la fonctionnalité de compatibilité des applications à la demande soit installée en premier. Si vous devez l'installer, consultez la section Installer la fonctionnalité de compatibilité des applications à la demande. Vous n'avez pas besoin d'installer Internet Explorer pour ajouter la fonctionnalité de compatibilité des applications à la demande.

> **Conseil**
>
> Dans Windows Server 2022, même si vous pouvez ajouter Internet Explorer 11 aux installations Server Core de Windows Server, **Microsoft Edge** doit être utilisé à la place. Microsoft Edge dispose du **mode Internet Explorer (mode Internet Explorer**) intégré, ce qui vous permet d'accéder aux sites web et applications Internet Explorer hérités directement à partir de Microsoft Edge. Pour plus d'informations sur le cycle de vie du produit pour Internet Explorer, consultez **faq sur le cycle de vie - Internet Explorer et Microsoft Edge**.

Sélectionnez l'onglet approprié pour votre méthode d'installation préférée.

Windows Update

Pour installer Internet Explorer 11 sur une installation Server Core de Windows Server à partir de Windows Update :

1. Vérifiez que vous avez installé la fonctionnalité de compatibilité des applications à la demande sur l'installation minimale de Windows Server.

2. Une fois de plus, suivez les étapes décrites dans la section Installer la fonctionnalité de compatibilité des applications à la demande, mais pour l'étape 3, exécutez la commande suivante à la place :

   PowerShell

   ```
   Add-WindowsCapability -Online -Name
   "Browser.InternetExplorer~~~~0.0.11.0"
   ```

   Le résultat ressemble à l'exemple suivant :

   Sortie

   ```
   Path          :
   Online        : True
   RestartNeeded : True
   ```

3. Une fois la commande terminée, redémarrez le serveur pour appliquer les modifications, puis installez les dernières mises à jour du système d'exploitation.

4. Après le redémarrage du serveur, vous pouvez accéder à Internet Explorer 11 en revenant à une invite PowerShell de `SConfig`, puis en exécutant la commande suivante :

   PowerShell

   ```
   & "$env:ProgramFiles\Internet Explorer\iexplore.exe"
   ```

> ⓘ **Important**
>
> Le double-clic pour ouvrir les fichiers enregistrés `.htm` localement n'est pas pris en charge. Toutefois, vous pouvez cliquer avec le **bouton droit** et choisir **Ouvrir avec Internet Explorer**, ou vous pouvez l'ouvrir directement à partir d'Internet Explorer en sélectionnant **Fichier**, puis **Ouvrir** et accéder au fichier.

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

Effectuer une mise à niveau sur place de Windows Server

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

Une mise à niveau sur place déplace votre serveur d'une version antérieure de Windows Server vers une version plus récente tout en conservant vos paramètres, rôles serveur et données intacts. Par exemple, vous pouvez effectuer une mise à niveau de Windows Server 2012 R2 vers Windows Server 2025. Lorsque vous effectuez une mise à niveau sur place, votre environnement reste opérationnel sur une version prise en charge avec les dernières fonctionnalités de sécurité et de performance, sans reconstruire.

Cet article explique comment effectuer une mise à niveau à l'aide de Windows Server configuration à partir du support d'installation ou de la mise à jour des fonctionnalités dans Windows Update.

Prerequisites

- Pour déterminer les versions de Windows Server et les chemins de mise à niveau pris en charge, consultez les chemins de mise à niveau sur place pris en charge par version.
- Droits d'administration sur le serveur cible.
- Sauvegarde complète de votre serveur, y compris le système d'exploitation, les applications, les données et toutes les machines virtuelles. Effectuez un test de restauration pour confirmer que la sauvegarde est valide et récupérable. Vous pouvez utiliser Windows Server sauvegarde ou une solution de sauvegarde partenaire.
- Fenêtre de maintenance planifiée, car un temps d'arrêt est nécessaire pendant la mise à niveau.
- Connaissance des éléments suivants :
  - Rôles et fonctionnalités qui prennent en charge une mise à niveau sur place. Consultez Upgrader et migrer des rôles et des fonctionnalités dans Windows Server.
  - Applications serveur Microsoft prises en charge sur Windows Server. Consultez Compatibilité des applications serveur Microsoft pour Windows Server.
  - Exigences de support pour les fournisseurs d'applications autres que Microsoft.

- Serveur qui :
  - Répond ou dépasse les exigences de hardware pour Windows Server.
  - N'est pas regroupé en cluster. Si vous exécutez un cluster, utilisez plutôt la fonctionnalité de mise à jourCluster-Aware ou une mise à niveau propagée du système d'exploitation de cluster .
- Clé de produit et méthode d'activation valides. Les clés et méthodes peuvent varier en fonction du canal de distribution à partir duquel vous avez reçu le support Windows Server, tel qu'un programme de licences commerciales, un canal de vente au détail ou un OEM.
- Emplacement permettant de stocker des fichiers à partir de votre serveur, tels qu'un lecteur flash USB ou un emplacement réseau.
- Si Configuration Manager est installé sur un serveur Windows Server 2012 ou Windows Server 2012 R2, suivez les instructions de prégradation et de post-mise à niveau à Infrastructure locale qui prend en charge Configuration Manager.

> **ⓘ Important**
>
> Bien que la plupart des rôles Windows Server prennent en charge une mise à niveau sur place, domaine Active Directory Contrôleurs sont une exception. Même si une mise à niveau sur place peut fonctionner, ne mettez pas à niveau les serveurs qui exécutent le rôle services de domaine Active Directory. Pour plus d'informations, consultez **Mise à niveau des contrôleurs de domaine vers une version plus récente de Windows Server**.

Selon que vous effectuez une mise à niveau à l'aide d'un support d'installation ou d'un Windows Update, vous devez remplir des conditions préalables supplémentaires. Sélectionnez l'onglet de votre méthode de mise à niveau :

Support d'installation

La méthode de mise à niveau du support d'installation s'applique uniquement aux serveurs non Azure. Pour mettre à niveau Windows Server dans une machine virtuelle Azure, consultez Mise à niveau sur place pour les machines virtuelles exécutant Windows Server dans Azure ou utiliser la méthode Windows Update.

- Support d'installation (image ISO, lecteur USB ou DVD) pour la version de Windows Server vers laquelle vous souhaitez effectuer une mise à niveau.

- Vous pouvez obtenir un support d'installation pour votre version cible de Windows Server à partir d'un fabricant d'équipement d'origine (OEM), d'un canal de distribution au détail, d'un abonnement Visual Studio ou du Centre d'administration Microsoft 365.

Collecter les informations de diagnostic de pré-mise à niveau

Collectez les informations de diagnostic de votre serveur avant la mise à niveau en cas d'échec de la mise à niveau. Stockez les fichiers de diagnostic où vous pouvez y accéder si votre serveur tombe en panne.

Pour collecter vos informations :

1. Ouvrez une invite PowerShell avec élévation de privilèges, notez votre répertoire actif et exécutez les commandes suivantes :

   PowerShell

   ```
   Get-ComputerInfo -Property WindowsBuildLabEx,WindowsEditionID | Out-File -
   FilePath .\computerinfo.txt
   systeminfo.exe | Out-File -FilePath systeminfo.txt
   ipconfig /all | Out-File -FilePath ipconfig.txt
   ```

   La `Get-ComputerInfo` commande nécessite PowerShell 5.1 ou version ultérieure. Si votre version de Windows Server n'inclut pas PowerShell 5.1, ouvrez l'Éditeur de Registre et recherchez les valeurs `BuildLabEx` et `EditionID` sous `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`.

2. Ouvrez l'Explorateur de fichiers, accédez au répertoire que vous avez noté et copiez les fichiers dans un lecteur flash USB ou un emplacement réseau hors de votre ordinateur.

Sauvegardez votre système d'exploitation, vos applications et vos machines virtuelles après avoir collecté vos informations système. Arrêtez ou migrez toutes les machines virtuelles en cours d'exécution sur le serveur. Vérifiez qu'aucune machine virtuelle n'est en cours d'exécution pendant la mise à niveau.

Effectuer la mise à niveau sur place

Vous pouvez effectuer la mise à niveau sur place à l'aide du support d'installation ou de Windows Update. Sélectionnez l'onglet de votre méthode de mise à niveau :

Support d'installation

> **Conseil**
>
> Vous recherchez un moyen de mettre à niveau sans support d'installation ? Utilisez l'onglet Windows Update pour mettre à niveau sans avoir besoin d'un support d'installation.

Exécutez le programme d'installation de Windows Server à partir de votre support d'installation pour effectuer la mise à niveau sur place. Cette procédure s'applique aux serveurs non Azure et non cluster exécutant Windows Server 2012 R2 ou une version ultérieure. Pendant la mise à niveau, votre serveur redémarre plusieurs fois.

Pour effectuer la mise à niveau sur place à l'aide du support d'installation :

1. Montez ou insérez le support d'installation. Ouvrez l'Explorateur de fichiers, accédez à la racine du support d'installation, puis ouvrez `setup.exe`. Par exemple, si vous avez monté une image ISO ou inséré un DVD en tant que lecteur D, le chemin du fichier est `D:\setup.exe`. Si **le contrôle de compte d'utilisateur** vous invite à autoriser le programme d'installation à apporter des modifications, sélectionnez **Oui**.

2. Par défaut, le programme d'installation télécharge automatiquement les mises à jour de l'installation. Si vous êtes d'accord avec les paramètres par défaut, sélectionnez **Suivant** pour continuer.

   Si vous ne souhaitez pas que le programme d'installation télécharge automatiquement les mises à jour, sélectionnez **Modifier la façon dont le programme d'installation télécharge les mises à jour**, sélectionnez l'option appropriée pour votre environnement, puis sélectionnez **Suivant**.

3. Si vous y êtes invité, entrez votre clé de produit, puis sélectionnez **Suivant**.

4. Sélectionnez l'édition de Windows Server que vous souhaitez installer, puis sélectionnez **Next**.

5. Passez en revue les avis applicables et les termes du contrat de licence. Si vous acceptez les termes, sélectionnez **Accepter**.

6. Sélectionnez **Conserver les fichiers, les paramètres et les applications** pour effectuer une mise à niveau sur place, puis sélectionnez **Suivant**.

7. Une fois l'installation terminée l'analyse de votre appareil, elle affiche l'écran **Prêt à installer** . Pour démarrer la mise à niveau sur place, sélectionnez **Installer**.

La mise à niveau sur place démarre et l'écran affiche la progression. Une fois la mise à niveau sur place terminée, votre serveur redémarre.

Vérifier la mise à niveau sur place

Une fois le serveur redémarré, vérifiez la mise à niveau réussie en vérifiant la version Windows Server et en testant vos applications.

1. Ouvrez une invite PowerShell avec élévation de privilèges. Exécutez la commande suivante pour vérifier que la version et l'édition correspondent à ce que vous attendiez.

   PowerShell

   ```
   Get-ComputerInfo -Property WindowsProductName
   ```

2. Vérifiez que toutes les applications s'exécutent et que les connexions clientes réussissent.

Si votre serveur ne fonctionne pas comme prévu après la mise à niveau sur place, analysez les fichiers journaux d'installation dans le répertoire `C:\Windows\Panther`. Téléchargez également l'outil SetupDiag pour analyser les fichiers journaux d'installation.

Si vous avez besoin d'aide technique, contactez Support Microsoft.

Contenu connexe

- Planez votre mise à niveau Windows Server
- Ajouter ou supprimer des rôles et des fonctionnalités
- Vue d'ensemble de la gestion Windows Server
- Commencez avec Windows Admin Center
- Planification de l'activation KMS (Key Management Services)

Last updated on 15/04/2026

Mettre à niveau et migrer des rôles et des fonctionnalités dans Windows Server

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

La mise à niveau ou la migration de rôles et de fonctionnalités dans Windows Server est essentielle pour maintenir la sécurité, les performances et la prise en charge. Cet article fournit une vue d'ensemble des rôles et fonctionnalités pouvant être mis à niveau sur place ou migrés vers un nouveau serveur. Il fournit également des liens vers des guides de migration détaillés pour chaque rôle et fonctionnalité, ainsi que des informations sur les outils de migration Windows Server et le service de migration de stockage. Utilisez ces informations pour planifier une transition fluide vers des versions plus récentes de Windows Server, réduire les temps d'arrêt et garantir une fiabilité continue pour vos charges de travail.

Vous pouvez mettre à jour les rôles et fonctionnalités vers des versions ultérieures de Windows Server de deux façons :

- **Migration:** Déplacez des rôles et des fonctionnalités vers un nouveau serveur exécutant la version plus récente de Windows Server.
- **Mise à niveau sur place :** Installez la nouvelle version de Windows Server sur celle existante, en conservant les rôles et les fonctionnalités en place.

Certains rôles et fonctionnalités prennent en charge les deux méthodes, tandis que d'autres peuvent uniquement prendre en charge la migration.

Vous pouvez migrer de nombreux rôles et fonctionnalités à l'aide des outils de migration Windows Server. Cette fonctionnalité est intégrée à Windows Server et vous aide à déplacer des rôles et des fonctionnalités vers un nouveau serveur. Pour les serveurs de fichiers et le stockage, utilisez le service de migration de stockage.

Les guides de migration prennent en charge les migrations de rôles et de fonctionnalités spécifiés d'un serveur vers un autre (et non des mises à niveau sur place). Sauf indication contraire des guides, vous pouvez migrer entre des ordinateurs physiques et virtuels. Vous pouvez également migrer entre les installations de Windows Server qui utilisent Server avec Expérience utilisateur ou Server Core.

> **Important**
>
> Avant de commencer à migrer des rôles et des fonctionnalités, vérifiez que les serveurs source et de destination exécutent les mises à jour les plus récentes disponibles pour leurs systèmes d'exploitation.

Avant de migrer ou de mettre à niveau vers une nouvelle version de Windows Server, passez en revue la politique de cycle de vie de prise en charge de cette version. Vérifiez que vous comprenez combien de temps il est pris en charge. Vous pouvez rechercher des informations de cycle de vie pour la version spécifique de Windows Server que vous envisagez d'utiliser.

Outils de migration de Windows Server

Windows Server Migration Tools vous permet de migrer des rôles de serveur, des fonctionnalités, des paramètres du système d'exploitation et d'autres données et partages vers des serveurs, y compris les versions ultérieures de Windows Server. Il s'agit d'une fonctionnalité de Windows Server. Elle est donc facilement installée à l'aide de l'Assistant Ajout de rôles et de fonctionnalités, ou de PowerShell. En savoir plus sur l'installation, l'utilisation et la suppression des outils de migration Windows Server.

> **Remarque**
>
> Les migrations entre sous-réseaux à l'aide des outils de migration Windows Server sont disponibles avec Windows Server 2012 et versions ultérieures. Les versions précédentes des Outils de migration Windows Server prennent uniquement en charge les migrations dans le même sous-réseau.

Matrice de mise à niveau et de migration

Agrandir le tableau

Rôle de serveur	Possibilité de mise à niveau sur place ?	Migration prise en charge ?	La migration peut-elle être effectuée sans temps d'arrêt ?
Services de certificats Active Directory	Oui	Oui	Non

Rôle de serveur	Possibilité de mise à niveau sur place ?	Migration prise en charge ?	La migration peut-elle être effectuée sans temps d'arrêt ?
Services de domaine Active Directory	Non recommandé. Utilisez l'installation propre du système d'exploitation pour obtenir des améliorations des performances et des fonctionnalités AD.	Oui	Oui
Services de fédération d'Active Directory	Non	Oui	Non (il faut ajouter de nouveaux nœuds à l'exploitation)
Services AD LDS (Active Directory Lightweight Directory Services)	Oui	Oui	Oui
Services de gestion des droits Active Directory	Oui	Oui	Non
Serveur DHCP	Oui	Oui	Oui
Serveur DNS	Oui	Oui	Non
Clustering de basculement	Oui avec la mise à niveau propagée du système d'exploitation du cluster ou lorsque le serveur est supprimé par le cluster pour la mise à niveau, puis ajouté à un autre cluster.	Oui	Oui pour les clusters de basculement avec des machines virtuelles Hyper-V ou des clusters de basculement exécutant le rôle Serveur de fichiers avec montée en puissance parallèle. Consultez Mise à niveau propagée du système d'exploitation de cluster.
Services de fichiers et de stockage	Oui	Varie selon la sous-fonctionnalité	Non
Hyper-V	Oui avec le processus de mise à niveau propagée du système d'exploitation de cluster	Oui	Oui pour les clusters de basculement avec des machines virtuelles Hyper-V ou des clusters de basculement exécutant le rôle Serveur de fichiers avec montée en puissance parallèle. Consultez Mise

Rôle de serveur	Possibilité de mise à niveau sur place ?	Migration prise en charge ?	La migration peut-elle être effectuée sans temps d'arrêt ?
			à niveau propagée du système d'exploitation de cluster.
Services d'impression et de télécopie	Non	Oui (avec `Printbrm.exe`)	Non
Services de Bureau à distance	Oui, pour tous les sous-rôles, mais la batterie de serveurs en mode mixte n'est pas prise en charge	Oui	Non
Serveur web (IIS)	Oui	Oui	Non
Expérience Windows Server Essentials	Oui	Oui	Non
Windows Server Update Services	Oui	Oui	Non
Dossiers de travail	Oui	Oui	Oui avec le processus de mise à niveau propagée du système d'exploitation de cluster .

Guides de migration

Vous trouverez ci-dessous des liens vers des guides de migration pour des rôles et fonctionnalités Windows spécifiques.

Active Directory

- Migrer l'autorité de certification
- Migrer le service de rôle Federation Services d'Active Directory
- Mise à niveau d'AD RMS vers Windows Server 2016
- Mettre à niveau des contrôleurs de domaine vers une version plus récente de Windows Server
- Guide de migration des services de domaine Active Directory et du serveur DNS

BranchCache

- BranchCache Migration Guide

DHCP

- Migrer le serveur DHCP
- Migrer un déploiement de basculement DHCP existant

Clustering de basculement

- Mettre à niveau un cluster de basculement Windows Server avec une mise à niveau continue du système d'exploitation de cluster
- Mise à niveau des clusters de basculement sur le même matériel
- Migrer des rôles de cluster
- Migrer des services et applications en cluster vers Windows Server 2012

Services de fichiers et de stockage

- Service de migration du stockage
- Migrer des services de fichiers et de stockage
- Mettre à niveau un cluster direct d'espaces de stockage

Hyper-V

- Migrer Hyper-V
- Mettre à niveau la version de la machine virtuelle dans Hyper-V sur Windows ou Windows Server

Serveur de stratégie réseau

- Migrer le serveur de stratégie réseau
- Migrer l'autorité d'inscription de santé

Services d'impression et de numérisation de document

- Migrer les services d'impression et des documents

Services de Bureau à distance

- Migrer les services Bureau à distance
- Migrer vos licences d'accès client des services Bureau à distance (CALs RDS)

Routage et accès à distance

- Vue d’ensemble de la migration VPN DirectAccess vers Always On
- RRAS Migration Guide

Serveur web (IIS)

- Serveur Web (IIS)

Windows Server Update Services

- Migrer Windows Server Update Services vers Windows Server 2012 R2

Autres guides de migration Windows

- Guide de migration d’utilisateurs et de groupes locaux
- IP Configuration Migration Guide

Last updated on 28/04/2026

Convertir les éditions de Windows Server et les types de licences

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

Après avoir installé Windows Server, vous pouvez effectuer une conversion entre les éditions (par exemple, l'évaluation en vente au détail ou Standard en centre de données) et basculer entre les types de licences (vente au détail, licence en volume et OEM). Cet article fournit des procédures pas à pas pour chaque scénario de conversion.

Pour plus d'informations sur les chemins et restrictions de mise à niveau sur place pris en charge, consultez Planez votre mise à niveau Windows Server.

Prerequisites

Avant de convertir votre Windows Server édition ou votre type de licence, vérifiez que vous disposez des points suivants :

- Clé de produit pour l'édition cible ou le type de licence.
- Invite de commandes avec élévation de privilèges ou session PowerShell sur le serveur que vous souhaitez convertir.
- Accès administratif au serveur.

Conversion d'une version d'évaluation en version commerciale

Vous pouvez convertir les versions d'évaluation et les éditions de Windows Server en versions et éditions commerciales. Par exemple, si vous installez la version d'évaluation de l'édition Standard (Expérience utilisateur), vous pouvez la convertir en version commerciale de l'édition Standard (Expérience de bureau) ou de l'édition Datacenter (Expérience de bureau).

Toutefois, vous ne pouvez pas convertir toutes les versions et éditions d'évaluation Windows Server en toutes versions ou éditions commerciales. Par exemple, si vous installez l'édition centre de données d'évaluation, vous pouvez uniquement la convertir en édition centre de données de vente au détail, et non pas en édition standard de vente au détail.

Comme Windows Server 2016, vous ne pouvez pas convertir les versions d'évaluation de l'expérience utilisateur en versions de vente au détail Core. Si vous installez la version d'évaluation Standard Core, vous ne pouvez la convertir qu'en version commerciale Datacenter Core, et non en version commerciale Standard Core.

Il est important d'exécuter la commande `DISM /online /Get-TargetEditions` comme indiqué dans la procédure suivante pour déterminer les versions commerciales vers lesquelles vous pouvez effectuer la conversion. Si la version commerciale que vous souhaitez n'est pas répertoriée comme version cible, vous devrez procéder à une nouvelle installation de la version commerciale souhaitée.

> ⓘ **Remarque**
>
> Pour vérifier que votre serveur exécute une version d'évaluation, vous pouvez exécuter l'une des commandes suivantes à partir d'une invite de commande avec élévation de privilèges :
>
> - Exécutez `DISM /online /Get-CurrentEdition` et vérifiez que le nom de l'édition actuelle inclut `Eval`.
> - Exécutez `slmgr.vbs /dlv` et vérifiez que la sortie inclut `EVAL`.

Si Windows n'est pas activé, le coin inférieur droit du bureau affiche le temps restant dans la période d'évaluation.

Windows Server Standard ou Datacenter

Si votre serveur exécute une version d'évaluation de Windows Server édition Standard ou Datacenter, vous pouvez la convertir en version commerciale disponible. Exécutez les commandes suivantes dans une invite de commandes avec élévation de privilèges ou une session PowerShell.

1. Déterminez le nom de l'édition actuelle en exécutant la commande suivante. La sortie est une forme abrégée du nom de l'édition. Par exemple, Windows Server Datacenter Édition d'évaluation (Desktop Experience) est `ServerDatacenterEval`.

   Invite de commandes Windows

   ```
   DISM /online /Get-CurrentEdition
   ```

2. Vérifiez dans quelles éditions l'installation actuelle peut être convertie en exécutant la commande suivante. À partir de la sortie, notez le nom de l'édition vers lequel vous souhaitez effectuer la conversion.

   Invite de commandes Windows

   ```
   DISM /online /Get-TargetEditions
   ```

3. Exécutez la commande suivante pour enregistrer le Termes du contrat de licence logiciel Microsoft pour Windows Server, que vous pouvez ensuite examiner. Remplacez l'espace réservé `<target edition>` par le nom d'édition que vous avez noté à l'étape précédente.

   Invite de commandes Windows

   ```
   DISM /online /Set-Edition:<target edition> /GetEula:C:\license.rtf
   ```

4. Saisissez le nom de la nouvelle édition et la clé de produit correspondante dans la commande suivante. Le processus de définition vous oblige à accepter les "Conditions de licence logicielle Microsoft" pour Windows Server que vous avez enregistrés précédemment.

   Invite de commandes Windows

   ```
   DISM /online /Set-Edition:<target edition> /ProductKey:<product key>
   /AcceptEula
   ```

   Par exemple:

   Invite de commandes Windows

   ```
   DISM /online /Set-Edition:ServerDatacenter /ProductKey:ABCDE-12345-ABCDE-
   12345-ABCDE /AcceptEula
   ```

Conseil

Pour plus d'informations sur Dism.exe, consultez DISM Command-line options (Options de ligne de commande DISM).

Important

Vous ne pouvez pas convertir un contrôleur de domaine Active Directory d'une évaluation en version commerciale. Dans ce cas, installez un autre contrôleur de domaine sur un serveur qui exécute une version commerciale. Migrez ensuite tous les rôles FSMO détenus par le contrôleur de domaine d'évaluation. Enfin, supprimez services de domaine Active Directory (AD DS) du contrôleur de domaine qui s'exécute sur la version d'évaluation. Pour plus d'informations, consultez Mettre à niveau les contrôleurs de domaine vers Windows Server.

Windows Server Essentials

Si le serveur exécute Windows Server Essentials, vous pouvez le convertir en version commerciale complète en entrant une clé de vente au détail, une licence en volume ou une clé OEM dans la commande suivante à l'invite de commandes avec élévation de privilèges :

Invite de commandes Windows

```
slmgr.vbs /ipk <license key>
```

Convertir Windows Server édition Standard en édition Datacenter

À tout moment après l'installation de Windows Server, vous pouvez convertir Windows Server édition Standard en édition Datacenter. Vous pouvez également exécuter `setup.exe` à partir du support d'installation pour mettre à niveau ou réparer l'installation (procédure parfois appelée « réparation sur place »). Si vous exécutez `setup.exe` pour mettre à niveau sur place ou réparer sur n'importe quelle édition de Windows Server, le résultat est la même édition avec laquelle vous avez commencé.

Vous pouvez convertir l'édition Standard de Windows Server en édition Datacenter comme suit :

1. Déterminez que Windows Server Standard est le nom de l'édition actuelle en exécutant la commande suivante. La sortie est une forme abrégée du nom de l'édition, par exemple Windows Server édition Standard (Expérience utilisateur) est `ServerStandard`.

   Invite de commandes Windows

   ```
   DISM /online /Get-CurrentEdition
   ```

2. Vérifiez que Windows Server Datacenter est une option valide à convertir en exécutant la commande suivante :

   Invite de commandes Windows

   ```
   DISM /online /Get-TargetEditions
   ```

3. Entrez `ServerDatacenter` et la clé de votre produit commercial dans la commande suivante :

   Invite de commandes Windows

   ```
   DISM /online /Set-Edition:ServerDatacenter /ProductKey:<product key>
   /AcceptEula
   ```

Conversion entre licence commerciale, licence en volume et licence OEM

À tout moment, après l'installation de Windows Server, vous pouvez convertir librement une licence commerciale, une licence sous licence en volume ou une licence OEM. L'édition (Standard ou Datacenter) reste la même pendant cette conversion. Si vous commencez par une version d'évaluation, convertissez-la en version commerciale en premier, puis convertissez-la entre les versions en exécutant la commande suivante à partir d'une invite de commandes avec élévation de privilèges. Fournissez votre clé de licence en volume, de version commerciale ou de version OEM.

Invite de commandes Windows

```
slmgr.vbs /ipk <product key>
```

Contenu connexe

Pour plus d'informations sur la mise à niveau de Windows Server, consultez les articles suivants :

- Overview des mises à niveau Windows Server
- Différences entre les options d'installation Server Core et Server avec expérience de bureau
- Performer une mise à niveau sur place de Windows Server

- Mise à niveau sur place pour les machines virtuelles exécutant Windows Server dans Azure

---

Last updated on 15/04/2026

Activation automatique de machine virtuelle dans Windows Server

16/08/2025

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

L'activation automatique d'ordinateur virtuel (AVMA) joue le rôle de mécanisme de preuve d'achat qui permet de garantir que les produits Windows sont utilisés conformément aux droits d'utilisation de logiciels et termes du contrat de licence logiciel Microsoft. AVMA vous permet d'activer des machines virtuelles Windows Server sur un hôte Windows Server Hyper-V correctement activé, même dans des environnements déconnectés. AVMA lie l'activation de la machine virtuelle à l'hôte de virtualisation sous licence et active la machine virtuelle lorsqu'il démarre. Lorsque vous utilisez AVMA, vous pouvez obtenir des rapports en temps réel sur l'utilisation et des données d'historique sur l'état de licence de la machine virtuelle. Les rapports et données de suivi sont disponibles sur l'hôte de virtualisation.

Applications pratiques

Sur les hôtes de virtualisation, AVMA offre plusieurs avantages. Les responsables de centres de données de serveur peuvent utiliser AVMA pour effectuer les tâches suivantes :

- Activer des machines virtuelles dans des emplacements distants.
- Activer des machines virtuelles avec ou sans connexion Internet.
- Suivre l'utilisation et les licences de machines virtuelles à partir de l'hôte de virtualisation, sans exiger de droits d'accès sur les systèmes virtualisés.

Les partenaires de contrat de licence de fournisseur de service (SPLA, Service Provider License Agreement) et d'autres fournisseurs d'hébergement n'ont pas besoin de partager les clés de produits avec des locataires ou d'accéder à la machine virtuelle d'un locataire pour l'activer. L'activation de la machine virtuelle est transparente pour le locataire quand AVMA est utilisée. Les fournisseurs d'hébergement peuvent utiliser les journaux serveur pour vérifier la conformité des licences et suivre l'historique de l'utilisation des clients.

Configuration système requise

Pour exécuter des machines virtuelles invitées sur un hôte de serveur de virtualisation, vous devez activer l'hôte. Vous pouvez obtenir des clés d'activation de l'hôte auprès du Centre d'administration Microsoft 365 ou de votre fournisseur OEM.

> **Notes**
>
> Dans un cluster de basculement, chaque hôte de serveur virtualisation du cluster doit être activé pour que les machines virtuelles invitées restent activées, quel que soit le serveur sur lequel elles s'exécutent.

AVMA nécessite une version Windows Server Datacenter avec le rôle hôte Hyper-V installé. La version de Windows Server de l'hôte détermine les versions qu'il peut activer dans une machine virtuelle invitée. Le tableau suivant répertorie les versions de machines virtuelles invitées que chaque version hôte peut activer. Une version hôte peut accéder à toutes les éditions (Datacenter, Standard ou Essentials) de ses versions de machines virtuelles invitées éligibles.

Agrandir le tableau

Version du serveur hôte	Machine virtuelle invitée Windows Server 2025	Machine virtuelle invitée Windows Server 2022	Machine virtuelle invitée Windows Server 2019	Machine virtuelle invitée Windows Server 2016	Machine virtuelle invitée Windows Server 2012 R2
Windows Server 2025	X	X	X	X	X
Windows Server 2022		X	X	X	X
Windows Server 2019			X	X	X
Windows Server 2016				X	X
Windows Server 2012 R2					X

> **Notes**
>
> AVMA ne fonctionne pas avec d'autres technologies de virtualisation de serveur.

Comment implémenter AVMA

Pour activer des machines virtuelles avec AVMA, vous utilisez une clé AVMA générique (détaillée dans les clés AVMA) qui correspond à la version de Windows Server que vous souhaitez activer. Pour créer une machine virtuelle et l'activer avec une clé AVMA, suivez ces étapes :

1. Sur le serveur qui héberge les machines virtuelles, installez et configurez le rôle Microsoft Hyper-V Server. Vérifiez que le serveur est correctement activé. Pour plus d'informations, consultez Installer Hyper-V Server.

2. Créez une machine virtuelle et installez un système d'exploitation Windows Server pris en charge dessus.

   > **ⓘ Important**
   >
   > Le service d'intégration Échange de données (également appelé Échange de paires clé-valeur) doit être activé dans les paramètres de la machine virtuelle pour que fonctionne AVMA. Elle est activée par défaut pour les nouvelles machines virtuelles.

3. Après avoir installé Windows Server sur la machine virtuelle, installez la clé AVMA sur la machine virtuelle. À partir de PowerShell ou d'une invite de commandes avec élévation de privilèges, exécutez la commande suivante :

   ```
   slmgr /ipk <AVMA_key>
   ```

La machine virtuelle s'active automatiquement, à condition que l'hôte de virtualisation soit lui-même activé.

> **Conseil**
>
> Vous pouvez également ajouter les clés AVMA dans tout fichier d'installation sans assistance.

Clés AVMA

Windows Server 2025

Agrandir le tableau

Edition	Key
Datacenter	YQB4H-NKHHJ-Q6K4R-4VMY6-VCH67

Edition	Key
Datacenter: Édition Azure	6NMQ9-T38WF-6MFGM-QYGYM-88J4F
Standard	WWVGQ-PNHV9-B89P4-8GGM9-9HPQ4

Rapports et suivi

L'échange de paires clé-valeur entre l'hôte de virtualisation et la machine virtuelle fournit des données de suivi en temps réel pour les systèmes d'exploitation invités, notamment des informations d'activation. Ces informations d'activation sont stockées dans le registre Windows de la machine virtuelle. Les données d'historique relatives aux demandes AVMA sont consignées dans l'observateur d'événements sur l'hôte de virtualisation.

Pour plus d'informations sur KVP, consultez Exchange de données : Utilisation de paires clé/valeur pour partager des informations entre l'hôte et l'invité sur Hyper-V.

> **Important**
>
> Les données KVP ne sont pas sécurisées. Elle peut être modifiée et n'est pas surveillée pour les modifications. Les données de la paire KVP doivent être supprimées si la clé AVMA est remplacée par une autre clé de produit (clé commercialisée, OEM ou de licence en volume).

Puisque le processus d'activation AVMA est transparent, les messages d'erreur ne s'affichent pas. Toutefois, les requêtes AVMA sont également enregistrées sur l'hôte de virtualisation dans l'Observateur d'événements dans le journal des applications avec l'ID d'événement **12310** et sur la machine virtuelle avec l'ID d'événement **12309**. Les événements suivants sont capturés sur les machines virtuelles :

Agrandir le tableau

Notification	Description
Réussite AVMA	La machine virtuelle a été activée.
Hôte non valide	L'hôte de virtualisation ne répond pas. Cette situation peut se produire lorsque le serveur n'exécute pas une version de Windows prise en charge.
Données non valides	Cet événement résulte généralement d'un échec de communication entre l'hôte de virtualisation et la machine virtuelle, souvent provoqué par un endommagement, un chiffrement ou une incompatibilité des données.

Notification	Description
Activation refusée	L'hôte de virtualisation n'a pas pu activer le système d'exploitation invité, car l'ID AVMA ne correspond pas.

Planification de l'activation des services de gestion de clés (KMS)

21/06/2025

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

Les informations suivantes soulignent les considérations de planification initiales que vous devez passer en revue pour l'activation basée sur le service de gestion de clés (KMS, Key Management Service).

Les services KMS utilisent un modèle client-serveur pour activer les clients, et sont utilisés pour l'activation en volume. Les clients KMS se connectent à un serveur KMS, nommé hôte KMS, pour l'activation. L'hôte KMS doit résider sur votre réseau local.

Les hôtes KMS n'ont pas besoin d'être des serveurs dédiés et le service KMS peut être co-hébergé avec d'autres services. Vous pouvez exécuter un hôte KMS sur n'importe quel système physique ou virtuel exécutant un système d'exploitation client Windows ou Windows Server pris en charge. Un hôte KMS s'exécutant sur un système d'exploitation Windows Server peut activer les ordinateurs exécutant à la fois des systèmes d'exploitation serveur et client. Toutefois, un hôte KMS s'exécutant sur un système d'exploitation client Windows ne peut activer que les ordinateurs exécutant également des systèmes d'exploitation clients.

Pour utiliser KMS, un hôte KMS a besoin d'une clé pour s'activer ou s'authentifier auprès de Microsoft. Cette clé est parfois appelée clé d'hôte KMS, mais elle est officiellement connue sous le nom de clé de licence en volume spécifique au client Microsoft (CSVLK). Vous pouvez obtenir cette clé à partir de la section Clés de produit du Centre de gestion des licences en volume pour les contrats suivants : Open, Open Value, Select, Entreprise et Licence pour fournisseur de services. Vous pouvez également obtenir une assistance en contactant votre Centre d'activation Microsoft local.

Exigences opérationnelles

Le service KMS peut activer des ordinateurs physiques et virtuels, mais pour autoriser l'activation basée sur le service KMS, un réseau doit comporter un nombre minimal d'ordinateurs physiques (nommé seuil d'activation). Les clients KMS effectuent l'activation une fois seulement que ce seuil est atteint. Pour vérifier que ce seuil d'activation est atteint, un hôte KMS compte le nombre d'ordinateurs physiques qui demandent une activation sur le réseau.

Les hôtes KMS comptent les connexions plus récentes. Lorsqu'un client ou un serveur contacte l'hôte KMS, ce dernier ajoute l'ID de l'ordinateur à son comptage, puis renvoie cette valeur

dans sa réponse. Le client ou le serveur s'active si ce nombre est assez élevé. Les clients s'activent si ce nombre est supérieur ou égal à 25. Les serveurs et les éditions en volume de produits Microsoft Office s'activent si ce nombre est supérieur ou égal à 5. Le service KMS ne compte que les connexions uniques dans les 30 derniers jours et ne stocke que les 50 contacts les plus récents.

Les activations KMS sont valides pendant 180 jours, une période appelée intervalle de validité de l'activation. Les clients KMS doivent renouveler leur activation en se connectant à l'hôte KMS au moins une fois tous les 180 jours pour rester activés. Par défaut, les ordinateurs clients KMS tentent de renouveler leur activation tous les sept jours. Une fois que l'activation d'un client a été renouvelée, l'intervalle de validité de l'activation est réinitialisé.

Un hôte KMS individuel peut prendre en charge un nombre illimité de clients KMS. Si vous possédez plus de 50 clients, nous vous recommandons au moins deux hôtes KMS au cas où le premier devienne indisponible. La plupart des organisations peuvent fonctionner avec pas plus de deux hôtes KMS pour leur infrastructure complète.

Une fois que le premier hôte KMS a été activé, la clé CSVLK utilisée sur le premier hôte peut être utilisée pour activer jusqu'à cinq hôtes KMS supplémentaires sur votre réseau (pour un total de six hôtes). Une fois qu'un hôte KMS a été activé, les administrateurs peuvent réactiver le même hôte jusqu'à neuf fois avec la même clé.

Si votre organisation a besoin de plus de six hôtes KMS, vous pouvez demander d'autres activations pour le CSVLK de votre organisation. Par exemple, si vous avez 10 emplacements physiques sous un contrat de licence en volume et que vous souhaitez que chaque emplacement dispose d'un hôte KMS local. Pour demander une telle exception, contactez votre Centre d'activation Microsoft.

Les ordinateurs qui exécutent des éditions de licence en volume de Windows Server et de client Windows sont, par défaut, des clients KMS qui ne nécessitent pas de configuration supplémentaire.

Si vous convertissez un ordinateur ayant le statut d'hôte KMS, de clé d'activation multiple (MAK) ou d'une version commerciale de Windows en un client KMS, l'installation de la clé de configuration de client KMS applicable est nécessaire. Pour plus d'informations, consultez Clés d'installation de client KMS.

Conditions requises en matière de réseau

L'activation basée sur le service KMS requiert la connectivité TCP/IP. Les clients et les hôtes KMS sont configurés par défaut pour utiliser le système DNS (Domain Name System). Les hôtes KMS utilisent les mises à jour dynamique DNS pour publier automatiquement les informations

que les clients KMS doivent trouver et s'y connecter. Vous pouvez accepter ces paramètres par défaut ou, si vous avez une configuration requise spéciale de sécurité et de réseau, vous pouvez configurer manuellement les clients et les hôtes KMS.

Par défaut, un hôte KMS est configuré pour utiliser TCP sur le port 1688.

Versions d'activation

Le tableau suivant récapitule les versions de client et d'hôte KMS pour les réseaux qui incluent des appareils Windows Server et clients Windows.

> **Important**
>
> Des mises à jour de Windows peuvent être requises sur le serveur KMS pour prendre en charge l'activation des clients plus récents. Si vous recevez des erreurs d'activation, vérifiez que vous disposez des mises à jour appropriées répertoriées dans le tableau ci-dessous.

Windows Server 2025

Agrandir le tableau

Groupe CSVLK	CSVLK peut être hébergé sur	les éditions Windows activées par cet hôte KMS
Licence en volume pour Windows Server 2025	• Windows Server 2025[1] • Windows Server 2022[1] • Windows Server 2019	• Windows Server 2025 (toutes éditions) • Windows Server 2022 (toutes éditions) • Canal semi-annuel Windows Server • Windows Server 2019 (toutes éditions) • Windows Server 2016 (toutes éditions) • Windows Server 2012 R2 (toutes éditions) • Windows Server 2012 (toutes éditions) • Windows Server 2008 R2 (toutes éditions) • Windows Server 2008 (toutes éditions) • Windows 11 Entreprise LTSC 2024 • Windows 11 Entreprise/Entreprise N • Windows 11 Professionnel/Professionnel N • Windows 11 Professionnel pour les stations de travail/Professionnel N pour les stations de travail • Windows 11 pour l'Éducation/Éducation N • Windows 10 Entreprise LTSC/LTSC N/LTSB • Windows 10 Entreprise/Entreprise N • Windows 10 Professionnel/Professionnel N

Groupe CSVLK	CSVLK peut être hébergé sur	les éditions Windows activées par cet hôte KMS
		• Windows 10 Professionnel pour les stations de travail/Professionnel N pour les stations de travail • Windows 10 pour l'Éducation/Éducation N • Windows 8.1 Enterprise • Windows 8.1 Professionnel • Windows 7 Entreprise • Windows 7 Professionnel

1. Azure active Windows Server Datacenter : édition Azure, ce qui signifie qu'il ne peut pas être configuré en tant qu'hôte KMS

Mises à jour de l'hôte KMS nécessaires

Selon le système d'exploitation exécuté par votre hôte KMS et les systèmes d'exploitation que vous souhaitez activer, vous devrez peut-être installer une ou plusieurs des mises à jour suivantes. Les mises à jour sont requises lorsque vous souhaitez activer une version de Windows plus récente que la version exécutée par votre hôte KMS.

> **Notes**
>
> Les mises à jour répertoriées sont le minimum requis. Lorsque des mises à jour cumulatives ultérieures ou des correctifs cumulatifs mensuels sont répertoriés en option, installez la dernière version disponible pour votre système d'exploitation afin de bénéficier de la sécurité et d'autres correctifs.

Agrandir le tableau

Version du système d'exploitation de l'hôte KMS	Version(s) du système d'exploitation du client KMS à activer	Mise à jour requise
Windows Server 2022	- Windows Server 2025	13 février 2024 - KB5034765 ou mise à jour cumulative plus récente
Windows Server 2019	- Windows Server 2025 (en anglais seulement) - Windows Server 2022	13 février 2024 - KB5034768 ou mise à jour cumulative plus récente 8 juin 2021 - KB5003646 ou mise à jour cumulative plus récente

Version du système d'exploitation de l'hôte KMS	Version(s) du système d'exploitation du client KMS à activer	Mise à jour requise
Windows Server 2016	- Windows Server 2022 - Windows Server 2019	8 juin 2021 - KB5003638 ou mise à jour cumulative plus récente
Windows Server 2016	- Windows Server 2019	3 décembre 2018 - KB4478877 ou mise à jour cumulative plus récente
Windows Server 2012 R2	- Windows Server 2019 - Windows Server 2016 - Windows 10	27 novembre 2018 - KB4467695 (préversion du correctif cumulatif mensuel) ou correctif cumulatif mensuel plus récent
Windows Server 2012 R2	- Windows Server 2016 - Windows 10	Correctif cumulatif de mise à jour de juillet 2016 pour Windows 8.1 et Windows Server 2012 R2 ou correctif cumulatif mensuel plus récent
Windows Server 2012	- Windows Server 2016 – Windows Server 2012 R2 - Windows 10	Correctif cumulatif de mise à jour de juillet 2016 pour Windows 2012 ou correctif cumulatif mensuel plus récent
Windows Server 2008 R2	– Windows Server 2012 R2 – Windows Server 2012 - Windows 10	Mise à jour qui permet aux hôtes KMS Windows 7 et Windows Server 2008 R2 d'activer Windows 10.
Windows 8.1	- Windows 10	Correctif cumulatif de mise à jour de juillet 2016 pour Windows 8.1 et Windows Server 2012 R2 ou correctif cumulatif mensuel plus récent
Windows 7	- Windows 10	Mise à jour qui permet aux hôtes KMS Windows 7 et Windows Server 2008 R2 d'activer Windows 10.

Renforcer l’activation des services de gestion des clés (KMS) grâce à une confiance matérielle

S’applique à: ✅ Windows Server 2025

L’activation de Hardware-Secured KMS est une forme renforcée d’activation en volume des Key Management Services (KMS) qui utilise l’attestation du Trusted Platform Module (TPM) 2.0 pour confirmer que les demandes d’activation proviennent d’environnements de confiance et supportés matériellement. Il lie l’activation à l’intégrité de l’appareil, ce qui atténue l’usurpation et aide à garantir que seuls les hôtes vérifiés et validés participent à l’activation.

Un hôte KMS qui n’est pas sécurisé matériellement dépend uniquement du logiciel pour valider l’activation, ce qui expose votre environnement davantage à des hôtes KMS non vérifiés ou émulés.

À partir de la mise à jour cumulative 2026-08 pour Windows Server 2025, la messagerie de préparation des hôtes KMS vous indique si un hôte répond aux exigences de sécurité matérielles, afin que vous puissiez vérifier et préparer votre environnement. Les changements d’activation qui reposent sur la confiance matérielle s’appliquent aux futures versions de Windows Server. Pour en savoir plus, voir Renforcer le service de gestion des clés (KMS) avec la confiance matérielle.

Après avoir lu cet article, vous pouvez identifier si un hôte KMS est sécurisé matériellement, comprendre en quoi il diffère d’un hôte qui ne l’est pas, et connaître les exigences que votre environnement doit satisfaire.

Fonctionnement de l’activation Hardware-Secured KMS

L’activation de Hardware-Secured KMS utilise l’attestation TPM 2.0 pour établir la confiance dans l’hôte KMS avant qu’il ne participe à l’activation. Le TPM fournit une mesure matérielle de l’hôte, et l’attestation valide cette mesure afin que les demandes d’activation proviennent d’un environnement fiable et vérifié.

L’attestation TPM fonctionne en trois parties :

- **Identité matérielle** : L’hôte KMS utilise une attestation soutenue par TPM pour prouver son identité matérielle, que Microsoft vérifie avant que l’hôte n’active les appareils.

- **Intégrité de la plateforme** : Le TPM confirme l'intégrité de l'hôte KMS.
- **Flux d'activation** : Après vérification, l'hôte KMS sert de manière sécurisée les demandes d'activation pour les appareils Windows.

Cette approche lie l'activation à un hôte de confiance, et non seulement à une configuration logicielle que quelqu'un peut copier ou usurper.

Parce que le matériel de l'appareil ancre la confiance plutôt que la seule configuration logicielle, KMS Hardware-Secured activation :

- Lie l'activation à l'intégrité de l'appareil.
- Résiste à toute altération en liant les secrets d'activation au matériel.
- Atténue l'usurpation et l'utilisation d'hôtes KMS émulés ou non vérifiés.
- Assure une activation perpétuelle sans renouvellement périodique.

Hôtes sécurisés matériellement KMS et KMS non sécurisés matériellement

Un hôte KMS opère dans l'un des deux États. Un hôte sécurisé matériellement KMS ajoute une racine de confiance matérielle, tandis qu'un hôte KMS non sécurisé matériellement repose uniquement sur le logiciel. Comprendre la différence vous aide à planifier le bon chemin pour votre environnement.

Agrandir le tableau

Aspect	Hôte sécurisé matériellement KMS	KMS non est un hôte sécurisé matériellement
Fondement de la confiance	Racine matérielle de confiance établie via l'attestation TPM 2.0.	Uniquement logiciel, ce qui est vulnérable à l'usurpation.
Configuration matérielle requise	TPM 2.0 installé et activé.	None.
Renouvellement de l'activation	Activation perpétuelle sans renouvellement nécessaire.	Activation standard de KMS sur Windows Server 2025. Une future version de Windows Server pourrait nécessiter un renouvellement périodique.
Quand utiliser	État recommandé, pour la confiance d'activation la plus forte et le moins d'entretien continu.	Transition d'état, pendant que vous préparez le matériel et terminez le passage vers un hôte sécurisé matériellement KMS.

Quand choisir un hôte sécurisé matériellement KMS

Un hôte *sécurisé matériellement KMS* est l'état recommandé. Cet hôte utilise l'attestation TPM 2.0 pour établir une confiance matérielle et assure une activation perpétuelle sans renouvellement. Choisissez cet état lorsque vous souhaitez le trust d'activation le plus fort et le moins d'entretien continu.

À quoi s'attendre d'un hôte KMS non sécurisé matériellement

Un hôte KMS non sécurisé matériellement utilise l'activation standard de KMS sur Windows Server 2025 et continue d'activer les clients comme il le fait aujourd'hui. Dans une future version de Windows Server, un hôte non sécurisé matériellement pourrait nécessiter un renouvellement périodique pour maintenir les clients activés. Préparez votre matériel dès maintenant à adopter une activation sécurisée par le matériel KMS avant ce changement. Pour en savoir plus, voir Renforcer le service de gestion des clés (KMS) avec la confiance matérielle.

Exigences pour un hôte sécurisé matériellement KMS

Pour fonctionner en tant qu'hôte sécurisé matériellement KMS, un serveur doit répondre à toutes les exigences suivantes :

- L'hôte dispose d'une puce TPM 2.0 installée et activée.
- Le matériel serveur est certifié dans le catalogue Windows Server.

Préparation de l'environnement pour une activation sécurisée matériellement KMS

Pour vous préparer à l'activation sécurisée par le matériel KMS, évaluez ce que vous avez aujourd'hui, surveillez les signaux de préparation et planifiez les modifications matérielles nécessaires.

Évalue ta configuration KMS actuelle

Commencez par comprendre votre infrastructure KMS existante afin de savoir quels hôtes sont déjà éligibles et quels changements nécessitent :

- Inventez vos hôtes KMS, qu'ils soient physiques et virtuels.
- Vérifiez que chaque hôte dispose d'une puce TPM 2.0 installée et activée.

- Confirmez que le matériel serveur de chaque hôte est certifié dans le catalogue Windows Server.

Pour confirmer qu'un hôte supporte la capacité d'attestation TPM, exécutez la commande suivante dans une session PowerShell élevée :

PowerShell

```powershell
Get-TpmSupportedFeature -FeatureList "Key Attestation"
```

Une réponse qui montre `Key Attestation` confirme que le serveur prend en charge la capacité d'attestation TPM pour l'activation de KMS Hardware-Secured.

Signaux de préparation du moniteur

À partir de la mise à jour cumulative 2026-08 pour Windows Server 2025, la messagerie de préparation des hôtes KMS vous aide à planifier à l'avance. Ce message est informatif et n'affecte pas l'activation. Les clients continuent d'activer comme ils le font aujourd'hui. La messagerie montre quels hôtes répondent déjà aux exigences de sécurité matérielles, afin que vous puissiez vous préparer à une activation Hardware-Secured KMS dans une future version de Windows Server. Pour en savoir plus sur ce changement, voir Renforcer le service de gestion des clés (KMS) avec la confiance matérielle.

Les signaux de préparation apparaissent sur deux surfaces :

- **Ligne de commande** : L'exécution `slmgr /dlv` affiche soit « Cet appareil est éligible pour servir d'hôte KMS avec une sécurité matérielle. » soit « Cet appareil ne répond pas aux exigences pour utiliser un hôte KMS avec une sécurité matérielle. »
- **Journaux d'événements** : Les entrées d'avertissement apparaissent sous **Applications et Services Journaux**>**de Clés Service de gestion des clés**.

Planifiez votre transition matérielle

Pour les hôtes qui ne sont pas encore éligibles, planifiez les changements qui les déplacent vers un État de Hardware-Secured KMS :

- Installez et activez TPM 2.0 sur des hôtes qui ne l'ont pas.
- Passez à du matériel certifié Windows Server lorsque le matériel actuel n'est pas certifié.
- Validez la préparation après avoir effectué des modifications matérielles pour confirmer que l'hôte est un hôte KMS Hardware-Secured.

Contenu connexe

- Planification de l'activation KMS (Key Management Services)
- Créer un hôte d'activation des Services de gestion des clés (KMS)
- Renforcer le service de gestion des clés (KMS) avec une confiance matérielle (Windows IT Pro Blog)

ⓘ**Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Last updated on 13/08/2026

Créer un hôte d'activation KMS (Key Management Services)

16/08/2025

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

Key Management Services (KMS) utilise un modèle client-serveur pour activer les clients Windows. KMS est utilisé pour l'activation en volume sur votre réseau local. Les clients KMS se connectent à un serveur KMS, appelé hôte KMS, pour l'activation. Les clients KMS qu'un hôte KMS peut activer dépendent de la clé hôte utilisée pour activer l'hôte KMS.

Cet article vous guide tout au long des étapes à suivre pour créer un hôte KMS. Pour plus d'informations sur kmS et les considérations relatives à la planification initiale, consultez la planification de l'activation des services de gestion des clés (KMS).

Prerequisites

Un seul hôte KMS peut prendre en charge un nombre illimité de clients KMS. Si vous avez plus de 50 clients, nous vous recommandons d'avoir au moins deux hôtes KMS si l'un de vos hôtes KMS devient indisponible. La plupart des organisations peuvent fonctionner avec quelques hôtes KMS pour l'ensemble de leur infrastructure.

Les hôtes KMS n'ont pas besoin d'être des serveurs dédiés. Vous pouvez héberger d'autres services sur un hôte KMS. Vous pouvez exécuter un hôte KMS sur n'importe quel système physique ou virtuel qui exécute un système d'exploitation client Windows Server ou Windows pris en charge.

La version de Windows que vous utilisez pour votre hôte KMS détermine la version de Windows que vous pouvez activer pour vos clients KMS. Pour obtenir de l'aide sur la détermination de la version appropriée pour votre environnement, consultez la table des versions d'activation.

Par défaut, LES hôtes KMS publient des enregistrements de ressources de service (SRV) dans votre système de noms de domaine (DNS). Par conséquent, les clients KMS peuvent détecter automatiquement l'hôte KMS et l'activer sans avoir besoin de configuration sur le client KMS. Vous pouvez désactiver la publication automatique et créer les enregistrements manuellement. Ces étapes sont nécessaires pour l'activation automatique si le service DNS ne prend pas en charge les mises à jour dynamiques.

Pour créer un hôte KMS, vous avez besoin des conditions préalables suivantes :

- Un ordinateur exécutant Windows Server ou Windows. Un hôte KMS s'exécutant sur Windows Server peut activer les ordinateurs exécutant à la fois des systèmes d'exploitation serveur et client. Toutefois, un hôte KMS s'exécutant sur un système d'exploitation client Windows ne peut activer que les ordinateurs exécutant également des systèmes d'exploitation clients.
- Un compte d'utilisateur membre du groupe Administrateurs sur l'hôte KMS.
- Les versions kmS et clientes qui sont compatibles les unes avec les autres et une version Windows qui peut héberger KMS. Pour plus d'informations, consultez la planification de l'activation kmS (Key Management Services).
- Clé d'hôte KMS pour votre organisation. Vous pouvez obtenir cette clé à partir du Centre d'administration Microsoft 365. Pour plus d'informations, consultez Rechercher et utiliser des clés de produit pour la gestion des licences en volume.
- Accès à Internet pour activer l'hôte KMS ou effectuer une activation par téléphone.

Installer et configurer un hôte KMS

Pour installer et configurer un hôte KMS, procédez comme suit.

Installer le rôle Services d'activation en volume

Pour installer le rôle Services d'activation en volume, exécutez la commande suivante dans une session PowerShell avec élévation de privilèges :

PowerShell

```
Install-WindowsFeature -Name VolumeActivation -IncludeManagementTools
```

Configurer le pare-feu Windows

Configurez le Pare-feu Windows pour autoriser KMS à recevoir le trafic réseau. Vous pouvez autoriser ce trafic pour tous les profils réseau, qui est le paramètre par défaut, ou pour n'importe quelle combinaison de profils de domaine, privé et réseau public. Par défaut, un hôte KMS est configuré pour utiliser le protocole TCP (Transmission Control Protocol) sur le port 1688.

Pour configurer la règle de pare-feu afin d'autoriser le trafic réseau uniquement pour les profils de réseau privé et domaine, exécutez la commande suivante :

PowerShell

```
Set-NetFirewallRule -Name SPPSVC-In-TCP -Profile Domain,Private -Enabled True
```

Utiliser l'Assistant Outils d'activation en volume pour configurer l'hôte

1. Ouvrez l'Assistant Outils d'activation en volume en exécutant la commande suivante :

   PowerShell

   ```
   vmw.exe
   ```

2. Dans la page d'introduction, sélectionnez **Suivant**.

3. Pour le type d'activation, sélectionnez **Key Management Service (KMS).** Pour le serveur, entrez **localhost** pour configurer le serveur local. Si vous souhaitez configurer un autre serveur, entrez son nom d'hôte. Cliquez sur **Suivant**.

4. Sélectionnez **Installer votre clé hôte KMS**, entrez la clé de produit de votre organisation, puis sélectionnez **Valider**.

5. Une fois la clé de produit installée, sélectionnez **Suivant** pour activer le produit.

6. Sous **Sélectionner un produit**, sélectionnez le produit que vous souhaitez activer, puis sélectionnez une méthode d'activation. Pour activer la clé en ligne, sélectionnez **Activer en ligne**, puis **commit**. Si vous êtes invité à confirmer l'activation de l'hôte KMS, sélectionnez **Oui**.

Terminer la configuration

Une fois l'activation terminée, la configuration de l'hôte KMS s'affiche.

- Si les paramètres de configuration répondent à vos besoins :

  1. Sélectionnez **Fermer** pour quitter l'Assistant. Le système crée des enregistrements DNS et vous pouvez commencer à activer les clients KMS.
  2. Si vous devez créer manuellement des enregistrements SRV pour publier l'hôte KMS, consultez Créer manuellement des enregistrements DNS plus loin dans cet article.

- Si vous souhaitez modifier les paramètres de configuration :

  1. Cliquez sur **Suivant**.

2. Modifiez les valeurs de configuration en fonction de vos besoins, puis sélectionnez **Valider**.

> ⓘ **Notes**
>
> Vous pouvez maintenant commencer à activer les clients KMS. Toutefois, un réseau doit d'abord avoir un nombre minimal d'ordinateurs (appelé seuil d'activation). Les hôtes KMS effectuent le suivi du nombre de connexions récentes. Lorsqu'un client ou un serveur contacte l'hôte KMS, l'hôte note l'ID de l'ordinateur, incrémente le nombre de contacts, puis retourne le nombre actuel dans sa réponse. Le client ou le serveur est activé si le nombre est suffisamment élevé :
>
> - Les clients Windows sont activés si le nombre est de 25 ou version ultérieure.
> - Windows Server et les éditions en volume des produits Microsoft Office sont activés si le nombre est supérieur ou égal à cinq.
>
> Dans le nombre, KMS inclut uniquement les connexions uniques des 30 derniers jours, et il stocke uniquement les 50 contacts les plus récents.

Créer manuellement des enregistrements DNS

Si votre service DNS ne prend pas en charge les mises à jour dynamiques, vous devez créer manuellement les enregistrements de ressources pour publier l'hôte KMS. Créez manuellement des enregistrements de ressources DNS pour KMS avec votre service DNS à l'aide des informations suivantes. Si vous modifiez le numéro de port par défaut dans la configuration de l'hôte KMS, ajustez également le numéro de port que vous utilisez pour les enregistrements de ressources.

Agrandir le tableau

Property	Value
Type	SRV
Service/Name	_vlmcs
Protocol	_tcp
Priority	0
Weight	0
Numéro de port	1688

Property	Value
Hostname	<FQDN-of-KMS-host>

Vous devez également désactiver la publication sur tous les hôtes KMS si votre service DNS ne prend pas en charge les mises à jour dynamiques. Pour obtenir des instructions, consultez Désactiver la publication d'enregistrements DNS plus loin dans cet article. En désactivant la publication, vous empêchez les journaux d'événements de collecter les événements de publication DNS ayant échoué.

> **Conseil**
>
> Les enregistrements de ressources créés manuellement peuvent également coexister avec les enregistrements de ressources que KMS héberge automatiquement publier dans d'autres domaines tant que tous les enregistrements sont conservés pour éviter les conflits.

Désactiver la publication d'enregistrements DNS

Pour désactiver la publication d'enregistrements DNS par l'hôte KMS :

1. Ouvrez l'Assistant Outils d'activation en volume en exécutant la commande suivante :

   ```
   PowerShell
   ```

   ```
   vmw.exe
   ```

2. Dans la page d'introduction, sélectionnez **Suivant**.

3. Pour le type d'activation, sélectionnez **Key Management Service (KMS).** Pour le serveur, entrez **localhost** pour configurer le serveur local. Si vous souhaitez configurer un autre serveur, entrez son nom d'hôte. Cliquez sur **Suivant**.

4. Sélectionnez **Ignorer la configuration**, puis sélectionnez **Suivant**.

5. En regard **des enregistrements DNS**, décochez la case **Publier** , puis sélectionnez **Valider**.

Remplacer un hôte KMS

30/07/2025

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

Cet article décrit les étapes et les meilleures pratiques pour migrer le rôle hôte KMS (Key Management Services) vers un nouveau serveur. La migration de l'hôte KMS est souvent nécessaire lorsque le système d'exploitation de l'hôte existant approche de sa fin de prise en charge. Il peut également être nécessaire en raison de modifications opérationnelles ou organisationnelles qui imposent de déplacer le rôle vers un autre serveur. Les instructions de ce guide fournissent un processus de migration fluide tout en conservant des services d'activation ininterrompus pour les clients Microsoft Windows et Microsoft Office. Aucune migration de données n'est nécessaire pendant ce processus, car l'hôte KMS ne s'appuie sur aucune base de données ou sauvegarde.

Avant de poursuivre vos tâches d'installation et de licence, passez en revue les détails suivants concernant votre nouvel hôte KMS :

- Vérifiez que vous avez accès à votre nouvelle clé de licence en volume spécifique au client (CSVLK). Votre fichier CSVLK est également appelé **clé hôte KMS** pour le système d'exploitation Microsoft Windows et Microsoft Office, qui sont obtenus via le Centre d'administration Microsoft 365. Le fichier CSVLK a une limite d'activation prédéfinie. Si vous rencontrez une erreur indiquant que vous avez dépassé la limite d'activation, vous pouvez réinitialiser la clé par requête. Pour en savoir plus, consultez Rechercher et utiliser des clés de produit pour la gestion des licences en volume.
- Si vous ne parvenez pas à trouver votre fichier CSVLK, contactez le support technique pour obtenir de l'aide sur les licences.

Prerequisites

- Le rôle **Services d'activation en volume** doit être installé sur l'appareil qui joue le rôle de nouvel hôte KMS. Pour en savoir plus, consultez Installer ou désinstaller des rôles, services de rôle ou fonctionnalités.

  Vous pouvez également exécuter la commande PowerShell suivante :

  PowerShell

  ```
  Install-WindowsFeature -Name VolumeActivation -IncludeManagementTools
  ```

- Vous devez être membre des groupes suivants :
  - Administrators
  - Domain Admins
  - Enterprise Admins
- Le fichier CSVLK doit être valide et accessible à partir du portail de licences de votre organisation ou du Centre d'administration Microsoft 365. Vérifiez que vous disposez du fichier CSVLK approprié pour les produits que vous activez, tels que :
  - Microsoft Windows OS CSVLK
  - Microsoft Office CSVLK
- Votre système d'exploitation doit disposer des dernières mises à jour Windows installées avant de configurer votre appareil en tant qu'hôte KMS. Pour en savoir plus, consultez les mises à jour requises de l'hôte KMS.

Vérifier les hôtes KMS existants

Avant de migrer vers un nouvel hôte KMS, il est recommandé d'inventorier votre environnement pour identifier tous les hôtes KMS existants. Cela permet de s'assurer qu'il n'existe pas d'hôtes KMS non autorisés ou inutiles présents. Les hôtes KMS non approuvés peuvent apparaître si un fichier CSVLK a été utilisé pour activer un appareil qui ne doit pas servir d'hôte KMS. Seuls les serveurs autorisés doivent être activés avec un fichier CSVLK et configurés en tant qu'hôtes KMS. L'exécution de ces actions peut être effectuée dans une invite de commandes avec élévation de privilèges ou dans une fenêtre PowerShell.

Récupérer un hôte KMS

Command Prompt

Pour récupérer les hôtes KMS par le système DNS (Domain Name System), exécutez la commande suivante :

Invite de commandes Windows

```
nslookup -type=srv _vlmcs._tcp
```

Pour récupérer les hôtes KMS par le nom de domaine complet (FQDN), exécutez la commande suivante :

Invite de commandes Windows

```
nslookup -type=SRV _vlmcs._tcp.mydomain.com
```

Pour récupérer des hôtes KMS par un serveur DNS spécifique, par exemple 8.8.8.8, exécutez la commande suivante :

Invite de commandes Windows

```
nslookup -type=SRV _vlmcs._tcp.mydomain.com 8.8.8.8
```

Si vous détectez des hôtes KMS non autorisés, vous pouvez les rétablir aux clients KMS en exécutant la commande suivante dans une fenêtre avec élévation de privilèges, puis redémarrer l'appareil. Remplacez la Clé de Licence en Volume Générique (GVLK) par votre propre GVLK :

```
slmgr.vbs /ipk <GVLK>
```

Vérifier l'activation du produit hôte KMS

Pour vérifier quels produits l'hôte KMS actuel active et vérifier que le nouvel hôte KMS active le même système d'exploitation Windows et les mêmes clients Microsoft Office, exécutez la commande suivante :

Invite de commandes Windows

```
cscript %windir%\system32\slmgr.vbs /dlv All
```

PowerShell

```
cscript $env:windir\system32\slmgr.vbs /dlv All
```

Vérifiez la sortie pour déterminer si l'hôte KMS traite les demandes d'activation pour le système d'exploitation Windows, Microsoft Office ou les deux. Les clés de produit partielles affichées peuvent vous aider à faire correspondre ces clés hôtes KMS (CSVLK) à vos enregistrements. En outre, passez en revue le journal des événements de l'hôte KMS pour identifier les clients qui envoient des demandes d'activation à cet hôte KMS.

Préparer l'hôte KMS

Avant de configurer votre environnement en tant qu'hôte KMS, commencez par une nouvelle installation du système d'exploitation cible sur le nouveau serveur. Pour savoir comment installer votre système d'exploitation Windows Server, consultez Installer Windows Server à partir du support d'installation. Vérifiez que toutes les mises à jour du système d'exploitation et tous les correctifs de sécurité disponibles sont appliqués et redémarrés si nécessaire. Il existe deux options disponibles pour configurer votre hôte KMS.

Hôte KMS du système d'exploitation Windows

Après avoir préparé le système d'exploitation hôte, l'étape suivante consiste à la configurer pour servir d'hôte KMS. Consultez Créer un hôte d'activation KMS (Key Management Services).

Vérifier les paramètres du pare-feu

Avant de continuer sur la gestion d'un hôte KMS, vérifiez que l'exception de pare-feu est configurée pour le port **1688** afin d'accepter les demandes d'activation des clients KMS. En outre, le port **135** (RPC anonyme) doit également être configuré.

GUI

1. Sélectionnez **Démarrer**, tapez **wf.msc**, puis sélectionnez-le pour ouvrir le **Pare-feu Windows Defender avec Advanced Security**.
2. Dans le volet gauche, sélectionnez **Règles de trafic entrant**.
3. Dans le volet droit, sélectionnez **Nouvelle règle** pour ouvrir l'Assistant des nouvelles règles entrantes.
4. Sous **Type de règle**, sélectionnez **Port**, puis sélectionnez **Suivant**.
5. Sous **Protocole et ports**, sélectionnez **TCP**, entrez **1688** dans le champ **Ports locaux spécifiques** , puis sélectionnez **Suivant**.
6. Sous **Action**, vérifiez que **l'option Autoriser la connexion** est sélectionnée, puis sélectionnez **Suivant**.
7. Sous **Profil**, **Domaine**, **Privé** et **Public** sont sélectionnés par défaut. Select **Next**.
8. Sous **Nom**, indiquez le nom souhaité pour votre règle, par exemple « Hôte KMS », puis sélectionnez **Terminer**.

Répétez ces étapes pour configurer le port **135**.

Pour vérifier que le trafic est autorisé via le port **1688** ou **135**, exécutez la commande suivante où les valeurs de **ComputerName** sont le nom de l'appareil ou l'adresse IP :

PowerShell

```
Test-NetConnection -ComputerName "MyDevice" -Port 1688
```

Lorsque la connexion réussit, l'entrée **TcpTestSucceeded** a la valeur **True**, tandis que si la connexion au port 1688 ne peut pas être établie (par exemple, si aucun service n'écoute ou en raison d'un pare-feu ou d'un problème réseau), **TcpTestSucceeded a** la valeur **False**.

Inscrire un hôte KMS

Après avoir configuré l'hôte KMS pour le système d'exploitation Windows et Microsoft Office, il peut s'inscrire automatiquement auprès du DNS si vos autorisations de domaine autorisent. Si l'inscription manuelle est requise, suivez les étapes de création manuelle d'enregistrements DNS.

Après avoir inscrit le nouvel hôte KMS dans DNS, vous pouvez supprimer l'ancien hôte KMS du DNS. Les appareils clients commencent à envoyer des demandes d'activation au nouvel hôte KMS, mais le nombre d'activations peut prendre un certain temps pour atteindre les seuils minimaux requis.

> ⓘ **Notes**
>
> - **Seuil d'activation du client KMS : KMS** nécessite au moins **25** demandes d'activation uniques du système d'exploitation client ou serveur pour commencer à activer le système d'exploitation client.
> - **Seuil d'activation du serveur KMS : KMS** nécessite au moins **5** demandes d'activation uniques du serveur ou du système d'exploitation client pour commencer à activer le système d'exploitation du serveur.

Pour confirmer la réussite de la migration, passez en revue le *journal des événements* sur le nouvel hôte KMS (**Observateur d'événements**>**Journal des applications et des services**>**Service de gestion des clés**). Vous pouvez également exécuter la commande suivante et passer en revue la sortie :

```
slmgr.vbs /dlv
```

Une fois que les appareils clients envoient des demandes d'activation au nouvel hôte, vous pouvez supprimer en toute sécurité l'ancien hôte KMS du DNS.

> ⓘ Notes
>
> - Pour supprimer la fonctionnalité hôte KMS de l'ancien hôte KMS, installez votre GVLK et redémarrez votre appareil.
> - La meilleure pratique consiste à arrêter complètement l'ancien hôte KMS pour s'assurer que les appareils clients passent au nouvel hôte KMS.
> - Si un appareil a été configuré pour un hôte KMS spécifique à l'aide `slmgr.vbs /skms` de , l'exécution `slmgr.vbs /ckms` efface cette configuration et permet aux appareils de détecter automatiquement le nouvel hôte KMS.

Résoudre les problèmes d'activation KMS

L'exécution de ces actions doit être effectuée dans une invite de commandes avec élévation de privilèges ou dans une fenêtre PowerShell. Pour résoudre d'autres problèmes, consultez Instructions pour résoudre les problèmes liés au service de gestion des clés (KMS).

See also

- Planification de l'activation KMS (Key Management Services)
- Options de Slmgr.vbs pour obtenir des informations sur l'activation en volume

Activation du client KMS et clés de produit

16/08/2025

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

Pour utiliser les services kmS (Key Management Services), vous devez disposer d'un hôte KMS disponible sur votre réseau local. Les ordinateurs qui s'activent avec un hôte KMS doivent avoir une clé de produit spécifique. Parfois appelée clé de client KMS, cette clé est officiellement connue sous le nom de clé de licence en volume générique (GVLK) Microsoft. Les ordinateurs qui exécutent des éditions de licence en volume de Windows Server et Windows client sont, par défaut, des clients KMS qui ne nécessitent pas de configuration supplémentaire, car la clé GVLK appropriée est déjà présente.

Il existe certains scénarios où vous devez ajouter le GVLK à l'ordinateur que vous souhaitez activer sur un hôte KMS, par exemple :

- Conversion d'un ordinateur à l'aide d'une clé d'activation multiple (MAK)
- Conversion d'une licence de vente au détail de Windows en client KMS
- Si l'ordinateur était auparavant un hôte KMS

Pour utiliser les kits GVLK répertoriés, vous avez besoin d'un hôte KMS sur votre réseau local. Si vous n'en avez pas, vous pouvez apprendre à créer un hôte KMS.

L'hôte KMS nécessite sa propre clé, appelée clé hôte KMS, pour activer ou s'authentifier auprès de Microsoft. Cette clé est disponible dans le Centre d'administration Microsoft 365 pour les contrats de licence Open, Open Value, Select, Enterprise et Services Provider. Vous pouvez obtenir de l'aide auprès du Centre d'activation Microsoft local.

> ⊗ **Attention**
>
> Lorsque vous activez Windows ou Windows Server avec un hôte KMS, les clés fournies ici sont destinées aux scénarios de licence en volume et **ne peuvent pas être utilisées** avec les éditions de vente au détail. Les clés client KMS **ne s'activent pas et ne peuvent pas servir** de clé de licence commerciale. Si vous avez installé une copie commerciale de Windows, vous devez utiliser une autre méthode d'activation, comme une clé MAK ou en achetant une licence commerciale authentique. Pour en savoir plus, consultez :
>
> - Activez Windows.
> - Tarification et licences Windows Server.

Installer une clé de produit

Si vous convertissez un ordinateur depuis un hôte KMS, une clé d'activation multiple (MAK) ou une version commerciale de Windows en un client KMS, installez la clé de produit applicable (GVLK) à partir de la liste figurant dans cet article. Pour installer une clé de produit client, ouvrez une invite de commandes d'administration sur le client, puis exécutez la commande suivante, puis **appuyez sur Entrée** :

Invite de commandes Windows

```
slmgr /ipk <product key>
```

Par exemple, pour installer la clé de produit pour Windows Server 2022 Datacenter Edition, exécutez la commande suivante, puis **appuyez sur Entrée** :

Invite de commandes Windows

```
slmgr /ipk WX4NM-KYWYW-QJJR4-XV3QB-6VM33
```

Clés de licence en volume génériques

Dans les tableaux ci-dessous, vous trouverez les clés GVLK pour chaque version et édition de Windows. LTSC est le *canal de maintenance à long terme*, tandis que LTSB est la *branche de maintenance à long terme*.

Canal semi-annuel Windows 11 et Windows 10

Consultez la fiche d'information du cycle de vie Windows pour plus d'informations sur les versions prises en charge et les dates de fin de service.

Agrandir le tableau

Édition du système d'exploitation	Clé de produit du client KMS
Windows 11 Professionnel Windows 10 Professionnel	W269N-WFGWX-YVC9B-4J6C9-T83GX
Windows 11 Professionnel N Windows 10 Professionnel N	MH37W-N47XK-V7XM9-C7227-GCQG9
Windows 11 Professionnel pour les Stations de travail Windows 10 Professionnel pour les Stations de travail	NRG8B-VKK3Q-CXVCJ-9G2XF-6Q84J

Édition du système d'exploitation	Clé de produit du client KMS
Windows 11 Professionnel pour les Stations de travail N Windows 10 Professionnel pour les Stations de travail N	9FNHH-K3HBT-3W4TD-6383H-6XYWF
Windows 11 Professionnel Éducation Windows 10 Professionnel Éducation	6TP4R-GNPTD-KYYHQ-7B7DP-J447Y
Windows 11 Professionnel Éducation N Windows 10 Professionnel Éducation N	YVWGF-BXNMC-HTQYQ-CPQ99-66QFC
Windows 11 Éducation Windows 10 Éducation	NW6C2-QMPVW-D7KKK-3GKT6-VCFB2
Windows 11 Éducation N Windows 10 Éducation N	2WH4N-8QGBV-H22JP-CT43Q-MDWWJ
Windows 11 Entreprise Windows 10 Entreprise	NPPR9-FWDCX-D2C8J-H872K-2YT43
Windows 11 Entreprise N Windows 10 Entreprise N	DPH2V-TTNVB-4X9Q3-TJR4H-KHJW4
Windows 11 Entreprise G Windows 10 Entreprise G	YYVX9-NTFWV-6MDM3-9PT4T-4M68B
Windows 11 Entreprise G N Windows 10 Entreprise G N	44RPN-FTY23-9VTTB-MP9BX-T84FV

Windows Entreprise LTSC et LTSB

Windows 11 LTSC 2024
Windows 10 LTSC 2021, 2019

Agrandir le tableau

Édition du système d'exploitation	Clé de produit du client KMS
Windows 11 Entreprise LTSC 2024 Windows 10 Entreprise LTSC 2021 Windows 10 Enterprise LTSC 2019	M7XTQ-FN8P6-TTKYV-9D4CC-J462D
Windows 11 Entreprise N LTSC 2024 Windows 10 Entreprise N LTSC 2021 Windows 10 Entreprise N LTSC 2019	92NFX-8DJQP-P6BBQ-THF9C-7CG2H

Versions antérieures du client Windows

Windows 8.1

Agrandir le tableau

Édition du système d'exploitation	Clé de produit du client KMS
Windows 8.1 Professionnel	GCRJD-8NW9H-F2CDX-CCM8D-9D6T9
Windows 8.1 Professionnel N	HMCNV-VVBFX-7HMBH-CTY9B-B4FXY
Windows 8.1 Entreprise	MHF9N-XY6XB-WVXMC-BTDCT-MKKG7
Windows 8.1 Entreprise N	TT4HM-HN7YT-62K67-RGRQJ-JFFXW

Windows Server LTSC

Windows Server 2025

Agrandir le tableau

Édition du système d'exploitation	Clé de produit du client KMS
Windows Server 2025 Standard	TVRH6-WHNXV-R9WG3-9XRFY-MY832
Windows Server 2025 Datacenter	D764K-2NDRG-47T6Q-P8T8W-YP6DF
Windows Server 2025 Datacenter : Azure Edition	XGN3F-F394H-FD2MY-PP6FD-8MCRC

Canal semi-annuel Windows Server

Windows Server, versions 20H2, 2004, 1909, 1903 et 1809

Agrandir le tableau

Édition du système d'exploitation	Clé de produit du client KMS
Windows Server Standard	N2KJX-J94YW-TQVFB-DG9YT-724CC
Windows Server Datacenter	6NMRW-2C8FM-D24W7-TQWMY-CWH2D

> **Important**
>
> Windows Server version 20H2 est arrivé en fin de service le 9 août 2022 et ne reçoit plus les mises à jour de sécurité. Cela inclut la mise hors service du canal semi-annuel (SAC) de Windows Server sans versions ultérieures.
>
> Les clients utilisant le canal SAC de Windows Server doivent passer à Azure Stack HCI. Les clients peuvent également utiliser le canal de maintenance Long-Term de Windows Server.

Versions antérieures de Windows Server

Windows Server, version 1803 | Windows Server 2008

Agrandir le tableau

Édition du système d'exploitation	Clé de produit du client KMS
Windows Server Standard	PTXN8-JFHJM-4WC78-MPCBR-9W4KR
Windows Server Datacenter	2HXDN-KRXHB-GPYC7-YCKFJ-7FVDG

Résolution des problèmes d'activation en volume Windows

Article • 07/05/2025 •

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

L'activation du produit est le processus de validation des logiciels après son installation sur un ordinateur spécifique. L'activation confirme que le produit est authentique (pas une copie frauduleuse) et que la clé de produit ou le numéro de série est valide et n'a pas été compromis ou révoqué. L'activation établit également un lien ou une relation entre la clé de produit et l'installation.

L'activation en volume est le processus qui consiste à activer des produits avec licence en volume. Pour devenir un client de licence en volume, une organisation doit configurer un contrat de licence en volume avec Microsoft. Microsoft propose des programmes de licence en volume personnalisés qui prennent en charge la taille et la préférence d'achat de l'organisation. Pour plus d'informations, consultez le Centre de gestion des licences en volume Microsoft.

Le Guide d'activation de Windows Server 2016 se concentre sur la technologie d'activation du service de gestion des clés (KMS). Cette section traite des problèmes courants et fournit des instructions de dépannage pour KMS et plusieurs autres technologies d'activation en volume.

Bonnes pratiques en matière d'activation en volume

Les articles suivants fournissent des informations techniques et des bonnes pratiques pour les technologies d'activation en volume de Microsoft.

Service de gestion de clés (KMS)

- Planifier l'activation en volume
- Présentation de KMS
- Déploiement de l'activation KMS
- Configuration des hôtes KMS
- Configuration du DNS
- Activer à l'aide du service de gestion des clés

Activation basée sur Active Directory (ADBA)

- Déployer l'activation basée sur Active Directory

- Activer à l'aide de l'activation basée sur Active Directory
- Vue d'ensemble de l'activation basée sur Active Directory

Activation de clé d'activation multiple (MAK)

- Utilisation de l'activation MAK
- Présentation de l'activation MAK
- Activation de clients MAK

Activation d'abonnement

- Activation de l'abonnement Windows 10
- Déployer des licences Windows 10 Entreprise
- Windows 10 Entreprise E3 dans le programme Fournisseur de solutions Cloud

Ressources pour résoudre les problèmes d'activation

Les articles suivants fournissent des instructions et des informations sur les outils permettant de résoudre les problèmes d'activation en volume :

- Instructions pour la résolution des problèmes liés au service de gestion des clés (KMS)
- Options de Slmgr.vbs pour obtenir des informations sur l'activation en volume
- Exemple : Résolution des problèmes des clients ADBA qui n'activent pas

Les articles suivants fournissent des conseils pour résoudre des problèmes d'activation plus spécifiques :

- Résolution des codes d'erreur d'activation courants
- Activation KMS : problèmes connus
- Activation MAK : problèmes connus
- Instructions pour la résolution des problèmes d'activation liés à DNS
- Comment reconstruire le fichier Tokens.dat

Instructions pour la résolution des problèmes liés au service de gestion des clés (KMS)

15/09/2025

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

Les clients d'entreprise configurent le service de gestion des clés (KMS) dans le cadre de leur processus de déploiement, car ils leur permettent d'utiliser un processus simple et simple pour activer Windows dans leurs environnements. En règle générale, une fois que vous avez configuré l'hôte KMS, les clients KMS se connectent automatiquement à l'hôte et s'activent eux-mêmes. Toutefois, le processus ne fonctionne pas comme prévu. Cet article vous guide tout au long de la résolution des problèmes que vous pouvez rencontrer.

Pour plus d'informations sur les entrées du journal des événements et le script `slmgr.vbs`, consultez Informations techniques de référence sur l'activation en volume.

Où commencer la résolution des problèmes KMS

Commençons par un bref rappel sur le fonctionnement du système d'activation KMS. KMS est un modèle client-serveur qui a des similitudes avec le protocole DHCP (Dynamic Host Configuration Protocol). Toutefois, au lieu de transmettre des adresses IP aux clients sur leur demande, KMS active l'activation du produit. KMS est également un modèle de renouvellement, dans lequel les clients essaient de réactiver à intervalle régulier. Il existe deux rôles : *l'hôte KMS* et le *client KMS*.

- L'hôte KMS exécute le service d'activation et active l'activation dans l'environnement. Pour configurer un hôte KMS, vous devez installer la clé KMS à partir du Centre de service de licence en volume (VLSC), puis activer le service.
- Le client KMS est le système d'exploitation Windows que vous déployez dans l'environnement et doit être activé. Les clients KMS peuvent exécuter n'importe quelle édition de Windows qui utilise l'activation en volume. Les clients KMS sont fournis avec une clé préinstallée, appelée *clé de licence en volume générique (GVLK)* ou *clé de configuration du client KMS*. La présence du GVLK est ce qui rend un système un client KMS. Les clients KMS utilisent des enregistrements SRV (Domain Name System) (`_vlmcs._tcp`DNS) pour identifier l'hôte KMS. Ensuite, les clients essaient automatiquement de découvrir et d'utiliser ce service pour s'activer eux-mêmes. Pendant la période de grâce des 30 premiers jours, ils essaient de s'activer toutes les deux heures.

Après avoir activé les clients KMS, ils essaient de renouveler leur activation tous les sept jours.

Du point de vue de la résolution des problèmes, vous devrez peut-être examiner à la fois les côtés de l'hôte et du client pour déterminer pourquoi un problème se produit.

Résolution des problèmes sur l'hôte KMS

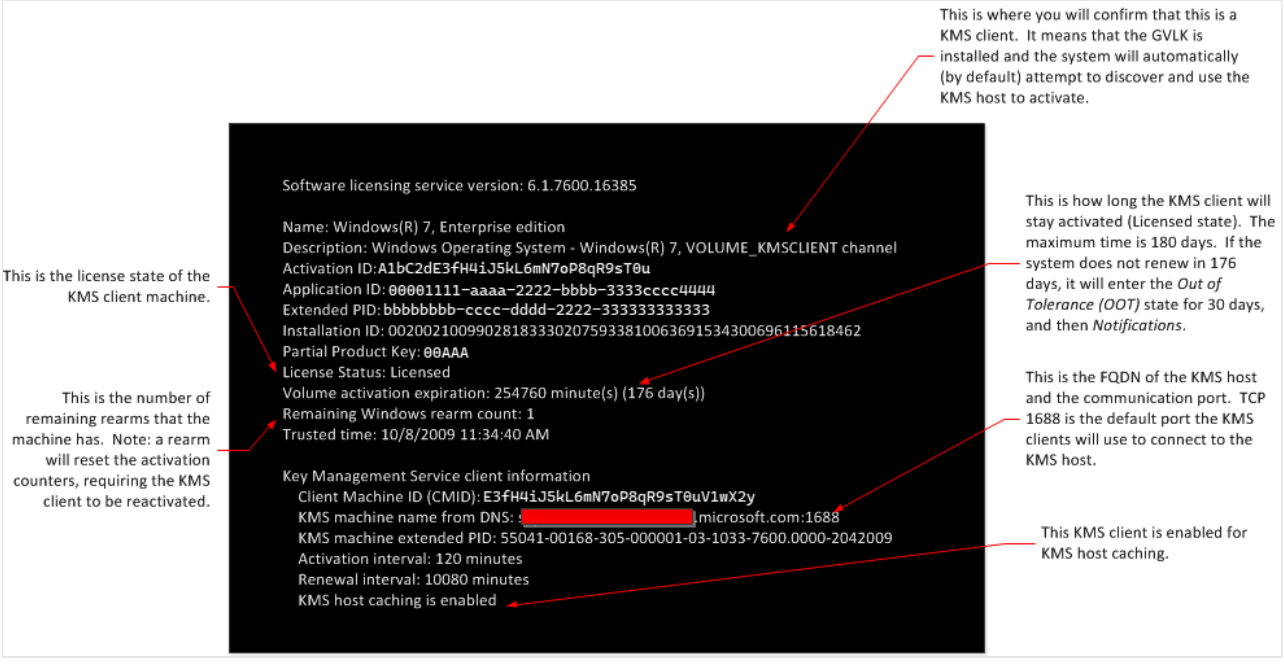
Lorsque vous examinez l'hôte KMS lors de la résolution des problèmes, vous devez examiner deux domaines :

- Vérifiez l'état du service de gestion de licences des logiciels de l'hôte en exécutant la commande `slmgr.vbs` à une invite de ligne de commande.
- Consultez l'Observateur d'événements pour connaître les événements liés aux licences ou à l'activation.

Slmgr.vbs et le service de gestion des licences logicielles

Vous pouvez utiliser l'outil `slmgr.vbs` en ligne de commande et l'Observateur d'événements pour résoudre les problèmes d'activation sur les clients KMS. Pour afficher une sortie détaillée du service Licences logicielles, ouvrez une invite de commandes en mode administrateur ou une fenêtre PowerShell et exécutez `slmgr.vbs /dlv`. La capture d'écran suivante montre les résultats de cette commande pour le client KMS et l'hôte KMS respectivement :

Client KMS



Voici quelques variables à prendre en compte dans la sortie lors de la résolution des problèmes :

- Les *informations de version* se situent en haut de la `slmgr.vbs /dlv` sortie. Les informations sur la version sont utiles pour déterminer si le service est à jour. Assurez-vous que tout est à jour, car le service KMS prend en charge différentes clés d'hôte KMS. Vous pouvez utiliser ces données pour déterminer si la version que vous utilisez actuellement prend en charge la clé hôte KMS que vous essayez d'installer. Pour plus d'informations sur les mises à jour, consultez Une mise à jour est disponible pour Windows Vista et pour Windows Server 2008 afin d'étendre la prise en charge de l'activation KMS pour Windows 7 et pour Windows Server 2008 R2 .

- Le *nom* indique l'édition de Windows en cours d'exécution sur le système hôte KMS. Vous pouvez utiliser ces informations pour résoudre les problèmes qui impliquent l'ajout ou la modification de la clé hôte KMS. Par exemple, vous pouvez utiliser ces informations pour vérifier si l'édition du système d'exploitation prend en charge la clé que vous essayez d'utiliser.

- La *description* vous indique la clé actuellement installée. Utilisez ce champ pour vérifier si la clé qui a d'abord activé le service était la bonne pour les clients KMS que vous avez déployés.

- *L'état de la licence* indique l'état du système hôte KMS. La valeur doit être **sous licence**. Toute autre valeur signifie que vous devez réactiver l'hôte.

- Le *nombre actuel* affiche un nombre compris entre **0** et **50**. Le nombre est cumulé entre les systèmes d'exploitation et indique le nombre de systèmes valides qui ont essayé d'être activés au cours d'une période de **30 jours** .

  Si le nombre est **égal à 0**, le service a été récemment activé ou aucun client valide n'est connecté à l'hôte KMS.

  Le nombre n'augmente pas au-dessus de **50**, quel que soit le nombre de systèmes valides dans l'environnement. Il est configuré pour ne mettre en cache que deux fois la stratégie de licence maximale retournée par un client KMS. La stratégie maximale définie par le système d'exploitation client Windows nécessite un décompte de **25** ou plus de l'hôte KMS pour s'activer. Par conséquent, le nombre maximum que l'hôte KMS peut avoir est soit **50** ou 2 x 25. Dans les environnements qui contiennent uniquement des clients KMS Windows Server, le nombre maximal sur l'hôte KMS est **de 10**. Cette limite est due au fait que le seuil des éditions de Windows Server est **de 5** (2 x 5 ou 10).

Un problème courant lié au nombre se produit lorsque l'environnement a un hôte KMS activé et suffisamment de clients, mais que le nombre n'augmente pas au-delà d'un. Lorsque ce problème se produit, cela signifie que l'image cliente déployée n'a pas été configurée correctement, de sorte que les systèmes n'ont pas d'ID de machine client unique (CMID). Pour plus d'informations, consultez les articles suivants :

- Le nombre actuel KMS n'augmente pas lorsque vous ajoutez de nouveaux ordinateurs clients Windows Vista ou Windows 7 au réseau.
- Le nombre de clients hôtes KMS n'augmente pas en raison de CMID en double.

Une autre raison pour laquelle le nombre peut ne pas augmenter est qu'il y a trop d'hôtes KMS dans l'environnement et que le nombre est distribué sur tous ces hôtes.

- **Écoute sur le port**. La communication avec KMS utilise RPC anonyme. Par défaut, les clients utilisent le port TCP 1688 pour se connecter à l'hôte KMS. Assurez-vous que ce port est ouvert entre vos clients KMS et l'hôte KMS. Vous pouvez modifier ou configurer le port sur l'hôte KMS. Pendant leur communication, l'hôte KMS envoie la désignation de port aux clients KMS. Si vous modifiez le port sur un client KMS, la désignation de port est remplacée lorsque ce client contacte l'hôte.

Nous sommes souvent interrogés sur la section *demandes cumulatives* de la `slmgr.vbs /dlv` sortie. En règle générale, ces données ne sont pas utiles pour la résolution des problèmes. L'hôte KMS conserve un enregistrement continu de l'état de chaque client KMS qui tente d'activer ou de réactiver. Les requêtes ayant échoué indiquent que l'hôte KMS ne prend pas en charge certains clients KMS. Par exemple, si un client KMS Windows 7 tente d'activer sur un hôte KMS activé à l'aide d'une clé KMS Windows Vista, l'activation échoue.

Les *demandes avec les lignes d'état des licences* décrivent tous les états de licence possibles, passés et présents. Du point de vue de la résolution des problèmes, ces données sont pertinentes uniquement si le nombre n'augmente pas comme prévu. Dans ce cas, vous devez voir le nombre de demandes ayant échoué en augmentation. Pour résoudre ce problème, vous devez vérifier la clé de produit utilisée pour activer le système hôte KMS. Notez également que les valeurs de requête cumulatives sont réinitialisées uniquement si vous réinstallez le système hôte KMS.

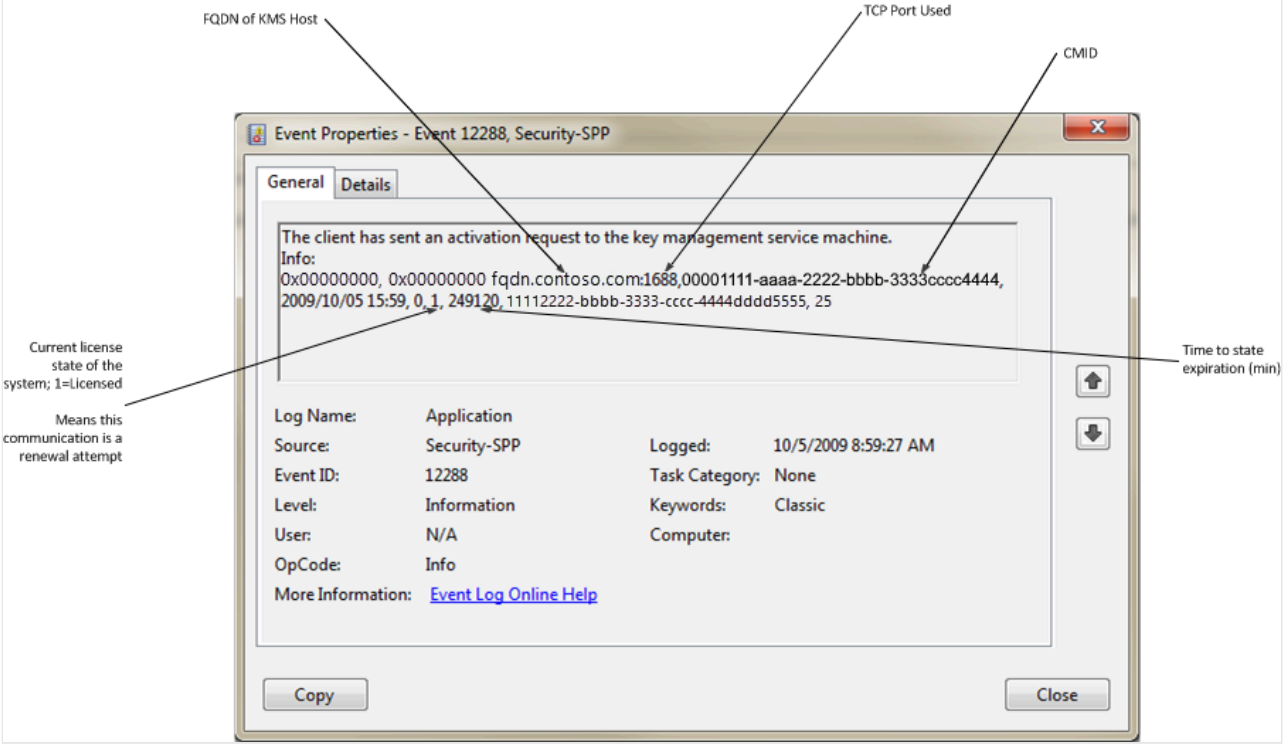
ID d'événement KMS

Les sections suivantes décrivent les événements clients que vous devez connaître pour vous aider à résoudre les problèmes potentiels plus efficacement. Lorsqu'un client KMS active ou réactive correctement, le client enregistre l'ID d'événement 12288 et l'ID d'événement 12289.

Client KMS

ID d'événement 12288 :

Capture d'écran suivante montrant un segment d'une entrée d'ID d'événement 12288 à partir du journal des événements KMS :



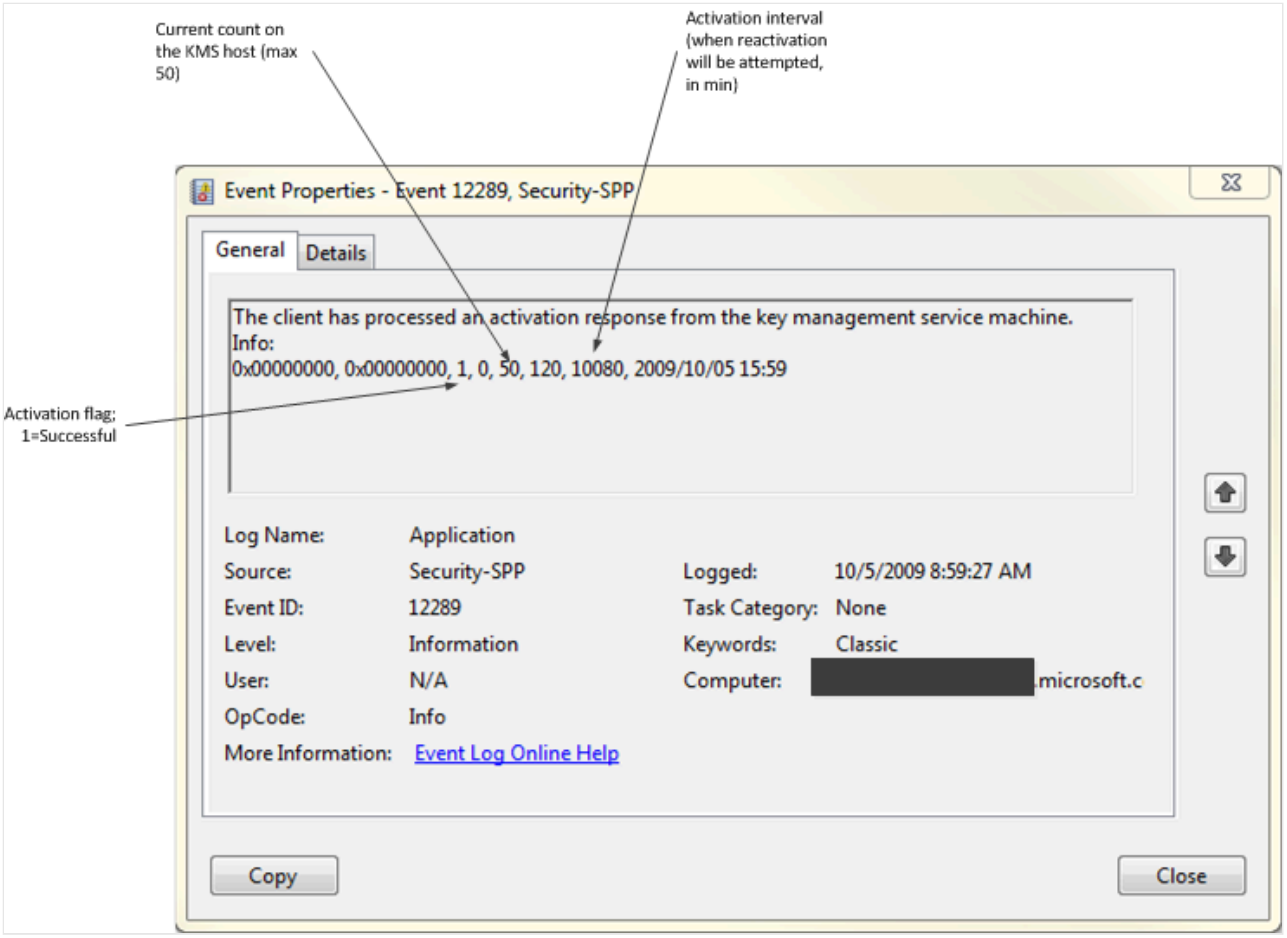
Si vous voyez uniquement l'ID d'événement 12288 sans ID d'événement correspondant 12289, le client KMS n'a pas pu atteindre l'hôte KMS, l'hôte KMS n'a pas répondu ou le client n'a pas reçu la réponse de l'hôte. Dans ces cas, vous devez vérifier que l'hôte KMS est détectable et que les clients KMS peuvent le contacter.

Les informations les plus pertinentes dans l'ID d'événement 12288 sont les données du champ *Informations* . Par exemple, le champ Info affiche l'état actuel du client et le port FQDN et TCP utilisés par le client lorsqu'il a essayé d'activer. Vous pouvez utiliser le nom de domaine complet dans les scénarios dans lesquels le décompte sur un hôte KMS n'augmente pas. Par exemple, s'il existe trop d'hôtes KMS disponibles pour les clients (systèmes légitimes ou non pris en charge), le nombre peut être distribué sur tous ces hôtes.

Une activation non réussie ne signifie pas toujours que le client a l'ID d'événement 12288 et non 12289. Une activation ou une réactivation ayant échoué peut également avoir les deux événements. Dans ce cas, vous devez examiner le deuxième événement pour vérifier la raison de l'échec.

ID d'événement 12289 :

Capture d'écran suivante montrant un segment d'une entrée d'ID d'événement 12289 à partir du journal des événements KMS :



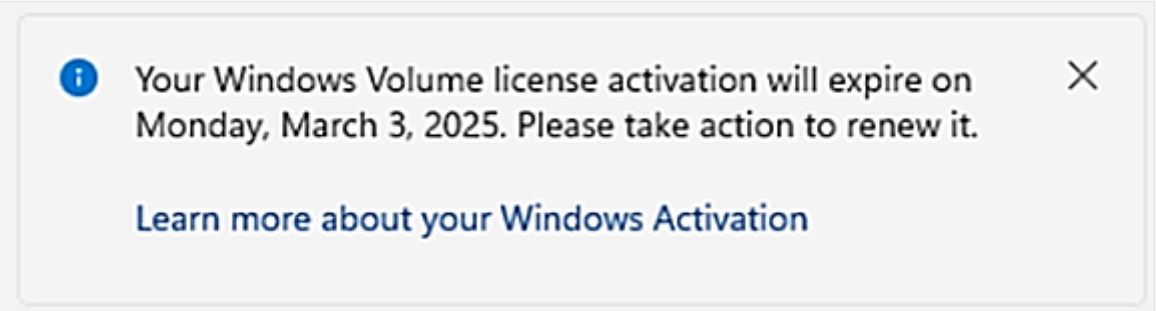
La section *Informations* de l'ID d'événement 12289 fournit les informations suivantes :

- *Indicateur d'activation*, qui indique si l'activation a réussi (**1**) ou échoué (**0**).
- *Nombre actuel sur l'hôte KMS*, qui affiche la valeur de comptage sur l'hôte KMS lorsque le client tente d'activer. Si l'activation échoue, cela peut être dû au fait que le nombre est insuffisant pour ce système d'exploitation client ou qu'il n'y a pas suffisamment de systèmes dans l'environnement pour générer le nombre.

Configuration requise pour le renouvellement du client KMS

L'activation KMS fonctionne sur un modèle de renouvellement, où chaque appareil client doit se connecter à un serveur hôte KMS au moins une fois tous les 180 jours pour maintenir l'activation. Par défaut, les clients KMS tentent de renouveler leur activation tous les sept jours. Une fois le renouvellement réussi, la période de validité de l'activation est réinitialisée pendant 180 jours.

Pour une raison quelconque, si l'exigence de renouvellement n'est pas remplie, vous recevez une notification contextuelle 30 jours avant la fin des 180 jours pour le renouvellement. La notification toast de renouvellement s'affiche également dans le volet d'activation :



Résoudre les exigences de renouvellement du client KMS

- Vous recevez cette notification *uniquement* si vous êtes sur un appareil appartenant à l'entreprise ou géré. S'il s'agit d'une erreur, obtenez une clé de vente au détail à partir du Microsoft Store.
- Si vous utilisez un appareil appartenant à l'entreprise ou géré, communiquez avec votre administrateur informatique. Voici quelques raisons possibles pour lesquelles vous pouvez recevoir ce message :
  - **L'hôte KMS est désactivé** : l'administrateur informatique doit configurer la version du client KMS avec le serveur KMS. Reportez-vous à Activer à l'aide du service de gestion des clés.
  - **Écoute sur un autre port** : la communication avec le service KMS utilise RPC anonyme. Par défaut, les clients utilisent le port TCP 1688 pour se connecter à l'hôte KMS. Vérifiez que ce port est ouvert entre vos clients KMS et l'hôte KMS. Vous pouvez configurer le port sur l'hôte KMS via le Pare-feu Windows avec Advanced Security.
  - **Vérifier la configuration DNS** : par défaut, les clients KMS utilisent le processus de découverte automatique pour interroger DNS pour obtenir une liste de serveurs. Pour plus d'informations, consultez Recommandations pour résoudre les problèmes d'activation liés au DNS.

Que demande le support technique ?

Si vos activations ne fonctionnent pas comme prévu après la résolution des problèmes, vous pouvez contacter le Support Microsoft pour obtenir de l'aide technique. L'ingénieur du support demande généralement les informations suivantes :

- Sortie de la commande `slmgr.vbs /dlv` sur l'hôte KMS et les systèmes clients KMS.

- Journaux des événements à partir de l’hôte KMS (journal du service de gestion des clés) et des systèmes clients KMS (journal des applications).

Options de Slmgr.vbs pour obtenir des informations sur l'activation en volume

16/08/2025

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

Slmgr.vbs est un script Visual Basic inclus dans Windows qui sert d'outil en ligne de commande pour gérer les licences et l'activation du système d'exploitation. Il vous permet d'installer et de modifier les clés de produit, d'activer Windows et de vérifier son état actuel d'activation ou de licence. Il prend également en charge des tâches telles que l'extension de la période de grâce d'activation (réarmement) et la résolution des problèmes liés à l'activation.

La syntaxe du script et des tables Slmgr.vbs de cet article décrivent chaque option de ligne de commande.

Invite de commandes Windows

```
slmgr.vbs [<ComputerName> [<User> <Password>]] [<Options>]
```

> ⓘ **Notes**
>
> Dans cet article, les crochets ([ ]) entourent les arguments facultatifs et les crochets (< >) entourent les espaces réservés. Lorsque vous tapez ces instructions, omettez les crochets et remplacez les espaces réservés à l'aide de valeurs correspondantes.
>
> Pour plus d'informations sur d'autres produits logiciels qui utilisent l'activation en volume, consultez les documents écrits pour ces applications.

Utilisation de Slmgr sur des ordinateurs distants

Pour gérer les clients distants, utilisez l'outil vaMT (Volume Activation Management Tool) version 1.2 ou ultérieure, ou créez des scripts WMI personnalisés qui connaissent les différences entre les plateformes. Pour plus d'informations, consultez Propriétés et méthodes WMI pour l'activation en volume.

> ⓘ **Important**
>
> En raison des modifications WMI dans Windows 7 et Windows Server 2008 R2, le script Slmgr.vbs n'est pas destiné à fonctionner sur plusieurs plateformes. L'utilisation de

Slmgr.vbs pour gérer un système Windows 7 ou Windows Server 2008 R2 à partir du système d'exploitation Windows Vista n'est pas pris en charge. La tentative de gestion d'un système plus ancien à partir de Windows 7 ou Windows Server 2008 R2 génère une erreur d'incompatibilité de version spécifique. Par exemple, l'exécution **de cscript slmgr.vbs <vista_machine_name> /dlv** produit la sortie suivante :

```
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

The remote machine does not support this version of SLMgr.vbs
```

Options générales de Slmgr.vbs

Agrandir le tableau

Option	Description
[<ComputerName>]	Nom d'un ordinateur distant. (La valeur par défaut est l'ordinateur local.)
[<Utilisateur>]	Compte disposant du privilège requis sur l'ordinateur distant.
[<Mot de passe>]	Mot de passe du compte disposant des privilèges requis sur l'ordinateur distant.

Options globales

Agrandir le tableau

Option	Description
/ipk <clé_produit>	Tente d'installer une clé de produit 5×5. La clé de produit fournie par le paramètre est confirmée valide et applicable au système d'exploitation installé. Si ce n'est pas le cas, une erreur est retournée. Si la clé est valide et applicable, la clé est installée. Si une clé est déjà installée, elle est remplacée en mode silencieux. Pour empêcher l'instabilité dans le service de licence, le système doit être redémarré ou le service de protection logicielle doit être redémarré. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges ou la valeur de registre des opérations utilisateur

Option	Description
	standard doit être définie pour autoriser les utilisateurs non privilégiés à un accès supplémentaire au service de protection logicielle.
/ato [<ID d'activation>]	Pour les éditions commerciales et les systèmes de volume qui ont une clé hôte KMS ou une clé d'activation multiple (MAK), **/ato** invite Windows à essayer l'activation en ligne. Pour les systèmes sur utilisant une clé de licence en volume générique (GVLK), **/ato** invite une tentative d'activation KMS. Les systèmes qui sont définis pour suspendre les tentatives d'activation KMS automatiques (**/stao**) essaient toujours l'activation KMS quand **/ato** est exécuté. **Note:** À compter de Windows 8 (et Windows Server 2012), l'option **/stao** est déconseillée. Utilisez l'option **/act-type** à la place. **L'ID d'activation**> du paramètre < développe **/ato** prise en charge pour identifier une édition Windows installée sur l'ordinateur. La spécification du < paramètre **ID d'activation**> isole les effets de l'option à l'édition associée à cet ID d'activation. Exécutez **tous slmgr.vbs /dlv pour** obtenir les ID d'activation pour la version installée de Windows. Si vous devez prendre en charge d'autres applications, consultez les instructions fournies par l'application pour obtenir des instructions supplémentaires. L'activation KMS ne nécessite pas de privilèges élevés. En revanche, l'activation en ligne nécessite une élévation, ou la valeur de Registre Standard User Operations doit être définie afin d'étendre l'accès des utilisateurs sans privilège au service de protection logicielle.
/dli [<ID_activation> | All]	Affiche les informations relatives à la licence. Par défaut, **/dli** affiche les informations de licence de l'édition Windows active installée. La spécification du < paramètre **ID d'activation**> affiche les informations de licence de l'édition spécifiée associée à cet ID d'activation. La spécification **de tous les** paramètres en tant que paramètre affiche les informations de licence pour tous les produits installés applicables. Cette opération ne nécessite pas de privilèges élevés.
/dlv [<ID d'activation> | Tout]	Affichez des informations détaillées sur la licence. Par défaut, **/dlv** affiche les informations de licence du système d'exploitation installé. La spécification du < paramètre **ID d'activation**> affiche les informations de licence de l'édition spécifiée associée à cet ID d'activation. La spécification du paramètre **All** affiche les informations de licence pour tous les produits installés applicables. Cette opération ne nécessite pas de privilèges élevés.
/xpr [<ID d'activation>]	Affichez la date d'expiration de l'activation pour le produit. Par défaut, la date fait référence à l'édition Actuelle de Windows et est principalement utile pour les clients

Option	Description
	KMS, car l'activation mak et commerciale est perpétuelle. La spécification du < paramètre **ID d'activation**> affiche la date d'expiration de l'activation de l'édition spécifiée associée à cet ID d'activation. Cette opération ne nécessite pas de privilèges élevés.

Options avancées

Agrandir le tableau

Option	Description
/cpky	Certaines opérations de maintenance nécessitent que la clé de produit soit disponible dans le Registre pendant les opérations OOBE (Out of Box Experience). L'option **/cpky** supprime la clé de produit du Registre pour empêcher ce vol de cette clé par du code malveillant. Pour les installations de vente au détail qui déploient des clés, la meilleure pratique consiste à exécuter cette option. Cette option n'est pas nécessaire pour les clés hôtes MAK et KMS, car il s'agit du comportement par défaut de ces clés. Cette option est requise uniquement pour d'autres types de clés dont le comportement par défaut n'est pas d'effacer la clé du Registre. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/ilc <fichier_de_licence>	Cette option installe le fichier de licence spécifié par le paramètre requis. Ces licences peuvent être installées en tant que mesure de résolution des problèmes, pour prendre en charge l'activation basée sur les jetons ou dans le cadre d'une installation manuelle d'une application intégrée. Les licences ne sont pas validées pendant ce processus : la validation de licence est hors du cadre pour Slmgr.vbs. Au lieu de cela, la validation est gérée par le service de protection logicielle au moment de l'exécution. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges ou la valeur de registre des opérations utilisateur standard doit être définie pour autoriser les utilisateurs non privilégiés à un accès supplémentaire au service de protection logicielle.
/rilc	Cette option réinstalle toutes les licences stockées dans %SystemRoot%\system32\oem et %SystemRoot%\System32\spp\tokens. Il s'agit de copies « connues et fiables » qui ont été stockées pendant l'installation. Toute licence correspondante trouvée dans le magasin approuvé est remplacée. Toutes les licences supplémentaires , par exemple, les licences d'émission

Option	Description
	d'autorité de confiance (TA), les licences pour les applications, ne sont pas affectées. Cette opération doit être exécutée dans une fenêtre d'invite de commandes avec élévation de privilèges, ou la valeur de Registre Des opérations utilisateur standard doit être définie pour autoriser les utilisateurs non privilégiés à accéder supplémentaire au service de protection logicielle.
/rearm	Cette option réinitialise les minuteurs d'activation. Le processus **/rearm** est également appelé par **sysprep /generalize**. Cette opération ne fait rien si l'entrée **de RegistreHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm** est définie sur **1**. Pour plus d'informations sur cette entrée de Registre, consultez Paramètres du Registre pour l'activation en volume. Cette opération doit être exécutée dans une fenêtre d'invite de commandes avec élévation de privilèges, ou la valeur de Registre Des opérations utilisateur standard doit être définie pour autoriser les utilisateurs non privilégiés à accéder supplémentaire au service de protection logicielle.
ID d'application /rearm-app <>	Réinitialise l'état des licences de l'application spécifiée.
/rearm-sku <ID d'application>	Réinitialise l'état de la licence de la référence SKU spécifiée.
/upk [<ID d'application>]	Cette option désinstalle la clé de produit de l'édition Actuelle de Windows. Après un redémarrage, le système est dans un état sans licence, sauf si une nouvelle clé de produit est installée. Si vous le souhaitez, vous pouvez utiliser le < paramètre **ID d'activation**> pour spécifier un autre produit installé. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/dti [<ID d'activation>]	Affiche l'ID d'installation pour l'activation hors connexion.
ID de confirmation /atp <>	Activez le produit à l'aide de l'ID de confirmation fourni par l'utilisateur.

Options du client KMS

Agrandir le tableau

Option	Description
/skms <Name[:Port] | :Port> [<ID d'activation>]	Cette option spécifie le nom et, éventuellement, le port de l'ordinateur hôte KMS à contacter. La définition de cette valeur désactive la détection automatique de l'hôte KMS. Si l'hôte KMS utilise uniquement le protocole Internet version 6 (IPv6), l'adresse doit être spécifiée au format <hostname> :<port>. Les adresses IPv6 contiennent des points-virgules (:), que le script Slmgr.vbs n'analyse pas correctement. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/skms-domain <FQDN> [<ID d'activation>]	Définit le domaine DNS spécifique dans lequel tous les enregistrements SRV KMS sont disponibles. Ce paramètre n'a aucun effet si l'hôte KMS unique spécifique est défini à l'aide de l'option **/skms** . Utilisez cette option, en particulier dans les environnements d'espace de noms disjoints, pour forcer KMS à ignorer la liste de recherche de suffixes DNS et rechercher les enregistrements hôtes KMS dans le domaine DNS spécifié à la place.
/ckms [<ID d'activation>]	Cette option supprime le nom d'hôte, l'adresse et les informations de port KMS spécifiés du Registre et restaure le comportement de découverte automatique KMS. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/skhc	Cette option active la mise en cache de l'hôte KMS (par défaut). Une fois que le client a découvert un hôte KMS opérationnel, ce paramètre empêche la priorité et le poids du DNS (Domain Name System) d'affecter toute communication ultérieure avec l'hôte. Si le système ne peut plus contacter l'hôte KMS opérationnel, le client tente de découvrir un nouvel hôte. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/ckhc	Cette option désactive la mise en cache de l'hôte KMS. Ce paramètre indique au client d'utiliser la découverte automatique DNS chaque fois qu'il tente l'activation KMS (recommandé lors de l'utilisation de la priorité et du poids). Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.

Options de configuration de l'hôte KMS

Agrandir le tableau

Option	Description
/sai <intervalle>	Cette option définit l'intervalle, en minutes, pour que les clients non activés essaient de se connecter à KMS. L'intervalle d'activation doit être compris entre 15 minutes et 30 jours, bien que la valeur par défaut (deux heures) soit recommandée. Le client KMS récupère initialement cet intervalle à partir du Registre, mais passe au paramètre KMS après avoir reçu la première réponse KMS. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/sri <Intervalle>	Cette option définit l'intervalle de renouvellement, en minutes, pour que les clients activés essaient de se connecter à KMS. L'intervalle de renouvellement doit être compris entre 15 minutes et 30 jours. Cette option est définie initialement sur le serveur KMS et les côtés clients. La valeur par défaut est 10 080 minutes (7 jours). Le client KMS récupère initialement cet intervalle à partir du Registre, mais passe au paramètre KMS après avoir reçu la première réponse KMS. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/sprt <port>	Cette option définit le port sur lequel l'hôte KMS écoute les demandes d'activation du client. Le port TCP par défaut est 1688. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/sdns	Activez la publication DNS par l'hôte KMS (par défaut). Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/cdns	Désactivez la publication DNS par l'hôte KMS. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/spri	Définissez la priorité KMS sur normale (valeur par défaut). Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/cpri	Définit la priorité KMS sur faible. Utilisez cette option pour réduire la contention de KMS dans un environnement co-hébergé, ce qui peut entraîner une raréfaction de KMS en fonction des

Option	Description
	autres applications ou des rôles de serveur actifs. Utilisez cette option avec soin. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/act-type [<Type d'activation>] [<Identifiant d'activation>]	Cette option définit une valeur dans le registre qui limite l'activation du volume à un seul type. Le type d'activation **1** limite l'activation à Active Directory uniquement. **2** le limite à l'activation KMS. **3** le limite à l'activation basée sur les jetons. L'option **0** autorise tout type d'activation et est la valeur par défaut.

Options de configuration de l'activation basée sur les jetons

Agrandir le tableau

Option	Description
/lil	Répertoriez les licences d'émission d'activation basées sur les jetons installées.
/ril <ILID ILvID><>	Supprime une licence d'émission installée avec activation par jeton. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges.
/stao	Définissez l'indicateur **d'activation basée sur les jetons uniquement** , désactivant l'activation KMS automatique. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges. Cette option a été supprimée dans Windows Server 2012 R2 et Windows 8.1. Utilisez l'option **/act-type** à la place.
/ctao	Effacez l'indicateur **d'activation basée sur les jetons** uniquement (valeur par défaut), en activant l'activation KMS automatique. Cette opération doit être exécutée à partir d'une fenêtre d'invite de commandes avec élévation de privilèges. Cette option a été supprimée dans Windows Server 2012 R2 et Windows 8.1. Utilisez l'option **/act-type** à la place.
/ltc	Répertoriez les certificats d'activation basés sur des jetons

Option	Description
	valides qui peuvent activer les logiciels installés.
/fta <empreinte_numérique_certificat> [<code_PIN>]	Forcer l'activation basée sur les jetons à l'aide du certificat identifié. Le numéro d'identification personnel (PIN) facultatif est fourni pour déverrouiller la clé privée sans invite de code confidentiel si vous utilisez des certificats protégés par du matériel (par exemple, des cartes à puce).

Options de configuration de l'activation basée sur Active Directory

Agrandir le tableau

Option	Description
/ad-activation-online <Product Key> [<Nom> de l'objet d'activation]	Collecte les données d'Active Directory et démarre l'activation de la forêt Active Directory à l'aide des informations d'identification utilisées par l'invite de commandes. L'accès administrateur local n'est pas obligatoire. Toutefois, l'accès en lecture/écriture au conteneur d'objets d'activation dans le domaine racine de la forêt est requis.
/ad-activation-get-IID <clé_produit>	Cette option démarre l'activation de la forêt Active Directory en mode téléphone. La sortie est l'ID d'installation (IID) qui peut être utilisé pour activer la forêt via le téléphone si la connectivité Internet n'est pas disponible. Lorsque l'IID est fourni dans l'appel téléphonique d'activation, un CID est retourné utilisé pour terminer l'activation.
/ad-activation-apply-cid <Product Key><Confirmation ID> [<Nom de l'objet> d'activation]	Lorsque vous utilisez cette option, entrez le CID fourni dans l'appel téléphonique d'activation pour terminer l'activation
[/name : <>AO_Name]	Si vous le souhaitez, vous pouvez ajouter l'option **/name** à l'une de ces commandes pour spécifier un nom pour l'objet d'activation stocké dans Active Directory. Le nom ne doit pas dépasser 40 caractères Unicode. Utilisez des guillemets doubles pour définir explicitement la chaîne de nom. Dans Windows Server 2012 R2 et Windows 8.1, vous pouvez ajouter le nom directement après **/ad-activation-online <Product Key>** et **/ad-activation-apply-cid** sans avoir à utiliser l'option **/name** .
/ao-list	Affiche tous les objets d'activation disponibles pour l'ordinateur local.

Option	Description
/del-ao <DN_objet_activation> /del-ao <RDN_AO>	Supprime l'objet d'activation spécifié de la forêt.

Contenu connexe

- Référence technique sur l'activation en volume
- Vue d'ensemble de l'activation en volume

Activation KMS : problèmes connus

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 résoudre rapidement les problèmes courants liés à l'activation KMS et MAK

Cet article décrit les questions courantes et les problèmes pouvant être rencontrés lors des activations du service de gestion des clés (KMS) et fournit des conseils pour résoudre les problèmes.

> ⓘ **Notes**
>
> Si vous pensez que votre problème est lié à DNS, consultez les procédures de résolution des problèmes courants pour les problèmes KMS et DNS.

Dois-je sauvegarder les informations de l'hôte KMS ?

La sauvegarde n'est pas nécessaire pour les hôtes KMS. Toutefois, si vous utilisez un outil pour nettoyer régulièrement les journaux d'événements, l'historique d'activation stocké dans les journaux peut être perdu. Si vous utilisez le journal des événements pour suivre ou documenter les activations KMS, exportez régulièrement le journal des événements du service de gestion des clés à partir du dossier Journaux des applications et des services de l'Observateur d'événements.

Si vous utilisez System Center Operations Manager, la base de données System Center Data Warehouse stocke les données du journal des événements pour la création de rapports. Par conséquent, vous n'avez pas besoin de sauvegarder les journaux d'événements séparément.

L'ordinateur client KMS est-il activé ?

Sur l'ordinateur client KMS, ouvrez le panneau de configuration **système** et recherchez le message **Windows activé** . Vous pouvez également exécuter Slmgr.vbs et utiliser l'option de ligne de commande **/dli** .

L'ordinateur client KMS ne s'active pas.

Vérifiez que le seuil d'activation KMS est atteint. Sur l'ordinateur hôte KMS, exécutez Slmgr.vbs et utilisez l'option de ligne de commande **/dli** pour déterminer le nombre actuel de l'hôte. Tant que l'hôte KMS n'a pas le nombre de 25, les ordinateurs clients Windows 7 ne peuvent pas être activés. Les clients KMS Windows Server 2008 R2 nécessitent un nombre KMS de 5 pour l'activation. Pour plus d'informations sur les exigences KMS, consultez le Guide de planification de l'activation en volume.

Sur l'ordinateur client KMS, recherchez l'ID d'événement 12289 dans le journal des événements de l'application. Vérifiez cet événement pour obtenir les informations suivantes :

- Le code de résultat **est-il 0** ? Tout autre chose est une erreur.
- Le nom d'hôte KMS est-il correct dans l'événement ?
- Le port KMS est-il correct ?
- L'hôte KMS est-il accessible ?
- Si le client exécute un pare-feu non-Microsoft, le port sortant doit-il être configuré ?

Sur l'ordinateur hôte KMS, recherchez l'ID d'événement 12290 dans le journal des événements KMS. Vérifiez cet événement pour obtenir les informations suivantes :

- L'hôte KMS a-t-il journaliser une demande de l'ordinateur client ? Vérifiez que le nom de l'ordinateur client KMS est répertorié. Vérifiez que le client et l'hôte KMS peuvent communiquer. Le client a-t-il reçu la réponse ?
- Si aucun événement n'est journalisé à partir du client KMS, la demande n'a pas atteint l'hôte KMS ou l'hôte KMS n'a pas pu le traiter. Assurez-vous que les routeurs ne bloquent pas le trafic à l'aide du port TCP 1688 (si le port par défaut est utilisé) et que le trafic avec état vers le client KMS est autorisé.

Que signifie ce code d'erreur ?

À l'exception des événements KMS qui ont l'ID d'événement 12290, Windows enregistre tous les événements d'activation dans le journal des événements de l'application sous le nom du fournisseur d'événements Microsoft-Windows-Security-SPP. Windows enregistre les événements KMS dans le journal du service de gestion des clés dans le dossier Applications et Services. Les professionnels de l'informatique peuvent exécuter Slui.exe pour afficher une description de la plupart des codes d'erreur liés à l'activation. La syntaxe générale de cette commande est la suivante :

Invite de commandes Windows

```
slui.exe 0x2a ErrorCode
```

Par exemple, si l'ID d'événement 12293 contient le code d'erreur 0x8007267C, vous pouvez afficher une description de cette erreur en exécutant la commande suivante :

Invite de commandes Windows

```
slui.exe 0x2a 0x8007267C
```

Pour plus d'informations sur des codes d'erreur spécifiques et sur la façon de les résoudre, consultez Résolution des codes d'erreur d'activation courants.

Les clients ne sont pas ajoutés au nombre de clients KMS

Pour réinitialiser l'ID d'ordinateur client (CMID) et d'autres informations d'activation de produit, exécutez **sysprep /generalize** ou **slmgr /rearm**. Sinon, chaque ordinateur client semble identique et l'hôte KMS ne les compte pas comme clients KMS distincts.

Les hôtes KMS ne peuvent pas créer d'enregistrements SRV

DNS (Domain Name System) peut restreindre l'accès en écriture ou bien ne pas prendre en charge le DNS dynamique (DDNS). Dans ce cas, accordez à l'hôte KMS un accès en écriture à la base de données DNS ou créez manuellement l'enregistrement de ressource de service (SRV). Pour plus d'informations sur les problèmes KMS et DNS, consultez Procédures de résolution des problèmes courants pour les problèmes KMS et DNS.

Seul le premier hôte KMS est en mesure de créer des enregistrements SRV

Si l'organisation a plusieurs hôtes KMS, les autres hôtes peuvent ne pas être en mesure de mettre à jour le SRV RR, sauf si les autorisations par défaut SRV sont modifiées. Pour plus d'informations sur les problèmes KMS et DNS, consultez Procédures de résolution des problèmes courants pour les problèmes KMS et DNS.

J'ai installé une clé KMS sur le client KMS

Les clés KMS doivent être installées uniquement sur les hôtes KMS, et non sur les clients KMS. Exécutez **slmgr.vbs -ipk <SetupKey>**. Pour les tables de clés que vous pouvez utiliser pour

configurer l'ordinateur en tant que client KMS, consultez les clés de configuration du client KMS. Ces clés sont connues publiquement et sont spécifiques à l'édition. N'oubliez pas de supprimer les RRS SRV inutiles du DNS, puis redémarrez les ordinateurs.

Échec d'un hôte KMS

Si un hôte KMS échoue, vous devez installer une clé hôte KMS sur un nouvel hôte, puis activer l'hôte. Assurez-vous que le nouvel hôte KMS a un SRV RR dans la base de données DNS. Si vous installez le nouvel hôte KMS à l'aide du même nom d'ordinateur et de la même adresse IP que l'hôte KMS ayant échoué, le nouvel hôte KMS peut utiliser l'enregistrement SRV DNS de l'hôte ayant échoué. Si le nouvel hôte a un autre nom d'ordinateur, vous pouvez supprimer manuellement le SRV DNS de l'hôte défaillant ou (si la récupération est activée dans DNS) autoriser DNS à le supprimer automatiquement. Si le réseau utilise DDNS, le nouvel hôte KMS crée automatiquement un nouveau SRV RR sur le serveur DNS. Le nouvel hôte KMS commence ensuite à collecter les demandes de renouvellement du client et commence à activer les clients dès que le seuil d'activation KMS est atteint.

Si vos clients KMS utilisent la découverte automatique, ils sélectionnent automatiquement un autre hôte KMS si l'hôte KMS d'origine ne répond pas aux demandes de renouvellement. Si les clients n'utilisent pas la découverte automatique, vous devez mettre à jour manuellement les ordinateurs clients KMS affectés à l'hôte KMS ayant échoué en exécutant **slmgr.vbs /skms**. Pour éviter ce scénario, configurez les clients KMS pour qu'ils utilisent la découverte automatique. Pour plus d'informations, consultez le Guide de déploiement d'activation en volume.

Activation MAK : problèmes connus

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 résoudre rapidement les problèmes courants liés à l'activation KMS et MAK

Cet article décrit les problèmes courants qui peuvent se produire pendant les activations de clé d'activation multiple (MAK) et fournit des conseils pour résoudre ces problèmes.

Comment puis-je savoir si mon ordinateur est activé ?

Sur l'ordinateur, ouvrez le panneau de configuration **système** et recherchez **Windows activé**. Vous pouvez également exécuter Slmgr.vbs et utiliser l'option de ligne de commande **/dli** .

L'ordinateur ne s'active pas sur Internet

Vérifiez que les ports requis sont ouverts dans le pare-feu. Pour obtenir la liste des ports, consultez le Guide de déploiement d'activation en volume.

Échec de l'activation d'Internet et de téléphone

Contactez un Centre d'activation Microsoft local. Pour les numéros de téléphone des centres d'activation Microsoft dans le monde entier, accédez aux centres d'activation des licences Microsoft dans le monde entier. Veillez à fournir les informations du contrat de licence en volume et la preuve d'achat lorsque vous appelez.

Slmgr.vbs /ato retourne un code d'erreur

Si Slmgr.vbs retourne un code d'erreur hexadécimal, déterminez le message d'erreur correspondant en exécutant le script suivant :

Invite de commandes Windows

```
slui.exe 0x2a 0x <ErrorCode>
```

Pour plus d’informations sur des codes d’erreur spécifiques et sur la façon de les résoudre, consultez Résolution des codes d’erreur d’activation courants.

Instructions pour résoudre les problèmes d'activation liés au DNS

16/08/2025

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

Vous devrez peut-être utiliser certaines de ces méthodes si une ou plusieurs des conditions suivantes sont remplies :

- Vous utilisez un média sous licence en volume et une clé de produit générique de licence en volume pour installer l'un des systèmes d'exploitation suivants :
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows 10
  - Windows 8.1
  - Windows 8
- L'Assistant Activation ne peut pas se connecter à un ordinateur hôte KMS.

Lorsque vous essayez d'activer un système client, l'Assistant Activation utilise DNS pour localiser un ordinateur correspondant exécutant le logiciel KMS. Si l'Assistant interroge DNS et ne trouve pas l'entrée DNS pour l'ordinateur hôte KMS, l'Assistant signale une erreur.

Passez en revue la liste suivante pour trouver une approche adaptée à vos circonstances :

- Si vous ne pouvez pas installer un hôte KMS ou si vous ne pouvez pas utiliser l'activation KMS, essayez de remplacer la clé de produit par une procédure MAK .
- Si vous devez installer et configurer un hôte KMS, utilisez la procédure Configurer un hôte KMS sur lequel activer les clients.
- Si le client ne peut pas localiser votre hôte KMS existant, utilisez les procédures suivantes pour résoudre les problèmes de vos configurations de routage. Ces procédures sont organisées du plus simple au plus complexe.
  - Vérifier la connectivité IP de base au serveur DNS
  - Vérifier la configuration de l'hôte KMS
  - Déterminer le type de problème de routage
  - Vérifier la configuration DNS
  - Créer manuellement un enregistrement SRV KMS
  - Affecter manuellement un hôte KMS à un client KMS

- Configurer l'hôte KMS à publier dans plusieurs domaines DNS

Remplacer la clé de produit par une clé MAK

Si vous ne pouvez pas installer un hôte KMS ou, pour une autre raison, vous ne pouvez pas utiliser l'activation KMS, remplacez la clé de produit par une clé MAK. Si vous avez téléchargé des images Windows à partir de Microsoft Developer Network (MSDN) ou de TechNet, les unités de conservation des stocks (SKU) répertoriées sous le média sont généralement des supports sous licence en volume, et la clé de produit fournie est une clé MAK.

Pour remplacer la clé de produit par une clé MAK, procédez comme suit :

1. Ouvrez une fenêtre d'invite de commandes avec privilèges élevés. Pour ce faire, appuyez sur la touche de logo Windows+X, cliquez avec le bouton droit sur **Invite de commandes**, puis sélectionnez **Exécuter en tant qu'administrateur**. Le cas échéant, le système vous invite à taper un mot de passe administrateur ou à le confirmer.
2. À l'invite de commandes, exécutez la commande suivante :

   Invite de commandes Windows

   ```
   slmgr -ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
   ```

   > ⓘ **Notes**
   >
   > L'espace réservé **xxxxx-xxxxx-xxxxx-xxxxx représente** votre clé de produit MAK.

Revenez à la liste des procédures.

Configurer un hôte KMS sur lequel activer les clients

L'activation KMS nécessite qu'un hôte KMS soit configuré pour que les clients s'activent auprès de lui. S'il n'existe aucun hôte KMS configuré dans votre environnement, installez et activez-en un à l'aide d'une clé d'hôte KMS appropriée. Après avoir configuré un ordinateur sur le réseau pour héberger le logiciel KMS, publiez les paramètres DNS (Domain Name System).

Pour plus d'informations sur le processus de configuration de l'hôte KMS, consultez Activer à l'aide du service de gestion des cléset installer et configurer VAMT.

Revenez à la liste des procédures.

Vérifier la connectivité IP de base au serveur DNS

Vérifiez la connectivité IP de base au serveur DNS à l'aide de la commande ping. Pour ce faire, procédez comme suit sur le client KMS qui rencontre l'erreur et l'ordinateur hôte KMS :

1. Ouvrez une fenêtre d'invite de commandes avec privilèges élevés.
2. À l'invite de commandes, exécutez la commande suivante :

   Invite de commandes Windows

   ```
   ping <DNS_Server_IP_address>
   ```

   > ⓘ **Notes**
   >
   > Si la sortie de cette commande n'inclut pas l'expression « Répondre à partir de », il existe un problème réseau ou un problème DNS que vous devez résoudre avant de pouvoir utiliser les autres procédures de cet article. Pour plus d'informations sur la résolution des problèmes TCP/IP si vous ne pouvez pas effectuer un test ping sur le serveur DNS, consultez Résolution avancée des problèmes tcp/IP.

Revenez à la liste des procédures.

Vérifier la configuration de l'hôte KMS

Vérifiez le Registre du serveur hôte KMS pour déterminer s'il s'inscrit auprès du DNS. Par défaut, un serveur hôte KMS inscrit dynamiquement un enregistrement SRV DNS une fois toutes les 24 heures.

> ⓘ **Important**
>
> Suivez attentivement les étapes décrites dans cette section. Des problèmes graves peuvent se produire si vous modifiez le Registre de manière incorrecte. Avant de le modifier, sauvegardez le Registre afin de pouvoir le restaurer en cas de problème.

Pour vérifier ce paramètre, procédez comme suit :

1. Démarrez l'Éditeur du Registre. Pour ce faire, cliquez avec le bouton droit sur **Démarrer**, sélectionnez **Exécuter**, tapez **regedit**, puis appuyez sur Entrée.
2. Recherchez la sous-clé **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** (précédemment **SL** au lieu de

SoftwareProtectionPlatform dans Windows Server 2008 et Windows Vista) et vérifiez la valeur de l'entrée **DisableDnsPublishing** . Cette entrée a les valeurs possibles suivantes :

- **0** ou non défini (valeur par défaut) : le serveur hôte KMS inscrit un enregistrement SRV une fois toutes les 24 heures.
- **1** : Le serveur hôte KMS n'inscrit pas automatiquement les enregistrements SRV. Si votre implémentation ne prend pas en charge les mises à jour dynamiques, consultez Créer manuellement un enregistrement SRV KMS.

3. Si l'entrée **DisableDnsPublishing** est manquante, créez-la (le type est DWORD). Si l'inscription dynamique est acceptable, laissez la valeur non définie ou définissez-la sur **0**.

Revenez à la liste des procédures.

Déterminer le type de problème de routage

Vous pouvez utiliser les commandes suivantes pour déterminer s'il s'agit d'un problème de résolution de noms ou d'un problème d'enregistrement SRV.

1. Sur un client KMS, ouvrez une fenêtre d'invite de commandes avec élévation de privilèges.

2. À l'invite de commandes, exécutez les commandes suivantes :

   Invite de commandes Windows

   ```
   cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
   cscript \windows\system32\slmgr.vbs -ato
   ```

   > ⓘ **Notes**
   >
   > Dans cette commande, <KMS_FQDN> représente le nom de domaine complet (FQDN) de l'ordinateur hôte KMS et <le port représente le port> TCP utilisé par KMS.

   Si ces commandes résolvent le problème, il s'agit d'un problème d'enregistrement SRV. Vous pouvez le résoudre en utilisant l'une des commandes documentées dans l'affectation manuelle d'un hôte KMS à une procédure cliente KMS .

3. Si le problème persiste, exécutez les commandes suivantes :

   Invite de commandes Windows

   ```
   cscript \windows\system32\slmgr.vbs -skms <IP Address>:<port>
   ```

```
cscript \windows\system32\slmgr.vbs -ato
```

> ⓘ **Notes**
>
> Dans cette commande, <l'adresse> IP représente l'adresse IP de l'ordinateur hôte KMS et <le port> représente le port TCP utilisé par KMS.

Si ces commandes résolvent le problème, il s'agit probablement d'un problème de résolution de noms. Pour plus d'informations sur la résolution des problèmes, consultez la procédure de vérification de la configuration DNS.

4. Si aucune de ces commandes ne résout le problème, vérifiez la configuration du pare-feu de l'ordinateur. Toutes les communications d'activation qui se produisent entre les clients KMS et l'hôte KMS utilisent le port TCP 1688. Les pare-feu sur le client KMS et l'hôte KMS doivent autoriser la communication sur le port 1688.

Revenez à la liste des procédures.

Vérifier la configuration DNS

> ⓘ **Notes**
>
> Sauf indication contraire, suivez ces étapes sur un client KMS qui a rencontré l'erreur applicable.

1. Ouvrez une fenêtre d'invite de commandes avec élévation de privilèges
2. À l'invite de commandes, exécutez la commande suivante :

Invite de commandes Windows

```
IPCONFIG /all
```

3. Dans les résultats de la commande, notez les informations suivantes :

   - Adresse IP affectée de l'ordinateur client KMS
   - Adresse IP du serveur DNS principal que l'ordinateur client KMS utilise
   - Adresse IP de la passerelle par défaut utilisée par l'ordinateur client KMS
   - Liste de recherche de suffixes DNS utilisée par l'ordinateur client KMS

4. Vérifiez que les enregistrements SRV de l'hôte KMS sont inscrits dans le DNS. Pour cela, procédez comme suit :

a. Ouvrez une fenêtre d'invite de commandes avec privilèges élevés.
b. À l'invite de commandes, exécutez la commande suivante :

Invite de commandes Windows

```
nslookup -type=all _vlmcs._tcp>kms.txt
```

c. Ouvrez le fichier KMS.txt généré par la commande. Ce fichier doit contenir une ou plusieurs entrées qui ressemblent à l'entrée suivante :

```
_vlmcs._tcp.contoso.com SRV service location:
priority = 0
weight = 0
port = 1688 svr hostname = kms-server.contoso.com
```

> ⓘ **Notes**
>
> Dans cette entrée, contoso.com représente le domaine de l'hôte KMS.

i. Vérifiez l'adresse IP, le nom d'hôte, le port et le domaine de l'hôte KMS.
ii. Si ces **entrées _vlmcs** existent et si elles contiennent les noms d'hôtes KMS attendus, accédez à Affecter manuellement un hôte KMS à un client KMS.

> ⓘ **Notes**
>
> Si la commande **nslookup** recherche l'hôte KMS, cela ne signifie pas que le client DNS peut trouver l'hôte KMS. Si la commande **nslookup** recherche l'hôte KMS, mais que vous ne pouvez toujours pas l'activer à l'aide de l'hôte KMS, vérifiez les autres paramètres DNS, tels que le suffixe DNS principal et la liste de recherche du suffixe DNS.

5. Vérifiez que la liste de recherche du suffixe DNS principal contient le suffixe de domaine DNS associé à l'hôte KMS. Si la liste de recherche n'inclut pas ces informations, accédez à la procédure Configurer l'hôte KMS pour publier dans plusieurs domaines DNS.

Revenez à la liste des procédures.

Créer manuellement un enregistrement SRV KMS

Pour créer manuellement un enregistrement SRV pour un hôte KMS qui utilise un serveur DNS Microsoft, procédez comme suit :

1. Sur le serveur DNS, ouvrez le Gestionnaire DNS. Pour ouvrir le Gestionnaire DNS, sélectionnez **Démarrer**, sélectionnez **Outils d'administration**, puis **DNS**.
2. Sélectionnez le serveur DNS sur lequel vous devez créer l'enregistrement de ressource SRV.
3. Dans l'arborescence de la console, développez **Zones de recherche directe**, cliquez avec le bouton droit sur le domaine, puis sélectionnez **Autres nouveaux enregistrements**.
4. Faites défiler la liste, sélectionnez **Emplacement du service (SRV),** puis **sélectionnez Créer un enregistrement**.
5. Tapez les informations suivantes :

    - Service : **_VLMCS**
    - Protocole : **_TCP**
    - Numéro de port : **1688**
    - Hôte offrant le service : **<*nom de domaine complet de l'hôte KMS*>**

6. Lorsque vous avez terminé, sélectionnez **OK**, puis **sélectionnez Terminé**.

Pour créer manuellement un enregistrement SRV pour un hôte KMS qui utilise un serveur DNS conforme à BIND 9.x, suivez les instructions de ce serveur DNS et fournissez les informations suivantes pour l'enregistrement SRV :

- Nom : **_vlmcs._TCP**
- Type : **SRV**
- Priorité : **0**
- Poids : **0**
- Port : **1688**
- Nom d'hôte : **<*nom de domaine complet ou nom A de l'hôte KMS*>**

Pour configurer un serveur DNS compatible BIND 9.x pour prendre en charge la publication automatique KMS, configurez le serveur DNS pour activer les mises à jour des enregistrements de ressources à partir d'hôtes KMS. Par exemple, ajoutez la ligne suivante à la définition de zone dans Named.conf ou dans Named.conf.local :

Invite de commandes Windows

```
allow-update { any; };
```

Affecter manuellement un hôte KMS à un client KMS

Par défaut, les clients KMS utilisent le processus de découverte automatique. Selon ce processus, un client KMS interroge DNS pour obtenir la liste des serveurs qui ont publié `_vlmcs`

des enregistrements SRV dans la zone d'appartenance du client. DNS retourne la liste des hôtes KMS dans un ordre aléatoire. Le client sélectionne un hôte KMS et tente d'établir une session dessus. Si cette tentative fonctionne, le client met en cache le nom de l'hôte KMS et tente de l'utiliser pour la prochaine tentative de renouvellement. Si le programme d'installation de session échoue, le client choisit de façon aléatoire un autre hôte KMS. Nous vous recommandons vivement d'utiliser le processus de découverte automatique.

Toutefois, vous pouvez affecter manuellement un hôte KMS à un client KMS particulier. Pour ce faire, procédez comme suit.

1. Sur un client KMS, ouvrez une fenêtre d'invite de commandes avec élévation de privilèges.
2. Selon votre implémentation, effectuez l'une des étapes suivantes :

    - Pour affecter un hôte KMS à l'aide du nom de domaine complet de l'hôte, exécutez la commande suivante :

        Invite de commandes Windows

        ```
        cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
        ```

    - Pour affecter un hôte KMS à l'aide de l'adresse IP de la version 4 de l'hôte, exécutez la commande suivante :

        Invite de commandes Windows

        ```
        cscript \windows\system32\slmgr.vbs -skms <IPv4Address>:<port>
        ```

    - Pour affecter un hôte KMS à l'aide de la version 6 de l'adresse IP de l'hôte, exécutez la commande suivante :

        Invite de commandes Windows

        ```
        cscript \windows\system32\slmgr.vbs -skms <IPv6Address>:<port>
        ```

    - Pour affecter un hôte KMS à l'aide du nom NETBIOS de l'hôte, exécutez la commande suivante :

        Invite de commandes Windows

        ```
        cscript \windows\system32\slmgr.vbs -skms <NETBIOSName>:<port>
        ```

- Pour revenir à la découverte automatique sur un client KMS, exécutez la commande suivante :

  Invite de commandes Windows

  ```
  cscript \windows\system32\slmgr.vbs -ckms
  ```

  > **Notes**
  >
  > Ces commandes utilisent les espaces réservés suivants :
  > - < >**KMS_FQDN** représente le nom de domaine complet (FQDN) de l'ordinateur hôte KMS
  > - <**IPv4Address**> représente l'adresse IP version 4 de l'ordinateur hôte KMS
  > - <**IPv6Address**> représente l'adresse IP version 6 de l'ordinateur hôte KMS
  > - <**NETBIOSName**> représente le nom NETBIOS de l'ordinateur hôte KMS
  > - <**le port**> représente le port TCP utilisé par KMS.

Configurer l'hôte KMS à publier dans plusieurs domaines DNS

> **Important**
>
> Suivez attentivement les étapes décrites dans cette section. Des problèmes graves peuvent se produire si vous modifiez le Registre de manière incorrecte. Avant de le modifier, sauvegardez le Registre afin de pouvoir le restaurer en cas de problème.

Comme décrit dans l'affectation manuelle d'un hôte KMS à un client KMS, les clients KMS utilisent généralement le processus de découverte automatique pour identifier les hôtes KMS. Ce processus nécessite que les `_vlmcs` enregistrements SRV soient disponibles dans la zone DNS de l'ordinateur client KMS. La zone DNS correspond au suffixe DNS principal de l'ordinateur ou à l'un des éléments suivants :

- Pour les ordinateurs joints à un domaine, le domaine de l'ordinateur tel qu'il est affecté par le système DNS (par exemple, ACTIVE Directory Domain Services (AD DS) DNS).
- Pour les ordinateurs de groupe de travail, le domaine de l'ordinateur affecté par le protocole DHCP (Dynamic Host Configuration Protocol). Ce nom de domaine est défini par l'option qui a la valeur de code 15 telle que définie dans La requête de commentaires (RFC) 2132.

Par défaut, un hôte KMS inscrit ses enregistrements SRV dans la zone DNS qui correspond au domaine de l'ordinateur hôte KMS. Par exemple, supposons qu'un hôte KMS joint le domaine contoso.com. Dans ce scénario, l'hôte KMS inscrit son `_vlmcs` enregistrement SRV sous la zone DNS contoso.com. Par conséquent, l'enregistrement identifie le service en tant que `_VLMCS._TCP.CONTOSO.COM`.

Si l'hôte KMS et les clients KMS utilisent différentes zones DNS, vous devez configurer l'hôte KMS pour publier automatiquement ses enregistrements SRV dans plusieurs domaines DNS. Pour ce faire, procédez comme suit :

1. Sur l'hôte KMS, démarrez l'Éditeur du Registre.
2. Recherchez, puis sélectionnez la sous-clé **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** (précédemment **SL** au lieu de **SoftwareProtectionPlatform** dans Windows Server 2008 et Windows Vista).
3. Dans le volet **Détails** , cliquez avec le bouton droit sur une zone vide, sélectionnez **Nouveau**, puis sélectionnez **Valeur à plusieurs chaînes**.
4. Pour le nom de la nouvelle entrée, entrez **DnsDomainPublishList**.
5. Cliquez avec le bouton droit sur la nouvelle entrée **DnsDomainPublishList** , puis sélectionnez **Modifier**.
6. Dans la boîte de dialogue **Modifier plusieurs chaînes** , tapez chaque suffixe de domaine DNS publié par KMS sur une ligne distincte, puis sélectionnez **OK**.

   > ⓘ **Notes**
   >
   > Pour Windows Server 2008 R2, le format de **DnsDomainPublishList** diffère. Pour plus d'informations, voir le Guide des informations techniques de référence sur l'activation en volume.

7. Utilisez l'outil d'administration des services pour redémarrer le service De protection logicielle (précédemment le service de gestion des licences logicielles dans Windows Server 2008 et Windows Vista). Cette opération crée les enregistrements SRV.
8. Vérifiez qu'à l'aide d'une méthode classique, le client KMS peut contacter l'hôte KMS que vous avez configuré. Vérifiez que le client KMS identifie correctement l'hôte KMS à la fois par nom et par adresse IP. Si l'une de ces vérifications échoue, examinez ce problème de résolution de client DNS.
9. Pour effacer les noms d'hôtes KMS précédemment mis en cache sur le client KMS, ouvrez une fenêtre d'invite de commandes avec élévation de privilèges sur le client KMS, puis exécutez la commande suivante :

   ```
   Invite de commandes Windows
   ```

```
cscript C:\Windows\System32\slmgr.vbs -ckms
```

Regénérer le fichier Tokens.dat

14/08/2025

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

Lorsque vous résolvez les problèmes d'activation de Windows, vous devrez peut-être reconstruire le fichier Tokens.dat. Cet article décrit en détail comment procéder.

Résolution

Pour reconstruire le fichier Tokens.dat, procédez comme suit :

1. Ouvrez une fenêtre d'invite de commandes avec élévation de privilèges : **Pour Windows 10**
   a. Ouvrez le menu **Démarrer**, puis tapez **cmd**.
   b. Dans les résultats de la recherche, cliquez sur **Invite de commandes**, puis sélectionnez **Exécuter en tant qu'administrateur**.

   pour windows 8.1
   a. Balayez à partir du bord droit de l'écran, puis appuyez sur **Rechercher**. Ou, si vous utilisez une souris, pointez en bas à droite de l'écran, puis sélectionnez **Rechercher**.
   b. Dans le champ de recherche, entrez **cmd**.
   c. Balayez l'écran ou cliquez avec le bouton droit sur l'icône d'**invite de commandes** affichée.
   d. Appuyez ou cliquez sur **Exécuter en tant qu'administrateur**.

   pour windows 7
   a. Ouvrez le menu **Démarrer**, puis tapez **cmd**.
   b. Dans les résultats de la recherche, cliquez avec le bouton droit sur **cmd.exe**, puis sélectionnez **Exécuter en tant qu'administrateur**.

2. Entrez la liste des commandes appropriées pour votre système d'exploitation.

   Pour Windows 10, Windows Server 2016 et versions ultérieures de Windows, entrez les commandes suivantes dans la séquence :

   Invite de commandes Windows

   ```
   net stop sppsvc
   cd %Systemdrive%\Windows\System32\spp\store\2.0\
   ren tokens.dat tokens.bar
   ```

```
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

Pour Windows 8.1, Windows Server 2012 et Windows Server 2012 R2, entrez les commandes suivantes dans la séquence :

Invite de commandes Windows

```
net stop sppsvc
cd %Systemdrive%\Windows\System32\spp\store\
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

Pour Windows 7, Windows Server 2008 et Windows Server 2008 R2, entrez les commandes suivantes dans la séquence :

Invite de commandes Windows

```
net stop sppsvc
cd
%Systemdrive%\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsof
t\SoftwareProtectionPlatform
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

3. Redémarrez l'ordinateur.

Plus d'informations

Après avoir régénéré le fichier Tokens.dat, vous devez réinstaller votre clé de produit à l'aide de l'une des méthodes suivantes :

- À la même invite de commandes avec élévation de privilèges, tapez la commande suivante, puis appuyez sur Entrée :

Invite de commandes Windows

```
cscript.exe %windir%\system32\slmgr.vbs /ipk <Product key>
```

> ⓘ **Important**

N’utilisez pas le commutateur **/upk** pour désinstaller une clé de produit. Pour installer une clé de produit sur une clé de produit existante, utilisez le commutateur **/ipk**.

- Cliquez avec le bouton droit sur **Mon ordinateur**, sélectionnez **Propriétés**, puis **Modifier la clé de produit**.

Pour plus d’informations sur les clés de configuration du client KMS, consultez clés de configuration du client KMS.

Options de déploiement de l'agent Azure Connected Machine

Vous pouvez connecter des machines dans votre environnement hybride directement avec Azure à l'aide de différentes méthodes, en fonction de vos besoins et des outils que vous préférez utiliser.

Méthodes d'intégration

Le tableau suivant met en évidence chaque méthode afin que vous puissiez déterminer celle qui convient le mieux à votre déploiement. Pour plus d'informations, suivez les liens pour afficher les étapes de chaque méthode.

Agrandir le tableau

Type de système d'exploitation pris en charge	Méthode	Description
Linux et Windows	de manière interactive	Installez manuellement l'agent sur un seul ou petit nombre de machines pour connecter des machines à l'aide d'un script de déploiement. À partir du portail Azure, vous pouvez générer un script et l'exécuter sur la machine pour automatiser les étapes d'installation et de configuration de l'agent.
Linux et Windows	De manière interactive ou à grande échelle	Connectez des machines à l'aide de PowerShell.
Linux et Windows	À grande échelle	Connectez des machines à grande échelle avec Ansible à l'aide du rôle d'intégration Azure Arc dans Ansible Core ou Ansible Automation Platform.
Linux et Windows	À grande échelle	Connectez des machines à l'aide d'un principal de service pour installer l'agent à grande échelle de manière non interactive.
Linux et Windows	À grande échelle	Installez l'agent Azure Arc sur des machines virtuelles VMware à grande échelle à l'aide de VMware vSphere avec Azure Arc. Avec VMware vSphere avec Azure Arc, vous pouvez connecter votre serveur VMware vCenter à Azure, découvrir automatiquement vos machines virtuelles VMware et installer l'agent Azure Arc sur ces

Type de système d'exploitation pris en charge	Méthode	Description
		machines virtuelles. Nécessite des outils VMware sur des machines virtuelles.
Linux et Windows	À grande échelle	Connectez votre cloud AWS via le connecteur multicloud activé par Azure Arc et activez la solutiond'intégration Arc pour la découverte automatique et l'intégration de machines virtuelles EC2.
Fenêtres	de manière interactive	Connecter des ordinateurs à partir de Windows Admin Center.
Fenêtres	de manière interactive	Connectez des machines Windows Server à Azure via la configuration d'Azure Arc.
Fenêtres	À grande échelle	Connectez des machines en exécutant des scripts PowerShell avec Configuration Manager.
Fenêtres	À grande échelle	Connecter des machines avec une séquence de tâches personnalisée Configuration Manager.
Fenêtres	À grande échelle	Connectez des machines Windows à l'aide de la stratégie de groupe.

> **ⓘ Important**
>
> Vous ne pouvez pas installer l'agent Connected Machine sur une machine virtuelle Azure. Le script d'installation vous avertit et effectue une restauration s'il détecte que le serveur s'exécute dans Azure.

Veillez à passer en revue les conditions préalables de base et les exigences de configuration réseau avant de déployer l'agent et les exigences spécifiques répertoriées dans les étapes de la méthode d'intégration que vous choisissez. Pour en savoir plus sur les modifications apportées par l'agent à votre système, consultez Vue d'ensemble de l'agent Azure Connected Machine.

Connexion automatique du serveur SQL

Lorsque vous connectez un serveur Windows ou Linux à Azure Arc sur lequel Microsoft SQL Server est également installé, les instances SQL Server sont également connectées automatiquement à Azure Arc. SQL Server activé par Azure Arc fournit un inventaire détaillé et des fonctionnalités de gestion supplémentaires pour vos instances et bases de données SQL Server. Dans le cadre du processus de connexion, une extension est déployée sur votre serveur

avec Azure Arc et les nouveaux rôles sont appliqués à vos bases de données et sql Server. Si vous ne souhaitez pas connecter automatiquement vos serveurs SQL à Azure Arc, vous pouvez choisir d'ajouter une balise au serveur Windows ou Linux avec le nom `ArcSQLServerExtensionDeployment` et la valeur `Disabled` lors de sa connexion à Azure Arc.

Pour plus d'informations, consultez Gérer la connexion automatique pour SQL Server activée par Azure Arc.

Contenu connexe

- Découvrez-en plus sur les prérequis et la configuration réseau requise de l'agent Azure Connected Machine.
- Passez en revue le guide de planification et de déploiement pour les serveurs avec Azure Arc.
- Apprenez-en davantage sur la reconfiguration, la mise à niveau et la suppression de l'agent Connected Machine.
- Essayez des serveurs avec Azure Arc à l'aide d'Azure Arc Jumpstart.

Last updated on 14/08/2026

Connecter des machines Windows Server à Azure via le programme d'installation d'Azure Arc

Vous pouvez intégrer des machines Windows Server directement à Azure Arc via un Assistant graphique inclus dans Windows Server. L'Assistant automatise le processus d'intégration en vérifiant les prérequis nécessaires pour réussir l'intégration d'Azure Arc, puis en récupérant et en installant la dernière version de l'agent Azure Connected Machine (AzCM). Une fois le processus de l'Assistant terminé, vous êtes dirigé vers votre machine Windows Server dans le portail Azure, où vous pouvez l'afficher et le gérer comme n'importe quelle autre ressource activée par Azure Arc.

Si la machine Windows Server est déjà en cours d'exécution dans Azure, il n'est pas nécessaire d'intégrer Azure Arc.

Pour Windows Server 2022, le programme d'installation d'Azure Arc est un composant facultatif que vous pouvez supprimer à l'aide de **l'Assistant Suppression de rôles et de fonctionnalités**. Pour Windows Server 2025 et versions ultérieures, le programme d'installation d'Azure Arc est une fonctionnalité à la demande. Les procédures de suppression et d'activation diffèrent entre les versions du système d'exploitation.

> **Remarque**
>
> La fonctionnalité Azure Arc Setup s'applique uniquement à Windows Server 2022 et versions ultérieures. Il a été publié dans la mise à jour cumulative du 10/10/2023.

Connexion automatique pour SQL Server

Lorsque vous connectez un serveur Windows ou Linux à Azure Arc sur lequel Microsoft SQL Server est également installé, les instances SQL Server sont également connectées automatiquement à Azure Arc. SQL Server activé par Azure Arc fournit un inventaire détaillé et des fonctionnalités de gestion supplémentaires pour vos instances et bases de données SQL Server. Dans le cadre du processus de connexion, une extension est déployée sur votre serveur avec Azure Arc et les nouveaux rôles sont appliqués à vos bases de données et votre SQL Server. Si vous ne souhaitez pas connecter automatiquement vos serveurs SQL à Azure Arc, vous pouvez choisir d'ajouter une balise au serveur Windows ou Linux avec le nom `ArcSQLServerExtensionDeployment` et la valeur `Disabled` lors de sa connexion à Azure Arc.

Pour plus d'informations, consultez Gérer la connexion automatique pour une instance SQL Server activée par Azure Arc.

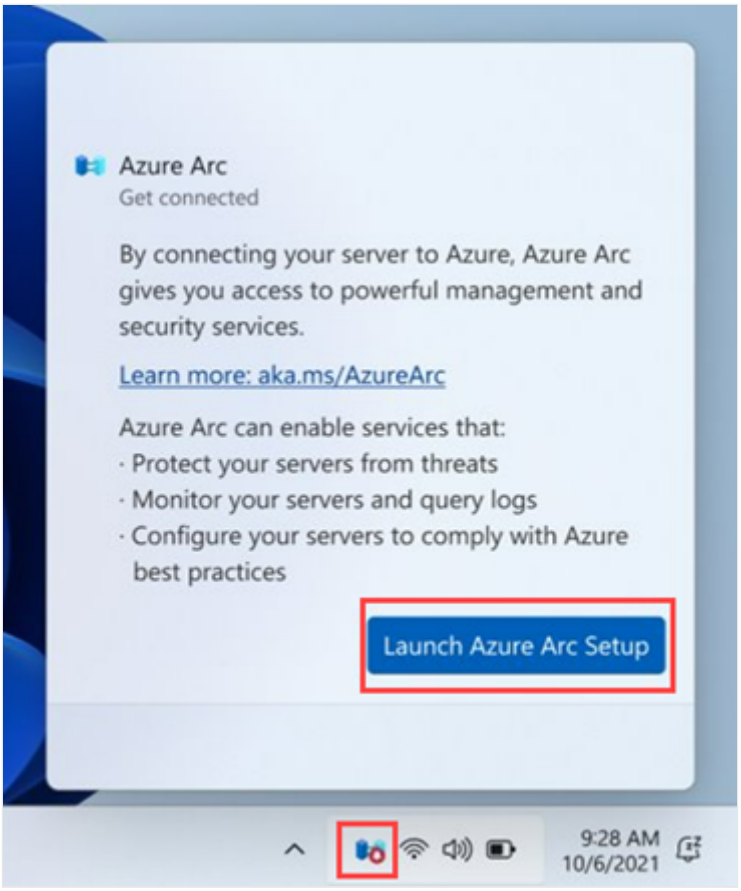
Conditions préalables

- Passez en revue les conditions préalables requises pour les serveurs avec Azure Arc et vérifiez que votre abonnement, votre compte Azure et vos ressources répondent aux exigences.
- Un abonnement Azure. Si vous n'en avez pas, créez un compte gratuit avant de commencer.
- Navigateur moderne (Microsoft Edge) pour l'authentification auprès de Microsoft Azure. La configuration de l'agent Azure Connected Machine nécessite une authentification auprès de votre compte Azure, soit via l'authentification interactive sur un navigateur moderne ou l'authentification du code d'appareil sur un appareil distinct (si la machine n'a pas de navigateur moderne).

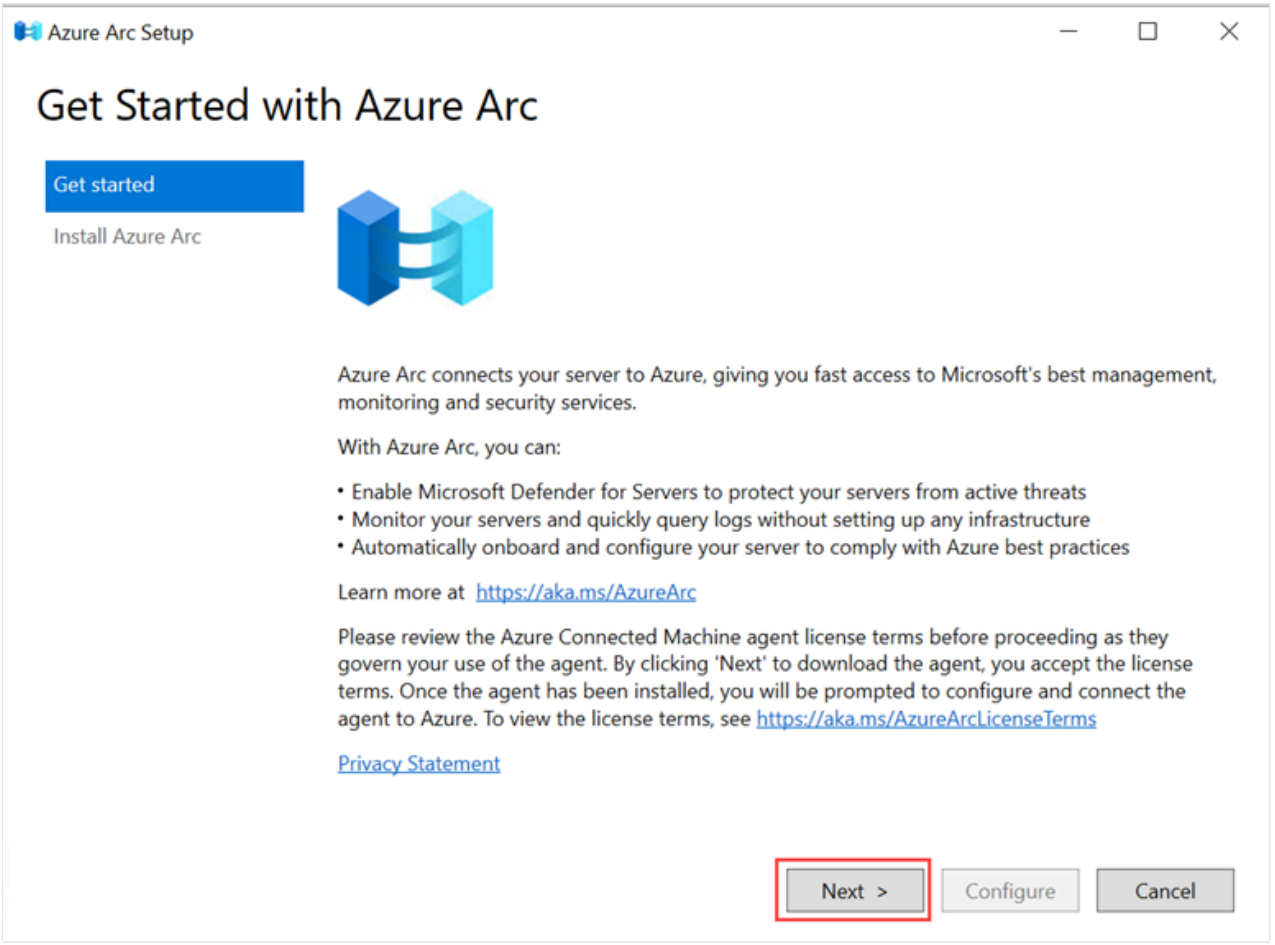
Lancer le programme d'installation d'Azure Arc et se connecter à Azure Arc

L'Assistant d'installation d'Azure Arc est lancé à partir d'une icône de barre d'état système en bas de la machine Windows Server lorsque la fonctionnalité d'installation d'Azure Arc est activée. Cette fonctionnalité est activée par défaut. Vous pouvez également lancer l'Assistant à partir d'une fenêtre contextuelle dans le Gestionnaire de serveur ou à partir du menu Démarrer de Windows Server.

1. Sélectionnez l'icône de barre d'état système Azure Arc, puis **lancez le programme d'installation d'Azure Arc**.



2. La fenêtre d'introduction de l'Assistant Installation d'Azure Arc explique les avantages de l'intégration de votre machine à Azure Arc. Lorsque vous êtes prêt à continuer, sélectionnez **Suivant**.



3. L'Assistant vérifie automatiquement les prérequis nécessaires pour installer l'Azure Connected Machine Agent sur votre ordinateur Windows Server. Une fois ce processus terminé et que l'agent est installé, sélectionnez **Configurer**.

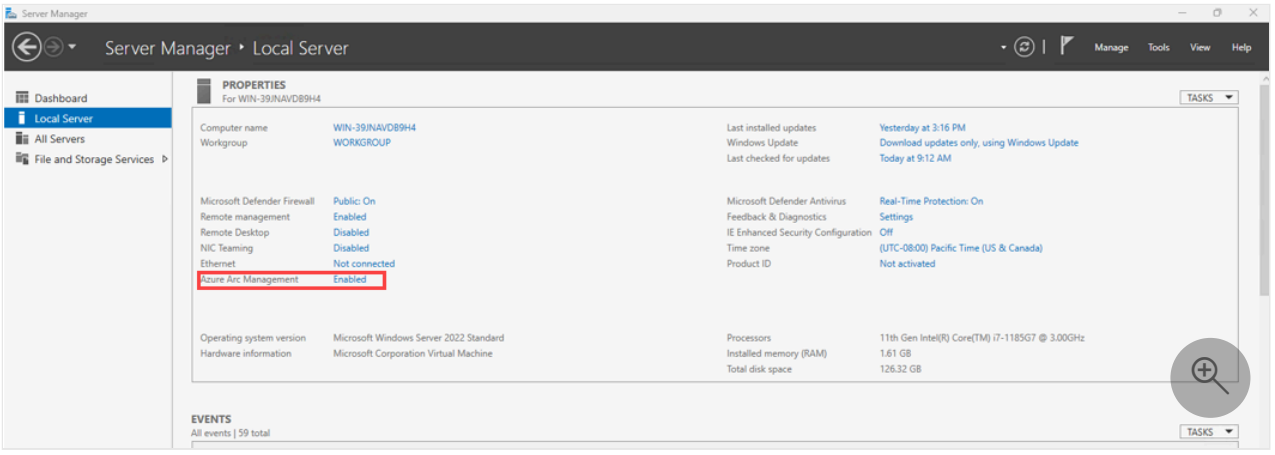
4. La fenêtre de configuration explique les étapes requises pour configurer l'agent Azure Connected Machine. Lorsque vous êtes prêt à commencer la configuration, sélectionnez **Suivant**.

5. Connectez-vous à Azure en sélectionnant le cloud Azure applicable, puis en sélectionnant **Se connecter à Azure**. Fournissez vos informations d'identification de connexion.

6. Dans les **détails de la ressource**, spécifiez les détails de la façon dont votre machine doit être représentée dans Azure, notamment le locataire, l'abonnement et le groupe de ressources. Cliquez sur **Suivant**.

7. Une fois la configuration terminée et que votre machine est intégrée à Azure Arc, sélectionnez **Terminer**.

8. Accédez au Gestionnaire de serveur et sélectionnez **Serveur local** pour afficher l'état de la machine dans le champ **Gestion d'Azure Arc**. Un ordinateur correctement intégré a l'état **Activé**.



Fonctions du Gestionnaire de serveur

Vous pouvez sélectionner le lien **Activé/désactivé** dans le champ **Gestion d'Azure Arc** du Gestionnaire de serveur pour lancer différentes fonctions en fonction de l'état de la machine :

- Si le programme d'installation d'Azure Arc n'est pas installé, la sélection de **Activé/désactivé** lance l'**Assistant Ajout de rôles et de fonctionnalités** .
- Si le programme d'installation d'Azure Arc est installé et que l'agent Azure Connected Machine n'est pas installé, sélectionner **Désactivé** lance `AzureArcSetup.exe`, le fichier exécutable de l'Assistant Installation d'Azure Arc.

- Si le programme d'installation d'Azure Arc est installé et que l'Azure Connected Machine Agent est déjà installé, la sélection de **Activé/désactivé** lance `AzureArcConfiguration.exe`, le fichier exécutable permettant de configurer l'Azure Connected Machine Agent pour qu'il fonctionne avec votre machine.

Afficher l'ordinateur connecté

L'icône de la barre d'état système Azure Arc située en bas de votre machine Windows Server indique si la machine est connectée à Azure Arc. Un symbole rouge signifie que l'ordinateur n'a pas installé l'agent Azure Connected Machine.

Pour afficher une machine connectée dans Azure Arc, sélectionnez l'icône, puis sélectionnez **Afficher la machine dans Azure**. Vous pouvez ensuite afficher la machine dans le portail Azure, comme vous le feriez pour d'autres ressources avec Azure Arc.

Désinstaller le programme d'installation d'Azure Arc

> **Remarque**
>
> La désinstallation du programme d'installation d'Azure Arc ne désinstalle pas l'agent Azure Connected Machine de la machine. Pour obtenir des instructions sur la désinstallation de l'agent, consultez Gestion et maintenance de l'Azure Connected Machine Agent.

Pour désinstaller Azure Arc Setup d'une machine Windows Server 2022 :

1. Dans le Gestionnaire de serveur, accédez à **l'Assistant Suppression de rôles et de fonctionnalités**.
2. Dans la page **Fonctionnalités** , décochez la case pour le **programme d'installation d'Azure Arc**.
3. Dans la page de confirmation, sélectionnez **Redémarrer automatiquement le serveur de destination si nécessaire**, puis sélectionnez **Supprimer**.

Pour désinstaller le programme d'installation d'Azure Arc via PowerShell, exécutez la commande suivante :

```
PowerShell
```

```
Disable-WindowsOptionalFeature -Online -FeatureName AzureArcSetup
```

Pour désinstaller Azure Arc Setup d'une machine Windows Server 2025 :

1. Ouvrez l'application Paramètres sur l'ordinateur, sélectionnez **Système**, puis sélectionnez **Fonctionnalités facultatives**.

2. Sélectionnez **AzureArcSetup**, puis **Supprimer**.

Pour désinstaller Azure Arc Setup d'une machine Windows Server 2025 à partir de la ligne de commande, exécutez la ligne de commande de code :

```
DISM /online /Remove-Capability /CapabilityName:AzureArcSetup~~~~
```

Contenu connexe

- Découvrez comment résoudre les problèmes liés à l'agent Azure Connected Machine.
- Consultez le Guide de planification et de déploiement pour planifier le déploiement de serveurs avec Azure Arc à n'importe quelle échelle et implémenter la gestion et la supervision centralisées.
- Pour plus d'informations sur les licences Windows Server sur une base de paiement par utilisation pour vos serveurs avec Arc, consultez Paiement à l'utilisation de Windows Server.

Last updated on 09/02/2026

Comment obtenir des mises à jour de sécurité étendues (ESU) pour Windows Server

Article • 23/05/2025 • S'applique à: ✅ Windows Server 2012, ✅ Windows Server 2012 R2

Les mises à jour de sécurité étendues (ESU) pour Windows Server incluent les mises à jour de sécurité et les bulletins évalués *critiques* et *importants*. Avant d'utiliser les mises à jour de sécurité étendues, il est recommandé de lire Vue d'ensemble des mises à jour de sécurité étendues pour Windows Server pour comprendre ce que sont les mises à jour de sécurité étendues, la durée pendant laquelle elles sont disponibles et les options dont vous disposez.

Comment obtenir des unités d'ESU dépend de l'emplacement d'hébergement de votre serveur. Vous pouvez accéder aux unités d'ESU via les options suivantes.

- **Machines virtuelles Azure : les machines virtuelles** applicables hébergées dans Azure sont automatiquement activées pour les ESU et ces mises à jour sont fournies gratuitement, il n'est pas nécessaire de déployer une clé MAK ou d'effectuer d'autres actions. Pour plus d'informations, consultez Mises à jour de sécurité étendues sur Azure.

- **Serveurs avec Azure Arc** : si vos serveurs sont locaux ou dans un environnement hébergé, vous pouvez inscrire vos machines Windows Server 2012 et 2012 R2 ou SQL Server 2012 pour les mises à jour de sécurité étendues via le portail Azure via Azure Arc. Une fois inscrit, vous êtes facturé mensuellement via votre abonnement Azure. Pour en savoir plus, consultez Les mises à jour de sécurité étendues activées par Azure Arc . [1]

- **Machines physiques et virtuelles non-Azure** : si vous ne pouvez pas vous connecter à l'aide d'Azure Arc, utilisez des mises à jour de sécurité étendues sur des machines virtuelles non-Azure, en utilisant une clé d'activation multiple (MAK) et en l'appliquant aux serveurs appropriés. Cette clé MAK permet aux serveurs Windows Update de savoir que vous pouvez continuer à recevoir des mises à jour de sécurité. Pour plus d'informations, consultez Accéder à votre clé d'activation multiple à partir du Centre d'administration Microsoft 365 . [1]

[1] Lorsque vous utilisez des serveurs avec Azure Arc et des machines autres qu'Azure, vous devez acheter des unités d'ESU. Pour acheter des ESU, vous devez disposer de Software Assurance via des programmes de licence en volume tels qu'un contrat Entreprise (EA), un abonnement Contrat Entreprise (EAS), l'inscription pour les solutions Éducation (EES) ou l'inscription au serveur et au cloud (SCE).

> ⓘ **Notes**

La mise à disposition de votre clé d'activation multiple peut prendre 3 à 5 jours ouvrables après l'achat d'unités d'ESU pour les machines virtuelles locales ou les serveurs physiques. Votre organisation peut également nécessiter du temps pour planifier et déployer les nouvelles clés. Avant d'acheter des unités d'ESU, vous devez garder ces délais à l'esprit.

Mises à jour de sécurité étendues sur Azure

Les machines virtuelles applicables hébergées dans Azure sont automatiquement activées pour l'ESU et ces mises à jour sont fournies gratuitement. Vous n'avez pas besoin de configurer quoi que ce soit, et il n'existe aucun frais supplémentaire pour l'utilisation des ESU avec des machines virtuelles Azure. Les unités d'ESU sont automatiquement remises aux machines virtuelles Azure si elles sont configurées pour recevoir des mises à jour.

Notes

Les mises à jour de sécurité étendues sont également gratuites dans certains produits Azure. Ces produits incluent Azure Dedicated Host, Azure VMware Solution, Azure Nutanix Solution, Azure Local et Azure Stack Hub et Edge. Certains de ces produits peuvent nécessiter une configuration supplémentaire. Pour plus d'aide, contactez le support Microsoft .

Les machines virtuelles Azure Classic (Microsoft.ClassicCompute) nécessitent également une configuration supplémentaire pour recevoir des mises à jour de sécurité étendues, car elles n'ont pas accès au service de métadonnées d'instance Azure qui détermine l'éligibilité des ESU.

Mises à jour de sécurité étendues activées par Azure Arc

Les mises à jour de sécurité étendues sont distribuées automatiquement aux serveurs avec Azure Arc s'ils sont connectés et inscrits aux mises à jour de sécurité étendues via Azure Arc. Cela peut également s'appliquer aux serveurs non Azure connectés à Azure Arc.

Vous pouvez souscrire à grande échelle à des unités ESU à l'aide d'Azure Policy ou du portail Azure. Il n'y a pas de frais initiaux, et vous êtes facturé mensuellement via votre abonnement Azure. Vous n'avez pas besoin d'activer de clés de produit.

Les serveurs avec Azure Arc vous permettent également d'utiliser d'autres services Azure, tels que :

- Azure Update Manager.
- Microsoft Defender pour le cloud.
- Azure Policy (Configuration de machine).
- Azure Monitor (VM Insights).

À partir de septembre 2023, vous pouvez activer Windows Server 2012 et 2012 R2 ESU via Azure Arc. Vous pouvez connecter des serveurs Windows Server 2012 et 2012 R2 à Azure Arc aujourd'hui, connecter des machines hybrides avec des serveurs avec Azure Arc.

Pour préparer l'activation de Windows Server 2012 et 2012R2 ESU sur vos serveurs avec Arc, procédez comme suit :

1. Connectez-vous au portail Azure.
2. Dans la barre de recherche, entrez *Serveurs - Azure Arc* et sélectionnez l'entrée de service correspondante.
3. Ajoutez votre machine Windows Server 2012 ou 2012 R2 existante à Azure Arc. Pour en savoir plus sur la prise en main des serveurs avec Azure Arc, consultez Connecter des machines hybrides avec des serveurs avec Azure Arc.

Pour en savoir plus sur les ESU avec Azure Arc, consultez Préparer la mise à jour de sécurité étendue pour Windows Server 2012 et fournir des mises à jour de sécurité étendues pour Windows 2012 et 2012 R2.

Accéder à votre clé d'activation multiple à partir du Centre d'administration Microsoft 365

Les clients qui ne peuvent pas se connecter à Azure Arc pour appliquer des ESU peuvent utiliser plusieurs clés d'activation (MAK) via le Centre d'administration Microsoft 365 :

1. Connectez-vous au Centre Administrateur Microsoft 365.
2. Sélectionner **les contrats d'affichage des licences en > volume de vos produits >**
3. Sélectionnez votre numéro de contrat utilisé pour acheter des unités d'ESU, les trois points en regard de celui-ci (icône Autres actions), puis sélectionnez **Afficher les clés de produit**. Toutes les clés de produit disponibles pour le contrat affiché sur cette page.
4. Une fois que vous disposez de votre clé MAK, installez la nouvelle clé sur vos serveurs éligibles. Pour en savoir plus sur l'installation et l'activation de votre clé MAK, consultez notre billet de blog Tech Community Obtention des mises à jour de sécurité étendues pour les appareils Windows éligibles.

Téléchargement et installation des mises à jour de sécurité étendues

La remise, le téléchargement et l'application d'ESU pour Windows Server ne diffèrent pas des autres mises à jour Windows. Les mises à jour fournies via les unités d'ESU sont uniquement des mises à jour *de sécurité* .

Avant de pouvoir télécharger et installer des ESU, vous devez avoir installé la dernière mise à jour de la pile de maintenance (SSU) et le package de préparation des licences. Pour en savoir plus sur les étapes nécessaires à l'installation du dernier package de préparation de l'authentification unique et de la préparation des licences, consultez KB5031043 : Procédure pour continuer à recevoir des mises à jour de sécurité après la fin du support étendu le 10 octobre 2023 .

Vous pouvez installer les mises à jour à l'aide des outils et processus que vous avez déjà en place. La seule différence est que le système doit être inscrit avec la clé générée dans la section précédente. Une fois le système inscrit, les mises à jour seront téléchargées et installées.

Pour les machines virtuelles hébergées dans Azure, le processus d'activation du serveur pour les ESU est automatiquement terminé pour vous. Les mises à jour doivent être téléchargées et installées sans configuration supplémentaire.

Fournir des mises à jour de sécurité étendues pour Windows Server

Cet article décrit les étapes permettant d'activer la distribution des mises à jour de sécurité étendues (ESU) aux machines Windows Server intégrées aux serveurs avec Arc. Vous pouvez activer les unités d'ESU sur ces machines individuellement ou à grande échelle. Les étapes s'appliquent à Windows Server 2012/2012 R2 et Windows Server 2016. Utilisez le sélecteur en haut de l'article pour choisir la version du système d'exploitation pour laquelle vous obtenez une licence.

Avant de commencer

Planifiez et préparez l'intégration de vos machines à des serveurs avec Azure Arc. Pour plus d'informations, consultez Se préparer à déployer les mises à jour de sécurité étendues pour Windows Server.

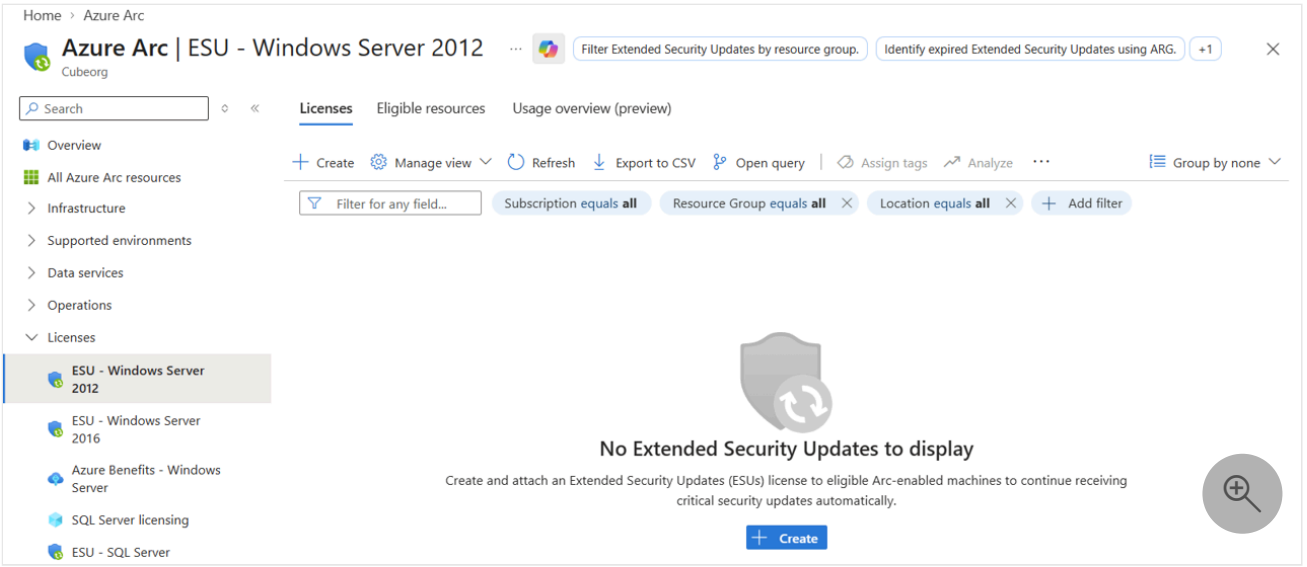
Vous avez également besoin du rôle Contributeur dans Azure RBAC pour créer et affecter des ESU aux serveurs avec Arc.

Gérer les licences ESU

> **Important**
>
> La période Windows Server 2012 et Windows Server 2012 R2 ESU se termine le 13 octobre 2026. La mise à jour de sécurité du 13 octobre 2026 est la dernière mise à jour fournie via les ESU. À minuit temps universel coordonné (UTC) le 14 octobre 2026, les licences ESU activées par Azure Arc se désactivent. Les ressources de licence restent disponibles pour l'affichage dans Azure, mais les serveurs liés à elles ne sont pas éligibles pour les mises à jour de sécurité publiées après le 13 octobre 2026. Migrez vos charges de travail ou mettez à niveau vers une version prise en charge de Windows Server avant la fin de la période ESU.

1. Dans votre navigateur, connectez-vous au portail Azure.

2. Dans le menu du service, sous **Licences**, sélectionnez **Licences Windows Server ESU**.



À partir de là, vous pouvez afficher et créer des **licences ESU** et afficher **ressources éligibles** pour les ESU.

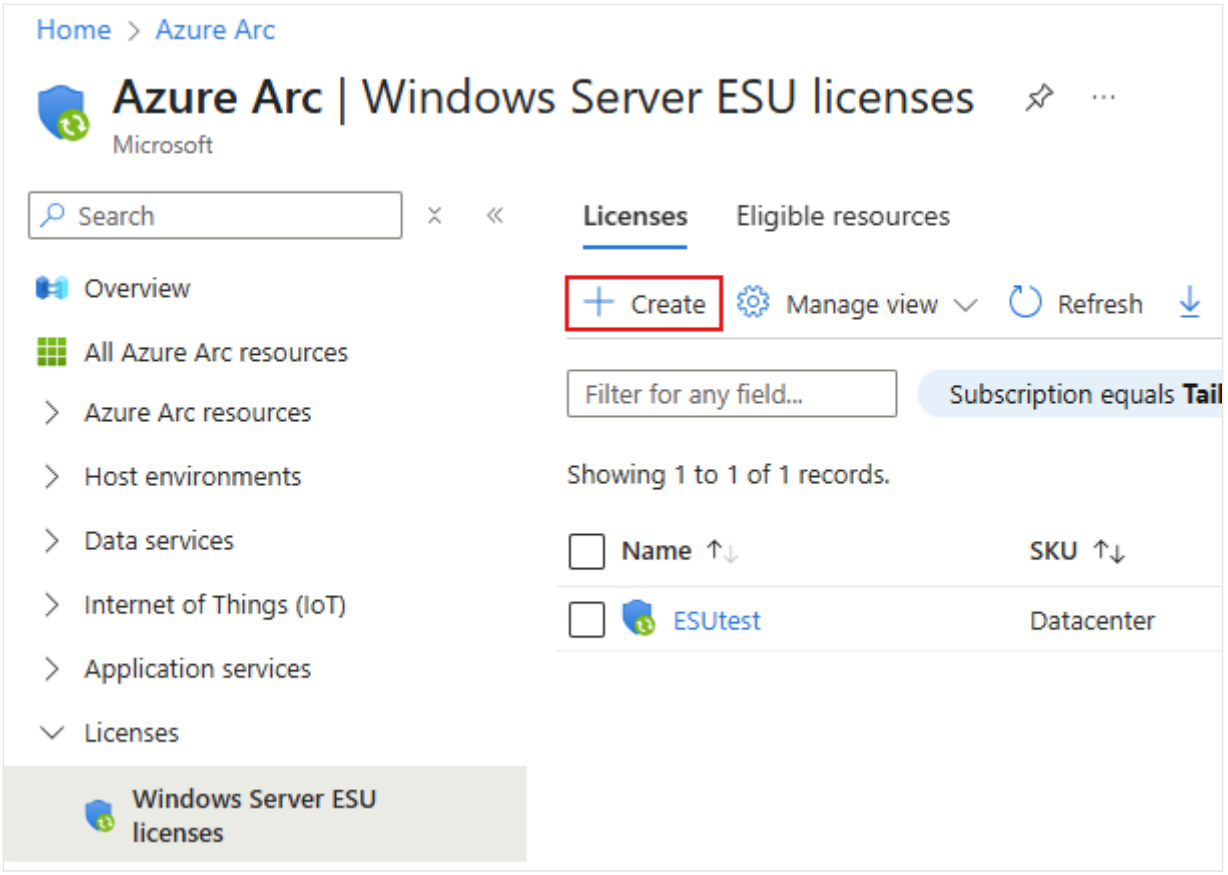
Créer des licences Azure Arc Windows Server

Tout d'abord, approvisionnez des licences de mise à jour de sécurité étendues à partir de Azure Arc. Liez ces licences à un ou plusieurs serveurs avec Arc que vous sélectionnez dans la section suivante.

> ⓘ **Remarque**
>
> Pour attribuer des licences ESU, vous devez attester qu'elles sont couvertes par SA ou SPLA.

Après avoir approvisionné une licence ESU, spécifiez la référence SKU (Standard ou Datacenter), le type de cœurs (physique ou vCore) et le nombre de cœurs. Vous pouvez également provisionner une licence de mise à jour de sécurité étendue dans un état désactivé afin qu'elle ne lance pas la facturation ou ne soit pas fonctionnelle lors de la création. Vous pouvez modifier les cœurs associés à la licence après le provisionnement.

L'onglet **Licences** affiche Azure Arc Windows Server licences disponibles. À partir de là, vous pouvez sélectionner une licence existante à appliquer ou créer une licence.



1. Pour créer une licence Windows Server, sélectionnez **Créer**, puis fournissez les informations requises pour configurer la licence sur la page.

   Pour plus d'informations sur la procédure d'exécution de cette étape, consultez les instructions d'approvisionnement de licence pour les mises à jour de sécurité étendues pour Windows Server.

2. Passez en revue les informations fournies, puis sélectionnez **Créer**.

   La licence que vous avez créée apparaît dans la liste. Vous pouvez le lier à un ou plusieurs serveurs avec Arc en suivant les étapes décrites dans la section suivante.

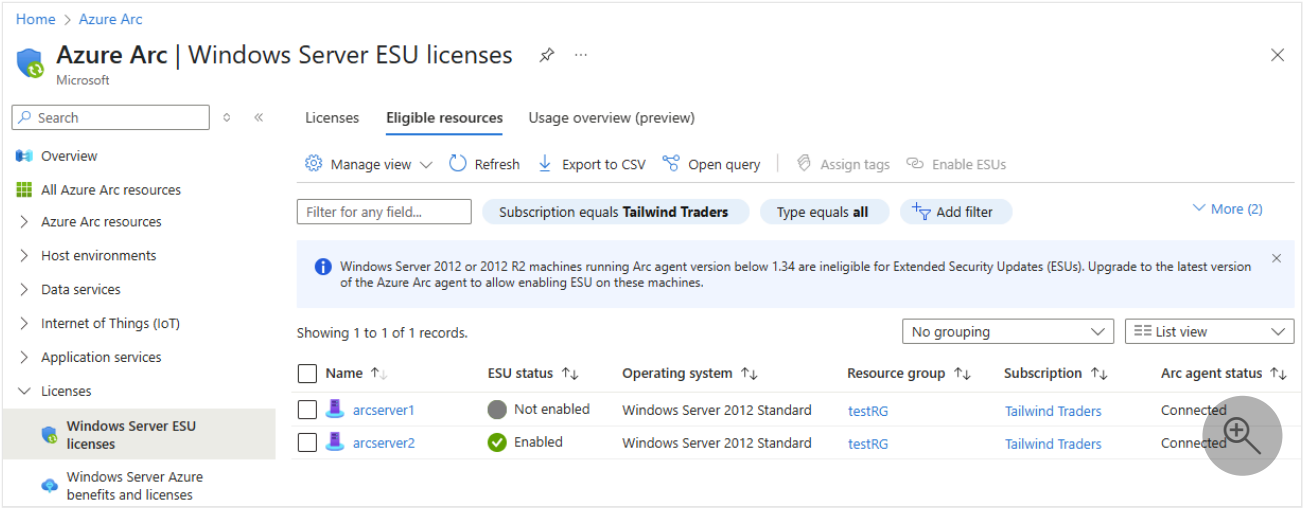
Lier des licences ESU aux serveurs avec Arc

Sélectionnez un ou plusieurs serveurs compatibles Arc pour établir un lien vers une licence de mise à jour de sécurité étendue. Une fois que vous avez lié un serveur à une licence ESU activée, le serveur peut recevoir Windows Server ESU.

> ⓘ **Remarque**
>
> Vous avez la possibilité de configurer votre solution de mise à jour corrective de votre choix pour recevoir ces mises à jour, que ce soit Update Manager, Windows Server Update

Services, Microsoft Updates, Microsoft Endpoint Configuration Manager ou une solution de gestion des correctifs tierce.

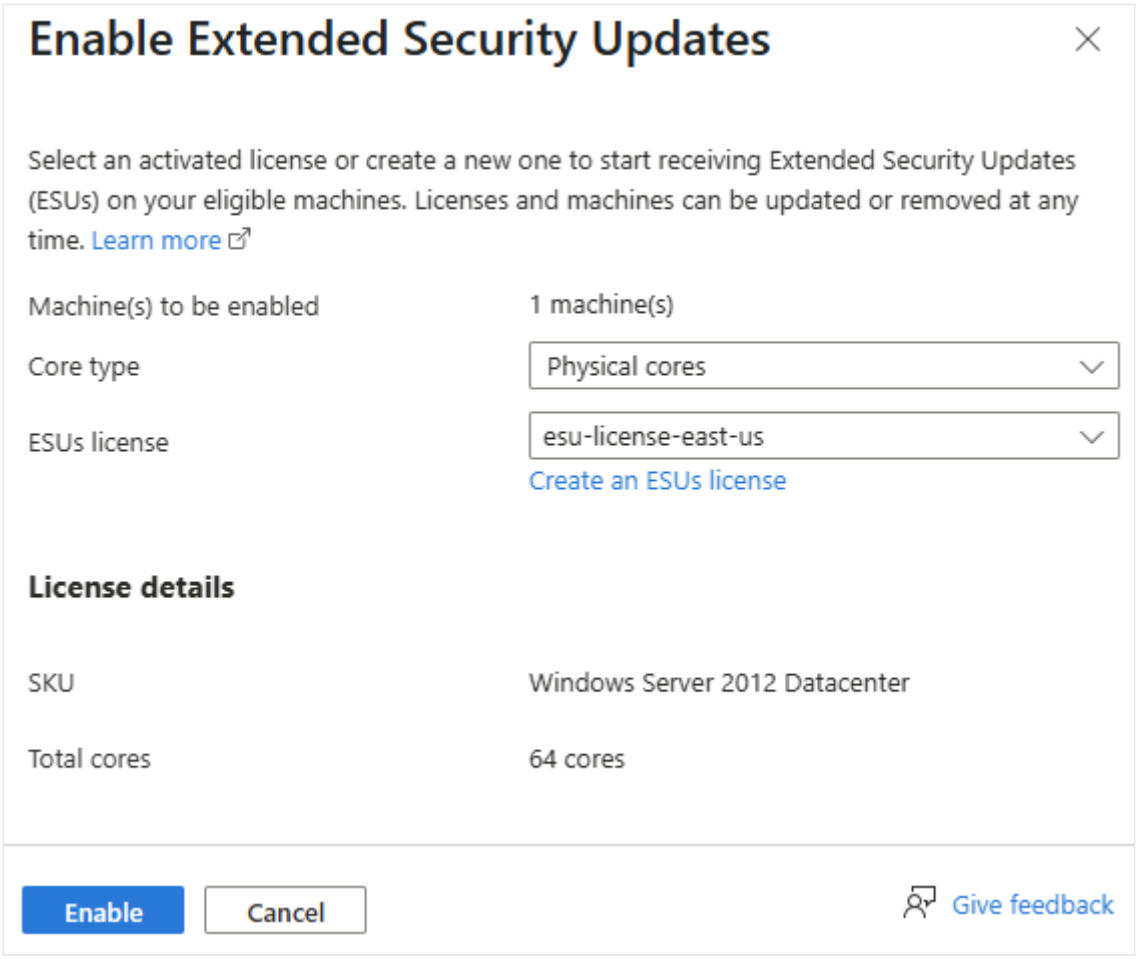
1. Sélectionnez l'onglet **Ressources éligibles** pour afficher la liste de tous vos serveurs avec Arc exécutant Windows Server 2012 et 2012 R2.



   La colonne **d'état des unités d'ESU** indique si la machine est activée pour les unités d'ESU.

2. Pour activer les unités d'ESU pour une ou plusieurs machines, sélectionnez-les dans la liste, puis sélectionnez **Activer les unités d'ESU**.

Dans le volet **Activer les mises à jour de sécurité étendues**, s'affiche le nombre d'ordinateurs sélectionnés pour activer l'ESU et les licences Windows Server disponibles pour s'appliquer. Sélectionnez une licence pour créer un lien vers les ordinateurs sélectionnés, puis sélectionnez **Activer**.



> ⓘ **Remarque**
>
> Vous pouvez créer une licence à partir de cette page, plutôt que de choisir une licence existante, en sélectionnant **Créer une licence ESU**.

Lorsque vous revenez à l'onglet **Ressources éligibles**, vous voyez que l'état des machines sélectionnées indique **Activé**.

Si des problèmes se produisent pendant le processus d'activation, consultez Résoudre les problèmes de remise des mises à jour de sécurité étendues pour Windows Server pour obtenir de l'aide.

Activer les ESU à grande échelle à l'aide de Azure Policy

Pour lier des serveurs à grande échelle à une licence Extended Security Update Azure Arc et verrouiller la modification ou la création de licences, envisagez d'utiliser les stratégies intégrées Azure suivantes :

- Activer la licence ESU (Extended Security Updates) pour protéger les machines Windows 2012 une fois leur cycle de vie de support terminé (préversion)

- Refuser la création ou la modification de licences ESU (Extended Security Update) (préversion)

Spécifiez stratégies Azure pour un abonnement ou groupe de ressources ciblé pour les scénarios d'audit et de gestion.

Autres cas de figure

Vous pouvez recevoir des correctifs de mises à jour de sécurité étendues sans frais supplémentaires dans certains scénarios. Deux de ces scénarios pris en charge par Azure Arc sont Dev/Test (Visual Studio) et Récupération d'urgence (avec l'avantage des instances DR de Software Assurance ou l'abonnement uniquement. Les deux scénarios nécessitent que vous utilisiez déjà Windows Server 2012/R2 ESU activés via Azure Arc pour des machines de production facturées.

> ⚠ **Avertissement**
>
> Ne créez pas de licence ESU Windows Server 2012/R2 uniquement pour les charges de travail Dev/Test ou Reprise d'activité après sinistre. Ne provisionnez pas de licence ESU uniquement pour des charges de travail non facturables. Vous payez pour tous les cœurs approvisionnés avec une licence ESU. Vous ne payez pas pour les cœurs de développement/test sur la licence si vous les étiquetez en fonction des qualifications suivantes.

Pour bénéficier de ces scénarios, vous devez déjà disposer des éléments suivants :

- **Licence ESU facturable.** Vous devez déjà avoir configuré et activé une licence WS2012 Arc ESU pour lier à des serveurs Azure Arc classiques s'exécutant dans des environnements de production (par exemple, des scénarios ESU facturés normalement). Provisionnez cette licence uniquement pour les cœurs facturables, et non pour les cœurs éligibles pour les mises à jour de sécurité étendues gratuites, telles que les cœurs de développement/test.

- **Serveurs compatibles avec Arc.** Enrôlez vos machines Windows Server 2012 et Windows Server 2012 R2 sur des serveurs compatibles Azure Arc pour le développement/test avec des abonnements Visual Studio ou pour la récupération d'urgence.

Pour inscrire des serveurs compatibles Azure Arc éligibles aux ESU sans frais supplémentaires, procédez comme suit pour baliser et lier :

1. Balisez à la fois la licence WS2012 Arc ESU (créée pour l'environnement de production avec des cœurs uniquement pour les serveurs d'environnement de production) et les serveurs

non-productifs activés par Azure Arc avec l'une des paires nom-valeur suivantes, correspondant à l'exception appropriée :

a. Nom : « Utilisation de l'ESU » ; Valeur : « WS2012 VISUAL STUDIO DEV TEST »

b. Nom : « Utilisation de l'ESU » ; Valeur : « Récupération après sinistre WS2012 »

Si vous utilisez la licence ESU pour plusieurs scénarios d'exception, marquez la licence avec la balise : Nom : « Utilisation ESU » ; Valeur : « WS2012 MULTIPURPOSE »

2. Liez la licence étiquetée (créée pour l'environnement de production avec des cœurs uniquement pour les serveurs de cet environnement) à vos machines Windows Server 2012 et Windows Server 2012 R2 activées par Azure Arc et étiquetées pour un usage non production. **Ne pas mettre en licence les cœurs de ces serveurs ni créer une licence ESU pour ces serveurs uniquement.**

Cette association ne déclenche pas de violation de conformité ou de blocage de l'application. Vous pouvez donc étendre l'application d'une licence au-delà de ses cœurs provisionnés. Il est attendu que la licence inclut uniquement les cœurs pour les serveurs en production et facturés. Les cœurs supplémentaires entraînent une surfacturation.

> ⓘ **Important**
>
> L'ajout de ces balises à votre licence ne rend pas la licence gratuite et ne réduit pas le nombre de cœurs de licence facturés. À l'aide de ces balises, vous pouvez lier vos machines Azure aux licences existantes déjà configurées avec des cœurs payables sans avoir à créer de nouvelles licences ou à ajouter d'autres cœurs à vos machines gratuites.

Exemple :

- Vous avez huit instances Windows Server 2012 R2 Standard, chacune avec huit cœurs physiques. Six de ces machines Windows Server 2012 R2 Standard sont en production, et deux de ces machines Windows Server 2012 R2 Standard sont éligibles à des ESU gratuites, car le système d'exploitation a été concédé sous licence via un abonnement Visual Studio Dev Test.
  - Tout d'abord, provisionnez et activez une licence ESU standard pour Windows Server 2012/R2 de l'édition Standard et disposant de 48 cœurs physiques pour couvrir les six machines de production. Liez cette licence ESU de production régulière à vos six serveurs de production.

- Ensuite, réutilisez cette licence existante, n'ajoutez pas de cœurs ou ne provisionnez pas de licence distincte et liez cette licence à vos deux machines standard Windows Server 2012 R2 hors production. Étiquetez la licence ESU et les deux machines Windows Server 2012 R2 Standard hors production avec le nom « Utilisation de l'ESU » et la valeur : « WS2012 VISUAL STUDIO DEV TEST ».
- Cela entraîne une licence ESU pour 48 cœurs, et vous payez pour ces 48 cœurs. Vous ne payez pas pour les 16 cœurs supplémentaires des serveurs de test de développement que vous avez ajoutés à cette licence, tant que vous balisez la licence ESU et les ressources du serveur de test de développement de manière appropriée.

> **Remarque**
>
> Vous avez besoin d'une licence de production régulière pour commencer, et vous payez uniquement pour les cœurs de production.

Mise à niveau à partir de Windows Server 2012/2012 R2

Lors de la mise à niveau d'une machine Windows Server 2012/2012R vers Windows Server 2016 ou version ultérieure, il n'est pas nécessaire de supprimer l'agent Connected Machine de la machine. La machine dans Azure peut voir le nouveau système d'exploitation quelques minutes après la fin de la mise à niveau. Les machines mises à niveau n'ont plus besoin de mises à jour ESU et ne sont plus éligibles à celles-ci. Toute licence ESU associée à la machine n'est pas automatiquement dissociée de la machine. Consultez Dissocier une licence pour savoir comment procéder manuellement.

Évaluer l'état des correctifs ESU pour WS2012

Pour détecter si les derniers correctifs de sécurité étendus Windows Server 2012/R2 ont été appliqués à vos serveurs avec Azure Arc, vous pouvez utiliser la stratégie Azure suivante : Les correctifs de sécurité étendus doivent être installés sur des machines Windows Server 2012 avec Arc. Cette définition de stratégie, alimentée par La configuration de l'ordinateur, identifie si le serveur a reçu les correctifs ESU les plus récents. Cela est observable à partir des vues d'affectation des invités et de conformité à la politique Azure dans le portail Azure.

Dernière mise à jour : 05/10/2026

Activer Hotpatch pour les machines virtuelles Azure Edition sur Azure Local

14/08/2025S'applique à: ✅ Windows Server 2022 Datacenter: Azure Edition hosted on Azure Local

Hotpatch pour Windows Server 2022 Datacenter : machines virtuelles Azure Edition hébergées sur Azure Local vous permet d'installer des mises à jour de sécurité sur une machine déployée par ISO sur Azure Local sans nécessiter de redémarrage après l'installation. Vous pouvez utiliser Hotpatch avec Expérience utilisateur et Server Core. Cet article explique comment configurer Hotpatch après l'installation ou la mise à niveau du système d'exploitation à l'aide d'ISO.

> ⓘ **Notes**
>
> Si vous utilisez Azure Marketplace, ne suivez pas les étapes décrites dans cet article. Utilisez plutôt les images suivantes d'Azure Marketplace qui sont prêtes pour le correctif à chaud :
>
> - Windows Server 2022 Datacenter : Azure Edition Hotpatch - Gen2
> - Windows Server 2022 Datacenter : Azure Edition Core - Gen2

Lorsque vous utilisez Hotpatch pour votre machine déployée ISO sur Azure Local, il existe quelques différences importantes avec l'expérience Hotpatch par rapport à l'utilisation de Hotpatch dans le cadre d'Azure Automanage pour machines virtuelles Azure.

Les différences sont les suivantes :

- La configuration de Hotpatch n'est pas disponible via Azure Update Manager.
- Hotpatch ne peut pas être désactivé.
- L'orchestration de mise à jour corrective automatique n'est pas disponible.
- L'orchestration doit être effectuée manuellement (par exemple, à l'aide de Windows Update via SConfig).

Prerequisites

Pour activer Hotpatch, vous devez disposer des conditions préalables suivantes avant de commencer :

- Windows Server 2022 Datacenter : Édition Azure hébergée sur une plateforme prise en charge, telle qu'Azure ou Azure Local avec les avantages Azure activés.
  - Azure Local doit être version 21H2 ou ultérieure.

- Consultez la section Fonctionnement de Hotpatch de l'article Hotpatch pour les nouvelles machines virtuelles.
- Accès réseau sortant ou règle de port de sortie autorisant le trafic HTTPS (TCP/443) vers les points de terminaison suivants :
  - `go.microsoft.com`
  - `software-static.download.prss.microsoft.com`

Préparer votre ordinateur

Avant de pouvoir activer Hotpatch pour votre machine virtuelle, vous devez préparer votre ordinateur en procédant comme suit :

1. Connectez-vous à votre ordinateur. Si vous êtes sur le serveur principal, dans le menu SConfig, entrez l'option **15**, puis `appuyez sur Entrée` pour ouvrir une session PowerShell. Si vous utilisez l'Expérience utilisateur, établissez une connexion Bureau à distance à votre machine virtuelle et lancez PowerShell.

2. Activez la sécurité basée sur la virtualisation en exécutant la commande PowerShell suivante pour configurer les paramètres de Registre corrects :

   PowerShell

   ```
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "EnableVirtualizationBasedSecurity"
       Value = "0x1"
       Force = $True
       PropertyType = "DWORD"
   }
   New-ItemProperty @parameters
   ```

3. Redémarrez votre ordinateur.

4. Configurez la taille de table Hotpatch dans le Registre en exécutant la commande PowerShell suivante :

   PowerShell

   ```
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Session
   Manager\Memory Management"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "HotPatchTableSize"
       Value = "0x1000"
       Force = $True
   ```

```
    PropertyType = "DWORD"
}
New-ItemProperty @parameters
```

5. Configurez le point de terminaison Windows Update pour Hotpatch dans le Registre en exécutant la commande PowerShell suivante :

```PowerShell
$registryPath = "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Update\TargetingInfo\DynamicInstalled\Hotpatch.amd64"
$nameParameters = $parameters = @{
    Path = $registryPath
    Name = "Name"
    Value = "Hotpatch Enrollment Package"
    Force = $True
}
$versionParameters = $parameters = @{
    Path = $registryPath
    Name = "Version"
    Value = "10.0.20348.1129"
    Force = $True
}
New-Item $registryPath -Force
New-ItemProperty @nameParameters
New-ItemProperty @versionParameters
```

Maintenant que vous avez préparé votre ordinateur, vous pouvez installer le package de maintenance Hotpatch.

Installer le package de maintenance Hotpatch

> ⓘ **Notes**
>
> La base de connaissances prérequise Hotpatch n'est pas publiée dans le catalogue Microsoft Update.

Pour pouvoir recevoir des mises à jour Hotpatch, vous devez télécharger et installer le package de maintenance Hotpatch. Dans votre session PowerShell, procédez comme suit :

1. Téléchargez le package autonome Microsoft Update (KB5003508) à partir du catalogue Microsoft Update et copiez-le sur votre ordinateur à l'aide de la commande PowerShell suivante :

```PowerShell
```

```
$parameters = @{
     Source = "https://go.microsoft.com/fwlink/?linkid=2211714"
     Destination = ".\KB5003508.msu"
}
Start-BitsTransfer @parameters
```

2. Pour installer le package autonome, exécutez la commande suivante :

```
PowerShell

wusa.exe .\KB5003508.msu
```

3. Suivez les invites. Une fois l'opération terminée, sélectionnez Terminer.

4. Pour vérifier l'installation, exécutez la commande suivante :

```
PowerShell

Get-HotFix | Where-Object {$_.HotFixID -eq "KB5003508"}
```

> ⓘ **Notes**
>
> Lorsque vous utilisez Server Core, les mises à jour sont définies pour être installées manuellement par défaut. Vous pouvez modifier ce paramètre à l'aide de l'utilitaire SConfig.

Étapes suivantes

Maintenant que vous avez configuré votre ordinateur pour Hotpatch, voici quelques articles qui peuvent vous aider à mettre à jour votre ordinateur :

- Patcher une installation Server Core.
- En savoir plus sur Windows Server Update Services (WSUS).

Activer Hotpatch pour les serveurs avec Azure Arc

S'applique à: ✅ Windows Server 2025

> **ⓘ Important**
>
> Hotpatch avec Azure Arc pour Windows Server 2025 est désormais disponible pour un abonnement mensuel. Pour en savoir plus sur la tarification, consultez Marre de tous les redémarrages ? Optez pour une mise à jour sans redémarrage pour Windows Server.

Hotpatch vous permet de mettre à jour votre installation de Windows Server sans exiger que vos utilisateurs redémarrent après l'installation. Cette fonctionnalité réduit le temps d'arrêt consacré aux mises à jour et permet à vos utilisateurs d'exécuter leurs charges de travail sans interruption. Pour plus d'informations sur le fonctionnement de Hotpatch, consultez Hotpatch pour Windows Server.

Windows Server 2025 offre la possibilité d'activer Hotpatch pour les serveurs avec Azure Arc. Pour utiliser Hotpatch sur des serveurs avec Azure Arc, il vous suffit de déployer l'agent Connected Machine et d'activer Windows Server Hotpatch. Cet article explique comment activer Hotpatch.

Prérequis

Avant de pouvoir activer Hotpatch sur les serveurs avec Arc pour Windows Server 2025, vous devez répondre aux exigences suivantes.

- Un serveur doit exécuter Windows Server 2025 (build 26100.1742 ou version ultérieure). Les versions en préversion ou les builds Windows Server Insiders ne sont pas prises en charge, car les correctifs chauds ne sont pas créés pour les systèmes d'exploitation de préversion.

- L'ordinateur doit exécuter l'une des éditions suivantes de Windows Server.
  - Windows Server 2025 Standard
  - Windows Server 2025 Datacenter
  - Windows Server 2025 Datacenter : Azure Edition. Cette édition n'a **pas** besoin d'être activée par Azure Arc, Hotpatch est déjà activée par défaut. Les prérequis techniques restants s'appliquent toujours.

- Les options d'installation **Server avec expérience utilisateur** et **Server Core** sont prises en charge.

- La machine physique ou virtuelle sur laquelle vous envisagez d'activer Hotpatch doit satisfaire les exigences de sécurité basée sur la virtualisation (VBS), également appelée mode de sécurité virtuel (VSM). Au minimum, la machine doit utiliser l'interface de microprogramme extensible unifiée (UEFI) avec le démarrage sécurisé activé. Par conséquent, pour une machine virtuelle sur Hyper-V, il doit s'agir d'une machine virtuelle génération 2.
- Un abonnement Azure. Si vous n'en avez pas encore, créez un compte gratuit avant de commencer.
- Votre serveur et votre infrastructure doivent satisfaire les conditions préalables de l'agent Connected Machine afin d'activer Azure Arc sur un serveur.
- La machine doit être connectée à Azure Arc (avec Arc). Pour en savoir plus sur l'intégration de votre machine à Azure Arc, consultez les options de déploiement de l'agent De machine connectée Azure.

Vérifier et activer le mode sécurisé virtuel si nécessaire

Lorsque vous activez Hotpatch à l'aide du portail Azure, il vérifie si le mode sécurisé virtuel (VSM) s'exécute sur la machine. Si VSM n'est pas en cours d'exécution, l'activation de hotpatch échouera et vous devrez activer VSM.

Vous pouvez également vérifier manuellement l'état de VSM avant d'activer Hotpatch. VSM peut être déjà activé si vous avez précédemment configuré d'autres fonctionnalités qui (comme Hotpatch) dépendent de VSM. Parmi les exemples courants de ces fonctionnalités, citons Credential guard ou protection basée sur la virtualisation de l'intégrité du code, également appelée intégrité du code protégé par hyperviseur (HVCI).

> **Conseil**
>
> Vous pouvez utiliser la stratégie de groupe ou un autre outil de gestion centralisé pour activer une ou plusieurs des fonctionnalités suivantes.
>
> - Protection des informations d'identification
> - Comptes d'ordinateur protégés par Credential Guard
> - Protection basée sur la virtualisation de l'intégrité du code
> - Lancement sécurisé de System Guard et protection SMM
> - Protection de la pile en mode noyau appliquée par le matériel
> - Serveur principal sécurisé

La configuration de l'une de ces fonctionnalités active également VSM.

Pour vérifier que VSM est configuré et en cours d'exécution, sélectionnez votre méthode préférée et examinez la sortie.

PowerShell

PowerShell

```
Get-CimInstance -Namespace 'root/Microsoft/Windows/DeviceGuard' -ClassName
'win32_deviceGuard' | Select-Object -ExpandProperty
'VirtualizationBasedSecurityStatus'
```

Si la sortie de commande est `2`, VSM est configuré et en cours d'exécution. Dans ce cas, passez directement à l'activation de Hotpatch sur Windows Server 2025.

Si la sortie n'est pas `2`, vous devez activer VSM.

▼ Pour activer VSM, développez cette section.

Activez VSM à l'aide de l'une des commandes suivantes.

PowerShell

PowerShell

```
New-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\DeviceGuard' -
Name 'EnableVirtualizationBasedSecurity' -PropertyType 'Dword' -Value 1 -Force
```

Conseil

Après avoir activé VSM, vous devez redémarrer votre serveur.

Après le redémarrage, réexécutez l'une des commandes suivantes pour vérifier que la sortie est maintenant `2`, afin de vous assurer que le VSM est en cours d'exécution.

PowerShell

PowerShell

```
Get-CimInstance -Namespace 'root/Microsoft/Windows/DeviceGuard' -ClassName
'win32_deviceGuard' | Select-Object -ExpandProperty
'VirtualizationBasedSecurityStatus'
```

Si la sortie n'est toujours pas `2`, VSM sur votre ordinateur a besoin d'un dépannage. La raison la plus probable est que les exigences en matière de matériel physique ou virtuel ne sont pas satisfaites. Reportez-vous à la documentation du fournisseur de votre plateforme matérielle ou de virtualisation. Par exemple, voici la documentation relative à VMware vSphere, Activer la sécurité basée sur la virtualisation sur une machine virtuelle existante.

Une fois que vous avez activé VSM et que vous vous êtes assuré qu'il est en cours d'exécution, passez à la section suivante.

Activer Hotpatch sur Windows Server 2025

1. Connectez la machine à Azure Arc, si elle n'était pas activée précédemment.
2. Une fois que vous avez connecté la machine à Azure Arc, connectez-vous au portail Azure Arc et accédez à **Azure Arc** → **Machines**.
3. Sélectionnez le nom de votre machine.
4. Sélectionnez **Hotpatch**, puis **Confirm**.
5. Attendez environ 10 minutes pour que les modifications s'appliquent. Si la mise à jour reste bloquée sur le statut *En attente*, passez au dépannage de l'agent Azure Arc.

Utilisation de Hotpatch sur Windows Server 2025

Chaque fois qu'un Hotpatch est disponible à partir de Windows Update, vous devez recevoir une invite pour l'installer. Étant donné que ces mises à jour ne sont pas publiées tous les mois, vous devrez peut-être attendre que le hotpatch suivant soit publié.

Vous pouvez éventuellement automatiser l'installation de hotpatch à l'aide d'outils de gestion des mises à jour, tels que Azure Update Manager (AUM).

Problèmes connus

Mises à jour multiples publiées en octobre 2025

En octobre 2025, Microsoft a publié plusieurs mises à jour qui ont été proposées à certains clients Windows Server. Si vous êtes inscrit à hotpatch ou prévoyez de vous inscrire et que vous envisagez d'installer les mises à jour hotpatch en novembre et décembre 2025, vérifiez que vos machines Windows Server s'exécutent **exactement** sur l'un des niveaux de mise à jour suivants.

- 14 octobre 2025 - **KB5066835** (build du système d'exploitation 26100.6899)
- 24 octobre 2025 - **KB5070893** (build du système d'exploitation 26100.6905) Mise à jour de sécurité pour Windows Server Update Services

Si vous avez installé l'une des autres mises à jour d'octobre, cela entraînera des mises à jour régulières non-hotpatch jusqu'au mois de référence suivant, actuellement prévu pour janvier 2026. Ces mises à jour nécessitent un redémarrage chaque mois. En particulier, la mise à jour suivante, si elle est installée, rend l'ordinateur incompatible avec les mises à jour à venir : 23 octobre 2025 - **KB5070881** (build du système d'exploitation 26100.6905) Hors bande, et toute autre mise à jour non répertoriée explicitement dans cette section.

Problème de licence des fonctionnalités dans les mises à jour d'octobre 2025

Un problème a été identifié avec les mises à jour de sécurité d'octobre 2025 pour Windows Server 2025. Cela peut avoir un impact sur les clients exécutant la mise à jour du 14 octobre 2025 - KB5066835 (build du système d'exploitation 26100.6899) ou une version ultérieure. En raison de ce problème, le comportement inattendu suivant peut être observé.

- L'activation du hotpatching Windows Server via Azure Arc sur de nouvelles machines peut échouer ou ne pas se terminer comme prévu. Au lieu de cela, l'activation des fonctionnalités reste dans l'état « En cours » jusqu'à ce que le problème soit résolu.
- Sur les ordinateurs précédemment activés pour le hotpatching Windows Server, la licence de fonctionnalité peut expirer, ce qui empêche l'installation de Hotpatch suivante. Au lieu de cela, la prochaine mise à jour entraîne un redémarrage si aucune action n'est effectuée.

Le hotpatching sur Windows Server 2025 Datacenter : Azure Edition n'est pas affecté par ce problème.

Pour résoudre ce problème, une série d'étapes manuelles est recommandée. L'échec de l'application de l'une ou l'autre solution de contournement entraînera des mises à jour régulières non-hotpatch jusqu'au prochain mois de référence prévu actuellement pour janvier 2026. Ces mises à jour nécessitent un redémarrage chaque mois.

Il existe deux façons d'appliquer la solution de contournement manuelle sur les machines affectées. Chacune des options fournies offre une solution complète. Vous devez appliquer la

solution de contournement sur chacun des ordinateurs concernés **avant** la prochaine mise à jour, qui est prévue dans la prochaine date de « mardi de correctif » du **11 novembre 2025**. L'application de la solution de contournement nécessite un redémarrage. Par conséquent, planifiez-le en conséquence.

Après avoir appliqué l'une ou l'autre solution de contournement, les mises à jour hotpatch publiées en novembre et décembre 2025 seront installées sans nécessiter de redémarrage.

Option 1 : Utiliser une stratégie de groupe ou locale pour activer la correction

1. Téléchargez et installez le package Windows 11 24H2, Windows 11 25H2 et Windows Server 2025 KB5062660 251028_18301 Feature Preview . Cela installe le modèle de stratégie de groupe ou local (`ADMX` fichier) pour cette correction spécifique.

2. Sélectionnez **Démarrer**, tapez **gpedit**, puis **modifiez la stratégie de groupe**. Accédez à **Configuration ordinateur\Modèles d'administration\KB5062660 251028_18301 Feature Preview\Windows 11, version 24H2, 25H2\KB5062660 251028_18301 Feature Preview**.

   Pour plus d'informations sur le déploiement et la configuration de cette stratégie de groupe spéciale, consultez Utiliser la stratégie de groupe pour activer une mise à jour désactivée par défaut.

3. Dans le volet de fenêtre de droite, ouvrez **KB5062660 251028_18301 Feature Preview**, sélectionnez **Activé**, puis **sélectionnez OK**.

4. Redémarrez l'ordinateur concerné.

5. Exécutez la commande suivante pour supprimer l'entrée **DeviceLicensingServiceCommandMutex** du Registre. Si cette entrée n'est pas présente sur l'appareil concerné, la suppression est ignorée.

   PowerShell

   ```
   try {
   Remove-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Subscriptions' -Name 'DeviceLicensingServiceCommandMutex' -ErrorAction Stop
   } catch {
   Write-Host "DeviceLicensingServiceCommandMutex entry not present, skipping removal."
   }
   ```

   Vous pouvez également utiliser votre outil d'édition de Registre ou votre solution d'automatisation préféré pour supprimer la même valeur. Ne supprimez pas toute la clé

de Registre.

Option 2 : Utiliser un script pour activer la correction

Ouvrez une fenêtre PowerShell avec élévation de privilèges sur chacune des machines affectées et exécutez les commandes suivantes. La dernière commande vous invite à redémarrer votre appareil. L'atténuation n'est pas terminée tant que l'ordinateur n'est pas redémarré et qu'il est recommandé de redémarrer immédiatement après l'exécution de ce script.

PowerShell

```
Stop-Service -Name 'HIMDS'
New-Item -Path
'HKLM:\SYSTEM\CurrentControlSet\Policies\Microsoft\FeatureManagement\Overrides' -
Force
New-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Policies\Microsoft\FeatureManagement\Overrides' -
PropertyType 'dword' -Name '4264695439' -Value 1 -Force
try {
  Remove-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Subscriptions' -Name 'DeviceLicensingServiceCommandMutex' -
ErrorAction Stop
} catch {
  Write-Host "DeviceLicensingServiceCommandMutex entry not present, skipping
removal."
}
Restart-Computer -Confirm
```

Étapes suivantes

Maintenant que Hotpatch est activé, voici quelques articles qui peuvent vous aider à mettre à jour votre ordinateur.

- Hotpatch pour Windows Server
- Appliquer un correctif à une installation Server Core
- Mise à jour corrective automatique des invités pour les machines virtuelles
- Gestionnaire de mises à jour Azure

Last updated on 31/10/2025

Intégrité de la publication de Windows

Trouvez rapidement des informations officielles sur les mises à jour Windows et les étapes de maintenance. Accédez à des ressources, des outils et des actualités sur les problèmes connus et les mesures de protection pour vous aider à planifier votre prochaine mise à jour. Vous voulez les dernières mises à jour de la santé des versions de Windows ? Suivez @WindowsUpdate sur X.



GET STARTED
Comment obtenir la mise à jour de...



DEPLOY
Guide opérationnel du client de...



REFERENCE
Feuille de route de Windows 11 :...



WHAT'S NEW
Guide d'un professionnel de...



DEPLOY
Guide opérationnel du démarrag...



OVERVIEW
Comprendre les mises à jour mensuelles...

Centre de messages

- Les mises à jour Windows sont disponibles pour les modifications de fuseau horaire en 2026 au Canada
- Action : les modifications renforcées de NTLMv1 peuvent affecter les connexions réseau sur les appareils sans Credential Guard
- Windows Server 2022 a atteint la fin du support standard

Afficher plus >

Windows 11, version 26H2

- Problèmes connus
- Problèmes résolus
- Notes de publication
- Informations sur la version de Windows 11
- Comment obtenir Windows 11, version 26H2

Windows 11, version 26H1

- Problèmes connus

Windows 11, version 25H2

- Problèmes connus

- Problèmes résolus
- Notes de publication
- Informations sur la version de Windows 11
- Ce qu'il faut savoir sur Windows 11, version 26H1

- Problèmes résolus
- Notes de publication
- Informations sur la version de Windows 11
- Comment obtenir Windows 11, version 25H2

Windows 10, version 22H2

- Problèmes connus
- Problèmes résolus
- Notes de publication
- Informations sur les versions Windows 10
- Comment obtenir Windows 10, version 22H2

Windows Server 2025

- Problèmes connus
- Problèmes résolus
- Notes de publication
- Informations sur la version Windows Server
- Nouveautés de Windows Server 2025

Windows Server 2022

- Problèmes connus
- Problèmes résolus
- Notes de publication
- Informations sur la version Windows Server
- Quoi de neuf dans Windows Server 2022

Versions supplémentaires

Consultez les détails sur les problèmes connus et résolus pour les autres versions de Windows et Windows Server pris en charge.

- Problèmes connus : versions antérieures

Des questions ? Rejoignez les heures d'ouverture !

Obtenez des conseils, des conseils et des astuces personnalisés et des réponses à vos questions.

Envoyer des commentaires

Partagez vos idées sur les fonctionnalités existantes ou des idées pour les nouvelles via le Hub de commentaires.

Aide

Ouvrez l'application Aide sur votre appareil Windows pour trouver des ressources permettant de résoudre les...

Windows Server - Termes du contrat de licence

13/07/2025

Passez en revue nos termes de licence liés à Windows Server.

- Logiciels supplémentaires pour Windows Server 2016
- Windows Server Technical Preview Expiration
- Conditions du contrat de licence Windows Server 2016 Technical Preview
- Termes du contrat de licence logiciel Microsoft - MICROSOFT. WINDOWSSERVER. SYSTEMINSIGHTS
- Termes du contrat de licence logiciel Microsoft - MICROSOFT. WINDOWSSERVER. SYSTEMINSIGHTS. CAPACITÉS
- Windows Admin Center - Termes du contrat de licence