# Documentation sur la gestion de Windows Server

Une fois que vous avez déployé Windows Server dans votre environnement, y compris les rôles spécifiques pour les fonctionnalités et fonctions dont vous avez besoin, l'étape suivante consiste à gérer ces serveurs. Windows Server inclut un certain nombre d'outils pour vous aider à comprendre votre environnement Windows Server, à gérer des serveurs spécifiques, à affiner les performances et à automatiser de nombreuses tâches de gestion.

## Gérer les systèmes et environnements Windows Server

### VUE D'ENSEMBLE

Vue d'ensemble de la gestion de Windows Server

Gérer Windows Server avec Azure

Gérer Windows Server avec Windows Admin Center

Gérer Windows Server avec System Center

Gérer les systèmes locaux avec le Gestionnaire de serveur

Gérer les systèmes et systèmes distants sans interface utilisateur avec les outils d'administration de serveur distant (RSAT)

## Gestion basée sur le cloud avec Azure Arc

### VUE D'ENSEMBLE

Qu'est-ce qu'un serveur avec Azure Arc ?

Azure Automanage pour les serveurs Azure Arc

### DÉPLOYER

Planifier le déploiement

### DÉMARRAGE

Connecter des machines à Azure Arc à l'aide d'un script de déploiement

Connecter des machines à grande échelle à l'aide d'un principal de service

Connecter des machines à Azure avec Windows Admin Center

ENTRAINEMENT

Learning path

## Windows Admin Center

VUE D'ENSEMBLE

Vue d'ensemble de Windows Admin Center

DÉPLOYER

Installer Windows Admin Center

DÉMARRAGE

Prise en main de Windows Admin Center

Gérer des serveurs avec Windows Admin Center

Connexion de Windows Server à des services hybrides Azure

## System Center

VUE D'ENSEMBLE

Vue d'ensemble de System Center

DÉMARRAGE

Gestionnaire de Machines Virtuelles

Operations Manager

Gestionnaire de protection des données

Obtenir System Center

## Collecter des informations sur votre environnement

VUE D'ENSEMBLE

System Insights

Configuration et collecte d'événements de démarrage

Journalisation de l'inventaire logiciel (SIL)

Journalisation des accès utilisateur (UAL)

## Paramétrer votre environnement Windows Server pour les performances

VUE D'ENSEMBLE

Recommandations en matière de réglage des performances

## Ligne de commande et script

VUE D'ENSEMBLE

Windows PowerShell

Windows Commands

## Accéder aux serveurs locaux, distants et virtuels

VUE D'ENSEMBLE

Services de Bureau à distance

## Gérer Windows Server sur Azure

VUE D'ENSEMBLE

Vue d'ensemble de la machine virtuelle Windows sur Azure

Azure Automanage

Security

Mises à jour et maintenance

Monitoring

Options de sauvegarde et de restauration

Outils d’automatisation de l’infrastructure

Disks

Networking

Availability options

## Versions antérieures de Windows Server

VUE D’ENSEMBLE

Documentation sur les versions précédentes de Windows

Rechercher des informations spécifiques

# Vue d’ensemble de la gestion de Windows Server

22/07/2025

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

Dans cet article, vous allez découvrir les différents outils et solutions disponibles pour gérer Efficacement Windows Server. Windows Server dispose de nombreux outils qui permettent aux administrateurs de connecter des applications, des réseaux et des services web dans une infrastructure.

Regardez la vidéo suivante pour obtenir une vue d’ensemble des outils de gestion Windows Server et découvrir comment choisir la solution appropriée pour les besoins de votre organisation.

https://learn-video.azurefd.net/vod/player?id=21d7b936-7942-456c-af48-8eedd36f04de&locale=fr-fr&embedUrl=%2Fwindows-server%2Fadministration%2Foverview

## Outils de gestion

Les outils principaux de gestion de votre infrastructure Windows Server sont les suivants :

- Windows Admin Center (Centre d'administration Windows)
- Outils de gestion locaux
- Azure Arc
- Centre système

Vous êtes probablement déjà familiarisé avec certains de ces outils, comme windows Server Microsoft Management Console (MMC). Toutefois, il est important d’être familiarisé avec toutes les offres Windows Server des outils de gestion afin de pouvoir choisir celle qui convient à votre organisation.

Cet article vous guide tout au long de chacune d’elles, décrivant leurs fonctionnalités et vous donne des ressources pour les télécharger et les configurer.

Sélectionnez un onglet pour en savoir plus sur chaque outil de gestion :

Windows Admin Center

Windows Admin Center est un ensemble d'outils d'administration de serveur basés sur un navigateur qui vous donne un contrôle total sur tous les aspects de votre infrastructure serveur. Il vous permet de configurer des fonctionnalités d'administration plus approfondies et plus avancées pour vos déploiements windows Server et cluster. Vous pouvez déployer localement Windows Admin Center sans utiliser Azure ou le cloud, ou vous pouvez l'intégrer directement dans le portail Azure. Il est également utile de gérer des serveurs sur des réseaux privés qui ne sont pas connectés à Internet.

Windows Admin Center est l'évolution moderne des outils de gestion intégrées, tels que le Gestionnaire de serveur et les consoles de gestion Microsoft (MMC), qui complètent d'autres solutions de gestion.

Voici un bref résumé des fonctionnalités de Windows Admin Center :

- Couvre les déploiements Windows Server uniques ou les clusters hyperconvergés.
- Inclut une interface basée sur un navigateur web.
- Prend en charge le mode déconnecté.
- Axé sur la gestion générale des serveurs, la configuration des rôles et la résolution des problèmes.

Si vous souhaitez en savoir plus sur Windows Admin Center, consultez Qu'est-ce que Windows Admin Center.

## Quand utiliser Windows Admin Center

Vous pouvez utiliser Windows Admin Center lorsque vous souhaitez :

- Gérez vos serveurs et clusters avec des versions modernisées d'outils familiers, tels que le Gestionnaire de serveur.
- Intégrez votre système à Azure pour connecter vos serveurs locaux à des services cloud pertinents avec Azure Arc.
- Simplifiez la gestion des clusters hyperconvergés Azure Local ou Windows Server.
- Utilisez des charges de travail simplifiées pour créer et gérer des machines virtuelles, des volumes Espaces de stockage direct, des solutions SDN (Software-Defined Networking), etc.

Pour commencer à utiliser Windows Admin Center, téléchargez Windows Admin Center, puis suivez les instructions d'installation. Une fois que vous avez configuré, découvrez comment commencer à utiliser Windows Admin Center lors de la prise en main de Windows Admin Center.

## Contenu connexe

Pour en savoir plus sur les différents outils qui comprennent des outils de gestion locaux, consultez les articles suivants :

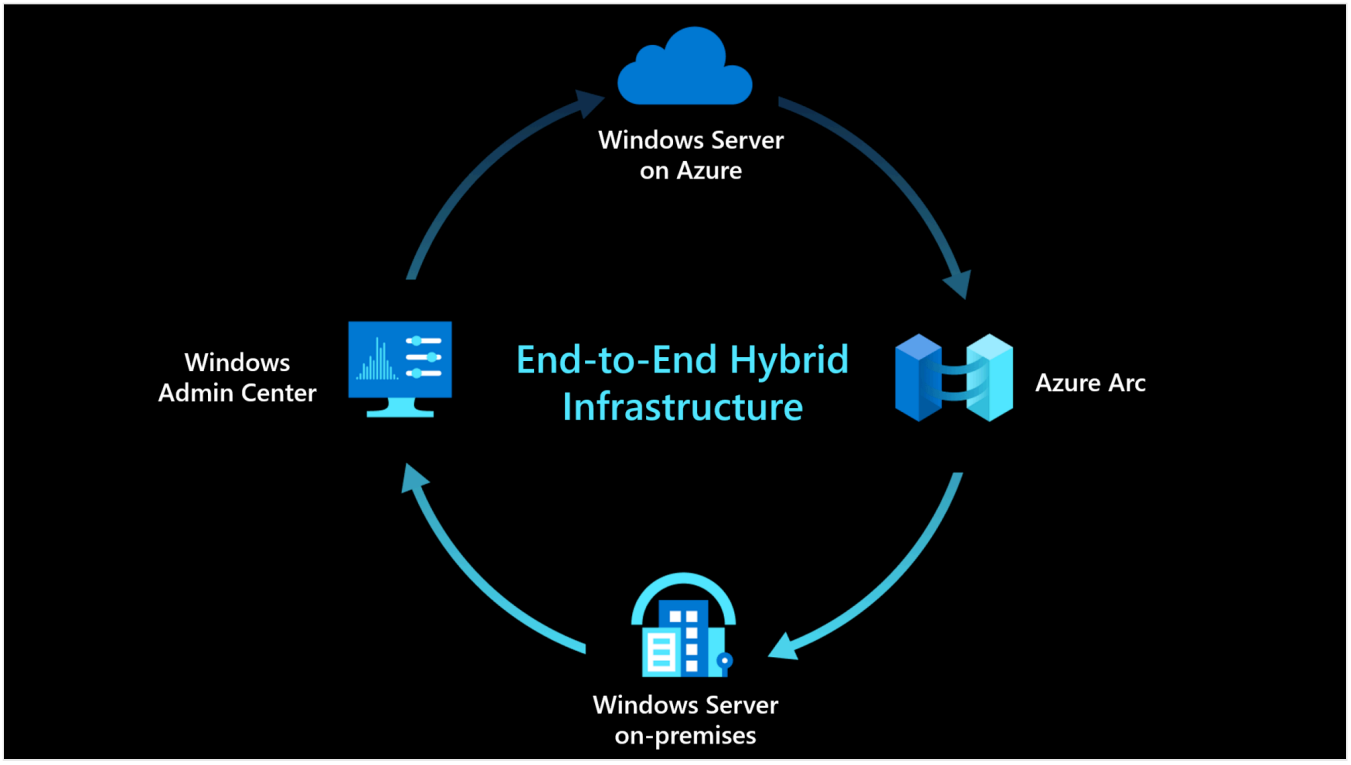
- Gestionnaire de serveur
- PowerShell
- Commandes Windows
- outils d’administration de serveur distant

# Ensemble, Windows Server et la gestion d'Azure c'est mieux

15/08/2025

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

Windows Server avec les fonctionnalités de gestion cloud Microsoft Azure vous permet de tirer encore plus parti de vos investissements Windows Server.




## Opérations cloud pour Windows Server dans un environnement hybride et multicloud

Lorsque vous connectez Windows Server exécutant un environnement local ou multicloud à Azure, il active l'intégration suivante :

Agrandir le tableau

| Fonction d'opérations | Description |
|---|---|
| **Govern** | |
| Azure Policy | Attribuez des configurations d'invité Azure Policy pour auditer les paramètres au sein de Windows Server. |

| Fonction d'opérations | Description |
|---|---|
| Balises Azure | Utiliser des balises pour organiser vos machines Windows Server, ressources Azure et hiérarchie de gestion |
| **Protect** | |
| Microsoft Defender pour le cloud | Protégez les serveurs non-Azure avec Microsoft Defender pour point de terminaison, compris dans Microsoft Defender pour le cloud, afin de détecter les menaces, gérer les vulnérabilités et monitorer de manière proactive les menaces de sécurité potentielles. Microsoft Defender pour le cloud présente les alertes et les suggestions de correction en fonction des menaces détectées. |
| Microsoft Sentinel | Les machines connectées aux serveurs avec Arc peuvent être configurées avec Microsoft Sentinel pour collecter des événements liés à la sécurité et les mettre en corrélation avec d'autres sources de données. |
| Azure Backup | Le service Sauvegarde Azure utilise l'agent Microsoft Azure Recovery Services (MARS) pour sauvegarder et restaurer des fichiers, dossiers et l'état du volume ou du système d'un ordinateur local vers Azure, ce qui vous permet de vous protéger contre les suppressions accidentelles ou malveillantes, la corruption et les ransomwares. |
| Azure Site Recovery (Récupération de site Azure) | Site Recovery réplique les charges de travail s'exécutant sur des machines virtuelles physiques et virtuelles à partir d'un site principal vers un emplacement secondaire ou Microsoft Azure. En cas d'interruption au niveau de votre site principal, vous basculez vers l'emplacement secondaire, depuis lequel vous pouvez accéder aux applications. Quand l'emplacement principal est de nouveau fonctionnel, vous pouvez effectuer une restauration automatique vers celui-ci. |
| **Configure** | |
| Azure Automation | Automatisez les tâches de gestion fréquentes et fastidieuses à l'aide de Runbooks PowerShell et Python.<br>Évaluez les modifications de configuration sur les logiciels installés, les services Microsoft, le Registre et les fichiers Windows et les démons Linux à l'aide du suivi des modifications et de l'inventaire.<br>Utilisez Update Management pour gérer les mises à jour du système d'exploitation pour vos serveurs Windows et Linux. |
| Azure Automanage (préversion) | Automatisez l'intégration et la configuration d'un ensemble de services Azure lorsque vous utilisez Automanage Machine pour les serveurs avec Arc. |
| Extensions de machine virtuelle | Fournit des tâches de configuration et d'automatisation post-déploiement à l'aide des extensions de machine virtuelle Arc prises en charge pour votre machine Windows ou Linux hors Azure. |
| **Monitor** | |

| Fonction d'opérations | Description |
| --- | --- |
| Azure Monitor | Surveillez les performances du système d'exploitation invité de l'ordinateur connecté et découvrez les composants d'application pour surveiller leurs processus et dépendances avec d'autres ressources à l'aide de VM Insights. Collectez d'autres données de journal, telles que les données de performances et les événements, à partir du système d'exploitation ou des charges de travail s'exécutant sur l'ordinateur avec l'agent Log Analytics. Ces données sont stockées dans un espace de travail Log Analytics. |
| **Étendre et se connecter** | |
| Microsoft Entra ID (système d'identification de Microsoft) | Connectez votre annuaire Windows Server Active Directory local à Microsoft Entra ID pour créer une identité hybride.<br>Les identités managées pour les serveurs avec Azure Arc fournissent aux serveurs une identité managée automatiquement dans l'ID Microsoft Entra. Vous pouvez utiliser cette identité pour vous authentifier auprès de n'importe quel service prenant en charge l'authentification Microsoft Entra, sans avoir d'informations d'identification dans votre code. |
| Réseau étendu Azure | Faites en sorte que les machines virtuelles Azure ressemblent à votre réseau local avec un réseau étendu Azure. Windows Admin Center peut configurer un VPN de site à site et étendre vos adresses IP locales dans votre réseau virtuel Azure pour vous permettre de migrer plus facilement des charges de travail vers Azure sans rompre les dépendances sur les adresses IP. |
| Adaptateur réseau Azure | Connectez vos serveurs locaux à un réseau virtuel Azure avec une carte réseau Azure. Laissez Windows Admin Center simplifier la configuration d'un VPN point à site à partir d'un serveur local dans un réseau virtuel Azure. |
| Azure File Sync | Synchronisez votre serveur de fichiers avec le cloud à l'aide d'Azure File Sync. Synchronisez les fichiers sur ce serveur avec des partages de fichiers Azure. Conservez tous vos fichiers localement ou utilisez la hiérarchisation cloud pour libérer de l'espace, et mettez uniquement en cache les fichiers les plus fréquemment utilisés sur le serveur, en hiérarchisant les données brutes dans le cloud. Les données dans le cloud peuvent être sauvegardées, ce qui évite d'avoir à vous soucier de la sauvegarde de serveur local. De plus, la synchronisation multisite permet de synchroniser un ensemble de fichiers sur plusieurs serveurs. |
| Réplica de stockage | Utilisez la réplication synchrone ou asynchrone basée sur des blocs sur une machine virtuelle dans Azure à l'aide du réplica de stockage. Vous pouvez configurer la réplication basée sur les blocs ou sur les volumes à un niveau serveur-à-serveur à l'aide du réplica de stockage sur un serveur ou une machine virtuelle secondaire. Windows Admin Center vous permet de créer une machine virtuelle Azure spécifiquement pour votre cible de réplication, ce qui vous aide à configurer correctement le stockage sur une nouvelle machine virtuelle Azure. Pour plus d'informations, consultez Réplication de serveur à serveur avec Storage Replica. |

Apprenez-en davantage sur le serveur avec Azure Arc sur qu'est-ce que le serveur avec Azure Arc et comment connecter Windows Server à des services hybrides Azure à l'aide de Windows Admin Center.

# Opérations cloud pour Windows Server sur Azure

Lorsque vous exécutez Windows Server sur Azure, il active l'intégration suivante :

Agrandir le tableau

| Fonction d'opérations | Description |
|---|---|
| **Govern** | |
| Azure Policy | Attribuez des configurations d'invité Azure Policy pour auditer les paramètres à l'intérieur de la machine. |
| Balises Azure | Utiliser des balises pour organiser vos serveurs Windows et vos ressources Azure et hiérarchie de gestion |
| **Protect** | |
| Microsoft Defender pour le cloud | Protégez les serveurs non-Azure avec Microsoft Defender pour point de terminaison, compris dans Microsoft Defender pour le cloud, afin de détecter les menaces, gérer les vulnérabilités et monitorer de manière proactive les menaces de sécurité potentielles. Microsoft Defender pour le cloud présente les alertes et les suggestions de correction en fonction des menaces détectées. |
| Microsoft Sentinel | Les machines Windows Server s'exécutant dans Azure peuvent être configurées avec Microsoft Sentinel pour collecter des événements liés à la sécurité et les mettre en corrélation avec d'autres sources de données. |
| Azure Backup | Sauvegarde Azure fournit des sauvegardes indépendantes et isolées pour vous protéger contre la destruction involontaire des données sur vos machines virtuelles. Les sauvegardes sont stockées dans un coffre Recovery Services avec gestion intégrée des points de récupération. |
| Azure Site Recovery (Récupération de site Azure) | Site Recovery réplique les charges de travail s'exécutant sur des machines virtuelles Azure de la région Azure principale vers une autre région Azure. Lorsqu'une panne se produit sur la région Azure principale, vous basculez vers l'autre région Azure et accédez aux applications à partir de là. Quand la région principale est de nouveau opérationnelle, vous pouvez effectuer une restauration automatique vers celle-ci. |
| Informatique confidentielle Azure | L'informatique confidentielle Azure offre des machines virtuelles confidentielles. Les machines virtuelles confidentielles sont destinées aux locataires avec des exigences de sécurité et de confidentialité élevées. Ces machines virtuelles fournissent une limite stricte d'application matérielle pour répondre à vos besoins en matière de sécurité. Vous pouvez utiliser des machines virtuelles confidentielles |

| Fonction d'opérations | Description |
| --- | --- |
| | pour les migrations sans apporter de modifications à votre code, avec la plateforme protégeant l'état de votre machine virtuelle contre la lecture ou la modification. |
| **Configure** | |
| Azure Automation | Automatisez les tâches de gestion fréquentes et fastidieuses à l'aide de Runbooks PowerShell et Python.<br>Évaluez les modifications de configuration sur les logiciels installés, les services Microsoft, le Registre et les fichiers Windows et les démons Linux à l'aide du suivi des modifications et de l'inventaire.<br>Utilisez Update Management pour gérer les mises à jour du système d'exploitation pour vos serveurs Windows et Linux. |
| Azure Automanage (préversion) | Automatisez l'intégration et la configuration d'un ensemble de services Azure lorsque vous utilisez Azure Automanage pour Windows Server.<br>Hotpatching est une nouvelle façon d'installer les mises à jour sur les machines virtuelles Windows Server Azure Edition prises en charge qui ne nécessitent pas de redémarrage après l'installation<br>SMB sur QUIC offre un « VPN SMB » pour les télémutateurs, les utilisateurs d'appareils mobiles et les succursales, offrant une connectivité sécurisée et fiable aux serveurs de fichiers de périphérie sur des réseaux non approuvés comme Internet. Pour en savoir plus sur SMB sur QUIC et sur la configuration de SMB sur QUIC, consultez SMB sur QUIC. |
| Extensions de machine virtuelle | Les extensions de machine virtuelle Azure sont de petites applications qui fournissent des tâches de configuration post-déploiement et d'automatisation sur des machines virtuelles Azure. Par exemple, si une machine virtuelle nécessite une installation logicielle, une protection antivirus ou la possibilité d'exécuter un script à l'intérieur, vous pouvez utiliser une extension de machine virtuelle. |
| Windows Admin Center dans le portail Azure | Utilisez Windows Admin Center (préversion) dans le portail Azure pour gérer le système d'exploitation Windows Server à l'intérieur d'une machine virtuelle Azure. Gérez les fonctions du système d'exploitation à partir du portail Azure et travaillez avec des fichiers dans la machine virtuelle sans utiliser le Bureau à distance ou PowerShell. |
| Commande d'exécution de machine virtuelle | La fonctionnalité Run Command utilise l'agent de machine virtuelle pour exécuter des scripts PowerShell au sein d'une machine virtuelle Windows Azure. |
| **Monitor** | |
| Azure Monitor | Surveillez les performances du système d'exploitation invité de l'ordinateur connecté et découvrez les composants d'application pour surveiller leurs processus et dépendances avec d'autres ressources à l'aide de VM Insights. Collectez d'autres données de journal, telles que les données de performances et les événements, à partir du système d'exploitation ou des charges de travail s'exécutant sur |

| Fonction d'opérations | Description |
| --- | --- |
| | l'ordinateur avec l'agent Log Analytics. Ces données sont stockées dans un espace de travail Log Analytics. |
| **Étendre et se connecter** | |
| Microsoft Entra ID (système d'identification de Microsoft) | Connectez votre annuaire Windows Server Active Directory local à Microsoft Entra ID pour créer une identité hybride.<br>Les identités managées pour les machines virtuelles Azure fournissent des services Azure avec une identité managée automatiquement dans Microsoft Entra ID. Vous pouvez utiliser cette identité pour vous authentifier auprès de n'importe quel service prenant en charge l'authentification Microsoft Entra, sans avoir d'informations d'identification dans votre code.<br>Améliorez la sécurité des machines virtuelles Windows dans Azure en intégrant l'authentification Microsoft Entra. Vous pouvez désormais utiliser l'ID Microsoft Entra comme plateforme d'authentification principale pour vous connecter à distance à l'aide du protocole RDP (Remote Desktop Protocol) dans Windows Server (à partir de l'édition Windows Server 2019 Datacenter) ou windows 10 (à partir de la version 1809). |

En savoir plus sur Windows Server sur Azure sur des machines virtuelles Windows dans Azure et sur la migration de Windows Server vers Azure sur Azure Migrate.

# Qu’est-ce qu’un serveur avec Azure Arc ?

Les serveurs avec Azure Arc vous permettent de gérer des serveurs physiques Windows et Linux et des machines virtuelles hébergées *en dehors* d’Azure, sur votre réseau d’entreprise ou avec un autre fournisseur de cloud. Avec Azure Arc, ces machines que vous hébergez en dehors d’Azure sont considérées comme des machines hybrides, avec une représentation de chaque machine dans Azure. Vous gérez ces machines hybrides dans Azure Arc de la même façon que vous gérez les machines virtuelles Azure natives.

Lorsque vous connectez une machine à Azure Arc, elle est traitée comme une ressource dans Azure. Chaque machine connectée a un ID de ressource Azure. Vous pouvez donc l’inclure dans un groupe de ressources Azure, ainsi que d’autres ressources Azure natives.

Pour connecter des machines hybrides à Azure, installez l’agent Azure Connected Machine sur la machine. Vous pouvez installer manuellement l’agent Connected Machine ou à grande échelle sur plusieurs ordinateurs à l’aide de la méthode de déploiement qui convient le mieux à votre scénario.

> **Remarque**
>
> Pour plus d’informations sur les différents services offerts par Azure Arc, voir **Choisir le bon service Azure Arc pour les machines**.

# Opérations cloud prises en charge

Lorsque vous connectez votre machine à des serveurs avec Azure Arc, vous pouvez effectuer de nombreuses fonctions opérationnelles, comme vous le feriez avec des machines virtuelles Azure natives. La liste suivante décrit certaines des principales actions prises en charge pour les machines connectées.

- **Govern**:
  - Attribuer Configurations de machine Azure pour auditer les paramètres à l’intérieur de la machine. Pour plus d’informations sur les coûts, consultez le guide de tarification d’Azure Policy.
- **Protect**:
  - Protégez les serveurs non-Azure à l’aide de Microsoft Defender pour point de terminaison, inclus via Microsoft Defender pour cloud, pour la détection des menaces, la gestion des vulnérabilités et pour surveiller de manière proactive les menaces de sécurité potentielles. Microsoft Defender pour le cloud présente les alertes et les suggestions de correction en fonction des menaces détectées.

    - Utilisez Microsoft Sentinel pour collecter des événements liés à la sécurité et les mettre en corrélation avec d'autres sources de données.
- **Configure**:
    - Utilisez Azure Automation pour des tâches de gestion fréquentes et fastidieuses à l'aide de Runbooks PowerShell et Python. Évaluez les modifications de configuration pour les logiciels installés, les services Microsoft, le Registre et les fichiers Windows et les démons Linux à l'aide de l'agent Azure Monitor pour le suivi des modifications et l'inventaire.
    - Pour gérer les mises à jour du système d'exploitation de vos serveurs Windows et Linux, utilisez le Gestionnaire de mise à jour Azure.
    - Utilisez l'inscription automatique des machines (en avant-première) pour configurer automatiquement des serveurs Arc activés avec un ensemble de fonctionnalités sélectionnées pour la surveillance, la sécurité et la gestion.
    - Effectuez des tâches de configuration post-déploiement et d'automatisation à l'aide des extensions de machine virtuelle de serveurs avec Arc prises en charge pour votre ordinateur Windows ou Linux non-Azure.
- **Monitor**:
    - Surveillez les performances du système d'exploitation et découvrez les composants d'application pour surveiller les processus et les dépendances avec d'autres ressources à l'aide de VM Insights.
    - Collectez d'autres données de journal, telles que les données de performances et les événements, à partir du système d'exploitation ou des charges de travail s'exécutant sur la machine à l'aide de l'agent Azure Monitor. Ces données sont stockées dans un espace de travail Log Analytics et contiennent des propriétés spécifiques à l'ordinateur, telles qu'un ID de ressource, pour prendre en charge l'accès aux journaux de contexte de ressource.

Pour en savoir plus sur la supervision, la sécurité et les services de mise à jour Azure dans les environnements hybrides et multiclouds, regardez la vidéo suivante.

https://www.youtube-nocookie.com/embed/mJnmXBrU1ao

> **Remarque**
>
> Ce service prend en charge **Azure Lighthouse**, qui permet aux fournisseurs de services de se connecter à leur propre locataire pour gérer les abonnements et les groupes de ressources que les clients ont délégués.

## Statut de l'assistant

Vous pouvez afficher l'état d'une machine connectée dans le portail **Azure sous Machines Azure Arc>**.

L'agent Connected Machine envoie des messages de pulsation au service à intervalles réguliers de 5 minutes. Si le service cesse de recevoir ces messages de pulsation d'un ordinateur, le service considère que cet ordinateur est hors connexion et l'état passe à **Déconnecté** dans les 15 à 30 minutes. Lorsque le service reçoit un message de pulsation de l'agent Connected Machine, l'état revient automatiquement à **Connecté**.

Si une machine reste déconnectée pendant 45 jours, son état peut passer à **Expiré**. Une machine expirée ne peut pas être gérée via Azure Arc tant qu'un administrateur de serveur ne se déconnecte pas, puis le reconnecte à Azure. La date d'expiration des informations d'identification de l'identité managée détermine la date exacte à laquelle un ordinateur expire. Les informations d'identification sont valides pour une durée de 90 jours maximum et sont renouvelées tous les 45 jours.

Si un ordinateur reçoit des messages d'erreur 429 ou affiche des états de connexion intermittents, il peut s'agir d'un ordinateur cloné incorrectement. Pour plus d'informations, consultez les instructions de clonage.

# Régions prises en charge

Pour obtenir la liste des régions prises en charge avec les serveurs avec Azure Arc, consultez la page Produits Azure par région.

Dans la plupart des cas, vous devez sélectionner la région Azure la plus proche géographiquement de l'emplacement de votre ordinateur lorsque vous créez le script d'installation. Les données au repos sont stockées dans la zone géographique Azure contenant la région que vous spécifiez, ce qui peut affecter votre choix de région si vous avez des exigences de résidence des données.

# Environnements pris en charge

Les serveurs avec Azure Arc prennent en charge la gestion des serveurs physiques et des machines virtuelles hébergés *en dehors* d'Azure. Pour plus d'informations sur les environnements pris en charge, consultez les prérequis de l'agent de machine connectée.

> **Remarque**
>
> Les serveurs avec Azure Arc ne sont pas conçus ou pris en charge pour permettre la gestion des machines virtuelles s'exécutant dans Azure.

# Limites du service

Il n'existe aucune limite au nombre de serveurs et d'extensions de machine virtuelle avec Arc que vous pouvez déployer dans un groupe de ressources ou un abonnement. La limite standard de 800 instances par groupe de ressources s'applique au type de ressource Portée de liaison privée Azure Arc.

# Résidence des données

Les serveurs avec Azure Arc stockent les données client. Par défaut, les données client restent dans la région dans laquelle le client déploie l'instance de service. Pour les régions ayant des exigences de résidence des données, les données client sont toujours conservées dans la même région. Par exemple, si vous inscrivez la machine auprès d'Azure Arc à l'aide de la région USA Est, les données sont stockées dans la région USA Est.

Par exemple, les informations de métadonnées d'instance sur l'ordinateur connecté sont collectées et stockées dans cette région. Ces métadonnées incluent les informations suivantes :

- Nom et version du système d'exploitation
- Nom de l'ordinateur
- Nom de domaine complet (FQDN) de l'ordinateur
- Version de l'agent Machine connectée

# Étapes suivantes

- Avant d'évaluer ou d'activer des serveurs avec Azure Arc sur plusieurs machines hybrides, consultez Vue d'ensemble de l'agent Connected Machine pour en savoir plus sur les spécifications et les détails techniques relatifs à l'agent, ainsi que sur les méthodes de déploiement.
- Essayez les serveurs avec Arc à l'aide du démarrage rapide d'Azure Arc.
- 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.
- Explorez le guide des opérations hybrides et multiclouds unifiées du Framework d'adoption cloud, ainsi que la gestion des identités et des accès pour les serveurs avec Azure Arc.

---

Last updated on 26/02/2026

# Meilleures pratiques concernant Azure Automanage pour les machines – Serveurs Azure Arc

23/06/2025

> ⊗ **Attention**
>
> Le 30 septembre 2027, le service Meilleures pratiques Azure Automanage sera mis hors service. Par conséquent, toute tentative de création d'un profil de configuration ou d'intégration d'un nouvel abonnement au service entraînera une erreur. Pour en savoir plus sur les modalités de migration vers Azure Policy avant cette date, cliquez **ici**.

> ⊗ **Attention**
>
> À compter du 1er février 2025, Azure Automanage commencera à déployer les modifications pour cesser la prise en charge et l'application de tous les services dépendant de l'agent Microsoft Monitoring Agent (MMA) déconseillé. Pour continuer à utiliser Change Tracking and Management, Insights de machine virtuelle, Update Management et Azure Automation, **migrez vers le nouvel agent Azure Monitor (AMA)**.

> ⊗ **Attention**
>
> Cet article fait référence à CentOS, une distribution Linux ayant atteint l'état EOL (fin du service). Veuillez considérer votre utilisation et votre planification en conséquence. Pour plus d'informations, consultez l'**aide relative à la fin de vie de CentOS**.

Ces services Azure sont automatiquement intégrés pour vous lorsque vous utilisez les meilleures pratiques d'Automanage pour les machines sur une machine virtuelle de serveur Azure Arc. Ils sont essentiels pour notre livre blanc sur les meilleures pratiques, que vous pouvez trouver dans notre Cloud Adoption Framework.

Nous allons intégrer et configurer automatiquement tous ces services, superviser leur fonctionnement et apporter les corrections nécessaires en cas de dérive. Pour en savoir plus, consultez Azure Automanage pour machines virtuelles.

## Systèmes d'exploitation pris en charge

Automanage prend en charge les systèmes d'exploitation suivants pour les serveurs Azure Arc :

- Windows Server 2012 R2, 2016, 2019, 2022
- CentOS 7.3+, 8
- RHEL 7.4+, 8
- Ubuntu 16.04, 18.04, 20.04
- SLES 12 (SP3-SP5 uniquement)

# Services participant

Agrandir le tableau

| Service | Descriptif | Profil de configuration[1] |
|---|---|---|
| Supervision des insights de machines | Azure Monitor pour machines surveille les performances et l'intégrité de vos machines virtuelles, y compris de leurs processus en cours d'exécution et de leurs dépendances vis-à-vis d'autres ressources. | Production |
| Gestion des mises à jour | Vous pouvez utiliser la solution Update Management d'Azure Automation pour gérer les mises à jour du système d'exploitation de vos machines. Vous pouvez rapidement évaluer l'état des mises à jour disponibles sur toutes les machines d'agent et gérer le processus d'installation des mises à jour nécessaires pour les serveurs. | Production, développement/test |
| Microsoft Antimalware | Microsoft Antimalware pour Azure offre une protection en temps réel qui permet d'identifier et de supprimer les virus, logiciels espions et autres logiciels malveillants. Il fournit des alertes lorsqu'un logiciel malveillant ou indésirable connu essaye de s'installer ou de s'exécuter sur vos systèmes Azure. **Remarque :** pour fonctionner correctement, Microsoft Antimalware requiert qu'aucun autre logiciel anti-programme malveillant ne soit installé. Cela n'est également pris en charge que pour Windows Server 2016 et versions ultérieures. | Production, développement/test |
| Suivi des modifications et inventaire | La fonctionnalité Suivi des modifications et inventaire combine les fonctions de suivi des modifications et d'inventaire pour vous permettre d'effectuer le suivi des modifications apportées à l'infrastructure des machines virtuelles et des serveurs. Le service prend en charge le suivi des modifications sur les services, les démons, les logiciels, le registre et les fichiers de votre environnement pour vous aider à diagnostiquer les changements indésirables et à déclencher des alertes. La prise en charge de l'inventaire vous permet d'interroger les | Production, développement/test |

| Service | Descriptif | Profil de configuration[1] |
| --- | --- | --- |
| | ressources intégrées pour voir les applications installées et d'autres éléments de configuration. | |
| Configuration d'une machine | La stratégie de configuration d'une machine est utilisée pour superviser la configuration de la machine et indiquer sa conformité. Le service Automanage installe la base de référence Azure pour la sécurité à l'aide de l'extension de configuration d'invité. Pour les machines Arc, le service de configuration des machines installe la base de référence en mode d'audit uniquement. Vous pouvez voir à quel niveau votre machine virtuelle n'est pas conforme à la base de référence. Toutefois, la non-conformité n'est pas automatiquement corrigée. | Production, développement/test |
| Compte Azure Automation | Azure Automation prend en charge la gestion tout au long du cycle de vie de votre infrastructure et des applications. | Production, développement/test |
| Espace de travail Log Analytics | Azure Monitor stocke des données de journal dans un espace de travail Log Analytics, qui est une ressource Azure et un conteneur où les données sont collectées, agrégées, et qui sert de limite d'administration. | Production, développement/test |

[1] La sélection de profil de configuration est disponible lorsque vous activez Automanage. Vous pouvez également créer votre propre profil personnalisé avec l'ensemble des services et paramètres Azure dont vous avez besoin.

# Étapes suivantes

Essayez d'activer le service Automanage pour machines dans le portail Azure.

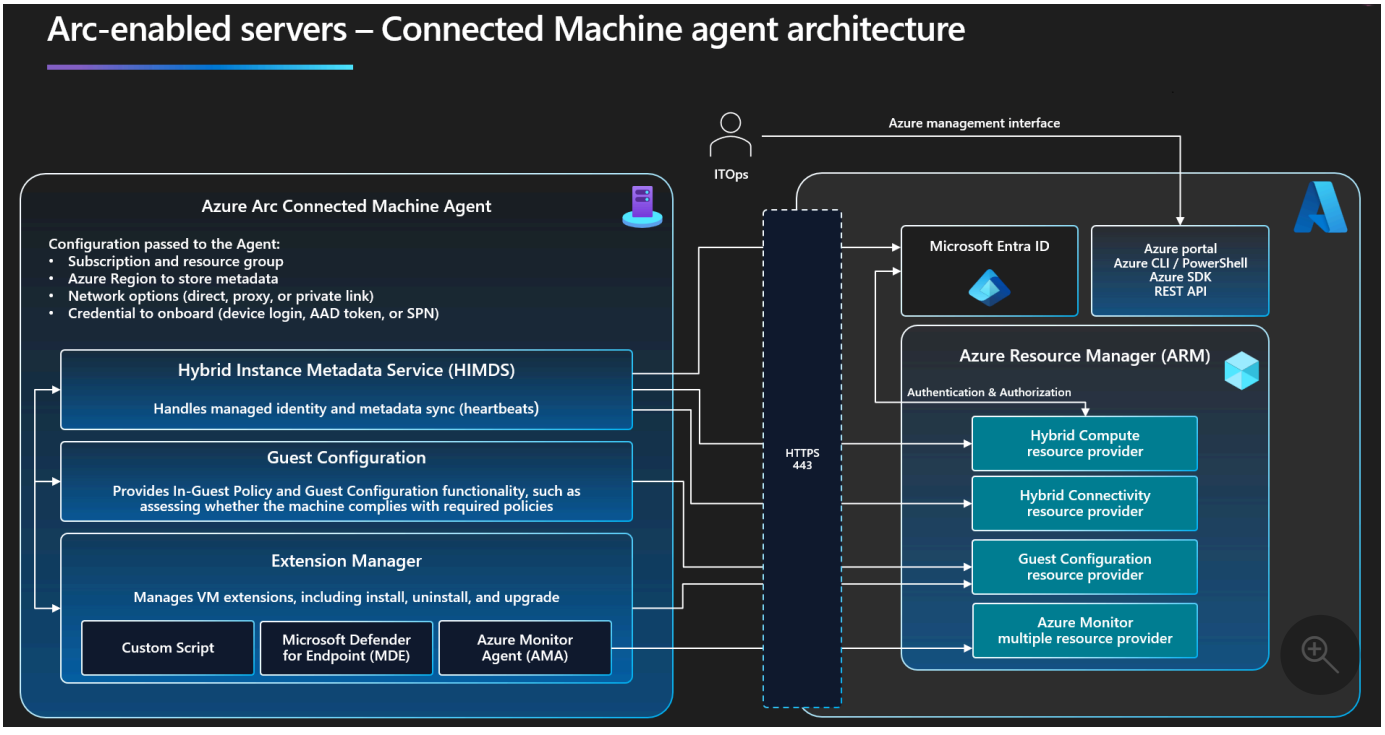
**Activer le service Automanage pour machines dans le portail Azure**

# Présentation de l’agent Azure Connected Machine

L’agent Azure Connected Machine vous permet de gérer les machines Windows et Linux hébergées en dehors d’Azure, sur votre réseau d’entreprise ou d’autres fournisseurs de cloud.

> **⚠ Avertissement**
>
> Seules les versions de l’agent Connected Machine de la dernière année sont officiellement prises en charge par le groupe de produits. Tous les clients doivent effectuer une mise à jour vers une version de l’agent dans cette fenêtre ou activer les mises à niveau automatiques de l’agent (préversion).

## Composants de l’agent




*Pour télécharger des diagrammes d’architecture en haute résolution, visitez Jumpstart Gems.*

Le package de l’agent Azure Connected Machine regroupe plusieurs composants logiques :

- Le service HIMDS (Hybrid Instance Metadata service) gère la connexion à Azure et l’identité Azure de l’ordinateur connecté.

- L'agent de configuration d'ordinateur fournit des fonctionnalités, comme l'évaluation de la conformité de l'ordinateur avec les stratégies requises et l'implémentation de la conformité.

  Notez le comportement suivant avec la configuration d'ordinateur Azure Policy pour un ordinateur déconnecté :
  - Une attribution Azure Policy qui cible les ordinateurs déconnectés n'est pas affectée.
  - L'attribution d'invité est stockée localement pendant 14 jours. Pendant la période de 14 jours, si l'agent Connected Machine se reconnecte au service, les attributions de stratégie sont réappliquées.
  - Les affectations sont supprimées après 14 jours et ne sont pas réaffectées à la machine après la période de 14 jours.

- L'agent Extension gère les extensions de machine virtuelle, notamment l'installation, la désinstallation et la mise à niveau. Azure télécharge les extensions et les copie dans le dossier `%SystemDrive%\%ProgramFiles%\AzureConnectedMachineAgent\ExtensionService\downloads` sur Windows, et dans `/opt/GC_Ext/downloads` sur Linux. Sur Windows, l'extension s'installe sur le chemin d'accès suivant `%SystemDrive%\Packages\Plugins\<extension>` et sur Linux, l'extension s'installe sur `/var/lib/waagent/<extension>`.

> ⓘ **Remarque**
>
> L'agent Azure Monitor (AMA) est un agent distinct qui collecte les données de surveillance. Il ne remplace pas l'agent Connected Machine. L'AMA remplace uniquement l'agent Log Analytics, l'extension Diagnostics et l'agent Telegraf pour les machines Windows et Linux.

## Proxy Azure Arc

Le service proxy Azure Arc est chargé d'agréger le trafic à partir des services de l'Agent Azure Connected Machine Agent et de toutes les extensions et de décider d'où acheminer ces données. Si vous utilisez la passerelle Azure Arc (préversion limitée) pour simplifier vos points de terminaison réseau, le service proxy Azure Arc est le composant local qui transfère les requêtes réseau via la passerelle Azure Arc au lieu de l'itinéraire par défaut. Le proxy Azure Arc s'exécute en tant que service réseau sur Windows et un compte d'utilisateur standard (arcproxy) sur Linux. Avant l'agent Azure Connected Machine version 1.51, ce service a été désactivé par défaut et doit rester désactivé, sauf si vous configurez l'agent pour utiliser la passerelle Azure Arc (préversion limitée). Avec la version 1.51 et ultérieure, le service proxy Arc est démarré par défaut, car il peut maintenant déterminer si l'ordinateur est configuré pour utiliser une passerelle Arc ou pour

communiquer directement avec les points de terminaison Arc et se comporter correctement. Si vous n'utilisez pas de passerelle Arc, vous pouvez toujours choisir de désactiver le service proxy Arc avec la commande `azcmagent config set connection.type direct` suivante.

# Ressources de l'agent

Cette section décrit les répertoires et les comptes d'utilisateur utilisés par l'agent Azure Connected Machine.

## Détails de l'installation de l'agent Windows

L'agent Windows est distribué en tant que package Windows Installer (MSI). Téléchargez l'agent Windows à partir du Centre de téléchargement Microsoft. L'installation de l'agent Connected Machine pour Windows applique à l'échelle du système les modifications de configuration suivantes :

- Le processus d'installation crée les dossiers suivants pendant l'installation.

Agrandir le tableau

| Directory | Description |
|---|---|
| %ProgramFiles%\AzureConnectedMachineAgent | CLI azcmagent et exécutables du service de métadonnées d'instance. |
| %ProgramFiles%\AzureConnectedMachineAgent\ExtensionService2\GC | Exécutables du service d'extension. |
| %ProgramFiles%\AzureConnectedMachineAgent\GCArcService2\GC | Exécutables du service de configuration d'ordinateur (stratégie). |
| %ProgramData%\AzureConnectedMachineAgent | Fichiers de configuration, de journal et de jeton d'identité pour azcmagent CLI et service de métadonnées d'instance. |
| %ProgramData%\GuestConfig | Téléchargements de packages d'extension, téléchargements de configuration d'ordinateur (stratégie) et journaux pour les services d'extension et |

| Directory | Description |
| --- | --- |
| | de configuration d'ordinateur. |
| %SYSTEMDRIVE%\packages | Exécutables du package d'extension |

- L'installation de l'agent crée les services Windows suivants sur l'ordinateur cible.

Agrandir le tableau

| Nom du service | Nom complet | Nom du processus | Description |
| --- | --- | --- | --- |
| himds | Service de métadonnées d'instance hybride Azure | `himds.exe` | Synchronise les métadonnées avec Azure et héberge une API REST locale pour permettre aux extensions et aux applications d'accéder aux métadonnées et de demander des jetons d'identité managée Microsoft Entra. |
| GCArcService | Service Arc de configuration d'ordinateur | `gc_arc_service.exe` (gc_service.exe antérieure à la version 1.36) | Audite et applique des stratégies de configuration d'ordinateur Azure sur la machine. |
| ExtensionService | Service d'extension de la configuration d'ordinateur | `gc_extension_service.exe` (gc_service.exe antérieure à la version 1.36) | Installe, met à jour et gère les extensions sur l'ordinateur. |

- L'installation de l'agent crée le compte de service virtuel suivant.

Agrandir le tableau

| Compte virtuel | Description |
| --- | --- |
| NT SERVICE\himds | Compte non privilégié utilisé pour exécuter Hybrid Instance Metadata Service. |

> **Conseil**
>
> Ce compte exige le droit « Se connecter en tant que service ». Ce droit est automatiquement accordé pendant l'installation de l'agent. Toutefois, si votre organisation configure des attributions de droits utilisateur avec la stratégie de groupe,

vous devrez peut-être ajuster votre objet de stratégie de groupe pour accorder le droit à « NT SERVICE\himds » ou « NT SERVICE\ALL SERVICES » pour permettre à l'agent de fonctionner.

- L'installation de l'agent crée le groupe de sécurité local suivant.

Agrandir le tableau

| Nom de groupe de sécurité | Description |
|---|---|
| Applications d'extension d'agent hybride | Les membres de ce groupe de sécurité peuvent demander des jetons Microsoft Entra pour l'identité managée affectée par le système. |

- L'installation de l'agent crée les variables environnementales suivantes.

Agrandir le tableau

| Name | Valeur par défaut |
|---|---|
| IDENTITY_ENDPOINT | `http://localhost:40342/metadata/identity/oauth2/token` |
| IMDS_ENDPOINT | `http://localhost:40342` |

- Plusieurs fichiers journaux, décrits dans le tableau suivant, permettent de résoudre les problèmes.

Agrandir le tableau

| Log | Description |
|---|---|
| %ProgramData%\AzureConnectedMachineAgent\Log\himds.log | Enregistre les détails de la pulsation et du composant de l'agent d'identité. |
| %ProgramData%\AzureConnectedMachineAgent\Log\azcmagent.log | Contient la sortie des commandes de l'outil azcmagent. |
| %ProgramData%\GuestConfig\arc_policy_logs\gc_agent.log | Enregistre des détails concernant le composant d'agent de configuration d'ordinateur (stratégie). |
| %ProgramData%\GuestConfig\ext_mgr_logs\gc_ext.log | Enregistre des détails sur l'activité du gestionnaire |

| Log | Description |
| --- | --- |
| | d'extensions (installation d'extension, désinstallation et événements de mise à niveau). |
| %ProgramData%\GuestConfig\extension_logs | Répertoire contenant des journaux d'activité pour des extensions individuelles. |

- Après avoir désinstallé l'agent, les artefacts suivants restent.
  - %ProgramData%\AzureConnectedMachineAgent\Log
  - %ProgramData%\AzureConnectedMachineAgent
  - %ProgramData%\GuestConfig
  - %SystemDrive%\packages

> **Remarque**
>
> Avant l'installation, excluez temporairement l'emplacement des fichiers d'installation de votre analyse antivirus/anti-programme malveillant. Cela empêche toute altération potentielle des fichiers et des interférences pendant l'installation.

## Détails de l'installation de l'agent Linux

Le format de package préféré pour la distribution (`.rpm` ou `.deb`) hébergée dans le référentiel de packages Microsoft fournit l'agent Connected Machine pour Linux. Le bundle de scripts shell Install_linux_azcmagent.sh installe et configure l'agent.

L'installation, la mise à niveau et la suppression de l'agent Connected Machine n'est pas nécessaire après le redémarrage du serveur.

L'installation de l'agent Connected Machine pour Linux applique à l'échelle du système les modifications de configuration suivantes.

- Le programme d'installation crée les dossiers d'installation suivants.

Agrandir le tableau

| Directory | Description |
| --- | --- |
| /opt/azcmagent/ | CLI azcmagent et exécutables du service de métadonnées d'instance. |
| /opt/GC_Ext/ | Exécutables du service d'extension. |

| Directory | Description |
|---|---|
| /opt/GC_Service/ | Exécutables du service de configuration d'ordinateur (stratégie). |
| /var/opt/azcmagent/ | Fichiers de configuration, de journal et de jeton d'identité pour azcmagent CLI et service de métadonnées d'instance. |
| /var/lib/GuestConfig/ | Téléchargements de packages d'extension, téléchargements de configuration d'ordinateur (stratégie) et journaux pour les services d'extension et de configuration d'ordinateur. |

- L'installation de l'agent crée les démons suivants.

Agrandir le tableau

| Nom du service | Nom complet | Nom du processus | Description |
|---|---|---|---|
| himdsd.service | Service Azure Connected Machine Agent | himds | Ce service implémente le service Hybrid Instance Metadata Service pour gérer la connexion à Azure et l'identité Azure de l'ordinateur connecté. |
| gcad.service | Service Arc GC | gc_linux_service | Audite et applique des stratégies de configuration d'ordinateur Azure sur la machine. |
| extd.service | Service d'extension | gc_linux_service | Installe, met à jour et gère les extensions sur l'ordinateur. |

- Plusieurs fichiers journaux, décrits dans le tableau suivant, permettent de résoudre les problèmes.

Agrandir le tableau

| Log | Description |
|---|---|
| /var/opt/azcmagent/log/himds.log | Enregistre les détails de la pulsation et du composant de l'agent d'identité. |
| /var/opt/azcmagent/log/azcmagent.log | Contient la sortie des commandes de l'outil azcmagent. |
| /var/lib/GuestConfig/arc_policy_logs | Enregistre des détails concernant le composant d'agent de configuration d'ordinateur (stratégie). |
| /var/lib/GuestConfig/ext_mgr_logs | Enregistre des détails sur l'activité du gestionnaire d'extensions (installation d'extension, désinstallation et événements de mise à niveau). |

| Log | Description |
|---|---|
| /var/lib/GuestConfig/extension_logs | Répertoire contenant des journaux d'activité pour des extensions individuelles. |

- L'installation de l'agent crée les variables d'environnement suivantes, définies dans `/lib/systemd/system.conf.d/azcmagent.conf`.

Agrandir le tableau

| Name | Valeur par défaut |
|---|---|
| IDENTITY_ENDPOINT | `http://localhost:40342/metadata/identity/oauth2/token` |
| IMDS_ENDPOINT | `http://localhost:40342` |

- Une fois l'agent désinstallé, les artefacts suivants restent.
  - /var/opt/azcmagent
  - /var/lib/GuestConfig

# Gouvernance des ressources de l'agent

L'agent Azure Connected Machine est conçu pour gérer la consommation des ressources de l'agent et du système. L'agent approche la gouvernance des ressources dans les conditions suivantes :

- Le service Configuration d'ordinateur (anciennement Configuration invité) peut utiliser jusqu'à 5 % du processeur pour évaluer des stratégies.

- Le service d'extension peut utiliser jusqu'à 5 % du processeur sur les machines Windows et 30 % du processeur sur les machines Linux pour installer, mettre à niveau, exécuter et supprimer des extensions. Une fois installées, certaines extensions peuvent imposer des limites de processeur plus restrictives. Il existe toutefois certaines exceptions :

Agrandir le tableau

| Type d'extension | Système d'exploitation | Limite UC |
|---|---|---|
| AzureMonitorLinuxAgent | Linux | 60% |
| AzureMonitorWindowsAgent | Windows | 100% |
| LinuxOsUpdateExtension | Linux | 60% |

| Type d’extension | Système d’exploitation | Limite UC |
|---|---|---|
| MDE.Linux | Linux | 60% |
| MicrosoftDnsAgent | Windows | 100% |
| MicrosoftMonitoringAgent | Windows | 60% |
| OmsAgentForLinux | Linux | 60% |

Pendant le fonctionnement normal, c’est-à-dire lorsque l’agent Azure Connected Machine est connecté à Azure et qu’il ne modifie pas activement une extension ou qu’il n’évalue pas une stratégie, vous pouvez vous attendre à ce que l’agent consomme les ressources système suivantes :

Agrandir le tableau

| | Windows | Linux |
|---|---|---|
| **Utilisation du processeur (normalisée à 1 cœur)** | 0.07% | 0.02% |
| **Utilisation de la mémoire** | 57 Mo | 42 Mo |

Les données de performances ci-dessus ont été recueillies en avril 2023 sur des machines virtuelles exécutant Windows Server 2022 et Ubuntu 20.04. Les performances réelles de l’agent et la consommation des ressources varient en fonction de la configuration matérielle et logicielle de vos serveurs.

## Limites de ressources personnalisées

Les limites de la gouvernance par défaut des ressources constituent la meilleure option pour la plupart des serveurs. Toutefois, de petites machines virtuelles et serveurs avec des ressources processeur limitées peuvent rencontrer des délais d’attente lors de la gestion des extensions ou de l’évaluation des stratégies, car il n’y a pas suffisamment de ressources processeur pour effectuer les tâches. À compter de la version d’agent 1.39, vous pouvez personnaliser les limites de processeur appliquées au gestionnaire d’extensions et aux services Configuration d’ordinateur pour permettre à l’agent d’effectuer ces tâches plus tard.

Si vous souhaitez voir les limites de ressources actuelles pour les services du gestionnaire d’extensions et de Configuration d’ordinateur, exécutez la commande suivante.

**Bash**

```
azcmagent config list
```

Dans la sortie, deux champs s'affichent, `guestconfiguration.agent.cpulimit` et `extensions.agent.cpulimit`, avec la limite de ressources actuelle spécifiée en tant que pourcentage. Sur une nouvelle installation de l'agent, les deux affichent `5`, car la limite par défaut est 5 % du processeur.

Pour passer à 80 % la limite de ressources du gestionnaire d'extensions, exécutez la commande suivante :

**Bash**

```
azcmagent config set extensions.agent.cpulimit 80
```

# Métadonnées d'instance

Les informations de métadonnées sur une machine connectée sont collectées une fois que l'agent Connected Machine s'est inscrit auprès des serveurs avec Azure Arc. Specifically:

- Nom, édition, type et version du système d'exploitation
- Nom de l'ordinateur
- Fabricant et modèle de l'ordinateur
- Nom de domaine complet (FQDN) de l'ordinateur
- Nom de domaine (s'il est joint à un domaine Active Directory)
- Nom de domaine complet (FQDN) Active Directory et DNS
- UUID (ID BIOS)
- Pulsation de l'agent Connected Machine
- Version de l'agent Machine connectée
- Clé publique pour l'identité managée
- État de conformité de la stratégie et détails (si vous utilisez des stratégies de configuration d'ordinateur)
- SQL Server installé (valeur booléenne)
- PostgreSQL installé (valeur booléenne)
- MySQL installé (valeur booléenne)
- ID de ressource de cluster (pour les machines locales Azure)
- Fabricant du matériel
- Modèle de matériel
- Famille de processeur, socket, nombre de cœurs physiques et de cœurs logiques

- Mémoire physique totale (pour les systèmes Linux, cela contient la valeur MemTotal de /proc/meminfo, qui est la RAM utilisable totale plutôt que la mémoire physique totale)
- Numéro de série
- Identifiant de ressource SMBIOS
- Informations sur l'interface réseau
  - IP address
  - Subnet
- Informations sur la licence Windows
  - État de la licence du système d'exploitation
  - Canal de la licence du système d'exploitation
  - Éligibilité des Mises à jour de sécurité étendue
  - État de la licence des Mises à jour de sécurité étendue
  - Canal de la licence des Mises à jour de sécurité étendue
- Fournisseur de cloud
- Métadonnées Amazon Web Services (AWS), lors de l'exécution dans AWS :
  - ID de compte
  - ID de l'instance
  - Region
- Métadonnées Google Cloud Platform (GCP), lors de l'exécution dans GCP :
  - ID de l'instance
  - Image
  - Type de machine
  - ID de projet
  - Numéro de projet
  - Comptes de service
  - Zone
- Métadonnées Oracle Cloud Infrastructure, lors de l'exécution dans OCI :
  - Nom complet

L'agent demande les informations de métadonnées suivantes à Azure :

- Emplacement de la ressource (ressource)
- ID de machine virtuelle
- Tags
- Certificat d'identité managée Microsoft Entra
- Affectations de la stratégie de configuration d'ordinateur
- Demandes d'extension : installation, mise à jour et suppression.

> **Remarque**
>
> Les serveurs avec Azure Arc ne collectent pas d'informations d'identification personnelle (PII) ou d'informations d'identification de l'utilisateur final ou stockent des données client.
>
> Les métadonnées client ne sont pas stockées ou traitées en dehors de la région dans laquelle le client déploie l'instance de service.

## Options de déploiement et exigences

Le déploiement de l'agent et la connexion de l'ordinateur nécessitent certaines conditions préalables. Vous devez également connaître la configuration réseau requise.

Nous proposons plusieurs options pour le déploiement de l'agent. Pour plus d'informations, consultez Planifier le déploiement et Options de déploiement.

## Instructions de clonage

Vous pouvez installer le package `azcmagent` en toute sécurité dans une image de référence, mais ne connectez pas cette machine à Azure Arc à l'aide de la commande `azcmagent connect`, sinon elle se voit attribuer un identifiant de ressource Azure unique. Si vous clonez vos machines à partir d'une image de référence connectée, chaque nouvelle machine utilise le même identifiant de ressource Azure, ce qui entraîne un état déconnecté.

Si votre serveur connecté reçoit des messages d'erreur 429, il est probable que vous ayez connecté le serveur à Azure, puis utilisé ce serveur comme image de référence pour le clonage. Comme les informations de la ressource ont été enregistrées dans l'image, les machines clonées créées à partir de cette image tentent d'envoyer des messages de pulsation à la même ressource.

Pour résoudre les messages de messages d'erreur 429 pour des machines existantes, exécutez `azcmagent disconnect --force-local-only` sur chaque machine clonée, puis réexécutez `azcmagent connect` en utilisant les informations d'identification appropriées pour connecter les machines au cloud avec un nom de ressource unique.

## Récupération d'urgence

Il n'existe aucune option de récupération d'urgence pour les serveurs avec Arc. En cas de panne dans une région Azure, le système bascule vers une autre région de la même zone géographique Azure (le cas échéant). Bien que cette procédure de basculement soit automatique, elle prend

un certain temps. L'agent Connected Machine est déconnecté pendant cette période et affiche l'état **Déconnecté** jusqu'à ce que le basculement soit terminé. Le système reviendra à sa région d'origine une fois la panne résolue.

Une panne d'Azure Arc n'affecte pas la charge de travail du client elle-même ; seule la gestion des serveurs applicables via Arc sera altérée.

## Déconnexion du serveur

L'agent Connected Machine envoie un message de pulsation régulier à Azure toutes les cinq minutes. Si un serveur avec Arc cesse d'envoyer des pulsations à Azure pendant plus de 15 minutes, cela peut signifier que le serveur est hors connexion, que la connexion réseau est bloquée ou que l'agent n'est pas en cours d'exécution.

Développez un plan de réponse et d'examen de ces incidents, y compris la configuration d'alertes Resource Health pour être averti lorsque de tels incidents se produisent. Pour en savoir plus, consultez Créer des alertes Resource Health dans le portail Azure et Dépanner les serveurs compatibles avec Azure Arc dans des scénarios hors connexion.

## Étapes suivantes

- Pour commencer l'évaluation des serveurs avec Azure Arc, consultez Démarrage rapide : Connecter des machines hybrides à des serveurs avec Azure Arc.
- Avant de déployer l'agent Azure Connected Machine et de l'intégrer à d'autres services de gestion et de supervision Azure, consultez le guide de planification et de déploiement.
- Consultez les informations de dépannage dans le Guide de dépannage des problèmes de connexion de l'agent.

---

Last updated on 28/07/2026

# Planifier et déployer des serveurs compatibles avec Azure Arc

Le déploiement d'un service d'infrastructure informatique ou d'une application métier est un défi pour toute entreprise. Pour l'exécuter correctement et éviter les surprises et les coûts non planifiés, vous devez planifier soigneusement pour vous assurer que vous êtes aussi prêt que possible. Un plan de déploiement de serveurs compatibles Azure Arc à n'importe quelle échelle doit couvrir les critères de conception et de déploiement qui doivent être remplis pour effectuer correctement les tâches.

Pour que le déploiement se déroule sans problème, votre plan doit clairement établir les points suivants :

- Rôles et responsabilités.
- Inventaire des serveurs physiques ou des machines virtuelles pour vérifier qu'ils répondent à la configuration réseau et système requise.
- Ensemble de compétences et formation requis pour permettre un déploiement réussi et une gestion continue.
- Critères d'acceptation et comment suivre leur succès.
- Outils ou méthodes à utiliser pour automatiser les déploiements.
- Les risques et les plans d'atténuation identifiés pour éviter les retards et les interruptions.
- Plan de prévention contre les perturbations pendant le déploiement.
- Chemin de réaffectation en cas de problème majeur.

Cet article vous aide à préparer un déploiement réussi de serveurs compatibles avec Azure Arc sur plusieurs serveurs physiques de production ou machines virtuelles dans votre environnement.

Pour en savoir plus sur les recommandations de déploiement à l'échelle, vous pouvez également vous référer à cette vidéo.

https://www.youtube-nocookie.com/embed/Cf1jUPOB_vs

## Prérequis

Tenez compte des exigences de base suivantes lorsque vous planifiez votre déploiement :

- Pour prendre en charge votre déploiement, vos machines doivent exécuter un système d'exploitation supporté pour l'agent Azure Connected Machine.
- Pour connecter votre déploiement, vos machines doivent disposer d'une connectivité à partir de votre réseau local ou d'un autre environnement cloud aux ressources dans Azure, directement ou via un serveur proxy.
- Pour installer et configurer l'agent Connected Machine, vous devez disposer d'un compte avec des privilèges élevés (c'est-à-dire un administrateur ou une racine) sur les machines.
- Pour intégrer des machines, vous devez disposer du rôle intégré Azure Connected Machine Onboarding.
- Pour lire, modifier et supprimer un ordinateur, vous devez disposer du rôle intégré Azure Administrateur de ressources de machine connectée.

Pour plus d'informations, consultez les conditions préalables et les conditions réseau requises pour installer l'agent Connected Machine.

## Azure limites d'abonnement et de service

Il n'existe aucune limite au nombre de serveurs compatibles avec Azure Arc que vous pouvez inscrire dans n'importe quel groupe de ressources, abonnement ou locataire unique.

Chaque serveur compatible Azure Arc est associé à un objet Microsoft Entra et compte dans votre quota de répertoire. Pour plus d'informations sur le nombre maximal d'objets que vous pouvez avoir dans un répertoire Microsoft Entra, consultez Microsoft Entra limites et restrictions de service.

# Pilote

Avant de déployer sur toutes les machines de production, commencez par évaluer le processus de déploiement avant de l'adopter largement dans votre environnement. Pour un pilote, identifiez un échantillon représentatif des machines qui ne sont pas essentielles à la capacité de votre entreprise à mener des activités. Veillez à prendre suffisamment de temps pour exécuter le pilote et évaluer son impact. Nous vous recommandons un minimum de 30 jours.

Établissez un plan formel pour décrire l'étendue et les détails du pilote. Votre plan doit généralement inclure les éléments suivants :

- **Objectifs** : Décrit les facteurs métier et techniques qui ont conduit à la décision qu'un pilote est nécessaire.

- **Critères de sélection** : spécifie les critères utilisés pour sélectionner les aspects de la solution que le pilote illustre.
- **Étendue** : décrit l'étendue du pilote, qui inclut, mais n'est pas limitée aux composants de solution, à la planification prévue, à la durée du pilote et au nombre de machines à cibler.
- **Critères de réussite et métriques** : définit les critères de réussite du pilote et les mesures spécifiques utilisées pour déterminer le niveau de réussite.
- **Plan de formation** : décrit le plan de formation des ingénieurs système, administrateurs, etc. qui sont nouveaux à Azure et à ses services pendant le pilote.
- **Plan de transition** : décrit la stratégie et les critères utilisés pour guider la transition du pilote à la production.
- **Retour arrière** : décrit les procédures pour revenir un pilote à l'état de prédéploiement.
- **Risques** : répertorie tous les risques identifiés pour mener le pilote et qui sont associés au déploiement de production.

# Phase 1 : créer une fondation

Dans cette phase, les ingénieurs système ou les administrateurs activent les fonctionnalités essentielles de l'abonnement Azure de leur organisation pour établir les bases avant d'activer les machines pour la gestion par les serveurs activés par Azure Arc et d'autres services Azure.

Agrandir le tableau

| Tâche | Détail | Durée estimée |
|---|---|---|
| Créez un groupe de ressources. | Un groupe de ressources dédié pour inclure uniquement des serveurs compatibles avec les Azure Arc et centraliser la gestion et la surveillance de ces ressources. | Une heure |
| Planifiez des étiquettes pour faciliter l'organisation des machines. | Évaluez et développez une stratégie de balisage alignée sur l'informatique, susceptible de vous aider à réduire la complexité de la gestion de vos serveurs Azure Arc et à simplifier la prise de décisions de gestion. | Un jour |
| Concevez et déployez Azure Monitor Logs. | Évaluez les considérations relatives à design et déploiement pour déterminer si votre organisation doit utiliser un espace de travail Log Analytics existant ou implémenter un autre espace de travail pour stocker les données de journal collectées à partir de serveurs et de machines hybrides. | Un jour |
| Élaborer un plan de gouvernance de Azure Policy. | Déterminez comment vous envisagez d'implémenter la gouvernance des serveurs hybrides et des machines au niveau de l'étendue de l'abonnement ou du groupe de ressources avec Azure Policy. | Un jour |

| Tâche | Détail | Durée estimée |
| --- | --- | --- |
| Configurez le contrôle d'accès en fonction du rôle. | Développez un plan d'accès pour contrôler qui a accès à la gestion des serveurs compatibles avec les Azure Arc et la possibilité d'afficher leurs données à partir d'autres services et solutions Azure. | Un jour |
| Identifiez les machines avec Azure Monitor Agent déjà installé. | Exécutez la requête de journal suivante dans Log Analytics pour prendre en charge la conversion des déploiements existants de Azure Monitor Agent en agent géré par l'extension : `Heartbeat <br> | summarize arg_max(TimeGenerated, OSType, ResourceId, ComputerEnvironment) by Computer <br> | where ComputerEnvironment == "Non-Azure" and isempty(ResourceId) <br> | project Computer, OSType` | Une heure |

# Phase 2 : Déployer des serveurs compatibles avec Azure Arc

Ensuite, nous complétons la base de la phase 1 en préparant et en déployant l'agent Connected Machine.

Agrandir le tableau

| Tâche | Détail | Durée estimée |
| --- | --- | --- |
| Téléchargez le script d'installation prédéfini. | Passez en revue et personnalisez le script d'installation prédéfini pour le déploiement à grande échelle de l'agent Connected Machine pour prendre en charge vos besoins de déploiement automatisé.<br><br>Exemples de ressources d'intégration à grande échelle :<br><br>• Script d'intégration à grande échelle via le principal de service pour Linux et Windows<br>• Intégration à grande échelle pour Linux et Windows via le portail Azure<br>• Intégration à grande échelle des machines AWS Linux et Windows à l'aide du connecteur multicloud | Un ou plusieurs jours en fonction des exigences, des processus organisationnels (par exemple, Change and Release Management) et de la méthode d'automatisation utilisée. |

| Tâche | Détail | Durée estimée |
| --- | --- | --- |
| | • Connecter les machines à grande échelle avec Ansible à l'aide du rôle d'intégration Azure Arc. | |
| Créez un principal du service. | Créez un principal de service pour connecter des machines de manière non interactive à l'aide de Azure PowerShell ou à partir du portail Azure. | Une heure. |
| Déployez l'agent Connected Machine sur vos serveurs et machines cibles. | Utilisez votre outil d'automatisation pour déployer les scripts sur vos serveurs et les connecter à Azure. | Un ou plusieurs jours selon votre plan de mise en production et si vous suivez un déploiement échelonné. |

> **Remarque**
>
> Vous pouvez afficher toutes les options de déploiement disponibles à **Options de déploiement de l'agent Azure Connected Machine**.

# Phase 3 : gérer et exploiter

Au cours de la phase 3, des administrateurs ou ingénieurs système peuvent activer l'automatisation de tâches manuelles pour gérer et exploiter l'agent Connected Machine et les machines pendant leur cycle de vie.

Agrandir le tableau

| Tâche | Détail | Durée estimée |
| --- | --- | --- |
| Créez une alerte de Resource Health. | Si un serveur cesse d'envoyer des pulsations à Azure pendant plus de 15 minutes, cela peut signifier que le serveur est hors connexion, que la connexion réseau est bloquée ou que l'agent n'est pas en cours d'exécution. Développez un plan pour répondre et examiner ces incidents et utiliser des alertes Resource Health pour être averti lorsqu'ils démarrent.<br><br>Spécifiez les éléments suivants lorsque vous configurez l'alerte :<br>Type de ressource = **serveurs activés Azure Arc**<br>**État actuel de la ressource** = **Indisponible**<br>**État précédent de la ressource** = **Disponible** | Une heure |

| Tâche | Détail | Durée estimée |
|---|---|---|
| Créez une alerte de Azure Advisor. | Pour une expérience optimale et des correctifs de sécurité et de bogues les plus récents, nous vous recommandons de maintenir l'agent Connected Machine à jour. Les agents obsolètes sont identifiés avec une alerte Azure Advisor.<br><br>Spécifiez les éléments suivants lorsque vous configurez l'alerte : **Recommendation type** = **Upgrade vers la dernière version de l'agent Connected Machine Azure** | Une heure |
| Mettre à jour l'agent d'ordinateur connecté Azure | L'agent Arc doit être mis à jour à mesure que de nouvelles versions sont publiées. Vous pouvez mettre à jour manuellement l'agent ou activer la mise à jour automatique (préversion publique). | 5-10 minutes |
| Assigner des stratégies Azure à votre étendue d'abonnement ou de groupe de ressources. | Affectez la **stratégie Enable Azure Monitor pour machines virtuelles** (et d'autres qui répondent à vos besoins) à l'étendue de l'abonnement ou du groupe de ressources. Avec Azure Policy, vous pouvez attribuer des définitions de stratégie qui installent les agents requis pour VM Insights dans votre environnement. | Variable |
| Activez Gestionnaire de mise à jour Azure pour vos serveurs compatibles Azure Arc. | Configurez Gestionnaire de mise à jour Azure sur vos serveurs Azure Arc pour gérer les mises à jour système de vos machines virtuelles Windows et Linux. Vous pouvez choisir de déployer des mises à jour à la demande ou d'appliquer des mises à jour à l'aide d'une planification personnalisée. | 5 minutes |

# Contenu connexe

- Découvrez les meilleures pratiques et les modèles de conception grâce à l'accélérateur de zone d'atterrissage Azure Arc pour hybride et multicloud.
- Apprenez-en davantage sur la reconfiguration, la mise à niveau et la suppression de l'agent Connected Machine.
- Consultez les informations de dépannage dans le Guide de dépannage des problèmes de connexion de l'agent.
- Découvrez comment simplifier le déploiement avec d'autres services Azure comme Azure Automation State Configuration et d'autres Azure extensions de machine virtuelle prises en charge.

Last updated on 17/04/2026

# Configurer Azure Site Recovery pour les serveurs Windows compatibles avec Arc

14/08/2025

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

L'outil de configuration Azure Site Recovery est conçu pour gérer et coordonner les processus de réplication, de basculement et de restauration automatique pour les machines virtuelles locales et Azure s'exécutant sur le système d'exploitation Windows Server avec Arc. Pendant cette préversion publique, l'outil est uniquement compatible avec les machines hyper-V, ce qui garantit que vos charges de travail locales restent opérationnelles pendant les pannes en les répliquant sur Azure en tant qu'emplacement secondaire.

Avec cette fonctionnalité, vous n'avez pas besoin d'installer manuellement l'agent Azure Site Recovery ou de le lier au coffre Recovery Service, au site Hyper-V ou à la stratégie de réplication, car cet outil s'occupe de ces tâches.

Par défaut, un compte de stockage Azure n'est pas inclus dans cette expérience. Pour continuer, vous devez créer un compte de stockage Azure ou utiliser un compte de stockage Azure existant à partir de votre abonnement Azure. Les deux options entraînent des coûts supplémentaires.

> ⓘ **Notes**
>
> - L'outil de configuration Azure Site Recovery gère la sécurité en exécutant toutes les vérifications localement sur votre serveur. Les résultats sont uniquement chargés sur votre compte de stockage Azure désigné, ce qui garantit que tout se produit dans le contexte de votre compte.
> - L'outil de configuration Azure Site Recovery doit être installé sur chaque serveur sur lequel vous souhaitez l'exécuter.

## Prerequisites

- Votre appareil doit exécuter un système d'exploitation Windows Server 2016 local ou ultérieur avec Arc avec un minimum de 4 Go de mémoire.
- Azure Arc doit être installé et configuré sur votre appareil.

- Vous devez utiliser les types de licence Windows Server Pay-as-you-go ou Software Assurance.
- Le rôle **Windows Server Hyper-V** doit être installé. Pour en savoir plus, consultez Installer ou désinstaller des rôles, services de rôle ou fonctionnalités.

  *Vous pouvez également* exécuter la commande suivante dans une fenêtre PowerShell avec élévation de privilèges :

  ```PowerShell
  Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
  ```

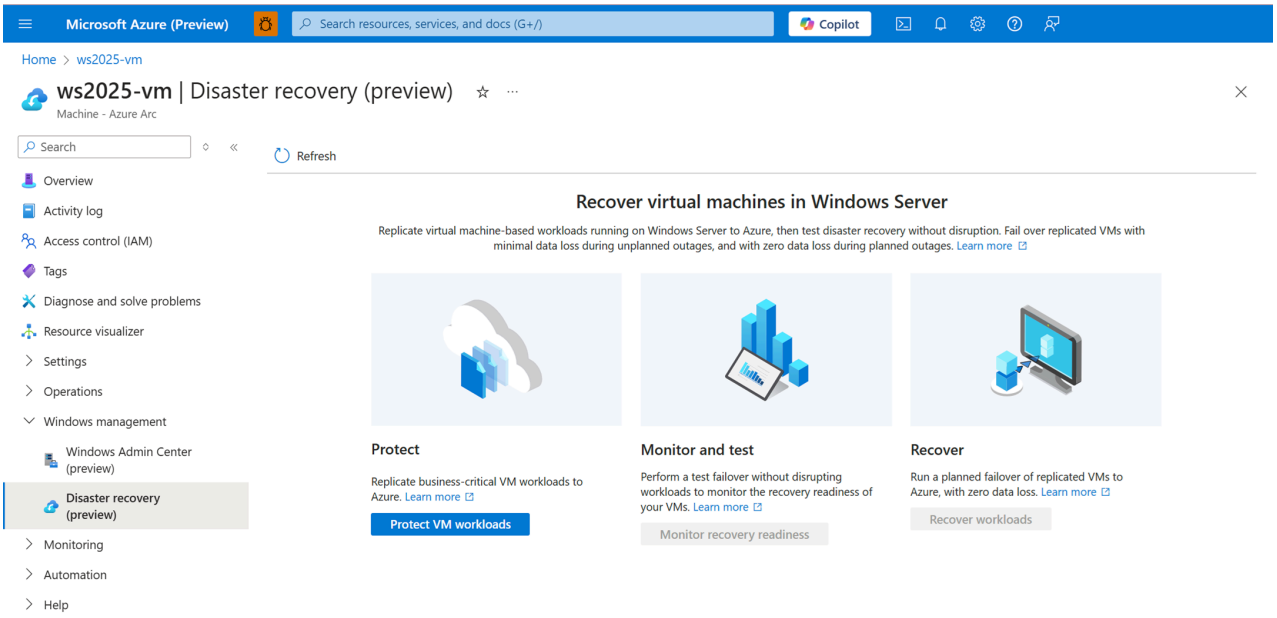
## Configurer la récupération de site Azure

Pour configurer Azure Site Recovery, l'agent Azure Site Recovery doit être installé sur votre appareil. Pour préparer l'infrastructure, la création ou l'utilisation d'un coffre, d'un site Hyper-V et d'une stratégie de réplication est requise. Une fois ces éléments en place, l'agent Azure Site Recovery est installé et associe la stratégie de réplication au nœud de cluster. Pour définir la récupération d'urgence dans votre environnement, procédez comme suit :

1. Accédez au Portail Azure, puis sélectionnez votre appareil Windows Server Arc.

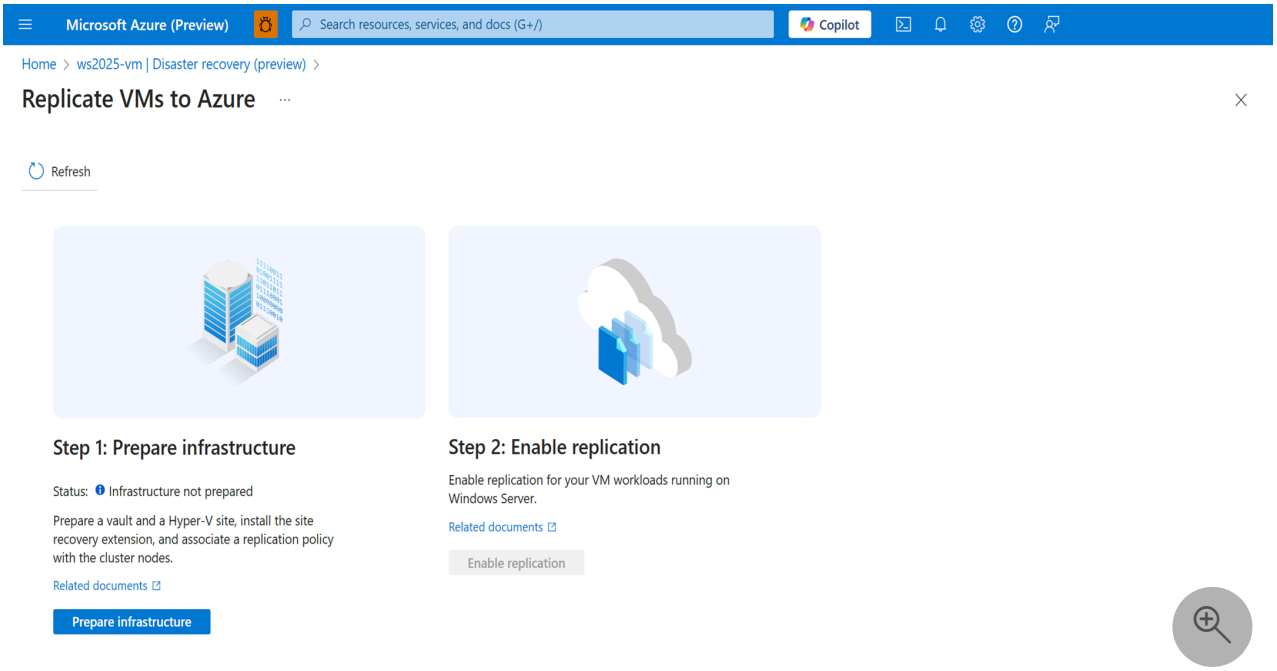
   > **Notes**
   >
   > Pendant la phase de préversion publique, sachez que cette fonctionnalité est accessible uniquement dans le cloud public.

2. Accédez à une ressource Windows Server 2016 ou ultérieure compatible Avec Arc. Cette machine virtuelle doit être l'hôte Hyper-V.
3. Dans le volet gauche, accédez à **la gestion De Windows**, puis sélectionnez **Configuration Azure Site Recovery (préversion)** .




4. Sélectionnez **Protéger les charges de travail de machine virtuelle pour accéder à la page Répliquer des machines virtuelles vers Azure**.

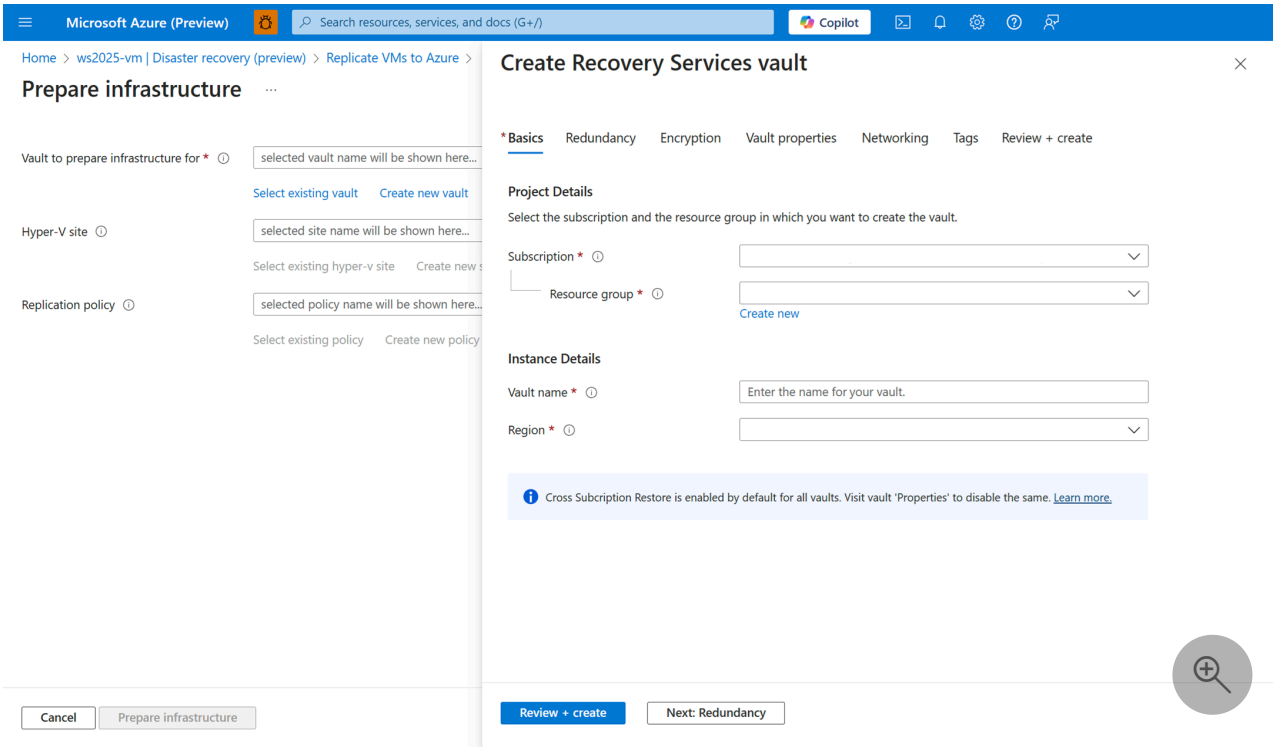
5. Sous **l'étape 1 : Préparer l'infrastructure**, sélectionnez **Préparer l'infrastructure**.




6. Dans la page **Préparer l'infrastructure** , les éléments suivants doivent être créés, sauf s'ils existent déjà :

   - Un coffre pour l'infrastructure.
   - Un site Hyper-V.
   - Stratégie de réplication.

S'il existe déjà, sélectionnez **Préparer l'infrastructure**. S'ils n'existent pas, créez chacun d'eux et sélectionnez **Vérifier + créer**. Une fois les trois générés, sélectionnez **Préparer l'infrastructure**.




7. Une fois les préparations de l'infrastructure terminées et l'extension Azure Site Recovery correctement installée sur le nœud, la notification contextuelle **Statut : Infrastructure préparée avec succès** s'affiche.

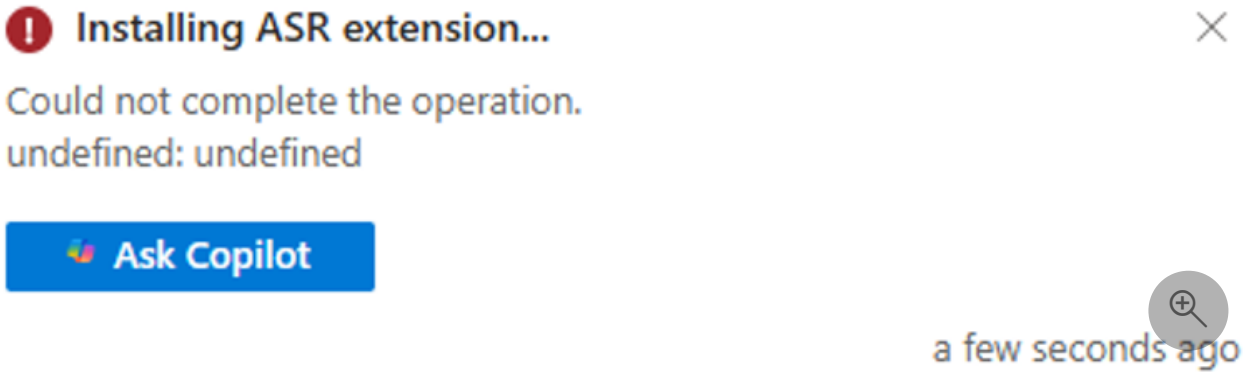
8. Enfin, sélectionnez **Activer la réplication**.

> ⓘ **Notes**
>
> La préparation et l'installation de l'agent d'infrastructure peuvent prendre jusqu'à 7 minutes. Vous pouvez actualiser l'état en sélectionnant le **bouton Actualiser** sur cette page. L'actualisation vous permet de revenir à la **page Répliquer des machines virtuelles vers Azure** .

# Problèmes connus

Comme l'outil de configuration Azure Site Recovery est en préversion, les utilisateurs peuvent rencontrer des problèmes techniques pendant le processus de déploiement. Pour atténuer certains problèmes, effectuez les actions suivantes :

- **Problème** : vous rencontrez l'erreur :




- **Solution** : aucune action n'est nécessaire, car cette erreur est temporaire. Accédez à **Gestion Windows** > **Configuration d'Azure Site Recovery (préversion)** > **Protéger les charges de travail de machine virtuelle** et vérifiez l'état de votre infrastructure dans **Étape 1 : Préparer l'infrastructure**.

- **Problème** : Vous rencontrez l'erreur PowerShell suivante :

```
error

Extension failed to install. Extension returned non-zero exit code for
Install: 1. Extension error output: std error:
C:\Packages\Plugins\Microsoft.SiteRecovery.Dra.Windows\1.0.0.6\script\Install
Asr.ps1 : Hyper-V is not installed.
  + CategoryInfo          : NotSpecified: (:) [Write-Error],
WriteErrorException
  + FullyQualifiedErrorId :
Microsoft.PowerShell.Commands.WriteErrorException,InstallAsr.ps1

Extension Error:
C:\Packages\Plugins\Microsoft.SiteRecovery.Dra.Windows\1.0.0.6\script\Install
Asr.ps1 : Hyper-V is not installed.
  + CategoryInfo          : NotSpecified: (:) [Write-Error],
WriteErrorException
  + FullyQualifiedErrorId :
Microsoft.PowerShell.Commands.WriteErrorException,InstallAsr.ps1
```

- **Solution** : cette erreur indique que Hyper-V peut ne pas être installé sur votre machine virtuelle. Exécutez la commande PowerShell suivante avec les droits d'administrateur :

```
PowerShell

Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
```

# Envoyer des commentaires sur les outils

Pour signaler les commentaires de l'application pour la récupération d'urgence ou si d'autres problèmes sont rencontrés, faites-nous savoir via le Hub de commentaires en effectuant les actions suivantes :

1. Exécutez la commande PowerShell suivante sur votre appareil en tant qu'administrateur pour collecter les journaux d'erreurs au format `.zip` :

   ```PowerShell
   azcmagent logs -o "C:\AzureArc\azcmagent-logs.zip"
   ```

2. Ouvrez le Hub de commentaires sur votre appareil.

3. Sous **Résumez votre feedback**, tapez **Azure Arc récupération d'urgence (version préliminaire)**.

4. Sous **Expliquer plus en détail (facultatif)**, fournissez-nous :

   a. Système d'exploitation et édition Windows Server que vous gérez.

   b. Instructions détaillées sur la reproduction de l'erreur rencontrée.

5. Sous **Choisir une catégorie**, sélectionnez **Problème**, sélectionnez **Windows Server** dans la liste déroulante, sélectionnez **Gestion** dans la liste déroulante secondaire, puis sélectionnez **OK**.

6. Sous **Rechercher des commentaires** similaires, consultez si d'autres utilisateurs ont soumis un problème similaire. Ensuite, sélectionnez **Suivant**.

7. Sous **Ajouter plus d'informations** et **laquelle des options suivantes décrit le mieux votre problème ?**, sélectionnez l'option la plus appropriée pour votre cas.

8. Sous **Pièces jointes (facultatif)**, fournissez-nous :

   a. Capture d'écran du problème.

   b. Joignez le fichier **azcmagent-logs.zip** .

9. Enfin, sélectionnez **Envoyer** pour envoyer vos commentaires à des fins de révision.

# Voir aussi

- Configurer l'évaluation des meilleures pratiques pour les serveurs Windows avec Arc
- configurer la prise en charge à distance des serveurs Windows avec Arc

# Configurer l’évaluation des meilleures pratiques pour les serveurs Windows avec Arc

14/08/2025

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

L’outil d’évaluation des meilleures pratiques analyse continuellement votre Serveur Windows pour évaluer ses configurations par rapport aux meilleures pratiques Windows. Ces évaluations peuvent être planifiées pour s’exécuter automatiquement ou lancées manuellement selon les besoins. L’évaluation évalue plusieurs aspects de l’environnement serveur, notamment les bases de référence du serveur, la sécurité du serveur, Hyper-V, les clusters de basculement et les services Iis (Internet Information Services). Il collecte et analyse également les données du serveur pour générer une liste de problèmes qui nécessitent des conseils de correction et des meilleures pratiques pour améliorer les performances de votre infrastructure de serveur, notamment le déploiement d’applications, de mises à jour logicielles et de systèmes d’exploitation.

L’outil Best Practices Assessment installe les trois extensions suivantes sur votre appareil :

- **Plateforme** d’évaluation : déploie la plateforme d’évaluation des meilleures pratiques sur votre ordinateur. Cette extension sert de plateforme pour le développement futur en tant que nouveaux scénarios d’évaluation des meilleures pratiques sont introduits.
- **Évaluation** de Windows Server : contient toutes les informations nécessaires sur les vérifications de validation qui doivent être exécutées sur votre appareil pour vous fournir les recommandations que vous voyez dans le Portail Azure. Une fois l’évaluation terminée, les résultats sont enregistrés dans un fichier journal local.
- **Agent Azure Monitor (AMA)** : collecte et charge le fichier journal dans votre espace de travail Log Analytics dans le cloud, en vous fournissant toutes les informations contenues dans le Portail Azure. Les classeurs sont utilisés pour visualiser les résultats et vous offrir une expérience de lecture plus facile.

> ⓘ **Notes**
>
> - L’outil Best Practices Assessment gère la sécurité en exécutant toutes les vérifications localement sur votre serveur. Les résultats sont uniquement chargés sur votre compte de stockage Azure désigné, ce qui garantit que tout se produit dans le contexte de votre compte.

- L'outil Best Practices Assessment doit être installé sur chaque serveur sur lequel vous souhaitez l'exécuter.
- L'installation des extensions requises sur un serveur Arc via PowerShell n'est actuellement pas prise en charge.

# Prérequis

- Votre appareil doit exécuter un système d'exploitation Windows Server 2016 local ou ultérieur avec Arc avec un minimum de 4 Go de mémoire.
- Si vous débutez avec Azure Arc, votre appareil doit être intégré. Pour plus d'informations, consultez Démarrage rapide : Connecter des machines hybrides avec des serveurs avec Azure Arc.
- Vous devez utiliser les types de licences Pay-as-you-go de Windows Server ou Software Assurance.

## Déployer l'évaluation des meilleures pratiques

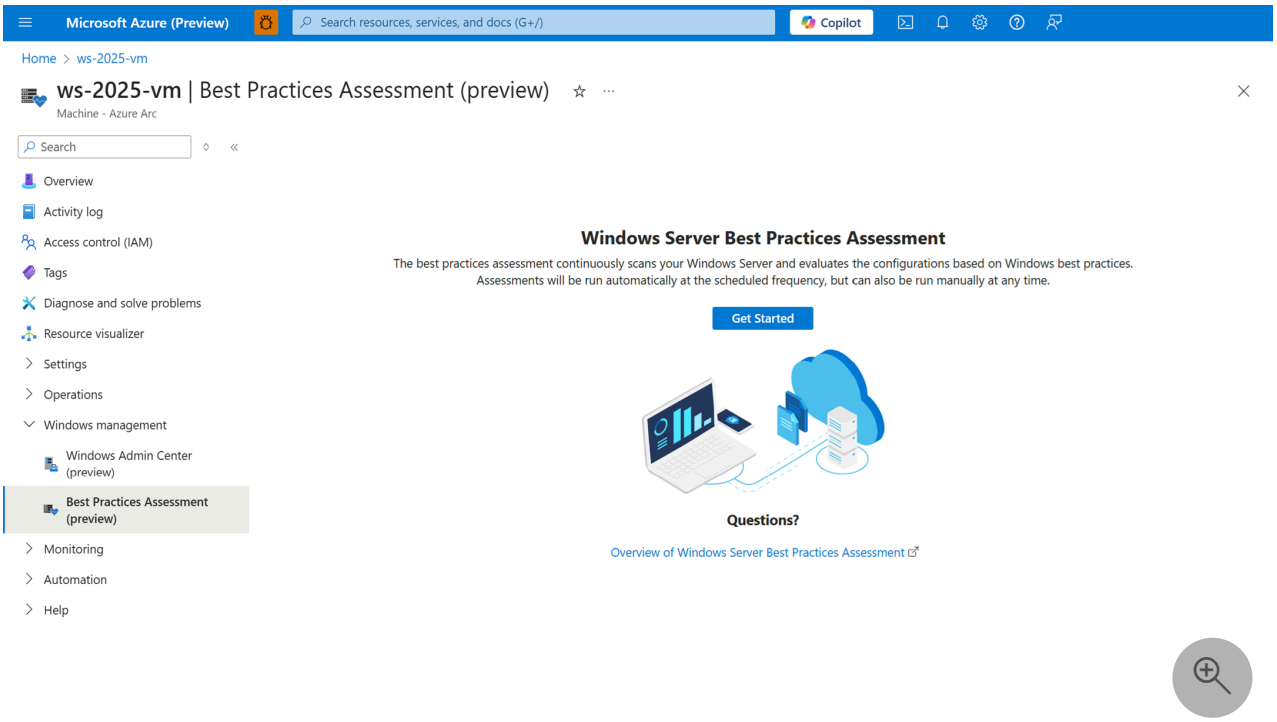
Pour déployer l'évaluation des meilleures pratiques, procédez comme suit :

1. Accédez au Portail Azure, puis sélectionnez votre appareil Windows Server Arc.

   > **Notes**
   >
   > Pendant la phase de préversion publique, sachez que cette fonctionnalité est accessible uniquement dans le cloud public.

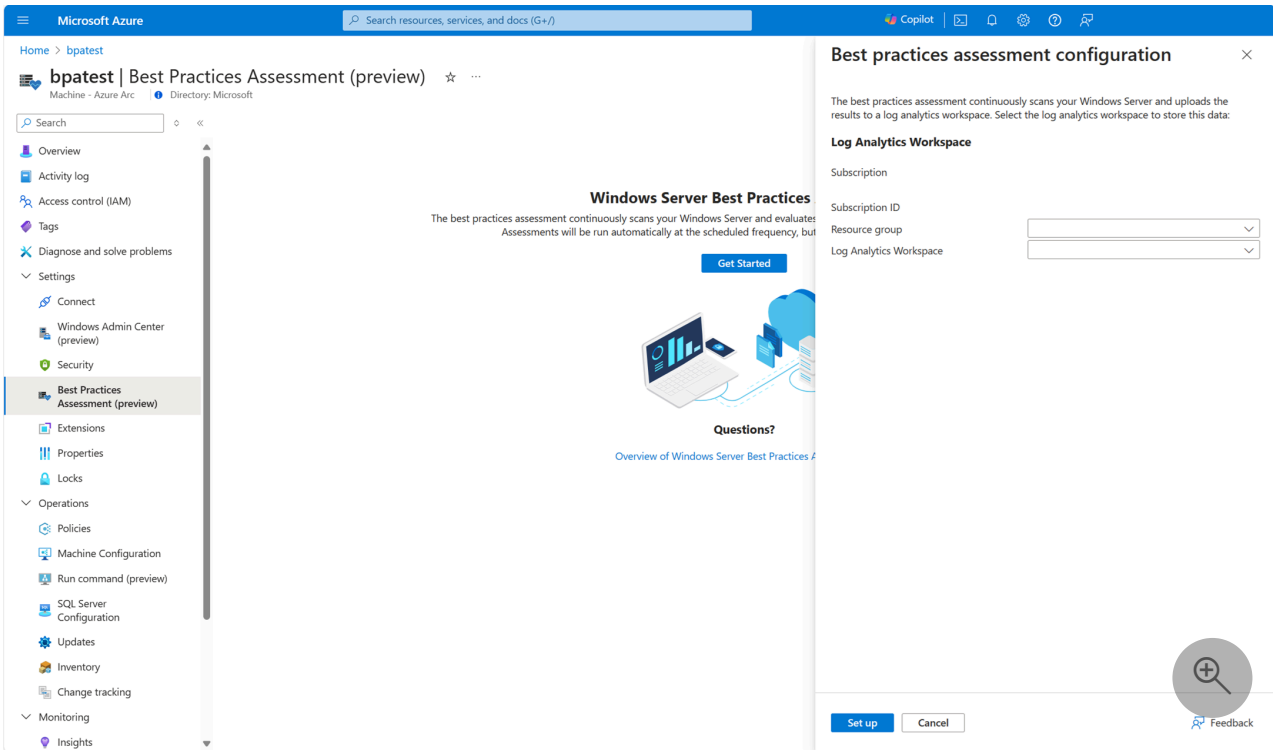
2. Accédez à une ressource Windows Server 2016 ou ultérieure compatible Avec Arc. Cette machine virtuelle doit être l'hôte Hyper-V.

3. Dans le volet gauche, accédez à **la gestion de Windows**, puis sélectionnez **Best Practices Assessment (aperçu)**.




4. Sélectionnez **Prise en main** pour accéder à la configuration **de l'évaluation** des meilleures pratiques.

5. Fournissez le groupe **de ressources et l'espace de travail** Log Analytics où les résultats de l'évaluation sont enregistrés, puis sélectionnez **Configurer**. Rappelez-vous que les frais s'appliquent aux données stockées dans votre espace de travail Log Analytics.

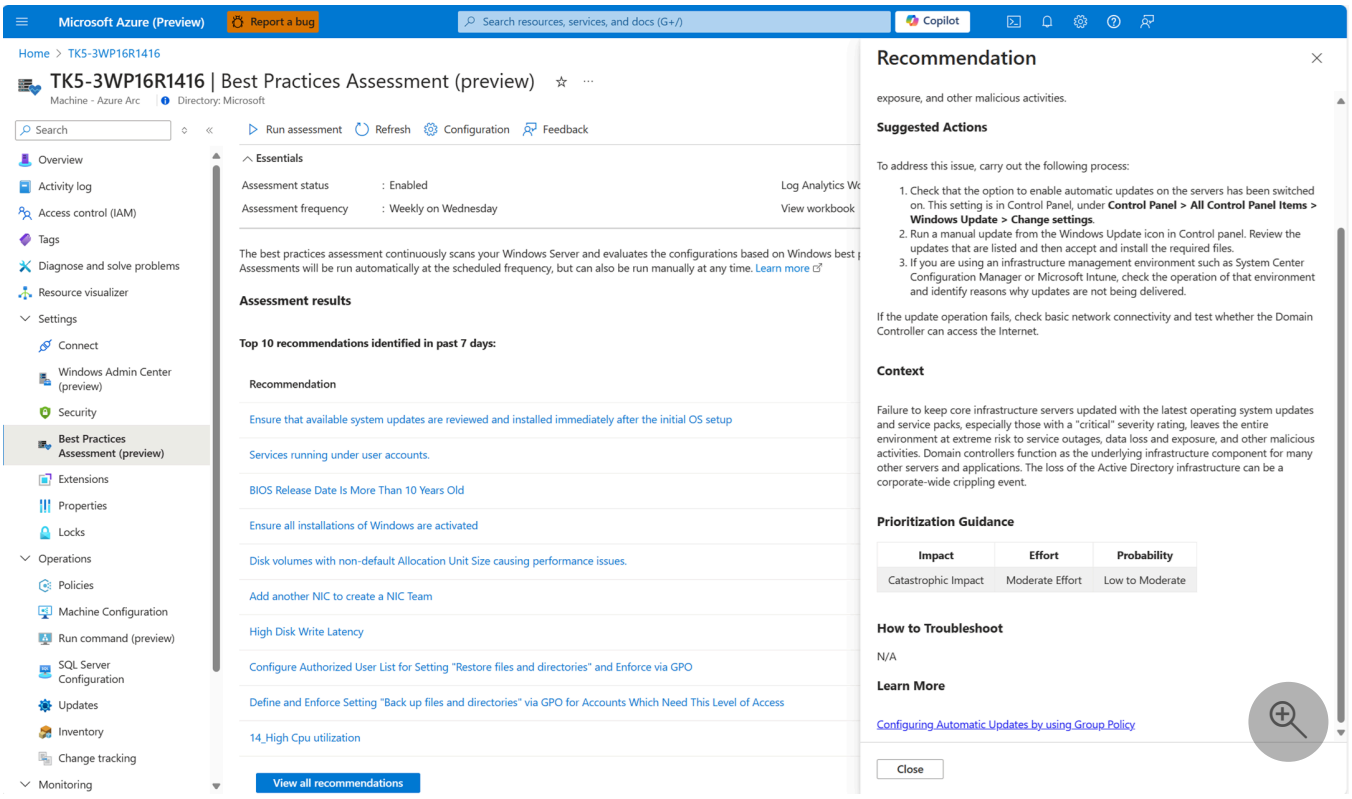



> ⓘ Notes

> Les temps d'installation varient et peuvent prendre jusqu'à 15 minutes. Vous pouvez actualiser l'état en sélectionnant le **bouton Actualiser** sur cette page.

6. Une fois le déploiement terminé, sélectionnez **Accéder à la ressource**, sélectionnez **Best Practices Assessment (préversion),** puis sélectionnez **Exécuter l'évaluation** en haut de la page.

L'exécution de l'évaluation pour la première fois prend jusqu'à 4 heures pour que l'évaluation s'exécute et fournisse des résultats.



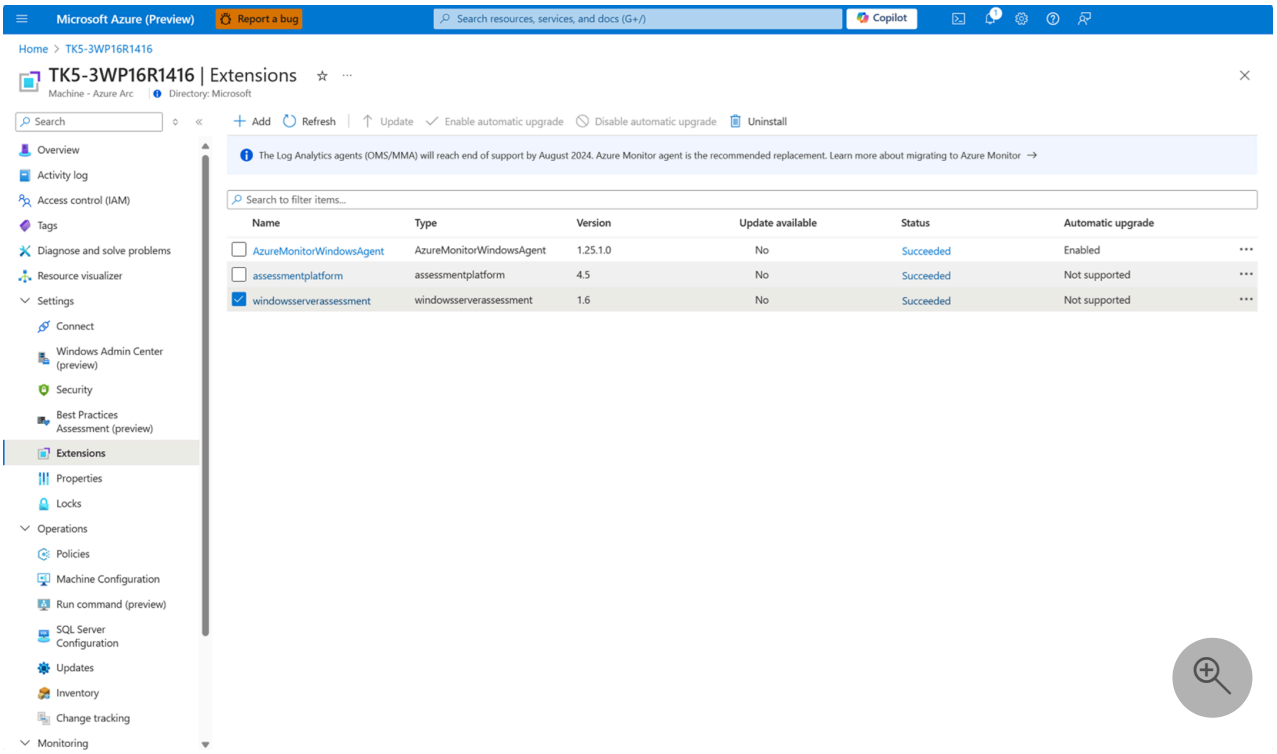

Pendant toute la durée de la préversion publique, nous proposons des mises à jour pour améliorer l'expérience. Pour mettre à jour **l'évaluation des meilleures pratiques (préversion)**, procédez comme suit :

1. Accédez à votre ressource.

2. Dans le volet gauche, développez **Paramètres** et sélectionnez **Extensions**.

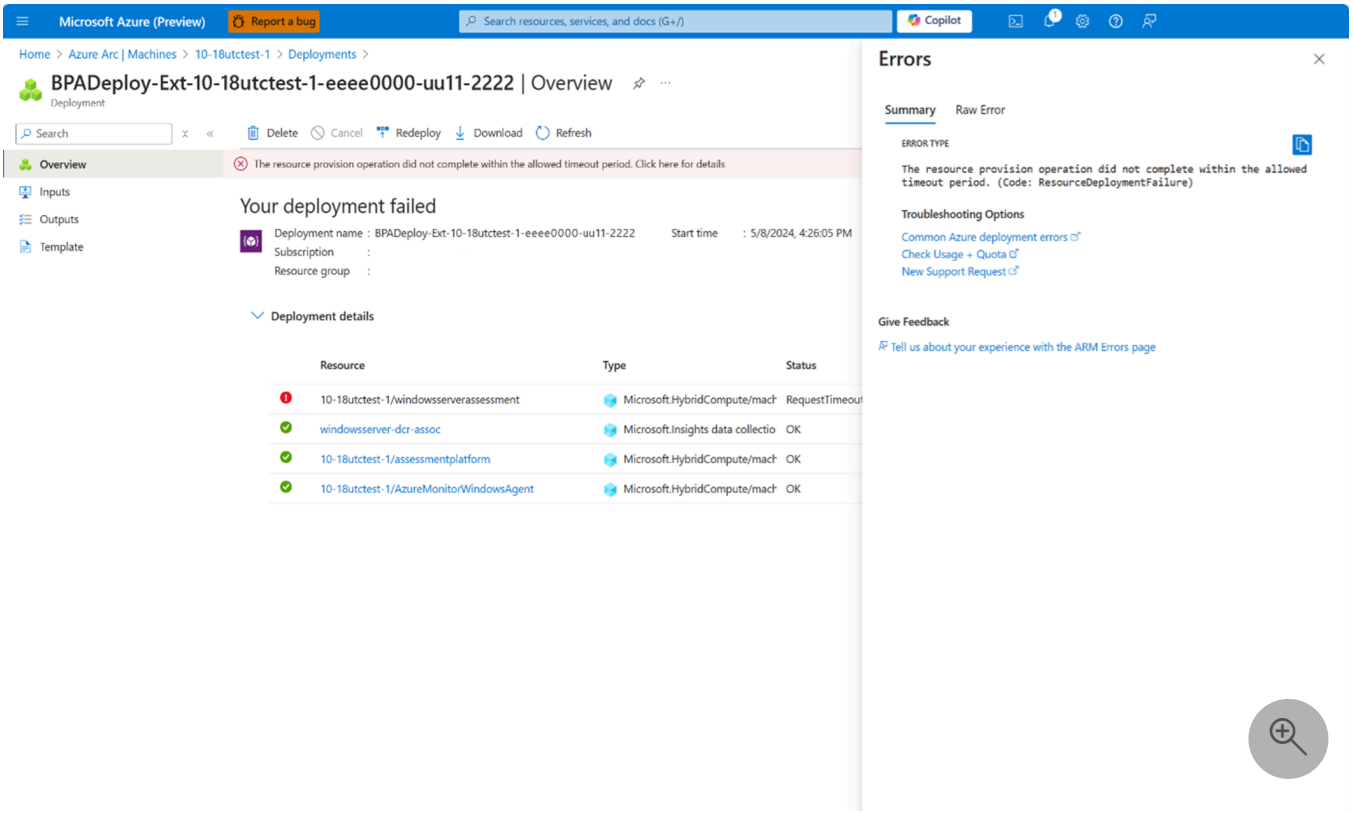
3. Sélectionnez le **bouton Mettre à jour** pour l'une des trois extensions disponibles :

   - `AzureMonitorWindowsAgent`
   - `assessmentplatform`
   - `windowsserverassessment`




# Résoudre les problèmes de déploiement

En cas d'échec de votre déploiement, la **notification de votre déploiement a échoué** s'affiche.




Si cette erreur se produit, votre extension doit être réactivée. Pour corriger ce problème, procédez comme suit :

1. Accédez à votre ressource.

2. Dans le volet gauche, développez **Paramètres** et sélectionnez **Extensions**.

3. Dans la **colonne Name** , où **windowsserverassessment** est affiché, suivez cette ligne pour localiser votre numéro de version sous la **ligne Version** .

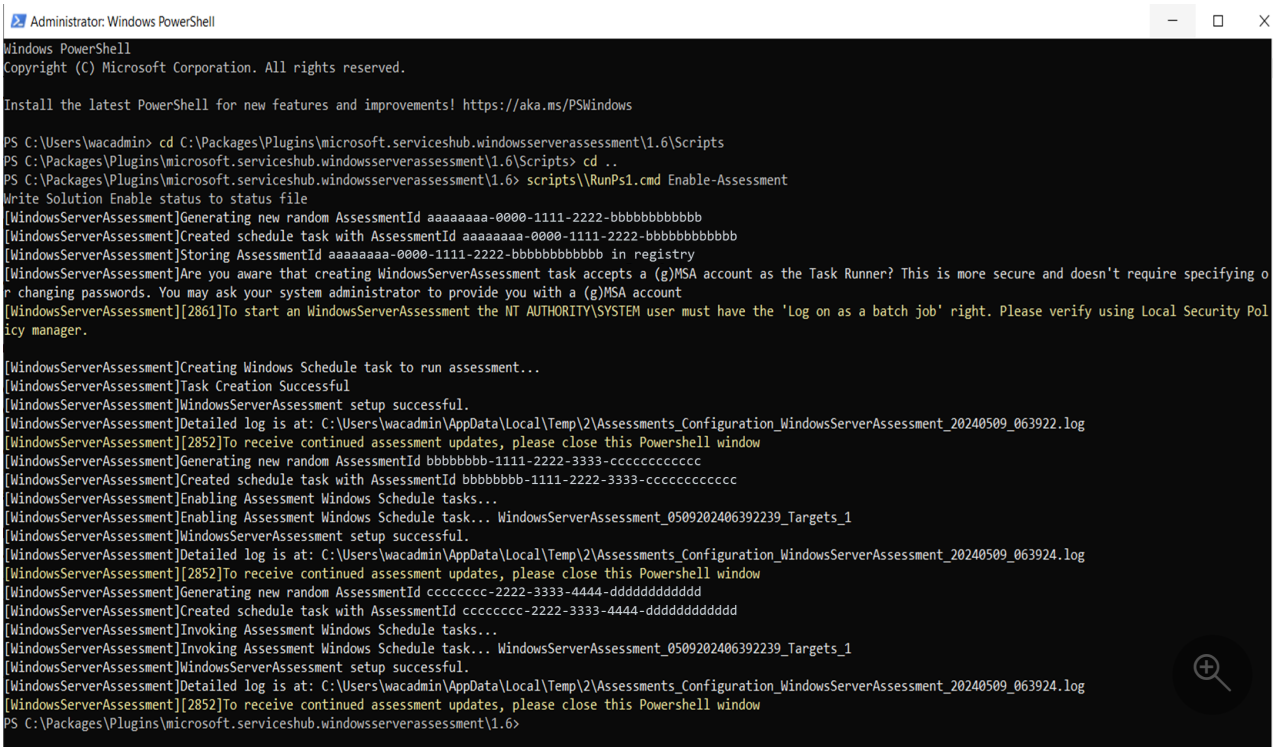
4. À distance sur votre appareil serveur et exécutez la commande suivante en tant qu'administrateur :

   PowerShell

   ```
   cd C:\Packages\Plugics\microsoft.serviceshub.windowsserverassessment\
   <VersionNumber>

   scripts\\RunPs1.cmd Enable-Assessment
   ```

   Les utilisateurs doivent s'attendre à la sortie suivante lors de l'exécution de ce script :

5. Une fois le script terminé, accédez à votre Portail Azure. Ouvrez votre ressource, sélectionnez **Best Practices Assessment (préversion)**, puis **exécutez l'évaluation**.

# Envoyer des commentaires sur les outils

Pour signaler les commentaires de l'application pour l'outil d'évaluation des meilleures pratiques ou si d'autres problèmes sont rencontrés, faites-nous savoir via le Hub de commentaires. Pour plus d'informations, consultez Envoyer des commentaires sur les outils. Sous **Résumer vos commentaires**, tapez **Azure Arc BPA (préversion)** et effectuez les étapes restantes.

# Voir aussi

- Configurer Azure Site Recovery pour les serveurs Windows activés pour Azure Arc
- Configurer la prise en charge à distance des serveurs Windows avec Arc

# Configurer la prise en charge à distance des serveurs Windows avec Arc

15/08/2025

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

En activant le support à distance (préversion), vous autorisez un professionnel du support Microsoft à résoudre votre problème plus rapidement en accédant à votre appareil à distance pour la résolution des problèmes. Vous avez un contrôle total sur le niveau d'accès que les professionnels du support Microsoft ont, la durée de l'accès et votre consentement est requis pour accéder à votre appareil. Le support Microsoft ne peut accéder à votre appareil qu'après avoir envoyé une demande de support. Pour savoir comment créer une demande, consultez Créer une demande de support Azure.

Une fois le support à distance activé, le support Microsoft obtient un accès temporaire à votre appareil. L'accès est effectué via un canal sécurisé, audité et conforme qui utilise HTTPS sur le port 443 avec le trafic chiffré TLS 1.2. Les actions que les professionnels du support Microsoft peuvent effectuer sont limitées à ce que vous autorisez, en utilisant Just Enough Administration (JEA). Ce processus implique l'accès authentifié entre vous et le support Microsoft pour les diagnostics, la résolution des problèmes et les actions de correction.

Pour simplifier la configuration et améliorer la résolution des problèmes de support, l'extension Arc de support à distance peut préinstaller l'agent de support distant sur tous les nœuds de cluster et configurer des tâches planifiées pour JEA. Le flux de travail JEA est le suivant :




# Prerequisites

- Votre appareil doit exécuter un système d'exploitation Windows Server 2016 local ou ultérieur avec Arc avec un minimum de 4 Go de mémoire.
- Si vous débutez avec Azure Arc, votre appareil doit être intégré. Pour plus d'informations, consultez démarrage rapide : Connecter des machines hybrides avec des serveurs avec Azure Arc.
- Vous devez utiliser les types de licences Windows Server Pay-as-you-go ou Software Assurance.

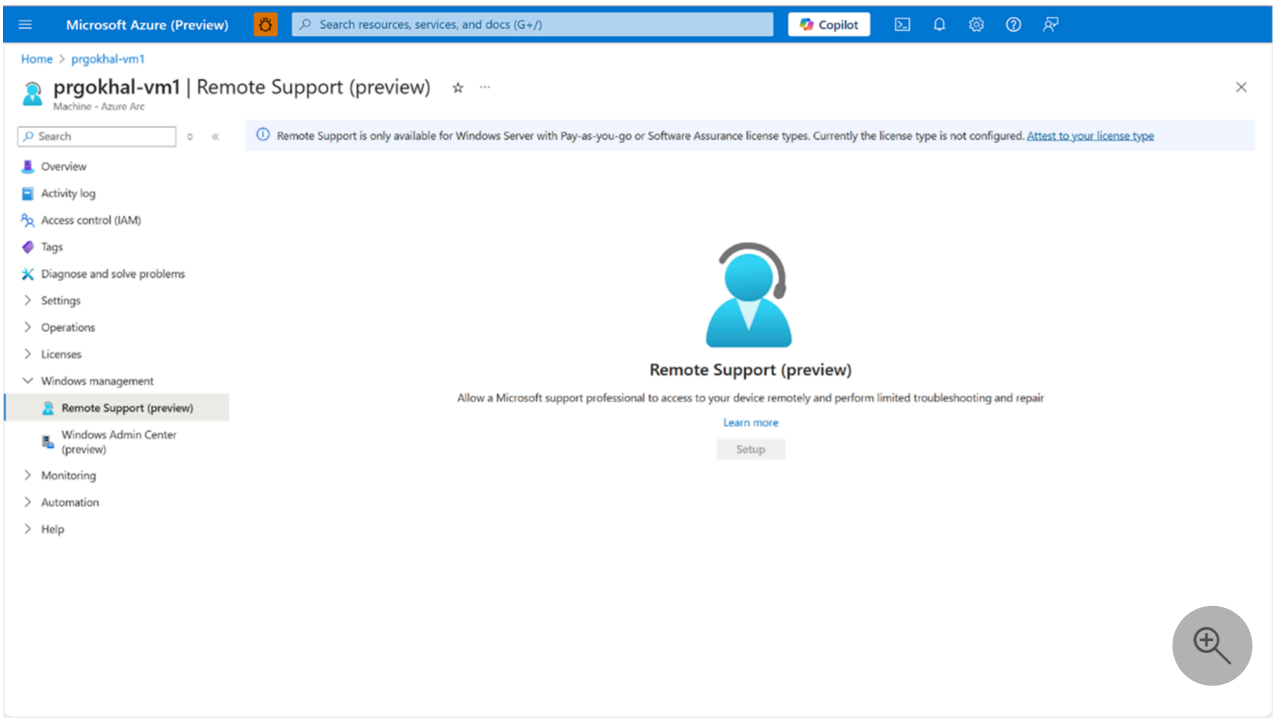
## Configurer la prise en charge à distance

Pour configurer la prise en charge à distance, procédez comme suit :

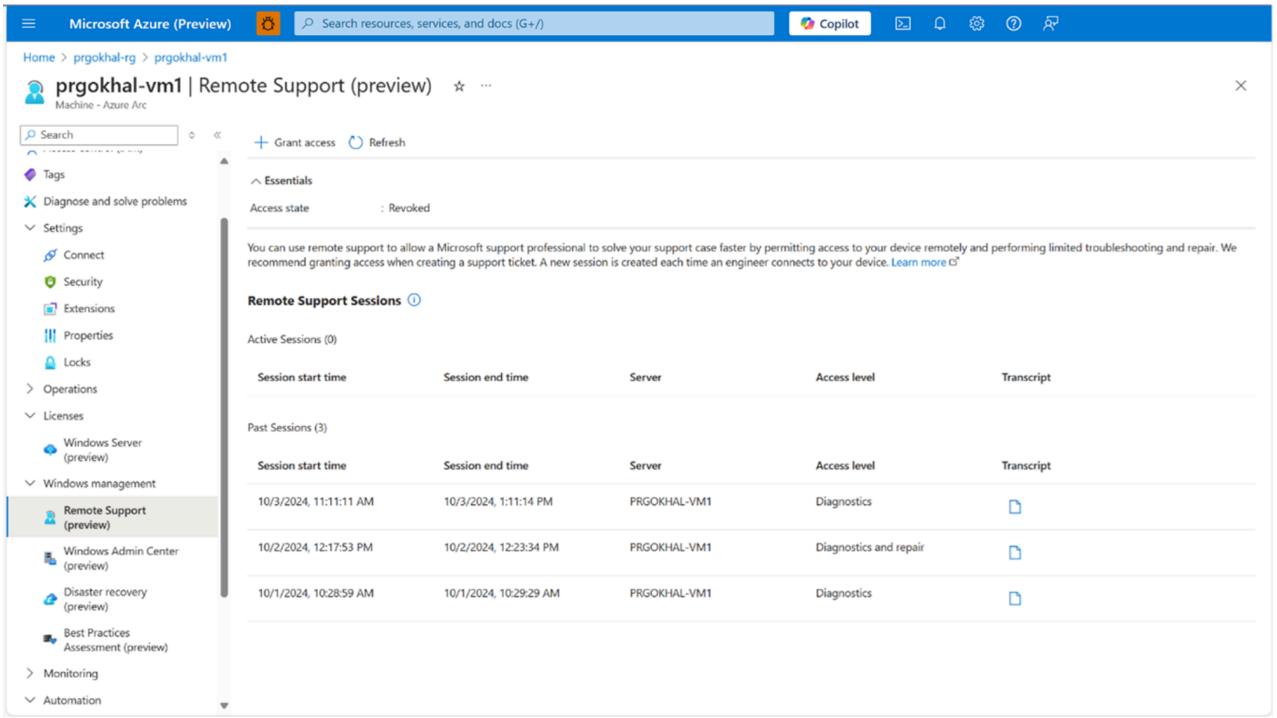
1. Accédez au Portail Azure, puis sélectionnez votre appareil Windows Server Arc. Cette machine virtuelle doit être l'hôte Hyper-V.

2. Dans le volet gauche, accédez à **la gestion de Windows**, puis sélectionnez **Support à distance (préversion)** .

3. Dans l'écran **Support à distance (préversion)**, sélectionnez **Configuration**.

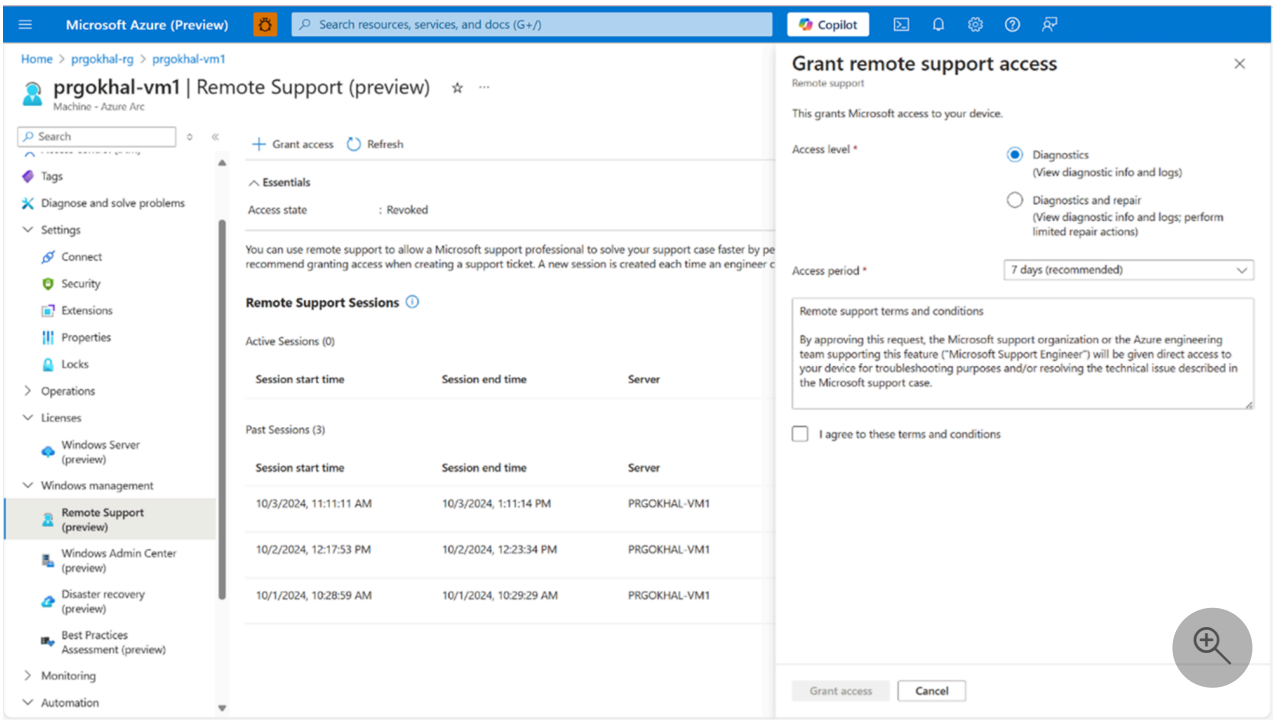



4. Une fois la configuration terminée, l'écran **Sessions de Support à Distance** s'affiche.




5. Pour accorder l'accès à une session de support à distance, sélectionnez **+ Accorder l'accès** en haut de la page.

6. Spécifiez le **niveau d'accès** et la **période d'accès** pour votre session.



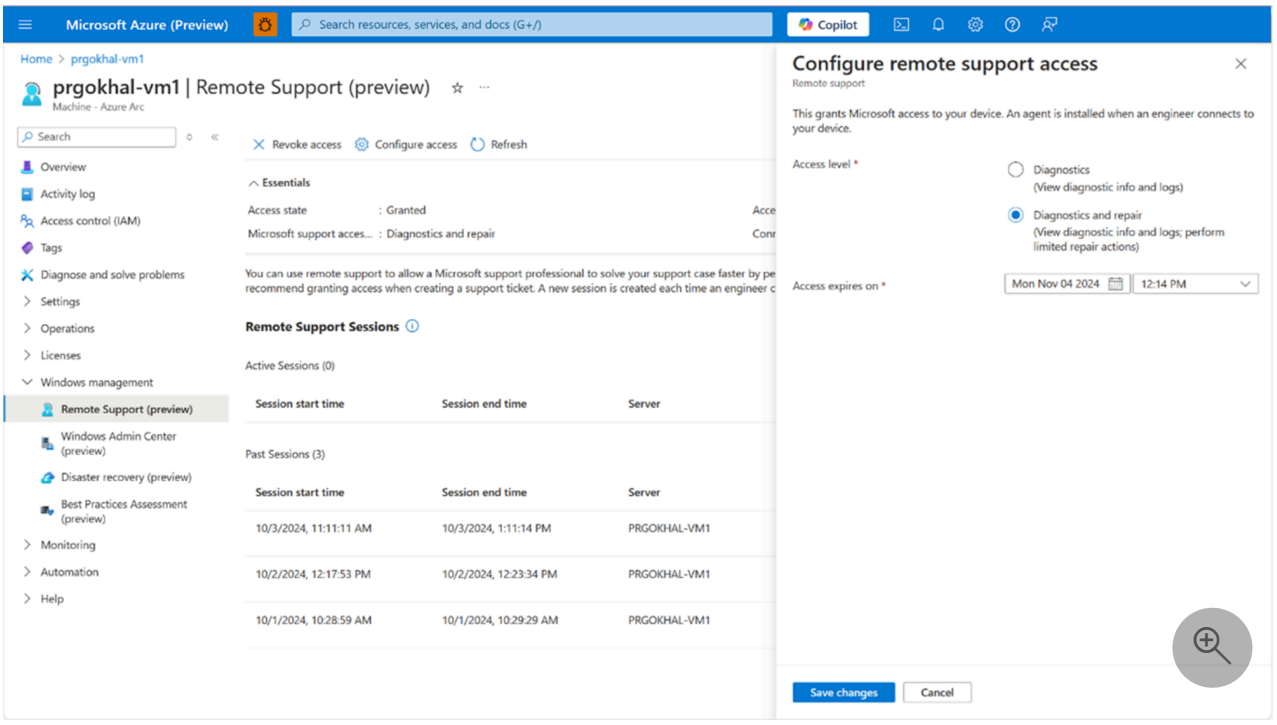

7. Lisez les conditions générales avant de sélectionner le **j'accepte ces conditions** case à cocher, puis sélectionnez **Accorder l'accès**.

# Configurer l'accès à la prise en charge à distance

Les utilisateurs peuvent également modifier le niveau d'accès et de durée à tout moment. Pour apporter ces modifications après la configuration, procédez comme suit :

1. Dans le volet gauche, accédez à **la gestion de Windows**, puis sélectionnez **Support à distance (préversion)** .

2. Sélectionnez **Configurer l'accès** en haut de la page.



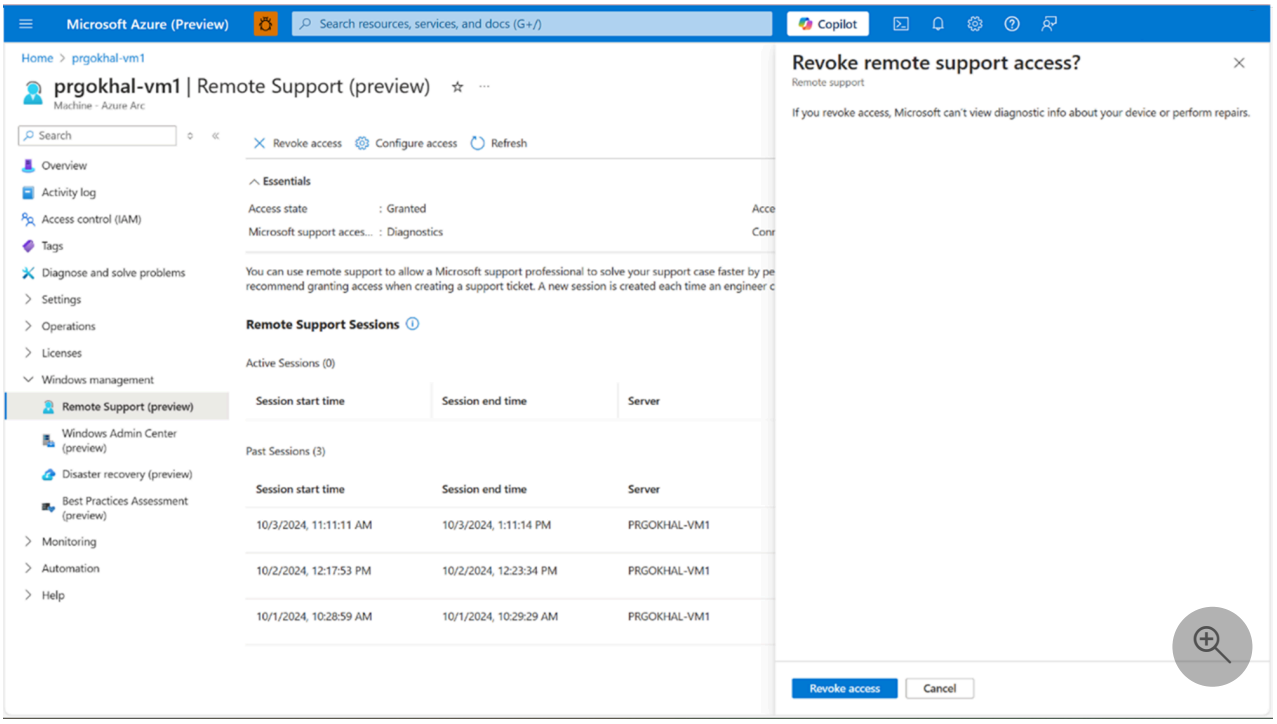

3. Une fois les modifications effectuées, sélectionnez **Enregistrer les modifications**.

# Révoquer l'accès à la prise en charge à distance

Si l'accès au support à distance n'est plus nécessaire, les utilisateurs peuvent choisir de révoquer l'accès à tout moment. Pour révoquer l'accès, procédez comme suit :

1. Dans le volet gauche, accédez à **la gestion de Windows**, puis sélectionnez **Support à distance (préversion)** .

2. Sélectionnez **Révoquer l'accès** en haut de la page, puis sélectionnez **Révoquer l'accès** dans l'écran **Révoquer l'accès au support à distance ?**




# Conditions générales du support à distance

Les conditions générales suivantes décrivent la façon dont les données sont gérées pendant les sessions de support à distance. Lisez-les attentivement avant d'accorder l'accès.

```
By approving this request, the Microsoft support organization or the Azure
engineering team
supporting this feature ("Microsoft Support Engineer") will be given direct access
to your device
for troubleshooting purposes and/or resolving the technical issue described in the
Microsoft
support case.

During a remote support session, a Microsoft Support Engineer may need to collect
logs. By enabling
remote support, you have agreed to a diagnostics log collection by a Microsoft
Support Engineer to
address a support case. You also acknowledge and consent to the upload and
retention of those logs
in an Azure storage account managed and controlled by Microsoft. These logs may be
accessed by
Microsoft in the context of a support case and to improve the health of Windows
Server.

The data will be used only to troubleshoot failures that are subject to a support
ticket, and will
not be used for marketing, advertising, or any other commercial purposes without
your consent. The
data may be retained for up to ninety (90) days and will be handled following our
standard privacy
```

```
practices.

Any data previously collected with your consent will not be affected by the
revocation of your
permission.
```

Pour plus d'informations sur la façon dont Microsoft traite les données personnelles, notamment les données traitées et à quelles fins, consultez la Déclaration de confidentialité Microsoft.

## Voir aussi

- Configurer Azure Site Recovery pour les serveurs Windows activés pour Arc
- Configurer l'évaluation des meilleures pratiques pour les serveurs Windows activés par Arc

# Vue d’ensemble de Windows Admin Center

16/08/2025S’applique à: ✅ Windows Admin Center, ✅ Windows Admin Center Preview

Windows Admin Center est un outil de gestion à distance pour Windows Server, pouvant s’exécuter n’importe où (environnement physique, virtuel, local, dans Azure ou hébergé) sans frais supplémentaires.

Pour connaître les nouveautés, consultez l’historique des versions.

## Télécharger maintenant

**Téléchargez Windows Admin Center** à partir du centre d’évaluation Microsoft.

Pour obtenir de l’aide sur l’installation, consultez Installer. Pour obtenir des conseils sur la prise en main de Windows Admin Center, consultez Prise en main.

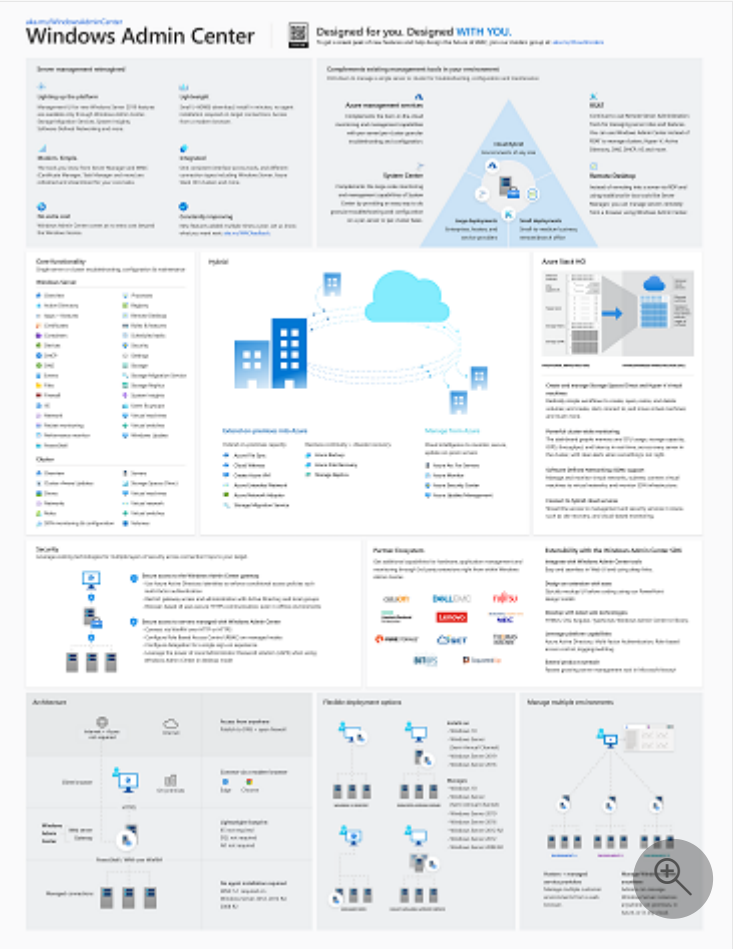
Pour mettre à jour les versions de Windows Admin Center qui ne sont pas des préversions, utilisez Microsoft Update ou téléchargez et installez manuellement Windows Admin Center. Chaque version non-Preview de Windows Admin Center est prise en charge jusqu’à 30 jours après la publication de la prochaine version non-Preview. Pour plus d’informations , consultez notre stratégie de support.

## Scénarios d’utilisation de Windows Admin Center

Voici quelques-unes des tâches que vous pouvez accomplir avec Windows Admin Center :

- **Simplifier la gestion de serveurs** : gérez vos serveurs et clusters avec des versions modernisées d’outils familiers tels que le Gestionnaire de serveur. Effectuez une installation en moins de cinq minutes et gérez les serveurs de votre environnement immédiatement, sans configuration supplémentaire requise. Pour plus d’informations, consultez Qu’est-ce que Windows Admin Center ?
- **Utiliser des solutions hybrides** : l’intégration à Azure vous permet de connecter éventuellement vos serveurs locaux à des services cloud appropriés. Pour plus d’informations, consultez Services hybrides Azure.
- **Rationaliser la gestion hyperconvergée**: simplifiez la gestion des clusters hyperconvergés Azure Local ou Windows Server. Utilisez des charges de travail simplifiées pour créer et gérer des machines virtuelles, des volumes Espaces de stockage direct, des solutions SDN (Software-Defined Networking), etc. Pour plus d’informations, consultez Gérer HCI.

Voici une vidéo qui vous donne une vue d'ensemble, suivie d'une affiche présentant plus de détails :
https://www.youtube-nocookie.com/embed/WCWxAp27ERk




Télécharger le PDF de cette affiche

# Aperçu rapide du contenu

Agrandir le tableau

| Understand | Plan |
| --- | --- |
| - Qu'est-ce que Windows Admin Center ?<br>- Questions fréquemment posées<br>- Étude de cas<br>- Produits de gestion associés | - Quel type d'installation vous convient ?<br>- Options d'accès utilisateur |

Agrandir le tableau

| Deploy | Configure |
| --- | --- |
| - Préparer votre environnement<br>- Installer Windows Admin Center | - Paramètres de Windows Admin Center<br>- Autorisations et contrôle d'accès utilisateur |

| Deploy | Configure |
| --- | --- |
| - Activer une haute disponibilité | - Connexions partagées<br>- Extensions<br>- Automatiser avec PowerShell |

Agrandir le tableau

| Use | Connexion à Azure |
| --- | --- |
| - Démarrer et ajouter des connexions<br>- Gérer les serveurs<br>- Déployer une infrastructure hyperconvergée<br>- Gérer l'infrastructure hyperconvergée<br>- Gérer les clusters de basculement<br>- Gestion des machines virtuelles<br>- Exploitation forestière | - Services hybrides Azure<br>- Connecter Windows Admin Center à Azure<br>- Déployer Windows Admin Center dans Azure<br>- Gérer les machines virtuelles Azure avec Windows Admin Center |

Agrandir le tableau

| Windows Admin Center dans Azure | Support |
| --- | --- |
| - Gérer des machines virtuelles Windows Server IaaS<br>- Gérer les serveurs activés pour Azure Arc (préversion)<br>- Gérer les clusters locaux Azure (préversion) | - Historique des versions<br>- Stratégie de support<br>- Étapes courantes de résolution des problèmes<br>- Problèmes connus |

Agrandir le tableau

| Extend |
| --- |
| - Vue d'ensemble des extensions<br>- Présentation des extensions<br>- Développer une extension<br>- Guides<br>- Extensions de publication |

# Découvrez les avantages que Windows Admin Center offre aux clients

- « Avec [Windows Admin Center], nous avons réduit de plus de 75 % le temps et les efforts nécessaires pour gérer le système de gestion. »

  *- Rand Morimoto, directeur de Convergent Computing*

- « Grâce à [Windows Admin Center], nous pouvons gérer nos clients à distance sans problème à partir d'un portail HTML5 et avec une intégration complète à Microsoft Entra ID, et nous pouvons améliorer la sécurité avec l'authentification multifacteur. »

  *- Silvio Di Benedetto, fondateur et consultant senior d'Inside Technologies*

- « Nous avons été en mesure de déployer des références SKU [Server Core] de manière plus efficace, d'améliorer l'efficacité des ressources, la sécurité et l'automatisation tout en obtenant un bon degré de productivité et en réduisant les erreurs qui peuvent se produire lors de la création de scripts uniquement. »

  *- Guglielmo Mengora, fondateur et PDG de VaiSulWeb*

- « Avec [Windows Admin Center] les clients en particulier sur le marché SMB disposent désormais d'un outil facile à utiliser pour gérer leur infrastructure interne. Il permet de réduire les tâches administratives et de gagner beaucoup de temps. Et le meilleur de celui-ci : il n'y a pas de frais de licence supplémentaires pour [Windows Admin Center] !

  *- Helmut Otto, directeur général de SecureGUARD*

Pour en savoir plus sur les entreprises qui utilisent Windows Admin Center dans leurs environnements de production, consultez Études de cas Windows Admin Center.

# Produits connexes

Windows Admin Center est conçu pour gérer un seul serveur ou cluster. Il complète, mais ne remplace pas les solutions de supervision et de gestion de Microsoft comme les Outils d'administration de serveur distant (RSAT), System Center, Intune ou Azure Stack.

Pour savoir comment Windows Admin Center complète d'autres solutions de gestion Microsoft, consultez Windows Admin Center et les solutions de gestion associées de Microsoft.

# Restez à jour

- Suivez-nous sur X (anciennement Twitter)
- Consultez nos blogs

# Forum aux questions sur Windows Admin Center

Voici des réponses aux questions les plus fréquemment posées sur Windows Admin Center.

# Qu'est-ce que Windows Admin Center ?

Windows Admin Center est une plateforme et un ensemble d'outils d'interface graphique utilisateur léger basé sur un navigateur pour les administrateurs informatiques afin de gérer Windows Server et le client Windows. Il s'agit de l'évolution des outils d'administration intégrés familiers, tels que le Gestionnaire de serveur et la Console de gestion Microsoft (MMC) en une expérience moderne, simplifiée, intégrée et sécurisée.

# Puis-je utiliser Windows Admin Center dans des environnements de production ?

Yes. Windows Admin Center est généralement disponible et prêt pour les déploiements d'utilisation et de production étendus. Les fonctionnalités actuelles de la plateforme et les outils de base répondent aux critères de publication standard de Microsoft et à notre barre de qualité pour la facilité d'utilisation, la fiabilité, les performances, l'accessibilité, la sécurité et l'adoption.

Les versions de Windows Admin Center (sans préversion) sont prises en charge en continu, en fonction des politique de cycle de vie moderne de Microsoft. Cela signifie que seule la dernière version de Windows Admin Center est gérée et prise en charge, et que les utilisateurs doivent rester à jour en effectuant une mise à niveau vers la dernière version de Windows Admin Center dans les 30 jours suivant la disponibilité pour rester pris en charge. Cette stratégie s'applique à la fois à la plateforme Windows Admin Center elle-même, ainsi qu'aux extensions Microsoft publiées (sans préversion) publiées dans le flux d'extension Windows Admin Center. Notez que certaines extensions peuvent être mises à jour plus fréquemment que d'autres, entre les versions de Windows Admin Center.

Pour plus d'informations sur les versions préliminaires de Windows Admin Center, consultez versions windows Insider Preview.

# Combien coûte-t-il d'utiliser Windows Admin Center ?

Windows Admin Center n’a aucun coût supplémentaire au-delà de Windows. Vous pouvez utiliser Windows Admin Center (disponible en téléchargement distinct) avec des licences valides de Windows Server ou du client Windows sans frais supplémentaires. Windows Admin Center est concédé sous licence sous un contrat de lisence d’utilisateur final (CLUF) supplémentaire Windows.

# Quelles versions de Windows Server puis-je gérer avec Windows Admin Center ?

Windows Admin Center est optimisé pour Windows Server 2025. Bien que Windows Admin Center fonctionne le mieux avec Windows Server 2025, il prend en charge la gestion de plusieurs versions que les clients utilisent déjà : Windows Server 2016 et versions ultérieures sont entièrement prises en charge. Il existe également des fonctionnalités limitées pour la gestion de Windows Server 2012.

# Pouvez-vous installer Windows Admin Center version 2410 alors qu’une ancienne version de Windows Admin Center est déjà installée ?

Oui, vous pouvez installer Windows Admin Center 2410 en même temps qu’une version de passerelle héritée, à condition de ne pas choisir les mêmes ports pour les deux installations.

# Puis-je modifier les ports utilisés par ma passerelle modernisée Windows Admin Center après l’installation ?

Oui, dans les Program Files pour Windows Admin Center, nous avons inclus un module PowerShell appelé `Microsoft.WindowsAdminCenter.Configuration.psm1`. Ce module vous permet de modifier votre configuration WAC après l’installation et se trouve dans le dossier **PowerShellModules** de votre installation (`C:\Program Files\WindowsAdminCenter\PowerShellModules\` par défaut). Pour modifier les ports utilisés par votre instance Windows Admin Center, exécutez la commande suivante :

**PowerShell**

```
Set-WACHttpsPort -Wacport <port> -ServicePortRangeStart <port> -ServicePortRangeEnd
<port>
```

# Existe-t-il des problèmes connus avec Windows Admin Center version 2410 ?

Oui, il existe des problèmes connus avec la passerelle modernisée. Pour obtenir la liste des problèmes connus, consultez notre page sur les problèmes connus

# Puis-je modifier les paramètres de configuration autres que les paramètres de port après l'installation ?

Oui, vous pouvez utiliser le module `Microsoft.WindowsAdminCenter.Configuration.psm1` PowerShell pour modifier vos paramètres de configuration. Il se trouve dans le dossier **PowerShellModules** de votre installation.

# Toutes les fonctionnalités de la version 2311 sont-elles disponibles dans la version 2410 ?

Oui, toutes les fonctionnalités de la version 2311 sont disponibles dans la version 2410. La version 2410 est une passerelle modernisée qui inclut une nouvelle interface utilisateur et une nouvelle expérience, mais elle conserve toutes les fonctionnalités de la version précédente. En savoir plus sur la version 2311 de Windows Admin Center.

# Windows Admin Center est-il un remplacement complet pour tous les outils en boîte et RSAT traditionnels ?

No. Bien que Windows Admin Center puisse gérer de nombreux scénarios courants, il ne remplace pas complètement tous les outils MMC (Microsoft Management Console) traditionnels. Pour obtenir un aperçu détaillé des outils inclus dans Windows Admin Center,

découvrez plus en détail la gestion des serveurs dans notre documentation. Windows Admin Center dispose des fonctionnalités clés suivantes dans sa solution du Gestionnaire de serveur :

- Affichage des ressources et de l'utilisation des ressources
- Certificate Management
- Managing Devices
- Event Viewer
- File Explorer
- Firewall Management
- Gestion des applications installées
- Configuration des utilisateurs et des groupes locaux
- Network Settings
- Affichage/fin des processus et création de vidages de processus
- Registry Editing
- Gestion des tâches planifiées
- Gestion des services Windows
- Activation/désactivation des rôles et fonctionnalités
- Gestion des machines virtuelles et des commutateurs virtuels Hyper-V
- Managing Storage
- Gestion du réplica de stockage
- Gestion des mises à jour Windows
- PowerShell console
- Connexion Bureau à distance

Windows Admin Center fournit également ces solutions :

- La gestion de l'ordinateur fournit un sous-ensemble des fonctionnalités du Gestionnaire de serveur pour la gestion des PC clients Windows 10 ou 11
- Le Gestionnaire de cluster de basculement prend en charge la gestion continue des clusters de basculement et des ressources de cluster
- Hyper-Converged Cluster Manager offre une toute nouvelle expérience adaptée aux espaces de stockage direct et Hyper-V. Il propose le tableau de bord et met l'accent sur les graphiques et les alertes pour la surveillance.

Windows Admin Center est complémentaire et ne remplace pas les outils d'administration de serveur distant, car les rôles tels que Active Directory, DHCP, DNS, IIS n'ont pas encore de fonctionnalités de gestion équivalentes dans Windows Admin Center.

# Windows Admin Center peut-il être utilisé pour gérer gratuitement Microsoft Hyper-V

## Server ?

Yes. Windows Admin Center peut être utilisé pour gérer Microsoft Hyper-V Server 2019 et Microsoft Hyper-V Server 2016.

## Puis-je déployer Windows Admin Center sur un ordinateur Windows ?

Oui, Windows Admin Center peut être installé sur Windows 10 (version 1709 ou ultérieure) et Windows 11. Windows Admin Center peut également être installé sur un serveur avec Windows Server 2016 ou version ultérieure en mode passerelle, puis accessible via un navigateur web à partir d'un ordinateur Windows 10. En savoir plus sur les options d'installation.

## J'ai entendu dire que Windows Admin Center utilise PowerShell sous le capot, puis-je voir les scripts réels qu'il utilise ?

Yes! Consultez les scripts PowerShell utilisés dans Windows Admin Center.

## Existe-t-il des plans pour Windows Admin Center pour gérer Windows Server 2008 R2 ou version antérieure ?

Windows Admin Center **ne prend plus en charge les fonctionnalités de** pour gérer Windows Server 2008 R2. Windows Admin Center s'appuie sur les fonctionnalités powerShell et les technologies de plateforme qui n'existent pas dans Windows Server 2008 R2 et versions antérieures, ce qui rend la prise en charge complète infeasible. Si vous ne l'avez pas encore fait, Microsoft recommande de passer à Azure ou de procéder à la mise à niveau vers la dernière version de Windows Server.

## Existe-t-il des plans pour Windows Admin Center pour gérer les connexions Linux ?

Nous étudions en raison de la demande du client, mais il n'existe actuellement aucun plan verrouillé à livrer, et la prise en charge peut se composer uniquement d'une connexion de console via SSH.

# Quels navigateurs web Windows Admin Center prend-il en charge ?

Les dernières versions de Microsoft Edge (Windows 10, version 1709 ou ultérieure), Google Chrome et Microsoft Edge Insider sont testés et pris en charge sur Windows 10 et versions ultérieures. Afficher les problèmes connus spécifiques du navigateur. D'autres navigateurs web modernes ou d'autres plateformes ne font actuellement pas partie de notre matrice de test et ne sont donc pas *officiellement* pris en charge.

# Comment Windows Admin Center gère-t-il la sécurité ?

Le trafic du navigateur vers la passerelle Windows Admin Center utilise HTTPS. Le trafic de la passerelle vers des serveurs managés est standard powerShell et WMI sur WinRM. Nous prenons en charge LAPS (solution de mot de passe d'administrateur local), la délégation contrainte basée sur les ressources, le contrôle d'accès de passerelle à l'aide d'Active Directory ou microsoft Entra ID et le contrôle d'accès en fonction du rôle pour la gestion des serveurs cibles.

# Windows Admin Center utilise-t-il CredSSP ?

Oui, dans certains cas, Windows Admin Center nécessite CredSSP. CredSSP est requis pour transmettre vos informations d'identification pour l'authentification aux ordinateurs au-delà du serveur spécifique que vous ciblez pour la gestion. Par exemple, si vous gérez des machines virtuelles sur **le serveur B**, mais que vous souhaitez stocker les fichiers vhdx pour ces machines virtuelles sur un partage de fichiers hébergé par **le serveur C**, Windows Admin Center doit utiliser CredSSP pour s'authentifier auprès du **serveur C** pour accéder au partage de fichiers.

Windows Admin Center gère automatiquement la configuration de CredSSP après avoir demandé votre consentement. Avant de configurer CredSSP, Windows Admin Center vérifie que le système dispose des dernières mises à jour CredSSP.

CredSSP est actuellement utilisé dans les domaines suivants :

- Utilisation du stockage SMB désagrégé dans l'outil machines virtuelles
- Utilisation de l'outil Mises à jour dans les solutions de gestion de cluster de basculement ou de Hyper-Converged, qui effectue Cluster-Aware mise à jour

# Existe-t-il des dépendances cloud ?

Windows Admin Center ne nécessite pas d'accès à Internet et ne nécessite pas Microsoft Azure. Windows Admin Center gère les instances Windows Server et Windows n'importe où : sur des systèmes physiques, ou dans des machines virtuelles sur n'importe quel hyperviseur ou s'exécutant dans n'importe quel cloud. Bien que Windows Admin Center s'intègre à différents services Azure, ces fonctionnalités sont facultatives et ne sont pas requises pour utiliser Windows Admin Center. Les connexions aux ressources azure **nécessitent** une connexion internet/réseau active et fonctionnelle, afin d'appliquer les modifications administratives et d'afficher les états.

# Existe-t-il d'autres dépendances ou conditions préalables ?

Windows Admin Center peut être installé sur windows 10 Fall Anniversary Update (1709) ou version ultérieure, ou Windows Server 2016 ou version ultérieure. Pour gérer Windows Server 2008 R2, 2012 ou 2012 R2, l'installation de Windows Management Framework 5.1 est requise sur ces serveurs. Il n'existe aucune autre dépendance. IIS, agents et SQL Server ne sont pas obligatoires.

# Qu'en est-il de l'extensibilité et de la prise en charge tierce ?

Windows Admin Center dispose d'un Kit de développement logiciel (SDK) pour permettre à tout le monde d'écrire sa propre extension. En tant que plateforme, la croissance de notre écosystème et l'activation de l'extensibilité des partenaires a été une priorité clé depuis le début. En savoir plus sur le sdk Windows Admin Center.

# Puis-je gérer l'infrastructure Hyper-Converged avec Windows Admin Center ?

Yes. Windows Admin Center prend en charge la gestion des clusters hyperconvergés exécutant Windows Server 2016 ou Windows Server 2019. La solution de gestionnaire de clusters

hyperconvergée dans Windows Admin Center était précédemment en préversion, mais elle est désormais **en disponibilité générale**, avec certaines nouvelles fonctionnalités en préversion. Pour plus d'informations, en savoir plus sur la gestion de l'infrastructure hyperconvergée.

# Windows Admin Center nécessite-t-il System Center ?

No. Windows Admin Center est complémentaire de System Center, mais System Center n'est pas requis. En savoir plus sur Windows Admin Center et System Center.

# Windows Admin Center peut-il remplacer System Center Virtual Machine Manager (SCVMM) ?

Windows Admin Center et SCVMM sont complémentaires ; Windows Admin Center est destiné à remplacer les composants logiciels enfichables MMC (Microsoft Management Console) traditionnels et l'expérience d'administration du serveur. Windows Admin Center n'est pas destiné à remplacer les aspects de surveillance de SCVMM. En savoir plus sur Windows Admin Center et System Center.

# Qu'est-ce que Windows Admin Center Preview, quelle version est adaptée à moi ?

Il existe deux versions de Windows Admin Center disponibles pour le téléchargement :

## Windows Admin Center (Centre d'administration Windows)

- Pour les administrateurs informatiques qui ne sont pas en mesure de mettre à jour fréquemment ou qui veulent plus de temps de validation pour les versions qu'ils utilisent en production, cette version est pour vous. Notre version en disponibilité générale actuelle est Windows Admin Center 1910.
- Les versions de Windows Admin Center (sans préversion) sont prises en charge en continu, en fonction des politique de cycle de vie moderne de Microsoft. Cela signifie que seule la dernière version de Windows Admin Center est gérée et prise en charge, et que les utilisateurs doivent rester à jour en effectuant une mise à niveau vers la dernière version de Windows Admin Center dans les 30 jours suivant la disponibilité pour rester pris en charge. Cette stratégie s'applique à la fois à la plateforme Windows Admin Center

elle-même, ainsi qu'aux extensions Microsoft publiées (sans préversion) publiées dans le flux d'extension Windows Admin Center. Notez que certaines extensions peuvent être mises à jour plus fréquemment que d'autres, entre les versions de Windows Admin Center. Pour plus d'informations sur les versions préliminaires de Windows Admin Center, consultez versions windows Insider Preview.

- Pour obtenir la dernière version, téléchargez ici.

### Aperçu de Windows Admin Center

- Pour les administrateurs informatiques qui veulent les fonctionnalités les plus récentes et les plus grandes sur une cadence régulière, cette version est pour vous. Notre intention est de fournir des mises à jour ultérieures tous les mois. La plateforme principale continue d'être prête pour la production et la licence fournit des droits d'utilisation de production. Ces builds introduisent de nouveaux outils et fonctionnalités clairement marqués comme PRÉVERSION et conviennent à l'évaluation et aux tests.
- Pour obtenir la dernière version Insider Preview, les Insiders inscrits peuvent télécharger Windows Admin Center Preview directement à partir de la page de téléchargement Windows Server Insider Preview, sous la liste déroulante Téléchargements supplémentaires. Si vous n'êtes pas inscrit en tant qu'Insider, consultez Prise en main de Windows Server sur le portail Windows Insiders for Business.

## Pourquoi « Windows Admin Center » a-t-il été choisi comme nom final pour « Project Honolulu » ?

Windows Admin Center est le nom officiel du produit « Project Honolulu » et renforce notre vision d'une expérience intégrée pour les administrateurs informatiques dans un large éventail de scénarios d'administration et de gestion de base. Il met également en évidence notre focus client sur les besoins de l'utilisateur administrateur informatique comme central pour la façon dont nous investissons et ce que nous fournissons.

## Où puis-je en savoir plus sur Windows Admin Center ou obtenir plus de détails ?

Notre page de lancement est le meilleur point de départ et contient des liens vers notre contenu de documentation nouvellement classé, l'emplacement de téléchargement, la façon de fournir des commentaires, des informations de référence et d'autres ressources.

# Qu’est-ce que l’historique des versions de Windows Admin Center ?

Afficher l’historique des versions ici.

# Je rencontre un problème avec Windows Admin Center, où puis-je obtenir de l’aide ?

Consultez notre guide de résolution des problèmes et notre liste de problèmes connus.

# Documentation de System Center

Documentation de System Center pour les versions 2016 et ultérieures. La documentation couvre la version LTSC de System Center.

## Configuration Manager

- Qu'est-ce que Configuration Manager
- Nouveautés
- Configurations prises en charge

En savoir plus >

## Data Protection Manager

- Qu'est-ce que Data Protection Manager ?
- Nouveautés
- Préparer le déploiement de serveurs DPM
- PowerShell

En savoir plus >

## Operations Manager

- Qu'est-ce qu'Operations Manager ?
- Nouveautés
- Planifier votre installation d'Operations Manager
- PowerShell
- REST API

En savoir plus >

## Un orchestrateur

- Qu'est-ce que Orchestrator ?
- Nouveautés
- Installer Orchestrator

En savoir plus >

## Service Manager

- Qu'est-ce que Service Manager ?
- Nouveautés
- Planifier Service Manager
- PowerShell

En savoir plus >

## Service Management Automation

- Qu'est-ce que Service Management Automation ?
- Nouveautés
- Déployer Service Management Automation
- PowerShell

En savoir plus >

## Virtual Machine Manager

## Service Provider Foundation

- Qu’est-ce que Virtual Machine Manager ?
- Nouveautés
- Planifier l’installation de Virtual Machine Manager
- PowerShell

En savoir plus >

- Qu’est-ce que Service Provider Foundation ?
- Nouveautés
- Planifier le déploiement de Service Provider Foundation
- PowerShell

En savoir plus >

# Ressources

## System Center

- Obtenir un essai gratuit
- Regarder System Center en action
- Gérer Windows 10 via la cogestion
- Blog
- Conversations

## UserVoice

- Operations Manager
- Virtual Machine Manager
- Data Protection Manager

# Gestionnaire de protection des données

> **Important**
>
> Service Provider Foundation (SPF) est supprimé de System Center 2025. Toutefois, SPF 2022 continuera de fonctionner avec les composants System Center 2025.

Chaque organisation a besoin d'une stratégie de continuité d'activité et de reprise d'activité (BCDR) pour garantir que les ressources sont disponibles pendant les pannes planifiées et non planifiées. Votre stratégie BCDR nécessite de sécuriser et de récupérer vos données et de maintenir en permanence vos charges de travail métier, applications et services disponibles en continu. System Center Data Protection Manager (DPM) est un système robuste de sauvegarde et de récupération d'entreprise qui contribue à votre stratégie BCDR en facilitant la sauvegarde et la récupération des données d'entreprise.

Pour obtenir des mises à jour sur les versions, les fonctionnalités et les améliorations de System Center, consultez le blog Tech Community.

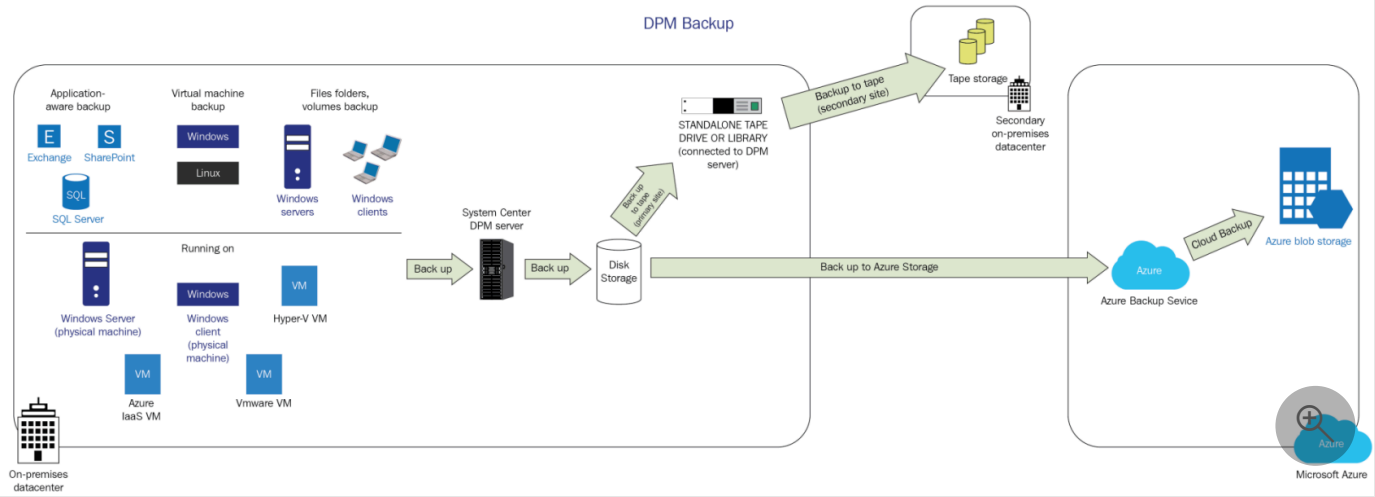
Vous pouvez déployer System Center DPM pour :

- **Sauvegarde tenant compte des applications** : sauvegarde des workloads Microsoft tenant compte des applications, notamment SQL Server, Exchange et SharePoint.
- **Sauvegarde** de fichiers : sauvegarde de fichiers, de dossiers et de volumes pour les ordinateurs exécutant des systèmes d'exploitation client Windows server et Windows.
- **Sauvegarde du système** : sauvegarder l'état du système ou exécuter des sauvegardes complètes d'ordinateurs physiques exécutant Windows Server ou des systèmes d'exploitation clients Windows.
- **Sauvegarde de** machine virtuelle : sauvegardez des machines virtuelles Hyper-V ou VMware exécutant Windows ou Linux. Vous pouvez sauvegarder une machine virtuelle entière ou exécuter des sauvegardes prenant en charge les applications des charges de travail Microsoft sur des machines virtuelles Hyper-V/VMware exécutant Windows.
- Obtenez une liste complète de ce que DPM peut sauvegarder ?

DPM peut stocker des données de sauvegarde dans :

- **Disque** : pour le stockage à court terme, DPM sauvegarde les données dans les pools de disques.
- **Azure** : Pour le stockage à court et à long terme, les données DPM stockées dans des pools de disques peuvent être sauvegardées dans le cloud Microsoft Azure à l'aide du service Sauvegarde Azure.
- **Bande** : pour le stockage à long terme, vous pouvez sauvegarder des données sur bande, qui peuvent ensuite être stockées hors site.

Lorsque des pannes se produisent et que les données sources ne sont pas disponibles, vous pouvez utiliser DPM pour restaurer facilement des données vers la source d'origine ou vers un autre emplacement. De cette façon, si les données d'origine ne sont pas disponibles en raison de problèmes planifiés ou inattendus, vous pouvez facilement restaurer des données à partir d'un autre emplacement. DPM utilise SQL Server comme base de données et vous protégez le serveur DPM lui-même à des fins de récupération d'urgence. Le diagramme suivant fournit une vue d'ensemble de la fonctionnalité de sauvegarde DPM.




# Étapes suivantes

En savoir plus sur le fonctionnement de DPM ?

---

Dernière mise à jour : 01/09/2025

# Responsable des opérations

> **Important**
>
> Service Provider Foundation (SPF) est supprimé de System Center 2025. Toutefois, SPF 2022 continuera de fonctionner avec les composants System Center 2025.

Bienvenue dans System Center - Operations Manager. Operations Manager fournit une surveillance de l'infrastructure flexible et rentable, permet de garantir les performances prévisibles et la disponibilité des applications vitales, et offre une surveillance complète pour votre centre de données et votre cloud, tant privé que public.

## Documentation du gestionnaire des opérations

- Prise en main de System Center - Operations Manager

  Écrit pour les clients qui sont nouveaux dans Operations Manager ou qui recherchent des informations « Nouveautés ».

- Planification pour System Center - Operations Manager

  Passez en revue les informations pour vous aider à planifier le déploiement d'Operations Manager dans votre organisation.

- Déploiement de System Center - Operations Manager

  Lisez ces articles pour découvrir comment déployer Operations Manager dans votre environnement.

- System Center - Guide des opérations de Operations Manager

  Lisez ces articles une fois que vous avez Operations Manager opérationnel et que vous souhaitez commencer à surveiller votre environnement et procédures pour les opérations quotidiennes.

- Guide de création du pack d'administration pour Operations Manager

  Le Guide de création du pack d'administration pour Operations Manager fournit des informations sur la création d'une supervision personnalisée pour votre service ou votre

application.

- System Center - Résolution des problèmes d'Operations Manager

  Lisez ces articles pour découvrir comment résoudre les problèmes d'Operations Manager dans votre environnement.

Pour obtenir des mises à jour sur les versions, les fonctionnalités et les améliorations de System Center, consultez le blog Tech Community.

---

Dernière mise à jour : 01/09/2025

# Qu’est-ce que Virtual Machine Manager ?

Bienvenue dans System Center Virtual Machine Manager (VMM) ! VMM fait partie de la suite System Center utilisée pour configurer, gérer et transformer des centres de données traditionnels. Il permet de fournir une expérience de gestion unifiée entre les services locaux, le fournisseur de services et le cloud Azure.

Les fonctionnalités VMM sont les suivantes :

- **Centre de données** : configurez et gérez vos composants de centre de données en tant qu’infrastructure unique dans VMM. Les composants du centre de données incluent les serveurs de virtualisation, les composants réseau et les ressources de stockage. VMM provisionne et gère les ressources nécessaires pour créer et déployer des machines virtuelles et des services sur des clouds privés.

- **Hôtes** de virtualisation : VMM peut ajouter, approvisionner et gérer des hôtes et des clusters de virtualisation Hyper-V et VMware.

- **Mise** en réseau : ajoutez des ressources réseau à l’infrastructure VMM, y compris les sites réseau définis par les sous-réseaux IP, les réseaux locaux virtuels (VLAN), les commutateurs logiques, l’adresse IP statique et les pools MAC. VMM fournit la virtualisation du réseau, notamment la prise en charge de la création et de la gestion de réseaux virtuels et de passerelles réseau. La virtualisation du réseau permet à plusieurs locataires d’avoir des réseaux isolés et leurs propres plages d’adresses IP pour renforcer la confidentialité et la sécurité. À l’aide de passerelles, les machines virtuelles sur les réseaux virtuels peuvent se connecter à des réseaux physiques sur le même site ou à différents emplacements.

- **Stockage** : VMM peut découvrir, classifier, provisionner, allouer et affecter un stockage local et distant. VMM prend en charge le stockage en bloc (réseaux SAN pour le canal à fibre, iSCSI et SAS).

- **Ressources** de bibliothèque : L’infrastructure VMM conserve une bibliothèque de ressources basées sur des fichiers et non basées sur des fichiers utilisées pour créer et déployer des machines virtuelles et des services sur des hôtes de virtualisation. Les ressources basées sur des fichiers incluent des disques durs virtuels, des images ISO et des scripts. Les ressources non basées sur des fichiers incluent des modèles et des profils utilisés pour normaliser la création de machines virtuelles. Les ressources de bibliothèque sont accessibles via des partages de bibliothèque.

- **Gestion** Azure : intégrez SCVMM avec Azure Arc pour gérer vos machines virtuelles en mode libre-service à l'aide du contrôle d'accès en fonction du rôle Azure. SCVMM compatible avec Azure Arc permet de construire des pipelines d'automatisation et en libre-service à l'aide de Kits de développement logiciel (SDK) Python, Java, JavaScript, Go et .NET ; Modèles Terraform, ARM et Bicep ; API REST Azure, CLI et PowerShell. SCVMM avec Azure Arc vous permet également d'accéder aux services de gestion Azure tels que Microsoft Defender pour le cloud, Azure Monitor, Azure Update Manager et Azure Policy, ce qui vous permet de sécuriser, de régir et de gérer vos machines virtuelles SCVMM à partir du cloud.

## Ressources

- Pour lire des billets de blog de l'équipe d'ingénierie VMM, consultez le blog System Center.

## Étapes suivantes

- En savoir plus sur la configuration système requise.
- Bien démarrer avec SCVMM activé pour Arc.

---

Dernière mise à jour : 01/09/2025

# Vue d’ensemble de System Center - Orchestrator

> **Important**
>
> Service Provider Foundation (SPF) est supprimé de System Center 2025. Toutefois, SPF 2022 continuera de fonctionner avec les composants System Center 2025.

En tant qu’administrateur informatique, vous effectuez probablement de nombreuses tâches et procédures pour maintenir votre environnement informatique sain. Vous pouvez avoir des tâches individuelles automatisées, mais en général, pas l’ensemble du processus. Avec System Center - Orchestrator, vous associez des tâches et procédures disparates à l’aide d’un Runbook Designer d’interface utilisateur graphique pour créer des solutions de bout en bout fiables, flexibles et efficaces dans votre environnement informatique. À l’aide d’Orchestrator, vous pouvez :

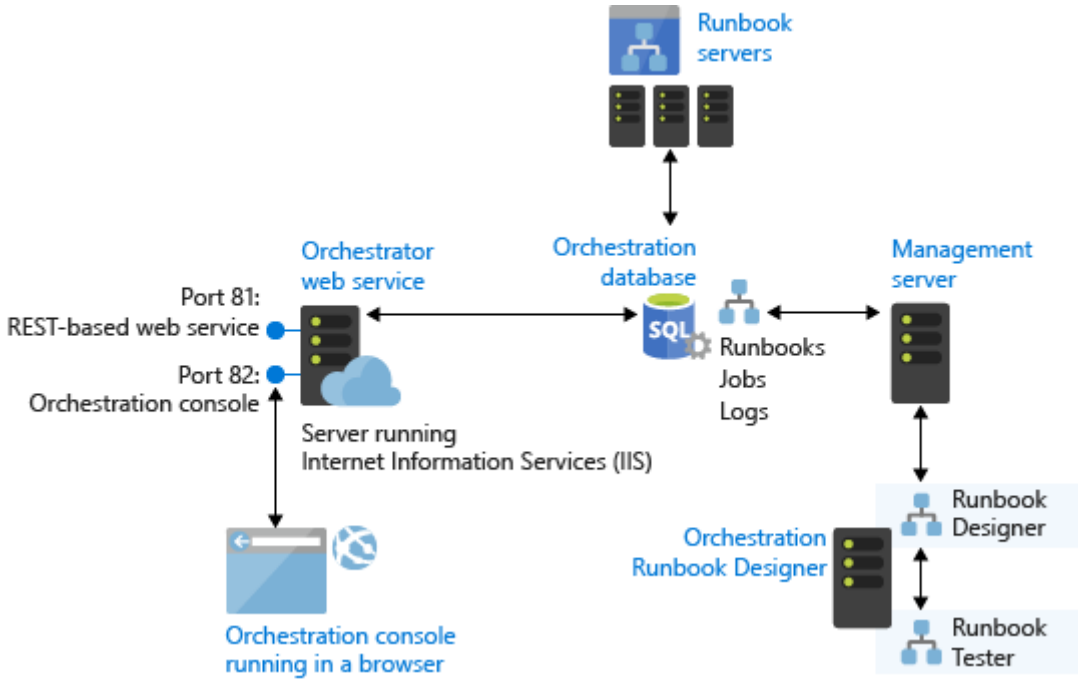
- Automatiser les traitements dans votre centre de données, quel que soit le matériel ou la plate-forme.
- Normaliser les meilleures pratiques pour améliorer l’efficacité opérationnelle.
- Connectez des systèmes de différents fournisseurs sans avoir à savoir comment utiliser des scripts et des langages de programmation.

Pour en savoir plus sur les prérequis, consultez Configuration système requise pour System Center Orchestrator.

Pour obtenir des mises à jour sur les versions, les fonctionnalités et les améliorations de System Center, consultez le blog Tech Community.

## Architecture de l'orchestrateur

Le diagramme suivant illustre chacune des fonctionnalités d’Orchestrator et la communication entre chacune d’elles.

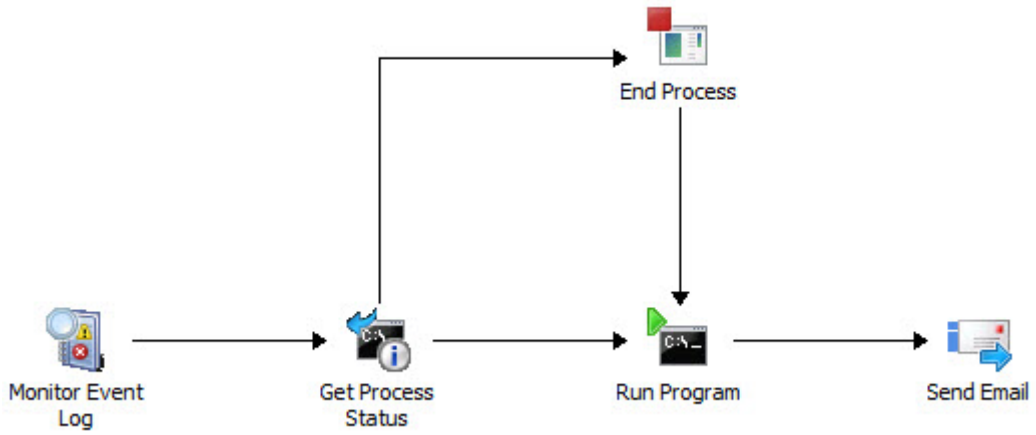



La base de données d'orchestration est au cœur de l'installation d'Orchestrator et contient tous les runbooks, paramètres de configuration et journaux. Le serveur management est requis comme couche de communication entre Runbook Designer et la base de données Orchestration. Un ou plusieurs serveurs Runbook communiquent directement avec la base de données pour récupérer les Runbook à exécuter et pour stocker des informations concernant les tâches créées à partir des Runbook. Le service Web communique également directement avec la base de données Orchestration et fournit une connexion au navigateur Web pour la console Orchestration.

## Automatisation à l'aide des runbooks

Pour automatiser une tâche ou un processus dans Orchestrator, vous utilisez Runbook Designer pour créer un runbook. Vous ajoutez des activités au Runbook en les faisant glisser depuis le volet **Activités** , puis en reliant les activités dans l'ordre de votre choix pour créer un flux de travail.

L'illustration suivante présente un Runbook simple.




Ce Runbook surveille un journal des événements. Lorsqu'il détecte l'événement spécifié, le Runbook vérifie l'état d'un traitement particulier dans Windows sur un ordinateur spécifique. Si le processus est en cours d'exécution, il est arrêté. Le Runbook démarre ensuite le traitement et envoie un courrier électronique pour avertir de la modification de l'état du processus.

Chaque activité de runbook se termine avant de passer à la suivante, et il existe des activités qui fournissent une logique complexe, par exemple, en exigeant que plusieurs activités soient terminées avant que le runbook poursuive. En utilisant une combinaison de logique sur les activités et des liaisons intelligentes, vous pouvez implémenter la logique dont a besoin votre scénario d'automatisation particulier.

## Façon dont Orchestrator traite un Runbook

Après avoir créé un runbook, vous le validez dans la base de données Orchestration en l'archivant. Vous pouvez ensuite utiliser Runbook Designer ou la console Orchestration pour démarrer et arrêter le runbook.

Une demande d'exécution d'un Runbook crée une *tâche* qui est stockée dans la base de données Orchestration. Chaque Runbook peut définir un serveur Runbook principal et un ou plusieurs serveurs secondaires qui traitent le Runbook si le serveur principal n'est pas disponible. Un service sur chaque serveur Runbook surveille en permanence la base de données d'orchestration pour les tâches qu'il peut traiter. Lorsqu'un serveur runbook détecte un travail, il journalise qu'il travaille sur le travail, copie le runbook localement, journalise qu'il exécute une instance du runbook, puis commence à traiter le runbook. Pour tout runbook ne contenant pas de moniteur, vous pouvez créer plusieurs requêtes de runbooks, ce qui signifie qu'un runbook unique peut avoir plusieurs tâches.

Lorsqu'un serveur Runbook traite une tâche, il crée une *instance* du Runbook en faisant une copie locale, puis en effectuant les actions définies dans le Runbook selon la logique de flux de travail incluse. Les informations d'état, les résultats de l'activité et les données sont enregistrées dans la base de données Orchestration afin que vous puissiez surveiller l'état en temps réel et historique du Runbook.

# Étendre Orchestration

Le tableau suivant présente plusieurs stratégies disponibles pour étendre les fonctionnalités fournies par une installation standard d'Orchestrator.

Agrandir le tableau

| La fonctionnalité d'Orchestrator | Descriptif |
|---|---|
| Pack d'intégration | Un pack d'intégration est un ensemble d'activités personnalisées spécifiques d'un produit ou d'une technologie. Microsoft et d'autres sociétés fournissent des packs d'intégration avec des activités pour interagir avec leur produit à partir d'un runbook Orchestration. |
| Trousse à outils d'intégration de l'orchestrateur | Orchestrator Integration Toolkit vous permet d'étendre votre bibliothèque d'activités au-delà de la collection d'activités et de packs d'intégration standard. Integration Toolkit possède des outils dotés d'Assistant pour la création d'activités et de packs d'intégration pour Orchestration. Les développeurs peuvent également utiliser integration Toolkit pour créer des packs d'intégration à partir d'activités personnalisées qu'ils créent à l'aide du Kit de développement logiciel (SDK) Orchestrator. |

# Étapes suivantes

Comment installer Orchestration.

---

Dernière mise à jour : 01/09/2025

# Vue d’ensemble de Service Management Automation

> **Important**
>
> Service Provider Foundation (SPF) est supprimé de System Center 2025. Toutefois, SPF 2022 continuera de fonctionner avec les composants System Center 2025.

Service Management Automation (SMA) est un ensemble d’outils intégrés en tant qu’extension SMA dans Windows Azure Pack pour Windows Server. Les professionnels de l’informatique et les développeurs informatiques peuvent utiliser SMA pour construire, exécuter et gérer des runbooks pour intégrer, orchestrer et automatiser les processus métier informatiques. Les runbooks SMA s’exécutent sur le moteur Windows PowerShell.

> **Remarque**
>
> Comme Windows Azure Pack est désormais déconseillé, vous pouvez utiliser le module complémentaire PowerShell ISE comme alternative. Pour plus d’informations, consultez présentation du module complémentaire ISE Service Management Automation.

Pour obtenir des mises à jour sur les versions, les fonctionnalités et les améliorations de System Center, consultez le blog Tech Community.

## Composants SMA

SMA utilise les trois composants sous-jacents suivants qui sont connectés à Windows Azure Pack via le point de terminaison de service SMA :

### Service Web

- Se connecte à Windows Azure Pack
- Distribue les tâches de Runbook aux Runbook Worker
- Prend en charge HTTPS
- Permet au groupe de sécurité de contrôler l'accès

### Runbook Worker

- Exécute des tâches de Runbook
- S'exécute sous un compte de service

### Module PowerShell

- Active la gestion SMA à l'aide des applets de commande Windows PowerShell

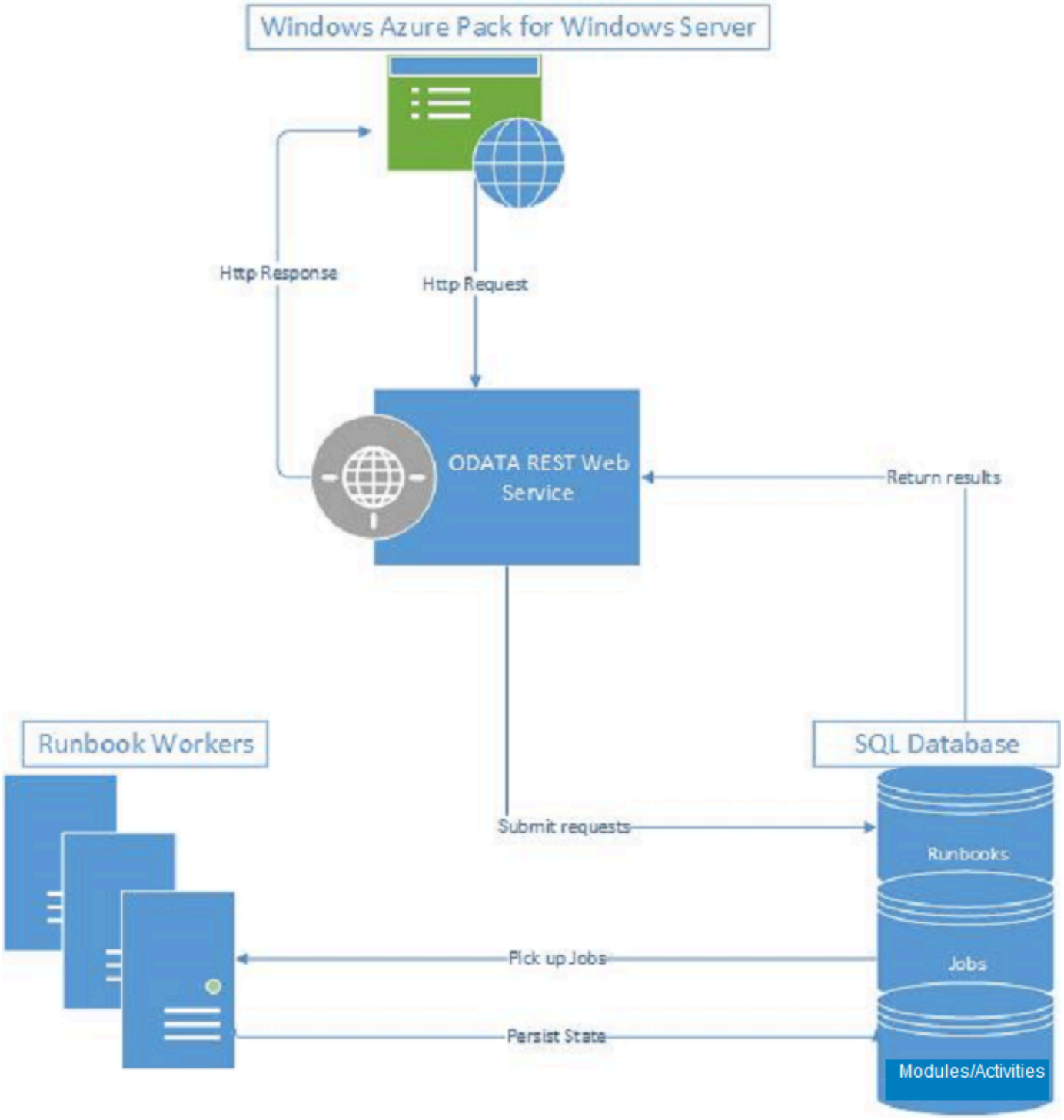
## Dois-je utiliser SMA ou System Center - Orchestrator ?

Le composant System Center - Orchestrator vous permet d'automatiser les processus métier et les opérations informatiques dans votre centre de données sans script ni programmation. Si vous préférez une approche de création graphique, utilisez Orchestrator.

SMA vous permet d'automatiser les processus métier et les opérations informatiques via PowerShell. Avec la prise en charge des dernières fonctionnalités PowerShell, vous pouvez utiliser SMA pour automatiser la gestion de tous les logiciels qui fournissent des applets de commande PowerShell, y compris d'autres composants System Center (même Orchestrator). Si vous souhaitez automatiser via PowerShell, utilisez Service Management Automation pour gérer toutes vos automatisations à partir d'un emplacement unique.

SMA a également une intégration approfondie avec Windows Azure Pack ; Toutefois, vous n'avez plus besoin d'utiliser le portail Windows Azure Pack pour créer des runbooks SMA. La création peut être effectuée dans PowerShell ISE via le module complémentaire PowerShell ISE. SMA prend désormais également en charge les runbooks de type de script PowerShell natifs. Vous pouvez en savoir plus sur les nouvelles fonctionnalités de SMA ici

Le diagramme suivant illustre chacune des fonctionnalités SMA et la communication avec une installation de Windows Azure Pack.




- Le service web SMA communique avec Windows Azure Pack et authentifie les utilisateurs.
- Les bases de données SQL Server stockent et récupèrent des Runbook, des ressources de Runbook, des activités, des modules d'intégration et des informations sur les tâches de Runbook.
- Les Runbook Worker exécutent les Runbook et ils peuvent être utilisés pour l'équilibrage de charge.
- Le portail de gestion dans Windows Azure Pack est l'endroit où vous créez, déboguez et démarrez et arrêtez des runbooks.

> **Important**
>
> Le **Guide** du développeur SMA est désormais disponible. Ce guide est un ensemble de documentation de référence sur l'API REST pour le service web SMA.

## Étapes suivantes

- Découvrez comment SMA exécute des runbooks.

---

Dernière mise à jour : 05/09/2025

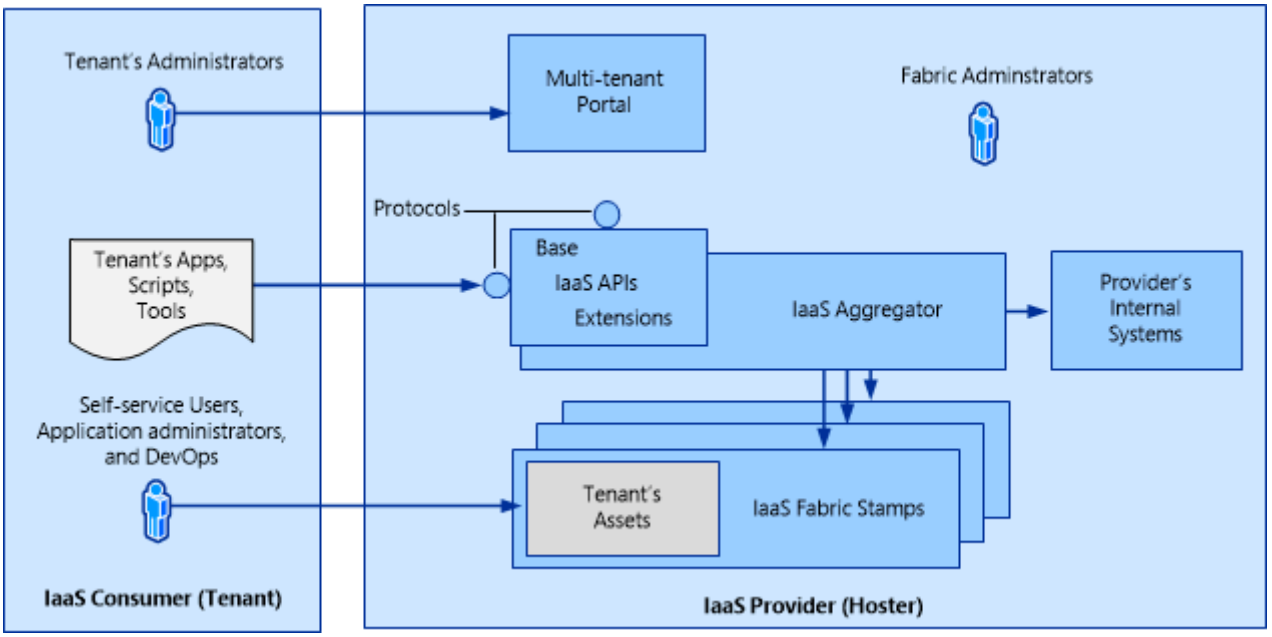
# Qu’est-ce que Service Provider Foundation ?

System Center - Virtual Machine Manager (VMM) fournit toutes les ressources nécessaires pour générer, gérer et surveiller une infrastructure cloud. Toutefois, les fournisseurs de services et les grandes entreprises ont besoin de fonctionnalités supplémentaires pour prendre en charge plusieurs locataires, intégrer des infrastructures à des portails en libre-service basés sur le web sophistiqués et distribuer des charges de travail de gestion sur plusieurs centres de données.

System Center - Service Provider Foundation (SPF), groupé avec System Center Orchestrator, fournit cette fonctionnalité avec une API Open Data Protocol extensible sur un service web REST (Representational State Transfer) qui interagit avec VMM.

SPF peut être utilisé par les fournisseurs de services pour offrir une infrastructure en tant que service (IaaS) à leurs clients. Si un fournisseur de services dispose d’un portail frontal pour les clients, les clients peuvent effectuer des demandes aux ressources du fournisseur d’hébergement sans quitter le portail. Les ressources cloud fournies par VMM peuvent être gérées à l’aide d’interfaces de gestion standard à partir d’appareils pris en charge n’importe où.

Le graphique suivant montre comment fonctionne SPF.




## Services SPF

SPF fournit de nombreux services :

- **Service web d'administration** : fournit des serveurs, des locataires et des balises pour Service Provider Foundation
- **Service** VMM : fournit l'accès aux fonctionnalités VMM
- **Service fournisseur** : utilisé par Windows Azure Pack

## Service web d'administration

- Les fournisseurs de services d'hébergement utilisent le service web d'administration pour créer et gérer les locataires, les rôles d'utilisateur, les serveurs, les marqueurs et d'autres objets d'administration.
- Vous pouvez accéder au service web Administrateur à l'aide de l'URL **https://server:8090/SC2012R2/Admin/Microsoft.Management.Odata.svc**

  > ⓘ **Remarque**
  >
  > L'URL ci-dessus s'applique à SPF 2016 et versions ultérieures.

- Les informations d'identification suivantes sont requises :

Agrandir le tableau

| Informations d'identification | Prérequis |
|---|---|
| Identité du pool d'applications Admin dans IIS | Doit être membre des groupes d'administration et du groupe SPF_Admin |
| Groupe d'administration dans Gestion des ordinateurs | Doit inclure les informations d'identification de l'identité du pool d'applications Admin |
| Groupe SPF_Admin dans Gestion de l'ordinateur | Doit inclure un utilisateur local qui est aussi membre du groupe Administrateurs, ainsi que les informations d'identification de l'identité du pool d'applications Administrateurs |

## Service web VMM

Le service web VMM appelle VMM pour effectuer des opérations demandées, telles que la création de machines virtuelles, de réseaux virtuels, de définitions de rôles utilisateur et d'autres structures pour le cloud. Ce service coordonne les changements parmi les participants et fournit les fonctionnalités dynamiques suivantes :

- Les applications portail et d'autres clients détectent les modifications apportées par SPF et VMM.

- VMM montre les modifications apportées aux applications du portail, à d'autres clients et à Service Provider Foundation.
- Service Provider Foundation reflète toutes les modifications apportées par les participants.

Vous pouvez utiliser l'applet `T:Microsoft.SystemCenter.Foundation.Cmdlet.New-SCSPFServer` de commande PowerShell pour inscrire une instance VMM. Vous pouvez accéder au service web VMM avec l'URL **https://server:8090/SC2012R2/VMM/Microsoft.Management.Odata.svc**.

> ⓘ **Remarque**
>
> L'URL ci-dessus s'applique à SPF 2016 et versions ultérieures.

Agrandir le tableau

| Informations d'identification | Prérequis |
|---|---|
| Identité du pool d'applications VMM dans IIS | Doit être membre des groupes d'administration et du groupe SPF_VMM |
| Groupe d'administration dans Gestion des ordinateurs | Doit inclure les informations d'identification de l'identité du pool d'applications VMM |
| Groupe SPF_VMM dans Gestion de l'ordinateur | Doit inclure un utilisateur local, membre du groupe d'administration, ainsi que les informations d'identification pour l'identité du pool d'applications VMM. |
| Rôle d'utilisateur administrateur dans VMM | Doit inclure les informations d'identification de l'identité du pool d'applications VMM en tant que membre du rôle d'utilisateur Administrateur |

## Service web d'utilisation

- Le service web Utilisation est utilisé uniquement par Windows Azure Pack et les fournisseurs de facturation tiers. Le point de terminaison du service web Utilisation ne doit pas être accessible à d'autres fins pour empêcher la perte de données en raison de requêtes inutiles ou erronées.
- Le service Web d'utilisation utilise des inscriptions d'instances des entrepôts de données Operations Manager (hébergées par VMM) pour recueillir des métriques sur l'utilisation des machines virtuelles par les locataires et d'autres données d'utilisation de l'infrastructure. Des données d'utilisation sont recueillies pour des processus tels que la facturation des fonctionnalités de rétrofacturation.

- Vous pouvez utiliser des applets de commande Windows PowerShell pour inscrire les paramètres de connexion de l'entrepôt de données Operations Manager dans la base de données SPF. Cette inscription permet à SPF d'agréger les données d'utilisation à partir des entrepôts de données.
- Le service web d'utilisation retourne des données d'utilisation en rapport avec chaque abonnement parmi les services.

Agrandir le tableau

| Informations d'identification | Prérequis |
|---|---|
| Identité du pool d'applications d'utilisation dans IIS | Doit être membre des groupes d'administration et du groupe SPF_Usage. |
| Groupe d'administration dans Gestion des ordinateurs | Doit inclure les informations d'identification de l'identité du pool d'applications Usage. |
| Groupe SPF_Usage dans Gestion de l'ordinateur | Doit inclure un utilisateur local qui est aussi membre du groupe Administrateurs, ainsi que les informations d'identification de l'identité du pool d'applications d'Utilisation. |
| Utilisateur de base de données dbo dans la base de données SQL Server OperationsManagerDW (sur le serveur Operations Manager) | Les informations d'identification de l'utilisateur qui a installé Operations Manager sont automatiquement utilisées pour se connecter à l'objet de sécurité dbo SQL Server. Les mêmes informations d'identification doivent être utilisées pour toutes les identités du pool d'applications SPF. |

Propriétés de base de données de la base de données OperationsManagerDW SQL Server (cliquez avec le bouton droit) sur le serveur Operations Manager.

## Service web du fournisseur

Pour fournir l'infrastructure en tant que service (IaaS), les fournisseurs de ressources utilisent le service web du fournisseur. Le service web du fournisseur fournit une API web Microsoft ASP.NET. Il ne s'agit pas d'un service Open Data (OData). Le service web du fournisseur utilise également les services web VMM et d'administration.

Agrandir le tableau

| Informations d'identification | Prérequis |
|---|---|
| Identité du pool d'applications de fournisseur dans IIS | Doit être membre des groupes d'administration et des groupes SPF_Provider, SPF_VMM et SPF_Admin |

| Informations d’identification | Prérequis |
|---|---|
| Groupe d’administration dans Gestion des ordinateurs | Doit inclure les informations d'identification de l'identité du pool d'applications de fournisseur |
| Groupe SPF_Provider dans Gestion de l'ordinateur | Doit inclure un utilisateur local membre du groupe des administrateurs et les informations d’identification de l’identité du pool d'applications du fournisseur. |

## Service web d'automatisation de la gestion des services.

Vous pouvez configurer des événements dans SPF que le service web Service Management Automation utilisera. Pour ce faire, le service web doit avoir des informations d’identification pour accéder aux services web SPF. Vous pouvez également utiliser PowerShell pour automatiser les runbooks.

Agrandir le tableau

| Informations d’identification | Prérequis |
|---|---|
| Une ou plusieurs identités de pool d’applications SPF, comme requis pour l’automatisation | Doit être membre du groupe d’administration sur le serveur avec Service Management Automation installé |

# Interaction avec SPF

Les hôtes et les locataires interagissent avec SPF comme suit :

- Les fournisseurs d’hébergement utilisent le service d’administration pour allouer la bande passante réseau, l’espace disque et les serveurs, qui représentent ensemble le cloud privé aux locataires.
- Les locataires représentent un client disposant d'une ressource sur le système de l'hébergeur. Les locataires consomment et gèrent les services proposés par le fournisseur d’hébergement. Chaque client a ses propres administrateurs, applications, scripts et autres outils.
- Un fournisseur d’hébergement gère les ressources disponibles par chaque locataire. L’hôte dispose d’un portail frontal existant, que tous les locataires peuvent utiliser.
- Les services de locataire sont approvisionnés pour les utilisateurs en libre-service par les administrateurs clients sous la forme de réseaux de machines virtuelles, de machines virtuelles, de matériel virtuel et d’infrastructure cloud.
- L’hébergeur alloue des ressources d’infrastructure dans un tampon. Les ressources des locataires peuvent être allouées aux tampons de la manière la plus appropriée pour

l’hébergeur. Les ressources peuvent être divisées sur plusieurs tampons (collection définie de ressources).

- SPF permet à l’hôte de présenter une expérience utilisateur transparente au locataire en agrégeant les données de chaque tampon et en permettant au locataire d’utiliser les API SPF pour accéder à ces données.
- À mesure que la demande du client augmente, l'hébergeur fournit des tampons supplémentaires pour répondre à cette demande.
- Chaque instance de VMM avec laquelle SPF interagit est appelée tampon de gestion. SPF peut interagir avec un maximum de cinq tampons.
    - Un environnement est une instance System Center qui prend en charge une infrastructure de plateforme virtualisée composée du serveur Virtual Machine Manager (VMM), des hôtes, des machines virtuelles et des paramètres de configuration tels que les comptes de service et les rôles d'utilisateur. Les tampons fournissent une limite logique. Par exemple, vous pouvez avoir un tampon distinct pour chaque site géré par un serveur VMM.
    - Les tampons doivent être surveillés et inclure une instance de System Center Operations Manager. Une instance Operations Manager peut fournir une surveillance pour plusieurs tampons.
- Les administrateurs de locataires peuvent interagir avec l’infrastructure VMM en configurant des clouds, des modèles, des rôles d’utilisateur et des utilisateurs en libre-service, entre autres. Un administrateur client dispose également de fonctionnalités utilisateur en libre-service.
- Les utilisateurs en libre-service reçoivent un sous-ensemble de ressources locataire pour pouvoir travailler. L’utilisation des ressources est contrôlée par quota. Par exemple, lorsque les utilisateurs déploient des machines virtuelles ou utilisent d’autres ressources, ils entraînent des points de quota jusqu’au nombre de points de quota disponibles alloués. Les utilisateurs en libre-service peuvent interagir avec les services, les modèles et les disques durs virtuels pour déployer et gérer des machines virtuelles.

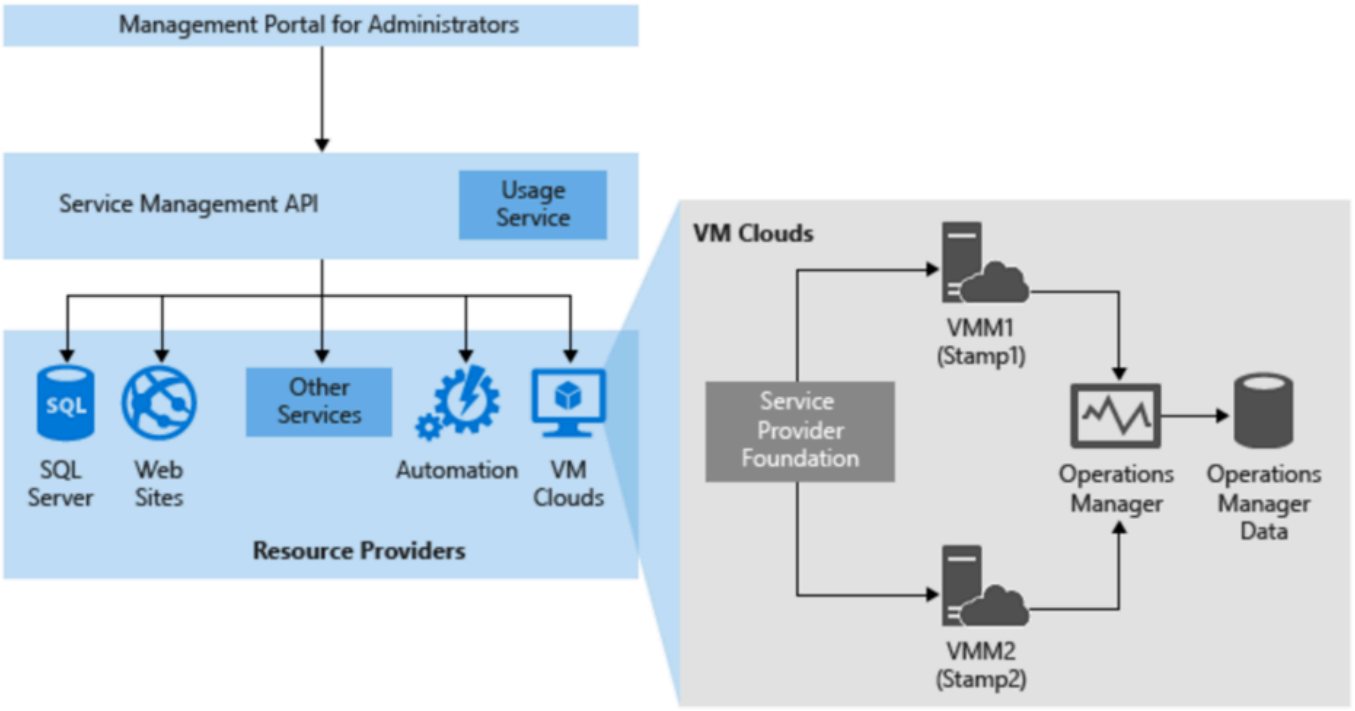
Ce graphique montre comment SPF interagit avec VMM




# VMM, SPF et Windows Azure Pack

Windows Azure Pack offre une expérience et un front-end de type Azure pour les clouds organisationnels. Azure Pack fournit un certain nombre de composants, et entre eux, le service cloud de machine virtuelle. Le service cloud de machine virtuelle s'intègre à VMM pour fournir les éléments suivants :

- Portail de gestion permettant à l'administrateur d'activer l'hébergement ou le service fourni pour configurer une infrastructure d'approvisionnement de machines virtuelles
- Portail de locataire dans lequel les locataires peuvent s'inscrire au service Clouds de machines virtuelles et approvisionner des machines virtuelles. Windows Azure Pack utilise SPF pour s'intégrer à VMM pour fournir le service Clouds de machine virtuelle, comme illustré dans le graphique suivant.




# Étapes suivantes

- Planifier le déploiement SPF

---

Dernière mise à jour : 20/08/2025

# En quoi consiste l'option d'installation minimale dans Windows Server ?

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

L'option Server Core est une option d'installation minimale disponible lorsque vous déployez l'édition Standard ou Datacenter de Windows Server. Server Core inclut la plupart des rôles de serveur, mais pas tous. Server Core a un encombrement de disque plus faible, et donc une surface d'attaque plus petite, car sa base de code est plus petite.

## Choix entre Server (Core) et Serveur avec Expérience utilisateur

Lorsque vous installez Windows Server, vous installez uniquement les rôles serveur que vous choisissez. Seul l'installation des rôles dont vous avez besoin permet de réduire l'encombrement global pour Windows Server. Toutefois, l'option d'installation du serveur avec expérience utilisateur installe toujours de nombreux services et autres composants dont vous n'avez souvent pas besoin pour un scénario d'utilisation particulier.

L'installation server Core élimine tous les services et autres fonctionnalités qui ne sont pas essentiels pour la prise en charge de certains rôles serveur couramment utilisés. Par exemple, un serveur Hyper-V n'a pas besoin d'une interface utilisateur graphique, car vous pouvez gérer pratiquement tous les aspects d'Hyper-V à partir de la ligne de commande à l'aide de Windows PowerShell ou à distance à l'aide du Gestionnaire Hyper-V.

## La différence de Server Core : fonctionnalités principales sans les fioritures

Quand vous avez terminé d'installer Server Core sur un système et que vous vous connectez pour la première fois, vous êtes surpris. La principale différence entre l'option d'installation du serveur avec expérience utilisateur et Server Core est que Server Core n'inclut pas les packages d'interpréteur de commandes d'interface utilisateur suivants :

- `Microsoft-Windows-Server-Shell-Package`
- `Microsoft-Windows-Server-Gui-Mgmt-Package`
- `Microsoft-Windows-Server-Gui-RSAT-Package`
- `Microsoft-Windows-Cortana-PAL-Desktop-Package`

En d'autres termes, il **n'existe aucun bureau** dans Server Core, par conception. Tout en conservant les fonctionnalités requises pour prendre en charge les applications métier traditionnelles et les charges de travail basées sur des rôles, Server Core n'a pas d'interface de bureau traditionnelle. Au lieu de cela, vous gérez Server Core à distance via la ligne de commande, PowerShell, un outil gui tel que RSAT ou Windows Admin Center.

En plus de l'absence d'interface utilisateur, Server Core diffère également de Serveur avec expérience de bureau des manières suivantes :

- Server Core n'a pas d'outils d'accessibilité
- Pas d'OOBE (expérience prête à l'emploi) pour la configuration de Server Core
- Aucune prise en charge audio
- Les services de notification Push Windows (WpnService et WpnUserService) ne sont pas installés. Les notifications Push pour les applications de plateforme Windows universelle (UWP) et les fonctionnalités MPNS (Microsoft Push Notification Service) ne sont pas prises en charge sur Server Core, car elles s'appuient sur les composants Expérience utilisateur (interpréteur de commandes GUI et runtime UWP).

Le tableau suivant indique les applications disponibles *localement* sur Server Core et Server avec expérience de bureau. **Important** : Dans la plupart des cas, vous pouvez exécuter des applications répertoriées comme « non disponibles » à distance à partir d'un ordinateur client Windows ou de Windows Admin Center pour gérer votre installation Server Core.

## Emplacements de téléchargement des fonctionnalités à la demande pour Server Core

Vous pouvez obtenir des packages Windows Server Feature on Demand (FoD) ultérieurs à partir de votre Centre de gestion des licences MS spécifique si vous avez actif Software Assurance. Vous avez besoin d'un compte Professionnel ou Scolaire Microsoft inscrit à VLSC ou Business Center pour accéder au téléchargement FoD.

Vous pouvez également avoir accès à Visual Studio Subscription. Vous avez besoin d'un compte Microsoft Famille, Professionnel ou Scolaire, inscrit à un abonnement Visual Studio actif, pour accéder au téléchargement FoD.

Vous pouvez télécharger la dernière version du serveur Insider FoD sur la page web Server Insider. Vous avez besoin d'un compte Microsoft Home, Work ou School, inscrit au programme Insider, pour accéder au téléchargement FoD.

## Fonctionnalité à la demande - fonctionnalités disponibles

La liste affiche les fonctionnalités disponibles à l'aide des fonctionnalités à la demande.

> **Notes**
>
> Cette liste est destinée à des informations de référence rapides. Il ne s'agit pas d'une liste complète.

Agrandir le tableau

| Application | Server Core | Server avec Expérience utilisateur |
|---|---|---|
| Invite de commandes | available | available |
| Windows PowerShell/ Microsoft .NET | available | available |
| Perfmon.exe | non disponible | available |
| Windbg (interface graphique) | supported | supported |
| Resmon.exe | non disponible | available |
| Regedit | available | available |
| Fsutil.exe | available | available |
| Disksnapshot.exe | non disponible | available |
| Diskpart.exe | available | available |
| Diskmgmt.msc | non disponible | available |
| Devmgmt.msc | non disponible | available |
| Gestionnaire de serveur | non disponible | available |
| Mmc.exe | non disponible | available |
| Eventvwr | non disponible | available |
| Wevtutil (Requêtes d'événements) | available | available |
| Services.msc | non disponible | available |
| Panneau de configuration | non disponible | available |
| Mise à jour de Windows (GUI) | non disponible | available |
| Explorateur Windows | non disponible | available |
| Taskbar | non disponible | available |
| Notifications de la barre des tâches | non disponible | available |

| Application | Server Core | Server avec Expérience utilisateur |
|---|---|---|
| Taskmgr | available | available |
| Internet Explorer ou Microsoft Edge | non disponible | available |
| Système d'aide intégré | non disponible | available |
| Environnement de Windows 10 | non disponible | available |
| Lecteur Windows Media | non disponible | available |
| PowerShell | available | available |
| PowerShell ISE | non disponible | available |
| PowerShell IME | available | available |
| Mstsc.exe | non disponible | available |
| Services Bureau à distance | available | available |
| Gestionnaire de Hyper-V | non disponible | available |
| WordPad [1] | non disponible | available |

[1] Pour lire `.RTF` les fichiers stockés localement sur Server Core, les utilisateurs peuvent copier des fichiers sur un autre ordinateur Windows où WordPad est présent.

Pour plus d'informations sur ce que Server Core inclut, consultez Rôles, Services de rôle et fonctionnalités inclus dans Windows Server - Server Core. Pour plus d'informations sur ce que Server Core n'inclut pas, consultez Rôles, Services de rôle et Fonctionnalités non inclus dans Server Core.

# Bien démarrer avec Server Core

Utilisez les informations suivantes pour installer, configurer et gérer l'option d'installation Server Core de Windows Server.

Installation de Server Core :

- Rôles, services de rôle et fonctionnalités inclus dans Server Core
- Rôles, services de rôle et fonctionnalités non inclus dans Server Core
- Installer l'option d'installation Server Core
- Configurer Server Core avec l'outil Sconfig

Utilisation de Server Core :

- Tâches d’administration Server Core de base à l’aide de Windows PowerShell ou de la ligne de commande
- Gérer le Server Core
- Mise à jour corrective de Server Core
- Configurer les fichiers de vidage mémoire

---

Last updated on 31/10/2025

# Rôles, services de rôle et fonctionnalités inclus dans Windows Server - Server Core

08/08/2025

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

Cet article décrit les rôles, les services de rôle et les fonctionnalités disponibles dans l'option d'installation Server Core de Windows Server. Ces informations peuvent vous aider à déterminer si l'option Server Core convient à votre environnement. Compte tenu de la liste complète, vous pouvez rechercher un rôle ou une fonctionnalité spécifique. Si votre recherche ne génère pas de résultats, cela signifie que le rôle ou la fonctionnalité particulier n'est pas inclus dans Server Core.

Par exemple, si vous recherchez **hôte de session de bureau distant**, vous ne le trouverez pas sur cette page. La raison en est que l'hôte de session Bureau à distance n'est **pas** inclus dans l'image Server Core. Passez à la section suivante pour voir ce qui est inclus dans les builds Server Core.

Rôles

L'option d'installation minimale inclut les rôles serveur suivants.

Agrandir le tableau

| Role | Name | Installé par défaut ? |
|---|---|---|
| Services de certificats Active Directory | AD-Certificate | N |
| Services de domaine Active Directory | AD-Domain-Services | N |
| Services de fédération Active Directory (AD FS) | ADFS-Federation | N |
| Services AD LDS (Active Directory Lightweight Directory Services) | ADLDS | N |
| Services AD RMS (Active Directory Rights Management Services) | ADRMS | N |

| Role | Name | Installé par défaut ? |
|---|---|---|
| Attestation d’intégrité de l’appareil | DeviceHealthAttestationService (Service d'attestation de l'état de santé des appareils) | N |
| Serveur DHCP | DHCP | N |
| Serveur DNS | Système de noms de domaine (DNS) | N |
| Services de fichiers et de stockage | FileAndStorage-Services | O |
| Service Guardian hôte | HostGuardianServiceRole | N |
| Hyper-V | Hyper-V | N |
| Services d'impression et de numérisation de document | Print-Services | N |
| Accès à distance | RemoteAccess | N |
| Services Bureau à distance | Remote-Desktop-Services | N |
| Services d’activation en volume | VolumeActivation | N |
| Serveur web IIS) | Web-Server | N |
| Expérience Windows Server Essentials | ServerEssentialsRole | N |
| Windows Server Update Services | UpdateServices | N |

# Voir aussi

- Rôles, services de rôle et fonctionnalités non dans Windows Server - Server Core

# Administrer un serveur Server Core

15/08/2025

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

Comme Server Core n'a pas d'interface utilisateur, vous devez utiliser des applets de commande Windows PowerShell, des outils en ligne de commande ou des outils distants pour effectuer des tâches d'administration de base. Les sections suivantes présentent une vue d'ensemble des commandes et des applets de commande PowerShell utilisées pour les tâches simples. Vous pouvez également utiliser Windows Admin Center, le portail de gestion unifié actuellement en préversion publique, pour administrer votre installation.

## Tâches d'administration à l'aide d'applets de commande PowerShell

Utilisez les informations suivantes pour effectuer des tâches d'administration simples avec des applets de commande Windows PowerShell.

### Définir une adresse IP statique

Lorsque vous installez un serveur Server Core, il a une adresse DHCP par défaut. Si vous avez besoin d'une adresse IP statique, vous pouvez la définir en effectuant les étapes suivantes.

- Pour afficher votre configuration réseau actuelle, utilisez `Get-NetIPConfiguration`.
- Pour afficher les adresses IP que vous utilisez déjà, utilisez `Get-NetIPAddress`.

Pour définir une adresse IP statique, procédez comme suit :

1. Exécutez le `Get-NetIPInterface`.
2. Notez le nombre dans la colonne **IfIndex** pour votre interface IP ou la chaîne **InterfaceDescription** . Si vous disposez de plusieurs cartes réseau, notez le numéro ou la chaîne correspondant à l'interface pour laquelle vous souhaitez définir l'adresse IP statique.
3. Exécutez l'applet de commande suivante pour définir l'adresse IP statique :

```
PowerShell

New-NetIPaddress -InterfaceIndex 12 -IPAddress 192.0.2.2 -PrefixLength 24 -
```

```
DefaultGateway 192.0.2.1
```

where:

- `InterfaceIndex` est la valeur **d'IfIndex** de l'étape 2. (Dans cet exemple, 12)
- `IPAddress` est l'adresse IP statique que vous souhaitez définir. (Dans cet exemple, 191.0.2.2)
- `PrefixLength` est la longueur du préfixe qui est une autre forme de masque de sous-réseau pour l'adresse IP que vous définissez. (Pour cet exemple, 24)
- `DefaultGateway` est l'adresse IP de la passerelle par défaut. (Pour cet exemple, 192.0.2.1)

4. Exécutez l'applet de commande suivante pour définir l'adresse du serveur client DNS :

```
PowerShell

Set-DNSClientServerAddress –InterfaceIndex 12 -ServerAddresses 192.0.2.4
```

where:

- `InterfaceIndex` est la valeur **d'IfIndex** de l'étape 2.
- `ServerAddresses` est l'adresse IP de votre serveur DNS.

5. Pour ajouter plusieurs serveurs DNS, exécutez la commande suivante :

```
PowerShell

Set-DNSClientServerAddress –InterfaceIndex 12 -ServerAddresses
192.0.2.4,192.0.2.5
```

où, dans cet exemple, `192.0.2.4` et `192.0.2.5` sont les deux adresses IP des serveurs DNS.

## Définir l'adresse IP DHCP

Si vous devez basculer vers DHCP, exécutez la commande suivante :

```
PowerShell

Set-DnsClientServerAddress –InterfaceIndex 12 –ResetServerAddresses
```

## Joindre un domaine

Utilisez les applets de commande suivantes pour joindre un ordinateur à un domaine.

1. Exécutez le `Add-Computer`. On vous demande de fournir à la fois les informations d'identification pour rejoindre le domaine et le nom de domaine.
2. Si vous devez ajouter un compte d'utilisateur de domaine au groupe Administrateurs local, exécutez la commande suivante :

```
net localgroup administrators /add <DomainName>\<UserName> & shutdown /r /t 0
```

## Renommer le serveur

Suivez les étapes ci-après pour renommer le serveur.

1. Déterminez le nom actuel du serveur avec la commande `hostname` ou `ipconfig`.
2. Exécutez la commande suivante :

```powershell
Rename-Computer -NewName "NewName" -Force | Restart-Computer -Force
```

## Activer le serveur

Exécutez le `slmgr.vbs –ipk\productkey`. Exécutez ensuite `slmgr.vbs –ato`. L'activation réussie ne produit pas de notification à la fin.

> ⓘ **Notes**
>
> Vous pouvez également activer le serveur par téléphone, via un serveur du service de gestion de clés (KMS), ou à distance. Pour l'activation à distance, exécutez l'applet de commande suivante à partir d'un ordinateur distant :

```
cscript windows\system32\slmgr.vbs <ServerName> <UserName> <password>:-ato
```

## Configurer le pare-feu Windows

Vous pouvez configurer le Pare-feu Windows localement sur l'ordinateur exécutant l'installation Server Core à l'aide des applets de commande et des scripts de Windows PowerShell. Consultez NetSecurity pour les applets de commande que vous pouvez utiliser pour configurer le Pare-feu Windows.

## Activer la communication à distance Windows PowerShell

Vous pouvez activer la communication à distance Windows PowerShell, qui permet d'exécuter sur un ordinateur des commandes qui ont été entrées dans Windows PowerShell sur un autre ordinateur. Activez la fonction de communication à distance de Windows PowerShell avec `Enable-PSRemoting`.

Pour plus d'informations, voir Questions fréquentes sur la communication à distance.

# Tâches d'administration à partir de la ligne de commande

Utilisez les informations de référence suivantes pour effectuer des tâches d'administration à partir de la ligne de commande.

## Commandes de configuration et d'installation

Agrandir le tableau

| Task | Command |
|---|---|
| Définir le mot de passe d'administrateur local | `net user administrator *` |
| Joindre un ordinateur à un domaine | `netdom join %computername% /domain:<domain> /userd:<domain>\<username> /passwordd:<password>`<br><br>Redémarrez l'ordinateur. |
| Confirmer le changement de domaine | `set` |
| Supprimer un ordinateur d'un domaine | `netdom remove <computername>` |
| Ajouter un utilisateur au groupe Administrateurs local | `net localgroup Administrators /add <domain>\<username>` |

| Task | Command |
| --- | --- |
| Supprimer un utilisateur du groupe Administrateurs local | `net localgroup Administrators /delete <domain>\<username>` |
| Ajouter un utilisateur à l'ordinateur local | `net user <domain>\<username> * /add` |
| Ajouter un groupe à l'ordinateur local | `net localgroup <group name> /add` |
| Renommer un ordinateur joint au domaine | `netdom renamecomputer %computername% /NewName:<new computer name> /userd:<domain>\<username> /passwordd:<password>` |
| Confirmer le nouveau nom de l'ordinateur | `set` |
| Renommer un ordinateur dans un groupe de travail | `netdom renamecomputer <currentcomputername> /NewName:<newcomputername>`<br><br>Redémarrez l'ordinateur. |
| Désactiver la gestion des fichiers de pagination | `wmic computersystem where name="<computername>" set AutomaticManagedPagefile=False` |
| Configurer un fichier de pagination | `wmic pagefileset where name="<path/filename>" set InitialSize=<initialsize>,MaximumSize=<maxsize>`<br><br>Où <*chemin/nom de fichier*> est le chemin d'accès et le nom du fichier de pagination, `<initialsize>` est la taille de départ du fichier de pagination en octets, et *maxsize* correspond à la taille maximale du fichier de page en octets. |
| Modifier une adresse IP statique | Enregistrez les informations pertinentes ou redirigez-les vers un fichier texte : `ipconfig /all >ipconfig.txt`<br><br>Vérifiez qu'il existe une liste d'interfaces : `netsh interface ipv4 set address <Name ID from interface list> source=static address=<preferred IP address> gateway=<gateway address>`<br><br>Exécutez `ipconfig /all` pour vérifier que DHCP activé est défini sur **Non**. |
| Définir une adresse DNS statique | `netsh interface ipv4 add dnsserver name=<name or ID of the network interface card> address=<IP address of the primary DNS server> index=1`<br><br>`netsh interface ipv4 add dnsserver name=<name of secondary DNS server> address=<IP address of the secondary DNS server> index=2`<br><br>Répétez le cas échéant pour ajouter des serveurs supplémentaires. Exécutez `ipconfig /all` pour vérifier que les adresses sont correctes. |

| Task | Command |
| --- | --- |
| Changer une adresse IP statique en adresse IP fournie par un DHCP | `netsh interface ipv4 set address name=<IP address of local system> source=DHCP`<br><br>Exécutez `ipconfig /all` pour vérifier que le DCHP activé est défini sur **Oui**. |
| Entrer une clé de produit | `slmgr.vbs –ipk <product key>` |
| Activer le serveur localement | `slmgr.vbs -ato` |
| Activer le serveur à distance | `cscript slmgr.vbs –ipk <product key><server name><username><password>`<br><br>`cscript slmgr.vbs -ato <servername> <username> <password>`<br><br>Obtenez le GUID de l'ordinateur en exécutant `cscript slmgr.vbs -did`, puis exécutez `cscript slmgr.vbs -dli <GUID>`<br><br>Vérifiez que l'état de la licence est défini sur **Licence (activé)**. |

## Commandes de mise en réseau et de pare-feu

Agrandir le tableau

| Task | Command |
| --- | --- |
| Configurer votre serveur pour utiliser un serveur proxy | `netsh Winhttp set proxy <servername>:<port number>`<br><br>Les installations Server Core ne peuvent pas accéder à Internet via un proxy qui nécessite un mot de passe pour autoriser les connexions. |
| Configurer votre serveur afin de ne pas utiliser le serveur proxy pour des adresses Internet | `netsh winhttp set proxy <servername>:<port number> bypass-list="<local>"` |
| Afficher ou modifier la configuration IPSEC | `netsh ipsec` |
| Afficher ou modifier la configuration NAP | `netsh nap` |
| Afficher ou modifier la traduction d'adresses IP en adresses physiques | `arp` |
| Afficher ou configurer la table de routage locale | `route` |
| Voir ou configurer les paramètres de serveur DNS | `nslookup` |

| Task | Command |
| --- | --- |
| Afficher les statistiques du protocole et les connexions réseau TCP/IP actuelles | `netstat` |
| Afficher les statistiques du protocole et les connexions TCP/IP actuelles en utilisant NetBIOS sur TCP/IP (NBT) | `nbtstat` |
| Afficher les sauts des connexions réseau | `pathping` |
| Suivre les sauts des connexions réseau | `tracert` |
| Afficher la configuration du routeur de multidiffusion | `mrinfo` |
| Activer l'administration à distance du pare-feu | `netsh advfirewall firewall set rule group="Windows Defender Firewall Remote Management" new enable=yes` |

## Mises à jour système et commandes de création de rapports d'erreurs

Agrandir le tableau

| Task | Command |
| --- | --- |
| Installer une mise à jour | `wusa \<update\>.msu /quiet` |
| Afficher les mises à jour installées | `systeminfo` |
| Supprimer une mise à jour | `expand /f: <update>.msu c:\test`<br><br>Accédez au répertoire c:\test\ et ouvrez le fichier <update>.xml dans un éditeur de texte. **Remplacez l'installation** par **Supprimer** et enregistrez le fichier.<br><br>Exécutez ensuite `pkgmgr /n:<update>.xml` |
| Configurer les mises à jour automatiques | Pour vérifier le paramètre actuel : `cscript %systemroot%\system32\scregedit.wsf /AU /v`<br><br>Pour activer les mises à jour automatiques : `cscript scregedit.wsf /AU 4`<br><br>Pour désactiver les mises à jour automatiques : `cscript %systemroot%\system32\scregedit.wsf /AU 1` |

| Task | Command |
| --- | --- |
| Activer le rapport d'erreurs | Pour vérifier le paramètre actuel : `serverWerOptin /query`<br><br>Pour envoyer automatiquement des rapports détaillés : `serverWerOptin /detailed`<br><br>Pour envoyer automatiquement des rapports récapitulatives : `serverWerOptin /summary`<br><br>Pour désactiver la création de rapports d'erreurs : `serverWerOptin /disable` |
| Participer au Programme d'amélioration de l'expérience client (CEIP) | Pour vérifier le paramètre actuel : `serverCEIPOptin /query`<br><br>Pour activer le programme CEIP : `serverCEIPOptin /enable`<br><br>Pour désactiver le programme CEIP : `serverCEIPOptin /disable` |

## Services, processus et commandes de performances

Agrandir le tableau

| Task | Command |
| --- | --- |
| Lister les services en cours d'exécution | `sc query` ou<br>`net start` |
| Démarrer un service | `sc start <service name>` ou<br>`net start <service name>` |
| Arrêter un service | `sc stop <service name>` ou<br>`net stop <service name>` |
| Obtenir une liste des applications en cours d'exécution et des processus associés | `tasklist` |
| Démarrer le Gestionnaire des tâches | `taskmgr` |
| Créer et gérer des sessions de suivi des événements et des journaux de performances | Pour créer un compteur, une trace, une collecte de données de configuration ou une API : `logman create`<br><br>Pour interroger les propriétés du collecteur de données : `logman query`<br><br>Pour démarrer ou arrêter la collecte de données :<br>`logman start`<br>`logman stop` |

| Task | Command |
| --- | --- |
| | Pour supprimer un collecteur : `logman delete`<br><br>Pour mettre à jour les propriétés d'un collecteur : `logman update`<br><br>Pour importer un jeu de collecteurs de données à partir d'un fichier XML ou l'exporter vers un fichier XML : `logman import`<br>`logman export` |

## Commandes du journal des événements

Agrandir le tableau

| Task | Command |
| --- | --- |
| Lister les journaux d'événements | `wevtutil el` |
| Interroger des événements dans un journal spécifié | `wevtutil qe /f:text <log name>` |
| Exporter un journal d'événements | `wevtutil epl <log name>` |
| Effacer un journal d'événements | `wevtutil cl <log name>` |

## Commandes du pilote matériel

Agrandir le tableau

| Task | Command |
| --- | --- |
| Ajouter un lecteur pour un nouveau périphérique matériel | Copiez le lecteur dans un dossier dans **%homedrive% <dossier du lecteur>**.<br><br>Exécutez `pnputil -i -a %homedrive%\<driver folder>\<driver\<.inf>` |
| Supprimer un pilote pour un périphérique matériel | Pour obtenir la liste des pilotes chargés, exécutez `sc query type= driver`.<br><br>Exécutez ensuite `sc delete <service_name>` |

# Configurer une installation Server Core de Windows Server et d'Azure Local avec l'outil de configuration de serveur (SConfig)

15/08/2025

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

Vous pouvez utiliser l'outil de configuration de serveur (SConfig) pour configurer et gérer une instance Windows Server ou Azure Local. Quand Windows Server est installé avec l'option d'installation minimale, SConfig est le principal moyen de configurer et de gérer les aspects courants du système d'exploitation, y compris :

- Configuration réseau
- Appartenance au domaine Active Directory
- Installation des mises à jour Microsoft
- Activation du système d'exploitation

> ⓘ **Notes**
>
> SConfig est un outil pratique qui est particulièrement utile si vous devez configurer ou dépanner un seul serveur. Cependant, ce n'est pas la seule façon de configurer des paramètres et il peut ne pas être efficace à grande échelle. Si vous devez configurer plus d'une poignée de serveurs, nous vous recommandons de tirer parti de processus d'installation plus automatisés, tels que les fichiers réponse (unattend.xml), Microsoft Deployment Toolkit (MDT) ou Microsoft Endpoint Configuration Manager. Si vous déployez un hôte de virtualisation ou une machine virtuelle, la meilleure façon d'installer et de configurer le système d'exploitation est souvent System Center Virtual Machine Manager (VMM).
>
> De même, pour une gestion continue sur plusieurs instances de serveur, nous vous recommandons d'adopter des approches de gestion à distance à l'aide d'outils tels que Windows Admin Center, Le Gestionnaire de serveur ou les composants de System Center. Vous pouvez également utiliser la stratégie de groupe pour configurer automatiquement de nombreux paramètres de système d'exploitation, tels que l'activation de la gestion à distance et la configuration des mises à jour. Chacun de ces outils fonctionne également bien avec les options d'installation minimale et Server avec

Expérience utilisateur, supprimant ou réduisant considérablement la nécessité de gérer localement un serveur à la fois.

Voici quelques éléments à garder à l'esprit à propos de SConfig :

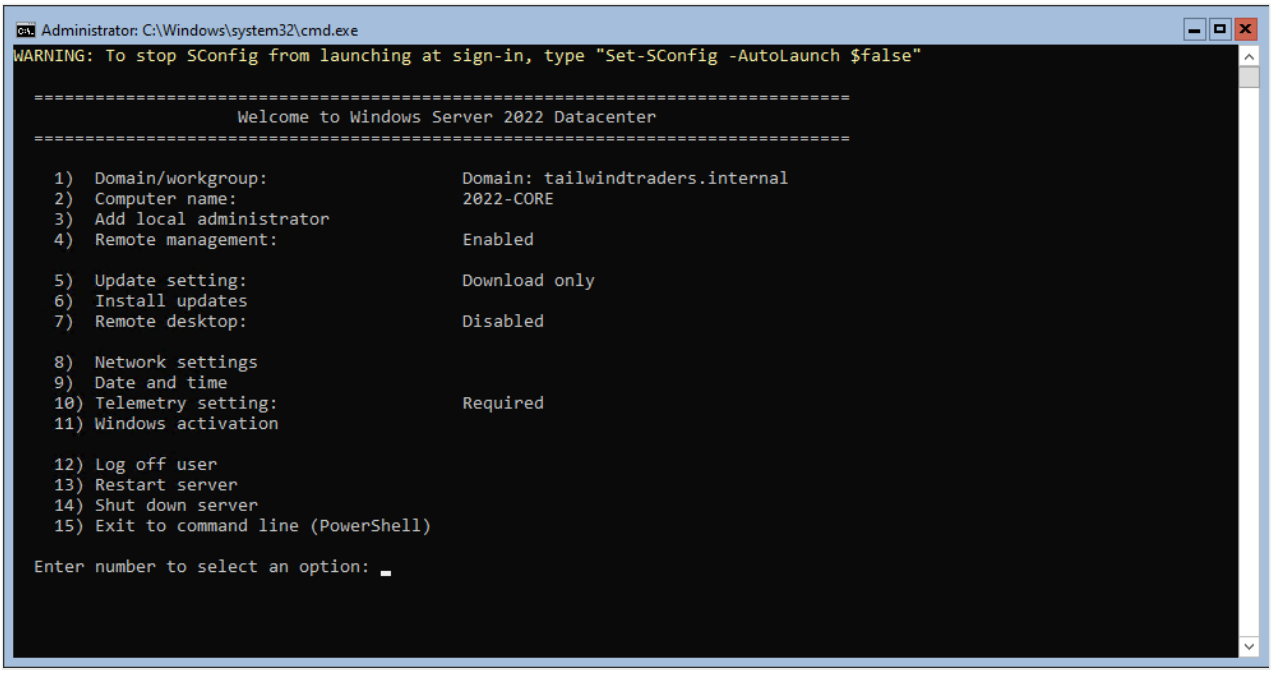
- À compter de Windows Server 2022 (déployé avec l'option d'installation Server Core) et Azure Local exécutent automatiquement SConfig après la connexion de l'utilisateur, sauf si autoLaunch est désactivé. Sur les versions précédentes de Windows Server, SConfig doit être lancé en utilisant `SConfig.cmd`.
- À compter de Windows Server 2022 et Azure Local, SConfig est basé sur PowerShell et redémarre automatiquement si vous fermez accidentellement la fenêtre PowerShell existante.
- Vous devez être membre du groupe Administrateurs local pour utiliser SConfig.
- Vous pouvez utiliser SConfig dans les scénarios suivants :
  - vous vous êtes connecté localement
  - vous êtes connecté avec Bureau à distance.
- Vous ne pouvez pas utiliser SConfig dans une session PowerShell distante. Si le serveur est déjà configuré de manière à prendre en charge la connectivité PowerShell distante, nous vous recommandons d'utiliser des outils plus évolutifs et riches en fonctionnalités pour gérer le serveur à distance.

# Démarrer SConfig

SConfig démarre automatiquement à partir de Windows Server 2022 (déployé dans l'option d'installation Server Core) et Azure Local. Pour exécuter SConfig sur des versions antérieures de Windows Server, effectuez ces étapes. Il est également possible d'exécuter SConfig sur Windows Server installé avec l'option d'installation Server avec Expérience utilisateur en utilisant ces étapes :

1. Lancez PowerShell.

2. Tapez `SConfig`, puis appuyez sur `Enter`. L'interface de l'outil de configuration de serveur s'ouvre.




> ⓘ Notes
>
> Le lancement de SConfig à partir d'une fenêtre d'invite de commandes (CMD) en exécutant `SConfig.cmd` fonctionne également dans Windows Server 2022 et Azure Local, comme dans les versions précédentes. Toutefois, cette méthode n'est plus développée et peut être supprimée dans les futures versions du système d'exploitation. La méthode recommandée pour lancer manuellement SConfig si nécessaire est d'exécuter `SConfig` dans une fenêtre PowerShell.

# Joindre un domaine ou groupe de travail

Les paramètres de domaine ou de groupe de travail Active Directory actuels s'affichent sur l'écran principal de SConfig. Vous pouvez joindre un domaine Active Directory ou un groupe de travail en accédant à la page **des paramètres du domaine/groupe de travail** à partir du menu principal et en suivant les instructions, en fournissant toutes les informations requises.

> ⓘ Notes
>
> Vous ne pourrez joindre un domaine que si l'ordinateur est en mesure de résoudre l'adresse DNS d'un contrôleur de domaine dans la forêt Active Directory Domain Services du domaine cible et si vous disposez des informations d'identification d'un compte autorisé à effectuer une opération de jonction de domaine. Vous devrez peut-être configurer des paramètres réseau et/ou la date et l'heure avant de joindre le domaine. Vous avez également la possibilité de modifier le nom de l'ordinateur dans le cadre de l'opération de jonction du domaine.

Pour joindre une instance de serveur autonome à un domaine avec SConfig, suivez ces étapes :

1. Dans le menu principal, tapez `1` et appuyez `Enter` pour entrer la page Modifier les paramètres **d'appartenance au domaine/groupe de travail** .
2. Dans le menu Modifier l'appartenance au domaine/groupe de travail, appuyez sur `D`.
3. Appuyez sur `Enter` pour joindre un domaine.
4. Tapez le nom du domaine à joindre, puis appuyez sur `Enter`.
5. Tapez le nom de l'utilisateur du domaine autorisé à joindre des ordinateurs au domaine. Utilisez le format `domain\user` ou `user@domain.com`, puis appuyez sur `Enter`.
6. À l'invite de mot de passe, indiquez le mot de passe de l'utilisateur spécifié, puis appuyez sur `Enter`.
7. À l'invite vous demandant si vous voulez changer le nom de l'ordinateur, appuyez sur `Y` ou `N`, puis appuyez sur `Enter`.
8. Si vous appuyez sur `Y`, indiquez le nouveau nom de l'ordinateur, puis appuyez sur `Enter`. Vous devez entrer à nouveau le mot de passe du compte d'utilisateur que vous avez spécifié lors de la jonction de l'ordinateur au domaine.
9. Vous serez invité à redémarrer l'ordinateur. Appuyez sur `Y`, puis sur `Enter` pour redémarrer l'ordinateur.
10. Une fois l'ordinateur redémarré, appuyez sur `ESC` pour changer d'utilisateur afin de pouvoir vous connecter avec un compte de domaine.

# Définir le nom de l'ordinateur

Le nom de l'ordinateur actuel s'affiche sur l'écran principal de SConfig. Vous pouvez modifier le nom de l'ordinateur en accédant à la page paramètres **nom** de l'ordinateur à partir du menu principal et en suivant les instructions.

Pour changer le nom de l'ordinateur, effectuez les étapes suivantes :

1. Dans le menu principal, tapez `2` et appuyez `Enter` pour entrer la page paramètres du **nom de l'ordinateur** .
2. À l'invite, indiquez le nouveau nom de l'ordinateur, puis appuyez sur `Enter`.
3. Si vous changez le nom d'un ordinateur joint à un domaine, spécifiez les informations d'identification d'un utilisateur ayant les autorisations nécessaires pour renommer le compte d'ordinateur. Appuyez sur `Enter` après avoir entré un nom d'utilisateur, puis tapez le mot de passe et appuyez sur `Enter`.
4. Quand vous êtes invité à redémarrer l'ordinateur, appuyez sur `Y`, puis sur `Enter`.

# Ajouter un administrateur local

Pour ajouter d'autres utilisateurs ou groupes au groupe Administrateurs local, utilisez l'option **Ajouter un administrateur local** dans le menu principal.

Ajoutez un compte d'utilisateur de domaine au groupe Administrateurs local, procédez comme suit :

1. Dans le menu principal, tapez `3` et appuyez `Enter` pour entrer la page **Ajouter des paramètres d'administrateur local** .
2. À l'invite, indiquez le nom d'utilisateur et appuyez sur `Enter`.

Les modifications sont immédiatement appliquées.

# Configuration de la gestion à distance

Vous pouvez activer différents scénarios de gestion à distance à partir de la page **Configurer les paramètres de gestion à distance** :

- **Activer ou désactiver la gestion à distance** autorise l'utilisation de PowerShell distant (également appelé Communication à distance PowerShell), Windows Admin Center et certains composants logiciels enfichables Microsoft Management Console. Elle est activée par défaut pour un réseau de domaine authentifié (si le serveur est joint à un domaine Active Directory) ou pour le sous-réseau local (pour les ordinateurs joints à un groupe de travail).
- **Activer ou désactiver la réponse à ping** permet d'utiliser des requêtes d'écho ICMP distantes (« ping ») pour vérifier la connectivité réseau. Il est désactivé par défaut.

1. Dans le menu principal, tapez `4` et appuyez `Enter` pour entrer la page Configurer les paramètres **de gestion à distance** .
2. Tapez `1` et appuyez sur `Enter` pour activer l'administration à distance, ou tapez `2` et appuyez sur `Enter` pour désactiver l'administration à distance.

## Configurer la réponse du serveur aux demandes d'écho ICMP (ping)

1. Dans le menu principal, tapez `4` et appuyez `Enter` pour entrer la page Configurer les paramètres **de gestion à distance** .
2. Pour activer la réponse du serveur au test ping, tapez `3` et appuyez sur `Enter`, et pour désactiver la réponse du serveur au test ping, tapez `4` et appuyez sur `Enter`.

# Mettre à jour les paramètres

Les paramètres de Microsoft Update s'affichent dans l'écran principal de SConfig. Vous pouvez configurer le serveur pour qu'il utilise des mises à jour automatiques ou manuelles sur la page paramètres de **paramètre de mise à jour** .

Lorsque **l'option Automatique** est sélectionnée, le système recherche et installe les mises à jour tous les jours à 3 h 00. (L'heure est interprétée en fonction du fuseau horaire effectif configuré sur le serveur, qui peut ou non être identique au fuseau horaire officiel dans la zone).

L'option **Télécharger uniquement** recherche les mises à jour, télécharge toutes les mises à jour disponibles, puis vous informe dans le Centre de notifications qu'elles sont prêtes à être installés. C'est l'option par défaut.

Lorsque **les mises à jour manuelles** sont sélectionnées, le système ne vérifie pas automatiquement les mises à jour.

> ⓘ **Notes**
>
> Le centre de notifications est disponible uniquement sur Windows Server installé avec l'option d'installation Serveur avec Expérience utilisateur, et il n'est visible que quand vous êtes connecté au serveur. Sur Server Core et Azure Local, vous ne recevrez aucune notification.

## Configurer les mises à jour

1. Dans le menu principal SConfig, tapez `5` et appuyez `Enter` pour entrer la page des paramètres de **paramètre de mise à jour** .
2. Passez en revue la configuration de la mise à jour, puis choisissez parmi les options suivantes :

    - Tapez `A`, puis appuyez sur `Enter` pour sélectionner les mises à jour à installer automatiquement.
    - Tapez `D`, puis appuyez sur `Enter` pour que les mises à jour soient recherchées périodiquement et téléchargées automatiquement, mais pas installées.
    - Tapez `M`, puis appuyez sur `Enter` pour rechercher manuellement les mises à jour.

## Installer les mises à jour

Vous pouvez choisir de rechercher des mises à jour dans les catégories suivantes :

- Toutes les mises à jour qualité
- Mises à jour qualité recommandées uniquement

- Mises à jour des fonctionnalités

> ⓘ **Notes**
>
> La **terminologie pour les types de mise à jour** (mais pas nécessairement la cadence de publication et la planification) est unifiée avec Windows 10 et Windows 11. Par conséquent, les *mises à jour des fonctionnalités* sont un autre nom pour ce qui est utilisé pour être appelés mises à niveau du système d'exploitation. Les mises à jour mensuelles régulières, y compris les mises à jour de sécurité, sont appelées *mises à jour qualité*.
>
> **Les mises à jour des fonctionnalités de Microsoft Update** sont actuellement disponibles uniquement pour Azure Local. Si vous souhaitez **mettre à niveau Windows Server** vers une version plus récente, vous devez utiliser un support d'installation traditionnel (tel qu'un ISO). À partir de là, vous **exécutez Setup.exe** directement ou tirez parti d'une solution d'automatisation telle que mentionnée précédemment. SConfig ne facilite pas spécifiquement ces scénarios.

La recherche retourne toutes les mises à jour disponibles dans la catégorie. Vous aurez la possibilité d'installer toutes les mises à jour disponibles, une mise à jour spécifique ou aucune des mises à jour disponibles.

1. Dans le menu principal de SConfig, tapez `6` et appuyez `Enter` pour entrer la page **Paramètres d'installation des mises à jour** .

2. Choisissez l'une des options suivantes :

   - Pour rechercher toutes les mises à jour qualité actuellement applicables au serveur, tapez `1`, puis appuyez sur `Enter`.
   - Pour rechercher seulement les mises à jour qualité recommandées applicables au serveur, tapez `2`, puis appuyez sur `Enter`.
   - Pour rechercher les mises à jour des fonctionnalités applicables au serveur, tapez `3`, puis appuyez sur `Enter`.

3. Une fois que vous avez effectué votre sélection, une liste des mises à jour disponibles s'affiche. Vous pouvez choisir une des options suivantes :

   - Pour installer toutes les mises à jour disponibles, tapez `A`, puis appuyez sur `Enter`.
   - Pour n'installer aucune des mises à jour disponibles, tapez `N`, puis appuyez sur `Enter`.
   - Pour installer une mise à jour spécifique de la liste, tapez `S`, puis appuyez sur `Enter`, tapez le numéro de la mise à jour, puis appuyez sur `Enter`.

# Configurer le Bureau à distance

L'état des paramètres du Bureau à distance est affiché dans l'écran principal de SConfig. Vous pouvez configurer les paramètres bureau à distance suivants en accédant à la page des paramètres **bureau à distance** et en suivant les instructions à l'écran :

- Activer le Bureau à distance pour les clients qui prennent en charge l'authentification au niveau du réseau (NLA)
- Activer le Bureau à distance pour les clients exécutant une des versions du logiciel Bureau à distance
- Désactiver le Bureau à distance

1. Dans le menu principal SConfig, tapez `7` et appuyez `Enter` pour entrer la page des paramètres **du Bureau à distance** .
2. Dans le menu Bureau à distance, tapez `E`, puis appuyez sur `Enter` pour activer le Bureau à distance. Vous pouvez aussi appuyer sur `D`, puis sur `Enter` pour désactiver le Bureau à distance.
3. Lors de l'activation du Bureau à distance, choisissez entre les options suivantes :

    - Pour autoriser uniquement les clients exécutant le Bureau à distance avec une authentification au niveau du réseau (plus sécurisée), tapez `1`, puis appuyez sur `Enter`.
    - Pour autoriser les clients exécutant n'importe quelle version du Bureau à distance (moins sécurisée), tapez `2`, puis appuyez sur `Enter`.

# Configurer le réseau

Par défaut, le système d'exploitation va tenter de provisionner une adresse réseau provenant d'un serveur DHCP. Si aucun serveur DHCP n'est disponible, il va affecter une adresse IP privée automatique (APIPA) à l'interface réseau. Vous pouvez aussi affecter manuellement une adresse IPv4 statique et spécifier le masque de sous-réseau et la passerelle par défaut. Lors de la configuration d'une adresse IPv4, vous pouvez aussi utiliser cette page de paramètres pour configurer des serveurs DNS principaux et secondaires.

1. Dans le menu principal, tapez `8` et appuyez `Enter` pour entrer la page **paramètres réseau** .
2. Dans cette liste d'interfaces disponibles, tapez le numéro de l'interface, comme `1`, puis appuyez sur `Enter` pour sélectionner cette interface.
3. Sur la page des paramètres de la **carte réseau**, choisissez l'une des options suivantes :
    a. Tapez `1`, puis appuyez sur `Enter` pour définir l'adresse de la carte réseau.

b. Appuyez sur `D`, et sur `Enter` pour configurer DHCP, ou appuyez sur `S` et sur `Enter` pour configurer une adresse IP statique.
c. Si vous choisissez l'option d'adresse IP statique, indiquez l'adresse IPv4, le masque de sous-réseau (en notation avec 4 points, par exemple `255.255.255.0`) et l'adresse de la passerelle par défaut en appuyant sur `Enter` après chaque entrée.

4. Tapez `2`, puis appuyez sur `Enter` pour définir l'adresse du serveur DNS.
   a. Spécifiez l'adresse IPv4 d'un serveur DNS préféré, puis appuyez sur `Enter`.
   b. Spécifiez l'adresse IPv4 d'un autre serveur DNS, puis appuyez sur `Enter`.
5. Tapez `3`, puis appuyez sur `Enter` pour effacer les paramètres actuels du serveur DNS.

## Paramètres de date et d'heure

La sélection de l'option Date et heure dans le menu principal ouvre l'applet Date et Heure du Panneau de configuration. Vous pouvez utiliser cette applet pour définir la date et l'heure, et pour modifier les paramètres de fuseau horaire.

## Configurer les données (de télémétrie) des diagnostics du système d'exploitation

Cette option vous permet de configurer si les informations statistiques anonymisées à propos de votre système sont transmises à Microsoft.

1. Dans le menu principal SConfig, tapez `10` et appuyez `Enter` pour entrer la page des paramètres de **paramètre de télémétrie** .
2. Pour modifier le paramètre de télémétrie, tapez `Y` pour Oui ou `N` pour Non, puis appuyez sur `Enter`.

> ⓘ **Notes**
>
> Windows Server et Azure Local ont une configuration par défaut différente concernant la télémétrie. Pour plus d'informations spécifiques à Windows Server, consultez **Configurer les données de diagnostic Windows dans votre organisation**. Pour Azure Local, consultez **l'extension de télémétrie et de diagnostic locale Azure**. Notez que vous ne pouvez pas configurer la collecte de données locale Azure dans SConfig. Pour en savoir plus sur l'approche de Microsoft en matière de confidentialité, consultez **Confidentialité chez Microsoft** .

## Activation de Windows

Cette option vous permet d'afficher l'état actuel de licence et d'activation, d'installer une clé de produit et d'activer Windows Server.

> ⓘ **Notes**
>
> L'activation est nécessaire seulement pour Windows Server. Cet élément de menu n'est pas disponible sur Azure Local, car le **déploiement local Azure** est un processus différent.

1. Dans le menu principal SConfig, tapez `11` et appuyez `Enter` pour entrer la page des paramètres **d'activation Windows** .
2. Choisissez l'une des options suivantes :

   - Tapez `1`, puis appuyez sur `Enter` pour voir l'état d'activation actuel.
   - Tapez `2`, puis appuyez sur `Enter` pour tenter l'activation avec la clé de produit actuellement installée.
   - Tapez `3`, puis appuyez sur `Enter` pour ajouter une nouvelle clé de produit. À l'invite, tapez la clé du produit, puis appuyez sur `Enter`. Appuyez à nouveau sur `Enter` une fois la clé de produit installée, puis revenez à ce menu et utilisez l'option `2` pour effectuer l'activation.

# Déconnecter l'utilisateur actuel

1. Dans le menu principal, tapez `12`, puis appuyez sur Entrée.
2. À l'invite vous demandant si vous êtes sûr, tapez `Y`, puis appuyez sur Entrée. L'utilisateur actuellement connecté sera déconnecté.

# Redémarrez le serveur

1. Dans le menu principal, tapez `13`, puis appuyez sur `Enter`.
2. À l'invite vous demandant si vous êtes sûr, tapez `Y`, puis appuyez sur Entrée. Le serveur va redémarrer.

# Arrêter le serveur

1. Dans le menu principal, tapez `14`, puis appuyez sur `Enter`.
2. À l'invite vous demandant si vous êtes sûr, tapez `Y`, puis appuyez sur Entrée. Le serveur va s'arrêter.

# Quitter pour la ligne de commande (PowerShell)

Cet élément de menu ferme le menu de SConfig et retourne à une invite PowerShell interactive (ou à une invite de commandes (CMD) pour Windows Server 2019 ou Windows Server 2016). Vous pouvez l'utiliser pour exécuter des commandes et des scripts PowerShell arbitraires pour la configuration avancée ou la résolution des problèmes. Bon nombre de ces options spécialisées ne sont pas disponibles nativement dans SConfig. Parmi les exemples figurent la configuration du stockage, les paramètres avancés de la carte réseau (tels que la configuration des IDs de VLAN), et l'installation des pilotes de périphérique.

> ⓘ **Notes**
>
> En règle générale, chaque paramètre disponible dans le système d'exploitation peut être contrôlé en utilisant des outils en ligne de commande ou des scripts. Cependant, la plupart de ces paramètres sont gérés plus facilement à distance en utilisant des outils graphiques comme Windows Admin Center, le Gestionnaire de serveur et System Center.

Pour quitter et accéder à PowerShell depuis le menu principal de SConfig, tapez `15`, puis appuyez sur `Enter`. Pour revenir à l'outil de configuration de serveur, tapez `SConfig`, puis appuyez sur `Enter`. Vous pouvez également commencer par Windows Server 2022 et Azure Local, tapez `exit`. Ceci ferme la fenêtre PowerShell actuelle et ouvre automatiquement une nouvelle instance de SConfig.

> ⓘ **Notes**
>
> Si vous avez lancé manuellement SConfig à partir d'une session d'invite de commandes (et non pas depuis une session PowerShell), quitter SConfig via l'option de menu `15` vous ramène à l'invite de commandes. Même si l'élément de menu indique **Quitter la ligne de commande (PowerShell)**, dans ce cas précis, il ne reste aucune session PowerShell interactive disponible.

## PowerShell est maintenant le shell par défaut sur Server Core.

Avant Windows Server 2022, le shell par défaut sur Server Core était l'invite de commandes (CMD). Elle était lancée par défaut quand l'utilisateur se connectait à Server Core. À partir de là, vous pouviez lancer SConfig ou exécuter des outils en ligne de commande arbitraires.

À compter de Windows Server 2022 (lorsqu'il est déployé avec l'option d'installation Server Core) et Azure Local, l'interpréteur de commandes par défaut est PowerShell. Il démarre par

défaut et SConfig est lancé automatiquement dans la fenêtre PowerShell. Si vous quittez SConfig en utilisant l'option de menu `15`, vous accédez à la session PowerShell interactive.

Cependant, si PowerShell est désinstallé, le shell par défaut redevient CMD. Contrairement aux versions précédentes du système d'exploitation, si PowerShell est désinstallé, SConfig ne s'exécute pas automatiquement ni manuellement. Vous ne pourrez utiliser que les outils en ligne de commande classiques tels que netsh.exe et diskpart.exe.

> ⓘ **Notes**
>
> Diskpart est déconseillé et peut ne pas fournir de fonctionnalités complètes. Par exemple, contrairement à PowerShell, il ne peut pas gérer les espaces de stockage.

Le changement du shell par défaut doit normalement être transparent pour la plupart des utilisateurs, car vous pouvez exécuter tous les mêmes outils en ligne de commande dans PowerShell que dans CMD. En outre, PowerShell a beaucoup plus de possibilités que CMD, à la fois en termes de fonctionnalités du langage interactif et de nombre de commandes disponibles. Cependant, dans certains scénarios limites, une commande dans PowerShell peut se comporter différemment de CMD, par exemple si vous utilisez la syntaxe des fichiers de commandes (comme `set foo=bar`) dans une session interactive. Si vous exécutez un fichier de commandes à la place, c'est-à-dire un fichier avec une extension `.cmd` ou `.bat`, il sera traité par CMD même s'il est lancé depuis PowerShell. Dans ce scénario, vous ne verrez pas de différences.

Vous pouvez passer explicitement à l'invite de commandes en tapant `cmd` dans PowerShell et en appuyant sur `Enter`. Vous pouvez aussi taper `start cmd` si vous préférez lancer une nouvelle fenêtre.

> ⓘ **Notes**
>
> Si vous envisagez de *recharger* une session PowerShell existante (par exemple, pour que les mises à jour de module prennent effet), le lancement de SConfig et sa sortie ne suffit pas. En effet, SConfig lui-même est une application PowerShell qui s'exécute dans une session PowerShell existante. Quitter SConfig vous amène à la session d'origine.
>
> Au lieu de cela, pour recharger une session PowerShell, tapez `exit`, puis appuyez sur `Enter`. Ceci va fermer la fenêtre PowerShell existante et une nouvelle fenêtre sera démarrée automatiquement. Notez que le rechargement d'une session PowerShell est spécifique aux installations Server Core de Windows Server et d'Azure Local. Sur les

installations du serveur avec Expérience utilisateur de Windows Server, vous devez lancer manuellement une nouvelle fenêtre PowerShell.

## Désactiver le démarrage automatique de SConfig

SConfig démarre automatiquement à partir de Windows Server 2022 (lorsqu'il est déployé avec l'option d'installation Server Core) et sur Azure Local. Vous pouvez faire cesser le lancement automatique de SConfig en exécutant la commande suivante dans PowerShell :

PowerShell

```
Set-SConfig -AutoLaunch $False
```

# Gérez un serveur Server Core

16/08/2025

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

Vous pouvez gérer un serveur Server Core de plusieurs façons :

- Utilisation de Windows Admin Center
- Utilisation des Outils d'administration de serveur distant s'exécutant sur Windows 10
- Localement et à distance avec Windows PowerShell
- À distance à l'aide du Gestionnaire de serveur
- À distance à l'aide d'un composant logiciel enfichable MMC
- Utilisation à distance des Services Bureau à distance

Vous pouvez également ajouter du matériel et gérer les pilotes localement, à condition de le faire à partir de la ligne de commande.

Vous devez tenir compte de certaines limitations et astuces importantes lorsque vous travaillez avec Server Core :

- Si vous fermez toutes les fenêtres d'invite de commandes et que vous souhaitez ouvrir une nouvelle fenêtre d'invite de commandes, vous pouvez le faire à partir du Gestionnaire des tâches. **Appuyez sur Ctrl+Alt+SUPPR**, sélectionnez **Démarrer le Gestionnaire** des tâches, sélectionnez **Plus d'informations** > **sur l'exécution du fichier**>, puis tapez **cmd.exe**. (Tapez **Powershell.exe** pour ouvrir une fenêtre de commande PowerShell.) Vous pouvez également vous déconnecter, puis vous reconnecter.
- Toute commande ou outil qui tente de démarrer l'Explorateur Windows ne fonctionne pas. Par exemple, l'exécution de **start .** à partir d'une invite de commandes ne fonctionne pas.
- Le rendu HTML et l'aide HTML ne sont pas pris en charge dans Server Core.
- Server Core prend en charge l'utilisation de Windows Installer en mode silencieux. Par conséquent, vous pouvez installer des outils et des utilitaires à partir de fichiers Windows Installer. Lors de l'installation de packages Windows Installer sur Server Core, utilisez l'option **/qb** pour afficher l'interface utilisateur de base.
- Pour modifier le fuseau horaire, exécutez **Set-Date**.
- Pour modifier les paramètres internationaux, exécutez le **contrôle intl.cpl**.
- **Control.exe** ne s'exécute pas seul. Vous devez l'exécuter avec **Timedate.cpl** ou **Intl.cpl**.
- **Winver.exe** n'est pas disponible dans Server Core. Utilisez **Systeminfo.exe** pour obtenir des informations de version.

# Gestion de Server Core avec Windows Admin Center

Windows Admin Center est une application de gestion basée sur un navigateur qui permet d'administrer localement des serveurs Windows Server, sans dépendance à Azure ou au cloud. Windows Admin Center vous donne un contrôle total sur tous les aspects de votre infrastructure de serveurs. Il s'avère utile pour la gestion sur les réseaux privés qui ne sont pas connectés à Internet. Vous pouvez installer Windows Admin Center sur un ordinateur Windows 10, un serveur de passerelle ou une installation de Windows Server avec Expérience de bureau. Une fois installé, vous pouvez vous connecter au système Server Core que vous souhaitez gérer.

# Gestion de Server Core à distance avec Gestionnaire de serveur

Le Gestionnaire de serveur est une console de gestion dans Windows Server qui vous permet de provisionner et de gérer des serveurs locaux et distants basés sur Windows à partir de vos bureaux. Le Gestionnaire de serveur n'a pas besoin d'un accès physique aux serveurs ou de la nécessité d'activer les connexions RDP (Remote Desktop Protocol) à chaque serveur. Le Gestionnaire de serveur prend en charge la gestion à distance et multiserveur.

Pour permettre à votre serveur local d'être géré par le Gestionnaire de serveur s'exécutant sur un serveur distant, exécutez l'applet de commande Windows PowerShell **Configure-SMRemoting.exe –Enable**.

# Gestion avec Microsoft Management Console

Vous pouvez utiliser de nombreux composants logiciels enfichables MMC (Microsoft Management Console) à distance pour gérer votre serveur Server Core.

Pour utiliser un composant logiciel enfichable MMC pour gérer un serveur Server Core qui est membre d'un domaine :

1. Démarrez un composant logiciel enfichable MMC, tel que Gestion de l'ordinateur.
2. Cliquez avec le bouton droit de la souris sur le snap-in, puis sélectionnez **Connecter à un autre ordinateur**.
3. Tapez le nom de l'ordinateur du serveur Server Core, puis sélectionnez **OK**. Vous pouvez maintenant utiliser le composant logiciel enfichable MMC pour gérer le serveur Server Core comme n'importe quel autre PC ou serveur.

Pour utiliser un composant logiciel enfichable MMC pour gérer un serveur Server Core qui *n'est pas* un membre de domaine :

1. Définissez d'autres informations d'identification à utiliser pour vous connecter à l'ordinateur Server Core. Pour ce faire, tapez la commande suivante à une invite de commandes sur l'ordinateur distant :

   ```
   cmdkey /add:<ServerName> /user:<UserName> /pass:<password>
   ```

   Si vous souhaitez être invité à entrer un mot de passe, omettez l'option **/pass** .

2. Lorsque vous y êtes invité, tapez le mot de passe du nom d'utilisateur que vous avez spécifié. Si le pare-feu sur le serveur Server Core n'est pas déjà configuré pour autoriser les composants logiciels enfichables MMC à se connecter, procédez comme suit pour configurer le Pare-feu Windows pour autoriser le composant logiciel enfichable MMC. Passez ensuite à l'étape 3.

3. Sur un autre ordinateur, démarrez un composant logiciel enfichable MMC, comme **Gestion des ordinateurs**.

4. Dans le volet de gauche, cliquez avec le bouton droit de la souris sur le snap-in, puis **sélectionnez Se connecter à un autre ordinateur**. (Par exemple, dans le composant Gestion de l'ordinateur, faites un clic droit sur **Gestion de l'ordinateur (local)**.)

5. Dans **un autre ordinateur**, tapez le nom de l'ordinateur du serveur Server Core, puis sélectionnez **OK**. Vous pouvez maintenant utiliser le composant logiciel enfichable MMC pour administrer le serveur en mode d'installation minimale comme vous le feriez sur n'importe quel autre ordinateur exécutant un système d'exploitation Windows Server.

## Pour configurer le Pare-feu Windows afin d'autoriser les snap-ins MMC à se connecter

Pour autoriser la connexion de n'importe quel composant logiciel enfichable MMC, exécutez la commande suivante :

PowerShell

```
Enable-NetFirewallRule -DisplayGroup "Windows Remote Management"
```

Pour autoriser uniquement les composants logiciels enfichables MMC spécifiques à se connecter, exécutez la commande suivante :

PowerShell

```
Enable-NetFirewallRule -DisplayGroup "<RuleGroup>"
```

Où *<RuleGroup>* est l'un des éléments suivants, en fonction du snap-in auquel vous souhaitez vous connecter :

Agrandir le tableau

| Composant logiciel enfichable MMC | Groupe de règles |
|---|---|
| Observateur d'événements | Gestion à distance des journaux des événements |
| Services | Gestion des services à distance |
| Dossiers partagés | Partage de fichiers et d'imprimantes |
| Task Scheduler | Journaux et alertes de performances, partage de fichiers et d'imprimantes |
| Gestion des disques | Gestion des volumes à distance |
| Pare-feu Windows Defender avec sécurité avancée | Gestion à distance du pare-feu Windows Defender |

**Notes**

Certains composants logiciels enfichables MMC n'ont pas de groupe de règles correspondant leur permettant de se connecter à travers le pare-feu. Toutefois, l'activation des groupes de règles pour l'observateur d'événements, les services ou les dossiers partagés permet à la plupart des autres composants logiciels enfichables de se connecter.

Par ailleurs, certains composants logiciels enfichables nécessitent une configuration supplémentaire pour pouvoir se connecter via le Pare-feu Windows :

- **Gestion des disques** : vous devez d'abord démarrer le service de disque virtuel (VDS) sur l'ordinateur Server Core. Vous devez également configurer les règles du composant logiciel enfichable Gestion des disques de manière appropriée sur le serveur qui exécute ce composant.
- **IP Security Monitor** : Vous devez d'abord activer la gestion à distance de ce snap-in. À l'invite de commandes, tapez `cscript c:\windows\system32\scregedit.wsf /im 1`
- **fiabilité et performances**: ce module complémentaire ne nécessite aucune configuration supplémentaire, mais lorsque vous l'utilisez pour surveiller un

ordinateur Server Core, vous ne pouvez surveiller que les données de performance. Les données de fiabilité ne sont pas disponibles.

## Gestion des Services Bureau à distance

Vous pouvez utiliser le Bureau à distance pour gérer un serveur Server Core à partir d'ordinateurs distants.

Avant de pouvoir accéder au Server Core, vous devez exécuter la commande suivante :

```
cscript C:\Windows\System32\Scregedit.wsf /ar 0
```

Cette commande permet au Bureau à distance pour le mode Administration d'accepter les connexions.

## Ajoutez un matériel et gérez les pilotes localement

Pour ajouter du matériel à un serveur Server Core, suivez les instructions fournies par le fournisseur de matériel pour l'installation de nouveau matériel.

Si le matériel n'est pas plug-and-play, vous devez installer le pilote manuellement. Pour ce faire, copiez les fichiers du pilote vers un emplacement temporaire sur le serveur, puis exécutez la commande suivante :

```
pnputil –i –a <driverinf>
```

Où *driverinf* est le nom de fichier du fichier .inf pour le pilote.

Redémarrez l'ordinateur le cas échéant.

Pour voir quels pilotes sont installés, exécutez la commande suivante :

```
sc query type= driver
```

**Notes**

N’oubliez pas d’inclure l’espace après le signe égal pour que la commande s’exécute correctement.

Pour désactiver un pilote de périphérique, exécutez la commande suivante :

```
sc delete <service_name>
```

Dans lequel *service_name* est le nom du service que vous avez obtenu lorsque vous avez exécuté la commande **sc query type= driver**.

# Configurer des fichiers d'image mémoire pour une installation minimale

14/08/2025

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

Suivez ces étapes pour configurer une image mémoire de votre installation minimale.

## Étape 1 : Désactiver la gestion automatique des fichiers de page système

La première étape consiste à configurer manuellement vos options d'échec et de récupération système. Celle-ci est indispensable pour effectuer les autres étapes.

Exécutez la commande suivante :

```
wmic computersystem set AutomaticManagedPagefile=False
```

## Étape 2 : Configurer le chemin de destination d'une image mémoire

Il n'est pas nécessaire de conserver le fichier de page sur la partition où le système d'exploitation est installé. Pour placer le fichier de page sur une autre partition, vous devez créer une entrée de Registre nommée **DedicatedDumpFile**. Vous pouvez définir la taille du fichier de pagination à l'aide de l'entrée de Registre **DumpFileSize** . Pour créer les entrées de Registre DedicatedDumpFile et DumpFileSize, procédez comme suit :

1. À l'invite de commandes, exécutez la commande **regedit** pour ouvrir l'Éditeur du Registre.
2. Recherchez la sous-clé suivante, puis cliquez dessus : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl
3. Cliquez sur **Modifier** > **Nouveau** > **Valeur de chaîne**.
4. Nommez la nouvelle valeur **DedicatedDumpFile**, puis appuyez sur Entrée.
5. Cliquez avec le bouton droit sur **DedicatedDumpFile**, puis cliquez sur **Modifier**.

6. Dans **données de valeur** tapez **<Drive>:\<Dedicateddumpfile.sys>**, puis cliquez sur **OK**.

> ⓘ **Notes**
>
> Remplacez <Lecteur> par un lecteur qui a suffisamment d'espace disque pour le fichier de pagination, et remplacez <Dedicateddumpfile.dmp> par le chemin complet du fichier dédié.

7. Cliquez sur **Modifier** > **Nouveau** > **Valeur DWORD**.
8. Tapez **DumpFileSize**, puis appuyez sur Entrée.
9. Cliquez avec le bouton droit sur **DumpFileSize**, puis cliquez sur **Modifier**.
10. Dans **Modifier la valeur DWORD**, sous **Base**, cliquez sur **Décimal**.
11. Dans **les données Valeur**, tapez la valeur appropriée, puis cliquez sur **OK**.

> ⓘ **Notes**
>
> La taille du fichier de l'image mémoire est en mégaoctets (Mo).

12. Quittez l'Éditeur du Registre.

Une fois que vous avez déterminé l'emplacement de la partition de l'image mémoire, configurez le chemin de destination du fichier de page. Pour afficher le chemin de destination actuel du fichier de page, exécutez la commande suivante :

```
wmic RECOVEROS get DebugFilePath
```

La destination par défaut de **DebugFilePath** est %systemroot%\memory.dmp. Pour modifier le chemin de destination actuel, exécutez la commande suivante :

```
wmic RECOVEROS set DebugFilePath = <FilePath>
```

Définissez <FilePath> sur le chemin de destination. Par exemple, la commande suivante définit le chemin de destination de l'image mémoire sur C:\WINDOWS\MEMORY.DMP:

```
```

```
wmic RECOVEROS set DebugFilePath = C:\WINDOWS\MEMORY.DMP
```

# Étape 3 : Définir le type d'image mémoire

Déterminez le type d'image mémoire à configurer pour votre serveur. Pour voir le type d'image mémoire actif, exécutez la commande suivante :

```
wmic RECOVEROS get DebugInfoType
```

Pour modifier le type d'image mémoire actif, exécutez la commande suivante :

```
wmic RECOVEROS set DebugInfoType = <Value>
```

La <valeur> peut être 0, 1, 2 ou 3, comme défini ci-dessous.

- 0 : Désactive la suppression d'une image mémoire.
- 1 : Image mémoire complète. Enregistre tout le contenu de la mémoire système lorsque votre ordinateur s'arrête de manière inattendue. Une image mémoire complète peut contenir des données provenant de processus en cours d'exécution lorsque l'image mémoire a été collecté.
- 2 : Image mémoire du noyau (par défaut). Enregistre uniquement la mémoire du noyau. Le processus d'enregistrement des informations dans un fichier journal se trouve accéléré lorsque votre ordinateur s'arrête de manière inattendue.
- 3 : Image mémoire de petite taille. Enregistre le plus petit ensemble d'informations utiles qui peuvent vous aider à identifier la raison pour laquelle votre ordinateur s'est arrêté de manière inattendue.

# Étape 4 : Configurer le serveur pour qu'il redémarre automatiquement après avoir généré une image mémoire

Par défaut, le serveur redémarre automatiquement après avoir généré une image mémoire. Exécutez la commande suivante pour afficher la configuration actuelle :

```
```

```
wmic RECOVEROS get AutoReboot
```

Si la valeur de **AutoReboot** est TRUE, le serveur redémarre automatiquement après avoir généré un vidage de mémoire. Aucune configuration n'est nécessaire et vous pouvez passer à l'étape suivante.

Si la valeur de **AutoReboot** est FALSE, le serveur ne redémarre pas automatiquement. Exécutez la commande suivante pour modifier la valeur :

```
wmic RECOVEROS set AutoReboot = true
```

# Étape 5 : Configurer le serveur pour remplacer le fichier d'image mémoire existant

Par défaut, le serveur remplace le fichier d'image mémoire existant lors de la création d'un nouveau fichier. Pour déterminer si les fichiers d'image mémoire existants sont déjà configurés pour être remplacés, exécutez la commande suivante :

```
wmic RECOVEROS get OverwriteExistingDebugFile
```

Si la valeur est 1, le serveur remplace le fichier d'image mémoire existant. Aucune configuration n'est nécessaire et vous pouvez passer à l'étape suivante.

Si la valeur est 0, le serveur ne remplace pas le fichier d'image mémoire existant. Exécutez la commande suivante pour modifier la valeur :

```
wmic RECOVEROS set OverwriteExistingDebugFile = 1
```

# Étape 6 : Définir une alerte d'administration

Déterminez si une alerte administrative est appropriée et définissez **SendAdminAlert** en conséquence. Pour afficher la valeur actuelle de SendAdminAlert, exécutez la commande suivante :

```
wmic RECOVEROS get SendAdminAlert
```

Les valeurs possibles de SendAdminAlert sont TRUE ou FALSE. Pour modifier la valeur SendAdminAlert existante sur true, exécutez la commande suivante :

```
wmic RECOVEROS set SendAdminAlert = true
```

# Étape 7 : Définir la taille du fichier de page de l'image mémoire

Pour vérifier les paramètres en cours du fichier de page, exécutez l'une des commandes suivantes :

```
wmic.exe pagefile
```

or

```
wmic.exe pagefile list /format:list
```

Par exemple, exécutez la commande suivante pour configurer la taille initiale et maximale de votre fichier de page :

```
wmic pagefileset where name="c:\\pagefile.sys" set
InitialSize=1000,MaximumSize=5000
```

# Étape 8 : Configurer le serveur pour générer une image mémoire manuelle

Vous pouvez générer manuellement une image mémoire en utilisant un clavier PS/2. Cette fonctionnalité est désactivée par défaut et n'est pas disponible pour les claviers USB (Universal Serial Bus).

Pour activer les images mémoire manuelles à l'aide d'un clavier PS/2, exécutez la commande suivante :

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters
/v CrashOnCtrlScroll /t REG_DWORD /d 1 /f
```

Pour déterminer si la fonctionnalité a été activée correctement, exécutez la commande suivante :

```
Reg query HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ i8042prt \
Parameters / v CrashOnCtrlScroll
```

Vous devez redémarrer le serveur pour que les modifications soient prises en compte. Vous pouvez redémarrer le serveur en exécutant la commande suivante :

```
Shutdown / r / t 0
```

Vous pouvez générer des images mémoire manuelles avec un clavier PS/2 connecté à votre serveur en maintenant la touche Ctrl Droite enfoncée tout en appuyant deux fois sur la touche Arrêt défil. La vérification des bogues de l'ordinateur retourne le code d'erreur 0xE2. Après avoir redémarré le serveur, un nouveau fichier d'image mémoire s'affiche dans le chemin de destination que vous avez établi à l'étape 2.

# Étape 9 : Vérifier que les fichiers d'image mémoire sont créés correctement

Vous pouvez utiliser l'utilitaire dumpchk.exe pour vérifier que les fichiers de vidage de la mémoire sont créés correctement. L'utilitaire dumpchk.exe n'est pas installé avec l'option d'installation minimale. Vous devez donc l'exécuter à partir d'un serveur en utilisant l'Expérience utilisateur, ou à partir de Windows 10. Les outils de débogage pour les produits Windows doivent être également installés.

L'utilitaire dumpchk.exe vous permet de transférer le fichier d'image mémoire, depuis votre installation minimale de Windows Server 2008 sur l'autre ordinateur, à l'aide du support de votre choix.

> ⚠ **Avertissement**
>
> Les fichiers de page peuvent être très volumineux, ainsi étudiez attentivement la méthode de transfert et les ressources demandées par la méthode.

Références supplémentaires

Pour obtenir des informations générales sur l'utilisation des fichiers d'image mémoire, consultez Vue d'ensemble des options du fichier d'image mémoire pour Windows.

Pour plus d'informations sur les fichiers d'image mémoire dédiés, consultez Utilisation de la valeur de Registre DedicatedDumpFile pour dépasser les limitations de l'espace sur le lecteur système lors de la capture d'une image mémoire système.

# Configurer les mises à jour de Windows Server Core

15/08/2025

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

La configuration des paramètres Windows Update sur une installation Windows Server Core peut être effectuée à l'aide du menu SConfig ou via la ligne de commande. Cet article décrit les étapes et les commandes nécessaires pour configurer les paramètres de Windows Update. Server Core permet l'installation des mises à jour Windows de la manière suivante :

- **Utilisation de Windows Update automatique** ou de **Windows Server Update Services** (WSUS). À l'aide de Windows Update, soit automatiquement, soit avec l'outil en ligne de commande WSUS, vous pouvez traiter les serveurs exécutant une installation Server Core.
- **Manuellement**. Même dans les organisations qui n'utilisent pas Windows Update ou WSUS, vous pouvez appliquer des mises à jour manuellement.

## Conditions préalables

- Votre appareil doit disposer d'une connexion Internet active.
- Le compte d'utilisateur effectuant des mises à jour Windows doit être membre du groupe **Administrateurs, Administrateurs** de **domaine** ou **Administrateurs d'entreprise** .
- Si le serveur est membre d'un domaine, l'agent Windows Update doit être configuré correctement via la stratégie de groupe. Les appareils Server Core prennent uniquement en charge l'option 4, **le téléchargement automatique et la planification de l'installation**, comme indiqué dans Configuration des mises à jour automatiques à l'aide de la stratégie de groupe. Consultez également la référence des paramètres de stratégie de groupe pour Windows et Windows Server.

## Afficher les mises à jour installées

Avant d'ajouter une nouvelle mise à jour à Server Core, vérifiez que les dernières mises à jour Windows sont installées en exécutant l'une des commandes suivantes :

PowerShell

```
Get-Hotfix | Sort-Object InstalledOn
```

PowerShell

```
Get-ComputerInfo -Property OsHotFixes
```

Invite de commandes Windows

```
systeminfo
```

Invite de commandes Windows

```
wmic qfe list
```

# Configurer les mises à jour Windows via SConfig

À compter de Windows Server 2002, le menu SConfig se charge une fois connecté. Si le menu SConfig n'apparaît pas, exécutez `sconfig` et sélectionnez **Entrée**. Une fois le menu chargé, procédez comme suit pour configurer vos paramètres :

1. Tapez **5**, sélectionnez **Entrée**. Sélectionnez l'une de ces options, puis **sélectionnez Entrée**.
   a. **1**) Automatique
   b. **2**) Télécharger uniquement
   c. **3**) Manuel

2. Tapez **6**, sélectionnez **Entrée**. Sélectionnez l'une de ces options, puis **sélectionnez Entrée**.
   a. **1**) Toutes les mises à jour qualité
   b. **2**) Mises à jour de qualité recommandées uniquement
   c. **3**) Mises à jour des fonctionnalités

# Configurer les mises à jour Windows via la ligne de commande

Invite de commandes

> **Conseil**
>
> VBScript est déconseillé. VBScript reste disponible en tant que fonctionnalité à la demande (FoD) et est préinstallé dans Windows Server 2025, mais envisagez d'utiliser PowerShell ou le menu SConfig pour configurer les paramètres de Windows Update. Pour en savoir plus sur la dépréciation de VBScript, consultez

https://techcommunity.microsoft.com/blog/windows-itpro-blog/vbscript-deprecation-timelines-and-next-steps/4148301.

Pour vérifier le paramètre Windows Update actuel, exécutez la commande suivante :

```
PowerShell

%systemroot%\system32\cscript %systemroot%\system32\scregedit.wsf /AU /v
```

Pour activer les mises à jour automatiques, exécutez la commande suivante :

```
PowerShell

Net stop wuauserv
%systemroot%\system32\cscript %systemroot%\system32\scregedit.wsf /AU /v 4
Net start wuauserv
```

Pour désactiver les mises à jour automatiques, exécutez la commande suivante :

```
PowerShell

Net stop wuauserv
%systemroot%\system32\cscript %systemroot%\system32\scregedit.wsf /AU /v 1
Net start wuauserv
```

Pour forcer Windows Update à détecter et installer immédiatement les mises à jour disponibles, exécutez la commande suivante :

```

wuauclt /detectnow
```

Selon les mises à jour installées, vous devrez peut-être redémarrer l'ordinateur. Le système n'avertit pas les mises à jour nécessitant un redémarrage. Pour déterminer si le processus d'installation s'est terminé, ouvrez **le Gestionnaire** des tâches en exécutant `taskmgr` et vérifiez que les processus **wuauclt** ou Programme d'installation **approuvé** ne sont pas en cours d'exécution activement.

# Appliquer manuellement une mise à jour de Windows Server

Pour supprimer la dernière mise à jour cumulative (LCU) après avoir installé les mises à jour combinées de la pile de maintenance (SSU) et du package LCU, utilisez l'applet `Remove-WindowsPackage` de commande ou l'option `Dism /Remove-Package` de ligne de commande avec le nom du package LCU comme argument. Vous trouverez le nom du package à l'aide de cette commande : DISM /online /get-packages.

Téléchargez le `.msu` fichier de mise à jour et choisissez votre méthode préférée pour installer la mise à jour.

PowerShell

À partir d'une invite PowerShell avec élévation de privilèges, exécutez la commande suivante :

PowerShell

```
Add-WindowsPackage -Online -Path "<folder_path>" -PackagePath "\
<update_file>.msu" -PreventPending
```

Le `-PreventPending` paramètre ignore l'installation du package si le package ou l'image Windows a des actions en ligne en attente.

Pour désinstaller manuellement une mise à jour, commencez par déterminer le nom de la mise à jour en exécutant la commande suivante :

PowerShell

```
Get-WindowsPackage -online -PackageName "*KB<NUM>*"
```

Exécutez ensuite la commande suivante pour désinstaller la mise à jour :

PowerShell

```
Remove-WindowsPackage -Online -PackageName "<package_name>"
```

# Mettre à jour avec Azure Update Manager

Vous pouvez également mettre à jour votre installation Windows Server Core à l'aide d'Azure Update Manager à partir du portail Azure.

# Gestionnaire de serveur

15/08/2025

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

Le Gestionnaire de serveur est une console de gestion centralisée dans Windows Server qui permet aux professionnels de l'informatique de provisionner et de gérer des serveurs locaux et distants à partir de leurs bureaux. Avec le Gestionnaire de serveur, vous pouvez administrer efficacement plusieurs serveurs sans avoir besoin d'un accès physique ou d'activer les connexions RDP (Remote Desktop Protocol). Le Gestionnaire de serveur prend en charge la gestion à distance, multiserveur et aide à augmenter le nombre de serveurs qu'un administrateur peut gérer.

Cet article fournit une vue d'ensemble des fonctionnalités du Gestionnaire de serveur, des tâches prises en charge et des conseils pour la gestion des serveurs dans votre environnement. Cet article contient les sections suivantes :

- Tâches que vous pouvez effectuer dans le Gestionnaire de serveur
- Démarrer le Gestionnaire de serveur
- Redémarrer les serveurs distants
- Exporter les paramètres du Gestionnaire de serveur vers d'autres ordinateurs

## Gérer des ordinateurs distants à partir d'un ordinateur client

La console gestionnaire de serveur est incluse avec les outils d'administration de serveur distant pour Windows 10 et Windows 11. Lorsque les outils d'administration de serveur distant sont installés sur un ordinateur client, vous ne pouvez pas gérer l'ordinateur local à l'aide du Gestionnaire de serveur ; Le Gestionnaire de serveur ne peut pas être utilisé pour gérer les ordinateurs ou les appareils exécutant un système d'exploitation client Windows. Vous pouvez utiliser le Gestionnaire de serveur seulement pour gérer des serveurs Windows.

### Démarrer le Gestionnaire de serveur sur un ordinateur client

1. Suivez les instructions des outils d'administration de serveur distant pour installer les outils d'administration de serveur distant pour Windows.

2. Dans l'écran de **démarrage** , cliquez sur **Gestionnaire de serveur**. La vignette **Gestionnaire** de serveur est disponible après avoir installé les outils d'administration de serveur distant.

3. Si ni les **outils d'administrationni les** vignettes gestionnaire de serveur ne s'affichent sur l'écran de **démarrage** après l'installation des outils d'administration de serveur distant et que la recherche du Gestionnaire de serveur sur l'écran de **démarrage** n'affiche pas les résultats, vérifiez que le paramètre **Afficher les outils d'administration** est activé. Pour afficher ce paramètre, pointez le curseur de la souris sur le coin supérieur droit de l'écran de **démarrage** , puis cliquez sur **Paramètres**. Si le paramètre **Afficher les outils d'administration** est désactivé, activez-le pour afficher les outils que vous avez installés dans le cadre des Outils d'administration de serveur distant.

Pour plus d'informations sur l'exécution des outils d'administration de serveur distant pour Windows 10 pour gérer les serveurs distants, consultez Outils d'administration de serveur distant sur le Wiki TechNet.

## Configurer la gestion à distance sur des serveurs que vous voulez gérer

Pour effectuer des tâches de gestion sur des serveurs distants en utilisant le Gestionnaire de serveur, les serveurs distants que vous voulez gérer doivent être configurés pour autoriser la gestion en utilisant le Gestionnaire de serveur et Windows PowerShell. Si la gestion à distance a été désactivée sur Windows Server et que vous souhaitez l'activer à nouveau, procédez comme suit.

### Configurer la gestion à distance du Gestionnaire de serveur

1. Effectuez l'une des opérations suivantes pour ouvrir le Gestionnaire de serveur s'il n'est pas déjà ouvert.

    - Dans la barre des tâches Windows, cliquez sur le bouton Gestionnaire de serveur.

    - Dans l'écran de **démarrage** , cliquez sur **Gestionnaire de serveur**.

2. Dans la zone **Propriétés** de la page **Serveurs locaux** , cliquez sur la valeur hypertexte de la propriété **de gestion à distance** .

3. Effectuez l'une des opérations suivantes, puis cliquez sur **OK**.

    - Pour empêcher la gestion à distance de cet ordinateur à l'aide du Gestionnaire de serveur ou de Windows PowerShell s'il est installé, décochez la case **Activer la gestion à distance de ce serveur à partir d'autres ordinateurs** .

- Pour permettre la gestion à distance de cet ordinateur en utilisant le Gestionnaire de serveur ou Windows PowerShell, sélectionnez **Activer la gestion à distance de ce serveur depuis d'autres ordinateurs**.

### Activer la gestion à distance du Gestionnaire de serveur sur Windows Server à l'aide de Windows PowerShell

1. Effectuez l'une des opérations suivantes.

   - Pour exécuter Windows PowerShell en tant qu'administrateur à partir de l'écran de **démarrage** , cliquez avec le bouton droit sur la vignette **Windows PowerShell** , puis cliquez sur **Exécuter en tant qu'administrateur**.

   - Pour exécuter Windows PowerShell en tant qu'administrateur à partir du bureau, cliquez avec le bouton droit sur le raccourci **Windows PowerShell** dans la barre des tâches, puis cliquez sur **Exécuter en tant qu'administrateur**.

2. Tapez ce qui suit, puis **appuyez sur Entrée** pour activer toutes les exceptions de règle de pare-feu requises.

   **Configure-SMremoting.exe -Enable**

   > ⓘ **Notes**
   >
   > Cette commande fonctionne également dans une invite de commandes ouverte avec des droits d'utilisateur élevés (Exécuter en tant qu'administrateur).

   si l'activation de la gestion à distance échoue, consultez about_remote_Troubleshooting sur Microsoft TechNet pour obtenir des conseils et des bonnes pratiques de dépannage.

## Tâches que vous pouvez effectuer dans le Gestionnaire de serveur

Le Gestionnaire de serveur rend l'administration des serveurs plus efficace en permettant aux administrateurs d'effectuer les tâches du tableau suivant en utilisant un seul outil. Les utilisateurs standard d'un serveur et des membres du groupe Administrateurs peuvent effectuer des tâches de gestion dans le Gestionnaire de serveur, mais par défaut, les utilisateurs standard ne peuvent pas effectuer certaines tâches, comme indiqué dans le tableau suivant.

Les administrateurs peuvent utiliser deux applets de commande Windows PowerShell dans le module d'applet de commande du Gestionnaire de serveur, Enable-

ServerManagerStandardUserremoting et Disable-ServerManagerStandardUserremoting, pour contrôler davantage l'accès des utilisateurs standard à d'autres données. La cmdlet **Enable-ServerManagerStandardUserremoting** peut fournir à un ou plusieurs utilisateurs standard, non-administrateur, un accès aux données d'événement, de service, de compteur de performances, ainsi qu'aux données de rôle et d'inventaire des fonctionnalités.

Agrandir le tableau

| Description de la tâche | Administrateurs (y compris le compte Administrateur intégré) | Utilisateurs de serveur standard |
|---|---|---|
| Ajoutez des serveurs distants à un pool de serveurs que le Gestionnaire de serveur peut être utilisé pour gérer. | Yes | No |
| Créez et modifiez des groupes personnalisés de serveurs, tels que des serveurs situés dans un emplacement géographique spécifique ou à des fins spécifiques. | Yes | Yes |
| Installez ou désinstallez des rôles, des services de rôle et des fonctionnalités sur les serveurs locaux ou distants exécutant Windows Server. En savoir plus sur l'ajout ou la suppression de rôles et de fonctionnalités dans Windows Server. | Yes | No |
| Afficher et modifier les fonctionnalités et rôles de serveur installés sur les serveurs locaux ou distants. Dans le Gestionnaire de serveur, les données des fonctionnalités et rôles sont affichées dans la langue de base du système, également appelée langue de l'interface utilisateur graphique par défaut du système, ou dans la langue sélectionnée lors de l'installation du système d'exploitation. | Yes | Les utilisateurs standard peuvent afficher et gérer des rôles et des fonctionnalités, et effectuer des tâches telles que l'affichage des événements de rôle, mais ne peuvent pas ajouter ou supprimer des services de rôle. |
| démarrez des outils de gestion tels que Windows PowerShell ou des composants logiciels enfichables mmc. Vous pouvez démarrer une session Windows PowerShell ciblée sur un serveur distant en cliquant avec le bouton droit sur le serveur dans la vignette **Serveurs** , puis en | Yes | Yes |

| Description de la tâche | Administrateurs (y compris le compte Administrateur intégré) | Utilisateurs de serveur standard |
| --- | --- | --- |
| cliquant sur **Windows PowerShell**. Vous pouvez démarrer les composants logiciels enfichables MMC à partir du menu **Outils** de la console Gestionnaire de serveur, puis pointer le MMC vers un ordinateur distant une fois le composant logiciel enfichable ouvert. | | |
| Gérez les serveurs distants avec différentes informations d'identification en cliquant avec le bouton droit sur un serveur dans la vignette **Serveurs** , puis en cliquant sur **Gérer sous**. Vous pouvez utiliser **Manage As** pour les tâches générales de gestion de serveur et des services de fichiers et de stockage. | Yes | No |
| Effectuer des tâches de gestion associées au cycle de vie opérationnel des serveurs, comme le démarrage ou l'arrêt de services, et démarrer d'autres outils qui vous permettent de configurer les paramètres réseau, les utilisateurs et les groupes, ainsi que les connexions Bureau à distance d'un serveur. | Yes | Les utilisateurs standard ne peuvent pas démarrer ou arrêter les services. Ils peuvent modifier le nom, le groupe de travail ou l'appartenance à un domaine et les paramètres Bureau à distance du serveur local, mais ils sont invités par le Contrôle de compte d'utilisateur à fournir des informations d'identification d'administrateur avant de pouvoir effectuer ces tâches. Ils ne peuvent pas modifier les paramètres de gestion à distance. |
| Effectuer des tâches de gestion associées au cycle de vie opérationnel des rôles installés sur les serveurs, notamment l'analyse des rôles pour une mise en conformité avec les meilleures pratiques. | Yes | Les utilisateurs standard ne peuvent pas exécuter d'analyses Best Practices Analyzer. |
| Déterminer l'état d'un serveur, identifier des événements critiques, analyser et dépanner des problèmes ou des échecs de configuration. | Yes | Yes |
| Personnaliser les événements, les données de performance, les services et résultats de Best Practices Analyzer au sujet desquels vous voulez être alerté dans le | Yes | Yes |

| Description de la tâche | Administrateurs (y compris le compte Administrateur intégré) | Utilisateurs de serveur standard |
|---|---|---|
| tableau de bord du Gestionnaire de serveur. | | |
| Redémarrez les serveurs. | Yes | No |
| Actualiser les données qui sont affichées dans la console du Gestionnaire de serveur à propos des serveurs gérés. | Yes | No |

# Démarrer le Gestionnaire de serveur

Le Gestionnaire de serveur démarre automatiquement par défaut sur Windows Server lorsqu'un membre du groupe Administrateurs se connecte à un serveur. Si vous fermez le Gestionnaire de serveur, redémarrez-le de l'une des façons suivantes. Cette section contient également les étapes pour modifier le comportement par défaut et pour empêcher le Gestionnaire de serveur de démarrer automatiquement.

## Démarrer le Gestionnaire de serveur à partir de l'écran de démarrage

- Dans l'écran de **démarrage** de Windows, cliquez sur la vignette **Gestionnaire de serveur** .

## Démarrer le Gestionnaire de serveur à partir du bureau Windows

- Dans la barre des tâches Windows, cliquez sur **Gestionnaire de serveur**.

## Empêcher le démarrage automatique du Gestionnaire de serveur

1. Dans la console gestionnaire de serveur, dans le menu **Gérer** , cliquez sur **Propriétés du Gestionnaire de serveur**.

2. Dans la boîte de dialogue **Propriétés du Gestionnaire de serveur**, activez la case à cocher **Ne pas démarrer automatiquement le Gestionnaire de serveur à l'ouverture de session**. Cliquez sur **OK**.

3. Vous pouvez aussi empêcher le démarrage automatique du Gestionnaire de serveur en activant le paramètre de stratégie de groupe **Ne pas démarrer automatiquement le Gestionnaire de serveur à l'ouverture de session**. Le chemin de ce paramètre de stratégie dans la console de l'éditeur de stratégie de groupe locale, est Configuration de l'ordinateur\Modèles d'administration\Système\Gestionnaire de serveur.

# Redémarrer les serveurs distants

Vous pouvez redémarrer un serveur distant à partir de la vignette **Serveurs** d'un rôle ou d'une page de groupe dans le Gestionnaire de serveur.

Le redémarrage d'un serveur distant force le serveur à redémarrer, même si des utilisateurs sont toujours connectés au serveur distant et que des programmes avec des données non enregistrées sont toujours ouverts. Ce comportement est différent de la fermeture ou du redémarrage de l'ordinateur local sur lequel vous êtes invité à enregistrer les données de programme non enregistrées et à confirmer que vous voulez forcer les utilisateurs connectés à fermer la session. Assurez-vous de pouvoir forcer d'autres utilisateurs à se déconnecter des serveurs distants et de pouvoir ignorer les données non enregistrées dans les programmes exécutés sur les serveurs distants.

Si une actualisation automatique se produit dans le Gestionnaire de serveur pendant qu'un serveur managé arrête et redémarre, les erreurs d'état d'actualisation et de facilité de gestion peuvent se produire pour le serveur managé, car le Gestionnaire de serveur ne peut pas se connecter au serveur distant tant qu'il n'a pas terminé de redémarrer.

## Redémarrer des serveurs distants dans le Gestionnaire de serveur

1. Ouvrez une page d'accueil de groupe de rôles ou de serveurs dans le Gestionnaire de serveur.

2. Sélectionnez un ou plusieurs serveurs distants que vous avez ajoutés au Gestionnaire de serveur. Appuyez longuement **sur Ctrl** lorsque vous cliquez pour sélectionner plusieurs serveurs à la fois. Pour plus d'informations sur l'ajout de serveurs au pool de serveurs du Gestionnaire de serveur, consultez Ajouter des serveurs au Gestionnaire de serveur.

3. Cliquez avec le bouton droit sur les serveurs sélectionnés, puis cliquez sur **Redémarrer le serveur**.

# Exporter les paramètres du Gestionnaire de serveur vers d’autres ordinateurs

Dans le Gestionnaire de serveur, votre liste de serveurs gérés est remplacée par les paramètres de la console du Gestionnaire de serveur, et les groupes personnalisés que vous avez créés sont stockés dans les deux fichiers suivants. Vous pouvez réutiliser ces paramètres sur d’autres ordinateurs exécutant la même version du Gestionnaire de serveur. Les Outils d’Administration de serveur distant doivent être exécutés sur des ordinateurs basés sur le client Windows pour y exporter les paramètres du Gestionnaire de serveur.

- % *appdata*%\Microsoft\Windows\ServerManager\Serverlist.xml
- % *appdata*%\Local\Microsoft_Corporation\ServerManager.exe_StrongName_*GUID*\6.2.0.0\user.config

> ⓘ **Notes**
>
> - Les informations d’identification Gérer en tant que (ou autres) pour les serveurs de votre pool de serveurs ne sont pas stockées dans le profil itinérant. Les utilisateurs du Gestionnaire de serveur doivent les ajouter sur chaque ordinateur à partir duquel ils veulent effectuer la gestion.
> - Le profil d’itinérance du partage réseau n’est pas créé jusqu'à ce qu'un utilisateur se connecte au réseau et se déconnecte pour la première fois. Le fichier **Serverlist.xml** est créé pour l’instant.

Vous pouvez exporter les paramètres du Gestionnaire de serveur, rendre portables les paramètres du Gestionnaire de serveur ou les utiliser sur d’autres ordinateurs de l’une des deux façons suivantes.

- Pour exporter les paramètres vers un ordinateur joint à un autre domaine, configurez l’utilisateur du Gestionnaire de serveur afin qu’il dispose d’un profil itinérant dans Utilisateurs et ordinateurs Active Directory. Vous devez être un administrateur de domaine pour modifier les propriétés des utilisateurs dans Utilisateurs et ordinateurs Active Directory.

- Pour exporter les paramètres vers un autre ordinateur dans un groupe de travail, copiez les deux fichiers précédents au même emplacement sur l’ordinateur à partir duquel vous voulez effectuer la gestion en utilisant le Gestionnaire de serveur.

## Exporter les paramètres du Gestionnaire de serveur vers d'autres ordinateurs joints à un domaine

1. Dans les utilisateurs et les ordinateurs Active Directory, ouvrez la boîte de dialogue **Propriétés** d'un utilisateur du Gestionnaire de serveur.

2. Sous l'onglet **Profil** , ajoutez un chemin d'accès à un partage réseau pour stocker le profil de l'utilisateur.

3. Effectuez l'une des opérations suivantes.

    - Sur les builds anglais (en-us) américains, les modifications apportées au fichier **Serverlist.xml** sont automatiquement enregistrées dans le profil. Passez à l'étape suivante.

    - Sur les autres versions, copiez les deux fichiers suivants depuis l'ordinateur qui exécute le Gestionnaire de serveur vers le partage réseau qui fait partie du profil itinérant de l'utilisateur.

        - % *appdata*%\Microsoft\Windows\ServerManager\Serverlist.xml

        - % *localappdata*%\Microsoft_Corporation\ServerManager.exe_StrongName_*GUID*\6.2.0.0\user.config

4. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue **Propriétés** .

## Exporter les paramètres du Gestionnaire de serveur vers des ordinateurs dans des groupes de travail

- Sur un ordinateur à partir duquel vous voulez gérer des serveurs distants, remplacez les deux fichiers suivants par les mêmes fichiers provenant d'un autre ordinateur qui exécute le Gestionnaire de serveur et qui dispose des paramètres souhaités.

    - % *appdata*%\Microsoft\Windows\ServerManager\Serverlist.xml

    - % *localappdata*%\Microsoft_Corporation\ServerManager.exe_StrongName_*GUID*\6.2.0.0\user.config

# Gérer le serveur local et la console du Gestionnaire de serveur

16/08/2025

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

Dans Windows Server, le Gestionnaire de serveur vous permet de gérer à la fois le serveur local (si vous exécutez le Gestionnaire de serveur sur Windows Server et non pas sous un système d'exploitation client Windows) et des serveurs distants qui exécutent Windows Server 2008 et des versions plus récentes du système d'exploitation Windows Server.

La page **Serveur local** du Gestionnaire de serveur affiche les propriétés du serveur, les événements, les données de compteur de service et de compteur de performances, ainsi que les résultats BPA (Best Practices Analyzer) pour le serveur local. Les vignettes Événements, Services, BPA et Performances fonctionnent comme dans les pages de rôles et de groupes de serveurs. Pour plus d'informations sur la configuration des données affichées dans ces vignettes, voir View et Configure Performance, Event, et Service Data et Run Best Practices Analyzer Scans et Manage Scan Results.

Les paramètres et les commandes de menu dans les barres de titre de la console du Gestionnaire de serveur s'appliquent globalement à tous les serveurs de votre pool de serveurs, et vous permettent d'utiliser le Gestionnaire de serveur pour gérer l'intégralité du pool de serveurs.

Cette rubrique contient les sections suivantes.

- Arrêter le serveur local
- Configurer les propriétés du Gestionnaire de serveur
- Gérer la console du Gestionnaire de serveur
- Personnaliser les outils qui sont affichés dans le menu Outils
- Gérer les rôles dans les pages d'accueil des rôles

## Arrêter le serveur local

Le menu **Tâches** de la vignette **Propriétés** du serveur local vous permet de démarrer une session Windows PowerShell sur le serveur local, d'ouvrir le composant logiciel enfichable mmc gestion de **l'ordinateur** ou d'ouvrir des composants logiciels enfichables mmc pour les rôles ou fonctionnalités installés sur le serveur local. Vous pouvez également arrêter le serveur local en

utilisant la commande **Arrêter le serveur local** dans ce menu **Tâches**. La commande **Arrêter le serveur local** est également disponible pour le serveur local dans la vignette **Serveurs** de la page **Tous les serveurs**, ou dans toute page de groupe ou de rôle dans laquelle le serveur local est représenté.

L'arrêt du serveur local à l'aide de cette méthode, contrairement à l'arrêt de Windows Server 2016 à partir de l'écran de **démarrage** , ouvre la boîte de dialogue **Arrêter Windows** , ce qui vous permet de spécifier des raisons d'arrêt dans la zone De suivi des événements **d'arrêt** .

> ⓘ **Notes**
>
> Seuls les membres du groupe Administrateurs peuvent arrêter ou redémarrer un serveur. Les utilisateurs standard ne peuvent pas arrêter ni redémarrer un serveur. Un clic sur la commande **Arrêter le serveur local** entraîne la fermeture des sessions serveur des utilisateurs standard. Cela correspond à l'expérience d'un utilisateur standard exécutant la commande **d'arrêt Alt+F4** à partir du bureau du serveur.

# Configurer les propriétés du Gestionnaire de serveur

Vous pouvez afficher ou modifier les paramètres suivants dans la vignette **Propriétés** sur la page **Serveur local** . Pour modifier la valeur d'un paramètre, cliquez sur la valeur du lien hypertexte du paramètre.

> ⓘ **Notes**
>
> En règle générale, les propriétés affichées dans la vignette **Propriétés** du serveur local ne peuvent être modifiées que sur le serveur local. Vous ne pouvez pas modifier les propriétés du serveur local à partir d'un ordinateur distant à l'aide du Gestionnaire de serveur, car la vignette **Propriétés** ne peut obtenir que des informations sur l'ordinateur local, et non sur les ordinateurs distants.
>
> Étant donné que de nombreuses propriétés affichées dans la vignette **Propriétés** sont contrôlées par les outils qui ne font pas partie du Gestionnaire de serveur (Panneau de configuration, par exemple), les modifications apportées aux paramètres **propriétés** ne sont pas toujours affichées dans la vignette **Propriétés** immédiatement. Par défaut, les données de la vignette **Propriétés** sont actualisées toutes les deux minutes. Pour actualiser immédiatement les données de vignette **Propriétés** , cliquez sur **Actualiser** dans la barre d'adresses du Gestionnaire de serveur.

Agrandir le tableau

| Setting | Description |
| --- | --- |
| computer name | Affiche le nom convivial de l'ordinateur et ouvre la boîte de dialogue **Propriétés système** , qui vous permet de modifier le nom du serveur, l'appartenance au domaine et d'autres paramètres système tels que les profils utilisateur. |
| Domaine (ou Groupe de travail, si le serveur n'appartient pas à un domaine) | Affiche le domaine ou groupe de travail duquel le serveur est un membre. Ouvre la boîte de dialogue **Propriétés système** , qui vous permet de modifier le nom du serveur, l'appartenance au domaine et d'autres paramètres système tels que les profils utilisateur. |
| Pare-feu Windows | Affiche l'état du Pare-feu Windows pour le serveur local. Ouvre **Panneau de configuration\Système et sécurité\Pare-feu Windows**. Pour plus d'informations sur la configuration du Pare-feu Windows, voir Pare-feu Windows avec fonctions avancées de sécurité et IPsec. |
| remote management | Affiche l'état de la gestion à distance du Gestionnaire de serveur et de Windows PowerShell. Ouvre la boîte de dialogue **Configurer la gestion à distance**. Pour plus d'informations sur la gestion à distance, consultez Configure la gestion à distance dans le Gestionnaire de serveur. |
| Remote Desktop | Indique si les utilisateurs peuvent se connecter au serveur à distance à l'aide de sessions Bureau à distance. Ouvre l'onglet **distant** de la boîte de dialogue **Propriétés système** . |
| Association de cartes réseau | Indique si le serveur local participe à l'association de cartes réseau. Ouvre la boîte de dialogue **Association de** cartes réseau et vous permet de joindre le serveur local à une équipe de carte réseau si vous le souhaitez. |
| Ethernet | Affiche l'état du réseau du serveur. Ouvre **Panneau de configuration\Réseau et Internet\Connexions réseau**. |
| Version du système d'exploitation | Ce champ en lecture seule affiche le numéro de version du système d'exploitation Windows exécuté par le serveur local. |
| Informations matérielles | Ce champ en lecture seule affiche le fabricant ainsi que le nom et le numéro de modèle du matériel de serveur. |
| Dernières mises à jour installées | Affiche le jour et l'heure de la dernière installation des mises à jour de Windows. Ouvre **Panneau de configuration\Système et sécurité\Windows Update**. |
| Windows Update | Affiche les paramètres de Windows Update pour le serveur local. Ouvre **Panneau de configuration\Système et sécurité\Windows Update**. |
| Dernière recherche de mises à jour | Affiche le jour et l'heure de la dernière recherche de mises à jour de Windows disponibles par le serveur. Ouvre **Panneau de configuration\Système et sécurité\Windows Update**. |

| Setting | Description |
| --- | --- |
| Rapport d'erreurs Windows | Affiche l'état de l'abonnement concernant le rapport d'erreurs Windows. Ouvre la boîte de dialogue **Configuration du rapport d'erreurs Windows**. Pour plus d'informations sur le rapport d'erreurs Windows, ses avantages, les déclarations de confidentialité et les paramètres d'abonnement, voir Rapport d'erreurs Windows. |
| Programme d'amélioration du produit | Affiche l'état de l'abonnement concernant le Programme d'amélioration de l'expérience utilisateur Windows. Ouvre la boîte de dialogue **Configuration du Programme d'amélioration de l'expérience utilisateur**. Pour plus d'informations sur le Programme d'amélioration de l'expérience utilisateur Windows, ses avantages et paramètres d'abonnement, voir Programme d'amélioration de l'expérience utilisateur Windows. |
| Configuration de sécurité renforcée d'Internet Explorer | Indique si la Configuration de sécurité renforcée d'Internet Explorer (également connue sous le nom de renforcement de IE ou IE ESC) est activée ou désactivée. Ouvre la boîte de dialogue **Configuration de sécurité renforcée d'Internet Explorer**. La Configuration de sécurité renforcée d'Internet Explorer est une mesure de sécurité pour les serveurs qui empêche l'ouverture des pages Web dans Internet Explorer. Pour plus d'informations sur la Configuration de sécurité renforcée d'Internet Explorer, ses avantages et paramètres, voir Internet Explorer : Configuration de sécurité renforcée. |
| time zone | Affiche le fuseau horaire du serveur local. Ouvre la boîte de dialogue **Date et heure**. |
| ID de produit | Affiche l'état d'activation de Windows et le numéro d'identification de produit (si Windows a été activé) du système d'exploitation Windows Server 2016. Il ne s'agit pas du même numéro que la clé de produit Windows. Ouvre la boîte de dialogue **Activation de Windows** . |
| Processors | Ce champ en lecture seule affiche le fabricant, le nom de modèle et des informations sur la vitesse des processeurs du serveur local. |
| Mémoire installée (RAM) | Ce champ en lecture seule affiche la quantité de mémoire RAM disponible, en gigaoctets. |
| Espace disque total | Ce champ en lecture seule affiche la quantité d'espace disque disponible, en gigaoctets. |

# Gérer la console du Gestionnaire de serveur

Les paramètres globaux qui s'appliquent à l'intégralité de la console du Gestionnaire de serveur et à tous les serveurs distants qui ont été ajoutés au pool de serveurs du Gestionnaire de serveur se trouvent dans les barres de titre en haut de la fenêtre de la console du Gestionnaire de serveur.

## Ajouter des serveurs au Gestionnaire de serveur

La commande qui ouvre la boîte de dialogue **Ajouter des serveurs** et vous permet d'ajouter des serveurs physiques ou virtuels distants au pool de serveurs du Gestionnaire de serveurs, se trouve dans le menu **Gérer** de la console Gestionnaire de serveur. Pour plus d'informations sur l'ajout de serveurs, consultez Ajouter des serveurs au Gestionnaire de serveur.

## Actualiser les données qui sont affichées dans le Gestionnaire de serveur

Vous pouvez configurer l'intervalle d'actualisation des données affichées dans le Gestionnaire de serveur dans la boîte de dialogue **Propriétés du Gestionnaire de serveur**, que vous ouvrez à partir du menu **Gérer**.

### Pour configurer l'intervalle d'actualisation dans le Gestionnaire de serveur

1. Dans le menu **Gérer** dans la console Gestionnaire de serveur, cliquez sur **Propriétés du Gestionnaire de serveur**.

2. Dans la boîte de dialogue **Propriétés du Gestionnaire de serveur**, spécifiez une période, en minutes, correspondant à la durée qui doit s'écouler entre les actualisations des données affichées dans le Gestionnaire de serveur. La valeur par défaut est 10 minutes. Cliquez sur OK quand vous avez terminé.

### Limitations d'actualisation

L'actualisation s'applique globalement aux données de tous les serveurs que vous avez ajoutés au pool de serveurs du Gestionnaire de serveur. Vous ne pouvez pas actualiser des données ni configurer différents intervalles d'actualisation pour des serveurs, rôles ou groupes individuels.

Quand des serveurs qui se trouvent dans un cluster sont ajoutés au Gestionnaire de serveur, qu'il s'agisse d'ordinateurs physiques ou de machines virtuelles, la première actualisation de données peut échouer ou afficher des données seule pour le serveur hôte des objets en cluster. Les actualisations suivantes affichent des données précises pour les serveurs physiques ou virtuels dans un cluster de serveurs.

Les données qui sont affichées dans les pages d'accueil des rôles dans le Gestionnaire de serveur pour les services Bureau à distance, le gestion des adresses IP, et les services de fichiers et de stockage ne sont pas actualisées automatiquement. Actualisez les données affichées

manuellement dans ces pages, en appuyant sur **F5** ou en cliquant sur **Actualiser** dans le titre de la console Gestionnaire de serveur pendant que vous êtes sur ces pages.

## Ajouter ou supprimer des rôles ou des fonctionnalités

Les commandes qui ouvrent l'Assistant Ajout de rôles et de fonctionnalités et suppriment les rôles et fonctionnalités, et vous permettent d'ajouter ou de supprimer des rôles, des services de rôle et des fonctionnalités aux serveurs de votre pool de serveurs, se trouvent dans le menu **Gérer** de la console Gestionnaire de serveur et le menu **Tâches** de la vignette **Rôles et fonctionnalités** sur les pages de rôle ou de groupe. Pour plus d'informations sur l'ajout ou la suppression de rôles ou de fonctionnalités, voir Installer ou désinstaller des rôles, des services de rôle ou des fonctionnalités.

Dans le Gestionnaire de serveur, les données des fonctionnalités et rôles sont affichées dans la langue de base du système, également appelée langue de l'interface utilisateur graphique par défaut du système, ou dans la langue sélectionnée lors de l'installation du système d'exploitation.

## Créer des groupes de serveurs

La commande qui ouvre la boîte de dialogue **Créer un groupe de serveurs** et qui vous permet de créer des groupes de serveurs personnalisés se trouve dans le menu **Gérer** de la console du Gestionnaire de serveur. Pour plus d'informations sur la façon de créer des groupes de serveurs, consultez Créer et gérer des groupes de serveurs.

## Empêcher l'ouverture automatique du Gestionnaire de serveur lors de l'ouverture de session

La case à cocher **Ne pas démarrer automatiquement le Gestionnaire de serveur à l'ouverture de session** dans la boîte de dialogue **Propriétés du Gestionnaire de serveur** contrôle si le Gestionnaire de serveur s'ouvre automatiquement à l'ouverture de session pour les membres du groupe Administrateurs sur un serveur local. Ce paramètre n'affecte pas le comportement du Gestionnaire de serveur quand il est exécuté sur Windows 10 dans le cadre des Outils d'administration de serveur distant. Pour plus d'informations sur la configuration de ce paramètre, consultez le Gestionnaire de serveur.

## Zoom avant ou arrière

Pour effectuer un zoom avant ou arrière sur votre vue de la console gestionnaire de serveur, vous pouvez utiliser les commandes **Zoom** dans le menu **Affichage** , ou appuyer sur **Ctrl+Plus**

(+) pour effectuer un zoom avant et **Ctrl+Moins (-)** pour effectuer un zoom arrière.

# Personnaliser les outils qui sont affichés dans le menu Outils

Le menu **Outils** du Gestionnaire de serveur inclut des liens logiciels vers des raccourcis dans le dossier **Outils d'administration** du **Panneau de configuration/Système et Sécurité**. Le dossier **Outils d'administration** contient une liste de raccourcis ou de fichiers LNK pour les outils de gestion disponibles, tels que les composants logiciels enfichables mmc. Le Gestionnaire de serveur remplit le menu **Outils** avec des liens vers ces raccourcis et copie la structure de dossiers du dossier **Outils d'administration** dans le menu **Outils** . Par défaut, les outils du dossier Outils d'administration sont classés dans une liste plate et triés par type et par nom. Dans le menu**Outils** du Gestionnaire de serveur, les éléments sont triés uniquement par nom, et non par type.

Pour personnaliser le menu **Outils** , copiez des raccourcis d'outil ou de script que vous souhaitez utiliser dans le dossier **Outils d'administration** . Vous pouvez également organiser vos raccourcis dans les dossiers, qui créent des menus en cascade dans le menu **Outils** . en outre, si vous souhaitez restreindre l'accès aux outils personnalisés dans le menu **Outils** , vous pouvez définir des droits d'accès utilisateur sur vos dossiers d'outils personnalisés dans Outils d'administration, ou directement sur l'outil d'origine ou les fichiers de script.

Nous vous déconseillons de réorganiser les outils d'administration et système, et tous les outils de gestion associés aux fonctionnalités et rôles installés sur le serveur local. Le déplacement des outils de gestion des fonctionnalités et rôles peut empêcher la réussite de la désinstallation de ces outils de gestion lorsque cela est nécessaire. Après la désinstallation d'un rôle ou d'une fonctionnalité, un lien non fonctionnel vers un outil dont le raccourci a été déplacé peut rester dans le menu **Outils** . Si vous réinstallez le rôle, un lien en double vers le même outil est créé dans le menu **Outils** , mais l'un des liens ne fonctionne pas.

Les outils des rôles et des fonctionnalités qui sont installés dans le cadre des Outils d'administration de serveur distant sur un ordinateur basé sur le client Windows peuvent toutefois être organisés en dossiers personnalisés. La désinstallation de la fonctionnalité ou du rôle parent n'a aucun effet sur les raccourcis d'outils qui sont disponibles sur un ordinateur distant qui exécute Windows 10.

La procédure suivante explique comment créer un exemple de dossier appelé *MyTools* et déplacer des raccourcis pour deux scripts Windows PowerShell dans le dossier qui sont ensuite accessibles à partir du menu Outils du Gestionnaire de serveur.

## Pour personnaliser le menu Outils en ajoutant des raccourcis dans Outils d'administration

1. créez un dossier appelé *MyTools* dans un emplacement pratique.

   > ⓘ **Notes**
   >
   > En raison des droits d'accès restrictifs sur le dossier **Outils d'administration** , vous n'êtes pas autorisé à créer un dossier directement dans le dossier **Outils d'administration** ; vous devez créer un dossier ailleurs (par exemple, sur le Bureau), puis copier le nouveau dossier dans le dossier **Outils d'administration** .

2. déplacez ou copiez *MyTools* dans **le Panneau de configuration/Systèmes et outils de sécurité/d'administration**. Par défaut, vous devez être membre du groupe Administrateurs sur l'ordinateur pour apporter des modifications au dossier **Outils d'administration** .

3. Si vous n'avez pas besoin de limiter les droits d'accès utilisateur sur vos raccourcis d'outils personnalisés, passez à l'étape 6. Sinon, cliquez avec le bouton droit sur le fichier outil (ou le dossier *MyTools* ), puis cliquez sur **Propriétés**.

4. Sous l'onglet **Sécurité** de la boîte de dialogue **Propriétés** du fichier, cliquez sur **Modifier**.

5. Pour les utilisateurs pour lesquels vous voulez limiter l'accès aux outils, désactivez les cases à cocher pour les autorisations **Lecture & exécution**, **Lecture** et **Écriture**. Ces autorisations sont héritées par le raccourci outil n le dossier **Outils d'administration** .

   si vous modifiez les droits d'accès d'un utilisateur pendant que l'utilisateur utilise le Gestionnaire de serveur (ou si le Gestionnaire de serveur est ouvert), vos modifications ne s'affichent pas dans le menu **Outils** tant que l'utilisateur n'a pas redémarré le Gestionnaire de serveur.

   > ⓘ **Notes**
   >
   > si vous limitez l'accès à un dossier entier que vous avez copié dans Les outils d'administration, les utilisateurs restreints ne peuvent voir ni le dossier ni son contenu dans le menu**Outils** du Gestionnaire de serveur.
   >
   > modifiez les autorisations pour le dossier dans le dossier **Outils d'administration** . Étant donné que les fichiers et dossiers masqués des outils d'administration sont toujours affichés dans le menu**Outils** du Gestionnaire de serveur, n'utilisez pas le paramètre **Masqué** dans la boîte de dialogue **Propriétés** d'un fichier ou dossier pour restreindre l'accès utilisateur aux raccourcis de votre outil personnalisé.

**Refuser** les autorisations remplacent toujours **autoriser** les autorisations.

6. Cliquez avec le bouton droit sur l'outil d'origine, le script ou le fichier exécutable pour lequel vous souhaitez ajouter des entrées dans le menu **Outils** , puis cliquez sur **Créer un raccourci**.

7. déplacez le raccourci vers le dossier *MyTools* dans Outils d'administration.

8. Actualisez ou redémarrez le Gestionnaire de serveur, si nécessaire, pour afficher le raccourci de votre outil personnalisé dans le menu **Outils** .

# Gérer les rôles dans les pages d'accueil des rôles

Une fois que vous avez ajouté des serveurs au pool de serveurs du Gestionnaire de serveur et que celui-ci a collecté des données d'inventaire sur les serveurs de votre pool, le Gestionnaire de serveur ajoute des pages au volet de navigation pour les rôles qui sont découverts sur les serveurs gérés. La vignette **Serveurs** sur les pages de rôle répertorie les serveurs gérés qui exécutent le rôle. Par défaut, **les événements**, **Best Practices Analyzer**, **Services** et les vignettes **Performances** affichent les données de tous les serveurs exécutant le rôle ; La sélection de serveurs spécifiques dans la vignette **Serveurs** limite l'étendue des événements, services, compteurs de performances et résultats BPA aux serveurs sélectionnés uniquement. Les outils de gestion sont généralement disponibles dans le menu **Outils** de console du Gestionnaire de serveur, une fois qu'un rôle ou une fonctionnalité a été installé ou découvert sur un serveur managé. Vous pouvez également cliquer avec le bouton droit sur les entrées du serveur dans la vignette **Serveurs** pour un rôle ou un groupe, puis démarrer l'outil de gestion que vous souhaitez utiliser.

Dans Windows Server 2016, les fonctionnalités et rôles suivants ont des outils de gestion qui sont intégrés à la console du Gestionnaire de serveur sous forme de pages.

- **Services de fichiers et de stockage** Les pages des services de fichiers et de stockage incluent des commandes et vignettes personnalisées pour la gestion des volumes, partages, disques virtuels iSCSI et pools de stockage. Quand vous ouvrez la page d'accueil du rôle Services de fichiers et de stockage dans le Gestionnaire de serveur, un volet rétractable s'ouvre et affiche des pages de gestion personnalisée pour les services de fichiers et de stockage. Pour plus d'informations sur le déploiement et la gestion des services de fichiers et de stockage, voir Services de fichiers et de stockage.

- **Services Bureau à distance** Les pages des services Bureau à distance incluent des commandes et vignettes personnalisées pour la gestion des sessions, licences, passerelles et bureaux virtuels. Pour plus d'informations sur le déploiement et la gestion des services Bureau à distance, consultez Services Bureau à distance.

- **Gestion des adresses IP (IPAM)** La page de rôle IPAM inclut une vignette **d'accueil** personnalisée contenant des liens vers des tâches courantes de configuration et de gestion IPAM, notamment un Assistant pour l'approvisionnement d'un serveur IPAM. La page d'accueil IPAM inclut également des vignettes pour afficher le réseau géré, le résumé de la configuration et les tâches planifiées.

  La gestion IPAM a quelques limitations dans le Gestionnaire de serveur. Contrairement aux pages de rôle et de groupe classiques, IPAM n'a pas de **serveurs**, **d'événements**, **de performances**, d'analyseur **de meilleures pratiques** ou de vignettes **Services** . Il n'existe pas modèle Best Practices Analyzer disponible pour IPAM ; les analyses Best Practices Analyzer sur IPAM ne sont pas prises en charge. Pour accéder aux serveurs de votre pool de serveurs qui exécutent IPAM, créez un groupe personnalisé de ces serveurs qui exécutent IPAM et accédez à la liste des serveurs à partir de la vignette **Serveurs** sur la page groupe personnalisé. Vous pouvez également accéder aux serveurs IPAM à partir de la vignette **Serveurs** sur la page **du groupe Tous les serveurs** .

  Les miniatures du tableau de bord affichent également des lignes limitées pour IPAM, par rapport aux miniatures pour d'autres rôles et groupes. En cliquant sur les lignes des miniatures IPAM, vous pouvez afficher des événements, données de performance et alertes d'état de la gestion pour les serveurs qui exécutent IPAM. Les services liés à IPAM peuvent être gérés à partir de pages pour les groupes de serveurs qui contiennent des serveurs IPAM, tels que la page du groupe **Tous les serveurs** .

  Pour plus d'informations sur le déploiement et la gestion d'IPAM, consultez Gestion des adresses IP (IPAM).

# Voir aussi

Le Gestionnaire de serveur ajoute des serveurs au Gestionnaire de serveurs pour créer et gérer l'affichage des groupes de serveurset configurer les performances, les événements et les services de données de service et les services bureau à distance (rdS) Gestion des adresses IP (IPAM)

# Configurer la gestion à distance dans le Gestionnaire de serveur

14/08/2025

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

Dans Windows Server, vous pouvez alors utiliser le Gestionnaire de serveur pour effectuer les tâches de gestion sur des serveurs distants. La gestion à distance est activée par défaut sur les serveurs qui exécutent Windows Server 2016. Pour gérer un serveur à distance à l'aide du Gestionnaire de serveur, vous devez ajouter le serveur dans le pool de serveurs du Gestionnaire de serveur.

Vous pouvez utiliser le Gestionnaire de serveur pour gérer les serveurs distants qui exécutent des versions plus anciennes de Windows Server, mais les mises à jour répertoriées ci-dessous sont requises pour gérer entièrement ces anciens systèmes d'exploitation.

Pour gérer les serveurs qui exécutent des versions de Windows Server antérieures à Windows Server 2016, installez les logiciels et mises à jour suivants pour rendre les anciennes versions de Windows Server gérables en utilisant le Gestionnaire de serveur dans Windows Server 2016.

Agrandir le tableau

| Système d'exploitation | Logiciels requis | Manageability |
|---|---|---|
| Windows Server 2012 R2 ou Windows Server 2012 | - .NET Framework 4.6<br>- Windows Management Framework 5.0. Le package de téléchargement Windows Management Framework 5.0 met à jour les fournisseurs WMI (Windows Management Instrumentation) sur Windows Server 2012 R2, Windows Server 2012 et Windows Server 2008 R2. Les fournisseurs WMI mis à jour permettent au Gestionnaire de serveur de collecter des informations sur les rôles et les fonctionnalités qui sont installés sur les serveurs gérés. Tant que la mise à jour n'est pas appliquée, les serveurs exécutant Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2 ont un état de facilité de gestion non **accessible**.<br>- La mise à jour des performances associée à l'article de la Base de connaissances 2682011 n'est plus nécessaire sur les serveurs qui exécutent Windows Server 2012 R2 ou Windows Server 2012. | |
| Windows Server 2008 R2 | - .NET Framework 4.5<br>- Windows Management Framework 4.0. Le package de téléchargement de Windows Management Framework 4.0 met à | |

| Système d'exploitation | Logiciels requis | Manageability |
| --- | --- | --- |
| | jour les fournisseurs WMI (Windows Management Instrumentation) sur Windows Server 2008 R2. Les fournisseurs WMI mis à jour permettent au Gestionnaire de serveur de collecter des informations sur les rôles et les fonctionnalités qui sont installés sur les serveurs gérés. Tant que la mise à jour n'est pas appliquée, les serveurs exécutant Windows Server 2008 R2 ont un état de facilité de gestion non **accessible**.<br>- La mise à jour des performances associée à l'article de la Base de connaissances 2682011 permet au Gestionnaire de serveur de collecter des données de performances auprès de Windows Server 2008 R2. | |
| Windows Server 2008 | - .NET Framework 4<br>- Windows Management Framework 3.0 Le package de téléchargement Windows Management Framework 3.0 met à jour les fournisseurs WMI (Windows Management Instrumentation) sur Windows Server 2008. Les fournisseurs WMI mis à jour permettent au Gestionnaire de serveur de collecter des informations sur les rôles et les fonctionnalités qui sont installés sur les serveurs gérés. Tant que la mise à jour n'est pas appliquée, les serveurs exécutant Windows Server 2008 ont l'état de facilité de gestion **Non accessible – Vérifiez que les versions antérieures exécutent Windows Management Framework 3.0**.<br>- La mise à jour des performances associée à l'article de la Base de connaissances 2682011 permet au Gestionnaire de serveur de collecter des données de performances auprès de Windows Server 2008. | |

Pour des informations détaillées sur la façon d'ajouter des serveurs qui se trouvent dans des groupes de travail à gérer ou de gérer des serveurs distants à partir d'un ordinateur de groupe de travail qui exécute le Gestionnaire de serveur, consultez Ajouter des serveurs au Gestionnaire de serveur.

# Activation ou désactivation de l'administration à distance

Dans Windows Server 2016, la gestion à distance est activée par défaut. Avant de pouvoir vous connecter à distance à un ordinateur qui exécute Windows Server 2016 à l'aide du Gestionnaire de serveur, la gestion à distance du Gestionnaire de serveur doit être activée sur l'ordinateur de destination si elle a été désactivée. Les procédures fournies dans cette section décrivent la manière de désactiver l'administration à distance et la manière de la réactiver si elle a été

désactivée. Dans la console du Gestionnaire de serveur, l'état de gestion à distance du serveur local s'affiche dans la zone **Propriétés** de la page **Serveur local** .

Les comptes d'administrateur local autres que le compte Administrateur intégré n'ont peut-être pas les droits requis pour gérer un serveur à distance, même si l'administration à distance est activée. Le paramètre de registre **LocalAccountTokenFilterPolicy** du contrôle de compte d'utilisateur distant doit être configuré pour autoriser les comptes locaux du groupe Administrateurs autres que le compte d'administrateur intégré à gérer à distance le serveur.

Dans Windows Server 2016, le Gestionnaire de serveur s'appuie sur WinRM (Windows Remote Management) et le modèle DCOM (Distributed Component Object Model) pour les communications à distance. Les paramètres contrôlés par la boîte de dialogue **Configurer la gestion à distance** affectent uniquement les parties du Gestionnaire de serveur et de Windows PowerShell qui utilisent WinRM pour les communications à distance. Ils n'affectent pas les parties du Gestionnaire de serveur qui utilisent le modèle DCOM pour les communications à distance. Par exemple, le Gestionnaire de serveur utilise WinRM pour communiquer avec des serveurs distants qui exécutent Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012, mais utilise DCOM pour communiquer avec les serveurs qui exécutent Windows Server 2008 et Windows Server 2008 R2, mais qui n'ont pas les mises à jour Windows Management Framework 4.0 ou Windows Management Framework 3.0 appliquées. La console MMC (Microsoft Management Console) et d'autres outils de gestion hérités utilisent le modèle DCOM. Pour plus d'informations sur la modification de ces paramètres, voir Configurer l'administration à distance via MMC ou un autre outil par le biais du modèle DCOM dans cette rubrique.

> ⓘ **Notes**
>
> Les procédures de cette section ne peuvent être réalisées que sur des ordinateurs qui exécutent Windows Server. Vous ne pouvez pas activer ou désactiver l'administration à distance sur un ordinateur qui exécute Windows 10 en utilisant ces procédures, car le système d'exploitation client ne peut pas être géré à l'aide du Gestionnaire de serveur.

- Pour activer l'administration à distance via WinRM, sélectionnez l'une des procédures suivantes :
  - Activer l'administration à distance via le Gestionnaire de serveur à l'aide de l'interface Windows
  - Activer l'administration à distance via le Gestionnaire de serveur à l'aide de Windows PowerShell

    - Activer l'administration à distance via le Gestionnaire de serveur dans la ligne de commande
    - Activer l'administration à distance via le Gestionnaire de serveur et Windows PowerShell dans des versions antérieures de Windows Server
- Pour désactiver la gestion à distance via WinRM et le Gestionnaire de serveur, sélectionnez l'une des procédures suivantes :
    - Pour désactiver la gestion à distance à l'aide d'une stratégie de groupe
    - Pour désactiver la gestion à distance à l'aide d'un fichier de réponses au cours d'une installation sans assistance
- Pour configurer la gestion à distance via DCOM, voir Pour configurer la gestion à distance via DCOM.

## Activer l'administration à distance via le Gestionnaire de serveur à l'aide de l'interface Windows

1. > ⓘ **Notes**
   >
   > Les paramètres qui sont contrôlés par la boîte de dialogue **Configurer l'administration à distance** n'affectent pas les parties du Gestionnaire de serveur qui utilisent DCOM pour les communications à distance.

   Sur l'ordinateur que vous voulez gérer à distance, ouvrez le Gestionnaire de serveur, s'il n'est pas déjà ouvert. Dans la barre des tâches Windows, cliquez sur **Gestionnaire de serveur**. Dans l'écran de **démarrage** , cliquez sur la vignette **Gestionnaire de serveur** .

2. Dans la zone **Propriétés** de la page **Serveurs locaux** , cliquez sur la valeur hypertexte de la propriété **de gestion à distance** .

3. Effectuez l'une des opérations suivantes, puis cliquez sur **OK**.

    - Pour empêcher la gestion à distance de cet ordinateur en utilisant le Gestionnaire de serveur (ou Windows PowerShell s'il est installé), désactivez la case à cocher **Activer la gestion à distance de ce serveur depuis d'autres ordinateurs**.
    - Pour permettre la gestion à distance de cet ordinateur en utilisant le Gestionnaire de serveur ou Windows PowerShell, sélectionnez **Activer la gestion à distance de ce serveur depuis d'autres ordinateurs**.

## Activer l’administration à distance via le Gestionnaire de serveur à l’aide de Windows PowerShell

1. Sur l’ordinateur que vous voulez gérer à distance, effectuez l’une des opérations ci-dessous pour ouvrir une session Windows PowerShell avec des droits d’utilisateur élevés.

    - Sur le bureau Windows, cliquez avec le bouton droit sur **Windows PowerShell** dans la barre des tâches, puis cliquez sur **Exécuter en tant qu’administrateur**.

    - Dans l’écran de **démarrage** de Windows, cliquez avec le bouton droit sur **Windows PowerShell**, puis, dans la barre de l’application, cliquez sur **Exécuter en tant qu’administrateur**.

2. tapez ce qui suit, puis **appuyez sur Entrée** pour activer toutes les exceptions de règle de pare-feu requises.

    **Configure-SMremoting.exe -enable**

## Activer l’administration à distance via le Gestionnaire de serveur dans la ligne de commande

1. Sur l’ordinateur que vous voulez gérer à distance, ouvrez une session d’invite de commandes avec des droits d’utilisateur élevés. Pour ce faire, dans l’écran **d’accueil** , tapez **cmd**, cliquez avec le bouton droit sur la vignette **d’invite de commandes** lorsqu’elle est affichée dans les résultats **des applications** , puis, dans la barre d’application, cliquez sur **Exécuter en tant qu’administrateur**.

2. Exécutez le fichier exécutable suivant :

    **%windir%\system32\Configure-SMremoting.exe**

3. Effectuez l'une des opérations suivantes :

    - Pour désactiver la gestion à distance, tapez **Configure-SMremoting.exe -disable**, puis **appuyez sur Entrée**.

    - Pour activer la gestion à distance, tapez **Configure-SMremoting.exe -enable**, puis **appuyez sur Entrée**.

    - Pour afficher le paramètre de gestion à distance actuel, tapez **Configure-SMremoting.exe -get**, puis appuyez sur Entrée.

## Activer l’administration à distance via le Gestionnaire de serveur et Windows PowerShell dans des versions antérieures de Windows Server

- Effectuez l'une des opérations suivantes :
  - Pour activer la gestion à distance sur les serveurs qui exécutent Windows Server 2012, consultez Activer la gestion à distance via le Gestionnaire de serveur à l’aide de l’interface Windows dans cette rubrique.
  - Pour activer la gestion à distance sur des serveurs qui exécutent Windows Server 2008 R2, consultez Gestion à distance avec le Gestionnaire de serveur dans l’aide de Windows Server 2008 R2.
  - Pour activer la gestion à distance sur les serveurs qui exécutent Windows Server 2008, consultez Activer et utiliser des commandes à distance dans Windows PowerShell.

## Pour configurer l’administration à distance via mmc ou un autre outil via DCOM

1. Procédez de l’une des manières suivantes pour ouvrir le composant logiciel enfichable Pare-feu Windows avec fonctions avancées de sécurité.
   - Dans la zone **Propriétés** de la page **Serveur local** dans le Gestionnaire de serveur, cliquez sur la valeur hypertexte de la propriété **pare-feu Windows** , puis sur **Paramètres avancés**.
   - Dans l’écran de **démarrage**, tapez **WF.msc**, puis cliquez sur le volet du composant logiciel enfichable lorsqu'il est affiché dans les résultats de l’onglet **Applications**.
2. Dans le volet d’arborescence, sélectionnez **Règles de trafic entrant**.
3. Vérifiez que les exceptions aux règles de pare-feu suivantes sont activées et qu’elles n’ont pas été désactivées par les paramètres de stratégie de groupe. Si certaines sont désactivées, passez à l’étape suivante.
   - Accès réseau COM+ (DCOM-In)
   - Gestion à distance des journaux des événements (NP-Entrée)
   - Gestion à distance des journaux d'événements (RPC)
   - Gestion des journaux d'événements à distance (RPC-EPMAP)

4. Cliquez avec le bouton droit sur les règles qui ne sont pas activées, puis cliquez sur **Activer la règle** dans le menu contextuel.

5. Fermez le composant logiciel enfichable Pare-feu Windows avec fonctions avancées de sécurité.

## Pour désactiver la gestion à distance à l'aide d'une stratégie de groupe

1. Procédez de l'une des manières suivantes pour ouvrir l'Éditeur de stratégie de groupe locale.

    - Sur un serveur exécutant Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012 , sur l'écran de **démarrage** , tapez **gpedit.msc**, puis cliquez sur la vignette **gpedit** quand elle est affichée.

    - Sur un serveur exécutant Windows Server 2008 R2 ou Windows Server 2008, dans la boîte de dialogue **Exécuter** , tapez **gpedit.msc**, puis **appuyez sur Entrée**.

2. Ouvrez **Configuration de l'ordinateur\Modèles d'administration\Composants Windows\Gestion à distance de Windows (WinRM)\Service WinRM**.

3. Dans le volet de contenu, double-cliquez sur **Autoriser la gestion des services à distance via WinRM**.

4. Dans la boîte de dialogue pour le paramètre de stratégie **Autoriser la gestion des services à distance via WinRM**, sélectionnez **Désactivé** pour désactiver la gestion à distance. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue paramètre de stratégie.

## Pour désactiver la gestion à distance à l'aide d'un fichier de réponses au cours d'une installation sans assistance

1. Créez un fichier de réponses d'installation sans assistance pour les installations Windows Server 2016 à l'aide du Gestionnaire d'images système Windows (Windows SIM). Pour plus d'informations sur la création d'un fichier de réponses et l'utilisation de Windows SIM, voir Qu'est-ce que Windows System Image Manager ? et Procédure pas à pas : déploiement basique de Windows pour les professionnels de l'informatique.

2. Dans votre fichier de réponses, recherchez le paramètre **Microsoft-Windows-Web-Services-for-Management-Core\EnableServerremoteManagement**.

3. Pour désactiver la gestion à distance du Gestionnaire de serveur par défaut sur tous les serveurs auxquels vous souhaitez appliquer le fichier de réponses, définissez **Microsoft-Windows-Web-Services-for-Management-Core \EnableServerremoteManagement** sur **False**.

   > ⓘ **Notes**
   >
   > Ce paramètre désactive la gestion à distance dans le cadre du processus de configuration du système d'exploitation. La configuration de ce paramètre n'empêche pas un administrateur d'activer la gestion à distance du Gestionnaire de serveur sur un serveur une fois la configuration du système d'exploitation terminée. Les administrateurs peuvent réactiver la gestion à distance du Gestionnaire de serveur en utilisant la procédure dans **Pour configurer la gestion à distance du Gestionnaire de serveur à l'aide de l'interface Windows** ou **Pour activer la gestion à distance du Gestionnaire de serveur à l'aide de Windows PowerShell** dans cette rubrique.
   >
   > Si vous désactivez la gestion à distance par défaut dans le cadre d'une installation sans assistance et que vous ne la réactivez pas sur le serveur après l'installation, les serveurs auxquels ce fichier de réponses s'applique ne peuvent pas être totalement gérés à l'aide du Gestionnaire de serveur. Les serveurs qui exécutent Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2012 (et dont la gestion à distance est désactivée par défaut) génèrent des erreurs d'état de gestion dans la console Gestionnaire de serveur après leur ajout au pool de serveurs du Gestionnaire de serveur.

# Paramètres du récepteur de la gestion distante de Windows (WinRM)

Le Gestionnaire de serveur s'appuie sur les paramètres de l'écouteur WinRM par défaut des serveurs distants que vous voulez gérer. Si le mécanisme d'authentification par défaut ou le numéro de port de l'écouteur WinRM d'un serveur distant a été modifié par rapport au paramètre par défaut, le Gestionnaire de serveur ne peut pas communiquer avec le serveur distant.

La liste ci-dessous indique les paramètres par défaut de l'écouteur WinRM pour une gestion à l'aide du Gestionnaire de serveur.

- Le service WinRM est en cours d'exécution.

- Un écouteur WinRM est créé pour accepter les demandes HTTP via le numéro de port 5985.
- Le numéro de port 5985 est activé dans les paramètres du Pare-feu Windows pour autoriser les demandes via WinRM.
- Les types d'authentification **Kerberos** et **Negotiate** sont activés.

Le numéro de port par défaut pour les communications de WinRM avec un ordinateur distant est 5985.

Pour plus d'informations sur la manière de configurer les paramètres de l'écouteur WinRM, à l'invite de commandes, saisissez **winrm help config** et appuyez sur Entrée.

# Voir aussi

Ajouter des serveurs au Gestionnaire de serveurWindows PowerShell : about_remote_Troubleshooting sur Windows Server TechCenterDescription du contrôle de compte d'utilisateur

# Ajouter des serveurs au Gestionnaire de serveur

15/08/2025

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

Dans Windows Server, vous pouvez gérer plusieurs serveurs distants en utilisant une même console du Gestionnaire de serveur. Les serveurs que vous voulez gérer en utilisant le Gestionnaire de serveur peuvent exécuter Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 ou Windows Server 2008. Notez que vous ne pouvez pas gérer une version plus récente de Windows Server avec une version antérieure du Gestionnaire de serveur.

Cette rubrique explique comment ajouter des serveurs au pool de serveurs du Gestionnaire de serveur.

> **Notes**
>
> Dans nos tests, le Gestionnaire de serveur dans Windows Server 2012 et les versions ultérieures de Windows Server peut être utilisé pour gérer jusqu'à 100 serveurs configurés avec une charge de travail standard. Le nombre de serveurs que vous pouvez gérer en utilisant une même console du Gestionnaire de serveur peut varier en fonction de la quantité de données que vous demandez aux serveurs gérés ainsi que des ressources matérielles et réseau disponibles pour l'ordinateur exécutant le Gestionnaire de serveur. Quand la quantité de données à afficher est sur le point d'atteindre la capacité des ressources de cet ordinateur, vous pouvez être confronté à des réponses lentes du Gestionnaire de serveur ainsi qu'à des retards dans les actualisations. Pour augmenter le nombre de serveurs que vous pouvez gérer en utilisant le Gestionnaire de serveur, nous recommandons de limiter la quantité de données d'événement que le Gestionnaire de serveur reçoit de vos serveurs gérés en utilisant les paramètres de la boîte de dialogue **Configurer les données d'événement**. Configurer les données d'événement peut être ouverte à partir du menu **Tâches** de la vignette **Événements** . Si vous devez gérer un grand nombre de serveurs au niveau de l'entreprise dans votre organisation, nous recommandons d'évaluer les produits de la suite Microsoft System Center .
>
> Le Gestionnaire de serveur peut recevoir uniquement des informations sur l'état en ligne ou hors connexion en provenance de serveurs exécutant Windows Server 2003. Si vous pouvez utiliser le Gestionnaire de serveur pour effectuer des tâches d'administration sur des serveurs exécutant Windows Server 2008 R2 ou Windows Server 2008, vous ne pouvez

cependant pas ajouter de rôles et de fonctionnalités aux serveurs exécutant Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003.

Le Gestionnaire de serveur ne peut pas être utilisé pour gérer une version plus récente du système d'exploitation Windows Server. Le Gestionnaire de serveur s'exécutant sur Windows Server 2012 R2, Windows Server 2012, Windows 8.1 ou Windows 8 ne peut pas être utilisé pour gérer des serveurs exécutant Windows Server 2016.

Cette rubrique contient les sections suivantes.

- Ajouter des serveurs à gérer
- Fournir des informations d'identification avec la commande Gérer en tant que

# Fournir des informations d'identification avec la commande Gérer en tant que

Quand vous ajoutez des serveurs distants au Gestionnaire de serveur, certains des serveurs que vous ajoutez peuvent demander des informations d'identification de compte utilisateur différentes pour pouvoir y accéder ou les gérer. Pour spécifier les informations d'identification d'un serveur managé différent de ceux que vous utilisez pour vous connecter à l'ordinateur sur lequel vous exécutez le Gestionnaire de serveur, utilisez la commande **Gérer en tant que** après avoir ajouté un serveur au Gestionnaire de serveur, accessible en cliquant avec le bouton droit sur l'entrée d'un serveur géré dans la vignette **Serveurs** d'un rôle ou d'une page d'accueil de groupe. Cliquez sur **Gérer sous** pour ouvrir la boîte de dialogue **Sécurité Windows** , dans laquelle vous pouvez fournir un nom d'utilisateur disposant de droits d'accès sur le serveur managé, dans l'un des formats suivants.

- *Nom d'utilisateur*
- *Nom d'utilisateur*@example.domain.com
- *Domaine**Nom d'utilisateur*

La boîte de dialogue **Sécurité Windows** ouverte par la commande **Gérer en tant** que ne peut pas accepter les informations d'identification de carte à puce ; la fourniture d'informations d'identification de carte à puce via le Gestionnaire de serveur n'est pas prise en charge. Les informations d'identification que vous fournissez pour un serveur géré à l'aide de la commande **Gérer** sous sont mises en cache et persistent tant que vous gérez le serveur à l'aide du même ordinateur sur lequel vous exécutez actuellement le Gestionnaire de serveur, ou tant que vous ne les remplacez pas en spécifiant des informations d'identification vides ou différentes pour le même serveur. Si vous exportez vos paramètres du Gestionnaire de serveur vers d'autres

ordinateurs ou configurez votre profil de domaine pour qu'il soit itinérant afin d'autoriser l'utilisation des paramètres du Gestionnaire de serveur sur d'autres ordinateurs, les informations d'identification **Gérer en tant que** serveurs dans votre pool de serveurs ne sont pas stockées dans le profil itinérant. Les utilisateurs du Gestionnaire de serveur doivent les ajouter sur chaque ordinateur à partir duquel ils veulent effectuer la gestion.

Après avoir ajouté des serveurs à gérer en suivant les procédures décrites dans cette rubrique, mais avant d'utiliser la commande **Gérer sous** pour spécifier d'autres informations d'identification qui peuvent être requises pour gérer un serveur que vous avez ajouté, les erreurs d'état de facilité de gestion suivantes peuvent être affichées pour le serveur :

- Erreur de résolution de cible Kerberos
- Erreur d'authentification Kerberos
- En ligne - Accès refusé

> ⓘ **Notes**
>
> Les rôles et fonctionnalités qui ne prennent pas en charge la commande **Gérer en tant** que incluent les services Bureau à distance (RDS) et le serveur ip de gestion des adresses IP (IPAM). Si vous ne pouvez pas gérer Services Bureau à distance (RDS) ou Serveur de gestion des adresses IP (IPAM) en utilisant les mêmes informations d'identification que celles utilisées sur l'ordinateur où le Gestionnaire de serveur s'exécute, essayez en ajoutant le compte que vous utilisez généralement pour gérer ces serveurs à distance au groupe Administrateurs sur l'ordinateur qui exécute le Gestionnaire de serveur. Ensuite, ouvrez une session sur l'ordinateur qui exécute le Gestionnaire de serveur avec le compte que vous utilisez pour gérer le serveur distant qui exécute RDS ou IPAM.

# Ajouter des serveurs à gérer

Vous pouvez ajouter des serveurs au Gestionnaire de serveur à gérer à l'aide de l'une des trois méthodes de la boîte de dialogue **Ajouter des serveurs** .

- **Active Directory Domain Services** Ajoutez des serveurs à administrer trouvés par Active Directory dans le même domaine que l'ordinateur local.
- **Entrée DNS (Domain Name System)** Recherchez les serveurs à gérer par nom d'ordinateur ou adresse IP.
- **Importer plusieurs serveurs** Spécifiez plusieurs serveurs à importer dans un fichier qui contient les serveurs listés par nom d'ordinateur ou adresse IP.

### Pour ajouter des serveurs au pool de serveurs

1. Si le Gestionnaire de serveur est déjà ouvert, passez à l'étape suivante. S'il n'est pas déjà ouvert, ouvrez-le en effectuant l'une des opérations suivantes.

    - Sur le bureau Windows, démarrez le **Gestionnaire de serveur** en cliquant sur Gestionnaire de serveur dans la barre des tâches Windows.

    - Dans l'écran de **démarrage** de Windows, cliquez sur la vignette Gestionnaire de serveur.

2. Dans le menu **Gérer** , cliquez sur **Ajouter des serveurs**.

3. Effectuez l'une des opérations suivantes.

    - Sous l'onglet **Active Directory** , sélectionnez les serveurs qui se trouvent dans le domaine actuel. **Appuyez sur Ctrl** tout en sélectionnant pour sélectionner plusieurs serveurs. Cliquez sur le bouton flèche droite pour déplacer les serveurs sélectionnés vers la liste **sélectionnée** .

    - Sous l'onglet **DNS** , tapez les premiers caractères d'un nom d'ordinateur ou d'une adresse IP, puis **appuyez sur Entrée** ou cliquez sur **Rechercher**. Sélectionnez les serveurs que vous voulez ajouter, puis cliquez sur le bouton avec la flèche droite.

    - Sous l'onglet **Importation** , recherchez un fichier texte qui contient les noms DNS ou les adresses IP des ordinateurs que vous souhaitez ajouter, un nom ou une adresse IP par ligne.

4. Une fois que vous avez terminé d'ajouter des serveurs, cliquez sur **OK**.

## Ajouter et gérer des serveurs dans des groupes de travail

Bien que l'ajout de serveurs qui se trouvent dans des groupes de travail au Gestionnaire de serveur réussisse, une fois qu'ils ont été ajoutés, la colonne **De facilité de gestion** de la vignette **Serveurs** sur un rôle ou une page de groupe de travail qui inclut un serveur de groupe de travail peut afficher **les informations d'identification non valides** qui se produisent lors de la tentative de connexion ou de collecte des données à partir du serveur de groupe de travail distant.

Ces erreurs ou des erreurs similaires peuvent se produire dans les conditions suivantes.

- Le serveur géré est dans le même groupe de travail que l'ordinateur qui exécute le Gestionnaire de serveur.

- Le serveur géré est dans un autre groupe de travail que l'ordinateur qui exécute le Gestionnaire de serveur.
- Un des ordinateurs est dans un groupe de travail, tandis que l'autre est dans un domaine.
- L'ordinateur qui exécute le Gestionnaire de serveur est dans un groupe de travail et les serveurs gérés distants sont sur un sous-réseau différent.
- Les deux ordinateurs se trouvent dans des domaines, mais il n'existe aucune relation d'approbation entre les deux domaines.
- Les deux ordinateurs se trouvent dans des domaines, mais il n'existe qu'une relation d'approbation à sens unique entre les deux domaines.
- Le serveur que vous souhaitez gérer a été ajouté à l'aide de son adresse IP.

### Pour ajouter des serveurs de groupe de travail distant au Gestionnaire de serveur

1. Sur l'ordinateur exécutant le Gestionnaire de serveur, ajoutez le nom du serveur de groupe de travail à la liste **TrustedHosts** . Cette opération est obligatoire dans le cadre de l'authentification NTLM. Pour ajouter un nom d'ordinateur à une liste existante d'hôtes approuvés, ajoutez le paramètre `Concatenate` à la commande suivante : Par exemple, pour ajouter l'ordinateur `Server01` à une liste existante d'hôtes approuvés, utilisez la commande suivante :

   ```
   Set-Item wsman:\localhost\Client\TrustedHosts Server01 -Concatenate -force
   ```

2. Déterminez si le serveur de groupe de travail que vous voulez gérer se trouve sur le même sous-réseau que l'ordinateur sur lequel vous exécutez le Gestionnaire de serveur.

   Si les deux ordinateurs se trouvent dans le même sous-réseau ou si le profil réseau du serveur de groupe de travail est défini sur **Privé** dans le **Centre de partage et** de réseau, passez à l'étape suivante.

   S'ils ne se trouvent pas dans le même sous-réseau ou si le profil réseau du serveur de groupe de travail n'est pas défini sur **Privé**, sur le serveur de groupe de travail, modifiez le paramètre de **gestion à distance Windows entrant (HTTP-In)** dans le Pare-feu Windows pour autoriser explicitement les connexions à partir d'ordinateurs distants en ajoutant les noms d'ordinateurs sous l'onglet **Ordinateurs** de la boîte de dialogue **Propriétés** du paramètre.

3. > **ⓘ Important**
   >
   > L'exécution de l'applet de commande à cette étape a pour effet de remplacer les mesures de Contrôle de compte d'utilisateur (UAC) qui empêchent l'exécution de processus élevés sur les ordinateurs de groupe de travail, sauf si le compte Administrateur ou Système intégré exécute ces processus. L'applet de commande permet aux membres du groupe Administrateurs de gérer le serveur de groupe de travail sans se connecter via le compte Administrateur intégré. En autorisant des utilisateurs supplémentaires à gérer le serveur de groupe de travail, vous pouvez réduire la sécurité de ce dernier. Cette opération est néanmoins plus sûre que de fournir les informations d'identification d'un compte Administrateur intégré à une multitude possible de personnes chargées de gérer le serveur de groupe de travail.

   Pour remplacer les restrictions UAC sur l'exécution de processus élevés sur les ordinateurs de groupe de travail, créez une entrée de Registre appelée **LocalAccountTokenFilterPolicy** sur le serveur de groupe de travail en exécutant l'applet de commande suivante.

   ```
   New-ItemProperty -Name LocalAccountTokenFilterPolicy -path
   HKLM:\SOFTWARE\Microsoft\Windows\Currentversion\Policies\System -propertytype
   DWord -value 1
   ```

4. Sur l'ordinateur sur lequel vous exécutez le Gestionnaire de serveur, ouvrez la page **Tous les serveurs** .

5. Si l'ordinateur qui exécute le Gestionnaire de serveur et le serveur de groupe de travail cible se trouvent dans le même groupe de travail, passez à la dernière étape. Si les deux ordinateurs ne se trouvent pas dans le même groupe de travail, cliquez avec le bouton droit sur le serveur de groupe de travail cible dans la vignette **Serveurs** , puis cliquez sur **Gérer en tant que**.

6. Connectez-vous au serveur de groupe de travail à l'aide du compte Administrateur intégré de ce dernier.

7. Vérifiez que le Gestionnaire de serveur est en mesure de se connecter au serveur de groupe de travail et de collecter des données à partir du serveur de groupe de travail en actualisant la page **Tous les serveurs** , puis en affichant l'état de facilité de gestion pour le serveur de groupe de travail.

### Pour ajouter des serveurs distants lorsque le Gestionnaire de serveur fonctionne sur un ordinateur de groupe de travail

1. Sur l'ordinateur exécutant le Gestionnaire de serveur, ajoutez des serveurs distants à la liste **TrustedHosts** de l'ordinateur local dans une session Windows PowerShell. Pour ajouter un nom d'ordinateur à une liste existante d'hôtes approuvés, ajoutez le paramètre `Concatenate` à la commande suivante : Par exemple, pour ajouter l'ordinateur `Server01` à une liste existante d'hôtes approuvés, utilisez la commande suivante :

   ```
   Set-Item wsman:\localhost\Client\TrustedHosts Server01 -Concatenate -force
   ```

2. Déterminez si le serveur que vous voulez gérer se trouve sur le même sous-réseau que l'ordinateur du groupe de travail sur lequel vous exécutez le Gestionnaire de serveur.

   Si les deux ordinateurs se trouvent dans le même sous-réseau ou si le profil réseau de l'ordinateur de groupe de travail est défini sur **Privé** dans le **Centre de partage et** de réseau, passez à l'étape suivante.

   S'ils ne se trouvent pas dans le même sous-réseau ou si le profil réseau de l'ordinateur du groupe de travail n'est pas défini sur **Privé**, sur l'ordinateur du groupe de travail exécutant le Gestionnaire de serveur, modifiez le paramètre **de gestion à distance Windows entrant (HTTP-In)** dans le Pare-feu Windows pour autoriser explicitement les connexions à partir d'ordinateurs distants en ajoutant les noms d'ordinateurs sous l'onglet **Ordinateurs** de la boîte de dialogue **Propriétés** du paramètre.

3. Sur l'ordinateur sur lequel vous exécutez le Gestionnaire de serveur, ouvrez la page **Tous les serveurs** .

4. vérifiez que le Gestionnaire de serveur est en mesure de se connecter au serveur distant et de collecter des données à partir du serveur distant en actualisant la page **Tous les serveurs** , puis en affichant l'état de facilité de gestion pour le serveur distant. Si la vignette **Serveurs** affiche toujours une erreur de facilité de gestion pour le serveur distant, passez à l'étape suivante.

5. Déconnectez-vous de l'ordinateur sur lequel vous exécutez le Gestionnaire de serveur, puis reconnectez-vous en utilisant le compte Administrateur intégré. Répétez l'étape précédente pour vérifier que le Gestionnaire de serveur peut se connecter au serveur distant et y collecter des données.

si vous avez suivi les procédures décrites dans cette section et que vous continuez à avoir des problèmes de gestion des ordinateurs de groupe de travail ou de gestion d'autres ordinateurs

à partir d'ordinateurs de groupe de travail, consultez about_remote_Troubleshooting sur le site web Microsoft.

## Ajouter et gérer des serveurs dans des clusters

Vous pouvez utiliser le Gestionnaire de serveur pour gérer les serveurs qui se trouvent dans des clusters de basculement (également appelés « clusters de serveur » ou MSCS). Les serveurs qui se trouvent dans des clusters de basculement (que les nœuds de cluster soient physiques ou virtuels) ont des comportements et des contraintes de gestion spécifiques dans le Gestionnaire de serveur.

- Les serveurs physiques et virtuels dans des clusters sont ajoutés automatiquement au Gestionnaire de serveur quand un des serveurs du cluster est ajouté au Gestionnaire de serveur. De même, quand vous supprimez un serveur en cluster dans le Gestionnaire de serveur, vous êtes invité à supprimer les autres serveurs du cluster.
- Le Gestionnaire de serveur n'affiche pas de données pour les serveurs virtuels en cluster, car les données sont dynamiques et elles sont identiques à celles du serveur sur lequel le nœud en cluster virtuel est hébergé. Vous pouvez sélectionner le serveur qui héberge le serveur virtuel pour afficher ses données.
- Si vous ajoutez un serveur au Gestionnaire de serveur en utilisant le nom d'objet du cluster virtuel du serveur, le nom d'objet virtuel s'affiche dans le Gestionnaire de serveur, au lieu du nom de serveur physique (attendu).
- Vous ne pouvez pas installer de rôles et de fonctionnalités sur un serveur virtuel en cluster.

# Voir aussi

Gestionnaire de serveurscréer et gérer des groupes de serveurs

# Ajouter ou supprimer des rôles et des fonctionnalités dans Windows Server

16/08/2025

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

Dans Windows Server, la console du Gestionnaire de serveur et les applets de commande Windows PowerShell pour le Gestionnaire de serveur vous permettent d'ajouter des rôles et des fonctionnalités à un serveur local ou distant, ou un disque dur virtuel hors connexion (VHD). Vous pouvez ajouter plusieurs rôles et fonctionnalités en même temps. Cet article explique comment ajouter ou supprimer des rôles et des fonctionnalités dans Windows Server, y compris plusieurs serveurs simultanément.

Pour plus d'informations sur les rôles et fonctionnalités disponibles dans Windows Server, consultez Comparaison des éditions de Windows Server.

## Prerequisites

Avant d'ajouter ou de supprimer des rôles, des services de rôle et des fonctionnalités, vérifiez que vous remplissez les conditions préalables suivantes :

- Utilisez un compte d'utilisateur administrateur. Vous devez également être administrateur sur tous les serveurs distants que vous gérez à l'aide du Gestionnaire de serveur ou des disques durs virtuels hors connexion que vous montez.
- Passez en revue et comprenez les dépendances ou conditions préalables spécifiques aux rôles ou fonctionnalités que vous envisagez d'ajouter, car certains rôles peuvent nécessiter une configuration ou des services supplémentaires pour fonctionner correctement. Pour plus d'informations, consultez Configurer des fonctionnalités à la demande dans Windows Server.
- Fournissez le support d'installation ou un autre chemin source pour les fichiers requis pour ajouter certaines fonctionnalités, telles que .NET Framework 3.5.
- Pour ajouter des rôles et des fonctionnalités sur des serveurs distants, ajoutez-les au Gestionnaire de serveur. Pour plus d'informations sur l'ajout de serveurs au Gestionnaire de serveur, consultez Ajouter des serveurs au Gestionnaire de serveur.
- Pour ajouter des rôles et des fonctionnalités à un disque dur virtuel hors connexion, le disque dur virtuel cible doit répondre aux exigences suivantes :

- Le disque dur virtuel doit exécuter la version de Windows Server qui correspond à la version du serveur sur lequel le disque dur virtuel est monté.
- Vérifiez que les fichiers VHD ne sont pas utilisés par d'autres processus ou montés ailleurs.
- Le disque dur virtuel (VHD) ne peut pas avoir plus d'un volume ou partition système.
- Pour un disque dur virtuel stocké sur un dossier partagé réseau, vous devez accorder des autorisations **de lecture** et d'écriture au compte d'ordinateur (ou système local) du serveur que vous sélectionnez pour monter le disque dur virtuel. L'accès au compte utilisateur uniquement n'est pas suffisant.

> ⓘ **Notes**
>
> - Vous pouvez ajouter des rôles et des fonctionnalités sur des serveurs distants avec le Gestionnaire de serveur sur la même version de Windows Server ou une version antérieure. Cette exigence inclut l'utilisation de la version de client Windows équivalente avec les outils d'administration de serveur distant (RSAT). Par exemple, Windows Server 2025 peut également ajouter des rôles et des fonctionnalités sur Windows Server 2022, mais Windows Server 2022 ne peut pas ajouter de rôles et de fonctionnalités sur Windows Server 2025.
>
> - Cet article ne couvre pas l'ajout de rôles Services Bureau à distance (RDS), qui a un processus d'installation différent dans le Gestionnaire de serveur. Pour plus d'informations sur l'ajout de rôles RDS, consultez Déployer un environnement services Bureau à distance.

# Ajouter des rôles et des fonctionnalités à Windows Server

Vous pouvez ajouter des rôles et des fonctionnalités sur un serveur local, un serveur distant ajouté au Gestionnaire de serveur ou un disque dur virtuel hors connexion, à l'aide de **l'Assistant Ajout de rôles et de fonctionnalités** dans le Gestionnaire de serveur, ou à l'aide d'applets de commande Windows PowerShell.

Sélectionnez l'onglet approprié.

Assistant des rôles et fonctions

Pour ajouter des rôles et des fonctionnalités à l'aide de l'Assistant Rôles et fonctionnalités dans le Gestionnaire de serveur, procédez comme suit :

1. Ouvrez le menu Démarrer, tapez **Le Gestionnaire de serveur**, puis ouvrez **le Gestionnaire de serveur**.

2. Sélectionnez **Gérer** dans le coin supérieur droit, puis sélectionnez **Ajouter des rôles et des fonctionnalités**. L'Assistant **Ajout de rôles et de fonctionnalités** s'ouvre.

3. Pour **avant de commencer**, passez en revue les informations, puis sélectionnez **Suivant**.

4. Pour **le type d'installation**, sélectionnez **Installation basée sur un rôle ou une fonctionnalité**, puis sélectionnez **Suivant**. Utilisez cette option pour ajouter tous les rôles et fonctionnalités à l'exception des services Bureau à distance. Pour plus d'informations sur l'ajout de rôles RDS, consultez Déployer un environnement services Bureau à distance.

5. Pour la **sélection** du serveur, sélectionnez le serveur sur lequel vous souhaitez ajouter des rôles et des fonctionnalités. Vous pouvez choisir le serveur local ou un serveur distant ajouté au Gestionnaire de serveur. Si vous souhaitez ajouter des rôles et fonctionnalités sur un disque dur virtuel hors connexion, sélectionnez **Sélectionner un disque dur virtuel**, sélectionnez le serveur sur lequel monter le disque dur virtuel, puis parcourez ou entrez son chemin d'accès au fichier. Cliquez sur **Suivant**.

6. Pour **les rôles de serveur**, sélectionnez les rôles que vous souhaitez ajouter. Vous n'avez pas besoin de sélectionner de rôles si vous souhaitez uniquement ajouter une fonctionnalité. Une fois que vous avez effectué vos sélections de rôle, sélectionnez **Suivant**.

   À mesure que vous poursuivez, l'Assistant vous informe automatiquement si des conflits se trouvent sur le serveur de destination qui peuvent empêcher l'ajout de rôles ou de fonctionnalités sélectionnés ou une opération normale. Vous êtes également invité à ajouter d'autres rôles et fonctionnalités nécessaires pour les rôles ou fonctionnalités que vous sélectionnez.

   Si vous envisagez de gérer le rôle à distance, soit à partir d'un autre serveur, soit à partir d'un ordinateur windows qui exécute les outils d'administration de serveur distant (RSAT), vous pouvez choisir de ne pas installer les outils de gestion et les composants logiciels enfichables pour les rôles sur le serveur de destination. Par défaut, les outils de gestion sont ajoutés.

7. Pour **fonctionnalités**, sélectionnez les rôles que vous souhaitez ajouter. Vous n'avez pas besoin de sélectionner de fonctionnalités si vous souhaitez uniquement ajouter un rôle. Une fois que vous avez effectué vos sélections de fonctionnalités, sélectionnez **Suivant**.

8. Pour **confirmation**, passez en revue les rôles et fonctionnalités que vous avez sélectionnés. Une fois que vous êtes prêt, sélectionnez **Installer**. Certains rôles et fonctionnalités vous obligent à redémarrer le serveur après l'installation. Cochez la case **Redémarrer automatiquement le serveur de destination si nécessaire** si vous souhaitez que le serveur redémarre automatiquement après l'installation.

   > **Conseil**
   >
   > Si vous devez spécifier les fichiers sources d'installation, sélectionnez **Spécifier un autre chemin source**. Vous pouvez également spécifier un fichier WIM (Windows Imaging) au format suivant, avec `WIM` comme préfixe et l'index dans lequel les fichiers de fonctionnalités se trouvent sous la forme d'un suffixe, par exemple `WIM:e:\sources\install.wim:4`. Toutefois, vous ne pouvez pas utiliser un fichier WIM directement comme source pour ajouter des rôles et des fonctions à un VHD hors ligne. Vous devez monter le disque dur virtuel hors connexion et pointer vers son chemin de montage pour les fichiers sources, ou pointer vers un dossier qui contient une copie du contenu du fichier WIM. Le chemin d'accès source ou le partage de fichiers doit accorder des autorisations **de lecture** au compte d'ordinateur du serveur de destination ; accorder l'accès au compte d'utilisateur n'est pas suffisant. Pour plus d'informations sur la liste des index dans un fichier **WIM, consultez Répertorier les images contenues dans un fichier WIM ou VHD**.
   >
   > Vous pouvez aussi exporter vos sélections dans un fichier de configuration XML utilisable pour effectuer des installations sans assistance avec Windows PowerShell. Pour exporter la configuration que vous avez spécifiée, sélectionnez **Exporter les paramètres de configuration**, puis enregistrez le fichier XML dans un emplacement pratique. Vous trouverez les étapes à suivre pour utiliser ce fichier de configuration dans la section **Ajouter des rôles et des fonctionnalités sur plusieurs serveurs**.

9. Une fois l'installation terminée, sélectionnez **Fermer**.

# Supprimer des rôles et des fonctionnalités de Windows Server

Vous pouvez supprimer des rôles et des fonctionnalités sur un serveur local, un serveur distant ajouté au Gestionnaire de serveur ou un disque dur virtuel hors connexion, à l'aide de

**l'Assistant Suppression de rôles et de fonctionnalités** dans le Gestionnaire de serveur ou à l'aide d'applets de commande Windows PowerShell.

Sélectionnez l'onglet approprié.

Assistant des rôles et fonctions

Pour supprimer des rôles et des fonctionnalités à l'aide de l'Assistant Rôles et fonctionnalités dans le Gestionnaire de serveur, procédez comme suit :

1. Ouvrez le menu Démarrer, tapez **Le Gestionnaire de serveur**, puis ouvrez **le Gestionnaire de serveur**.

2. Sélectionnez **Gérer** dans le coin supérieur droit, puis sélectionnez **Supprimer les rôles et les fonctionnalités**. **L'Assistant Suppression de rôles et de fonctionnalités** s'ouvre.

3. Pour **avant de commencer**, passez en revue les informations, puis sélectionnez **Suivant**.

4. Pour la **sélection** du serveur, sélectionnez le serveur sur lequel vous souhaitez supprimer des rôles et des fonctionnalités. Vous pouvez choisir le serveur local ou un serveur distant ajouté au Gestionnaire de serveur. Si vous souhaitez supprimer des rôles et des fonctionnalités sur un disque dur virtuel hors connexion, sélectionnez **un disque dur virtuel**, sélectionnez le serveur sur lequel monter le disque dur virtuel, puis parcourez ou entrez son chemin d'accès au fichier. Cliquez sur **Suivant**.

5. Pour **les rôles de serveur**, sélectionnez les rôles que vous souhaitez supprimer. Vous n'avez pas besoin de sélectionner de rôles si vous souhaitez uniquement supprimer une fonctionnalité. Une fois que vous avez effectué vos sélections de rôle, sélectionnez **Suivant**.

   Au fur et à mesure que vous avancez, l'assistant vous invite automatiquement à supprimer tous les autres rôles et fonctionnalités requis par les rôles ou fonctionnalités que vous sélectionnez.

6. Pour **les fonctionnalités**, sélectionnez les rôles que vous souhaitez supprimer. Vous n'avez pas à sélectionner de fonctionnalités si vous souhaitez uniquement supprimer un rôle. Une fois que vous avez effectué vos sélections de fonctionnalités, sélectionnez **Suivant**.

7. Pour **confirmation**, passez en revue les rôles et fonctionnalités que vous avez sélectionnés. Une fois que vous êtes prêt, sélectionnez **Supprimer**. Certains rôles et fonctionnalités vous obligent à redémarrer le serveur après la suppression. Cochez la

case **Redémarrer automatiquement le serveur de destination si nécessaire** si vous souhaitez que le serveur redémarre automatiquement après la suppression.

8. Une fois la suppression terminée, sélectionnez **Fermer**.

## Agent virtuel

Si vous rencontrez des problèmes lors de l'installation ou de la suppression de rôles et de fonctionnalités, vous pouvez essayer notre agent virtuel. Il peut vous aider à identifier et résoudre rapidement les problèmes liés aux rôles et fonctionnalités.

Essayer notre agent virtuel

## Contenu connexe

Configurer des fonctionnalités à la demande

ⓘ **Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

# Configurer des fonctionnalités à la demande dans Windows Server

15/08/2025

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

Cette rubrique décrit comment supprimer des fichiers de fonctionnalités dans une configuration de type Fonctionnalités à la demande en utilisant l'applet de commande Uninstall-WindowsFeature.

Les fonctionnalités à la demande sont une fonctionnalité, introduite dans Windows 8 et Windows Server 2012, qui vous permet de supprimer des fichiers de rôle et de fonctionnalités (parfois appelés charge *utile* de fonctionnalité) du système d'exploitation pour économiser de l'espace disque, et d'installer des rôles et des fonctionnalités à partir d'emplacements distants ou de supports d'installation au lieu d'ordinateurs locaux. Vous pouvez supprimer des fichiers de fonctionnalités d'ordinateurs virtuels ou physiques en cours d'exécution. Vous pouvez également ajouter ou supprimer des fichiers de fonctionnalités dans les fichiers WIM (Windows Image) ou les disques durs virtuels hors connexion pour créer une copie reproductible des configurations de type Fonctionnalités à la demande.

Dans une configuration de type Fonctionnalités à la demande, quand des fichiers de fonctionnalités ne sont pas disponibles sur un ordinateur et qu'ils sont requis par une installation, vous pouvez spécifier que Windows Server 2012 R2 ou Windows Server 2012 doit récupérer ces fichiers dans un magasin de fonctionnalités côte à côte (un dossier partagé contenant des fichiers de fonctionnalités et accessible à l'ordinateur sur le réseau), depuis Windows Update ou des supports d'installation. Par défaut, lorsque les fichiers de fonctionnalités ne sont pas disponibles sur le serveur cible, Fonctionnalités à la demande recherche les fichiers de fonctionnalités manquants en effectuant les tâches suivantes, dans l'ordre indiqué.

1. Recherche à un emplacement spécifié par des utilisateurs de l'Assistant Ajout de rôles et de fonctionnalités ou de commandes d'installation DISM
2. Évaluation de la configuration du paramètre de stratégie de groupe, **configuration ordinateur\Modèles d'administration\System\Spécifier les paramètres pour l'installation facultative des composants et la réparation des composants**
3. Recherche sur Windows Update

Vous pouvez remplacer le comportement par défaut de Fonctionnalités à la demande en effectuant l'une des opérations suivantes.

- Spécification d'un autre chemin d'accès source dans le cadre de l'applet de commande `Install-WindowsFeature`, en ajoutant le paramètre `Source`
- Spécification d'un autre chemin source dans la page **Confirmer l'installation des options** pendant que vous installez des fonctionnalités à l'aide de l'Assistant Ajout de rôles et de fonctionnalités
- Configuration du paramètre de stratégie de groupe, **spécifier les paramètres pour l'installation facultative des composants et la réparation des composants**

Cette rubrique contient les sections suivantes.

- Créer un fichier de fonctionnalités ou un magasin côte à côte
- Méthodes de suppression des fichiers de fonctionnalités
- Supprimer des fichiers de fonctionnalités à l'aide de Uninstall-WindowsFeature

# Créer un fichier de fonctionnalités ou un magasin côte à côte

Cette section décrit comment configurer un dossier partagé de fichiers de fonctionnalités distant (également appelé « magasin côte à côte ») qui stocke les fichiers nécessaires pour installer des rôles, des services de rôle et des fonctionnalités sur des serveurs exécutant Windows Server 2012 R2 ou Windows Server 2012. Après avoir configuré un magasin de fonctionnalités, vous pouvez installer des rôles, des services de rôle et des fonctionnalités sur des serveurs qui exécutent ces systèmes d'exploitation, et spécifier le magasin de fonctionnalités comme emplacement des fichiers sources d'installation.

## Pour créer un magasin de fichiers de fonctionnalités

1. Créez un dossier partagé sur un serveur de votre réseau. Par exemple, *network**share**sxs*.
2. Vérifiez que les autorisations appropriées sont affectées au magasin de fonctionnalités. Le chemin d'accès source ou le partage de fichiers doit accorder des autorisations **de lecture** au groupe **Tout le monde** (non recommandé pour des raisons de sécurité), ou aux comptes d'ordinateur (*DOMAIN**SERverNAME*$) des serveurs sur lesquels vous envisagez d'installer des fonctionnalités à l'aide de ce magasin de fonctionnalités ; l'octroi de l'accès au compte d'utilisateur n'est pas suffisant.

   Vous pouvez accéder aux paramètres du partage de fichiers et des autorisations en effectuant l'une des opérations suivantes sur le Bureau Windows.

- Cliquez avec le bouton droit sur le dossier partagé, cliquez sur **Propriétés**, puis modifiez les utilisateurs autorisés et leurs droits d'accès au dossier sous l'onglet **Sécurité** .

- Cliquez avec le bouton droit sur le dossier partagé, pointez sur **Partager avec**, puis cliquez sur **Personnes spécifiques**.

> ⓘ **Notes**
>
> Les serveurs qui se trouvent dans des groupes de travail ne peuvent pas accéder aux partages de fichiers externes, même si le compte d'ordinateur du serveur de groupe de travail dispose d'autorisations **de lecture** sur le partage externe. D'autres emplacements sources qui fonctionnent pour les serveurs de groupes de travail sont notamment les supports d'installation, Windows Update, et les disques durs virtuels ou les fichiers WIM qui sont stockés sur le serveur de groupe de travail local.

3. Copiez le dossier **Sources\SxS** de votre support d'installation Windows Server vers le dossier partagé que vous avez créé à l'étape 1.

## Installer le .NET Framework 3.5 et d'autres fonctionnalités à la demande

À compter de Windows Server 2012 et Windows 8, les fichiers de fonctionnalités pour .NET Framework 3.5 (qui incluent .NET Framework 2.0 et .NET Framework 3.0) ne sont pas disponibles sur l'ordinateur local par défaut. Les fichiers ont été supprimés. Les fichiers de fonctionnalités qui ont été supprimés dans une configuration Fonctionnalités à la demande, ainsi que les fichiers de fonctionnalités pour le .NET Framework 3.5, sont disponibles par le biais de Windows Update. Par défaut, si des fichiers de fonctionnalités ne sont pas disponibles sur le serveur de destination qui exécute Windows Server 2012 ou des versions ultérieures, le processus d'installation recherche les fichiers manquants en se connectant à Windows Update. Vous pouvez remplacer le comportement par défaut en configurant un paramètre de stratégie de groupe ou en spécifiant un autre chemin source lors de l'installation, que vous utilisiez l'interface graphique de l'Assistant Ajout de rôles et de fonctionnalités ou une ligne de commande.

Vous pouvez installer le .NET Framework 3.5 en effectuant l'une des opérations suivantes :

- Appliquez la procédure Pour installer le .NET Framework 3.5 en exécutant l'applet de commande Install-WindowsFeature pour ajouter le paramètre `Source` et spécifiez une source à partir de laquelle obtenir les fichiers de fonctionnalités .NET Framework 3.5. Si vous n'ajoutez pas le paramètre `Source` , le processus d'installation détermine d'abord si

un chemin d'accès aux fichiers de fonctionnalités a été spécifié par des paramètres de stratégie de groupe et, si aucun chemin d'accès n'est trouvé, il recherche les fonctionnalités manquantes à l'aide de Windows Update.

- Utilisez Pour installer le .NET Framework 3.5 en utilisant l'Assistant Ajout de rôles et de fonctionnalités pour spécifier un autre emplacement de fichier source dans la page **Confirmer les options d'installation** de l'Assistant Ajout de rôles et de fonctionnalités.

- Appliquez la procédure Pour installer le .NET Framework 3.5 à l'aide de DISM pour obtenir des fichiers à partir de Windows Update par défaut ou en spécifiant un chemin d'accès source vers le support d'installation.

Configurez d'autres sources pour les fichiers de fonctionnalités dans la stratégie de groupe pour le .NET Framework 3.5 ou d'autres fonctionnalités, si les fichiers de fonctionnalités sont introuvables sur l'ordinateur local.

> ⓘ **Important**
>
> Lorsque vous installez des fichiers de fonctionnalités à partir d'une source distante, le chemin d'accès source ou le partage de fichiers doit accorder des autorisations **de lecture** au groupe **Tout le monde** (non recommandé pour des raisons de sécurité) ou au compte ordinateur (système local) du serveur de destination ; accorder l'accès au compte d'utilisateur n'est pas suffisant.
>
> Les serveurs qui se trouvent dans des groupes de travail ne peuvent pas accéder aux partages de fichiers externes, même si le compte d'ordinateur du serveur de groupe de travail dispose d'autorisations **de lecture** sur le partage externe. D'autres emplacements sources qui fonctionnent pour les serveurs de groupes de travail sont notamment les supports d'installation, Windows Update, et les disques durs virtuels ou les fichiers WIM qui sont stockés sur le serveur de groupe de travail local.
>
> Vous pouvez spécifier un fichier WIM comme autre source du fichier de fonctionnalités quand vous installez des rôles, des services de rôle et des fonctionnalités sur un serveur physique en cours d'exécution. Le chemin source d'un fichier WIM doit être au format suivant, avec **WIM** comme préfixe et l'index dans lequel les fichiers de fonctionnalités se trouvent sous la forme d'un suffixe : **WIM :e :\sources\install.wim :4**. Cependant, vous ne pouvez pas ajouter un fichier WIM directement comme source pour l'installation de rôles, de services de rôle et de fonctionnalités sur un disque dur virtuel hors connexion : vous devez monter le disque dur virtuel hors connexion et pointer vers son chemin de montage pour les fichiers sources, ou pointer vers un dossier contenant une copie du contenu du fichier WIM.

## Pour installer le .NET Framework 3.5 à l'aide de l'applet de commande Install-WindowsFeature

1. Effectuez une des opérations suivantes pour ouvrir une session Windows PowerShell avec des droits utilisateur élevés.

   > ⓘ **Notes**
   >
   > Si vous installez des rôles et des fonctionnalités depuis un serveur distant, vous n'avez pas besoin d'exécuter Windows PowerShell avec des droits d'utilisateur élevés.

   - Sur le bureau Windows, cliquez avec le bouton droit sur **Windows PowerShell** dans la barre des tâches, puis cliquez sur **Exécuter en tant qu'administrateur**.
   - Dans l'écran de **démarrage** de Windows, cliquez avec le bouton droit sur la vignette Windows PowerShell, puis, dans la barre d'application, cliquez sur **Exécuter en tant qu'administrateur**.
   - Sur un serveur exécutant l'option d'installation Server Core de Windows Server 2012 R2 ou Windows Server 2012, tapez **PowerShell** dans une invite de commandes, puis **appuyez sur Entrée**.

2. tapez la commande suivante, puis **appuyez sur Entrée**. Dans l'exemple suivant, les fichiers sources se trouvent dans un magasin côte à côte (abrégé en tant que **SxS**) dans le support d'installation sur le lecteur D.

   ```
   Install-WindowsFeature NET-Framework-Core -Source D:\Sources\SxS
   ```

   Si vous voulez que la commande utilise Windows Update comme source pour les fichiers de fonctionnalités manquants ou si une source par défaut a déjà été configurée par la stratégie de groupe, il est inutile d'ajouter le paramètre `Source` , à moins que vous ne souhaitiez spécifier une source différente.

## Pour installer le .NET Framework 3.5 en utilisant l'Assistant Ajout de rôles et de fonctionnalités

1. Dans le menu **Gérer** dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.

2. Sélectionnez un serveur de destination qui exécute Windows Server 2016.

3. Dans la page **Sélectionner les fonctionnalités** de l'Assistant Ajout de rôles et de fonctionnalités, sélectionnez **.NET Framework 3.5**.

4. Si l'ordinateur local y est autorisé par les paramètres de stratégie de groupe, le processus d'installation tente d'obtenir les fichiers de fonctionnalités manquants à l'aide de Windows Update. Cliquez sur **Installer** ; vous n'avez pas besoin de passer à l'étape suivante.

   Si les paramètres de stratégie de groupe ne vous autorisent à le faire ou si vous voulez utiliser une autre source pour les fichiers de fonctionnalités du .NET Framework 3.5, dans la page **Confirmer les sélections d'installation** de l'Assistant, cliquez sur **Spécifier un autre chemin d'accès source**.

5. Fournissez un chemin d'accès à un magasin côte à côte (appelé **SxS**) dans le support d'installation ou dans un fichier WIM. Dans l'exemple suivant, le support d'installation se trouve sur le disque D.

   **D:\Sources\SxS**

   Pour spécifier un fichier WIM, ajoutez un préfixe **WIM :** et ajoutez l'index de l'image à utiliser dans le fichier WIM en tant que suffixe, comme illustré dans l'exemple suivant.

   **WIM:***server_name***\share\install.wim:3**

6. Cliquez sur **OK**, puis sur **Installer**.

## Pour installer le .NET Framework 3.5 à l'aide de DISM

1. Effectuez une des opérations suivantes pour ouvrir une session Windows PowerShell avec des droits utilisateur élevés.

   > ⓘ **Notes**
   >
   > Si vous installez des rôles et des fonctionnalités depuis un serveur distant, vous n'avez pas besoin d'exécuter Windows PowerShell avec des droits d'utilisateur élevés.

   - Sur le bureau Windows, cliquez avec le bouton droit sur **Windows PowerShell** dans la barre des tâches, puis cliquez sur **Exécuter en tant qu'administrateur**.
   - Dans l'écran de **démarrage** de Windows, cliquez avec le bouton droit sur la vignette Windows PowerShell, puis, dans la barre d'application, cliquez sur **Exécuter en tant**

**qu'administrateur**.

- Sur un serveur exécutant l'option d'installation server Core, tapez **PowerShell** dans une invite de commandes, puis **appuyez sur Entrée**.

2. Exécutez l'une des commandes DISM suivantes.

   - Si l'ordinateur a accès à Windows Update ou si un emplacement de fichier source par défaut a déjà été configuré dans la stratégie de groupe, exécutez la commande suivante.

     ```
     DISM /online /Enable-Feature /Featurename:NetFx3 /All
     ```

   - Si l'ordinateur a accès au support d'installation, exécutez une commande similaire à la suivante. Dans l'exemple suivant, le support d'installation du système d'exploitation se trouve sur le disque D. Le paramètre `LimitAccess` empêche la commande d'essayer de contacter Windows Update ou un serveur qui exécute les services WSUS.

     ```
     DISM /online /Enable-Feature /Featurename:NetFx3 /All /LimitAccess
     /Source:d:\sources\sxs
     ```

> ⓘ **Notes**
>
> La DISM respecte la casse.

## Configurer d'autres sources pour les fichiers de fonctionnalités dans la stratégie de groupe

Le paramètre de stratégie de groupe décrit dans cette section spécifie les emplacements sources autorisés pour les fichiers du .NET Framework 3.5 et d'autres fichiers de fonctionnalités qui ont été supprimés dans le cadre d'une configuration Fonctionnalités à la demande. Le paramètre de stratégie **Spécifier des paramètres pour l'installation des composants facultatifs et la réparation de composants** se trouve dans le dossier **Configuration ordinateur\Modèles d'administration\Système** dans la Console de gestion des stratégies de groupe ou l'Éditeur de stratégie de groupe locale.

> ⓘ **Notes**
>
> Vous devez être membre du groupe Administrateurs pour modifier des paramètres de stratégie de groupe sur l'ordinateur local. Si les paramètres de stratégie de groupe de l'ordinateur que vous voulez gérer sont contrôlés au niveau du domaine, vous devez être membre du groupe Administrateurs du domaine pour modifier des paramètres de stratégie de groupe.

### Pour configurer un autre chemin d'accès source par défaut dans la stratégie de groupe

1. Dans l'Éditeur de stratégie de groupe locale ou la Console de gestion des stratégies de groupe, ouvrez le paramètre de stratégie suivant.

   **Configuration ordinateur\Modèles d'administration\Système\Spécifier des paramètres pour l'installation des composants facultatifs et la réparation de composants**

2. Sélectionnez **Activé** pour activer le paramètre de stratégie, s'il n'est pas déjà activé.

3. Dans la zone de texte **Autre chemin d'accès au fichier source** dans la zone **Options**, spécifiez un chemin d'accès complet à un dossier partagé ou un fichier WIM. Pour spécifier un fichier WIM comme autre emplacement de fichier source, ajoutez le préfixe **WIM :** au chemin d'accès et ajoutez l'index de l'image à utiliser dans le fichier WIM en tant que suffixe. Voici quelques exemples de valeurs que vous pouvez spécifier.

   - chemin d'accès à un dossier partagé : *****server_name***\share***folder_name*
   - chemin d'accès à un fichier WIM, dans lequel **3** représente l'index de l'image dans laquelle les fichiers de fonctionnalités sont trouvés :
     **WIM :***server_name***\share\install.wim :3**

4. Si vous ne voulez pas que les ordinateurs contrôlés par ce paramètre de stratégie recherchent les fichiers manquants sur Windows Update, sélectionnez **Ne jamais télécharger la charge utile à partir de Windows Update**.

5. Si les ordinateurs contrôlés par ce paramètre de stratégie reçoivent généralement des mises à jour par le biais des services WSUS, mais que vous préférez passer par Windows Update plutôt que par les services WSUS pour rechercher les fichiers manquants, sélectionnez **Contacter Windows Update directement pour télécharger le contenu de réparation au lieu de Windows Server Update Services (WSUS)**.

6. Cliquez sur **OK** lorsque vous avez terminé de modifier ce paramètre de stratégie, puis fermez l'éditeur de stratégie de groupe.

# Méthodes de suppression des fichiers de fonctionnalités

Deux méthodes sont disponibles pour supprimer des fichiers de fonctionnalités de Windows Server dans une configuration de type Fonctionnalités à la demande.

- Le paramètre `remove` de la cmdlet `Uninstall-WindowsFeature` vous permet de supprimer des fichiers de fonctionnalités d'un serveur ou d'un disque dur virtuel hors connexion exécutant Windows Server 2012 R2 ou Windows Server 2012. Les valeurs valides pour le paramètre `remove` sont les noms des rôles, des services de rôle et des fonctionnalités.

- Les commandes de gestion et de maintenance des images de déploiement (DISM) vous permettent de créer des fichiers WIM personnalisés qui économisent l'espace disque en omettant les fichiers de fonctionnalités qui sont inutiles ou qui peuvent être obtenus auprès d'autres sources distantes. Pour plus d'informations sur l'utilisation de DISM pour préparer des images personnalisées, consultez Comment activer ou désactiver des fonctionnalités Windows.

# Supprimer des fichiers de fonctionnalités en utilisant Uninstall-WindowsFeature

Vous pouvez utiliser la cmdlet Uninstall-WindowsFeature pour désinstaller des rôles, des services de rôle et des fonctionnalités des serveurs et des disques durs virtuels hors connexion qui exécutent Windows Server 2012 R2 ou Windows Server 2012, et pour supprimer des fichiers de fonctionnalités. Si vous le souhaitez, vous pouvez à la fois désinstaller et supprimer les mêmes rôles, services de rôle et fonctionnalités dans la même commande.

> **ⓘ Important**
>
> Quand vous supprimez des fichiers de fonctionnalités pour un rôle, un service de rôle ou une fonctionnalité, les rôles, les services de rôle et les fonctionnalités qui dépendent des fichiers que vous supprimez sont également supprimés. Si vous supprimez des fichiers de fonctionnalités pour un service de rôle ou un sous-composant et qu'aucun autre service de rôle ni sous-composant pour le rôle ou le composant parent ne demeure installé, les fichiers pour tout le rôle ou le composant parent sont supprimés. Pour afficher tous les fichiers de fonctionnalités qui seraient supprimés par la commande `Uninstall-WindowsFeature -remove`, ajoutez le paramètre `whatif` à la commande pour l'exécuter et afficher les résultats sans réellement supprimer les fichiers de fonctionnalités.

## Pour supprimer des fichiers de rôles et de fonctionnalités en utilisant Uninstall-WindowsFeature

1. Effectuez une des opérations suivantes pour ouvrir une session Windows PowerShell avec des droits utilisateur élevés.

   > ⓘ **Notes**
   >
   > Si vous désinstallez des rôles et des fonctionnalités sur un serveur distant, vous n'avez pas besoin d'exécuter Windows PowerShell avec des droits d'utilisateur élevés.

   - Sur le bureau Windows, cliquez avec le bouton droit sur **Windows PowerShell** dans la barre des tâches, puis cliquez sur **Exécuter en tant qu'administrateur**.
   - Dans l'écran de **démarrage** de Windows, cliquez avec le bouton droit sur la vignette Windows PowerShell, puis, dans la barre d'application, cliquez sur **Exécuter en tant qu'administrateur**.
   - Sur un serveur exécutant l'option d'installation server Core, tapez **PowerShell** dans une invite de commandes, puis **appuyez sur Entrée**.

2. Tapez ce qui suit, puis **appuyez sur Entrée**.

   ```
   Uninstall-WindowsFeature -Name <feature_name> -computerName <computer_name> -
   remove
   ```

   **Exemple:** La gestion des licences Bureau à distance est le dernier service de rôle restant des services Bureau à distance installés. La commande désinstalle la gestion des licences Bureau à distance, puis supprime les fichiers de fonctionnalités pour l'ensemble du rôle Services Bureau à distance du serveur spécifié, *contoso_1*.

   ```
   Uninstall-WindowsFeature -Name rdS-Licensing -computerName contoso_1 -remove
   ```

   **Exemple:** Dans l'exemple suivant, la commande supprime les services de domaine active directory et la gestion des stratégies de groupe d'un disque dur virtuel hors connexion. Le rôle et la fonction sont d'abord désinstallés, puis leurs fichiers de fonctions supprimés entièrement du VHD hors connexion, *Contoso.vhd*.

> **Notes**
>
> Vous devez ajouter le paramètre `computerName` si vous exécutez la cmdlet depuis un ordinateur exécutant Windows 8.1 ou Windows 8.
>
> si vous entrez le nom d'un fichier de disque dur virtuel à partir d'un partage réseau, ce partage doit accorder des autorisations de **lecture** et **d'écriture** au compte d'ordinateur du serveur que vous avez sélectionné pour monter le disque dur virtuel. L'accès au compte d'utilisateur uniquement ne suffit pas. Le partage peut accorder des autorisations **de lecture** et **d'écriture** au groupe **Tout le monde** pour autoriser l'accès au disque dur virtuel, mais pour des raisons de sécurité, cela n'est pas recommandé.

```
Uninstall-WindowsFeature -Name AD-Domain-Services,GPMC -VHD
C:\WS2012VHDs\Contoso.vhd -computerName ContosoDC1
```

# Voir aussi

Installer ou désinstaller des rôles, des services de rôle ou des fonctionnalitésOptions d'installation de Windows ServerComment activer ou désactiver les fonctionnalités WindowsVue d'ensemble de la maintenance et de la gestion des images de déploiement (DISM)

# Afficher et configurer les données de performances, d'événements et de services

14/08/2025

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

Cette rubrique explique comment afficher et configurer les entrées du journal des événements, les compteurs de performance et les alertes de service affichés pour les serveurs locaux et distants dans le Gestionnaire de serveur.

Les données des journaux de performances, de services et d'événements sont affichées à deux emplacements dans la console du Gestionnaire de serveur dans Windows Server.

- Dans le tableau de bord, vous pouvez cliquer sur les lignes **Événements**, **Performances** et **Services** des miniatures pour configurer les données d'événements, de performances et de journal de service que vous souhaitez voir pour les rôles, l'ensemble du pool de serveurs du Gestionnaire de serveurs, les groupes créés par l'utilisateur de serveurs et le serveur local. Le fait de cliquer sur les lignes hypertexte ouvre les boîtes de dialogue **Affichage des détails** qui vous permettent de spécifier les données sur lesquelles vous souhaitez être alerté dans le tableau de bord. Après avoir configuré les données des journaux d'événements, de service et de performances que vous souhaitez mettre en surbrillance dans les miniatures du tableau de bord, les entrées de journal qui correspondent aux critères que vous avez spécifiés sont répertoriées en bas des boîtes de dialogue **Affichage des détails** .

- **Les vignettes Événements**, **Services** et **Performances** font partie des pages d'accueil de rôle et de groupe. Les commandes du menu **Tâches** de ces vignettes vous permettent de spécifier les données que vous souhaitez collecter à partir de serveurs managés. Les vignettes comportent des filtres et des requêtes qui, si vous le souhaitez, vous permettent de mieux restreindre les entrées de journal affichées dans chaque vignette.

Cette rubrique contient les sections suivantes.


- Que sont les miniatures ?
- Afficher et configurer les événements
- Afficher et configurer les compteurs de performances
- Gérer les services et configurer les alertes de service
- Afficher et copier les entrées liées aux événements et aux performances

# Que sont les miniatures ?

*Les miniatures sont affichées* dans le tableau de bord du Gestionnaire de serveur pour chaque rôle (la miniature d'un rôle reflète les données collectées sur tous les serveurs du pool gestionnaire de serveurs qui exécutent le rôle), pour chaque groupe de **serveurs** , pour le groupe Tous les serveurs (tous les serveurs du pool Gestionnaire de serveurs) et pour le serveur local. Une fois que le Gestionnaire de serveur a obtenu des données à partir des serveurs gérés, des miniatures sont créées automatiquement pour les rôles qui s'exécutent sur des serveurs dans le pool de serveurs.

si la console du Gestionnaire de serveur s'exécute sur un ordinateur client dans le cadre des outils d'administration de serveur distant, il n'existe aucune miniature de **serveur local** .

La miniature dévoile un aperçu rapide de l'état et de la gestion des rôles, des serveurs et des groupes de serveurs. La ligne de titre miniature change de couleur (et les nombres mis en surbrillance sont affichés dans la marge gauche) lorsque les événements, compteurs de performances, résultats best practices Analyzer, services ou problèmes de facilité de gestion générale répondent aux critères que vous configurez dans les boîtes de dialogue **Affichage** détaillé ouvertes en cliquant sur les lignes miniatures. Le tableau qui suit décrit les données dévoilées dans les miniatures.

Agrandir le tableau

| Ligne miniature | Description |
|---|---|
| Manageability | La facilité de gestion d'un serveur comprend plusieurs mesures : si le serveur est en ligne ou hors connexion, s'il est accessible et qu'il fournit des données au Gestionnaire de serveur, si l'utilisateur connecté à l'ordinateur local dispose de droits de l'utilisateur adéquats pour accéder au serveur distant ou pour le gérer, si l'ordinateur distant exécute tous les logiciels requis pour assurer sa gestion à distance ou si le serveur est configuré d'une manière qui lui permet d'être interrogé et géré à l'aide du Gestionnaire de serveur. Les seules données de gérabilité que le Gestionnaire de serveur peut collecter à partir d'un serveur qui exécute Windows Server 2003 correspondent à l'état en ligne ou hors connexion du serveur. Pour obtenir des informations détaillées sur les erreurs d'état de la facilité de gestion et leur résolution, consultez le forum du Gestionnaire de serveur. |
| Events | Vous pouvez configurer la ligne **Événements** d'une miniature pour afficher des alertes lorsque les événements sont enregistrés qui correspondent aux niveaux de gravité, aux sources, aux périodes, aux serveurs ou aux ID d'événement que vous spécifiez. Affichez des détails sur les événements et modifiez les alertes que vous souhaitez voir en cliquant sur la ligne **Événements** , puis en ouvrant la boîte de dialogue **Affichage des détails des événements** pour le rôle ou le groupe de serveurs. |
| Services | Vous pouvez configurer la ligne **Services** pour afficher des alertes lorsque les services se trouvent dans un rôle ou un groupe de serveurs qui correspondent aux types de |

| Ligne miniature | Description |
| --- | --- |
| | démarrage, à l'état du service, aux noms de service et aux serveurs que vous spécifiez dans la boîte de dialogue **Affichage des détails des services** .<br><br>Après qu'un serveur a été ajouté au pool de serveurs du Gestionnaire de serveur, les alertes de service sur le service Détection matériel noyau peuvent s'afficher si aucun utilisateur n'est connecté au serveur géré. Cela se produit dans la mesure où le service Détection matériel noyau ne s'exécute que si des utilisateurs sont connectés au serveur géré ou à une session Bureau à distance sur le serveur géré. Pour éviter de voir les alertes du service de détection matérielle Shell pour ce cas, cliquez sur **Services** dans les miniatures des groupes de serveurs, y compris le groupe **Tous les serveurs** . Dans la boîte de dialogue **Affichage détaillé des services**, dans la liste déroulante **Services**, désélectionnez la case à cocher **Détection matériel noyau**, puis cliquez sur **OK**. |
| Performance | Vous pouvez configurer la ligne **de performances** pour afficher des alertes pour un rôle ou un groupe de serveurs lorsque des alertes de performances correspondent aux types de ressources, aux serveurs ou aux périodes que vous spécifiez dans la boîte de dialogue **Affichage des détails** des performances.<br><br>Par défaut, les compteurs de performances sont désactivés. Les serveurs gérés exécutant des systèmes d'exploitation plus récents que Windows Server 2003, pour lesquels des compteurs de performances n'ont pas été démarrés, affichent généralement des erreurs d'état de la gestion indiquant **En ligne – Compteurs de performances non démarré** dans la vignette **Serveurs** des pages de rôle ou de groupe. Pour activer les compteurs de performances pour les serveurs gérés, dans la page **Tous les serveurs** , cliquez avec le bouton droit sur les entrées de la vignette **Performances** qui affichent une valeur **d'état du compteurdésactivé**, puis cliquez sur **Démarrer les compteurs de performances**. Vous pouvez également démarrer des compteurs de performances en cliquant avec le bouton droit sur les entrées des serveurs dans la vignette **Serveurs** de pages de rôle ou de groupe, puis en cliquant sur **Démarrer les compteurs de performances**. |
| Résultats BPA | Vous pouvez configurer la ligne de **résultats BPA** pour afficher des alertes pour un rôle ou un groupe de serveurs lorsque les résultats de l'analyse BPA sont trouvés qui correspondent aux niveaux de gravité, aux serveurs ou aux catégories BPA que vous spécifiez dans la boîte de dialogue **Affichage des détails des résultats BPA** . |

# Afficher et configurer les événements

Dans cette section, vous allez découvrir comment configurer les données de journaux des événements qui sont recueillies à partir des serveurs dans le pool de serveurs du Gestionnaire de serveur et les événements que vous souhaitez mettre en évidence dans les miniatures.

> ⓘ **Notes**

Les événements au sujet desquels vous voulez être alerté dans les miniatures sont un sous-ensemble de l'ensemble des événements que vous demandez au Gestionnaire de serveur de recueillir à partir des serveurs gérés. Bien que le fait de modifier les critères d'événements dans la boîte de dialogue **Configurer les données d'événement** dans la vignette **Événements** puisse changer le nombre d'alertes visibles dans le tableau de bord du Gestionnaire de serveur, le fait de modifier les critères d'alertes d'événements dans les miniatures n'a aucun impact sur les données de journaux des événements recueillies à partir des serveurs gérés.

## Pour configurer les événements collectés sur les serveurs gérés

1. Dans la console du Gestionnaire de serveur, ouvrez n'importe quelle page à l'exception du tableau de bord. Vous pouvez configurer les événements que vous souhaitez collecter à partir de serveurs gérés dans la vignette **Événements** sur les pages de rôle, de groupe de serveurs ou de serveur local.

2. Dans le menu **Tâches** de la vignette **Événements** , cliquez sur **Configurer les données d'événement**.

3. sélectionnez les niveaux de gravité d'événement que vous souhaitez recueillir sur les serveurs gérés dans le groupe choisi. Par défaut, les niveaux de gravité **Critique**, **Erreur** et **Avertissement** sont sélectionnés.

4. Précisez une période pendant laquelle les événements doivent survenir. La durée par défaut pour les événements est de 24 heures.

5. sélectionnez les fichiers de journaux des événements à partir desquels vous souhaitez recueillir des événements. Les valeurs par défaut sont **Application**, **Setup** et **System**.

6. Pour enregistrer vos modifications, cliquez sur **OK** pour fermer la boîte de dialogue **Configurer les données d'événement** . Les données d'événements sont actualisées automatiquement lors de l'enregistrement de vos modifications.

## Pour configurer les événements mis en surbrillance dans les miniatures

1. si le Gestionnaire de serveur est déjà ouvert, passez à l'étape suivante. S'il n'est pas déjà ouvert, ouvrez-le en effectuant l'une des opérations suivantes.

    - Sur le bureau Windows, démarrez le **Gestionnaire de serveur** en cliquant sur Gestionnaire de serveur dans la barre des tâches Windows.

- Dans l'écran de **démarrage** de Windows, cliquez sur la vignette Gestionnaire de serveur.

2. Dans la page du tableau de bord, dans une miniature de la vignette **Rôles et groupes de serveurs**, cliquez sur la ligne **Événements**.

3. Dans la boîte de dialogue **Affichage Détails des événements**, ajoutez un niveau de gravité aux événements que vous souhaitez afficher. Par défaut, les miniatures affichent uniquement les alertes en surbrillance pour les événements critiques. Notez que le nombre d'événements affichés dans la boîte de dialogue **Affichage** détaillé augmente lorsque vous ajoutez un niveau de gravité sur lequel vous souhaitez être alerté.

4. Dans le champ **Sources d'événements** , sélectionnez les sources d'événements sur lesquelles vous souhaitez être alerté. La valeur par défaut est **All**.

5. si cette miniature concerne un rôle installé sur plusieurs serveurs ou un groupe de plusieurs serveurs, vous pouvez sélectionner les serveurs pour lesquels vous souhaitez recevoir des alertes d'événement dans la liste déroulante **Serveurs** .

6. Dans le champ **période** , spécifiez une période allant jusqu'à 1440 minutes, 24 heures ou 1 jour.

7. Dans le champ **ID** d'événement, tapez les numéros d'ID d'événement d'événements spécifiques sur lesquels vous souhaitez être alerté. Vous pouvez taper une plage d'ID d'événements séparés par un tiret (-) et exclure des ID d'événements de la plage en tapant le tiret avant l'ID d'événements ou la plage d'ID d'événements que vous voulez exclure. Par exemple, la valeur **1,3,5-99,-76** signifie que les alertes sont déclenchées pour les ID d'événement 1 et 3, et tous les événements avec des ID compris entre 5 et 99, à l'exception de l'ID d'événement 76.

8. Lorsque vous modifiez les critères d'affichage des alertes, le nombre d'alertes d'événements affichées dans le volet de résultats au bas de la boîte de dialogue peut changer. sélectionnez des entrées dans la liste, puis cliquez sur **Masquer les alertes** pour les empêcher d'affecter le nombre d'alertes affiché dans la miniature source. Appuyez longuement **sur Ctrl** lorsque vous sélectionnez des alertes pour sélectionner plusieurs alertes à la fois. Vous pouvez réaliser cette opération pour les alertes qui sont conformes à vos critères d'alerte d'événement mais que vous n'avez pas besoin de voir.

9. Cliquez sur **Afficher tout** pour retourner les alertes masquées dans la liste.

10. Cliquez sur **OK** pour enregistrer vos modifications, fermez la boîte de dialogue **Affichage des détails** et affichez les modifications de l'alerte d'événement dans la miniature source.

# Afficher et configurer les données du journal des performances

Dans cette section, vous allez découvrir comment configurer les données de journaux des performances qui sont recueillies à partir des serveurs dans le pool de serveurs du Gestionnaire de serveur et les compteurs de performance que vous souhaitez mettre en évidence dans les miniatures.

Par défaut, les compteurs de performances sont désactivés. Les serveurs gérés exécutant des systèmes d'exploitation plus récents que Windows Server 2003, pour lesquels des compteurs de performances n'ont pas été démarrés, affichent généralement des erreurs d'état de la gestion indiquant **En ligne – Compteurs de performances non démarré** dans la vignette **Serveurs** des pages de rôle ou de groupe. Pour activer les compteurs de performances pour les serveurs gérés, dans la page **Tous les serveurs** , cliquez avec le bouton droit sur les entrées de la vignette **Performances** qui affichent une valeur **d'état du compteurdésactivé**, puis cliquez sur **Démarrer les compteurs de performances**. Vous pouvez également démarrer des compteurs de performances en cliquant avec le bouton droit sur les entrées des serveurs dans la vignette **Serveurs** de pages de rôle ou de groupe, puis en cliquant sur **Démarrer les compteurs de performances**.

> ⓘ **Notes**
>
> Les alertes de performances affichées dans les miniatures sont un sous-ensemble de l'ensemble des données de compteurs de performance que vous demandez au Gestionnaire de serveur de recueillir à partir des serveurs gérés. Bien que le fait de modifier les critères d'alertes de performances dans la boîte de dialogue **Configurer les données d'événement** dans la vignette **Performances** puisse changer le nombre d'alertes visibles dans le tableau de bord du Gestionnaire de serveur, le fait de modifier les critères d'alertes de performances dans les miniatures n'a aucun impact sur les données de journaux de performances recueillies à partir des serveurs gérés.
>
> Pour cette raison, l'âge maximal des données de performance que vous pouvez afficher dans les miniatures ne peut pas être supérieur à la période d'affichage du graphique maximale configurée dans la boîte de dialogue **Configurer des alertes de performances**. Par exemple, si la valeur **Période d'affichage du graphique** de **Configurer des alertes de performances** est de **1 jour**, la valeur maximale du champ **Période** d'une boîte de dialogue **Vue détaillée des performances** que vous avez ouverte à partir du tableau de bord **1 jour**, **24 heures** ou **1 440 minutes**.

## Pour configurer les données du journal des performances collectées sur les serveurs gérés

1. Dans la console du Gestionnaire de serveur, ouvrez n'importe quelle page à l'exception du tableau de bord. Vous pouvez configurer les données de performances que vous souhaitez collecter à partir de serveurs managés dans la vignette **Performances** sur les pages de rôle, de groupe de serveurs ou de serveur local.

2. Pour recueillir des données de journaux de performances à partir de serveurs gérés, vous devez activer les compteurs de performance. Si les compteurs de performances sont désactivés, cliquez avec le bouton droit sur une entrée dans la liste des vignettes **Performances** , puis cliquez sur **Démarrer les compteurs de performances**. La collecte de données avec les compteurs de performance peut nécessiter un certain temps en fonction du nombre de serveurs à partir desquels les données sont recueillies et de la bande passante réseau disponible. Affichez l'état dans la colonne **État du compteur** .

3. Dans le menu **Tâches** de la vignette **Performances** , cliquez sur **Configurer les alertes de performances**.

4. Pour les serveurs appartenant au groupe sélectionné ou qui exécutent le rôle sélectionné, spécifiez le pourcentage d'utilisation du processeur à partir duquel vous souhaitez que le Gestionnaire de serveur recueille des alertes de compteurs de performance. La valeur par défaut est 85 %.

5. Précisez (en mégaoctets) la mémoire disponible restante dont doivent disposer les serveurs avant la collecte des alertes des compteurs de performances. La valeur par défaut est 2 Mo.

6. Spécifiez une période affichée par les graphiques pour les ressources **utilisation du processeur** et la **mémoire disponible** dans la vignette **Performances** de la page sélectionnée. La période par défaut est définie à une journée. Cliquez sur **Enregistrer**.

   Notez que le nombre d'alertes de performances dans la vignette **Performances** et le mappage des alertes au fil du temps, comme indiqué par le graphique, peuvent changer après avoir cliqué sur **Enregistrer**.

   > ⓘ **Notes**
   >
   > pour les machines virtuelles utilisant la **mémoire dynamique**, l'augmentation du seuil des alertes de performance peut entraîner des alertes faussement positives.

7. Pour actualiser la liste des alertes de performances collectées à partir de vos serveurs, dans le menu **Tâches** , cliquez sur **Actualiser**.

## Pour configurer les alertes de performance mises en surbrillance dans les miniatures

1. Dans la page du tableau de bord, dans une miniature de la vignette **Rôles et groupes de serveurs**, cliquez sur la ligne **Performances**.

2. Dans la boîte de dialogue **Affichage Détails des performances**, activez ou désactivez les cases à cocher pour les seuils de performances de ressources au sujet desquels vous souhaitez recevoir des alertes dans le champ **Type de ressource**. Notez que le nombre d'alertes de performances affichées dans la boîte de dialogue **Affichage détaillé** peut augmenter lorsque vous ajoutez un seuil de performances de ressource sur lequel vous souhaitez être alerté.

3. si cette miniature concerne un rôle installé sur plusieurs serveurs ou un groupe de plusieurs serveurs, vous pouvez sélectionner les serveurs pour lesquels vous souhaitez des alertes de performances dans la liste déroulante **Serveurs** .

4. Dans le champ **période** , spécifiez une période allant jusqu'à 1440 minutes, 24 heures ou 1 jour.

5. Lorsque vous modifiez les critères d'affichage des alertes, le nombre d'alertes affichées dans le volet de résultats au bas de la boîte de dialogue peut changer. Cliquez sur **Masquer les alertes** pour masquer toutes les alertes antérieures à l'heure actuelle, et empêchez-les d'affecter le nombre d'alertes affiché dans la miniature source.

6. Cliquez sur **Afficher tout** pour retourner les alertes masquées dans la liste.

7. Cliquez sur **OK** pour enregistrer vos modifications, fermez la boîte de dialogue **Affichage des détails** et affichez les modifications de l'alerte de performances dans la miniature source.

## Pour afficher les propriétés des alertes de performance

1. Effectuez l'une des opérations suivantes.

    - Dans la page du tableau de bord, dans une miniature de la vignette **Rôles et groupes de serveurs**, cliquez sur la ligne **Performances**.

    - Ouvrez une page d'accueil de rôle ou de groupe et recherchez la vignette **Performances** du rôle ou du groupe.

2. Double-cliquez sur une alerte de performance dans la liste pour afficher ses propriétés. Vous pouvez également cliquer avec le bouton droit sur une alerte de performances, puis cliquer sur **Afficher les propriétés**.

3. Dans la boîte de dialogue **Propriétés d'alerte de performance**, sélectionnez des entrées de journaux pour afficher des informations sur les processus associés aux entrées dans la zone **Processus**.

4. Après avoir vérifié les propriétés d'alerte de performance, fermez la boîte de dialogue.

## Analyser les données de performance et résoudre les problèmes

pour plus d'informations sur l'analyse des données de compteurs de performance que vous pouvez afficher dans le Gestionnaire de serveur et sur la résolution des problèmes de performances sur les serveurs gérés, voir les ressources suivantes.

- Analyse des données de performances
- Résolution des problèmes de performance

pour plus d'informations sur l'analyse avancée des performances et les outils d'analyse disponibles pour Windows Server 2012 et versions ultérieures de Windows Server, consultez Performances sur MSDN.

# Gérer les services et configurer les alertes de service

Dans cette section, découvrez comment démarrer, arrêter, redémarrer, suspendre ou reprendre des services qui sont affichés dans la vignette **Services** sur les pages de rôle et de groupe de serveurs dans le Gestionnaire de serveur. Vous pouvez aussi configurer les services au sujet desquels vous êtes alerté dans des miniatures du tableau de bord du Gestionnaire de serveur.

> ⓘ **Notes**
>
> Vous ne pouvez pas modifier le type de démarrage des services, les dépendances des services, les options de récupération ou d'autres propriétés de services dans la vignette Services du Gestionnaire de serveur. Pour modifier les propriétés du service à l'exception de l'état du service, ouvrez le composant logiciel enfichable **Services**. Un raccourci pour ouvrir le composant logiciel enfichable **Services** est disponible dans le menu **Outils** du Gestionnaire de serveur.

### Pour démarrer, arrêter, redémarrer, suspendre ou reprendre un service

1. Dans la console du Gestionnaire de serveur, ouvrez une page quelconque à l'exception du tableau de bord (autrement dit, toute page d'accueil de groupe ou de rôle).
2. Dans la vignette **Services** du rôle ou du groupe, cliquez avec le bouton droit sur un service.
3. Dans le menu contextuel, cliquez sur l'action à laquelle vous souhaitez soumettre le service. Si vous arrêtez le service, la seule action que vous pouvez réaliser est de le démarrer. De même, si vous le suspendez, la seule action possible est de le reprendre.
4. Notez que lorsque vous démarrez, arrêtez, redémarrez, suspendez ou reprenez un service, la valeur de la colonne **État** change pour le service dans la vignette **Services** .

## Pour configurer les alertes de service mises en surbrillance dans les miniatures

1. Dans la page du tableau de bord, dans une miniature de la vignette **Rôles et groupes de serveurs**, cliquez sur la ligne **Services**.
2. Dans la boîte de dialogue **Affichage Détails des services**, sélectionnez les types de démarrage pour les services au sujet desquels vous voulez recevoir des alertes. Par défaut, **Automatique (début différé)** et **Automatique** sont sélectionnés.
3. sélectionnez les états de service pour lesquels vous souhaitez être alerté. Par défaut, **tout** est sélectionné.
4. sélectionnez les services pour lesquels vous souhaitez être alerté. Par défaut, **tout** est sélectionné.
5. sélectionnez les serveurs associés au rôle ou au groupe pour lequel vous souhaitez recevoir des alertes concernant des services. Par défaut, **tout** est sélectionné.
6. Lorsque vous modifiez les critères d'affichage des alertes, le nombre d'alertes affichées dans le volet de résultats au bas de la boîte de dialogue peut changer. Cliquez sur **Masquer les alertes** pour masquer toutes les alertes antérieures à l'heure actuelle, et empêchez-les d'affecter le nombre d'alertes affiché dans la miniature source.
7. Cliquez sur **Afficher tout** pour retourner les alertes masquées dans la liste.
8. Cliquez sur **OK** pour enregistrer vos modifications, fermez la boîte de dialogue **Affichage des détails** et affichez les modifications d'alerte de service dans la miniature source.

# Afficher et copier les entrées liées aux événements, aux services et aux performances

Vous pouvez copier des propriétés d'entrée d'événement, de service ou de performances dans les boîtes de dialogue **Affichage des détails** et les vignettes **Événements** et **Performances** d'un rôle ou d'un groupe. Cliquez avec le bouton droit sur un événement ou une entrée de performances, puis cliquez sur **Copier**.

La vignette **Événements** vous permet également d'afficher un aperçu des propriétés d'événement dans la moitié inférieure de la vignette en sélectionnant un événement dans la liste. Pour copier les propriétés affichées dans l'aperçu, cliquez avec le bouton droit sur le volet d'aperçu, puis cliquez sur **Copier**.

## Voir aussi

Gestionnaire de serveurFiltrer, trier et interroger les données dans les vignettes du Gestionnaire de serveur

# Afficher les détails et notifications de la tâche

14/08/2025

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

Dans le Gestionnaire de serveur dans Windows Server 2012 R2 ou Windows Server 2012, lorsque vous effectuez des tâches de gestion telles que l'ajout de rôles et de fonctionnalités, l'actualisation des services, l'actualisation des données affichées dans la console du Gestionnaire de serveur ou la création d'un groupe personnalisé de serveurs, une notification s'affiche dans la zone **Notifications** de l'en-tête de la console Gestionnaire de serveur. Notifications et boîte de dialogue **Détails** de la tâche que vous pouvez ouvrir à partir du menu **Notifications** en cliquant sur l'icône d'indicateur, afficher l'état des tâches utilisateur ou des demandes, vous montrer si une tâche a échoué et vous aider à résoudre les problèmes en pointant vers des messages d'erreur détaillés sur les échecs de tâche.

## Zone Notifications

La zone **Notifications** dans la barre de menus du Gestionnaire de serveur, marquée par une icône d'indicateur, affiche les résultats des tâches que vous démarrez dans le Gestionnaire de serveur. Les notifications vous indiquent si les tâches que vous avez démarrées dans le Gestionnaire de serveur ont réussi ou échoué. Lorsque les notifications sont consultables, le nombre de notifications disponibles est affiché en regard de l'icône d'indicateur. Si une tâche a échoué, elle ne peut être qu'partiellement terminée (par exemple, si elle n'a pas pu être effectuée sur tous les serveurs distants sur lesquels vous souhaitez effectuer la tâche) ou terminée avec des avertissements, l'indicateur **notifications** devient rouge. Les tâches pour lesquelles des notifications s'affichent sont notamment les suivantes.

- Actualisation manuelle des données affichées dans le Gestionnaire de serveur (les notifications sont affichées pour les actualisations automatiques uniquement en cas d'échec des actualisations)
- démarrage ou arrêt des services
- Installation ou désinstallation de rôles, de services de rôle et de fonctionnalités
- démarrage d'une analyse BPA (Best Practices Analyzer)
- ajout de serveurs distants à gérer (les notifications sont affichées pour les échecs afin de contacter ou actualiser les données affichées pour les serveurs distants)

Les éléments du menu **Notifications** affichent une barre de progression, une brève description de la tâche, le nom du serveur cible pour la tâche (ou l'un des serveurs cibles, si plusieurs serveurs cibles ont été sélectionnés), un lien vers un contrôle ou une boîte de dialogue connexe, le cas échéant, et un menu **Tâches** . Le menu **Tâches** affiche les commandes qui s'appliquent à la notification active (notification sur laquelle le curseur de la souris est pointé). Par exemple, si vous arrêtez un service, vous pouvez cliquer sur **Redémarrer** dans le menu **Tâches** de la notification pour redémarrer le service.

Les notifications sont particulièrement utiles pour installer ou désinstaller des rôles, des services de rôle et des fonctionnalités. Par exemple, si vous démarrez une installation de fonctionnalité sur un serveur distant, vous pouvez fermer l'Assistant Ajout de rôles et de fonctionnalités pendant que l'installation est toujours en cours, mais la tâche active reste dans la liste **notifications** . L'élément **Notifications** affiche une barre de progression pour l'installation et vous permet de rouvrir l'Assistant Ajout de rôles et de fonctionnalités, si nécessaire, en cliquant sur **Ajouter des rôles et des fonctionnalités.** Les éléments de cette liste vous avertissent si une installation a échoué ou si d'autres étapes de configuration sont requises pour terminer le déploiement de la fonctionnalité.

Les notifications jouent également un rôle IMPORTANT dans la résolution des problèmes avec les tâches ou les processus dans le Gestionnaire de serveur. Pour plus d'informations sur l'utilisation des messages dans la zone **Notifications** et la boîte de dialogue **Détails** des tâches pour résoudre les échecs de tâches ou les processus, consultez le forum du Gestionnaire de serveur.

Pour supprimer une notification que vous ne souhaitez plus voir dans la liste **notifications** , placez le curseur de la souris sur la notification, puis cliquez sur **Supprimer la tâche** (**X**).

# Affichage et dépannage des tâches à l'aide des détails de la tâche

La commande **Détails** de la tâche en bas du menu **Notifications** ouvre la boîte de dialogue Détails de la **tâche** , qui fournit une description complète des événements de tâche (démarrage, arrêt, avertissements, réussites ou échecs). Comme d'autres contrôles de liste dans le Gestionnaire de serveur, tels que les vignettes **Événements**, **Services** et **Best Practices Analyzer** , vous pouvez filtrer et créer des requêtes à exécuter sur les tâches affichées dans la boîte de dialogue Détails de la **tâche** . (Pour plus d'informations sur le filtrage et la création de requêtes sur les contrôles de liste, consultez Filtrer, trier et interroger des données dans les vignettes Gestionnaire de serveur). Dans le volet supérieur, vous pouvez passer en revue les notifications telles qu'elles ont été affichées dans le menu **Notifications** et voir le nombre de notifications qui ont été générées sur la même tâche. la sélection d'une notification dans le volet supérieur affiche des informations complètes sur la notification dans le volet inférieur.

Le volet inférieur est particulièrement utile pour dépanner les tâches qui ont échoué. Si le gestionnaire de serveur ne peut pas se connecter à un serveur ni obtenir des données pour un serveur qui est membre du pool de serveurs, les entrées de ce volet contiennent souvent des messages détaillés, y compris l'intégralité du texte de la Gestion à distance de Windows (WinRM) sous-jacente, la mise en réseau ou les problèmes de sécurité qui empêchent le Gestionnaire de serveur de communiquer avec un serveur cible.

## Voir aussi

Filtrer, trier et interroger des données dans les vignettes du Gestionnaire de serveurForum du gestionnaire de serveur.

# Exécuter des analyses Best Practices Analyzer et gérer les résultats des analyses

14/08/2025

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

Dans la gestion De Windows, *les bonnes pratiques* sont des recommandations qui sont considérées comme idéales, dans des circonstances typiques, pour configurer un serveur tel que défini par les experts. Par exemple, il est reconnu comme meilleure pratique pour la plupart des applications serveur de ne laisser ouverts que les ports nécessaires à ces applications pour communiquer avec d'autres ordinateurs du réseau, et de bloquer les ports inutilisés. Bien que le non-respect des meilleures pratiques, même les plus capitales, ne soit pas forcément problématique, se conformer à ces méthodes conseillées permet néanmoins de détecter les configurations de serveur pouvant entraîner des performances médiocres, une fiabilité douteuse, des conflits inattendus, des risques de sécurité accrus ou d'autres problèmes potentiels.

Best Practices Analyzer (BPA) est un outil de gestion de serveur disponible dans Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 et Windows Server 2008 R2. Il peut aider les administrateurs à réduire les transgressions faites aux bonnes pratiques en analysant les rôles installés sur des serveurs gérés qui exécutent une version prise en charge et en signalant les transgressions détectées à l'administrateur.

Vous pouvez exécuter des analyses BPA à partir du Gestionnaire de serveur, à l'aide de l'interface graphique utilisateur de BPA ou à l'aide d'applets de commande dans Windows PowerShell. À compter de Windows Server 2012, vous pouvez analyser simultanément un ou plusieurs rôles, sur plusieurs serveurs, que vous utilisiez la vignette de Best Practices Analyzer dans la console du Gestionnaire de serveur ou les applets de commande Windows PowerShell pour exécuter les analyses. Vous pouvez également demander à BPA d'exclure ou d'ignorer les résultats des analyses que vous ne souhaitez pas consulter.

Cette rubrique contient les sections suivantes.


- Trouver Best Practices Analyzer (BPA)
- Fonctionnement de BPA
- Exécution de Best Practices Analyzer sur des rôles
- Gérer les résultats de l'analyse

# Rechercher BPA

Vous trouverez la vignette Best Practices Analyzer sur les pages de rôle et de groupe de serveurs du Gestionnaire de serveur dans Windows Server, ou vous pouvez ouvrir une session Windows PowerShell avec des droits d'utilisateur élevés pour exécuter des applets de commande Best Practices Analyzer.

# Fonctionnement de BPA

BPA fonctionne en mesurant le niveau de conformité d'un rôle par rapport aux règles des bonnes pratiques instituées dans huit catégories différentes chargées d'évaluer l'efficacité, la fiabilité et l'intégrité d'un rôle. Les résultats de ces mesures se traduisent par l'un des trois niveaux de gravité décrits dans le tableau ci-dessous.

Agrandir le tableau

| Niveau de gravité | Descriptif |
|---|---|
| Erreur | Des résultats définis en tant qu'erreurs sont renvoyés lorsqu'un rôle ne respecte pas les conditions d'une règle relevant des meilleures pratiques et que des problèmes d'ordre fonctionnel sont attendus. |
| Informations | Des résultats à titre d'informations conformes sont renvoyés lorsqu'un rôle satisfait aux conditions d'une règle des meilleures pratiques. |
| Warning | Des résultats d'avertissement sont renvoyés si les résultats de non-conformité peuvent causer des problèmes en cas de modifications. L'application peut être jugée conforme par rapport à son fonctionnement actuel, mais peut ne pas remplir les conditions d'une règle si des modifications ne sont pas apportées à ses paramètres de configuration ou de stratégie. Par exemple, une analyse des services Bureau à distance peut montrer un résultat d'avertissement si un serveur de licences n'est pas disponible pour le rôle, car même si aucune connexion distante n'est active au moment de l'analyse, le fait de ne pas avoir de serveur de licences empêche de futures connexions distantes d'obtenir des licences d'accès client valides. |

## Catégories de règles

Le tableau suivant détaille les catégories des règles de bonnes pratiques par rapport aux rôles mesurés pendant une analyse Best Practices Analyzer.

Agrandir le tableau

| Nom de catégorie | Descriptif |
|---|---|
| Sécurité | Les règles de sécurité sont appliquées pour mesurer le risque relatif d'un rôle de se trouver exposé à des menaces telles que des utilisateurs malveillants ou non autorisés, à la perte ou au vol de données confidentielles ou protégées. |
| Performances | Les règles de performances s'appliquent pour mesurer la capacité d'un rôle à traiter des requêtes et à remplir les fonctions qui lui ont été attribuées dans l'entreprise, dans les délais prévus étant donné la charge de travail de ce rôle. |
| Paramétrage | Les règles de configuration sont appliquées pour identifier des paramètres de rôle pouvant nécessiter des modifications au niveau du rôle afin que celui-ci s'exécute de façon optimale. Les règles de configuration permettent d'empêcher l'apparition de conflits entre paramètres pouvant se solder par des messages d'erreur ou par l'impossibilité pour le rôle d'assurer les fonctions qui lui ont été assignées dans l'entreprise. |
| Stratégie | Des règles de stratégie sont appliquées pour identifier les paramètres de stratégie de groupe ou de Registre Windows pouvant nécessiter des modifications au niveau d'un rôle pour que celui-ci fonctionne de façon optimale et en toute sécurité. |
| Opération | Les règles d'opération sont appliquées pour identifier les échecs possibles d'un rôle lors de l'exécution des tâches qui lui ont été prescrites dans l'entreprise. |
| Prédéploiement | Les règles de prédéploiement sont appliquées avant le déploiement d'un rôle installé dans l'entreprise. Elles permettent aux administrateurs d'évaluer si les meilleures pratiques ont été respectées avant que le rôle ne soit utilisé à des fins de production. |
| Post-déploiement | Les règles de postdéploiement sont appliquées une fois que tous les services requis ont démarré pour un rôle, et après que le rôle s'exécute dans l'entreprise. |
| Prérequis | Les règles en matière de conditions préalables expliquent les paramètres de configuration, les paramètres de stratégie et les fonctionnalités qui sont nécessaires au rôle avant que l'analyseur BPA puisse appliquer des règles spécifiques à partir d'autres catégories. Une condition préalable dans les résultats d'analyse indique qu'un paramètre incorrect, un programme manquant, une stratégie activée ou désactivée de façon incorrecte, un paramètre de clé de Registre ou un autre élément de configuration a empêché BPA d'appliquer une ou plusieurs règles au cours d'une analyse. Un résultat de condition préalable n'implique pas la notion de conformité ou non-conformité. Cela signifie simplement qu'une règle n'a pas pu être appliquée et que, par conséquent, elle ne fait pas partie des résultats de l'analyse. |

# Exécution d'analyses BPA (Best Practices Analyzer) dans des rôles

Vous pouvez effectuer des analyses BPA sur des rôles par le biais de l'interface graphique utilisateur BPA dans le Gestionnaire de serveur, ou à l'aide d'applets de commande Windows

PowerShell.

Dans Windows Server, certains rôles vous invitent à spécifier des paramètres supplémentaires tels que les noms de serveurs spécifiques ou de partages qui exécutent des parties de rôles, ou les ID de sous-modèles, avant de commencer une analyse BPA. Pour des analyses BPA dans des modèles exigeant l'apport de paramètres supplémentaires, utilisez les applets de commande BPA ; l'interface graphique utilisateur BPA ne peut pas accepter des paramètres supplémentaires comme les ID de sous-modèles. Par exemple, l'ID de sous-modèle **FSRM** représente le sous-modèle BPA des services de fichiers pour le Gestionnaire de ressources du serveur de fichiers, un service de rôle des services de fichiers et de stockage. Pour exécuter une analyse uniquement sur le service de rôle Outils de gestion de ressources pour serveur de fichiers, exécutez une analyse BPA à l'aide d'applets de commande Windows PowerShell et ajoutez le paramètre `SubmodelId` à votre applet de commande.

Bien qu'il soit impossible de passer des paramètres supplémentaires à une analyse que vous démarrez dans l'interface graphique utilisateur de BPA, la vignette BPA dans le Gestionnaire de serveur affiche les résultats de l'analyse BPA la plus récente, quelle que soit la manière dont vous avez lancé l'analyse.

- Analyse des rôles à l'aide de l'interface graphique utilisateur BPA
- Analyse des rôles à l'aide des applets de commande Windows PowerShell

## Analyse de rôles à l'aide de l'interface graphique utilisateur BPA

Procédez comme suit pour analyser un ou plusieurs rôles dans l'interface graphique utilisateur BPA.

### Pour analyser des rôles à l'aide de l'interface graphique utilisateur BPA

1. Effectuez une des actions suivantes pour ouvrir le Gestionnaire de serveur s'il n'est pas déjà ouvert.
    - Dans la barre des tâches Windows, cliquez sur le bouton Gestionnaire de serveur.
    - Dans l'écran de **démarrage** , cliquez sur la vignette Gestionnaire de serveur.
2. Dans le volet de navigation, ouvrez la page d'un rôle ou d'un groupe.

    Lorsque vous exécutez des analyses BPA à partir de la page d'un rôle ou d'un groupe, tous les rôles installés sur les serveurs du groupe sont analysés.

3. Dans le menu **Tâches** de la vignette **Best Practices Analyzer** , cliquez sur **Démarrer l'analyse BPA**.

4. En fonction du nombre de règles que vous évaluez pour le rôle ou le groupe sélectionné, l'exécution de l'analyse BPA peut prendre plusieurs minutes.

## Analyse de rôles à l'aide d'applets de commande Windows PowerShell

Appliquez les procédures suivantes pour analyser un ou plusieurs rôles au moyen d'applets de commande Windows PowerShell.

> ⓘ **Notes**
>
> Les procédures de cette section ne montrent pas toutes les applets de commande ni tous les paramètres. Pour plus d'informations sur les opérations BPA dans Windows PowerShell, dans votre session Windows PowerShell, entrez **Get-help***BPACmdlet-full*, où *BPACmdlet* peut être l'une des valeurs suivantes. Vous trouverez également des rubriques d'aide sur les applets de commande BPA sur Windows Server TechCenter.

- **Get-BPAmodel**
- **Invoke-BPAmodel**
- **Get-BPAResult**
- **Set-BPAResult**

### Pour analyser un rôle unique à l'aide d'applets de commande Windows PowerShell

1. Effectuez l'une des opérations suivantes pour exécuter Windows PowerShell avec des droits utilisateur élevés.

    - Pour exécuter Windows PowerShell en tant qu'administrateur à partir de l'écran de **démarrage** , cliquez avec le bouton droit sur la vignette **Windows PowerShell** dans les résultats **des applications** , puis, dans la barre d'application, cliquez sur **Exécuter en tant qu'administrateur**.

    - Pour exécuter Windows PowerShell en tant qu'administrateur à partir du bureau, cliquez avec le bouton droit sur le raccourci **Windows PowerShell** dans la barre des tâches, puis cliquez sur **Exécuter en tant qu'administrateur**.

2. À compter de Windows PowerShell 3.0, les modules d'applets de commande sont importés automatiquement dans votre session Windows PowerShell lors de la première utilisation d'une applet de commande du module. Vous n'avez pas besoin d'importer ou de charger le module d'applets de commande BPA.

3. recherchez les ID de modèle de tous les rôles pour lesquels les analyses BPA peuvent être effectuées en entrant l'applet de commande **Get-Bpamodel** , comme illustré dans l'exemple suivant.

   ```
   Get-Bpamodel
   ```

4. Dans les résultats de l'étape 3, repérez les ID de modèles des rôles pour lesquels vous voulez effectuer une analyse BPA.

5. Entrez l'une des commandes suivantes pour démarrer l'analyse BPA pour un rôle en particulier. Pour plusieurs rôles, séparez les ID des modèles par des virgules.

   ```
   Invoke-BPAmodel -modelId <modelID_from_Step3>
   ```

   ```
   Invoke-BPAmodel <modelID_from_Step3>
   ```

   **Exemple:** `Invoke-BPAmodel -modelId Microsoft/Windows/DNSServer,Microsoft/Windows/FileServices`

   > ⓘ **Notes**
   >
   > L'ID de modèle inclut l'intégralité du chemin d'accès affiché dans la colonne **ID** ; Par exemple, **Microsoft/Windows/Hyper-V**.

   Vous pouvez également démarrer une analyse sur un rôle spécifique à partir des résultats de l'étape 3 en transférant les résultats de l'applet de commande `Get-BPAmodel` à l'applet de commande `Invoke-BPAmodel` , comme indiqué dans l'exemple suivant.

   ```
   Get-BPAmodel <model_ID> | Invoke-BPAmodel
   ```

   L'exécution de cette applet de commande sans spécifier d'ID de modèle entraîne le transfert de tous les modèles renvoyés par l'applet de commande `Get-BPAmodel` vers l'applet de commande `Invoke-BPAmodel`, et démarre des analyses sur tous les modèles disponibles sur les serveurs qui ont été ajoutés au pool de serveurs Gestionnaire de serveur.

### Pour analyser tous les rôles à l'aide d'applets de commande Windows PowerShell

1. Ouvrez une session Windows PowerShell avec des droits d'utilisateur élevés, si ce n'est déjà fait. Reportez-vous à la procédure précédente pour obtenir des instructions.

2. Redirigez tous les rôles pour lesquels les analyses BPA peuvent être effectuées dans l'applet de commande `Invoke-BPAmodel` pour démarrer les analyses.

   ```
   Get-BPAmodel | Invoke-BPAmodel
   ```

3. Une fois l'analyse terminée, Windows PowerShell retourne des résultats similaires aux suivants pour chaque rôle analysé.

   ```
   modelId                 :  Microsoft/Windows/FileServices
   SubmodelId              :
   Success                 :  True
   Scantime                :  1/01/2012  12:18:40 PM
   ScantimeUtcOffset       :  -08:00:00
   detail                  :  {server_name1, server_name2}
   ```

# Gérer les résultats des analyses

Après avoir réalisé une analyse BPA dans l'interface graphique utilisateur, vous pouvez afficher les résultats de l'analyse dans une vignette BPA. Lorsque vous sélectionnez un résultat dans une vignette, un volet de visualisation dans cette dernière affiche les propriétés du résultat, et notamment un élément indiquant si le rôle est conforme à la meilleure pratique qui lui est associé. Si un résultat n'est pas conforme et si vous souhaitez savoir comment résoudre les problèmes décrits dans les propriétés de ce résultat, servez-vous des liens hypertexte des avertissements et des erreurs signalés dans les propriétés pour accéder à des rubriques d'aide sur le site Windows Server TechCenter.

> ⓘ **Notes**
>
> Les résultats d'analyse BPA ne sont pas automatiquement enregistrés ou archivés. Lorsque vous soumettez un modèle ou un sous-modèle à une nouvelle analyse, les résultats de la dernière analyse sont remplacés. Pour enregistrer les résultats de l'analyse BPA pour l'archivage, l'impression ou l'envoi à d'autres utilisateurs, consultez **Pour afficher les résultats BPA des sessions Windows PowerShell dans différents formats** de cette section.

# Exclure et inclure des résultats BPA

Si vous n'avez pas besoin d'afficher certains résultats BPA, tels que ceux qui sont récurrents dans vos analyses BPA mais ne nécessitent aucune résolution, vous pouvez exclure ces résultats à l'aide de l'interface graphique utilisateur de BPA ou des applets de commande BPA dans Windows PowerShell. Les résultats peuvent être réintégrés à tout moment.

> ⓘ **Notes**
>
> Lorsque vous excluez des résultats, ceux-ci sont également exclus de l'affichage sur les serveurs gérés. D'autres administrateurs ne peuvent pas voir les résultats exclus sur les serveurs gérés. Pour exclure les résultats de l'affichage dans une console du Gestionnaire de serveur local uniquement, créez une requête personnalisée au lieu d'utiliser la commande **Exclure le résultat** .

## Exclure des résultats d'analyse

Le paramètre **Exclure** est persistant ; les résultats que vous excluez restent exclus dans les analyses futures du même modèle sur le même ordinateur, sauf si elles sont à nouveau incluses.

Vous pouvez exclure des résultats d'analyse en exécutant l'applet de commande `Set-BPAResult` avec le paramètre `Exclude` . Comme avec la vignette de Best Practices Analyzer dans le Gestionnaire de serveur, vous pouvez exclure des objets de résultats individuels ou un ensemble de résultats dont les champs (catégorie, titre et gravité, par exemple) sont égaux à certaines valeurs spécifiées ou les contiennent. Par exemple, vous pouvez exclure tous les résultats **de performances** d'un ensemble de résultats d'analyse pour un modèle.

> ⓘ **Notes**
>
> Vous devez exécuter au moins une analyse BPA dans un modèle avant de pouvoir utiliser des procédures dans cette section.

### Pour exclure des résultats d'analyse à l'aide de l'interface graphique utilisateur

1. Ouvrez une page de groupe de rôles ou de serveurs dans le Gestionnaire de serveur.
2. Dans la vignette Best Practices Analyzer pour le rôle ou le groupe de serveurs, cliquez avec le bouton droit sur un résultat dans la liste, puis cliquez sur **Exclure le résultat**.

Le résultat n'apparaît plus dans la liste des résultats.

3. Pour afficher les résultats exclus dans l'interface utilisateur, exécutez la requête intégrée **Résultats exclus**. Cliquez sur **Requêtes de recherche enregistrées**, puis sur **Résultats exclus**.

   Après avoir exécuté la requête **Résultats exclus** , notez que le texte du sous-titre de vignette, une description des résultats affichés dans la liste, passe aux **résultats exclus**. Seuls les résultats exclus s'affichent dans la liste.

### Pour exclure des résultats d'analyse à l'aide d'applets de commande Windows PowerShell

1. Ouvrez une session Windows PowerShell avec des droits de l'utilisateur élevés.

2. Excluez des résultats spécifiques d'une analyse de modèle en exécutant la commande suivante :

   ```
   Get-BPAResult -modelId <model ID> | Where { $_.<Field Name> -eq "Value"} | Set-BPAResult -Exclude $true
   ```

   La commande précédente récupère les éléments de résultat d'analyse BPA pour l'ID de modèle représenté par *l'ID de modèle*.

   La deuxième section de la commande filtre les résultats de l'applet `Get-BPAResult` de commande pour récupérer uniquement les résultats d'analyse pour lesquels la valeur d'un champ de résultat, représentée par *le nom du champ*, correspond au texte entre guillemets.

   La dernière partie de la commande qui suit la deuxième barre verticale exclut les résultats filtrés par la précédente section de l'applet de commande.

   **Exemple:** `Get-BPAResult -Microsoft/Windows/FileServices | Where { $_.Severity -eq "Information"} | Set-BPAResult -Exclude $true`

## Inclure des résultats d'analyse

Lorsque vous voulez afficher des résultats d'analyse exclus, il suffit de les inclure. Le paramètre **Include** est persistant ; les résultats inclus restent inclus dans les analyses futures du même modèle sur le même ordinateur.

### Pour inclure des résultats d'analyse à l'aide de l'interface graphique utilisateur

1. Ouvrez une page de groupe de rôles ou de serveurs dans le Gestionnaire de serveur.
2. Dans la vignette Best Practices Analyzer pour le rôle ou le groupe de serveurs, cliquez avec le bouton droit sur un résultat exclu dans la liste de requêtes **Résultats exclus** , puis cliquez sur **Inclure le résultat**.

   Le résultat n'apparaît plus dans la liste des résultats exclus. Effacez la requête en cliquant sur **Effacer tout** pour afficher le résultat inclus dans la liste de tous les résultats inclus.

### Pour inclure des résultats d'analyse à l'aide d'applets de commande Windows PowerShell

1. Ouvrez une session Windows PowerShell avec des droits de l'utilisateur élevés.
2. Incluez des résultats spécifiques d'une analyse de modèle en tapant la commande suivante, puis en appuyant sur **Entrée**.

   ```
   Get-BPAResult -modelId <model Id> | Where { $_.<Field Name> -eq "Value" } | Set-BPAResult -Exclude $false
   ```

   La commande précédente récupère les éléments de résultat de l'analyse BPA pour le modèle représenté par *l'ID de modèle*.

   La deuxième partie de la commande, après le premier caractère de canal ( **|** ) filtre les résultats de l'applet de commande **Get-BPAResult** pour récupérer uniquement les résultats de l'analyse pour lesquels la valeur du champ de résultat, représentée par *le nom* du champ, correspond au texte entre guillemets.

   La dernière partie de la commande, après le deuxième caractère de canal, inclut les résultats filtrés par la deuxième partie de l'applet de commande, en définissant la valeur du paramètre **-Exclude** sur **false**.

   **Exemple:** `Get-BPAResult -Microsoft/Windows/FileServices | Where { $_.Severity -eq "Information"} | Set-BPAResult -Exclude $false`

## Afficher et exporter des résultats d'analyse BPA dans Windows PowerShell

Pour afficher et gérer les résultats d'analyse à l'aide des applets de commande Windows PowerShell, consultez les procédures suivantes. Avant d'utiliser l'une des procédures suivantes, exécutez au moins une analyse BPA sur un au moins un modèle ou un sous-modèle.

## Pour afficher les résultats de l'analyse la plus récente d'un rôle à l'aide de Windows PowerShell

1. Ouvrez une session Windows PowerShell avec des droits de l'utilisateur élevés.

2. Obtenez les résultats de l'analyse la plus récente pour un ID de modèle spécifié. Tapez ce qui suit, dans lequel le modèle est représenté par *l'ID de modèle*, puis **appuyez sur Entrée**. Vous pouvez obtenir les résultats de plusieurs ID de modèles en séparant les ID par des virgules.

   `Get-BPAResult <model ID>`

   **Exemple:** `Get-BPAResult Microsoft/Windows/DNSServer,Microsoft/Windows/FileServices`

   Si vous avez analysé un sous-modèle ou un modèle (un service de rôle, par exemple), procurez-vous seulement les résultats du sous-modèle en question en incluant son ID dans l'applet de commande.

   **Exemple:** `Get-BPAResult Microsoft/Windows/FileServices -SubmodelID FSRM`

## Pour afficher ou enregistrer des résultats BPA à partir de sessions Windows PowerShell dans différents formats

- Dans Windows PowerShell, chaque résultat BPA ressemble à ce qui suit.

```
ResultNumber     :  14
ResultId         :  1557706192
modelId          :  Microsoft/Windows/FileServices
SubmodelId       :  FSRM
RuleId           :  16
computerName     :  server_name1, server_name2
Context          :  FileServices
Source           :  server_name1
Severity         :  Information
Category         :  Configuration
Title            :  Access Denied remediation requires remote management be
enabled on this server
Problem          :
Impact           :
Resolution       :
compliance       :  The File Server Best Practices Analyzer scan has
determined that you are in compliance with this best practice.
help             :
Excluded         :  False
```

Effectuez l'une des opérations suivantes.

- Pour mettre en forme des résultats BPA dans un tableau, exécutez l'applet de commande suivante en ajoutant les propriétés de résultat de l'exemple précédent que vous souhaitez afficher.

  ```
  Get-BPAResult model ID | format-Table -Property
  <property1,property2,property3...>
  ```

  **Exemple:** `Get-BPAResult Microsoft/Windows/FileServices | format-Table -Property modelId,SubmodelId,computerName,Source,Severity,Category,Title,Problem,Impact,Resolution,compliance,help`

- Pour mettre en forme des résultats BPA dans une grille basée sur l'interface graphique utilisateur, avec un filtre pour les chaînes de caractères et des en-têtes de colonne sur lesquels vous pouvez cliquer pour trier des résultats, exécutez l'applet de commande suivante.

  ```
  Get-BPAResult <model ID> | OGV
  ```

- Pour exporter les résultats BPA vers un fichier HTML qui peut être archivé ou envoyé aux destinataires de courrier électronique, exécutez l'applet de commande suivante, où *le chemin représente le chemin d'accès* et le nom de fichier dans lequel vous souhaitez enregistrer les résultats HTML.

  ```
  Get-BPAResult <model ID> | convertTo-Html | Set-Content <path>
  ```

  **Exemple:** `Get-BPAResult Microsoft/Windows/FileServices | convertTo-Html | Set-Content C:\BPAResults\FileServices.htm`

- Pour exporter les résultats BPA vers un fichier texte de valeurs séparées par des virgules (CSV), exécutez l'applet de commande suivante, où *le chemin représente le chemin d'accès* et le nom du fichier texte dans lequel vous souhaitez enregistrer les résultats CSV. Les résultats CSV peuvent être importés dans Microsoft Excel ou tout autre programme affichant des données dans des feuilles de calcul ou des grilles.

  ```
  Get-BPAResult <model ID> | Export-CSV <path>
  ```

  **Exemple:** `Get-BPAResult Microsoft/Windows/FileServices | Export-CSV C:\BPAResults\FileServices.txt`

# Voir aussi

Contenu de résolution de Best Practices Analyzer sur le site Windows Server TechCenterFiltrer, trier et interroger des données dans les vignettes du Gestionnaire de serveurGérer plusieurs serveurs distants avec le Gestionnaire de serveur

# créer et gérer des groupes de serveurs

14/08/2025

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

Cette rubrique décrit la manière de créer des groupes de serveurs personnalisés définis par l'utilisateur dans le Gestionnaire de serveur dans Windows Server.

## Groupes de serveurs

Les serveurs que vous ajoutez au pool de serveurs sont affichés dans la page **Tous les serveurs** du Gestionnaire de serveur. Vous pouvez créer des groupes de serveurs personnalisés avec les serveurs que vous avez ajoutés. Les groupes de serveurs vous permettent d'afficher et de gérer un sous-ensemble plus petit de votre pool de serveurs en tant qu'unité logique ; Par exemple, vous pouvez créer un groupe appelé **Serveurs de comptabilité** pour tous les serveurs du service Comptabilité de votre organisation, ou un groupe appelé Chicago pour tous les serveurs situés géographiquement à **Chicago** . Après avoir créé un groupe de serveurs, la page d'accueil du groupe dans le Gestionnaire de serveur affiche des informations sur les événements, services, compteurs de performance, résultats Best Practices Analyzer ainsi que les fonctionnalités et rôles installés pour le groupe dans son ensemble.

Les serveurs peuvent être membres de plusieurs groupes.

### Pour créer un nouveau groupe de serveurs

1. Dans le menu **Gérer** , cliquez sur **Créer un groupe de serveurs**.
2. Dans la zone de texte **Nom du groupe de** serveurs, tapez un nom convivial pour votre groupe de serveurs, tel que **Les serveurs comptables**.
3. ajoutez des serveurs à la liste **sélectionnée** à partir du pool de serveurs ou ajoutez d'autres serveurs au groupe à l'aide des onglets **Active Directory**, **DNS** ou **importation** . Pour plus d'informations sur l'utilisation de ces onglets, consultez ajouter des serveurs au Gestionnaire de serveur dans ce guide.
4. Une fois que vous avez terminé d'ajouter des serveurs au groupe, cliquez sur **OK**. Le nouveau groupe s'affiche dans le volet de navigation du Gestionnaire de serveur sous le groupe **Tous les serveurs** .

### Pour modifier un groupe de serveurs existant

1. Effectuez l'une des opérations suivantes.

    - Dans le volet de navigation du Gestionnaire de serveur, cliquez avec le bouton droit sur un groupe de serveurs, puis cliquez sur **Modifier le groupe de serveurs**.
    - Dans la page d'accueil du groupe de **serveurs**, ouvrez le menu **Tâches** de la vignette Serveurs, puis cliquez sur **Modifier le groupe de serveurs**.

2. mModifiez le nom du groupe ou ajoutez ou supprimez des serveurs dans le groupe.

    > ⓘ Notes
    >
    > la suppression de serveurs dans un groupe de serveurs ne supprime pas les serveurs dans le Gestionnaire de serveur. Les serveurs que vous supprimez d'un groupe restent dans le groupe **Tous les serveurs** , dans le pool de serveurs.

3. Une fois les modifications apportées au groupe terminées, cliquez sur **OK**.

### Pour supprimer un groupe de serveurs existant

1. Effectuez l'une des opérations suivantes.

    - Dans le volet de navigation du Gestionnaire de serveur, cliquez avec le bouton droit sur un groupe de serveurs, puis cliquez sur **Supprimer le groupe de serveurs**.
    - Dans la page d'accueil du groupe de **serveurs**, ouvrez le menu **Tâches** de la vignette Serveurs, puis cliquez sur **Supprimer le groupe de serveurs**.

2. Lorsque vous êtes invité à vous assurer que vous souhaitez supprimer le groupe de serveurs, cliquez sur **Oui**.

    > ⓘ Notes
    >
    > La suppression d'un groupe de serveurs ne supprime pas les serveurs dans le Gestionnaire de serveur. Les serveurs qui étaient dans un groupe supprimé restent dans le groupe **Tous les serveurs** , dans le pool de serveurs.

3. Une fois les modifications apportées au groupe terminées, cliquez sur **OK**.

## Voir aussi

ajouter des serveurs au Gestionnaire de serveurGestionnaire de serveur

# Filtrer, trier et interroger des données dans les vignettes du Gestionnaire de serveur

14/08/2025

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

Dans Windows Server, les vignettes dans le Gestionnaire de serveur vous permettent de filtrer et trier des données, et de créer et enregistrer des requêtes personnalisées. Vous pouvez trier, utiliser des filtres de mots clés et exécuter des requêtes dans les vignettes Événements, Performances, Best Practices Analyzer, Services, et Rôles et fonctionnalités dans des pages de groupes de rôles ou de serveurs du Gestionnaire de serveur.

Cette rubrique contient les sections suivantes.

- Filtrer les entrées de liste dans les vignettes
- trier les entrées de liste dans les vignettes
- créer et exécuter des requêtes personnalisées sur les données des vignettes

## Filtrer les entrées de liste dans les vignettes

La zone de texte **Filtre** est un moyen rapide de réduire la liste des entrées affichées dans une vignette uniquement à celles qui contiennent une chaîne de texte spécifiée.

### Pour appliquer un filtre à la liste des entrées dans une vignette

1. Ouvrez une page de groupe de rôles ou de serveurs dans le Gestionnaire de serveur.
2. Dans la zone de texte **Filtre** d'une vignette Événements, Performances, Best Practices Analyzer, Services ou Rôles et fonctionnalités, tapez une chaîne sur laquelle vous souhaitez filtrer.

   par exemple, si vous souhaitez afficher uniquement les événements avec un ID d'événement 1014, tapez **1014** dans la zone de texte **Filtrer** . Tous les événements collectés qui contiennent la chaîne **1014** dans au moins un champ sont retournés en tant que résultats.
3. Notez que le filtre modifie le texte de la description sous le titre de la vignette. Au lieu de **tous les** résultats, il indique **les résultats filtrés**.
4. Pour effacer le filtre, supprimez la chaîne dans la zone de filtre ou cliquez sur **X**.

# trier les entrées de liste dans les vignettes

Triez les entrées de liste dans les vignettes du Gestionnaire de serveur en cliquant sur les en-têtes de colonne. Lorsque vous cliquez sur un en-tête de colonne la première fois, les valeurs alphanumériques de la colonne sont triées dans l'ordre croissant (flèche pointant vers le haut) ; pour les trier par ordre décroissant (flèche vers le bas), cliquez une nouvelle fois dessus.

# créer et exécuter des requêtes personnalisées sur les données des vignettes

Vous pouvez créer des requêtes personnalisées dans les vignettes Événements, Performances, Best Practices Analyzer, Services ou Rôles et fonctionnalités du Gestionnaire de serveur. Par défaut, la zone de la barre d'outils de vignette dans laquelle vous sélectionnez des critères pour générer une requête personnalisée est masquée ; Cliquez sur **Développer** (bouton chevron sur le bord droit de la barre d'outils de vignette) pour afficher les critères de requête.

## Pour créer une requête personnalisée pour des données de vignette

1. Ouvrez une page de groupe de rôles ou de serveurs dans le Gestionnaire de serveur.
2. Dans une vignette Événements, Performances, Best Practices Analyzer, Services ou Rôles et fonctionnalités, développez la zone de génération de requêtes en cliquant sur **Développer**.
3. Cliquez sur **Ajouter des critères** pour ouvrir une liste d'attributs (ou de champs) qui s'appliquent aux entrées de la vignette.
4. Sélectionnez les critères à ajouter. Lorsque vous avez terminé, cliquez sur **Ajouter**. Les critères que vous avez choisis sont ajoutés dans la zone de création de requêtes.
5. Cliquez sur l'opérateur hypertexte pour sélectionner un opérateur. Par exemple, pour des critères numériques ou une date et une heure, la valeur par défaut est **inférieur ou égal à**.
6. Spécifiez des valeurs acceptables pour les critères. Par exemple, si vous avez sélectionné **Date et heure**, spécifiez une date au format *j/m/aaaa*.
7. Répétez ces étapes à partir de l'étape 3 pour ajouter d'autres critères à votre requête.

   Vous pouvez ajouter des doublons de critères déjà présents dans votre requête, mais les doublons sont ajoutés à la requête avec l'opérateur **ou** l'opérateur.

   par exemple, pour interroger les ID d'événement 1003 ou 1014, vous devez d'abord ajouter les critères d'ID à votre requête, rendre la valeur d'ID égale à **1003**, puis ajouter un

deuxième critère d'ID à votre requête, ce qui rend la valeur du deuxième ID égal à **1014**. La requête obtenue est **et ID est égal à 1003 ou ID est égal à 1014**.

8. Lorsque vous avez terminé d'ajouter des critères et de spécifier des opérateurs et des valeurs, cliquez sur **Enregistrer** pour enregistrer la requête.

9. Entrez un nom convivial pour la requête. Par exemple, la requête créée à l'étape précédente peut être nommée **événements de licence**.

10. Lorsque vous avez terminé d'afficher les résultats de la requête, cliquez sur **Effacer tout** pour effacer tous les filtres et requêtes, puis afficher toutes les entrées de la liste.

11. Pour exécuter une requête enregistrée, cliquez sur **Requêtes de recherche enregistrées**, puis sur le nom de la requête enregistrée à exécuter.

12. Pour supprimer une requête enregistrée, cliquez sur **Requêtes de recherche enregistrées**, puis sur **X** en regard du nom de la requête enregistrée à supprimer.

# Voir aussi

Vue du Gestionnaire de serveuret configuration des données de performances, d'événement et de service

# Raccourcis clavier pour le Gestionnaire de serveur

08/08/2025

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

Comme le Gestionnaire de serveur a été entièrement repensé à compter de Windows Server 2012, les raccourcis clavier qui fonctionnaient dans la console du Gestionnaire de serveur dans Windows Server 2008 R2 ou Windows Server 2008 ne sont pas nécessairement les mêmes commandes. Cette rubrique décrit les nouveaux raccourcis clavier et les touches d'accès pour le Gestionnaire de serveur dans Windows Server 2012 et les versions plus récentes de Windows Server.

Les commandes qui n'ont pas leurs propres raccourcis clavier ou touches d'accès sont accessibles en appuyant sur la touche **Tab** et en parcourant leur groupe de contrôles lorsqu'il est au focus.

## Clés d'accès

### Zone de contrôle active dans le Gestionnaire de serveur

### Vignette d'accueil

Agrandir le tableau

| Groupe de contrôles | Clé d'accès |
|---|---|
| Vignette Bienvenue - Onglet Démarrage rapide | **Alt+Q** |
| Vignette Bienvenue - onglet Nouveautés | **Alt+W** |
| Vignette Bienvenue - Onglet En savoir plus | **Alt+L** |
| Vignette Bienvenue - commande Masquer | **Alt+D** |

### Miniatures de rôles et de groupes

Agrandir le tableau

| Groupe de contrôles | Clé d'accès |
|---|---|
| Vignette Rôles et groupes de serveurs | **Alt+R** |

### Contrôles des en-têtes de la console

Agrandir le tableau

| Groupe de contrôles | Clé d'accès |
|---|---|
| Bouton Précédent dans la barre d'adresses | **Alt+Flèche gauche** ou **Retour arrière** |
| Bouton Transférer dans la barre d'adresse | **Alt+flèche droite** |
| Refresh | **F5** |
| Zone Notifications, ouvrir la boîte de dialogue Détails de la tâche | **Alt+N** |
| Menu Gérer | **Alt+M** |
| Menu Affichage | **Alt+V** |
| menu d'aide | **Alt+H** |
| Ouvrir l'aide du Gestionnaire de serveur | **F1** |
| Zoom avant | **Ctrl+Plus (+)** |
| Zoom arrière | **Ctrl+Moins (-)** |
| Afficher la console à 100 % | **Ctrl+0** |

### Vignettes sur les pages Rôle, Groupe ou Serveur local

Agrandir le tableau

| Groupe de contrôles | Clé d'accès |
|---|---|
| Vignette Propriétés de la page Serveur local | **Alt+P** |
| Vignette Événements de la page de rôles, de groupes ou de serveurs locaux | **Alt+E** |
| Vignette Services de la page de rôles, de groupes ou de serveurs locaux | **Alt+R** |
| Vignette Best Practices Analyzer (BPA) de la page Rôle, Groupe ou Serveur local | **Alt+B** |
| Vignette Performances de la page de rôles, de groupes ou de serveurs locaux | **Alt+O** |
| Vignette Rôles et fonctionnalités de la page de rôles, de groupes ou de serveurs locaux | **Alt+A** |
| Vignette Serveurs de la page Tous les serveurs | **Alt+A** |

### Navigation dans la vignette Propriétés du serveur local

Agrandir le tableau

| Groupe de contrôles | Clé d'accès |
|---|---|
| computer name | Alt+C |
| Dernières mises à jour installées | Alt+L |
| Domaine ou groupe de travail | Alt+D |
| Mise à jour de Windows | Alt+W |
| Dernière recherche de mises à jour | Alt+S |
| remote management | Alt+R |
| Pare-feu Windows | Alt+F |
| Remote Desktop | Alt+K |
| Rapport d'erreurs Windows | Alt+G |
| Association de cartes réseau | Alt+T |
| Programme d'amélioration du produit | Alt+X |
| Connexion Ethernet câblée | Alt+O |
| Configuration de sécurité renforcée d'Internet Explorer | Alt+Y |
| time zone | Alt+Z |

### Navigation dans les vignettes Événements, Services, BPA, Performances, et Rôles et fonctionnalités

Agrandir le tableau

| Groupe de contrôles | Clé d'accès |
|---|---|
| Menu Tâches | Alt+T |
| Contrôle de filtre | Alt+F |
| contrôle de requête | Alt+Q |
| Enregistrer des requêtes | Alt+S |

# Installer et gérer les outils d'administration de serveur distant dans Windows

22/08/2025

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

Les outils d'administration de serveur distant (RSAT) pour Windows Server sont un ensemble d'utilitaires qui permettent aux administrateurs informatiques de gérer à distance les rôles et fonctionnalités sur les systèmes Windows Server à partir d'un ordinateur client Windows. Cet article fournit une vue d'ensemble des outils d'administration de serveur distant (RSAT) pour Windows. L'article explique également comment les installer et les utiliser pour gérer les rôles et fonctionnalités Windows Server à partir d'un ordinateur client Windows Server ou Windows.

La méthode d'installation des outils RSAT varie en fonction de votre plateforme. Veillez à sélectionner votre plateforme dans les boutons au début de l'article.

## Qu'est-ce que les outils d'administration de serveur distant ?

RSAT inclut plusieurs types d'outils pour vous aider à gérer les serveurs à distance :

- **Gestionnaire de** serveur - Console centrale pour les tâches du serveur
- **Composants logiciels enfichables MMC** : Outils concentrés pour des services spécifiques
- **Modules PowerShell** - Scripts de ligne de commande et automatisation
- **Outils en ligne de commande** - Contrôle serveur direct à partir de l'invite de commandes

Ces outils simplifient l'administration à distance, ce qui facilite la configuration, la surveillance et la résolution des problèmes des environnements Windows Server n'importe où.

### Outils disponibles

Vous pouvez utiliser les RSAT suivants à partir d'un serveur Windows ou d'un ordinateur client Windows. Le tableau suivant vous montre quels outils sont disponibles pour chaque plateforme.

Agrandir le tableau

| Nom de l'outil RSAT | Descriptif | Windows Server | Client Windows (fonctionnalité à la demande) | Client Windows (DISM) |
|---|---|---|---|---|
| **Outils d'administration des fonctionnalités** | | | | |
| Utilitaires d'administration du chiffrement de lecteur BitLocker | Gérer le chiffrement de lecteur BitLocker sur des serveurs distants. | ✅ | ✅ | ✅ |
| Outils d'extensions de serveur BITS | Administrer les extensions du service de transfert intelligent en arrière-plan. | ✅ | ❌ | ❌ |
| Outils DataCenterBridging LLDP | Configurez les paramètres Data Center Bridging et LLDP. | ✅ | ✅ | ✅ |
| Outils de clustering de basculement | Gérer et configurer des clusters de basculement. | ✅ | ✅ | ✅ |
| Client Gestion des adresses IP (IPAM) | Administrer l'infrastructure d'adresses IP à l'aide d'IPAM. | ✅ | ✅ | ✅ |
| Outils d'équilibrage de charge réseau | Configurez et gérez les clusters d'équilibrage de charge réseau. | ✅ | ✅ | ✅ |
| Outils de machine virtuelle protégée | Gérer les machines virtuelles protégées. | ✅ | ❌ | ❌ |
| Outils SNMP | Administrer les services et les paramètres SNMP. | ✅ | ❌ | ❌ |
| Outils du service de migration de stockage | Gérer les services de migration de stockage. | ✅ | ✅ | ✅ |
| Module de réplica de stockage pour Windows PowerShell | Configurez et gérez la réplication du stockage. | ✅ | ✅ | ✅ |
| Module System Insights pour Windows PowerShell | Accéder à l'analytique prédictive pour Windows Server. | ✅ | ✅ | ✅ |
| Outils de serveur WINS | Gérer les serveurs WINS (Windows Internet Name Service). | ✅ | ❌ | ❌ |

| Nom de l'outil RSAT | Descriptif | Windows Server | Client Windows (fonctionnalité à la demande) | Client Windows (DISM) |
|---|---|---|---|---|
| **Outils d'administration des rôles** | | | | |
| Outils AD DS et AD LDS | Gérer les services de domaine Active Directory et les services d'annuaire léger. | ✅ | ✅ | ✅ |
| Hyper-V Outils de gestion | Gérez Hyper-V ordinateurs hôtes et machines virtuelles. | ✅ | ❌ | ✅ |
| Outils des services Bureau à distance | Gérer l'hôte de session Bureau à distance, la passerelle et d'autres rôles RDS. | ✅ | ✅ | ✅ |
| Outils Windows Server Update Services | Administrer des serveurs WSUS et gérer les mises à jour pour les systèmes Windows. | ✅ | ✅ | ✅ |
| Outils des services de certificats Active Directory | Gérer les services de certificats AD et les composants associés. | ✅ | ✅ | ✅ |
| Outils de gestion des droits des services Active Directory | Administrer les services AD Rights Management. | ✅ | ❌ | ❌ |
| Outils du serveur DHCP | Administrer et configurer des serveurs et des étendues DHCP. | ✅ | ✅ | ✅ |
| Outils du serveur DNS | Gérez les serveurs, zones et enregistrements DNS. | ✅ | ✅ | ✅ |
| Outils de serveur de télécopie | Gérer les rôles et les paramètres du serveur de télécopie. | ✅ | ❌ | ❌ |
| Outils Des services de fichiers | Administrer des dossiers partagés, des quotas et des ressources de serveur de fichiers. | ✅ | ✅ [1] | ✅ [1] |

| Nom de l'outil RSAT | Descriptif | Windows Server | Client Windows (fonctionnalité à la demande) | Client Windows (DISM) |
|---|---|---|---|---|
| Outils de gestion des contrôleurs de réseau | Gérer les contrôleurs réseau dans Windows Server. | ✅ | ✅ | ✅ |
| Outils de politiques réseau et d'accès | Administrer les stratégies réseau et les services d'accès. | ✅ | ❌ | ❌ |
| Outils de Services d'Impression et de Documents | Administrer des serveurs d'impression et des imprimantes. | ✅ | ❌ | ❌ |
| Outils de gestion de l'accès à distance | Gérer les rôles d'accès à distance et les services VPN. | ✅ | ✅ | ✅ |
| Outils d'activation de volume | Configurez et gérez les services d'activation en volume. | ✅ | ✅ | ✅ |
| Outils des services de déploiement Windows | Gérer les services de déploiement Windows pour les installations de système d'exploitation basées sur le réseau. | ✅ | ❌ | ❌ |
| Gestionnaire de serveur | Console de gestion centralisée pour la gestion des rôles et fonctionnalités du serveur. | ✅ [2] | ✅ | ✅ |

1. Les outils de gestion des services pour NFS sur des ordinateurs locaux et distants peuvent être ajoutés en tant que fonctionnalité facultative Windows à l'aide de DISM.
2. Le Gestionnaire de serveur est inclus dans Windows Server par défaut et n'est pas répertorié en tant qu'outil d'administration de serveur distant.

Pour en savoir plus sur les fonctionnalités disponibles à la demande RSAT, consultez la liste des services RSAT disponibles via des fonctionnalités à la demande.

# Prerequisites

Pour utiliser les outils d'administration de serveur distant, vous avez besoin des prérequis suivants :

- Un ordinateur exécutant l'un des systèmes d'exploitation suivants :

- Windows 10 (mise à jour cumulative d'octobre 2018 ou ultérieure) Éditions Pro ou Entreprise uniquement
- Éditions Windows 11 Professionnel ou Entreprise uniquement
- Toute version prise en charge de Windows Server

- Privilèges d'administration sur l'ordinateur sur lequel rsaT est installé.
- Privilèges d'administration sur les systèmes Windows Server distants pour le service que vous souhaitez gérer.
- Connectivité réseau aux systèmes Windows Server distants que vous souhaitez gérer.

# Installer les outils d'administration de serveur distant

Pour installer les outils d'administration de serveur distant sur Windows Server, sélectionnez votre méthode préférée :

Gestionnaire de serveur

Pour installer des disques RSAT à l'aide du Gestionnaire de serveur, procédez comme suit :

1. Connectez-vous à l'ordinateur Windows Server avec un compte disposant de privilèges d'administrateur.
2. Ouvrez le **Gestionnaire de serveur** à partir du menu Démarrer ou de la barre des tâches.
3. Dans le Gestionnaire de serveur, sélectionnez **Gérer** dans le coin supérieur droit.
4. Sélectionnez **Ajouter des rôles et des fonctionnalités** dans le menu déroulant.
5. Dans **l'Assistant Ajout de rôles et de fonctionnalités**, sélectionnez **Suivant** jusqu'à atteindre la section **Fonctionnalités** .
6. Dans la section **Sélectionner des fonctionnalités** , faites défiler vers le bas pour rechercher la catégorie **Outils d'administration de serveur distant** .
7. Développez la catégorie **Outils d'administration de serveur distant** pour afficher les outils disponibles.
8. Sélectionnez les outils spécifiques que vous souhaitez installer en cochant les cases correspondantes.

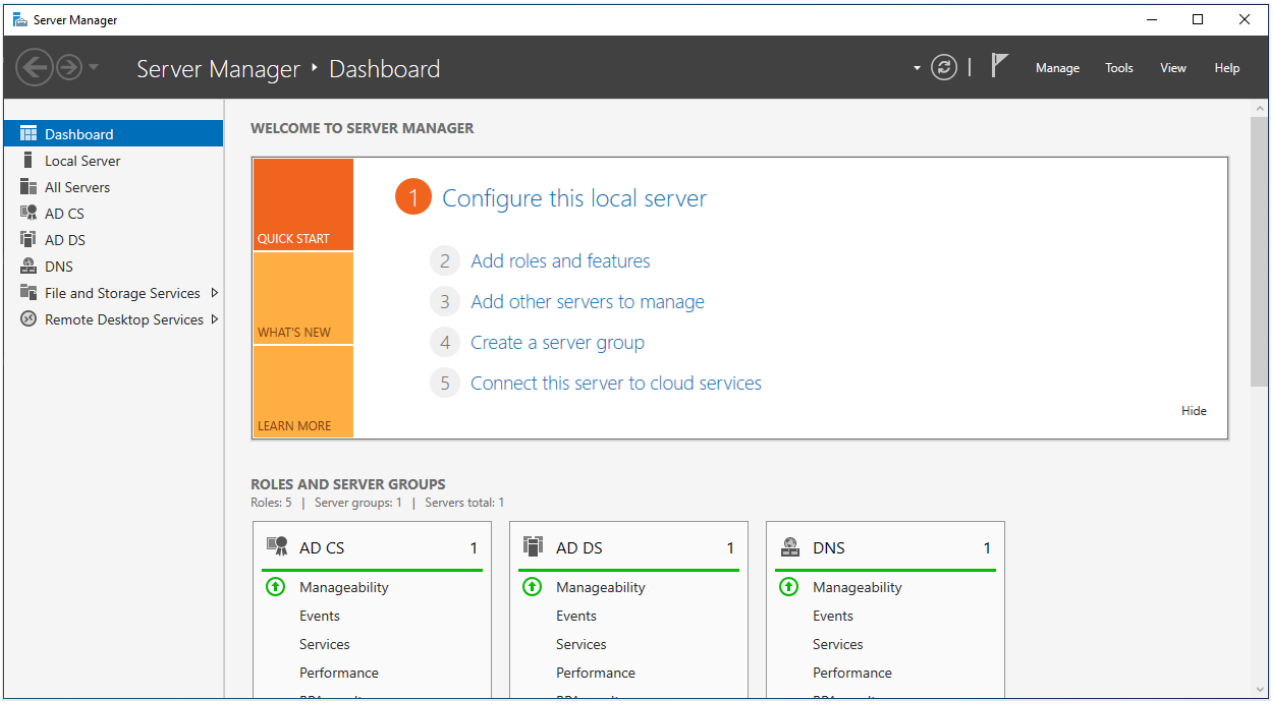
9. Sélectionnez **Suivant** , puis **installez** pour commencer le processus d'installation.
10. Attendez la fin de l'installation, puis sélectionnez **Fermer**.
11. Une fois l'installation terminée, vous pouvez accéder aux outils dans le menu **Outils** du Gestionnaire de serveur ou sélectionner **Outils Windows** dans le menu Démarrer.

# Gérer les serveurs locaux et distants avec le Gestionnaire de serveur

Le Gestionnaire de serveur peut être utilisé avec les autres outils inclus dans les outils d'administration de serveur distant pour gérer les serveurs locaux et distants à partir d'une seule expérience. Vous pouvez utiliser le Gestionnaire de serveur pour installer, configurer et gérer des rôles et des fonctionnalités sur plusieurs serveurs distants à partir d'une seule console.

Le Gestionnaire de serveur est inclus dans Windows Server par défaut et n'a pas besoin d'être installé séparément. Dans les étapes suivantes, vous allez utiliser le Gestionnaire de serveur pour ajouter un exemple d'outil d'administration de serveur distant et lancer l'outil de gestion associé.

1. Pour les nouvelles installations de Windows Server, le Gestionnaire de serveur s'ouvre automatiquement par défaut. Si le Gestionnaire de serveur ne s'ouvre pas automatiquement, ouvrez le menu Démarrer, puis sélectionnez **Gestionnaire de serveur**.




2. Dans le Gestionnaire de serveur, sélectionnez **Gérer** dans le coin supérieur droit.

3. Sélectionnez **Ajouter des rôles et des fonctionnalités** dans le menu déroulant.
4. Dans **l'Assistant Ajout de rôles et de fonctionnalités**, sélectionnez **Suivant** jusqu'à atteindre la section **Fonctionnalités** .
5. Développez la catégorie **Outils d'administration du serveur distant** , puis développez la catégorie **Outils d'administration de rôle** .
6. Cochez la case en regard des **outils de serveur DNS**, puis sélectionnez **Suivant**.
7. Sélectionnez **Installer** pour commencer le processus d'installation.
8. Sélectionnez **Fermer** une fois l'installation terminée.
9. Pour gérer un serveur DNS, sélectionnez **Outils** dans le coin supérieur droit du Gestionnaire de serveur, puis sélectionnez **DNS** dans le menu déroulant.
10. Vous pouvez maintenant utiliser la console du Gestionnaire DNS pour gérer le serveur DNS ou cliquer avec le bouton droit sur le nom du serveur dans le volet gauche pour vous connecter à un autre serveur DNS.

Pour en savoir plus sur l'utilisation du Gestionnaire de serveur pour gérer les serveurs distants, consultez Gestionnaire de serveur.

# Contenu connexe

- Configurer des fonctionnalités à la demande dans Windows Server
- Configurer la gestion à distance dans le Gestionnaire de serveur
- Gestionnaire de serveur '

# Vue d’ensemble d’OpenSSH pour Windows

16/08/2025

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

OpenSSH est la version open source des outils Secure Shell (SSH) utilisés par les administrateurs de Linux et d’autres non-Windows pour la gestion multiplateforme des systèmes distants. Depuis windows 10 build 1809 et Windows Server 2019, OpenSSH est disponible en tant que fonctionnalité à la demande.

SSH est basé sur une architecture client-serveur où le système sur lequel l’utilisateur travaille est le client et le système distant géré est le serveur. OpenSSH comprend une gamme de composants et d’outils conçus pour fournir une approche sécurisée et simple de l’administration du système à distance.

Le tableau suivant répertorie l’état d’installation par défaut d’OpenSSH pour Windows sur différentes versions de Windows.

Agrandir le tableau

| Version de Windows | État d’installation SSH |
|---|---|
| Windows Server 2019 | Non installé, installez et activez à l’aide de fonctionnalités facultatives |
| Windows Server 2022 | Non installé, installez et activez à l’aide de fonctionnalités facultatives |
| Windows Server 2025 | Installé, mais non activé |
| Windows 10 build 1809+ | Non installé, installez et activez à l’aide de fonctionnalités facultatives |

OpenSSH pour Windows comporte les commandes suivantes intégrées.

- `ssh` est le composant client SSH qui s’exécute sur le système local de l’utilisateur
- `sshd` est le composant serveur SSH qui doit s’exécuter sur le système géré à distance
- `ssh-keygen` génère, gère et convertit des clés d’authentification pour SSH
- `ssh-agent` stocke les clés privées utilisées pour l’authentification par clé publique
- `ssh-add` ajoute des clés privées à la liste autorisée par le serveur
- `ssh-keyscan` aide à collecter les clés d’hôte SSH publiques à partir d’hôtes
- `sftp` est le service qui fournit le protocole de transfert de fichiers sécurisé et s’exécute sur SSH
- `scp` est un utilitaire de copie de fichiers qui s’exécute sur SSH

> **Conseil**

La documentation se concentre sur l'utilisation d'OpenSSH sur Windows, notamment l'installation et la configuration, les commandes et les cas d'usage spécifiques à Windows. Une documentation détaillée supplémentaire sur les fonctionnalités OpenSSH courantes est disponible en ligne à **OpenSSH.com**.

Les commentaires sur Windows OpenSSH sont accueillis et peuvent être fournis en créant des problèmes GitHub dans notre dépôt GitHub OpenSSH. Le projet open source OpenSSH est géré par les développeurs du projet OpenBSD. Le fork Microsoft de ce projet se trouve dans GitHub.

# Étapes suivantes

- Bien démarrer avec OpenSSH

# Prise en main d'OpenSSH pour Windows

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

OpenSSH est un outil de connectivité pour la connexion à distance qui utilise le protocole SSH. Il chiffre tout le trafic entre le client et le serveur pour éliminer les écoutes clandestines, le détournement de connexion et d'autres attaques.

Un client compatible OpenSSH peut être utilisé pour se connecter à des appareils clients Windows Server et Windows.

Cet article utilise la fonction OpenSSH on Demand intégrée dans Windows et Windows Server. Microsoft prend en charge et assure cette version via Windows Update, c'est donc l'option recommandée pour la plupart des utilisateurs.

Microsoft maintient également PowerShell/openssh-portable, un fork du projet OpenSSH open source en amont. Ses versions peuvent différer de la version sous Windows.

## Prerequisites

Avant de commencer, votre ordinateur doit répondre aux exigences suivantes :

- Un appareil exécutant au moins Windows Server 2019 ou Windows 10 (build 1809).
- PowerShell 5.1 ou ultérieur.
- Compte membre du groupe Administrateurs intégré.

### Vérification des prérequis

Pour valider votre environnement, ouvrez une session PowerShell avec élévation de privilèges et procédez comme suit :

- Entrez *winver.exe* et appuyez sur Entrée pour afficher les détails de la version de votre appareil Windows.
- Exécutez le `$PSVersionTable.PSVersion`. Vérifiez que votre version principale est d'au moins 5 et que votre version secondaire est au moins 1. En savoir plus sur l'installation de PowerShell sur Windows.

- Pour vérifier quand vous êtes administrateur, exécutez la commande suivante. La sortie s'affiche `True` lorsque vous êtes membre du groupe Administrateurs intégré.

  **PowerShell**

  ```
  (New-Object
  Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurr
  ent())).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)
  ```

## Activer le serveur OpenSSH

À compter de Windows Server 2025, OpenSSH est maintenant installé par défaut. Vous pouvez également activer ou désactiver le service `sshd` dans Gestionnaire de serveur.

GUI

Pour activer SSHD à l'aide de Gestionnaire de serveur :

1. Dans **Gestionnaire de serveur**, dans le volet de navigation à gauche, sélectionnez **Local Server**.
2. Dans la fenêtre **Propriétés** , recherchez **l'accès SSH distant**.
3. Sélectionnez **Activé** pour activer le service OpenSSH.

> ⓘ **Remarque**
>
> Si vous devez autoriser ou restreindre des utilisateurs ou des groupes spécifiques à l'aide d'OpenSSH pour l'accès à distance, ajoutez-les au groupe d'utilisateurs **OpenSSH Users** .

## Se connecter à OpenSSH Server

Une fois installé, vous pouvez vous connecter à OpenSSH Server à partir d'un Windows ou d'un appareil Windows Server avec le client OpenSSH installé. À partir d'une invite PowerShell, exécutez la commande suivante.

**PowerShell**

```
ssh domain\username@servername
```

Une fois connecté, vous obtenez un message similaire à la sortie suivante.

PowerShell

```
The authenticity of host 'servername (10.00.00.001)' can't be established.
ECDSA key fingerprint is SHA256:(<a large string>).
Are you sure you want to continue connecting (yes/no)?
```

La saisie de *yes* ajoute ce serveur à la liste des hôtes SSH connus sur votre client Windows.

À ce stade, le service vous invite à saisir votre mot de passe. Par mesure de sécurité, les caractères de votre mot de passe ne s'affichent pas lorsque vous les saisissez.

Une fois connecté, vous devez voir l'invite d'interpréteur de commandes Windows suivante :

PowerShell

```
domain\username@SERVERNAME C:\Users\username>
```

# Désactiver le serveur OpenSSH

Vous pouvez désactiver le service `sshd` dans Gestionnaire de serveur.

GUI

Pour désactiver SSHD à l'aide de Gestionnaire de serveur :

1. Dans **Gestionnaire de serveur**, dans le volet de navigation à gauche, sélectionnez **Local Server**.
2. Dans la fenêtre **Propriétés** , recherchez **l'accès SSH distant**.
3. Sélectionnez **Désactivé** pour désactiver le service OpenSSH.

> ⓘ **Remarque**
>
> Si vous devez autoriser ou restreindre des utilisateurs ou des groupes spécifiques à l'aide d'OpenSSH pour l'accès à distance, ajoutez-les au groupe d'utilisateurs **OpenSSH Users** .

Si le service était en cours d'utilisation lorsque vous l'avez désinstallé, vous devez redémarrer Windows.

## Étapes suivantes

Maintenant que vous avez terminé d'installer OpenSSH Server pour Windows, voici quelques articles qui peuvent vous aider à apprendre à l'utiliser :

- En savoir plus sur l'utilisation de paires de clés pour l'authentification dans la gestion des clés OpenSSH
- En savoir plus sur la configuration OpenSSH Server pour Windows

ⓘ**Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Last updated on 08/09/2026

# Configuration d'OpenSSH Server pour Windows Server et Windows

13/08/2025

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

Cet article décrit la configuration spécifique à Windows pour OpenSSH Server (sshd).

OpenSSH gère une documentation détaillée sur les options de configuration en ligne à OpenSSH.com. Cette documentation n'est pas dupliquée dans ce jeu de documentation.

## Fichiers de configuration OpenSSH

OpenSSH contient des fichiers de configuration pour les paramètres serveur et client. OpenSSH est open source et a été ajouté aux systèmes d'exploitation clients Windows Server et Windows à partir de Windows Server 2019 et Windows 10 (build 1809). La documentation open source pour les fichiers de configuration OpenSSH n'est pas répétée ici. Les fichiers de configuration du client se trouvent dans la page manuelle ssh_config. Les fichiers de configuration du serveur OpenSSH se trouvent dans la page manuelle sshd_config.

OpenSSH Server lit les données de configuration par `%programdata%\ssh\sshd_config` défaut. Vous pouvez spécifier un autre fichier de configuration en exécutant `sshd.exe` le `-f` paramètre. Si le fichier est manquant, sshd en génère une avec la configuration par défaut au démarrage du service.

Dans Windows, le client OpenSSH (ssh) lit les données de configuration à partir d'un fichier de configuration dans l'ordre suivant :

1. Via `ssh.exe` le démarrage avec le `-F` paramètre, avec un chemin d'accès à un fichier de configuration et un nom d'entrée de ce fichier spécifié.
2. Via le fichier de configuration d'un utilisateur à l'adresse `%userprofile%\.ssh\config`.
3. Via le fichier de configuration à l'échelle du système à l'adresse `%programdata%\ssh\ssh_config`.

## Configuration de l'interpréteur de commandes par défaut pour OpenSSH dans Windows

L'interpréteur de commandes par défaut fournit l'expérience qu'un utilisateur voit lors de la connexion au serveur à l'aide de SSH. La valeur par défaut initiale dans Windows est l'invite de

commandes Windows (cmd.exe). Windows inclut également PowerShell et les interpréteurs de commandes autres que Microsoft sont également disponibles pour Windows et peuvent être configurés comme interpréteur de commandes par défaut pour un serveur.

Pour définir l'interpréteur de commandes par défaut, vérifiez d'abord que le dossier d'installation d'OpenSSH se trouve sur le chemin d'accès système. Pour Windows, le dossier d'installation par défaut est `%systemdrive%\Windows\System32\openssh`. La commande suivante montre le paramètre de chemin d'accès actuel et ajoute le dossier d'installation OpenSSH par défaut à celui-ci.

Agrandir le tableau

| Interpréteur de commandes | Commande à utiliser |
|---|---|
| Command | `path` |
| PowerShell | `$env:path` |

Vous pouvez configurer l'interpréteur de commandes ssh par défaut dans le Registre Windows en ajoutant le chemin complet à l'exécutable de l'interpréteur de commandes dans `HKEY_LOCAL_MACHINE\SOFTWARE\OpenSSH` la valeur `DefaultShell` de chaîne.

L'exemple de commande PowerShell avec élévation de privilèges suivant définit l'interpréteur de commandes `powershell.exe` par défaut pour OpenSSH Server. (La définition de ce chemin d'accès ne s'applique pas au client OpenSSH.)

PowerShell

```
$NewItemPropertyParams = @{
    Path         = "HKLM:\SOFTWARE\OpenSSH"
    Name         = "DefaultShell"
    Value        = "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
    PropertyType = "String"
    Force        = $true
}
New-ItemProperty @NewItemPropertyParams
```

# Configurations Windows dans sshd_config

Dans Windows, sshd lit les données de configuration par `%programdata%\ssh\sshd_config` défaut. Vous pouvez spécifier un autre fichier de configuration en exécutant `sshd.exe` le `-f` paramètre. Si le fichier est manquant, sshd en génère une avec la configuration par défaut au démarrage du service.

Les sections suivantes décrivent les paramètres de configuration spécifiques à Windows qui sont possibles par le biais d'entrées dans sshd_config. Il existe d'autres paramètres de configuration possibles qui ne sont pas répertoriés ici. Ils sont abordés en détail dans la documentation Win32 OpenSSH.

> **Conseil**
>
> OpenSSH Server (sshd) lit le fichier de configuration au démarrage du service. Toutes les modifications apportées au fichier de configuration nécessitent le redémarrage du service.

## AllowGroups, AllowUsers, DenyGroups, DenyUsers

Vous pouvez contrôler les utilisateurs et les groupes qui peuvent se connecter au serveur à l'aide des directives et `AllowGroups` `AllowUsers` des `DenyGroups` `DenyUsers` instructions. Les directives d'autorisation et de refus sont traitées dans l'ordre suivant : `DenyUsers`, , `AllowUsers` `DenyGroups`, et enfin `AllowGroups`.

Tous les noms de compte doivent être spécifiés en minuscules.

Pour plus d'informations sur les modèles et les caractères génériques dans ssh_config, consultez la page manuelle sshd_config OpenBSD.

Lorsque vous configurez des règles basées sur des utilisateurs/groupes avec un utilisateur ou un groupe de domaine, utilisez le format suivant : `user?domain*`.

Windows autorise plusieurs formats pour spécifier des principaux de domaine, mais peut entrer en conflit avec les modèles Linux standard. Pour cette raison, `*` il est utilisé pour couvrir les noms de domaine complets (FQDN). En outre, cette approche utilise `?`, au lieu de `@`, pour éviter les conflits avec le `username@host` format.

Les utilisateurs, les groupes et les comptes connectés à Internet sont toujours résolus en leur nom de compte local (aucune partie de domaine, similaire aux noms Unix standard). Les utilisateurs et les groupes de domaine sont strictement résolus au format `domain_short_name\user_name`.

Toutes les règles de configuration basées sur les utilisateurs et les groupes doivent respecter ce format.

L'exemple suivant refuse `contoso\admin` à l'hôte 192.168.2.23 et bloque tous les utilisateurs du domaine Contoso. Il permet également aux utilisateurs membres des groupes et `contoso\sshusers` des `contoso\serveroperators` groupes.

sshd_config

```
DenyUsers contoso\admin@192.168.2.23
DenyUsers contoso\*
AllowGroups contoso\sshusers contoso\serveroperators
```

L'exemple suivant permet à l'utilisateur `localuser` de se connecter à partir de l'hôte 192.168.2.23 et permet aux membres du groupe `sshusers`.

sshd_config

```
AllowUsers localuser@192.168.2.23
AllowGroups sshusers
```

## AuthenticationMethods

Pour Windows OpenSSH, les seules méthodes d'authentification disponibles sont `password` et `publickey`.

> **Important**
>
> L'authentification via un compte Microsoft Entra n'est actuellement pas prise en charge.

## AuthorizedKeysFile

La valeur par défaut est `.ssh/authorized_keys`. Si vous ne spécifiez pas de chemin absolu, OpenSSH recherche le fichier par rapport à votre répertoire de base, par `C:\Users\username` exemple . Si l'utilisateur appartient au groupe d'administrateurs, `%programdata%/ssh/administrators_authorized_keys` il est utilisé à la place.

> **Conseil**
>
> Le fichier *administrators_authorized_keys* doit uniquement avoir des entrées d'autorisation pour le compte et `NT Authority\SYSTEM` le `BUILTIN\Administrators` groupe de sécurité. Le compte NT Authority\SYSTEM doit disposer d'un contrôle total. Le `BUILTIN\Administrators` groupe de sécurité est requis pour permettre aux administrateurs de gérer les clés autorisées. Vous pouvez choisir l'accès requis. Pour accorder des autorisations, vous pouvez ouvrir une invite PowerShell avec élévation de privilèges et

exécuter la commande `icacls.exe "C:\ProgramData\ssh\administrators_authorized_keys" /inheritance:r /grant "Administrators:F" /grant "SYSTEM:F"`.

## ChrootDirectory (prise en charge ajoutée dans v7.7.0.0)

Cette directive est uniquement prise en charge avec les sessions SFTP. Une session à distance dans `cmd.exe` laquelle ne respecte `ChrootDirectory` pas . Pour configurer un serveur chroot sftp uniquement, définissez `ForceCommand` sur internal-sftp. Vous pouvez également configurer SCP avec chroot en implémentant un interpréteur de commandes personnalisé qui autorise uniquement SCP et SFTP.

## GSSAPIAuthentication

L'argument de configuration spécifie si l'authentification `GSSAPIAuthentication` utilisateur basée sur GSSAPI (Kerberos) est autorisée. La valeur par défaut pour `GSSAPIAuthentication` est non.

L'authentification GSSAPI nécessite également l'utilisation du commutateur spécifiant le nom d'hôte `-K` lorsque vous utilisez le client OpenSSH. Vous pouvez également créer une entrée correspondante dans la configuration du client SSH. Dans Windows, le client OpenSSH lit les données de configuration par `%userprofile%\.ssh\config` défaut.

Voici un exemple de configuration du client GSSAPI OpenSSH :

config

```
# Specify a set of configuration arguments for a host matching the
# pattern SERVER01.contoso.com.
#
# Patterns are case sensitive.
Host SERVER01.contoso.com
    # Enables GSSAPI authentication.
    GSSAPIAuthentication yes
    # Forward (delegate) credentials to the server.
    GSSAPIDelegateCredentials yes
```

> **ⓘ Important**
>
> GSSAPI est disponible uniquement à partir de Windows Server 2022, Windows 11 et Windows 10 (mise à jour de mai 2021 ).

## HostKey

Les valeurs par défaut sont les suivantes :

sshd_config

```
#HostKey __PROGRAMDATA__/ssh/ssh_host_rsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_dsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ecdsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ed25519_key
```

Si les valeurs par défaut ne sont pas présentes, sshd les génère automatiquement au démarrage d'un service.

## Match

Correspond aux conditions à l'aide d'un ou plusieurs critères. Lors d'une correspondance, les arguments de configuration suivants sont appliqués. La correspondance utilise les règles de modèle couvertes dans la section AllowGroups, AllowUsers, DenyGroups, DenyUsers . Les noms d'utilisateur et de groupe doivent être en minuscules.

## PermitRootLogin

Non applicable dans Windows. Pour empêcher les administrateurs de se connecter, utilisez les administrateurs avec la `DenyGroups` directive.

## SyslogFacility

Si vous avez besoin d'une journalisation basée sur des fichiers, utilisez `LOCAL0`. Les journaux sont générés sous `%programdata%\ssh\logs`. Pour toute autre valeur, y compris la valeur par défaut, AUTH dirige la journalisation vers ETW. Pour plus d'informations, consultez Les fonctionnalités de journalisation dans Windows .

## Arguments de configuration

L'argument de configuration suivant est disponible à partir de Windows Server 2022, Windows 11 et Windows 10 (mise à jour de mai 2021 ) :

- `GSSAPIAuthentication`

Les arguments de configuration suivants ne sont pas disponibles dans la version OpenSSH fournie dans Windows Server et Windows :

- `AcceptEnv`
- `AllowStreamLocalForwarding`
- `AuthorizedKeysCommand`
- `AuthorizedKeysCommandUser`
- `AuthorizedPrincipalsCommand`
- `AuthorizedPrincipalsCommandUser`
- `ExposeAuthInfo`
- `GSSAPICleanupCredentials`
- `GSSAPIStrictAcceptorCheck`
- `HostbasedAcceptedKeyTypes`
- `HostbasedAuthentication`
- `HostbasedUsesNameFromPacketOnly`
- `IgnoreRhosts`
- `IgnoreUserKnownHosts`
- `KbdInteractiveAuthentication`
- `KerberosAuthentication`
- `KerberosGetAFSToken`
- `KerberosOrLocalPasswd`
- `KerberosTicketCleanup`
- `PermitTunnel`
- `PermitUserEnvironment`
- `PermitUserRC`
- `PidFile`
- `PrintLastLog`
- `PrintMotd`
- `RDomain`
- `StreamLocalBindMask`
- `StreamLocalBindUnlink`
- `StrictModes`
- `X11DisplayOffset`
- `X11Forwarding`
- `X11UseLocalhost`
- `XAuthLocation`

# Authentification basée sur des clés dans OpenSSH pour Windows

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

La plupart des authentifications dans les environnements Windows se font avec une paire de nom d'utilisateur/mot de passe, ce qui fonctionne bien pour les systèmes qui partagent un domaine commun. Lorsque vous travaillez sur plusieurs domaines, comme entre les systèmes locaux et hébergés dans le cloud, ce type d'authentification devient vulnérable aux intrusions par force brute.

Par comparaison, les environnements Linux utilisent généralement des paires de clés publiques/privées pour piloter l'authentification qui ne nécessite pas l'utilisation de mots de passe devinables. OpenSSH inclut des outils pour prendre en charge l'authentification basée sur des clés, en particulier :

- **ssh-keygen** pour générer des clés sécurisées.
- **ssh-agent** et **ssh-add** pour stocker en toute sécurité des clés privées.
- **scp** et **sftp** pour copier en toute sécurité des fichiers de clé publique lors de l'utilisation initiale d'un serveur.

Ce document fournit une vue d'ensemble de l'utilisation de ces outils sur Windows pour commencer à utiliser l'authentification basée sur des clés avec Secure Shell (SSH). Si vous n'êtes pas familiarisé avec la gestion des clés SSH, nous vous recommandons vivement de consulter le document NIST IR 7966, intitulé *Sécurité de la gestion des accès interactif et automatisé à l'aide de Secure Shell (SSH)*.

L'authentification basée sur des clés dans OpenSSH pour Windows fonctionne avec des comptes Windows locaux et des comptes Active Directory (domaine). Les comptes Microsoft Entra ID ne prennent pas en charge l'authentification basée sur des clés.

> **Note**
>
> Windows OpenSSH ne prend pas en charge les directives `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser`. Cela signifie que vous ne pouvez pas extraire dynamiquement des clés SSH à partir d'Active Directory à l'aide de ces directives, comme vous pourriez le faire sur un système Linux. Pour plus d'informations sur les options de configuration prises en charge, consultez la configuration d'OpenSSH Server pour Windows Server et Windows.

# Paires de clés

Les paires de clés font référence aux fichiers de clé publique et privée utilisés par certains protocoles d'authentification.

L'authentification par clé publique SSH utilise des algorithmes de chiffrement asymétriques pour générer deux fichiers clés , un *privé* et l'autre *public*. Chaque fichier de clé privée est l'équivalent d'un mot de passe et doit rester protégé dans toutes les circonstances. Si quelqu'un détient votre clé privée, il peut se connecter en votre nom à n'importe quel serveur SSH auquel vous avez accès. La clé publique est ce qui est placé sur le serveur SSH et peut être partagée sans compromettre la clé privée.

Le serveur SSH et le client peuvent utiliser l'authentification basée sur des clés pour comparer la clé publique d'un nom d'utilisateur fourni par rapport à la clé privée. Si la clé publique côté serveur ne peut pas être validée par rapport à la clé privée côté client, l'authentification échoue.

Vous pouvez implémenter l'authentification multifacteur avec des paires de clés en entrant une phrase secrète lorsque vous générez la paire de clés. Pour plus d'informations, consultez Génération de clé utilisateur. L'utilisateur est invité à entrer la phrase secrète pendant l'authentification. La phrase secrète combinée à la présence de la clé privée est utilisée sur le client SSH pour authentifier l'utilisateur.

> **ⓘ Important**
>
> Une session distante ouverte via l'authentification basée sur des clés n'a pas d'informations d'identification utilisateur associées. Par conséquent, la session n'est pas capable d'authentification sortante en tant qu'utilisateur. Ce comportement est voulu.

# Génération d'une clé d'hôte

Les clés publiques ont des exigences de liste de contrôle d'accès (ACL) spécifiques qui, sur Windows, équivaut à autoriser uniquement l'accès aux administrateurs et à l'utilisateur système. La première fois que le `sshd` service est utilisé, la paire de clés pour l'hôte est générée automatiquement.

> **ⓘ Important**
>
> Vous devez installer OpenSSH Server avant de pouvoir exécuter les commandes de cet article. Pour plus d'informations, consultez Prise en main d'OpenSSH pour Windows.

Par défaut, vous devez démarrer `sshd` manuellement. Pour le configurer pour démarrer automatiquement chaque fois que le serveur est redémarré, exécutez les commandes suivantes à partir d'une invite PowerShell avec élévation de privilèges sur votre serveur :

PowerShell

```
# Set the sshd service to be started automatically.
Get-Service -Name sshd | Set-Service -StartupType Automatic

# Start the sshd service.
Start-Service sshd
```

Étant donné qu'aucun utilisateur n'est associé au `sshd` service, les clés hôtes sont stockées sous *C :\ProgramData\ssh*.

# Génération d'une clé utilisateur

Pour utiliser l'authentification par clé, vous devez d'abord générer des paires de clés publiques/privées pour votre client. Vous pouvez utiliser `ssh-keygen.exe` pour générer des fichiers clés. Vous pouvez spécifier les algorithmes de génération de clés suivants :

- Algorithme de signature numérique (DSA)
- Rivest-Shamir-Adleman (RSA)
- Algorithme de signature numérique à courbe elliptique (ECDSA)
- Ed25519

Si vous ne spécifiez pas d'algorithme, Ed25519 est utilisé. Un algorithme et une longueur de clé forts doivent être utilisés, comme ECDSA dans cet exemple.

Pour générer des fichiers clés à l'aide de l'algorithme ECDSA, exécutez la commande suivante dans une fenêtre PowerShell ou Invite de commandes sur votre client :

PowerShell

```
ssh-keygen -t ecdsa
```

La sortie de la commande doit ressembler aux lignes suivantes, sauf qu'elle `username` est remplacée par votre nom d'utilisateur :

Output

```
Generating public/private ecdsa key pair.
Enter file in which to save the key (C:\Users\username/.ssh/id_ecdsa):
```

À l'invite, vous pouvez sélectionner **Entrée** pour accepter le chemin d'accès au fichier par défaut, ou vous pouvez spécifier un chemin d'accès ou un nom de fichier pour vos clés générées.

Ensuite, vous êtes invité à utiliser une phrase secrète pour chiffrer vos fichiers de clé privée. En général, nous vous déconseillons d'utiliser une phrase secrète vide, car la phrase secrète fonctionne avec le fichier clé pour fournir une authentification à deux facteurs. Mais pour cet exemple, vous pouvez laisser le mot de passe vide.

Output

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\username/.ssh/id_ecdsa.
Your public key has been saved in C:\Users\username/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:OIzc1yE7joL2Bzy8!gS0j8eGK7bYaH1FmF3sDuMeSj8 username@LOCAL-HOSTNAME

The key's randomart image is:
+--[ECDSA 256]--+
|        .        |
|         o       |
|    . + + .      |
|   o B * = .     |
|   o= B S .      |
|   .=B O o       |
|  + =+% o        |
| *oo.O.E         |
|+.o+=o. .        |
+----[SHA256]-----+
```

Vous disposez maintenant d'une paire de clés ECDSA publique/privée à l'emplacement spécifié. Le fichier .pub est la clé publique, et le fichier sans extension est la clé privée :

Output

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/3/2021   2:55 PM            464 id_ecdsa
-a----         6/3/2021   2:55 PM            103 id_ecdsa.pub
```

Un fichier de clé privée est l'équivalent d'un mot de passe et doit être protégé de la même façon que vous protégez votre mot de passe. Vous pouvez utiliser `ssh-agent` pour stocker en toute sécurité vos clés privées dans un contexte de sécurité Windows associé à votre compte Windows. Pour configurer le `ssh-agent` service de manière à démarrer automatiquement chaque fois que votre ordinateur est redémarré et à utiliser `ssh-add` pour stocker la clé privée,

exécutez les commandes suivantes à une invite PowerShell avec élévation de privilèges sur votre serveur :

PowerShell

```
# By default, the ssh-agent service is disabled. Configure it to start
automatically.
# Run the following command as an administrator.
Get-Service ssh-agent | Set-Service -StartupType Automatic

# Start the service.
Start-Service ssh-agent

# The following command should return a status of Running.
Get-Service ssh-agent

# Load your key files into ssh-agent.
ssh-add $env:USERPROFILE\.ssh\id_ecdsa
```

Après avoir ajouté la clé au `ssh-agent` service sur votre client, le `ssh-agent` service récupère automatiquement la clé privée locale et le transmet à votre client SSH.

> ⓘ **Important**
>
> Nous vous recommandons de sauvegarder votre clé privée dans un emplacement sécurisé, puis de la supprimer du système local *après* l'avoir ajoutée au `ssh-agent` service. La clé privée ne peut pas être récupérée à partir de l'agent lorsqu'un algorithme fort, tel qu'ECDSA, est utilisé dans cet exemple. Si vous perdez l'accès à la clé privée, vous devez créer une paire de clés et mettre à jour la clé publique sur tous les systèmes avec lesquels vous interagissez.

# Déployer la clé publique

Pour utiliser la clé utilisateur que vous avez créée précédemment, vous devez placer le contenu de votre clé publique (*\.ssh\id_ecdsa.pub*) sur le serveur dans un fichier texte. Le nom et l'emplacement du fichier varient selon que le compte d'utilisateur est membre du groupe d'administrateurs local ou d'un compte d'utilisateur standard. Les sections suivantes couvrent les utilisateurs standard et administratifs.

## Utilisateur standard

Vous devez placer le contenu de votre clé publique (*\.ssh\id_ecdsa.pub*) sur le serveur dans un fichier texte appelé `authorized_keys` en *C :\Users\username\.ssh*. Vous pouvez copier votre clé

publique à l'aide de l'utilitaire de transfert de fichiers sécurisé OpenSSH `scp` ou à l'aide de PowerShell pour écrire la clé dans le fichier.

Vous pouvez utiliser le code suivant pour copier la clé publique sur le serveur. Dans la dernière ligne, remplacez `username` par votre nom d'utilisateur. Au départ, vous êtes invité à entrer un mot de passe pour le compte d'utilisateur du serveur.

PowerShell

```
# Get the public key file generated previously on your client.
$authorizedKey = Get-Content -Path $env:USERPROFILE\.ssh\id_ecdsa.pub

# Generate the PowerShell command to run remotely that copies the public key file
generated previously on your client to the authorized_keys file on your server.
$remotePowershell = "powershell New-Item -Force -ItemType Directory -Path
$env:USERPROFILE\.ssh; Add-Content -Force -Path
$env:USERPROFILE\.ssh\authorized_keys -Value '$authorizedKey'"

# Connect to your server and run the PowerShell command by using the
$remotePowerShell variable.
ssh username@domain1@contoso.com $remotePowershell
```

## Utilisateur administratif

Vous devez placer le contenu de votre clé publique (*\.ssh\id_ecdsa.pub*) sur le serveur dans un fichier texte appelé `administrators_authorized_keys` en *C :\ProgramData\ssh*. Vous pouvez copier votre clé publique à l'aide de l'utilitaire de transfert de fichiers sécurisé OpenSSH `scp` ou à l'aide de PowerShell pour écrire la clé dans le fichier. La liste de contrôle d'accès sur ce fichier doit être configurée pour autoriser uniquement l'accès aux administrateurs et à l'utilisateur système.

Vous pouvez utiliser le code suivant pour copier la clé publique sur le serveur et configurer la liste de contrôle d'accès. Dans la dernière ligne, remplacez `username` par votre nom d'utilisateur. Au départ, vous êtes invité à entrer un mot de passe pour le compte d'utilisateur du serveur.

> **Note**
>
> Cet exemple montre les étapes pour créer le fichier `administrators_authorized_keys`. Ce fichier s'applique uniquement aux comptes d'administrateur. Vous devez l'utiliser au lieu du fichier spécifique à l'utilisateur à l'emplacement du profil de l'utilisateur.

PowerShell

```
# Get the public key file generated previously on your client.
$authorizedKey = Get-Content -Path $env:USERPROFILE\.ssh\id_ecdsa.pub

# Generate the PowerShell command to run remotely that copies the public key file
generated previously on your client to the authorized_keys file on your server.
$remotePowershell = "powershell Add-Content -Force -Path
$env:ProgramData\ssh\administrators_authorized_keys -Value
'''$authorizedKey''';icacls.exe
""$env:ProgramData\ssh\administrators_authorized_keys"" /inheritance:r /grant
""Administrators:F"" /grant ""SYSTEM:F"""

# Connect to your server and run the PowerShell command by using the
$remotePowerShell variable.
ssh username@domain1@contoso.com $remotePowershell
```

Pour les versions non localisées anglaises du système d'exploitation, le script doit être modifié pour refléter les noms de groupes en conséquence. Pour éviter les erreurs qui peuvent se produire lorsque vous accordez des autorisations aux noms de groupe, vous pouvez utiliser l'identificateur de sécurité (SID) à la place du nom du groupe. Vous pouvez récupérer le SID en exécutant `Get-LocalGroup | Select-Object Name, SID`. Lorsque vous utilisez le SID à la place du nom du groupe, il doit être précédé d'un astérisque (*). Dans l'exemple suivant, le groupe **Administrateurs** utilise le SID `S-1-5-32-544`:

PowerShell

```
$remotePowershell = "powershell Add-Content -Force -Path
$env:ProgramData\ssh\administrators_authorized_keys -Value
'''$authorizedKey''';icacls.exe
""$env:ProgramData\ssh\administrators_authorized_keys"" /inheritance:r /grant ""*S-
1-5-32-544:F"" /grant ""SYSTEM:F"""
```

Ces étapes terminent la configuration requise pour utiliser l'authentification basée sur clé avec OpenSSH sur Windows. Après avoir exécuté ces commandes PowerShell, vous pouvez vous connecter à l'hôte `sshd` à partir de n'importe quel client disposant de la clé privée.

---

Last updated on 03/10/2025

# Comment gérer OpenSSH avec la Stratégie de Groupe

15/02/2024

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

La Stratégie de Groupe vous permet de spécifier des configurations gérées pour les utilisateurs et les ordinateurs. Cette page vous aidera à créer un objet de stratégie de groupe pour gérer le composant Serveur OpenSSH.

## Prérequis

Avant de commencer, les conditions suivantes doivent être remplies au préalable :

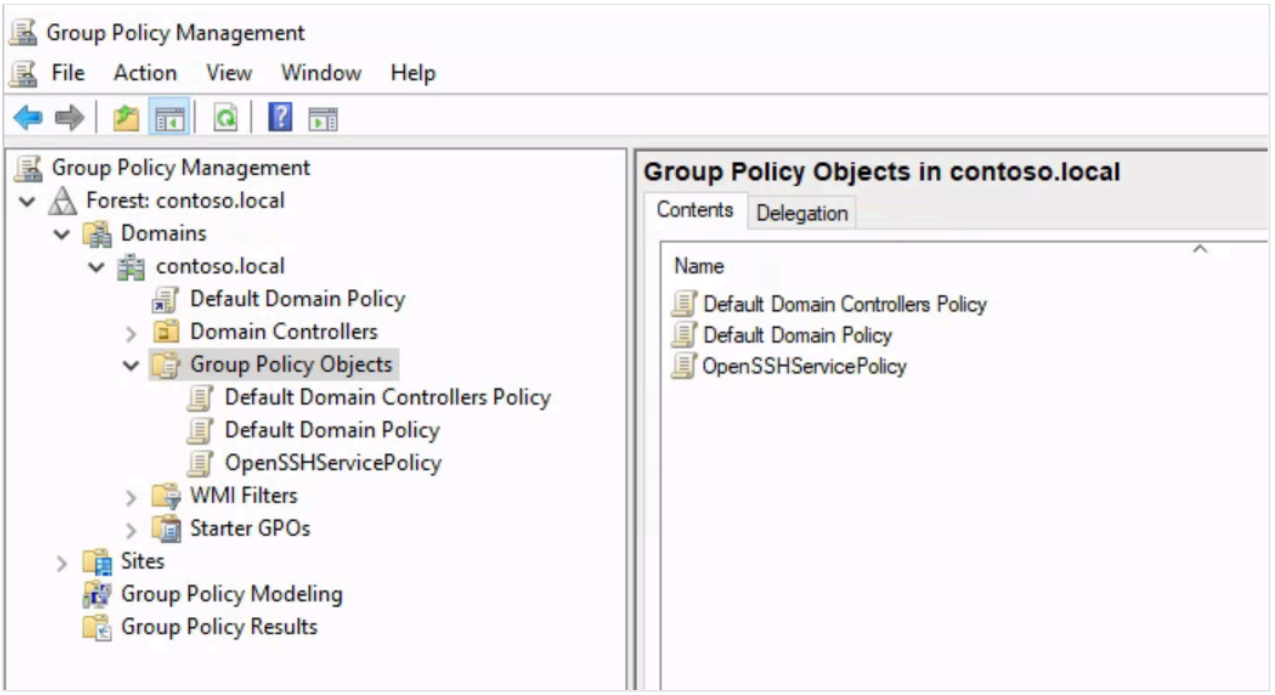
- Vous avez des droits d'administrateur sur l'appareil local et les permissions appropriées pour mettre à jour la Stratégie de Groupe sur votre contrôleur de domaine
- Vous gérez la version intégrée d'OpenSSH
- Vous gérez des systèmes d'exploitation où OpenSSH et la Stratégie de Groupe sont présents

## Créer un objet de stratégie de groupe

Pour créer une Stratégie de Groupe pour gérer OpenSSH, veuillez suivre la procédure suivante :

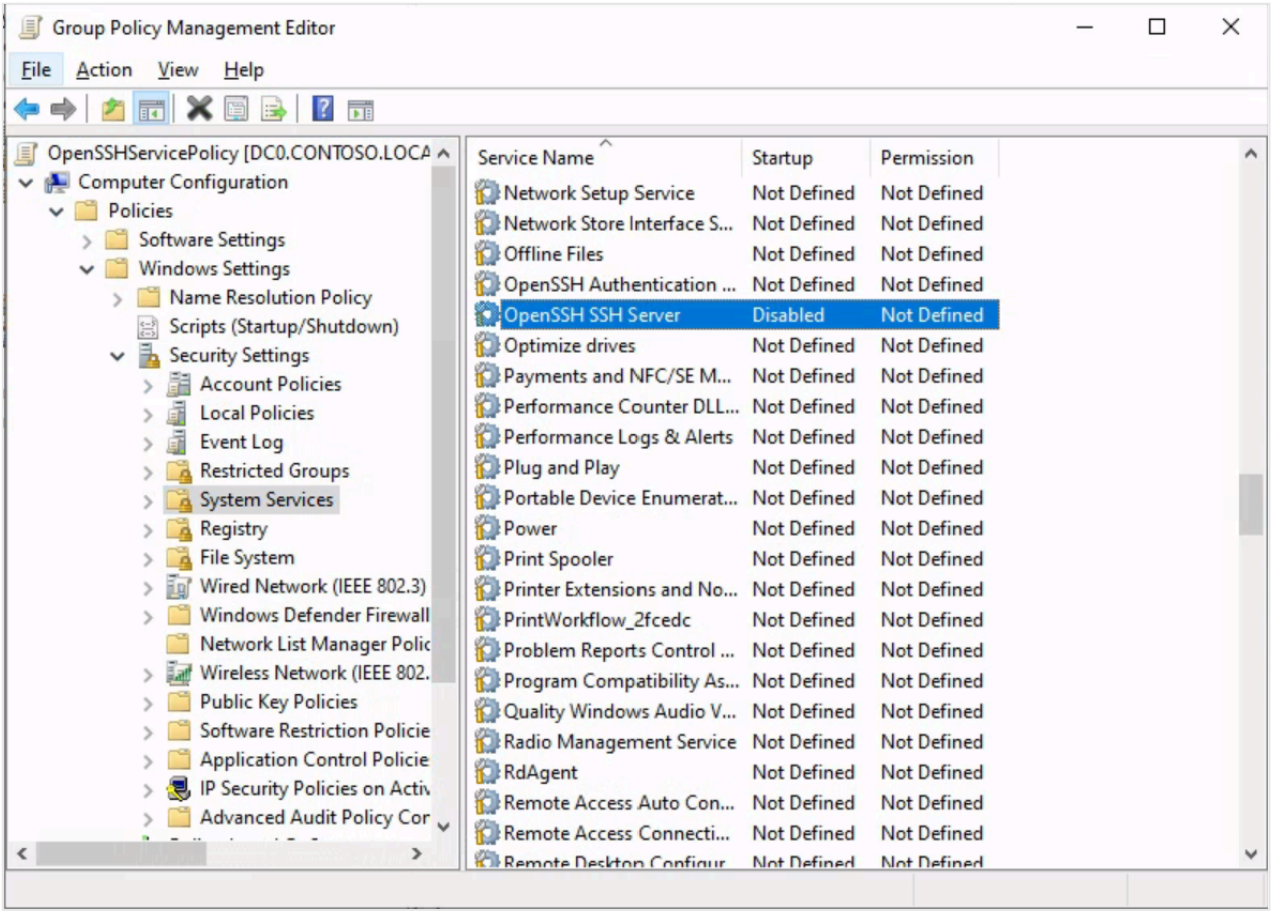
1. Ouvrez l'outil de gestion de stratégie de groupe.
2. Dans le volet de navigation, développez `Forest: your forest name`, développez `Domains`, développez votre domaine.
3. Sélectionnez `Group Policy Objects`.
4. Faites un clic droit sur `Group Policy Objects`, puis sélectionnez Nouveau pour créer un nouvel Objet.

5. Nommez l'Objet de manière à ce qu'il puisse être identifié comme gérant OpenSSH.




6. Double-cliquez sur le nouvel Objet.
7. Naviguez vers l'onglet `Settings`.
8. Faites un clic droit sur `Computer Configuration`, puis sélectionnez `Edit...`.
9. Dans le volet de navigation, développez `Computer Configuration`, développez `Policies`, développez `Windows Settings`, développez `Security Settings`, puis sélectionnez `System Services`.
10. Double-cliquez sur `OpenSSH SSH Server` dans la liste des services.
11. Cliquez sur le symbole de vérification `Define this policy setting`.

12. Sélectionnez le mode de démarrage de service souhaité; `Automatic`, `Manual`, `Disabled`.




13. Sélectionnez `Apply`.

# Vue d’ensemble de Windows Server Update Services (WSUS)

Article • 05/05/2025 •

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

Windows Server Update Services (WSUS) permet aux administrateurs informatiques de déployer les dernières mises à jour du produit Microsoft. Grâce à WSUS, vous pouvez gérer entièrement la distribution des mises à jour publiées par Microsoft Update sur les ordinateurs de votre réseau. Cet article fournit une vue d’ensemble de ce rôle de serveur et des informations supplémentaires sur la façon de déployer et d’assurer la maintenance des services WSUS.

> ⓘ **Notes**
>
> WSUS est déconseillé et n’ajoute plus de nouvelles fonctionnalités. Toutefois, elle continue d’être prise en charge pour les déploiements de production et reçoit des mises à jour de sécurité et de qualité en fonction du cycle de vie du produit. Pour plus d’informations, consultez Fonctionnalités supprimées ou non développées dans Windows Server.

## Description du rôle serveur WSUS

Un serveur WSUS vous fournit les fonctionnalités dont vous avez besoin pour gérer et distribuer des mises à jour par le biais d’une console de gestion. Un serveur WSUS peut également être la source de mises à jour d’autres serveurs WSUS de l’organisation. Le serveur WSUS qui agit en tant que source des mises à jour est appelé serveur en amont. Dans une implémentation WSUS, au moins un serveur WSUS de votre réseau doit se connecter à Microsoft Update pour obtenir les informations sur les mises à jour disponibles. En tant qu’administrateur, vous pouvez déterminer le nombre d’autres serveurs WSUS se connectant directement à Microsoft Update en fonction de la configuration et de la sécurité du réseau.

WSUS inclut les fonctionnalités suivantes :

- Applets de commande Windows PowerShell pour gérer les tâches administratives les plus importantes dans WSUS.
- Fonctionnalité d’algorithme de hachage sécurisé 256 bits (SHA-256) pour une sécurité supplémentaire.
- Séparation du client et du serveur : les versions de l’agent Windows Update (WUA) peuvent être déployées indépendamment de WSUS.

# Cas pratiques

La gestion des mises à jour est le processus de contrôle du déploiement et de la gestion des versions de logiciels intermédiaires dans les environnements de production. Elle vous aide à assurer l'efficacité des opérations, à surmonter les failles de sécurité et à maintenir la stabilité de votre environnement de production. Le maintien d'un niveau de confiance connu dans les systèmes d'exploitation et les logiciels d'application de votre organisation vous permet d'éviter les vulnérabilités de sécurité qui, si elles sont exploitées, peuvent entraîner une perte de revenus et de propriété intellectuelle. La réduction de cette menace vous oblige à configurer correctement les systèmes, à utiliser les derniers logiciels et à installer les mises à jour logicielles recommandées.

Les principaux scénarios dans lesquels WSUS ajoute une valeur commerciale sont les suivants :

- gestion des mises à jour centralisée ;
- automatisation de la gestion des mises à jour.

## Utiliser Windows PowerShell pour gérer WSUS

Pour que les administrateurs système puissent automatiser leurs opérations, ils ont besoin de couverture par le biais d'une automatisation de ligne de commande. L'objectif principal est de faciliter l'administration WSUS en fournissant un moyen aux administrateurs système d'automatiser leurs opérations quotidiennes. L'ajout d'opérations WSUS principales à Windows PowerShell permet aux administrateurs d'augmenter la productivité, de réduire la courbe d'apprentissage des nouveaux outils et d'augmenter la cohérence entre les opérations similaires. Les applets de commande Windows PowerShell pour les opérations WSUS ajoutent flexibilité et souplesse pour l'administrateur système.

# Plateforme de mise à jour unifiée

À compter du 28 mars 2023, WSUS prend en charge les mises à jour de la plateforme de mise à jour unifiée (UUP) pour les clients Windows 11 version 21H2. Pour plus d'informations, consultez Planifier vos déploiements WSUS.

> **ⓘ Important**
>
> Cette modification nécessite une installation de mise à jour ou l'ajout manuel de types MIME (Multipurpose Internet Mail Extensions) à Internet Information Services (IIS) sur les serveurs WSUS. Les clients utilisant Windows 11 version 22H2 peuvent échouer à installer

les mises à jour à partir de WSUS si le serveur n'est pas mis à jour. Pour plus d'informations, consultez **considérations relatives à l'UUP**.

## Contenu connexe

Pour plus d'informations sur la planification, le déploiement et la gestion de WSUS, consultez les guides suivants :

- Déployer Windows Server Update Services
- Update Management avec Windows Server Update Services

# Déployer Windows Server Update Services

Article • 02/11/2024 •

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

WSUS (Windows Server Update Services) permet aux administrateurs informatiques de déployer les dernières mises à jour de produits Microsoft. WSUS est un rôle de serveur Windows Server qui peut être installé pour gérer et distribuer des mises à jour. Un serveur WSUS peut être la source des mises à jour pour les autres serveurs WSUS de l'organisation. Le serveur WSUS qui agit en tant que source des mises à jour est appelé serveur en amont.

Dans une implémentation WSUS, au moins un serveur WSUS du réseau doit se connecter à Microsoft Update pour obtenir les informations sur les mises à jour disponibles. Vous pouvez déterminer, en fonction de la configuration et de la sécurité du réseau, le nombre d'autres serveurs se connectant directement à Microsoft Update.

Ce guide fournit des informations conceptuelles pour la planification et le déploiement de WSUS.

- Planifier votre déploiement WSUS
- Étape 1 : installer le rôle serveur WSUS
- Étape 2 : configurer WSUS
- Étape 3 : approuver et déployer des mises à jour dans WSUS
- Étape 4 : configurer les paramètres de stratégie de groupe pour les mises à jour automatiques

---

## Commentaires

**Cette page a-t-elle été utile ?** Yes No

# Planifier votre déploiement WSUS

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

La première étape du déploiement de WSUS (Windows Server Update Services) consiste à prendre des décisions importantes, par exemple le choix du scénario de déploiement de WSUS, le choix d'une topologie de réseau et la prise de connaissance de la configuration requise.

## 1.1. Passer en revue les considérations initiales et la configuration requise

### Configuration requise

La configuration requise pour les logiciels de base de données et le matériel dépend du nombre d'ordinateurs client mis à jour dans votre organisation. Avant d'activer le rôle serveur WSUS, vérifiez que le serveur répond à la configuration requise et que vous disposez des autorisations nécessaires pour effectuer l'installation en vous conformant aux recommandations suivantes :

- La configuration matérielle requise du serveur pour activer le rôle WSUS dépend de la configuration matérielle requise. Les configurations matérielles minimales requises pour WSUS sont les suivantes :
  - **Processeur** : processeur x64 de 1,4 gigahertz (GHz) (2 Ghz ou plus rapide recommandé)
  - **Mémoire** : WSUS nécessite 2 Go de RAM supplémentaires en sus de la mémoire requise par le serveur et tous les autres services ou logiciels.
  - **Espace disque disponible** : 40 Go ou plus sont recommandés.
    - La gestion des mises à jour locales avec la plateforme de mise à jour unifiée (UUP) nécessite 10 Go d'espace supplémentaire par version Windows et architecture de processeur pour chaque version. Pour en savoir plus, consultez la section Considérations relatives à l'UUP.
  - **Carte réseau** : 100 mégabits par seconde (Mbps) ou plus (1 Go est recommandé)

> ⓘ **Remarque**

> Ces instructions partent du principe que les clients WSUS se synchronisent avec le serveur toutes les huit heures pour un total de 30 000 clients. Si la synchronisation est plus fréquente, la charge du serveur augmentera en conséquence.

- Mises à jour logicielles requises :
  - **Windows Server 2016, 2019 et 2022** : mise à jour cumulative 2023-02 ou mise à jour cumulative ultérieure
  - **Windows Server 2012 et 2012 R2** : mise à jour cumulative 2023-03 ou mise à jour cumulative ultérieure
  - Si vous ne parvenez pas à installer ces mises à jour, vous pouvez ajouter manuellement les types MIME requis pour UUP au serveur WSUS.
- Configuration logicielle requise :
  - Pour consulter des rapports, WSUS nécessite Microsoft Report Viewer Redistributable 2008. Sur Windows Server 2016, WSUS exige Microsoft Report Viewer Runtime 2012
- Si vous installez des rôles ou des mises à jour logicielles qui vous demandent de redémarrer le serveur une fois l'installation terminée, redémarrez le serveur avant d'activer le rôle serveur WSUS.
- Microsoft .NET Framework 4.0 doit être installé sur le serveur sur lequel le rôle serveur WSUS sera installé.
- Vérifiez que le compte que vous envisagez d'utiliser pour installer WSUS est un membre du groupe Administrateurs local.
- Le compte Autorité NT\Service réseau doit disposer des autorisations de contrôle total pour les dossiers suivants afin que le composant logiciel enfichable Administration WSUS s'affiche correctement :
  - %windir%\Temp
  - %windir%\Microsoft.NET\Framework\v4.0.30319\Fichiers de ASP.NET temporaires

    > **Remarque**
    >
    > Il est possible que ce chemin d'accès n'existe pas avant l'installation du rôle Serveur Web qui contient Internet Information Services (IIS).

## Considérations relatives à l'installation

Au cours du processus d'installation, WSUS installera les éléments suivants par défaut :

- API .NET et applets de commande Windows PowerShell
- Base de données interne Windows, qui est utilisée par WSUS
- Services utilisés par WSUS, à savoir :
  - Service de mise à jour
  - Service Web de création de rapports
  - Service Web client
  - Service Web d'authentification Web simple
  - Service de synchronisation de serveur
  - Service Web d'authentification DSS

## Considérations à propos des UUP

À compter du 28 mars 2023, les appareils Windows 11, version 22H2 locaux recevront des mises à jour qualité au moyen de la plateforme de mise à jour unifiée (UUP). UUP local interagit avec WSUS et Microsoft Configuration Manager. La mise à jour des fonctionnalités de Windows 11, version 22H2 sera mise à jour tous les mois afin que vous puissiez facilement déployer la dernière version sur vos clients. Les mises à jour qualité UUP continuent d'être cumulatives et incluent toutes les corrections de qualité et de sécurité Windows publiées. Bien que les mises à jour UUP ne puissent pas être supprimées au moyen de WSUS, les clients qui effectuent la mise à jour à l'aide de l'UUP local bénéficient des fonctionnalités suivantes :

- Possibilité pour les utilisateurs finaux d'acquérir des fonctionnalités à la demande et des packs linguistiques dans les environnements WSUS ou Configuration Manager.
- Réparation automatique des corruptions
- Réduction de la taille des téléchargements client des mises à jour qualité

Afin de préparer les mises à jour UUP locales, assurez-vous que les conditions suivantes sont remplies :

- Lors du stockage local de contenu pour WSUS, le serveur WSUS télécharge environ 10 Go de contenu par version Windows et architecture de processeur pour chaque version. Par exemple, 20 Go de contenu supplémentaires sont téléchargés pour x64 et arm64 pour Windows 11, version 22H2.

- Installez l'une des mises à jour suivantes sur les serveurs WSUS ou ajoutez manuellement les types MIME requis pour UUP au serveur WSUS :
  - **Windows Server 2016, 2019 et 2022** : mise à jour cumulative 2023-02 ou mise à jour cumulative ultérieure

- **Windows Server 2012 et 2012 R2** : mise à jour cumulative 2023-03 ou mise à jour cumulative ultérieure

> **Conseil**
>
> Si vous rencontrez une erreur `Cannot add duplicate collection entry of type 'mimeMap'`, consultez Conseils de dépannage WSUS.

## Ajouter manuellement les types MIME requis pour UUP

Deux types de fichiers sont requis pour la gestion des mises à jour locales avec UUP. Les types MIME `.msu` et `.wim` doivent être ajoutés aux serveurs WSUS pour prendre en charge UUP en local. Si vous ne parvenez pas à mettre à jour les serveurs WSUS, vous pouvez suivre ces étapes pour ajouter manuellement les types de fichiers requis :

1. Ouvrez **Gestionnaire des services Internet (IIS)** .
2. Sélectionnez le nom du serveur WSUS dans le volet **Connexions**. Si le nom du serveur WSUS ne s'affiche pas, sélectionnez **Connecter à un serveur** dans le menu **Fichier**, puis saisissez le nom du serveur.
3. Dans la **vue Fonctionnalités**, cliquez sur **Types MIME**, puis sur **Ouvrir la fonctionnalité** dans le volet **Actions**.

   > **Important**
   >
   > Assurez-vous d'avoir sélectionné le serveur et non le site lors de l'ajout des types MIME. Le site d'administration WSUS nécessite que l'entrée de type MIME soit héritée plutôt que locale.
4. Cliquez sur **Ajouter** dans le volet **Actions** pour les **types MIME**.
5. Saisissez les informations suivantes dans la fenêtre **Ajouter un type MIME** :

   - Extension de nom de fichier : `.wim`
   - Type MIME : `application/x-ms-wim`
6. Cliquez sur **OK** lorsque vous avez terminé d'ajouter le type MIME.
7. Ajoutez un autre type MIME en recliquant sur **Ajouter**, puis saisissez les informations suivantes :

   - Extension de nom de fichier : `.msu`

- Type MIME : `application/octet-stream`

8. Cliquez sur **OK** lorsque vous avez terminé d'ajouter le type MIME.

## Considérations sur les fonctionnalités à la demande

Configurer des ordinateurs client (y compris les serveurs) pour mettre à jour à l'aide de WSUS entraîne les limitations suivantes :

1. Les rôles de serveur dont les charges utiles ont été supprimées à l'aide des fonctionnalités à la demande ne peuvent pas être installés à la demande à partir de Microsoft Update. Vous devez fournir une source d'installation au moment où vous essayez d'installer ces rôles de serveur, ou configurer une source pour les fonctionnalités à la demande dans la stratégie de groupe.

2. Les éditions client Windows ne pourront pas installer XXX.NET 3.5 à la demande à partir du web. Les mêmes considérations que pour les rôles de serveur s'appliquent à .NET 3.5.

   > ⓘ **Remarque**
   >
   > La configuration d'une source d'installation de fonctionnalités à la demande n'implique pas WSUS. Pour en savoir plus sur comment configurer les fonctionnalités, voir Configurer des fonctionnalités à la demande dans Windows Server.

3. Les appareils d'entreprise exécutant Windows 10, version 1709 ou version 1803 ne peuvent pas installer de fonctionnalités à la demande directement à partir de WSUS. Pour installer Fonctionnalités à la demande, créez un fichier de fonctionnalité (magasin côte à côte) ou obtenez le package Fonctionnalités à la demande auprès de l'une des sources suivantes :

   - Centre de services de licence en volume (VLSC) - Accès VL requis
   - Portail OEM - Accès OEM requis
   - Téléchargement MSDN - Abonnement MSDN requis

     Les packages de fonctionnalités à la demande obtenus individuellement peuvent être installés à l'aide des options de ligne de commande DISM.

## Base de données WSUS requise

WSUS requiert l'une des bases de données suivantes :

- Base de données interne Windows
- Toute version de Microsoft SQL Server prise en charge. Pour en savoir plus, consultez la politique de support Microsoft.

WSUS prend en charge les éditions suivantes de SQL Server :

- Norme
- Entreprise
- Express

> ⓘ **Remarque**
>
> SQL Server Express 2008 R2 a une limite de taille de base de données de 10 Go. Cette taille de base de données semble suffisante pour WSUS, même si l'utilisation de cette base de données ne présente pas d'avantage notable par rapport à WID. La base de données WID dispose d'une mémoire RAM requise de 2 Go, en plus de la configuration système requise standard de Windows Server.

Vous pouvez installer le rôle WSUS sur un ordinateur distinct du serveur de base de données. Dans ce cas, les critères supplémentaires suivants s'appliquent :

1. Le serveur de base de données ne peut pas être configuré en tant que contrôleur de domaine.
2. Le serveur WSUS ne peut pas exécuter les services Bureau à distance.
3. Le serveur de base de données doit se trouver dans le même domaine Active Directory que le serveur WSUS ou il doit avoir une relation d'approbation avec le domaine Active Directory du serveur WSUS.
4. Le serveur WSUS et le serveur de base de données doivent se trouver dans le même fuseau horaire, ou ils doivent être synchronisés sur la même source de temps universel coordonné (Heure de Greenwich).

> ⓘ **Important**
>
> Lorsque WSUS utilise une base de données SQL Server distante, activez SQL Server Extended Protection for Authentication (EPA) pour aider à protéger la connexion à la base de données. Pour plus d'informations, voir **Sécuriser la connexion SQL Server**.

# 1.2. Choisir le scénario de déploiement de WSUS

Cette section décrit les fonctionnalités de base de tous les déploiements de WSUS. Utilisez cette section pour vous familiariser avec un déploiement simple impliquant un seul serveur WSUS ainsi qu'avec des scénarios plus complexes, tels qu'une hiérarchie de serveurs WSUS ou un serveur WSUS sur un segment de réseau isolé.

## Déploiement de WSUS simple

Le déploiement de WSUS le plus simple est constitué d'un serveur à l'intérieur du pare-feu d'entreprise qui sert les ordinateurs client sur un intranet privé. Le serveur WSUS se connecte à Microsoft Update pour télécharger les mises à jour. Cette opération est connue sous le nom de *synchronisation*. Au cours de la synchronisation, WSUS détermine si de nouvelles mises à jour ont été mises à disposition depuis la dernière synchronisation. S'il s'agit de votre première synchronisation de WSUS, toutes les mises à jour sont disponibles en téléchargement.

> ⓘ **Remarque**
>
> La synchronisation initiale peut durer plus d'une heure. Toutes les synchronisations suivantes devraient être considérablement plus rapides.

Par défaut, le serveur WSUS utilise le port 80 pour le protocole HTTP et le port 443 pour le protocole HTTPS pour obtenir les mises à jour de Microsoft. Si un pare-feu d'entreprise est installé entre votre réseau et Internet, vous devrez ouvrir ces ports sur le serveur qui communique directement avec Microsoft Update. Si vous prévoyez d'utiliser des ports personnalisés pour cette communication, vous devez ouvrir ces ports à la place. Vous pouvez configurer plusieurs serveurs WSUS à synchroniser avec un serveur WSUS parent. Par défaut, le serveur WSUS utilise le port 8530 pour le protocole HTTP et le port 8531 pour le protocole HTTPS pour fournir les mises à jour aux postes de travail clients.

## Plusieurs serveurs WSUS

Les administrateurs peuvent déployer plusieurs serveurs exécutant WSUS qui synchronisent tout le contenu à l'intérieur de l'intranet de leur organisation. Vous pouvez exposer un seul serveur sur Internet ; il sera le seul à télécharger les mises à jour de Microsoft Update. Ce serveur est configuré comme le serveur en amont, c'est-à-dire la source sur laquelle les serveurs en aval se synchronisent. Le cas échéant, les serveurs peuvent être situés sur un réseau multisite afin d'offrir la meilleure connectivité à tous les ordinateurs client.

## Serveur WSUS déconnecté

Si la stratégie d'entreprise ou d'autres circonstances limitent l'accès des ordinateurs à Internet, les administrateurs peuvent configurer un serveur interne pour exécuter WSUS. Il peut s'agir, par exemple, d'un serveur connecté à l'intranet, mais isolé d'Internet. Après avoir téléchargé, testé et approuvé les mises à jour sur ce serveur, un administrateur exporte les métadonnées et le contenu de mise à jour vers un DVD. Les métadonnées et le contenu de mise à jour sont importés du DVD vers les serveurs exécutant WSUS à l'intérieur de l'intranet.

## Hiérarchies de serveurs WSUS

Vous pouvez créer des hiérarchies complexes de serveurs WSUS. Dans la mesure où vous pouvez synchroniser un serveur WSUS avec un autre serveur WSUS plutôt qu'avec Microsoft Update, vous n'avez besoin que d'un seul serveur WSUS connecté à Microsoft Update. Lorsque vous liez des serveurs WSUS entre eux, il existe un serveur WSUS en amont et un serveur WSUS en aval. Le déploiement d'une hiérarchie de serveurs WSUS présente les avantages suivants :

- Vous pouvez télécharger les mises à jour une fois à partir d'Internet, puis les distribuer aux ordinateurs client en utilisant les serveurs en aval. Cette méthode permet d'économiser la bande passante sur la connexion Internet d'entreprise.
- Vous pouvez télécharger les mises à jour sur un serveur WSUS qui est physiquement plus proche des ordinateurs client, par exemple dans les filiales.
- Vous pouvez configurer des serveurs WSUS séparés pour servir des ordinateurs client qui utilisent différentes langues de produits Microsoft.
- Vous pouvez adapter WSUS à une grande organisation qui dispose de plus d'ordinateurs client qu'un serveur WSUS ne peut efficacement gérer.

> ⓘ **Remarque**
>
> Nous vous conseillons de ne pas créer une hiérarchie de serveurs WSUS avec une profondeur de plus de trois niveaux. Chaque niveau ajoute du temps pour propager les mises à jour sur tous les serveurs connectés. Même s'il n'existe aucune limite théorique à une hiérarchie, seuls les déploiements avec une hiérarchie d'une profondeur de cinq niveaux ont été testés par Microsoft.

De plus, les serveurs en aval doivent avoir la même version ou une version antérieure de WSUS comme source de synchronisation du serveur en amont.

Vous pouvez connecter des serveurs WSUS en mode autonome (pour obtenir une gestion distribuée) ou en mode Réplica (pour obtenir une gestion centralisée). Vous n'avez pas besoin de déployer une hiérarchie de serveurs qui utilise un seul mode : vous pouvez déployer une solution WSUS qui utilise à la fois des serveurs WSUS autonomes et des serveurs WSUS réplicas.

### Mode autonome

Le mode autonome, également appelé gestion distribuée, est l'option d'installation par défaut pour WSUS. En mode autonome, un serveur WSUS en amont partage des mises à jour avec des serveurs en aval pendant la synchronisation. Les serveurs WSUS en aval sont administrés séparément et ne reçoivent pas le statut d'approbation des mises à jour ni les informations sur les groupes d'ordinateurs du serveur en amont. En utilisant le modèle de gestion distribuée, chaque administrateur de serveur WSUS sélectionne des langues de mise à jour, crée des groupes d'ordinateurs, affecte des ordinateurs à des groupes, teste et approuve les mises à jour, et vérifie que les mises à jour appropriées sont installées dans les groupes d'ordinateurs adéquats.

### Mode Réplica :

Le mode Réplica, également appelé gestion centralisée, fonctionne en ayant un serveur WSUS en amont qui partage des mises à jour, un statut d'approbation et des groupes d'ordinateurs avec des serveurs en aval. Les serveurs réplicas héritent des approbations de mise à jour et ne sont pas administrés séparément du serveur WSUS en amont.

> ⓘ **Remarque**
>
> Si vous configurez plusieurs serveurs réplica pour une connexion à un serveur WSUS en amont unique, ne planifiez pas l'exécution de la synchronisation en même temps sur chaque serveur réplica. Vous éviterez ainsi de soudaines surtensions dans l'utilisation de la bande passante.

## Succursales

Vous pouvez exploiter la fonctionnalité de filiale de Windows pour optimiser le déploiement de WSUS. Ce type de déploiement présente les avantages suivants :

1. Cela permet de réduire l'utilisation de la liaison WAN et d'améliorer la réactivité des applications. Pour activer l'accélération fournie par BranchCache pour l'accès au contenu délivré le serveur WSUS, vous devez installer la fonctionnalité BranchCache sur le serveur et les clients, puis vérifier que le service BranchCache a démarré. Aucune autre étape n'est requise.

2. Dans les filiales avec des connexions à bande passante faible au bureau central, mais avec des connexions à bande passante élevée à Internet, la fonctionnalité de filiale peut également être utilisée. Dans ce cas, vous pouvez configurer des serveurs WSUS en aval pour qu'ils obtiennent des informations sur les mises à jour à installer du serveur WSUS central, mais qu'ils téléchargent les mises à jour à partir de Microsoft Update.

## Équilibrage de charge réseau

L'équilibrage de la charge réseau augmente la fiabilité et les performances de votre réseau WSUS. Vous pouvez configurer plusieurs serveurs WSUS qui partagent un seul cluster de basculement exécutant SQL Server. Dans cette configuration, vous devez utiliser une installation de SQL Server complète, et non l'installation de la base de données interne Windows qui est fournie par WSUS, et le rôle de base de données doit être installé sur tous les serveurs frontaux WSUS. Vous pouvez également faire en sorte que tous les serveurs WSUS utilisent un système de fichiers distribués (DFS) pour stocker leur contenu.

**Configuration WSUS pour NLB** : par rapport à la configuration WSUS 3.2 pour NLB, un appel de configuration spécial et des paramètres ne sont plus nécessaires pour configurer WSUS pour NLB. Vous devez uniquement installer chaque serveur WSUS en tenant compte des considérations suivantes.

- WSUS doit être configuré à l'aide de l'option de base de données SQL au lieu de WID.
- Si vous stockez les mises à jour localement, le même dossier de contenu doit être partagé entre les serveurs WSUS utilisant la même base de données SQL.
- Le programme d'installation WSUS doit être effectué en série. Les tâches post-installation ne peuvent pas être exécutées simultanément sur plusieurs serveurs partageant la même base de données SQL.
- Chaque serveur WSUS front-end doit exécuter la même version du système d'exploitation, y compris le même niveau de mise à jour cumulative.

## Déploiement de WSUS avec des ordinateurs client itinérants

Si le réseau comprend des utilisateurs mobiles qui se connectent au réseau à partir de différents emplacements, vous pouvez configurer WSUS pour permettre aux utilisateurs itinérants de mettre à jour leurs ordinateurs client à partir du serveur WSUS qui leur est le plus proche géographiquement. Par exemple, vous pouvez déployer un serveur WSUS dans chaque région et utiliser un sous-réseau DNS différent pour chacune. Tous les ordinateurs client peuvent être dirigés vers le même serveur WSUS, qui résout chaque sous-réseau en serveur WSUS physique le plus proche.

# 1.3. Choisir la stratégie de stockage WSUS

WSUS (Windows Server Update Services) utilise deux types de systèmes de stockage : une base de données pour stocker les métadonnées de configuration WSUS et de mise à jour, et un système de fichiers local facultatif pour stocker les fichiers de mise à jour. Avant d'installer WSUS, vous devez décider du mode d'implémentation du stockage.

Les mises à jour sont constituées de deux parties : les métadonnées qui décrivent la mise à jour et les fichiers requis pour installer la mise à jour. Les métadonnées de mise à jour sont généralement beaucoup plus petites que la mise à jour réelle et stockées dans la base de données WSUS. Les fichiers de mise à jour sont stockés sur un serveur WSUS local ou sur un serveur Web Microsoft Update.

## Base de données WSUS

WSUS requiert une base de données pour chaque serveur WSUS. WSUS prend en charge l'utilisation d'une base de données qui se trouve sur un ordinateur différent du serveur WSUS, avec quelques restrictions. Pour obtenir la liste des bases de données prises en charge et des limitations de bases de données distantes, consultez la section 1.1 Passer en revue les considérations initiales et la configuration requise dans ce guide.

La base de données WSUS stocke les informations suivantes :

- Informations de configuration du serveur WSUS
- Métadonnées qui décrivent chaque mise à jour
- Informations sur les ordinateurs client, les mises à jour et les interactions

Si vous installez plusieurs serveurs WSUS, vous devez conserver une base de données distincte pour chaque serveur WSUS, qu'il s'agisse d'un serveur autonome ou réplica. Vous ne pouvez pas stocker plusieurs bases de données WSUS sur une seule instance de SQL Server, sauf dans les clusters NLB (Network Load Balancing) qui utilisent le basculement SQL Server.

SQL Server, SQL Server Express et la base de données interne Windows fournissent les mêmes caractéristiques de performances pour une configuration sur un serveur unique, où la base de données et le service WSUS sont situés sur le même ordinateur. Une configuration sur un serveur unique peut prendre en charge plusieurs milliers d'ordinateurs client WSUS.

> ⓘ **Remarque**
>
> Ne tentez pas de gérer WSUS en accédant directement à la base de données. La manipulation directe de la base de données peut entraîner une altération de la base de données. Il est possible que l'endommagement ne soit pas immédiatement évident, mais il peut empêcher des mises à niveau vers la version suivante du produit. Vous pouvez gérer WSUS en utilisant la console WSUS ou les interfaces de programmation d'applications (API) WSUS.

## WSUS avec la base de données interne Windows

Par défaut, l'Assistant Installation crée et utilise une base de données interne Windows nommée SUSDB.mdf. Cette base de données est située dans le dossier %windir%\wid\data\, où %windir% est le lecteur local sur lequel le logiciel du serveur WSUS est installé.

> ⓘ **Remarque**
>
> La base de données interne Windows (WID) a été introduite dans Windows Server 2008.

WSUS prend en charge l'authentification Windows uniquement pour la base de données. Vous ne pouvez pas utiliser l'authentification SQL Server avec WSUS. Si vous utilisez la base de données interne Windows pour la base de données WSUS, le programme d'installation de WSUS crée une instance de SQL Server nommée server\Microsoft##WID, où server est le nom de l'ordinateur. Avec l'une ou l'autre des options de la base de données, le programme d'installation de WSUS crée une base de données nommée SUSDB. Le nom de cette base de données n'est pas configurable.

Nous vous conseillons d'utiliser la base de données interne Windows dans les cas suivants :

- L'organisation n'a pas encore acheté et n'a pas besoin d'un produit SQL Server pour une autre application.
- L'organisation n'a pas besoin d'une solution NLB WSUS.

- Vous avez l'intention de déployer plusieurs serveurs WSUS (par exemple, dans les filiales). Dans ce cas, vous devez envisager d'utiliser la base de données interne Windows sur les serveurs secondaires, même si vous utilisez SQL Server pour le serveur WSUS racine. Comme chaque serveur WSUS nécessite une instance distincte de SQL Server, vous rencontrerez rapidement des problèmes de performance de la base de données si une seule instance de SQL Server gère plusieurs serveurs WSUS.

La base de données interne Windows ne fournit pas d'interface utilisateur ni d'outils de gestion de base de données. Si vous sélectionnez cette base de données pour WSUS, vous devez utiliser des outils externes pour gérer la base de données. Pour en savoir plus, consultez :

- Sauvegarde et restauration des données WSUS et sauvegarde de votre serveur
- Réindexer la base de données WSUS

### WSUS avec SQL Server

Nous vous conseillons d'utiliser SQL Server avec WSUS dans les cas suivants :

1. Vous avez besoin d'une solution WSUS d'équilibrage de la charge réseau.
2. Au moins une instance de SQL Server est déjà installée.
3. Vous ne pouvez pas exécuter le service SQL Server sous un compte local non système ou à l'aide de l'authentification SQL Server. WSUS prend en charge l'authentification Windows uniquement.

## Stockage des mises à jour WSUS

Lorsque les mises à jour sont synchronisées sur votre serveur WSUS, les fichiers de mise à jour et les métadonnées sont stockés à deux endroits différents. Les métadonnées sont stockées dans la base de données WSUS. Les fichiers de mise à jour peuvent être stockés sur votre serveur WSUS ou sur les serveurs Microsoft Update, selon la configuration de vos options de synchronisation. Si vous choisissez de stocker les fichiers de mise à jour sur votre serveur WSUS, les ordinateurs client téléchargent les mises à jour approuvées à partir du serveur WSUS local. Sinon, les ordinateurs client téléchargent les mises à jour approuvées directement à partir de Microsoft Update. L'option la plus appropriée pour votre organisation dépend de la bande passante du réseau pour Internet, de la bande passante du réseau sur l'intranet et de la disponibilité de stockage en local.

Vous pouvez sélectionner une autre solution de stockage des mises à jour pour chaque serveur WSUS que vous déployez.

### Stockage de serveur WSUS en local

Le stockage en local des fichiers de mise à jour est l'option par défaut lorsque vous installez et configurez WSUS. Cette option permet d'économiser la bande passante sur la connexion d'entreprise à Internet, car les ordinateurs client téléchargent les mises à jour directement à partir du serveur WSUS local.

Cette option nécessite que le serveur dispose d'un espace disque suffisant pour stocker toutes les mises à jour nécessaires. Au minimum, WSUS nécessite 20 Go pour stocker les mises à jour localement ; toutefois, nous vous recommandons d'au moins 40 Go. Pour plus d'informations sur la projection de la quantité d'espace disque nécessaire, consultez la configuration système requise et les considérations relatives à l'UUP.

> **Important**
>
> Choisissez un dossier sécurisé auquel seuls les administrateurs peuvent accéder pour le stockage local des mises à jour.

### Stockage étendu sur les serveurs Microsoft Update

Vous pouvez stocker les mises à jour à distance sur les serveurs Microsoft Update. Cette option est utile si la plupart des ordinateurs client se connectent au serveur WSUS via une connexion de réseau étendu lente, mais qu'ils se connectent à Internet via une connexion à bande passante élevée.

Dans ce cas, le serveur WSUS racine se synchronise avec Microsoft Update et reçoit les métadonnées de mise à jour. Après que vous avez approuvé les mises à jour, les ordinateurs client téléchargent les mises à jour approuvées à partir des serveurs Microsoft Update.

## 1.4. Choisir les langues de mise à jour WSUS

Lorsque vous déployez une hiérarchie de serveurs WSUS, vous devez identifier les mises à jour des langues requises dans toute l'organisation. Vous devez configurer le serveur WSUS racine pour télécharger les mises à jour dans toutes les langues utilisées dans toute l'organisation.

Par exemple, le siège social peut nécessiter les mises à jour des langues anglaise et française, mais une filiale a besoin des mises à jour des langues anglaise, française et allemande, et une autre a besoin des mises à jour des langues anglaise et espagnole. Dans ce cas, vous configurez le serveur WSUS racine pour télécharger les mises à jour en anglais, français, allemand et

espagnol. Vous configurez ensuite le serveur WSUS de la première filiale pour télécharger les mises à jour en anglais, français et allemand uniquement, puis celui de la deuxième filiale pour télécharger les mises à jour en anglais et espagnol uniquement.

La page **Choisir les langues** de l'Assistant Configuration de WSUS vous permet d'obtenir des mises à jour dans toutes les langues ou un sous-ensemble de langues. La sélection d'un sous-ensemble de langues permet d'économiser de l'espace disque, mais il est IMPORTANT de choisir toutes les langues requises par tous les serveurs en aval et les ordinateurs client d'un serveur WSUS.

Voici quelques remarques IMPORTANTES concernant la langue de mise à jour que vous devez garder à l'esprit avant de configurer cette option :

- Incluez toujours l'anglais en plus de toutes les autres langues requises dans toute l'organisation. Toutes les mises à jour sont basées sur des modules linguistiques en anglais.
- Les serveurs en aval et les ordinateurs client ne recevront pas toutes les mises à jour dont ils ont besoin si vous n'avez pas sélectionné toutes les langues nécessaires pour le serveur en amont. Veillez à sélectionner toutes les langues nécessaires à tous les ordinateurs client associés à tous les serveurs en aval.
- Vous devez généralement télécharger les mises à jour dans toutes les langues sur le serveur WSUS racine qui est synchronisé avec Microsoft Update. Cette sélection garantit que tous les serveurs en aval et ordinateurs client recevront les mises à jour dans les langues requises.

Si vous stockez les mises à jour localement et que vous avez configuré un serveur WSUS pour télécharger les mises à jour dans un nombre limité de langues, vous remarquerez peut-être que certaines mises à jour sont disponibles dans des langues autres que celles que vous avez spécifiées. De nombreux fichiers de mise à jour sont des lots de plusieurs langues différentes, qui comprennent au moins l'une des langues spécifiées sur le serveur.

**Serveurs en amont**

> ⓘ **Remarque**
>
> Configurez les serveurs en amont pour synchroniser les mises à jour dans toutes les langues requises par les serveurs de réplication en aval. Vous ne serez pas informé des mises à jour nécessaires pour les langues non synchronisées.

Les mises à jour apparaîtront en tant que **Non applicable** sur les ordinateurs client qui requièrent la langue. Pour éviter ce problème, assurez-vous que toutes les langues du système d'exploitation sont incluses dans les options de synchronisation du serveur WSUS. Vous pouvez voir toutes les langues du système d'exploitation en accédant à l'affichage **Ordinateurs** de la console d'administration WSUS et trier les ordinateurs en fonction de la langue du système d'exploitation. Toutefois, vous pouvez inclure d'autres langues si vous disposez d'applications Microsoft dans plusieurs langues (par exemple, si la version française de Microsoft Word est installée sur certains ordinateurs qui utilisent la version anglaise de Windows).

Le choix des langues pour un serveur en amont n'est pas le même que celui pour un serveur en aval. Les procédures ci-dessous expliquent comment identifier les différences.

## Pour choisir les langues de mise à jour d'un serveur de synchronisation à partir de Microsoft Update

1. Dans l'Assistant Configuration WSUS :

    - Pour obtenir les mises à jour dans toutes les langues, cliquez sur **Télécharger les mises à jour dans toutes les langues, y compris les nouvelles langues**.
    - Pour obtenir les mises à jour uniquement dans certaines langues, cliquez sur **Télécharger les mises à jour uniquement dans ces langues**, puis sélectionnez les langues pour lesquelles vous souhaitez obtenir des mises à jour.

## Pour choisir les langues de mise à jour d'un serveur en aval

1. Si le serveur en amont a été configuré pour télécharger les fichiers de mise à jour dans un sous-ensemble de langues : dans l'Assistant Configuration WSUS, cliquez sur **Télécharger les mises à jour dans ces langues uniquement (Seules les langues marquées d'un astérisque sont prises en charge par le serveur en amont.)**, puis sélectionnez les langues pour lesquelles vous souhaitez obtenir des mises à jour.

    > ⓘ **Remarque**
    >
    > Vous devez effectuer cette opération même si vous voulez que le serveur en aval puisse télécharger les mêmes langues que le serveur en amont.

2. Si le serveur en amont a été configuré pour télécharger les fichiers de mise à jour dans toutes les langues : dans l'Assistant Configuration WSUS, cliquez sur **Télécharger les mises à jour dans toutes les langues prises en charge par le serveur en amont**.

> ⓘ **Remarque**
>
> Vous devez effectuer cette opération même si vous voulez que le serveur en aval puisse télécharger les mêmes langues que le serveur en amont. Ce paramètre permet au serveur en amont de télécharger les mises à jour dans toutes les langues, y compris celles qui n'étaient pas initialement configurées pour le serveur en amont. Si vous ajoutez des langues sur le serveur en amont, vous devez copier les nouvelles mises à jour sur ses serveurs de réplication.
>
> La modification des options de langue uniquement sur le serveur en amont peut entraîner une incohérence entre le nombre de mises à jour approuvées sur le serveur central et le nombre de mises à jour approuvées sur les serveurs de réplication.

## 1.5. Planifier les groupes d'ordinateurs WSUS

WSUS vous permet de cibler les mises à jour vers des groupes d'ordinateurs client afin que vous puissiez vous assurer que des ordinateurs spécifiques obtiennent toujours les mises à jour adéquates au moment le plus approprié. Par exemple, si tous les ordinateurs d'un service (tel que l'équipe Comptabilité) ont une configuration spécifique, vous pouvez configurer un groupe pour cette équipe, décider des mises à jour dont leurs ordinateurs ont besoin et l'heure à laquelle elles doivent être installées, puis utiliser les rapports WSUS pour évaluer les mises à jour pour l'équipe.

> ⓘ **Remarque**
>
> Si un serveur WSUS est exécuté en mode réplica, vous ne pouvez pas créer de groupes d'ordinateurs sur ce serveur. Tous les groupes d'ordinateurs nécessaires pour les ordinateurs client du serveur de réplication doivent être créés sur le serveur WSUS qui est la racine de la hiérarchie de serveurs WSUS. Pour en savoir plus sur le mode réplica, consultez **Exécuter le mode réplica WSUS**.

Les ordinateurs sont toujours affectés au groupe **Tous les ordinateurs** et ils restent affectés au groupe **Ordinateurs non attribués** tant que vous ne les affectez pas à un autre groupe. Les ordinateurs peuvent appartenir à plusieurs groupes.

Les groupes d'ordinateurs peuvent être configurés en hiérarchies (par exemple, le groupe Traitement des paies et le groupe Compte fournisseurs sous le groupe Comptabilité). Les mises à jour qui sont approuvées pour un groupe supérieur sont automatiquement déployées vers les

groupes inférieurs, en plus du groupe supérieur. Dans cet exemple, si vous approuvez Update1 pour le groupe Comptabilité, la mise à jour sera déployée vers tous les ordinateurs du groupe Comptabilité, tous les ordinateurs du groupe Traitement des paies et tous les ordinateurs du groupe Compte fournisseurs.

Comme les ordinateurs peuvent être affectés à plusieurs groupes, il est possible qu'une mise à jour soit approuvée plusieurs fois pour le même ordinateur. Toutefois, la mise à jour ne sera déployée qu'une seule fois et tous les conflits seront résolus par le serveur WSUS. Pour poursuivre avec l'exemple précédent, si ComputerA est affecté au groupe Traitement des paies et au groupe Compte fournisseurs, et si Update1 est approuvée pour les deux groupes, elle ne sera déployée qu'une seule fois.

Vous pouvez affecter les ordinateurs à des groupes d'ordinateurs en adoptant l'une des deux méthodes, à savoir le ciblage côté serveur ou le ciblage côté client. Voici les définitions de chaque méthode :

- **Ciblage côté serveur** : vous affectez manuellement un ou plusieurs ordinateurs client à plusieurs groupes simultanément.
- **Ciblage côté client** : vous utilisez la stratégie de groupe ou modifiez les paramètres de registre sur les ordinateurs client pour permettre à ces ordinateurs de s'ajouter automatiquement aux groupes d'ordinateurs précédemment créés.

## Résolution des conflits

Le serveur applique les règles suivantes pour résoudre les conflits et déterminer l'action résultante sur les clients :

1. Priorité
2. Installer/Désinstaller
3. Date limite

### Priorité

Les actions associées au groupe présentant la priorité la plus élevée remplacent les actions des autres groupes. Plus un groupe apparaît profondément dans la hiérarchie des groupes, plus sa priorité est élevée. La priorité est attribuée uniquement en fonction de la profondeur. Toutes les branches ont la même priorité. Par exemple, le niveau deux du groupe sous la branche Bureaux a une priorité supérieure à celle du niveau un du groupe sous la branche Serveurs.

Dans l'exemple de texte suivant du volet Hiérarchie de la console Services de mise à jour, pour un serveur WSUS nommé WSUS-01, les groupes d'ordinateurs nommés Ordinateurs de bureau et Serveurs ont été ajoutés au groupe par défaut **Tous les ordinateurs** . Les deux groupes Ordinateurs de bureau et Serveurs se trouvent au même niveau hiérarchique.

- **Services de mise à jour**
  - **WSUS-01**
    - **Mises à jour**
    - **Ordinateurs**
      - **Tous les ordinateurs**
        - **Ordinateurs non affectés**
        - **Ordinateurs de bureau**
          - **Ordinateurs de bureau-L1**
            - **Ordinateurs de bureau-L2**
        - **Serveurs**
          - **Serveurs-L1**
    - **Serveurs en aval**
    - **Synchronisations**
    - **Rapports**
    - **Options**

Dans cet exemple, le niveau deux du groupe sous la branche Ordinateurs de bureau (Bureaux-L2) a une priorité supérieure à celle du niveau un du groupe sous la branche Serveurs (Serveurs-L1). En conséquence, pour un ordinateur qui appartient aux deux groupes Bureaux-L2 et Serveurs-L1, toutes les actions pour le groupe Bureaux-L2 ont priorité sur les actions spécifiées pour le groupe Serveurs-L1.

## Priorité d'installation et de désinstallation

Les actions d'installation remplacent les actions de désinstallation. Les installations obligatoires remplacent les installations facultatives (ces dernières sont uniquement disponibles via l'API et la modification d'une approbation pour une mise à jour à l'aide la console d'administration WSUS supprime toutes les approbations facultatives).

## Priorité des échéances

Les actions qui ont une échéance remplacent celles qui n'en ont pas. Les actions dont les échéances sont plus proches remplacent celles qui sont plus lointaines.

# 1.6. Planifier les considérations sur les performances WSUS

Il existe quelques domaines que vous devez soigneusement planifier avant de déployer WSUS pour obtenir des performances optimisées. Les principaux domaines sont les suivants :

- Configuration du réseau
- Téléchargement différé
- Filtres
- Installation
- Déploiements de mises à jour importantes
- Service de transfert intelligent en arrière-plan (BITS)

## Configuration du réseau

Pour optimiser les performances sur les réseaux WSUS, tenez compte des suggestions suivantes :

1. Configurez les réseaux WSUS dans une topologie Hub and Spoke plutôt que dans une topologie hiérarchique.

2. Utilisez le tri de masques réseau DNS pour les ordinateurs client itinérants et configurez les ordinateurs client itinérants pour obtenir des mises à jour à partir du serveur WSUS local.

## Téléchargement différé

Vous pouvez approuver des mises à jour et télécharger les métadonnées de mise à jour avant de télécharger les fichiers de mise à jour : cette méthode est appelée *téléchargement différé*. Lorsque vous différer les téléchargements, une mise à jour n'est téléchargée qu'après avoir été approuvée. Nous vous conseillons de différer les téléchargements, car cela permet d'optimiser l'espace disque et la bande passante du réseau.

Dans une hiérarchie de serveurs WSUS, WSUS configure automatiquement tous les serveurs en aval pour qu'ils utilisent le paramètre de téléchargement différé du serveur WSUS racine. Vous pouvez modifier ce paramètre par défaut. Par exemple, vous pouvez configurer un serveur en amont pour effectuer des synchronisations immédiates et complètes, puis configurer un serveur en aval pour différer les téléchargements.

Si vous déployez une hiérarchie de serveurs WSUS connectés, il est recommandé de ne pas imbriquer profondément les serveurs. Si vous activez les téléchargements différés et qu'un serveur en aval demande une mise à jour qui n'est pas approuvée sur le serveur en amont, la

requête du serveur en aval force le téléchargement sur le serveur en amont. Le serveur en aval télécharge ensuite la mise à jour lors d'une synchronisation ultérieure. Dans une hiérarchie profonde de serveurs WSUS, des retards peuvent se produire lorsque les mises à jour dont demandées, téléchargées, puis transmises par la hiérarchie de serveurs. Par défaut, les téléchargements différés sont activés lorsque vous stockez des mises à jour en local. Vous pouvez modifier cette option manuellement.

## Filtres

WSUS vous permet de filtrer les synchronisations des mises à jour par langue, produit et classification. Dans une hiérarchie de serveurs WSUS, WSUS configure automatiquement tous les serveurs en aval pour qu'ils utilisent les options de filtrage des mises à jour qui sont sélectionnées sur le serveur WSUS racine. Vous pouvez reconfigurer les serveurs de téléchargement pour recevoir uniquement un sous-ensemble des langues.

Par défaut, les produits à mettre à jour sont Windows et Office, et les classifications par défaut sont Mises à jour critiques, Mises à jour de sécurité et Mises à jour de définitions. Pour économiser l'espace disque et la bande passante, nous vous conseillons de vous limiter aux langues que vous utilisez vraiment.

## Installation

Les mises à jour sont généralement constituées de nouvelles versions de fichiers qui existent déjà sur l'ordinateur qui est mis à jour. Sur un niveau binaire, il est possible que ces fichiers existants ne soient pas très différents des versions mises à jour. La fonctionnalité des fichiers d'installation rapide identifie les octets exacts entre les versions, crée et distribue des mises à jour de ces différences uniquement, puis fusionne le fichier existant avec les octets mis à jour.

Cette fonctionnalité est parfois appelée « remise delta », car elle télécharge uniquement le delta (la différence) entre deux versions d'un fichier. Les fichiers d'installation rapide sont plus volumineux que les mises à jour distribuées aux ordinateurs client, car ils contiennent toutes les versions possibles de chaque fichier à mettre à jour.

Vous pouvez utiliser les fichiers d'installation rapide pour limiter la bande passante consommée sur le réseau local, étant donné que WSUS transmet uniquement le delta applicable à une version particulière d'un composant mis à jour. Toutefois, cela se fait au prix de la bande passante supplémentaire entre votre serveur WSUS, les serveurs WSUS en amont et Microsoft Update, et nécessite de l'espace disque supplémentaire. Par défaut, WSUS n'utilise pas les fichiers d'installation express.

Les mises à jour ne sont pas toutes appropriées pour une distribution à l'aide de fichiers d'installation rapide. Si vous sélectionnez cette option, vous obtenez des fichiers d'installation rapide pour toutes les mises à jour. Si vous ne stockez pas les mises à jour localement, l'agent Windows Update décide s'il faut télécharger les fichiers d'installation express ou les distributions de mise à jour complète.

## Déploiements de mises à jour importantes

Lorsque vous déployez des mises à jour importantes (par exemple, des Service Packs), vous pouvez éviter de saturer le réseau en utilisant les pratiques suivantes :

1. Utilisez la limitation de bande passante du service de transfert intelligent en arrière-plan (BITS). Les limitations de bande passante du service BITS peuvent être contrôlées selon le créneau horaire, mais elles s'appliquent à toutes les applications qui utilisent le service BITS. Pour savoir comment contrôler la limitation BITS, consultez Stratégies de groupe.

2. Utilisez la limitation de bande passante des services Internet Information Services pour limiter la bande passante à un ou plusieurs services Web.

3. Utilisez des groupes d'ordinateurs pour contrôler le lancement. Un ordinateur client s'identifie en tant que membre d'un groupe d'ordinateurs particulier lorsqu'il envoie des informations au serveur WSUS. Le serveur WSUS utilise ces informations pour déterminer les mises à jour à déployer sur cet ordinateur. Vous pouvez configurer plusieurs groupes d'ordinateurs et approuver de manière séquentielle les téléchargements de Service Packs volumineux pour un sous-ensemble de ces groupes.

## Service de transfert intelligent en arrière-plan (BITS)

WSUS utilise le protocole du service de transfert intelligent en arrière-plan (BITS) pour toutes ses tâches de transfert de fichiers. Cela comprend les téléchargements vers les ordinateurs client et les synchronisations du serveur. Le service BITS permet aux programmes de télécharger des fichiers en utilisant la bande passante de rechange. Le service BITS gère les transferts de fichiers par le biais de déconnexions du réseau et de redémarrages de l'ordinateur. Pour en savoir plus, voir : Service de transfert intelligent en arrière-plan (BITS).

# 1.7. Planifier les paramètres des Mises à jour automatiques

Vous pouvez spécifier une date limite pour approuver les mises à jour sur le serveur WSUS. La date limite oblige les ordinateurs client à installer la mise à jour à une heure spécifique, mais il existe différentes situations, selon si la date limite a expiré, si la file d'attente comprend d'autres mises à jour que l'ordinateur doit installer et si la mise à jour (ou une autre mise à jour de la file d'attente) requiert un redémarrage.

Par défaut, les Mises à jour automatiques interrogent le serveur WSUS au sujet des mises à jour approuvées toutes les 22 heures moins un décalage aléatoire. Si de nouvelles mises à jour doivent être installées, elles sont téléchargées. Vous pouvez définir une valeur comprise entre 1 et 22 heures pour le délai entre chaque cycle de détection.

Vous pouvez manipuler les options de notification comme suit :

1. Si les Mises à jour automatiques sont configurées pour avertir l'utilisateur que des mises à jour sont prêtes à être installées, la notification est envoyée au journal système et à la zone de notification de l'ordinateur client.

2. Lorsqu'un utilisateur disposant des informations d'identification appropriées clique sur l'icône de la zone de notification, la fonction Mises à jour automatiques affiche les mises à jour disponibles à installer. L'utilisateur doit cliquer sur **Installer** pour démarrer l'installation. Un message s'affiche si l'installation de la mise à jour nécessite un redémarrage de l'ordinateur pour être complète. Si un redémarrage est requis, la fonction Mises à jour automatiques ne peut pas détecter les mises à jour supplémentaires tant que l'ordinateur n'a pas été redémarré.

Si les Mises à jour automatiques sont configurées pour installer les mises à jour selon une planification, les mises à jour applicables sont téléchargées et marquées comme prêtes à être installées. Les Mises à jour automatiques avertissent les utilisateurs qui disposent des informations d'identification appropriées en utilisant une icône de la zone de notification, et un événement est consigné dans le journal système.

Au jour et à l'heure planifiés, les Mises à jour automatiques installent la mise à jour et redémarrent l'ordinateur (si nécessaire), même si aucun administrateur local n'a ouvert de session. Si un administrateur local a ouvert une session et que l'ordinateur requiert un redémarrage, les Mises à jour automatiques affichent un avertissement et un compte à rebours pour le redémarrage. Sinon, l'installation se déroule en arrière-plan.

Si l'ordinateur doit être redémarré et qu'un utilisateur a ouvert une session, une boîte de dialogue de compte à rebours similaire s'affiche, qui avertit l'utilisateur au sujet du redémarrage imminent. Vous pouvez manipuler les redémarrages de l'ordinateur avec une stratégie de groupe.

Une fois les nouvelles mises à jour téléchargées, les Mises à jour automatiques interrogent le serveur WSUS au sujet de la liste des packages approuvés pour confirmer que les packages téléchargés sont toujours valides et approuvés. Cela signifie que, si un administrateur WSUS supprime des mises à jour de la liste des mises à jour approuvées alors que les Mises à jour automatiques téléchargent les mises à jour, seules celles qui sont toujours approuvées sont en réalité installées.

## Étape suivante

**Étape 1 : installer le rôle serveur WSUS**

---

Last updated on 28/07/2026

# Etape 1 : Installer le rôle serveur WSUS

16/08/2025

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

L'étape suivante du déploiement de votre serveur WSUS consiste à installer le rôle serveur WSUS.

Gestionnaire de serveur

La procédure suivante explique comment installer le rôle serveur WSUS à l'aide du Gestionnaire de serveur.

1. Ouvrez une session sur le serveur sur lequel vous envisagez d'installer le rôle serveur WSUS en utilisant un compte qui est membre du groupe Administrateurs local.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**.
3. Dans la page **Avant de commencer** , cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type d'installation**, confirmez que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, choisissez l'emplacement du serveur (à partir d'un pool de serveurs ou d'un disque dur virtuel). Après avoir sélectionné l'emplacement, choisissez le serveur sur lequel vous voulez installer le rôle de serveur WSUS, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Services WSUS (Windows Server Update Services)** . **La fenêtre « Ajouter les fonctionnalités requises pour Windows Server Update Services » s'ouvre.** Cliquez sur **Ajouter les fonctionnalités**, puis sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, laissez les sélections par défaut et cliquez sur **Suivant**.

   > ⓘ **Important**
   >
   > WSUS requiert uniquement la configuration du rôle Serveur Web par défaut. Si vous êtes invité à indiquer une autre configuration du rôle Serveur Web lors de

la configuration de WSUS, vous pouvez accepter en toute sécurité les valeurs par défaut et continuer la configuration de WSUS.

8. Dans la page **Services WSUS (Windows Server Update Services)** , cliquez sur **Suivant**.

9. Dans la page **Sélectionner des services de rôle** , laissez les sélections par défaut et cliquez sur **Suivant**.

   > **Conseil**
   >
   > Vous devez sélectionner un type de base de données. Si les options de base de données sont toutes décochées (non sélectionnées), les tâches postérieures à l'installation échouent.

10. Dans la page **Sélection de l'emplacement du contenu** , tapez un emplacement valide pour stocker les mises à jour. Par exemple, vous pouvez créer un dossier nommé WSUS_database à la racine du lecteur K spécifiquement à cette fin, et tapez **k:\WSUS_database** comme emplacement valide.

11. Cliquez sur **Suivant**. La page **Rôle de serveur web (IIS)** s'affiche. Vérifiez les informations, puis cliquez sur **Suivant**. Dans **Sélectionner les services de rôle à installer pour le serveur Web (IIS)** , conservez les valeurs par défaut, puis cliquez sur **Suivant**.

12. Dans la page **Confirmer les sélections d'installation** , passez en revue les options sélectionnées, puis cliquez sur **Installer**. L'Assistant d'installation de WSUS s'exécute. Le processus peut durer plusieurs minutes.

13. Une fois l'installation de WSUS terminée, dans la fenêtre de résumé de la page **Progression de l'installation** , cliquez sur **Lancer les tâches de post-installation**. Le message suivant s'affiche : **Veuillez patienter pendant la configuration de votre serveur**. Une fois la tâche terminée, le message suivant s'affiche : **Configuration terminée**. Cliquez sur **Fermer**.

14. Dans **Gestionnaire de serveur**, vérifiez si une notification s'affiche pour vous informer qu'un redémarrage est requis. Cela peut varier en fonction du rôle serveur installé. Si un redémarrage est requis, veillez à redémarrer le serveur pour terminer l'installation.

# Étape suivante

## Étape 2 : configurer WSUS

# Étape 2 : configurer WSUS

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

Après avoir installé le rôle serveur Windows Server Update Services (WSUS) sur votre serveur, vous devez le configurer correctement. Vous devez également configurer vos ordinateurs clients pour qu'ils reçoivent les mises à jour du serveur WSUS.

## 2.1. Configurer des connexions réseau

Avant de commencer le processus de configuration, assurez-vous de connaître les réponses aux questions suivantes :

- Le pare-feu du serveur est-il configuré pour autoriser les clients à accéder au serveur ?
- Cet ordinateur peut-il se connecter au serveur en amont (le serveur désigné pour télécharger les mises à jour à partir de Microsoft Update) ?
- Connaissez-vous le nom du serveur proxy et les informations d'identification de l'utilisateur nécessaires pour s'y connecter, le cas échéant ?

Vous pouvez ensuite commencer à configurer les paramètres réseau WSUS suivants :

- **Mises à jour** : spécifiez la façon dont ce serveur doit obtenir des mises à jour (à partir de Microsoft Update ou d'un autre serveur WSUS).
- **Proxy** : si vous identifiez que WSUS doit utiliser un serveur proxy pour avoir accès à Internet, configurez les paramètres du proxy sur le serveur WSUS.
- **Pare-feu** : si vous identifiez que WSUS se trouve derrière un pare-feu d'entreprise, effectuez des étapes supplémentaires sur l'appareil de périphérie pour autoriser le trafic WSUS.

> ⓘ **Important**
>
> Si vous n'avez qu'un seul serveur WSUS, il doit avoir accès à Internet, car il doit télécharger les mises à jour à partir de Microsoft. Si vous avez plusieurs serveurs WSUS, un seul serveur a besoin d'un accès à Internet. Les autres ont uniquement besoin d'un accès réseau au serveur

WSUS connecté à Internet. Vos ordinateurs clients n'ont pas besoin d'accès à Internet. Ils ont uniquement besoin d'un accès réseau à un serveur WSUS.

**Conseil**

Si votre réseau est *isolé* (s'il n'a pas accès à Internet du tout), vous pouvez toujours utiliser WSUS pour fournir des mises à jour aux ordinateurs clients sur le réseau. Cette approche nécessite deux serveurs WSUS. Un serveur WSUS avec accès à Internet collecte les mises à jour de Microsoft. Un deuxième serveur WSUS sur le réseau protégé envoie les mises à jour aux ordinateurs clients. Les mises à jour sont exportées du premier serveur sur un support amovible, transportées à travers la zone de séparation, puis importées dans le deuxième serveur. Cette configuration est avancée et dépasse la portée de cet article.

## 2.1.1. Configurer votre pare-feu pour permettre à votre premier serveur WSUS de se connecter aux domaines Microsoft sur Internet

Si vous avez un pare-feu d'entreprise entre WSUS et Internet, vous devez peut-être le configurer pour garantir que WSUS obtient les mises à jour. Pour obtenir des mises à jour de Microsoft Update, le serveur WSUS utilise les ports 80 et 443 avec le protocole HTTP et HTTPS. Même si la plupart des pare-feu d'entreprise autorisent ce type de trafic, certaines sociétés limitent l'accès à Internet à partir des serveurs en raison de stratégies de sécurité. Si votre entreprise restreint l'accès, vous devez configurer votre pare-feu pour permettre à votre serveur WSUS d'accéder aux domaines Microsoft.

Votre premier serveur WSUS doit disposer d'un accès sortant aux ports 80 et 443 sur les domaines suivants :

- http://windowsupdate.microsoft.com
- http ://*.windowsupdate.microsoft.com
- https ://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http ://*.windowsupdate.com

- http://download.windowsupdate.com
- https://download.microsoft.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com
- http://go.microsoft.com
- http://dl.delivery.mp.microsoft.com
- https://dl.delivery.mp.microsoft.com
- http://*.delivery.mp.microsoft.com
- https://*.delivery.mp.microsoft.com

Si vous gérez les mises à jour Microsoft 365, ce qui nécessite Microsoft Configuration Manager, consultez Gérer les mises à jour des applications Microsoft 365 avec Microsoft Configuration Manager pour plus d'informations sur les domaines que vous devez autoriser.

> **Important**
>
> Vous devez configurer votre pare-feu pour autoriser le premier serveur WSUS à accéder à n'importe quelle URL au sein de ces domaines. Les adresses IP associées à ces domaines changent constamment. Par conséquent, n'essayez pas d'utiliser des plages d'adresses IP à la place.

## 2.1.2. Configurer le pare-feu pour permettre à d'autres serveurs WSUS de se connecter au premier serveur

Si vous avez plusieurs serveurs WSUS, vous devez configurer les autres serveurs WSUS pour accéder au premier serveur (*le plus haut*). Vos autres serveurs WSUS reçoivent ensuite toutes leurs informations de mise à jour à partir du serveur le plus haut. Cette configuration vous permet de gérer l'ensemble de votre réseau à l'aide de la console d'administration WSUS sur le serveur principal.

Vos autres serveurs WSUS doivent avoir un accès sortant au serveur principal via deux ports. Par défaut, ces ports sont 8530 et 8531. Vous pouvez modifier ces ports, comme décrit dans

Configurer le serveur web IIS du serveur WSUS pour utiliser TLS pour certaines connexions plus loin dans cet article.

> ⓘ **Remarque**
>
> Si la connexion réseau entre les serveurs WSUS est lente ou coûteuse, vous pouvez configurer un ou plusieurs autres serveurs WSUS pour recevoir les charges utiles de mise à jour directement de Microsoft. Dans ce cas, seule une petite quantité de données est envoyée de ces serveurs WSUS au serveur le plus haut. Pour que cette configuration fonctionne, les autres serveurs WSUS doivent avoir accès aux mêmes domaines Internet que le serveur principal.

> ⓘ **Remarque**
>
> Si vous disposez d'une grande organisation, vous pouvez utiliser des chaînes de serveurs WSUS connectés, plutôt que de faire en sorte que tous vos autres serveurs WSUS se connectent directement au serveur principal. Par exemple, vous pouvez avoir un deuxième serveur WSUS qui se connecte au serveur principal et configurer les autres serveurs WSUS pour qu'ils se connectent au deuxième serveur WSUS.

## 2.1.3. Configurer vos serveurs WSUS pour utiliser un serveur proxy, si nécessaire

Si le réseau d'entreprise utilise des serveurs proxy, les serveurs proxy doivent prendre en charge les protocoles HTTP et HTTPS. Ils doivent également utiliser l'authentification de base ou l'authentification Windows. Vous pouvez répondre à ces exigences en utilisant l'une des configurations suivantes :

- Un serveur proxy unique qui prend en charge deux canaux de protocole. Dans ce cas, définissez un canal pour utiliser le protocole HTTP et l'autre canal pour utiliser HTTPS.

  > ⓘ **Remarque**
  >
  > Vous pouvez configurer un serveur proxy qui gère les deux protocoles pour WSUS pendant l'installation du logiciel du serveur WSUS.

- Deux serveurs proxy, chacun d'eux prend en charge un seul protocole. Dans ce cas, configurez un serveur proxy pour utiliser HTTP et l'autre serveur proxy pour utiliser HTTPS.

## Pour configurer WSUS pour utiliser deux serveurs proxy

1. Connectez-vous à l'ordinateur que vous envisagez d'utiliser comme serveur WSUS à l'aide d'un compte membre du groupe Administrateurs locaux.

2. Installez le rôle serveur WSUS. Lorsque vous utilisez l'Assistant Configuration WSUS, comme expliqué dans Configurer WSUS à l'aide de l'Assistant Configuration WSUS, ne spécifiez pas de serveur proxy.

3. Ouvrez l'invite de commandes (*Cmd.exe*) en tant qu'administrateur :
   a. Dans le menu **Démarrer**, cherchez **Invite de commandes**.
   b. Cliquez avec le bouton droit sur **Invite de commandes**, puis sélectionnez **Exécuter en tant qu'administrateur**.
   c. Si la boîte de dialogue **Contrôle de compte d'utilisateur** s'affiche, entrez les informations d'identification appropriées (le cas échéant), vérifiez que l'action qu'elle affiche est ce que vous souhaitez, puis sélectionnez **Continuer**.

4. Dans l'invite de commandes, accédez au dossier *C :\Program Files\Update Services\Tools* . Entrez la commande suivante :

   ```
   wsusutil ConfigureSSLproxy [<proxy-server proxy-port>] -enable
   ```

   Dans cette commande :

   - *proxy_server* est le nom du serveur proxy qui prend en charge HTTPS.
   - *proxy_port* est le numéro de port du serveur proxy.

5. Fermez l'invite de commandes.

## Pour ajouter un serveur proxy à la configuration WSUS

1. Ouvrez la console d'administration WSUS.

2. Sous **Update Services**, développez le nom du serveur, puis sélectionnez **Options**.

3. Dans le volet **Options** , sélectionnez **Mettre à jour la source et le serveur proxy**, puis accédez à l'onglet **Serveur proxy** .

4. Sélectionnez **Utiliser un serveur proxy lors de la synchronisation**, puis entrez le nom et le numéro de port du serveur proxy dans les zones correspondantes. Le numéro de port par défaut est 80.

5. Si le serveur proxy exige que vous utilisiez un compte d'utilisateur spécifique, sélectionnez **Utiliser les informations d'identification de l'utilisateur pour vous connecter au serveur proxy**. Entrez le nom d'utilisateur, le domaine et le mot de passe requis dans les zones correspondantes.

6. Si le serveur proxy prend en charge l'authentification de base, sélectionnez **Autoriser l'authentification de base (le mot de passe est envoyé en texte clair).**

7. Sélectionnez **OK**.

### Pour supprimer un serveur proxy de la configuration WSUS

1. Dans la console d'administration WSUS, sous **Update Services**, développez le nom du serveur, puis sélectionnez **Options**.

2. Dans le volet **Options** , sélectionnez **Mettre à jour la source et le serveur proxy**, puis accédez à l'onglet **Serveur proxy** .

3. Décochez la case **Utiliser un serveur proxy pendant la synchronisation**.

4. Sélectionnez **OK**.

## 2.1.4. Configurer votre pare-feu pour permettre aux ordinateurs clients d'accéder à un serveur WSUS

Vos ordinateurs clients doivent tous se connecter à l'un de vos serveurs WSUS. Chaque ordinateur client doit disposer d'un accès sortant à deux ports sur le serveur WSUS. Par défaut, ces ports sont 8530 et 8531.

# 2.2. Configurer WSUS en utilisant l'Assistant Configuration de WSUS

Les procédures décrites dans les sections suivantes utilisent l'Assistant Configuration WSUS pour configurer les paramètres WSUS. L'Assistant Configuration WSUS s'affiche la première fois que vous démarrez la console de gestion WSUS. Vous pouvez également utiliser le volet **Options** dans la console d'administration WSUS pour configurer les paramètres WSUS. Pour plus

d'informations sur l'utilisation du volet **Options** , consultez les procédures suivantes dans d'autres sections de cet article :

- Ajouter un serveur proxy à la configuration WSUS
- Activer le ciblage côté client

## Démarrez l'Assistant et configurez les paramètres initiaux

1. Dans le tableau de bord du Gestionnaire de serveur, sélectionnez **Outils**>**Windows Server Update Services**.

   > ⓘ **Remarque**
   >
   > Si la boîte de dialogue **Terminer l'installation de WSUS s'affiche** , sélectionnez **Exécuter**. Dans la boîte de dialogue **Terminer l'installation de WSUS** , sélectionnez **Fermer** une fois l'installation terminée.

   L'Assistant Configuration WSUS s'ouvre.

2. Dans la page **Avant de commencer**, vérifiez les informations et sélectionnez **Suivant**.

3. Dans la page **Rejoindre le programme d'amélioration de Microsoft Update** , lisez les instructions. Conservez la sélection par défaut pour participer au programme ou décochez la case dans le cas contraire. Sélectionnez ensuite **Suivant**.

## Configurer les paramètres en amont et du serveur proxy

1. Dans la page **Choisir un serveur en amont** , sélectionnez l'une des options suivantes :

   - **Synchroniser à partir de Microsoft Update**
   - **Synchroniser à partir d'un autre serveur Windows Server Update Services**

   Si vous choisissez de synchroniser à partir d'un autre serveur WSUS, procédez comme suit :

   a. Spécifiez le nom du serveur et le port sur lequel ce serveur doit communiquer avec le serveur en amont.

   b. Pour utiliser TLS, sélectionnez **Utiliser SSL lors de la synchronisation des informations de mise à jour**. Les serveurs utilisent le port 443 pour la synchronisation. (Vérifiez que ce serveur et le serveur en amont prennent en charge TLS.)

c. Si ce serveur est un serveur de **réplique, sélectionnez Ceci est une réplique du serveur en amont**.

2. Après avoir sélectionné les options de votre déploiement, sélectionnez **Suivant**.

3. Si WSUS a besoin d'un serveur proxy pour accéder à Internet, configurez les paramètres de proxy suivants. Sinon, ignorez cette étape.

   a. Dans la page **Spécifierun serveur proxy, sélectionnez Utiliser un serveur proxy lors de la synchronisation**. Entrez ensuite le nom du serveur proxy et le numéro de port (port 80 par défaut) dans les zones correspondantes.

   b. Si vous souhaitez vous connecter au serveur proxy à l'aide d'informations d'identification utilisateur spécifiques, sélectionnez **Utiliser les informations d'identification de l'utilisateur pour vous connecter au serveur proxy**. Entrez ensuite le nom d'utilisateur, le domaine et le mot de passe de l'utilisateur dans les zones correspondantes.

      Si vous souhaitez activer l'authentification de base pour l'utilisateur qui se connecte au serveur proxy, sélectionnez **Autoriser l'authentification de base (le mot de passe est envoyé en clair)** .

4. Sélectionnez **Suivant**.

5. Dans la page **Se connecter au serveur en amont** , sélectionnez **Démarrer la connexion**.

6. Dès que WSUS se connecte au serveur, sélectionnez **Suivant**.

## Sélectionner des langues, des produits et des classifications

1. Dans la page **Choisir des langues** , vous pouvez sélectionner les langues à partir desquelles WSUS reçoit des mises à jour : toutes les langues ou un sous-ensemble de langues. La sélection d'un sous-ensemble de langues permet d'économiser de l'espace disque, mais il est important de sélectionner toutes les langues dont ont besoin tous les clients de ce serveur WSUS.

   Si vous choisissez d'obtenir les mises à jour dans certaines langues uniquement, sélectionnez **Télécharger les mises à jour dans ces langues uniquement**, puis sélectionnez les langues correspondantes. Sinon, laissez la valeur par défaut.

   > ⚠ **Avertissement**

> Si vous sélectionnez l'option **Télécharger les mises à jour uniquement dans ces langues** et qu'un serveur WSUS en aval y est connecté, cette option force le serveur en aval à utiliser uniquement les langues sélectionnées.

2. Sélectionnez **Suivant**.

3. Dans la page **Choisir des** produits, spécifiez les produits pour lesquels vous souhaitez mettre à jour. Sélectionnez des catégories de produits, telles que Windows ou des produits spécifiques, tels que Windows Server 2019. La sélection d'une catégorie de produits entraîne celle de tous les produits de cette catégorie.

4. Sélectionnez **Suivant**.

5. La page **Choisir les classifications** permet de sélectionner les classifications de mise à jour que vous voulez obtenir. Sélectionnez toutes les classifications ou un sous-ensemble d'entre eux, puis sélectionnez **Suivant**.

## Configurer la planification de synchronisation

1. Dans la page **Définir la planification de synchronisation** , sélectionnez s'il faut effectuer la synchronisation manuellement ou automatiquement.

    - Si vous sélectionnez **Synchroniser manuellement**, vous devez démarrer le processus de synchronisation à partir de la console d'administration WSUS.

    - Si vous sélectionnez **Synchroniser automatiquement**, le serveur WSUS se synchronise à intervalles définis.

      Pour **la première synchronisation**, définissez l'heure, puis spécifiez le nombre de synchronisations par jour que vous souhaitez que ce serveur effectue. Par exemple, si vous spécifiez quatre synchronisations par jour, à partir de 3 h 00, les synchronisations se produisent à 3 h 00, 9 h 00, 13 h 00 et 19 h 00.

2. Sélectionnez **Suivant**.

## Terminer l'Assistant

1. Dans la page **Terminée** , si vous souhaitez démarrer la synchronisation immédiatement, sélectionnez **Commencer la synchronisation initiale**. Si vous ne sélectionnez pas cette option, vous devez utiliser la console de gestion WSUS pour effectuer la synchronisation initiale.

2. Si vous souhaitez en savoir plus sur d'autres paramètres, sélectionnez **Suivant**. Dans le cas contraire, sélectionnez **Terminer** pour terminer l'assistant et finaliser la configuration initiale de WSUS.

Quand vous sélectionnez **Terminer**, la console d'administration WSUS s'affiche. Vous utilisez cette console pour gérer votre réseau WSUS, comme décrit dans les sections ultérieures de cet article.

## 2.3. Sécuriser WSUS avec le protocole TLS

Vous devez utiliser le protocole TLS pour sécuriser votre réseau WSUS. WSUS peut utiliser TLS pour authentifier les connexions et chiffrer et protéger les informations de mise à jour.

> ⚠ **Avertissement**
>
> La sécurisation de WSUS à l'aide du protocole TLS est importante pour la sécurité de votre réseau. Si votre serveur WSUS n'utilise pas correctement TLS pour sécuriser ses connexions, un attaquant peut modifier les informations de mise à jour cruciales lorsqu'il est envoyé d'un serveur WSUS à un autre, ou du serveur WSUS aux ordinateurs clients. *Dans ce cas, l'attaquant peut installer des logiciels malveillants sur des ordinateurs clients.*

> ⓘ **Important**
>
> Les clients et les serveurs en aval configurés pour utiliser TLS ou HTTPS doivent également être configurés pour utiliser un nom de domaine complet (FQDN) pour leur serveur WSUS en amont.

### 2.3.1. Activer TLS/HTTPS sur le service IIS du serveur WSUS pour utiliser TLS/HTTPS

Pour commencer le processus d'utilisation de TLS/HTTPS, vous devez activer la prise en charge de TLS sur le service IIS (Internet Information Services) du serveur WSUS. Cet effort implique la création d'un certificat SSL (TLS/Secure Sockets Layer) pour le serveur.

Les étapes requises pour obtenir un certificat TLS/SSL pour le serveur dépassent l'étendue de cet article et dépendent de votre configuration réseau. Pour plus d'informations et pour obtenir des instructions sur l'installation des certificats et la configuration de cet environnement, consultez la documentation relative aux services de certificats Active Directory.

## 2.3.2. Configurer le serveur web IIS du serveur WSUS pour utiliser TLS pour certaines connexions

WSUS requiert deux ports pour les connexions à d'autres serveurs WSUS et aux ordinateurs clients. Un port utilise TLS/HTTPS pour envoyer des *métadonnées* de mise à jour (informations cruciales sur les mises à jour). Par défaut, le port 8531 est utilisé à cet effet. Un deuxième port utilise le protocole HTTP pour envoyer des charges utiles de mise à jour. Par défaut, le port 8530 est utilisé à cet effet.

> ⓘ **Important**
>
> Vous ne pouvez pas configurer l'ensemble du site web WSUS pour exiger TLS. WSUS est conçu pour chiffrer uniquement les métadonnées de mise à jour. Windows Update distribue les mises à jour de la même façon.
>
> Pour empêcher un attaquant de falsifier les charges utiles de mise à jour, toutes les charges utiles de mise à jour sont signées en utilisant un ensemble spécifique de certificats de signature approuvés. En outre, un hachage de chiffrement est calculé pour chaque charge utile de mise à jour. Le hachage est envoyé à l'ordinateur client sur la connexion HTTPS sécurisée des métadonnées, en même temps que les autres métadonnées de la mise à jour. Lorsqu'une mise à jour est téléchargée, le logiciel client vérifie la signature numérique et le hachage de la charge utile. Si la mise à jour a changé, elle n'est pas installée.

Vous devez exiger TLS uniquement pour les racines virtuelles IIS suivantes :

- **SimpleAuthWebService**
- **DSSAuthWebService**
- **ServerSyncWebService**
- **APIremoting30**
- **ClientWebService**

Vous ne devez pas exiger TLS pour les racines virtuelles suivantes :

- **Contenu**
- **Inventaire**

- **ReportingWebService**
- **SelfUpdate**

Le certificat de l'autorité de certification (CA) doit être importé dans le magasin de CA racine de confiance de l'ordinateur local de chaque serveur WSUS, ou, si le magasin existe, dans le magasin de CA racine de confiance de WSUS.

Pour plus d'informations sur l'utilisation de certificats TLS/SSL dans IIS, consultez Comment configurer SSL sur IIS 7 ou version ultérieure.

> ⓘ **Important**
>
> Vous devez utiliser le stockage de certificats de l'ordinateur local. Vous ne pouvez pas utiliser le magasin de certificats d'un utilisateur.

Normalement, vous devez configurer IIS afin d'utiliser le port 8531 pour les connexions HTTPS et le port 8530 pour les connexions HTTP. Si vous changez ces ports, vous devez utiliser deux numéros de port adjacents. Le numéro de port utilisé pour les connexions HTTP doit être exactement le numéro de port utilisé pour les connexions HTTPS moins 1.

Vous devez réinitialiser le `ClientServicingProxy` proxy client si le nom du serveur, la configuration TLS ou le numéro de port change.

## 2.3.3. Configurer WSUS pour utiliser le certificat de signature TLS/SSL pour ses connexions clientes

1. Connectez-vous au serveur WSUS à l'aide d'un compte membre du groupe Administrateurs WSUS ou du groupe Administrateurs locaux.
2. Dans le menu **Démarrer** , entrez **CMD**, cliquez avec le bouton droit sur **Invite de commandes**, puis sélectionnez **Exécuter en tant qu'administrateur**.
3. Accédez au dossier *C :\Program Files\Update Services\Tools* .
4. Dans l'invite de commandes, entrez la commande suivante :

   ```
   wsusutil configuressl <certificate-name>
   ```

   Dans cette commande, *le nom de certificat* est le nom DNS (Domain Name System) du serveur WSUS.

### 2.3.4. Sécuriser la connexion SQL Server, si nécessaire

Si vous utilisez WSUS avec une base de données SQL Server distante, la connexion entre le serveur WSUS et le serveur de base de données n'est pas sécurisée via TLS. Cette situation crée un vecteur d'attaque potentiel. Pour protéger cette connexion, tenez compte des recommandations suivantes :

- Activez la protection étendue SQL Server pour l'authentification (EPA) sur l'instance SQL Server, et configurez le paramètre de chiffrement que votre version SQL Server exige. L'EPA valide les informations de liaison au canal afin de contribuer à protéger la connexion. Après avoir activé l'EPA, vérifiez que la synchronisation WSUS se termine correctement. Pour plus d'informations, consultez les meilleures pratiques de sécurité SQL Server.
- Déplacez la base de données WSUS sur le serveur WSUS.
- Déplacez le serveur de base de données distant et le serveur WSUS sur un réseau privé.
- Déployez le protocole IPsec (Internet Protocol security) pour sécuriser le trafic réseau. Pour plus d'informations sur IPsec, consultez Création et utilisation des stratégies IPsec.

### 2.3.5. Créer un certificat de signature de code pour la publication locale, si nécessaire

Outre la distribution des mises à jour que Microsoft fournit, WSUS prend en charge la publication locale. Vous pouvez utiliser la publication locale pour créer et distribuer des mises à jour que vous concevez vous-même, avec vos propres charges utiles et comportements.

L'activation et la configuration de la publication locale n'entrent pas dans le cadre de cet article. Pour plus d'informations, consultez Publication locale.

> **Important**
>
> La publication locale est un processus complexe très souvent inutile. Avant de décider d'activer la publication locale, vous devez examiner attentivement la documentation et déterminer si vous souhaitez utiliser cette fonctionnalité et comment l'utiliser.

## 2.4. Configuration des groupes d'ordinateurs WSUS

Les groupes d'ordinateurs représentent une part importante de l'utilisation efficace de WSUS. Vous pouvez utiliser des groupes d'ordinateurs pour tester et cibler les mises à jour sur des

ordinateurs spécifiques. Il existe deux groupes d'ordinateurs par défaut : Tous les ordinateurs et Ordinateurs non affectés. Par défaut, lorsque chaque ordinateur client contacte pour la première fois le serveur WSUS, ce dernier l'ajoute à ces deux groupes.

Vous pouvez créer autant de groupes d'ordinateurs personnalisés que nécessaire pour gérer les mises à jour dans votre organisation. Il est recommandé de créer au moins un groupe d'ordinateurs pour tester les mises à jour avant de les déployer vers d'autres ordinateurs de votre organisation.

## 2.4.1. Choisir une approche pour attribuer des ordinateurs clients à des groupes d'ordinateurs

Il existe deux approches pour attribuer des ordinateurs clients à des groupes d'ordinateurs. La bonne approche pour votre organisation dépend de la façon dont vous gérez généralement vos ordinateurs clients.

- **Ciblage côté serveur** : cette approche est la cible par défaut. Dans cette approche, vous attribuez des ordinateurs clients à des groupes d'ordinateurs en utilisant la console d'administration WSUS.

  Cette approche vous permet de déplacer rapidement des ordinateurs clients d'un groupe à un autre quand les circonstances changent. Toutefois, vous devez déplacer manuellement les nouveaux ordinateurs clients du groupe Ordinateurs non attribués vers le groupe d'ordinateurs approprié.

- **Ciblage côté client** : dans cette approche, vous attribuez chaque ordinateur client à des groupes d'ordinateurs en utilisant des paramètres de stratégie définis sur l'ordinateur client lui-même.

  Cette approche facilite l'attribution des nouveaux ordinateurs clients aux groupes appropriés. Vous effectuez cette opération dans le cadre de la configuration de l'ordinateur client pour recevoir les mises à jour du serveur WSUS. Toutefois, vous ne pouvez pas affecter d'ordinateurs clients à des groupes d'ordinateurs ou les déplacer d'un groupe d'ordinateurs vers un autre via la console d'administration WSUS. Vous devez plutôt modifier les stratégies des ordinateurs clients.

## 2.4.2. Activer le ciblage côté client, le cas échéant

> ⓘ **Important**

Ignorez les étapes décrites dans cette section si vous envisagez d'utiliser le ciblage côté serveur.

1. Dans la console d'administration WSUS, sous **Update Services**, développez le serveur WSUS, puis sélectionnez **Options**.
2. Dans le volet **Options** , sélectionnez **Ordinateurs**. Accédez à l'onglet **Général** , puis sélectionnez **Utiliser les paramètres de stratégie de groupe ou de Registre sur les ordinateurs**.

### 2.4.3. Créer les groupes d'ordinateurs souhaités

> ⓘ **Remarque**
>
> Vous devez créer des groupes d'ordinateurs dans la console d'administration WSUS, que vous utilisiez le ciblage côté serveur ou le ciblage côté client pour ajouter des ordinateurs clients aux groupes d'ordinateurs.

1. Dans la console d'administration WSUS, sous **Services de mise à jour**, développez le serveur WSUS, développez **Ordinateurs**, cliquez avec le bouton droit sur **Tous les ordinateurs**, puis sélectionnez **Ajouter un groupe d'ordinateurs**.
2. Dans la boîte de dialogue **Ajouter un groupe d'ordinateurs**, dans **Nom**, spécifiez le nom du nouveau groupe. Sélectionnez ensuite **Ajouter**.

## 2.5. Configurer des ordinateurs clients pour établir des connexions TLS avec le serveur WSUS

En supposant que vous configurez le serveur WSUS pour protéger les connexions des ordinateurs clients à l'aide de TLS, vous devez configurer les ordinateurs clients pour approuver ces connexions TLS.

Le certificat TLS/SSL du serveur WSUS doit être importé dans le magasin AC racine de confiance des ordinateurs clients, ou dans le magasin AC racine de confiance du service de mise à jour automatique des ordinateurs clients, le cas échéant.

> ⓘ **Important**

Vous devez utiliser le stockage de certificats de l'ordinateur local. Vous ne pouvez pas utiliser le magasin de certificats d'un utilisateur.

Les ordinateurs clients doivent approuver le certificat que vous liez au serveur WSUS. Selon le type de certificat utilisé, vous devez peut-être configurer un service permettant aux ordinateurs clients d'approuver le certificat lié au serveur WSUS.

Si vous utilisez la publication locale, vous devez également configurer les ordinateurs clients pour qu'ils approuvent le certificat de signature de code du serveur WSUS. Pour obtenir des instructions, consultez Publication locale.

## 2.6. Configurer des ordinateurs clients pour recevoir des mises à jour à partir du serveur WSUS

Par défaut, vos ordinateurs clients reçoivent des mises à jour de Windows Update. Ils doivent être configurés pour recevoir des mises à jour du serveur WSUS à la place.

**ⓘ Important**

Cet article présente un ensemble d'étapes pour configurer les ordinateurs clients avec une stratégie de groupe. Ces étapes sont appropriées dans de nombreux cas. Toutefois, de nombreuses autres options sont disponibles pour configurer le comportement des mises à jour sur les ordinateurs clients, notamment l'utilisation de la gestion des appareils mobiles. Pour obtenir de la documentation sur ces options, consultez **Gérer les paramètres Windows Update supplémentaires**.

### 2.6.1. Choisir le jeu de stratégies correct à modifier

Si Active Directory est configuré dans votre réseau, vous pouvez configurer un ou plusieurs ordinateurs simultanément en les incluant dans un objet de stratégie de groupe (GPO), puis en configurant cet objet de stratégie de groupe avec les paramètres WSUS.

Nous vous recommandons de créer un objet de stratégie de groupe qui contient uniquement des paramètres WSUS. Liez ce GPO WSUS à un conteneur Active Directory approprié pour votre environnent.

Dans un environnement simple, vous pouvez lier un seul GPO WSUS au domaine. Dans un environnement plus complexe, vous pouvez lier plusieurs GPO WSUS à plusieurs unités

d’organisation. Lorsque vous liez des GPO à des unités d'organisation, vous pouvez appliquer les paramètres de stratégie WSUS à différents types d'ordinateurs.

Si vous n’utilisez pas Active Directory dans votre réseau, vous devez configurer chaque ordinateur à l’aide de l’éditeur de stratégie de groupe local.

## 2.6.2. Modifier les stratégies pour configurer les ordinateurs clients

Suivez les étapes décrites dans les sections suivantes pour configurer les ordinateurs clients à l’aide des paramètres de stratégie.

> ⓘ **Remarque**
>
> Ces instructions supposent que vous utilisez les versions les plus récentes des outils de modification de stratégie. Dans les versions antérieures des outils, les stratégies peuvent être organisées différemment.

### Ouvrez l’éditeur de stratégie et accédez à l’élément Windows Update

1. Ouvrez l’objet de stratégie approprié :

    - Si vous utilisez Active Directory, ouvrez la console de gestion des stratégies de groupe, accédez à l’objet de stratégie de groupe sur lequel vous souhaitez configurer WSUS, puis sélectionnez **Modifier**. Développez ensuite **Configuration de l’ordinateur** et développez **Stratégies**.
    - Si vous n’utilisez pas Active Directory, ouvrez l’éditeur de stratégie de groupe local. La stratégie de l’ordinateur local s’affiche. Développez **Configuration ordinateur**.

2. Dans l'objet que vous avez étendu à l'étape précédente, étendez **Modèles d'administration**>**Composants Windows**>**Windows Update**. Si votre système d’exploitation est Windows 10 ou Windows 11, sélectionnez également **Gérer l’expérience utilisateur final**.

### Modifier le paramètre des mises à jour automatiques

1. Dans le volet d’informations, double-cliquez sur **Configurer les mises à jour automatiques**. La stratégie **Configuration du service Mises à jour automatiques** s’ouvre.

2. Sélectionnez **Activé**, puis sélectionnez l'option souhaitée sous le paramètre **Configurer la mise à jour automatique** pour gérer la façon dont la fonctionnalité de mise à jour automatique doit télécharger et installer les mises à jour approuvées.

   Nous vous recommandons d'utiliser le paramètre **Téléchargement automatique et planification des installations**. Il garantit que les mises à jour que vous approuvez dans WSUS sont téléchargées et installées en temps voulu, sans avoir besoin d'intervention de l'utilisateur.

3. Si vous le souhaitez, modifiez d'autres parties de la stratégie. Pour plus d'informations, consultez Gérer des paramètres Windows Update supplémentaires.

   > ⓘ **Remarque**
   >
   > Les **mises à jour d'installation à partir d'autres paramètres de produits Microsoft** n'ont aucun effet sur les ordinateurs clients recevant des mises à jour de WSUS. Les ordinateurs clients reçoivent toutes les mises à jour approuvées pour elles sur le serveur WSUS.

4. Sélectionnez **OK** pour fermer la stratégie **Configurer les mises à jour automatiques**.

## Modifier le paramètre pour spécifier un serveur intranet pour héberger des mises à jour

1. Dans le volet d'informations, double-cliquez sur **Spécifier l'emplacement intranet du service de mise à jour Microsoft**. Si votre système d'exploitation est Windows 10 ou Windows 11, revenez d'abord au nœud **Windows Update** de l'arborescence, puis sélectionnez **Gérer les mises à jour proposées à partir du service Windows Server Update**.

   La stratégie **Spécifier l'emplacement intranet du service de mise à jour Microsoft** s'ouvre.

2. Sélectionnez **Activé**, puis entrez l'URL du serveur WSUS dans les zones **Définir le service de mise à jour intranet pour détecter les mises à jour** et **Définir le serveur de statistiques intranet**.

   > ⚠ **Avertissement**
   >
   > Veillez à inclure le bon port dans l'URL. En supposant que vous configurez le serveur pour qu'il utilise TLS comme recommandé, vous devez spécifier le port configuré pour HTTPS. Par exemple, si vous choisissez d'utiliser le port 8531 pour HTTPS et que le nom

de domaine du serveur est wsus.contoso.com, vous devez entrer `https://wsus.contoso.com:8531` dans les deux zones de texte.

3. Sélectionnez **OK** pour fermer la stratégie **Spécifier l'emplacement intranet du service de mise à jour Microsoft**.

### Configurer le ciblage côté client, le cas échéant

Si vous choisissez d'utiliser le ciblage côté client, procédez comme suit dans cette section pour spécifier le groupe d'ordinateurs approprié pour les ordinateurs clients que vous configurez.

> ⓘ **Remarque**
>
> Ces étapes supposent que vous venez de suivre les étapes de modification des stratégies pour configurer les ordinateurs clients.

1. Dans l'éditeur de stratégie, accédez à l'élément **Windows Update** . Si votre système d'exploitation est Windows 10 ou Windows 11, sélectionnez également **Gérer les mises à jour proposées à partir du service Windows Server Update**.

2. Dans le volet d'informations, double-cliquez sur **Activer le ciblage côté client**. La stratégie **Activer le ciblage côté client** s'ouvre.

3. Sélectionnez **Enabled**. Sous **Nom du groupe cible pour cet ordinateur**, entrez le nom du groupe d'ordinateurs WSUS auquel vous souhaitez ajouter les ordinateurs clients.

   Si vous exécutez une version actuelle de WSUS, vous pouvez ajouter les ordinateurs clients à plusieurs groupes d'ordinateurs en entrant les noms des groupes séparés par des points-virgules. Par exemple, vous pouvez entrer **Comptabilité;Direction** pour ajouter les ordinateurs clients aux groupes d'ordinateurs Comptabilité et Direction.

4. Sélectionnez **OK** pour fermer la stratégie **Activer le ciblage côté client**.

## 2.6.3. Permettre à l'ordinateur client de se connecter au serveur WSUS

Les ordinateurs clients n'apparaissent pas dans la console d'administration WSUS tant qu'ils ne se connectent pas au serveur WSUS pour la première fois.

1. Attendez que les modifications apportées à la stratégie prennent effet sur l'ordinateur client.

   Si vous utilisez un objet de stratégie de groupe basé sur Active Directory pour configurer les ordinateurs clients, le mécanisme de mise à jour des stratégies de groupe prend un certain temps pour remettre les modifications à un ordinateur client. Si vous souhaitez accélérer ce processus, vous pouvez ouvrir l'invite de commandes avec des privilèges élevés, puis entrer la commande **gpupdate /force**.

   Si vous utilisez l'éditeur de stratégie de groupe local pour configurer un ordinateur client individuel, les modifications prennent effet immédiatement.

2. Redémarrez l'ordinateur client. Cela permet de garantir que le logiciel Windows Update sur l'ordinateur détecte les changements de la stratégie.

3. Laissez l'ordinateur client analyser les mises à jour. Cette analyse prend généralement un certain temps.

   Vous pouvez accélérer le processus à l'aide de l'une des options suivantes :

   - Sur Windows 10 ou 11, utilisez la page Paramètres de **Windows Update** pour rechercher manuellement les mises à jour.
   - Dans les versions de Windows antérieures à Windows 10, utilisez l'icône **Windows Update** dans le Panneau de configuration pour rechercher manuellement les mises à jour.
   - Sur les versions de Windows antérieures à Windows 10, ouvrez l'invite de commandes avec des privilèges élevés, puis entrez la commande **wuauclt /detectnow**.

## 2.6.4 Vérifier la réussite de la connexion de l'ordinateur client au serveur WSUS

Si vous effectuez toutes les étapes précédentes, vous voyez les résultats suivants :

- L'ordinateur client recherche bien les mises à jour. (Il est possible qu'il ne trouve pas de mises à jour applicables à télécharger et à installer.)

- Au bout d'environ 20 minutes, l'ordinateur client apparaît dans la liste des ordinateurs affichés dans la console d'administration WSUS, en fonction du type de ciblage :

  - Si vous utilisez le ciblage côté serveur, l'ordinateur client s'affiche dans les groupes d'ordinateurs Tous les ordinateurs et Ordinateurs non attribués.

- Si vous utilisez le ciblage côté client, l'ordinateur client apparaît dans le groupe d'ordinateurs Tous les ordinateurs et dans le groupe d'ordinateurs que vous sélectionnez lors de la configuration de l'ordinateur client.

### 2.6.5. Configurer le ciblage côté serveur de l'ordinateur client, le cas échéant

Si vous utilisez le ciblage côté serveur, vous devez maintenant ajouter le nouvel ordinateur client aux groupes d'ordinateurs appropriés.

1. Dans la console d'administration WSUS, recherchez le nouvel ordinateur client. Il doit apparaître dans les groupes d'ordinateurs Tous les ordinateurs et Ordinateurs non attribués de la liste d'ordinateurs du serveur WSUS.
2. Cliquez avec le bouton droit sur l'ordinateur client et sélectionnez **Changer l'appartenance**.
3. Dans la boîte de dialogue, sélectionnez les groupes d'ordinateurs appropriés et sélectionnez **OK**.

## Étape suivante

**Étape 3 : Approuver et déployer des mises à jour**

---

Last updated on 28/07/2026

# Etape 3 : Approuver et déployer des mises à jour dans WSUS

16/08/2025

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

Les ordinateurs d'un groupe d'ordinateurs contactent automatiquement le serveur WSUS dans les 24 heures suivantes pour obtenir des mises à jour. Vous pouvez utiliser la fonctionnalité de création de rapports WSUS pour déterminer si ces mises à jour ont été déployées sur les ordinateurs de test. Lorsque les tests sont correctement effectués, vous pouvez approuver les mises à jour pour les groupes d'ordinateurs applicables dans votre organisation.

## 3.1. Approuver et déployer des mises à jour WSUS

Utilisez la procédure suivante pour approuver et déployer des mises à jour.

### Pour approuver et déployer des mises à jour WSUS

1. Dans la console d'administration WSUS, cliquez sur **Mises à jour**. Dans le volet droit, un résumé de l'état de mise à jour s'affiche pour **toutes les mises à jour**, **mises à jour critiques**, **mises à jour de sécurité** et **mises à jour WSUS**.
2. Dans la section **Toutes les mises à jour** , cliquez sur **Mises à jour nécessaires par les ordinateurs**.
3. Dans la liste des mises à jour, sélectionnez celles à approuver pour une installation dans votre groupe d'ordinateurs de test. Les informations relatives à une mise à jour sélectionnée sont disponibles dans le volet inférieur du panneau **Mises à jour** . Pour sélectionner plusieurs mises à jour successives, maintenez la touche **Maj** enfoncée tout en cliquant sur les noms des mises à jour. Pour sélectionner plusieurs mises à jour non incohérentes, appuyez sur la touche **Ctrl** enfoncée tout en cliquant sur les noms des mises à jour.
4. Cliquez avec le bouton droit sur la sélection, puis cliquez sur **Approuver**.
5. Dans la boîte de dialogue **Approuver les mises à jour** , sélectionnez votre groupe de tests, puis cliquez sur la flèche vers le bas.
6. Cliquez sur **Approuvé pour l'installation**, puis sur **OK**.

7. La fenêtre **Progression de l'approbation** s'affiche, qui affiche la progression des tâches qui affectent l'approbation de mise à jour. Une fois le processus d'approbation terminé, cliquez sur **Fermer**.

# 3.2. Configurer les règles d'approbation automatique

Approbations automatiques vous permet de déterminer comment approuver automatiquement l'installation des mises à jour pour les groupes sélectionnés et comment approuver les révisions des mises à jour existantes.

## Pour configurer Approbations automatiques

1. Dans la console d'administration WSUS, sous **Update Services**, développez le serveur WSUS, puis cliquez sur **Options**. La fenêtre **Options** s'ouvre.

2. Dans **Options**, cliquez sur **Approbations automatiques**. La boîte de dialogue Approbations automatiques s'ouvre.

3. Dans **Mettre à jour les règles**, cliquez sur **Nouvelle règle**. La boîte de dialogue **Ajouter une règle** s'ouvre.

4. Dans **ajouter une règle**, à **l'étape 1 : sélectionnez Propriétés**, sélectionnez n'importe quelle option unique ou combinaison d'options dans les éléments suivants :

    - **Lorsqu'une mise à jour se trouve dans une classification spécifique**
        - Lorsque vous sélectionnez la classification **des mises à niveau** , sachez que les mises à jour des fonctionnalités Windows publiées tous les mois sont également classées comme **mises à niveau**. L'approbation automatique de ces mises à jour peut entraîner la mise à niveau du système d'exploitation des appareils. Les appareils Windows 10 applicables peuvent par exemple être mis à niveau vers Windows 11. En outre, les mises à jour de fonctionnalité nécessitent un espace disque supplémentaire. Pour plus d'informations, consultez les considérations relatives à l'UUP lors de la planification de votre déploiement WSUS.

    - **Lorsqu'une mise à jour se trouve dans un produit spécifique**

    - **Définir une échéance pour l'approbation**

5. À **l'étape 2 : modifiez les propriétés**, cliquez sur chacune des options répertoriées, puis sélectionnez les options appropriées pour chacune d'elles.

6. À **l'étape 3 : Spécifiez un nom**, tapez un nom pour votre règle, puis cliquez sur **OK**.

7. Cliquez sur **OK** pour fermer la boîte de dialogue Approbations automatiques.

## 3.3. Passer en revue les mises à jour installées avec les rapports WSUS

24 heures après avoir approuvé les mises à jour, vous pouvez utiliser la fonctionnalité de création de rapports WSUS pour déterminer si les mises à jour ont été déployées sur les ordinateurs du groupe de test. Pour vérifier l'état d'une mise à jour, vous pouvez utiliser la fonctionnalité de création de rapports WSUS comme suit.

### Pour passer en revue les mises à jour

1. Dans le volet de navigation de la console d'administration WSUS, cliquez sur **Rapports**.
2. Dans la page **Rapports** , cliquez sur le rapport **De synthèse de l'état de mise à jour** . La fenêtre **Rapports de mises à jour** s'affiche.
3. Si vous souhaitez filtrer la liste des mises à jour, sélectionnez les critères que vous souhaitez utiliser, par exemple **, Inclure des mises à jour dans ces classifications**, puis cliquez sur **Exécuter le rapport**.
4. Le volet **Rapports de mises à jour** s'affiche. Vous pouvez vérifier l'état de mises à jour individuelles en sélectionnant la mise à jour dans la section gauche du volet. La dernière section du volet de rapport indique la synthèse de l'état de la mise à jour.
5. Vous pouvez enregistrer ou imprimer ce rapport en cliquant sur l'icône appropriée de la barre d'outils.
6. Après avoir testé les mises à jour, vous pouvez les approuver pour une installation dans les groupes d'ordinateurs applicables de votre organisation.

# Étape suivante

**Étape 4 : Configurer les paramètres de stratégie de groupe pour les mises à jour automatiques**

# Etape 4 : Configurer les paramètres de stratégie de groupe pour fonctionnalité Mises à jour automatiques

16/08/2025

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

Dans un environnement Active Directory, vous pouvez utiliser la stratégie de groupe pour définir la manière dont les ordinateurs et les utilisateurs interagissent avec Windows Update pour obtenir des mises à jour automatiques à partir de Windows Server Update Services (WSUS). Cet article fait référence à ces ordinateurs et utilisateurs en tant que *clients WSUS*.

Cet article contient deux sections principales :

- La section Paramètres de stratégie de groupe pour les mises à jour de clients WSUS fournit des conseils normatifs et des informations comportementales relatives aux paramètres de Windows Update et du Planificateur de maintenance de la stratégie de groupe, qui contrôlent la manière dont les clients WSUS peuvent interagir avec Windows Update pour obtenir des mises à jour automatiques.
- Les sous-sections suivantes sont fournies dans les sous-sections suivantes :
  - Accès aux paramètres de Windows Update dans Stratégie de groupe fournit des conseils d'ordre général sur l'utilisation de l'Éditeur de gestion des stratégies de groupe (GPME). Cela permet aussi d'obtenir des informations sur l'accès aux paramètres des extensions de stratégie et le Planificateur de maintenance dans la stratégie de groupe pour les services de mise à jour.
  - La section Termes et définitions définit les termes relatifs à WSUS et aux services de mise à jour.

## Paramètres de stratégie de groupe pour les mises à jour de clients WSUS

Cette section fournit des informations relatives aux trois extensions de stratégie de groupe suivantes. Ces extensions contiennent les paramètres que vous pouvez utiliser pour configurer la manière dont les clients WSUS interagissent avec Windows Update pour recevoir des mises à jour automatiques.

- Configuration ordinateur > Paramètres de stratégie de Windows Update

- Configuration ordinateur > Paramètres du planificateur de maintenance
- Configuration utilisateur > Paramètres de stratégie de Windows Update

> ⓘ **Notes**
>
> Cet article part du principe que vous utilisez déjà une stratégie de groupe et que vous connaissez bien celle-ci. Si vous n'êtes pas familiarisé avec la stratégie de groupe, nous vous recommandons de consulter les informations de la section **Informations supplémentaires** de cet article avant d'essayer de configurer les paramètres de stratégie pour WSUS.

Le rôle serveur WSUS est intégré à Windows Server. Par défaut, les paramètres de stratégie de groupe pour les clients WSUS sont inclus dans la stratégie de groupe.

## Configuration ordinateur > Paramètres de stratégie de Windows Update

Cette section fournit des détails sur les paramètres de stratégie basés sur l'ordinateur suivants :

- Autoriser l'installation immédiate des mises à jour automatiques
- Autoriser les non-administrateurs à recevoir les notifications de mise à jour
- Autoriser les mises à jour signées provenant d'un emplacement intranet du service de mise à jour Microsoft
- Redémarrez toujours automatiquement à l'heure planifiée
- Fréquence de détection des mises à jour automatiques
- Configurer la fonctionnalité Mises à jour automatiques
- Retarder le redémarrage des installations planifiées
- Ne pas ajuster l'option par défaut à « Installer les mises à jour et arrêter » dans la boîte de dialogue Arrêter Windows
- Ne pas se connecter à des emplacements Internet Windows Update
- Ne pas afficher l'option « Installer les mises à jour et arrêter » dans la boîte de dialogue Arrêter Windows
- Activer le ciblage côté client
- Activation de la fonctionnalité de gestion de l'alimentation par Windows Update pour la sortie de veille automatique du système lors de l'installation de mises à jour planifiées
- Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées de mises à jour automatiques
- Redemander un redémarrage avec les installations planifiées
- Replanifier les installations planifiées des mises à jour automatiques
- Spécifier l'emplacement intranet du service de mise à jour Microsoft

- Activer les mises à jour recommandées par la fonctionnalité Mises à jour automatiques
- Activer les notifications d'applications

Dans le GPME, les stratégies Windows Update pour la configuration basée sur l'ordinateur se trouvent dans le chemin d'accès <>>des**stratégies**> de**configuration**> ordinateur**modèles**> d'administration**Windows**>**Components Windows Update**.

> ⓘ **Notes**
>
> Par défaut, ces paramètres ne sont pas configurés.

## Autoriser l'installation immédiate des mises à jour automatiques

Vous pouvez utiliser ce paramètre pour spécifier si les mises à jour automatiques installent automatiquement les mises à jour qui n'interrompent pas les services Windows ou redémarrent Windows.

> ⓘ **Notes**
>
> Si le paramètre de stratégie **Configurer les mises à jour automatiques** est défini sur **Désactivé**, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Les mises à jour ne sont pas installées immédiatement. Les administrateurs locaux peuvent modifier ce paramètre à l'aide de l'Éditeur d'objets de stratégie de groupe. |
| **Enabled** | Les mises à jour automatiques installent immédiatement les mises à jour une fois téléchargées et prêtes à être installées. |
| **Disabled** | Les mises à jour ne sont pas installées immédiatement. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Autoriser les non-administrateurs à recevoir les notifications de mise à jour

Vous pouvez utiliser ce paramètre pour spécifier si les utilisateurs non administratifs reçoivent des notifications de mise à jour en fonction du paramètre configurer la stratégie **Configurer les mises à jour automatiques** .

> ⓘ Notes
>
> Si le paramètre de stratégie **Configurer les mises à jour automatiques** est **Désactivé** ou **Non configuré**, ce paramètre de stratégie est sans effet.

> ⓘ Important
>
> Ce paramètre de stratégie est activé par défaut.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| Non configuré | Les utilisateurs voient toujours une invite de consentement **du contrôle de compte d'utilisateur** et nécessitent des autorisations élevées pour gérer les mises à jour. Un administrateur local peut modifier ce paramètre à l'aide de l'Éditeur d'objets de stratégie de groupe.<br><br>Dans Windows Vista, les utilisateurs voient également une invite de consentement **du contrôle de compte d'utilisateur** lors du masquage, de la restauration et de l'annulation des mises à jour, et ils ont besoin d'autorisations élevées pour masquer, restaurer ou annuler les mises à jour. |
| Enabled | Windows Update et Microsoft Update incluent des non-administrateurs lors de la détermination de l'utilisateur connecté qui reçoit des notifications de mise à jour. Les utilisateurs non administratifs peuvent installer tout le contenu de mise à jour facultatif, recommandé et important pour lequel ils reçoivent une notification. Les utilisateurs ne voient pas d'invite de consentement **du contrôle de compte d'utilisateur** . Les utilisateurs n'ont pas besoin d'autorisations élevées pour installer ces mises à jour, à l'exception des mises à jour qui contiennent des modifications apportées à l'interface utilisateur, aux termes du contrat de licence logiciel Microsoft ou aux paramètres Windows Update.<br><br>Dans Windows 8 et versions ultérieures, et Windows RT, ce paramètre de stratégie n'a aucun effet. |
| Disabled | Seuls les administrateurs connectés reçoivent des notifications de mise à jour. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Autoriser les mises à jour signées provenant d'un emplacement intranet du service de mise à jour Microsoft

Vous pouvez utiliser ce paramètre pour spécifier si les mises à jour automatiques acceptent les mises à jour signées par des entités autres que Microsoft lorsque la mise à jour est trouvée sur un emplacement intranet du service de mise à jour Microsoft.

> **Notes**
>
> Les mises à jour provenant d'un service autre qu'un service de mise à jour Intranet Microsoft doivent toujours être signées par Microsoft. Ce paramètre de stratégie n'affecte pas ces mises à jour.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Les mises à jour apportées à l'emplacement du service Microsoft Update intranet doivent être signées par Microsoft. |
| **Enabled** | Les mises à jour automatiques acceptent les mises à jour reçues via le service de mise à jour Microsoft sur l'intranet si elles sont signées par un certificat trouvé dans le stockage de certificats des éditeurs approuvés de l'ordinateur local. |
| **Disabled** | Les mises à jour apportées à l'emplacement du service Microsoft Update intranet doivent être signées par Microsoft. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Toujours redémarrer automatiquement à l'heure planifiée

Vous pouvez utiliser ce paramètre pour spécifier si un minuteur de redémarrage commence toujours immédiatement après que Windows Update installe des mises à jour importantes, au lieu d'avertir les utilisateurs sur l'écran de connexion pendant au moins deux jours.

> **Notes**
>
> Si le paramètre de stratégie **Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées de mises à jour automatiques** est activé, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Windows Update ne modifie pas le comportement de redémarrage de l'ordinateur. |
| **Enabled** | Un minuteur de redémarrage commence toujours immédiatement après que Windows Update installe des mises à jour importantes, au lieu que les utilisateurs soient avertis d'abord sur l'écran de connexion pendant au moins deux jours.<br><br>Le minuteur de redémarrage peut être configuré pour démarrer avec n'importe quelle valeur comprise entre 15 et 180 minutes. Quand le temps configuré pour le minuteur expire, le redémarrage se poursuit même si des utilisateurs sont connectés à l'ordinateur. |
| **Disabled** | Windows Update ne modifie pas le comportement de redémarrage de l'ordinateur. |

**Options:** Si ce paramètre est activé, vous pouvez spécifier le temps écoulé après l'installation des mises à jour avant le redémarrage forcé de l'ordinateur.

## Fréquence de détection des mises à jour automatiques

Vous pouvez utiliser ce paramètre pour spécifier les heures utilisées par Windows pour déterminer la durée d'attente avant de vérifier les mises à jour disponibles. Le temps d'attente exact est compris entre 80 et 100 % des heures spécifiées dans cette fréquence. Par exemple, si cette stratégie est utilisée pour spécifier une fréquence de détection de 20 heures, tous les clients auxquels cette stratégie applique attendent entre 16 et 20 heures avant de vérifier les mises à jour.

> ⓘ Notes
>
> - Le paramètre **Spécifier l'emplacement intranet du service de mise à jour Microsoft** doit être **Activé** pour que cette stratégie prenne effet.
> - Si le paramètre de stratégie **Configurer les mises à jour automatiques** est **Désactivé**, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Windows vérifie les mises à jour disponibles à l'intervalle par défaut de 22 heures. |
| **Enabled** | Windows vérifie les mises à jour disponibles à l'intervalle spécifié. |
| **Disabled** | Windows vérifie les mises à jour disponibles à l'intervalle par défaut de 22 heures. |

**Options:** Si ce paramètre est activé, vous pouvez spécifier l'intervalle de temps en heures pendant lequel Windows Update attend avant de vérifier les mises à jour.

## Configurer la fonctionnalité Mises à jour automatiques

Vous pouvez utiliser ce paramètre pour spécifier si les mises à jour automatiques sont activées sur cet ordinateur.

Vous pouvez configurer des mises à jour automatiques sous **Configuration ordinateur\Modèles d'administration\Composants Windows\Windows Update\Gérer l'expérience utilisateur final\Configurer les mises à jour automatiques**.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | L'utilisation des mises à jour automatiques n'est pas spécifiée au niveau de la stratégie de groupe. Un administrateur peut toujours configurer les mises à jour automatiques par le biais de l'application Paramètres, sous **Paramètres**>**Update &**options**Avancées windows Update**>**de** sécurité>. |
| **Enabled** | Windows reconnaît quand l'ordinateur est en ligne et utilise sa connexion Internet pour rechercher les mises à jour disponibles dans Windows Update. Pour utiliser ce paramètre, vous devez sélectionner l'une des cinq options répertoriées après ce tableau. Les administrateurs locaux sont autorisés à utiliser le panneau de configuration Windows Update pour sélectionner une option de configuration de leur choix. Toutefois, les administrateurs locaux ne sont pas autorisés à définir la configuration des mises à jour automatiques **sur Désactivé**. |
| **Disabled** | Les utilisateurs doivent télécharger et installer manuellement toutes les mises à jour client disponibles à partir du service Windows Update public en accédant à **Settings**> Update**&security**>**Windows Update**. |

**Options:** Si ce paramètre est activé, vous devez sélectionner l'une des options suivantes :

Agrandir le tableau

| Option | Behavior |
| --- | --- |
| **2 : notification du téléchargement et de l'installation automatique** | Quand Windows Update trouve des mises à jour qui s'appliquent à l'ordinateur, les utilisateurs sont notifiés que des mises à jour sont prêtes pour téléchargement. Les utilisateurs peuvent ensuite exécuter Windows Update pour télécharger et installer des mises à jour disponibles. |
| **3 : téléchargement automatique et notification des installations** | Il s'agit de l'option activée par défaut. Windows Update trouve des mises à jour applicables et les télécharge en arrière-plan. Les utilisateurs ne sont pas avertis ou interrompus pendant ce processus. Une fois les téléchargements terminés, les utilisateurs sont notifiés que des mises à jour sont prêtes pour installation. Les utilisateurs peuvent ensuite exécuter Windows Update pour installer les mises à jour téléchargées. |
| **4 - Téléchargement automatique et planification des installations** | Vous pouvez spécifier la planification d'installation à l'aide de cette option de stratégie de groupe. Si aucune planification n'est spécifiée, la planification par défaut pour toutes les installations est chaque jour à 3h. Si des mises à jour nécessitent un redémarrage pour terminer l'installation, Windows redémarre automatiquement l'ordinateur. Si un utilisateur est connecté à l'ordinateur quand Windows est prêt à redémarrer, l'utilisateur est notifié et peut choisir de retarder le redémarrage.<br><br>Depuis Windows 8, vous pouvez configurer l'installation des mises à jour lors de la maintenance automatique au lieu d'utiliser une planification spécifique liée à Windows Update. La maintenance automatique installe les mises à jour quand l'ordinateur n'est pas utilisé, et évite de les installer quand l'ordinateur fonctionne sur batterie. Si la maintenance automatique ne parvient pas à installer les mises à jour dans les deux jours qui suivent, Windows Update installe les mises à jour directement. Les utilisateurs sont alors avertis d'un redémarrage en attente. Un redémarrage ne se produit que s'il n'y a aucun risque de perte accidentelle de données. |
| **5 - Autoriser l'administrateur local à choisir les paramètres** | Les administrateurs locaux sont autorisés à utiliser le panneau de configuration des mises à jour automatiques pour choisir les options de configuration. Par exemple, un administrateur local peut choisir une heure d'installation planifiée. Les administrateurs locaux ne sont pas autorisés à définir la configuration pour les mises à jour automatiques **sur Désactivé**. |
| **7 : téléchargement automatique, notification pour l'installation, notification pour le redémarrage** | *Cette option est disponible uniquement dans Windows Server 2016 et versions ultérieures.* Les administrateurs locaux peuvent utiliser Windows Update pour poursuivre les installations ou redémarrer manuellement. Windows télécharge les mises à jour applicables à l'appareil et informe les utilisateurs que les mises à jour sont prêtes à être installées. Une fois les mises à jour installées, les utilisateurs sont avertis de redémarrer l'appareil. |

ⓘ Notes

Sur Windows Server, l'option **Configurer les mises à jour automatiques** est configurée sur **3** dans le Registre par défaut. Cette valeur n'est pas reflétée dans l'éditeur de stratégies de groupe (GPO). Si un administrateur configure l'option sur un autre paramètre, le nouveau paramètre prend effet. La définition du paramètre **de stratégie Configurer les mises à jour automatiques** sur **Non configuré** entraîne le comportement du téléchargement et de l'installation automatique des mises à jour.

## Délai de redémarrage pour les installations planifiées

Vous pouvez utiliser ce paramètre pour spécifier la durée d'attente des mises à jour automatiques avant de continuer avec un redémarrage planifié.

> **Notes**
>
> Cette stratégie s'applique uniquement lorsque les mises à jour automatiques sont configurées pour effectuer des installations planifiées des mises à jour. Si le paramètre de stratégie **Configurer les mises à jour automatiques** est **Désactivé**, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Une fois les mises à jour installées, le temps d'attente par défaut de 15 minutes s'écoule avant tout redémarrage planifié. |
| **Enabled** | Une fois l'installation terminée, un redémarrage planifié se produit après l'expiration du nombre spécifié de minutes. |
| **Disabled** | Une fois les mises à jour installées, le temps d'attente par défaut de 15 minutes s'écoule avant tout redémarrage planifié. |

**Options:** Si ce paramètre est activé, vous pouvez spécifier la durée en minutes pendant laquelle les mises à jour automatiques attendent avant de continuer avec un redémarrage planifié.

## Ne pas définir l'option par défaut sur « Installer les mises à jour et éteindre » dans la boîte de dialogue Arrêt de Windows

Vous pouvez utiliser ce paramètre pour spécifier si l'option **Installer les mises à jour et arrêter** est autorisée comme choix par défaut dans la boîte de dialogue **Arrêter Windows** .

> ⓘ Notes
>
> Ce paramètre de stratégie n'a aucun effet si l'option« **Installer les mises à jour**> et arrêter » des**modèles d'administration des stratégies**>> deconfiguration >>**d'ordinateur**de nom>> de stratégie windows ne s'affiche pas dans le <paramètre de stratégie Arrêter Windows.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| Non configuré | **Installer les mises à jour et arrêter** est l'option par défaut dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles pour l'installation au moment où l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. |
| Enabled | Le dernier choix d'arrêt de l'utilisateur est l'option par défaut dans la boîte de dialogue **Arrêter Windows** . Parmi les exemples de choix d'arrêt, citons **Hibernate** et **Restart**. Ce comportement se produit indépendamment de la disponibilité de l'option **Installer les mises à jour et arrêter** dans cette boîte de dialogue sous **Que souhaitez-vous que l'ordinateur fasse ?**. |
| Disabled | **Installer les mises à jour et arrêter** est l'option par défaut dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles pour l'installation au moment où l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Ne pas se connecter à des emplacements Internet Windows Update

Vous pouvez utiliser ce paramètre pour spécifier que Windows ne doit plus se connecter aux services de mise à jour publique. Même lorsque Windows Update est configuré pour recevoir des mises à jour d'un service de mise à jour Intranet, il récupère régulièrement les informations du service Windows Update public. Cette information permet des connexions futures à Windows Update et à d'autres services, tels que Microsoft Update ou Microsoft Store.

> ⓘ Notes
>
> Cette stratégie s'applique uniquement quand cet ordinateur est configuré pour se connecter à un service de mise à jour Intranet à l'aide du paramètre de stratégie **Spécifier l'emplacement Intranet du service de mise à jour Microsoft**.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Les ordinateurs peuvent récupérer des informations à partir de services de mise à jour publics tels que Windows Update et Microsoft Store. |
| **Enabled** | Windows ne se connecte plus aux services de mise à jour publique tels que Windows Update ou Microsoft Store. Ce paramètre entraîne l'arrêt du fonctionnement de la plupart des fonctionnalités de l'application Microsoft Store.<br><br>Les utilisateurs qui recherchent des mises à jour à l'aide de l'application Paramètres ou du Panneau de configuration voient uniquement les mises à jour du service de mise à jour intranet. Ils ne se voient pas proposer l'option **Vérifier en ligne pour les mises à jour de Windows Update**.<br><br>Les programmes qui utilisent les API de l'Agent Windows Update ne peuvent pas rechercher de mises à jour à partir d'un service autre que le service de mise à jour intranet. |
| **Disabled** | Les ordinateurs peuvent récupérer des informations à partir des services de mise à jour publique. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Ne pas afficher l'option « Installer les mises à jour et éteindre » dans la boîte de dialogue Arrêt de Windows

Vous pouvez utiliser ce paramètre pour spécifier si l'option **Installer les mises à jour et arrêter** s'affiche dans la boîte de dialogue **Arrêter Windows** .

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | L'option **Installer les mises à jour et arrêter** est disponible dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles lorsque l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. Un administrateur local peut modifier ce paramètre à l'aide d'une stratégie locale. |
| **Enabled** | **Installer les mises à jour et arrêter** ne figure pas comme un choix dans la boîte de dialogue **Arrêter Windows**, même si des mises à jour sont disponibles pour installation lorsque l'utilisateur sélectionne l'option **Arrêter** pour éteindre l'ordinateur. |

| État du paramètre de stratégie | Behavior |
| --- | --- |
| **Disabled** | L'option **Installer les mises à jour et arrêter** est l'option par défaut dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles pour l'installation lorsque l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Activer le ciblage côté client

Vous pouvez utiliser ce paramètre pour spécifier le nom ou les noms du groupe cible configurés dans la console WSUS qui reçoit les mises à jour de WSUS.

> ⓘ Notes
>
> Cette stratégie s'applique uniquement quand cet ordinateur est configuré pour prendre en charge les noms de groupes cibles spécifiés dans WSUS. Si le nom du groupe cible n'existe pas dans WSUS, il est ignoré jusqu'à sa création. Si le paramètre de stratégie **Spécifier l'emplacement Intranet du service de mise à jour Microsoft** est désactivé ou n'est pas configuré, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
| --- | --- |
| **Non configuré** | Aucune information de groupe cible n'est envoyée à WSUS. Un administrateur local peut modifier ce paramètre à l'aide d'une stratégie locale. |
| **Enabled** | Les informations de groupe cible spécifiées sont envoyées à WSUS, qui l'utilise pour déterminer quelles mises à jour doivent être déployées sur cet ordinateur. Si WSUS prend en charge plusieurs groupes cibles, vous pouvez utiliser cette stratégie pour spécifier plusieurs noms de groupes, séparés par des points-virgules, si vous ajoutez les noms de groupe cible dans la liste des groupes d'ordinateurs dans WSUS. Dans le cas contraire, vous devez spécifier un seul groupe. |
| **Disabled** | Aucune information de groupe cible n'est envoyée à WSUS. |

**Options:** Utilisez cet espace pour spécifier un ou plusieurs noms de groupes cibles.

## Activation de Windows Update Power Management pour réveiller automatiquement l'ordinateur pour installer des mises à jour planifiées

Vous pouvez utiliser ce paramètre pour spécifier si Windows Update utilise les fonctionnalités Windows Power Management ou Power Options pour réveiller automatiquement l'ordinateur à partir de la veille prolongée si les mises à jour sont planifiées pour l'installation.

L'ordinateur se réveille automatiquement uniquement si Windows Update est configuré pour installer automatiquement les mises à jour. Si l'ordinateur est en veille prolongée lorsque l'heure d'installation planifiée se produit et qu'il existe des mises à jour à appliquer, Windows Update utilise les fonctionnalités Windows Power Management ou Power Options pour réveiller automatiquement l'ordinateur pour installer les mises à jour. Windows Update réveille également l'ordinateur et installe une mise à jour si une échéance d'installation se produit.

L'ordinateur ne se réveille pas, sauf s'il existe des mises à jour à installer. Si l'ordinateur est sur batterie, il n'installe pas les mises à jour lorsque Windows Update le réveille. L'ordinateur reprend automatiquement la mise en veille prolongée en deux minutes.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Windows Update ne met pas l'ordinateur en veille prolongée pour installer les mises à jour. Un administrateur local peut modifier ce paramètre à l'aide d'une stratégie locale. |
| **Enabled** | Windows Update met l'ordinateur en veille prolongée pour installer les mises à jour dans les conditions répertoriées précédemment. |
| **Disabled** | Windows Update ne met pas l'ordinateur en veille prolongée pour installer les mises à jour. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées de mises à jour automatiques

Vous pouvez utiliser ce paramètre pour spécifier que pour terminer une installation planifiée, les mises à jour automatiques attendent que tout utilisateur connecté pour redémarrer l'ordinateur, au lieu de provoquer le redémarrage automatique de l'ordinateur.

> ⓘ Notes

Cette stratégie s'applique uniquement lorsque les mises à jour automatiques sont configurées pour effectuer des installations planifiées des mises à jour. Si le paramètre de stratégie **Configurer les mises à jour automatiques** est **Désactivé**, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Les mises à jour automatiques informent l'utilisateur du redémarrage automatique de l'ordinateur en cinq minutes pour terminer l'installation. |
| **Enabled** | Les mises à jour automatiques ne redémarrent pas automatiquement un ordinateur pendant une installation planifiée si un utilisateur est connecté à l'ordinateur. Au lieu de cela, si les mises à jour ne peuvent pas prendre effet tant que l'ordinateur n'est pas redémarré, les mises à jour automatiques informent l'utilisateur de redémarrer l'ordinateur. |
| **Disabled** | Les mises à jour automatiques informent l'utilisateur du redémarrage automatique de l'ordinateur en cinq minutes pour terminer l'installation. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Redemander un redémarrage avec les installations planifiées

Vous pouvez utiliser ce paramètre pour spécifier la durée d'attente des mises à jour automatiques avant d'inviter à nouveau un redémarrage planifié.

**Important**

Cette stratégie s'applique uniquement lorsque les mises à jour automatiques sont configurées pour effectuer des installations planifiées des mises à jour. Si le paramètre de stratégie **Configurer les mises à jour automatiques** est **Désactivé**, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Un redémarrage planifié se produit 10 minutes après que le message de demande de redémarrage a été ignoré. Un administrateur local peut modifier ce paramètre à |

| État du paramètre de stratégie | Behavior |
| --- | --- |
| | l'aide d'une stratégie locale. |
| **Enabled** | Une fois qu'une invite de redémarrage est reportée, un redémarrage planifié se produit après le nombre de minutes spécifié. |
| **Disabled** | Un redémarrage planifié se produit 10 minutes après que le message de demande de redémarrage a été ignoré. |

**Options:** Lorsque ce paramètre est activé, vous pouvez spécifier la durée en minutes qui s'écoule avant que les utilisateurs ne soient invités à nouveau à propos d'un redémarrage planifié.

## Replanifier les installations planifiées des mises à jour automatiques

Vous pouvez utiliser ce paramètre pour spécifier la durée d'attente des mises à jour automatiques après le démarrage d'un ordinateur avant de poursuivre une installation planifiée qui a été manquée précédemment.

> ⓘ **Notes**
>
> Cette stratégie s'applique uniquement lorsque les mises à jour automatiques sont configurées pour effectuer des installations planifiées des mises à jour. Si le paramètre de stratégie **Configurer les mises à jour automatiques** est **Désactivé**, cette stratégie est sans effet.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
| --- | --- |
| **Non configuré** | Une installation planifiée manquée se produit une minute après le démarrage suivant de l'ordinateur. |
| **Enabled** | Une installation planifiée manquée se produit le nombre spécifié de minutes après le démarrage suivant de l'ordinateur. |
| **Disabled** | Une installation planifiée manquée se produit avec l'installation planifiée suivante. |

**Options:** Lorsque ce paramètre de stratégie est activé, vous pouvez spécifier le nombre de minutes à attendre après le démarrage suivant de l'ordinateur avant qu'une installation planifiée manquée se produise.

## Spécifier l'emplacement Intranet du service de mise à jour Microsoft

Vous pouvez utiliser ce paramètre pour spécifier un serveur intranet pour héberger des mises à jour à partir de Microsoft Update. Lorsque vous spécifiez un serveur, vous pouvez utiliser WSUS pour mettre à jour automatiquement les ordinateurs sur votre réseau.

Vous pouvez utiliser ce paramètre pour spécifier un serveur WSUS sur votre réseau qui fonctionne comme un service de mise à jour interne. Au lieu d'utiliser les services Windows Update et Microsoft Update publics disponibles sur Internet, les clients WSUS recherchent les mises à jour applicables dans ce service. Activer ce paramètre signifie que les utilisateurs de votre organisation ne doivent pas passer par un pare-feu pour obtenir des mises à jour. Cela vous donne également l'opportunité de tester les mises à jour avant de les déployer.

Pour utiliser ce service, vous devez définir les valeurs de noms de deux serveurs : celui à partir duquel le client détecte et télécharge les mises à jour, et celui vers lequel les stations de travail mises à jour chargent les statistiques. Les valeurs ne doivent pas nécessairement être différentes si les deux services sont configurés sur le même serveur.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Les clients se connectent directement au site web Windows Update. |
| **Enabled** | Les clients se connectent au serveur WSUS spécifié, au lieu de Windows Update, pour rechercher et télécharger des mises à jour. Si les mises à jour automatiques ne sont pas désactivées par stratégie ou par préférence utilisateur, les mises à jour automatiques recherchent, téléchargent et installent les mises à jour à partir du serveur WSUS spécifié, au lieu de Windows Update.<br><br>Dans la page **Paramètres de Windows Update** ou la page **Windows Update** du Panneau de configuration dans les anciennes versions de Windows, les utilisateurs voient généralement les mises à jour du serveur WSUS spécifié, et non celles de Windows Update. Les utilisateurs voient également une option **Vérifier en ligne les mises à jour via Windows Update**, qui leur permet d'accéder aux services de mise à jour publique sur Internet. Vous pouvez supprimer cette option à l'aide du paramètre **Ne pas se connecter à des emplacements Internet de mise à jour Windows**.<br><br>Les applications qui utilisent les API de l'agent Windows Update pour rechercher, télécharger et installer des mises à jour fonctionnent normalement sur le serveur WSUS spécifié. Les applications peuvent demander spécifiquement d'utiliser les services de mise à jour publics sur Internet. Vous pouvez supprimer cette option à l'aide du paramètre **Ne pas se connecter à des emplacements Internet de mise à jour Windows**. |

| État du paramètre de stratégie | Behavior |
| --- | --- |
| **Disabled** | Les clients se connectent directement au site web Windows Update. |

**Options:** Lorsque ce paramètre de stratégie est activé, vous devez spécifier le service de mise à jour intranet que les clients WSUS utilisent lors de la détection des mises à jour et du serveur de statistiques Internet vers lequel les clients WSUS mis à jour chargent des statistiques. Le tableau suivant fournit des exemples de valeurs :

Agrandir le tableau

| Option de définition | Valeur d'exemple |
| --- | --- |
| Configurer le service intranet de mise à jour pour la détection des mises à jour | `https://wsus01:8531` |
| Configurer le serveur intranet de statistiques | `https://IntranetUpd01` |

## Activer les mises à jour recommandées par la fonctionnalité Mises à jour automatiques

Vous pouvez utiliser ce paramètre pour spécifier si les mises à jour automatiques fournissent des mises à jour importantes et recommandées à partir de WSUS.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
| --- | --- |
| **Non configuré** | Les mises à jour automatiques continuent de fournir des mises à jour importantes si elles sont déjà configurées pour le faire. |
| **Enabled** | Les mises à jour automatiques installent les mises à jour recommandées et les mises à jour importantes de WSUS. |
| **Disabled** | Les mises à jour automatiques continuent de fournir des mises à jour importantes si elles sont déjà configurées pour le faire. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Activer les notifications d'applications

Vous pouvez utiliser ce paramètre pour spécifier si les utilisateurs voient des messages de notification améliorés détaillés sur les logiciels proposés à partir du service Microsoft Update.

Les messages de notification améliorés communiquent la valeur et promeuvent l'installation et l'utilisation de logiciels facultatifs. Ce paramètre de stratégie est destiné à des environnements peu gérés dans lesquels vous autorisez l'utilisateur à accéder au service Microsoft Update.

Si vous n'utilisez pas le service Microsoft Update, le paramètre de stratégie **Notifications logicielles** n'a aucun effet.

Si le paramètre de stratégie **Configurer les mises à jour automatiques** est **Désactivé** ou **Non configuré**, le paramètre de stratégie **Notifications d'application** est sans effet.

> ⓘ Notes
>
> Par défaut, ce paramètre de stratégie est désactivé.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Les utilisateurs ne reçoivent pas de messages pour les applications facultatives. Un administrateur local peut modifier ce paramètre à l'aide du Panneau de configuration ou d'une stratégie locale. |
| **Enabled** | Un message de notification s'affiche sur l'ordinateur de l'utilisateur lorsque le logiciel proposé est disponible. L'utilisateur peut sélectionner la notification pour ouvrir Windows Update et obtenir des informations supplémentaires sur le logiciel ou l'installer. L'utilisateur peut également sélectionner **Fermer ce message** ou **Afficher ultérieurement** pour différer la notification. |
| **Disabled** | Les utilisateurs ne sont pas proposés de messages de notification détaillés pour les applications ou mises à jour facultatives. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Configuration ordinateur > Paramètres du Planificateur de maintenance

Dans le paramètre **Configurer les mises à jour automatiques** , si vous sélectionnez l'option **4 - Téléchargement automatique et planification de l'installation** , vous pouvez spécifier les paramètres du planificateur de maintenance dans la console de gestion des stratégies de groupe (GPMC). Si vous ne sélectionnez pas l'option **4** dans le paramètre **Configurer les mises à jour automatiques** , vous n'avez pas besoin de configurer ces paramètres pour les mises à jour automatiques.

Les paramètres du planificateur de maintenance se trouvent dans le chemin d'accès aux**modèles d'administration des stratégies**> de **configuration**>> ordinateur,**Planificateur de maintenancedes composants**> Windows. L'extension Planificateur de maintenance de la stratégie de groupe contient les paramètres suivants :

- Limite d'activation de maintenance automatique
- Délai aléatoire de maintenance automatique
- Stratégie de sortie de veille automatique

## Limite de l'activation de la maintenance automatique

Vous pouvez utiliser ce paramètre pour configurer la limite d'activation de maintenance automatique.

L'heure de début d'activation est l'heure programmée quotidienne où la maintenance automatique commence.

> **Notes**
>
> Ce paramètre est lié à l'option **4** dans **Configurer les mises à jour automatiques**. Si vous ne sélectionnez pas l'option 4 dans **Configurer les mises à jour automatiques**, vous n'avez pas besoin de configurer ce paramètre.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | L'heure planifiée quotidienne s'applique aux ordinateurs clients dans le Panneau de configuration de la page **Maintenance automatique** . |
| **Enabled** | Tous les paramètres par défaut ou modifiés configurés sur les ordinateurs clients du Panneau de configuration sur la page **Maintenance automatique** (ou dans certaines versions du client, la page **Maintenance** ) sont remplacés. |
| **Disabled** | L'heure planifiée quotidienne s'applique dans le Panneau de configuration sur la page **Maintenance automatique** . |

## Délai aléatoire de maintenance automatique

Vous pouvez utiliser ce paramètre pour configurer le délai aléatoire pour l'activation automatique de la maintenance.

Le délai aléatoire de maintenance est la longueur maximale du délai appliqué à la maintenance automatique, en commençant par sa limite d'activation. Ce paramètre est utile pour les machines virtuelles où une maintenance aléatoire peut être une exigence en matière de performances.

> **Notes**
>
> Ce paramètre est lié à l'option **4** dans **Configurer les mises à jour automatiques**. Si vous ne sélectionnez pas l'option **4** dans **Configurer les mises à jour automatiques**, vous n'avez pas besoin de configurer ce paramètre.

Par défaut, lorsque ce paramètre est activé, le délai aléatoire de maintenance standard est **PT4H**.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Un délai aléatoire de quatre heures est appliqué à la maintenance automatique. |
| **Enabled** | Un délai aléatoire qui dure jusqu'à la durée spécifiée est appliqué à la maintenance automatique. |
| **Disabled** | Aucun délai aléatoire n'est appliqué à la maintenance automatique. |

## Stratégie de sortie de veille automatique

Vous pouvez utiliser ce paramètre pour configurer la stratégie de mise en éveil pour la maintenance automatique.

La stratégie de mise en éveil spécifie si la maintenance automatique effectue une demande de mise en éveil sur l'ordinateur d'exploitation pour une maintenance planifiée quotidienne.

> **Notes**
>
> Si la stratégie de sortie de veille de l'ordinateur d'exploitation est explicitement désactivée, ce paramètre est sans effet. Ce paramètre est lié à l'option **4** dans **Configurer les mises à jour automatiques**. Si vous ne sélectionnez pas l'option **4** dans **Configurer les mises à jour automatiques**, vous n'avez pas besoin de configurer ce paramètre.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| **Non configuré** | Le paramètre de mise en éveil s'applique dans le Panneau de configuration sur la page **Maintenance automatique** . |
| **Enabled** | La maintenance automatique tente de définir une stratégie de mise en éveil du système d'exploitation et d'effectuer une demande de mise en éveil pour l'heure planifiée quotidienne, si nécessaire. |
| **Disabled** | Le paramètre de mise en éveil s'applique dans le Panneau de configuration sur la page **Maintenance automatique** . |

## Configuration utilisateur > Paramètres de stratégie de Windows Update

Cette section fournit des détails sur les paramètres de stratégie basés sur l'utilisateur suivants :

- Ne pas afficher l'option « Installer les mises à jour et arrêter » dans la boîte de dialogue Arrêter Windows
- Ne pas ajuster l'option par défaut à « Installer les mises à jour et arrêter » dans la boîte de dialogue Arrêter Windows
- Supprimer l'accès à l'utilisation de toutes les fonctionnalités de Windows Update

Dans le GPME, les paramètres utilisateur des mises à jour automatiques des ordinateurs se trouvent dans le chemin d'accès <>> des stratégies de**configuration**>> utilisateur**modèles**> d'administration**Windows**>**Update**. Les paramètres sont répertoriés dans le même ordre qu'ils apparaissent dans les extensions Configuration de l'ordinateur et Configuration utilisateur dans la stratégie de groupe, lorsque l'onglet **Paramètres** de la stratégie Windows Update est sélectionné pour trier les paramètres par ordre alphabétique.

> **Notes**
>
> Par défaut, sauf indication contraire, ces paramètres ne sont pas configurés.

Pour chacun de ces paramètres, vous pouvez procéder comme suit pour activer, désactiver ou naviguer entre les paramètres.

### Ne pas afficher l'option « Installer les mises à jour et éteindre » dans la boîte de dialogue Arrêt de Windows

Vous pouvez utiliser ce paramètre pour spécifier si l'option **Installer les mises à jour et arrêter** s'affiche dans la boîte de dialogue **Arrêter Windows** .

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| Non configuré | L'option **Installer les mises à jour et arrêter** s'affiche dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles lorsque l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. |
| Enabled | **Installer les mises à jour et arrêter** ne figure pas comme un choix dans la boîte de dialogue **Arrêter Windows**, même si des mises à jour sont disponibles pour installation lorsque l'utilisateur sélectionne l'option **Arrêter** pour éteindre l'ordinateur. |
| Disabled | L'option **Installer les mises à jour et arrêter** s'affiche dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles lorsque l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Ne pas définir l'option par défaut sur « Installer les mises à jour et éteindre » dans la boîte de dialogue Arrêt de Windows

Vous pouvez utiliser ce paramètre pour spécifier si l'option **Installer les mises à jour et arrêter** est autorisée comme choix par défaut dans la boîte de dialogue **Arrêter Windows** .

> ⓘ Notes
>
> Ce paramètre de stratégie n'a aucun effetsi les <modèles**d'administration**> des stratégies de**configuration**>> utilisateur de nom>>de stratégie**windows composants**> Windows Update**n'affichent pas les mises à jour**> d'installation et l'option Arrêter dans la boîte de dialogue Arrêter Windows est activée.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
|---|---|
| Non configuré | L'option **Installer les mises à jour et arrêter** est l'option par défaut dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles pour l'installation lorsque |

| État du paramètre de stratégie | Behavior |
| --- | --- |
| | l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. |
| **Enabled** | Le dernier choix d'arrêt de l'utilisateur est l'option par défaut dans la boîte de dialogue **Arrêter Windows** . Parmi les exemples de choix d'arrêt, citons **Hibernate** et **Restart**. Ce comportement se produit indépendamment de la disponibilité de l'option **Installer les mises à jour et arrêter** dans cette boîte de dialogue sous **Que souhaitez-vous que l'ordinateur fasse ?**. |
| **Disabled** | L'option **Installer les mises à jour et arrêter** est l'option par défaut dans la boîte de dialogue **Arrêter Windows** si les mises à jour sont disponibles pour l'installation lorsque l'utilisateur sélectionne l'option **Arrêter** pour arrêter l'ordinateur. |

**Options:** Il n'existe aucune option pour ce paramètre.

## Supprimer l'accès à l'utilisation de toutes les fonctionnalités Windows Update

Vous pouvez utiliser ce paramètre pour supprimer l'accès du client WSUS à Windows Update.

> ⓘ Notes
>
> Ce paramètre n'est pas pris en charge sur Windows 10 et versions ultérieures, et Windows Server 2016 et versions ultérieures.

Agrandir le tableau

| État du paramètre de stratégie | Behavior |
| --- | --- |
| **Non configuré** | Les utilisateurs peuvent se connecter au site web Windows Update. |
| **Enabled** | Toutes les fonctionnalités de Windows Update sont supprimées. L'accès est bloqué sur le site web Windows Update.<br><br>Les mises à jour automatiques Windows sont également désactivées. L'utilisateur n'est pas informé des mises à jour critiques et ne reçoit pas de mises à jour critiques de Windows Update. Vous pouvez configurer l'une des options de notification répertoriées après ce tableau. Ce paramètre de stratégie empêche également le Gestionnaire de périphériques d'installer automatiquement les mises à jour des pilotes à partir du site web Windows Update. |

| État du paramètre de stratégie | Behavior |
|---|---|
| **Disabled** | Les utilisateurs peuvent se connecter au site web Windows Update. |

**Options:** Si ce paramètre est activé, vous pouvez sélectionner l'une des options suivantes :

Agrandir le tableau

| Option | Behavior |
|---|---|
| **0 - Ne pas afficher de notifications** | Tous les accès aux fonctionnalités de Windows Update sont supprimés et aucune notification n'est affichée. |
| **1 - Afficher des notifications de redémarrage requis** | Les notifications sur les redémarrages requis pour terminer une installation sont affichées. |

# Informations supplémentaires

Cette section fournit plus d'informations sur l'utilisation, l'ouverture et l'enregistrement des paramètres WSUS dans la stratégie de groupe. Cette section fournit également des définitions pour les termes utilisés dans cet article. Pour les administrateurs connaissant les versions précédentes de WSUS (WSUS 3.2 et versions antérieures), il existe un tableau qui résume les différences entre les versions de WSUS.

## Accès aux paramètres de Windows Update dans Stratégie de groupe

Les procédures suivantes décrivent comment utiliser des objets de stratégie de groupe (GPO) et d'autres paramètres de stratégie de groupe.

> ⓘ **Notes**
>
> Pour effectuer ces procédures, vous devez être membre du groupe **Administrateurs du domaine** ou de son équivalent.

### Pour ouvrir un objet de stratégie de groupe

1. Sur votre contrôleur de domaine, accédez à**Gestion des stratégies de groupe desoutils**>**du Gestionnaire de serveur**>. GPMC s'ouvre.

2. Dans le volet latéral, développez votre forêt. Par exemple, double-cliquez sur **Forêt : example.com**.

3. Dans le volet latéral, double-cliquez sur **Domaines**, puis double-cliquez sur le domaine pour lequel vous souhaitez gérer un objet de stratégie de groupe. Par exemple, double-cliquez sur **example.com**.

4. Exécutez l'une des étapes suivantes :

   - Pour ouvrir un objet GPO existant au niveau du domaine afin de la modifier :
     a. Double-cliquez sur le domaine contenant l'objet de stratégie de groupe que vous souhaitez gérer.
     b. Cliquez avec le bouton droit sur la stratégie de domaine que vous souhaitez gérer, puis sélectionnez **Modifier**. Le GPME ouvre ses portes.

   - Pour créer un nouvel objet de stratégie de groupe et l'ouvrir afin de le modifier :
     a. Cliquez avec le bouton droit sur le domaine pour lequel vous souhaitez créer un objet de stratégie de groupe, puis sélectionnez Créer un objet de stratégie de groupe **dans ce domaine, puis liez-le ici**.
     b. Dans la boîte de dialogue **Nouvel objet** de stratégie de groupe, sous **Nom**, entrez un nom pour le nouvel objet de stratégie de groupe, puis sélectionnez **OK**.
     c. Cliquez avec le bouton droit sur votre nouvel objet de stratégie de groupe, puis sélectionnez **Modifier**. Le GPME ouvre ses portes.

## Pour ouvrir l'extension Windows Update ou Planificateur de maintenance de la stratégie de groupe

Dans le GPME, effectuez l'une des étapes suivantes :

- Développez**les modèles**>**d'administration**des stratégies >**de configuration**> ordinateur**Windows Components**>**Windows Update**.

- Développez les**stratégies**>**de configuration**> utilisateur**modèles**> d'administration**Windows Components**>**Windows Update**.

- Développez les**stratégies**>**de configuration**> ordinateur**modèles**> d'administration**Planificateur de maintenance des composants**> Windows.

Pour plus d'informations sur la stratégie de groupe, consultez Vue d'ensemble de la stratégie de groupe.

## Pour configurer les paramètres de stratégie de groupe

Après avoir ouvert l'extension de la stratégie de groupe souhaitée, vous pouvez utiliser les étapes suivantes pour activer, désactiver ou passer d'un paramètre à l'autre :

1. Double-cliquez sur le paramètre que vous souhaitez afficher ou modifier.
2. Exécutez l'une des étapes suivantes :
    - Pour conserver l'état non spécifié par défaut du paramètre, sélectionnez **Non configuré**.
    - Pour activer le paramètre, sélectionnez **Activé**.
    - Pour désactiver le paramètre, sélectionnez **Désactivé**.
3. Dans **Options**, si des options sont répertoriées, conservez les valeurs par défaut ou modifiez-les si nécessaire.
4. Exécutez l'une des étapes suivantes :
    - Pour enregistrer vos modifications et passer au paramètre suivant, sélectionnez **Appliquer**, puis sélectionnez **Paramètre suivant**.
    - Pour enregistrer vos modifications et fermer la boîte de dialogue, sélectionnez **OK**.
    - Pour ignorer toutes les modifications non enregistrées et fermer la boîte de dialogue, sélectionnez **Annuler**.

## Termes et définitions

Cet article utilise les termes suivants :

Agrandir le tableau

| Term | Definition |
|---|---|
| Mises à jour automatiques ou mises à jour automatiques | Planification et téléchargement automatiques des mises à jour par l'agent Windows Update. Les mises à jour automatiques sont le composant ordinateur client intégré aux systèmes d'exploitation Windows et Windows Server pour obtenir des mises à jour à partir de Microsoft Update ou de Windows Update. |
| Serveur autonome | Un serveur WSUS en aval sur lequel les administrateurs peuvent gérer les composants WSUS. |
| Serveur en aval | Un serveur WSUS qui obtient des mises à jour à partir d'un autre serveur WSUS plutôt qu'à partir de Microsoft Update ou Windows Update. |
| Extension de la stratégie de groupe ou extension de la stratégie de groupe | Une collection de paramètres dans la stratégie de groupe qui contrôle la manière dont les utilisateurs et les ordinateurs auxquels les stratégies s'appliquent peuvent configurer et utiliser différents services et fonctionnalités Windows. Les administrateurs peuvent utiliser WSUS avec la stratégie de groupe pour la configuration côté client du client Mises à jour automatiques, afin de s'assurer que |

| Term | Definition |
| --- | --- |
| | les utilisateurs ne puissent pas désactiver ou contourner les stratégies de mise à jour d'entreprise.<br><br>WSUS ne nécessite pas l'utilisation d'Active Directory ou de la stratégie de groupe. La configuration client peut également être appliquée à l'aide d'une stratégie de groupe locale ou en modifiant le registre Windows. |
| Service de mise à jour interne | Référence informelle à une infrastructure réseau qui utilise un ou plusieurs serveurs WSUS pour distribuer des mises à jour. |
| Serveur réplica | Un serveur WSUS en aval qui reflète les approbations et les paramètres sur le serveur en amont auquel il est connecté. Vous ne pouvez pas gérer WSUS sur un serveur réplica. |
| Microsoft Update | Un site Internet Microsoft qui stocke et distribue des mises à jour pour des ordinateurs Windows, des pilotes de périphérique, des systèmes d'exploitation Windows et d'autres produits logiciels Microsoft. |
| Software Update Services (SUS) | Le produit prédécesseur de WSUS. |
| Updates | Une collection de révisions logicielles, de correctifs à chaud, de service packs, de packs de fonctionnalités et de pilotes de périphériques qui peuvent être installés sur un ordinateur pour étendre les fonctionnalités ou améliorer les performances et la sécurité. |
| Mettre à jour des fichiers | Fichiers requis pour installer une mise à jour sur un ordinateur. |
| Mettre à jour les informations ou mettre à jour les métadonnées | Les informations relatives à une mise à jour, par opposition aux fichiers binaires dans un package de mise à jour. Par exemple, les métadonnées fournissent des informations sur les propriétés d'une mise à jour afin de savoir ce que la mise à jour est utile. Les métadonnées incluent également les Termes du contrat de licence logiciel Microsoft. Le package de métadonnées téléchargé pour une mise à jour est généralement plus petit que le package du fichier de mise à jour. |
| Mettre à jour la source | L'emplacement sur lequel un serveur WSUS se synchronise pour obtenir des fichiers de mise à jour. Cet emplacement peut être Microsoft Update ou un serveur WSUS en amont. |
| Serveur en amont | Un serveur WSUS qui fournit des fichiers de mise à jour à un autre serveur WSUS en aval. |
| Windows Server Update Services (WSUS) | Un programme de rôle serveur qui s'exécute sur un ou plusieurs ordinateurs Windows Server dans un réseau d'entreprise. Une infrastructure WSUS vous permet de gérer les mises à jour des ordinateurs sur votre réseau à installer.<br><br>Vous pouvez utiliser WSUS pour approuver ou décliner des mises à jour avant publication, pour forcer l'installation de mises à jour à une date précise et pour obtenir des rapports détaillés sur les mises à jour requises pour chaque ordinateur |

| Term | Definition |
| --- | --- |
| | de votre réseau. Vous pouvez configurer WSUS pour approuver automatiquement certaines classes de mises à jour, notamment, des mises à jour critiques, des mises à jour de sécurité, des packs de service et des pilotes. Vous pouvez également utiliser WSUS pour approuver les mises à jour pour la détection uniquement, afin de voir quels ordinateurs nécessitent une mise à jour particulière sans avoir à installer la mise à jour.<br><br>Dans une implémentation WSUS, au moins un serveur WSUS du réseau doit pouvoir se connecter à Microsoft Update pour obtenir les mises à jour disponibles. En fonction de la configuration et de la sécurité du réseau, l'administrateur peut déterminer le nombre d'autres serveurs se connectant directement à Microsoft Update.<br><br>Vous pouvez configurer un serveur WSUS pour obtenir des mises à jour sur Internet à partir de Microsoft Update, de Windows Update ou du Microsoft Store. |
| Mise à jour de Windows | Un site Internet Microsoft qui stocke et distribue des mises à jour pour ordinateurs Windows, des pilotes de périphériques et des systèmes d'exploitation Windows. Windows Update est également le nom d'un service qui s'exécute sur les ordinateurs Windows et détecte, télécharge et installe les mises à jour.<br><br>En fonction des configurations de l'ordinateur et de la stratégie, l'agent Windows Update peut télécharger des mises à jour à partir des emplacements suivants :<br><br>- Microsoft Update.<br><br>- Windows Update.<br><br>- Microsoft Store.<br><br>- Service de mise à jour Internet (réseau) (WSUS).<br><br>Les ordinateurs non gérés dans un environnement basé sur WSUS utilisent généralement Windows Update pour se connecter directement via Internet à Windows Update, Microsoft Update ou Microsoft Store afin d'obtenir des mises à jour. |
| Client WSUS | Ordinateur qui reçoit des mises à jour d'un service de mise à jour intranet WSUS. Si les paramètres de stratégie de groupe contrôlent l'interaction utilisateur avec les mises à jour automatiques, un client WSUS est un utilisateur d'un ordinateur dans un environnement WSUS. |

# Gestion des mises à jour avec les services WSUS (Windows Server Update Services)

15/08/2025

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

Vous devez vérifier la page d'accueil de la console d'administration WSUS régulièrement pour connaître la conformité globale des mises à jour et l'intégrité du réseau. Vérifiez fréquemment les journaux des applications si vous soupçonnez des problèmes tels que des échecs de téléchargement ou des ordinateurs clients qui échouent à envoyer des informations au serveur WSUS. Ce guide fournit des informations qui vous aident à gérer Windows Server Update Services.

## Contenu de ce guide

Dans ce guide, vous trouverez des informations sur :

- Configuration des synchronisations de mise à jour
- Gestion des ordinateurs clients WSUS et des groupes d'ordinateurs WSUS
- Affichage et gestion des mises à jour
- WSUS et le Site du catalogue
- Opérations de mise à jour
- Assistant de nettoyage du serveur
- Mode de réplica WSUS en cours d'exécution
- Conseils de dépannage et messages WSUS

# Configuration des synchronisations de mise à jour

16/08/2025

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

Lors de la synchronisation, un serveur WSUS télécharge les mises à jour (métadonnées et fichiers de mise à jour) depuis une source de mise à jour. Il télécharge également les nouvelles classifications et catégories de produits, le cas échéant. Lors de la première synchronisation du serveur WSUS, celui-ci télécharge toutes les mises à jour que vous avez spécifiées quand vous avez configuré des options de synchronisation. Après la première synchronisation, votre serveur WSUS télécharge uniquement les mises à jour à partir de la source de mise à jour,ainsi que les révisions dans les métadonnées pour les mises à jour existantes et les expirations des mises à jour.

Le premier téléchargement des mises à jour par un serveur WSUS peut prendre beaucoup de temps. Si vous configurez plusieurs serveurs WSUS, vous pouvez accélérer le processus dans une certaine mesure en téléchargeant toutes les mises à jour sur un serveur WSUS, puis en copiant les mises à jour dans les répertoires de contenu des autres serveurs WSUS.

Vous pouvez copier du contenu d'un répertoire de contenu d'un serveur WSUS vers un autre. L'emplacement du répertoire de contenu est spécifié quand vous exécutez la procédure de post-installation WSUS. Vous pouvez utiliser l'outil wsusutil.exe pour exporter les métadonnées de mise à jour d'un serveur WSUS vers un fichier. Vous pouvez ensuite importer ce fichier vers d'autres serveurs WSUS.

# Configuration des synchronisations de mise à jour

La page **Options** est le point d'accès central dans la console d'administration WSUS pour personnaliser la façon dont votre serveur WSUS synchronise les mises à jour. Vous pouvez spécifier les mises à jour qui sont synchronisées automatiquement, où votre serveur obtient les mises à jour, les paramètres de connexion et la planification de la synchronisation. Vous pouvez également utiliser l'Assistant Configuration à partir de la page **Options** pour configurer ou reconfigurer votre serveur WSUS à tout moment.

## Synchronisation de la mise à jour par produit et classification

Un serveur WSUS télécharge les mises à jour en fonction des produits ou des familles de produits (par exemple, Windows ou Windows Server 2008, Datacenter Edition) et des

classifications (par exemple, mises à jour critiques ou mises à jour de sécurité) que vous spécifiez. Lors de la première synchronisation, le serveur WSUS télécharge toutes les mises à jour disponibles dans les catégories que vous avez spécifiées. Au cours des synchronisations suivantes, votre serveur WSUS télécharge uniquement les dernières mises à jour (ou les modifications apportées aux mises à jour déjà disponibles sur votre serveur WSUS) pour les catégories que vous avez spécifiées.

Vous pouvez spécifier des produits et des classifications de mise à jour dans la page **Options** sous **Produits et Classifications**. Les produits sont listés dans une hiérarchie, regroupés par famille de produits. Si vous sélectionnez Windows, vous sélectionnez automatiquement chaque produit qui appartient à cette hiérarchie de produits. En cochant la case parente, vous sélectionnez tous les éléments sous celle-ci, ainsi que toutes les versions futures. Le fait de cocher les cases enfants n'entraîne pas la sélection des cases parents. La sélection par défaut pour les produits est tous les produits Windows, tandis que ceux sont les mises à jour critiques et de sécurité qui sont sélectionnées par défaut pour les classifications.

Si un serveur WSUS s'exécute en mode Réplica, vous ne pouvez pas effectuer cette tâche. Pour plus d'informations sur le mode Réplica, consultez Mode Réplica pour l'exécution du serveur WSUS et Étape 1 : Préparer votre déploiement WSUS.

### Pour spécifier les produits et classifications de mise à jour pour la synchronisation

1. Dans la console d'administration WSUS, cliquez sur le nœud **Options** .
2. Cliquez sur **Produits et classifications**, puis cliquez sur l'onglet **Produits**.
3. Cochez les cases des produits ou des familles de produits que vous souhaitez mettre à jour avec WSUS, puis cliquez sur **OK**.
4. Sous l'onglet Classifications, cochez les cases des **classifications** de mise à jour que votre serveur WSUS doit synchroniser, puis cliquez sur **OK**.

> **Notes**
>
> Vous pouvez supprimer des produits ou des classifications de la même façon. Votre serveur WSUS cesse alors de synchroniser les nouvelles mises à jour pour les produits que vous avez retirés. Toutefois, les mises à jour qui ont été synchronisées pour ces produits avant leur retrait restent sur votre serveur WSUS et sont listées comme disponibles.
>
> Pour supprimer ces produits, refusez la mise à jour, comme indiqué dans Les opérations de mise à jour, puis utilisez l'Assistant Nettoyage du serveur pour les supprimer.

## Synchronisation des mises à jour par langue

Votre serveur WSUS télécharge les mises à jour en fonction des langues que vous spécifiez. Vous pouvez synchroniser les mises à jour dans toutes les langues dans lesquelles elles sont disponibles, ou vous pouvez spécifier un sous-ensemble de langues. Si vous avez une hiérarchie de serveurs WSUS et que vous devez télécharger les mises à jour dans différentes langues, assurez-vous que vous avez spécifié toutes les langues nécessaires sur le serveur en amont. Sur un serveur en aval, vous pouvez spécifier un sous-ensemble des langues que vous avez spécifiées sur le serveur en amont.

## Synchronisation des mises à jour à partir du Catalogue Microsoft Update

Pour plus d'informations sur la synchronisation des mises à jour à partir du site du Catalogue Microsoft Update, consultez : WSUS et le site du Catalogue.

# Configuration des paramètres de serveur proxy

Vous pouvez configurer votre serveur WSUS pour qu'il utilise un serveur proxy pendant la synchronisation avec un serveur en amont ou Microsoft Update. Ce paramétrage s'applique uniquement quand votre serveur WSUS exécute des synchronisations. Par défaut, votre serveur WSUS tente de se connecter directement au serveur en amont ou à Microsoft Update.

### Pour spécifier un serveur proxy pour la synchronisation

1. Dans la console d'administration WSUS, cliquez sur **Options**, puis sur **Mettre à jour la source et le serveur proxy**.

2. Sous l'onglet **Serveur proxy** , activez la case **à cocher Utiliser un serveur proxy lors de la synchronisation** , puis tapez le nom du serveur et le numéro de port du serveur proxy.

   > ⓘ **Notes**
   >
   > Configurez WSUS avec le numéro de port que le serveur proxy est censé utiliser d'après sa configuration.

   - Pour vous connecter au serveur proxy avec des informations d'identification de l'utilisateur spécifiques, cochez la case **Utiliser les informations d'identification de l'utilisateur pour se connecter au serveur proxy**, puis entrez le nom d'utilisateur, le domaine et le mot de passe de l'utilisateur dans les zones correspondantes.

- Pour activer l'authentification de base de l'utilisateur qui se connecte au serveur proxy, cochez la case **Autoriser l'authentification de base (mot de passe envoyé non codé)**.

3. Cliquez sur **OK**.

> ⓘ **Notes**
>
> Étant donné que WSUS lance tout son trafic réseau, il n'est pas nécessaire de configurer le Pare-feu Windows sur un serveur WSUS connecté directement à Microsoft Update.

# Configuration de la source de mise à jour

La source de mise à jour est l'emplacement à partir duquel votre serveur WSUS obtient ses mises à jour et ses métadonnées de mise à jour. Vous pouvez spécifier que la source de mise à jour soit Microsoft Update ou un autre serveur WSUS (le serveur WSUS qui agit en tant que source de mise à jour est le serveur en amont, tandis que votre serveur est le serveur en aval).

Les options de personnalisation de la synchronisation de votre serveur WSUS avec la source de mise à jour sont les suivantes :

- Vous pouvez spécifier un port personnalisé pour la synchronisation. Pour plus d'informations sur la configuration des ports, consultez Étape 3 : Configurer WSUS dans le guide de déploiement WSUS.
- Vous pouvez utiliser SSL (Secure Sockets Layer) pour sécuriser la synchronisation des informations de mise à jour entre les serveurs WSUS. Pour plus d'informations sur l'utilisation du protocole SSL, consultez la section 3.5. Sécuriser WSUS avec le protocole SSL (Secure Sockets Layer) de l'Étape 3 : Configurer WSUS du guide de déploiement WSUS.

# Synchronisation manuelle ou automatique

Vous pouvez synchroniser votre serveur WSUS manuellement ou spécifier une heure pour qu'il se synchronise automatiquement.

## Pour synchroniser manuellement le serveur WSUS

1. Dans la console d'administration WSUS, cliquez sur **Options**, puis sur **Planification de synchronisation**.

2. Cliquez **sur Synchroniser manuellement**, puis sur **OK**.

## Pour configurer une planification de synchronisation automatique

1. Dans la console d'administration WSUS, cliquez sur **Options**, puis sur **Planification de synchronisation**.
2. Cliquez **sur Synchroniser automatiquement**.
3. Pour **la première synchronisation**, sélectionnez l'heure à laquelle vous souhaitez que la synchronisation démarre chaque jour.
4. Pour **Synchronisations par jour**, sélectionnez le nombre de synchronisations que vous souhaitez effectuer chaque jour. Si, par exemple, vous souhaitez quatre synchronisations par jour à compter de 3h00, les synchronisations auront lieu à 3h00, 9h00, 15h00 et 21h00 chaque jour. (Notez qu'un décalage de temps aléatoire est ajouté à l'heure de synchronisation planifiée afin d'espacer les connexions serveur à Microsoft Update.)
5. Cliquez sur **OK**.

## Pour synchroniser immédiatement votre serveur WSUS

1. Dans la Console d'administration WSUS, sélectionnez le nœud de serveur supérieur.
2. Dans le volet **Vue d'ensemble** , sous **État de synchronisation**, cliquez **sur Synchroniser maintenant**.

> ⓘ **Notes**
>
> La synchronisation est lancée par le serveur en aval.

# Gestion des ordinateurs clients WSUS et des groupes d'ordinateurs WSUS

16/08/2025

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

Le nœud Ordinateurs est le point d'accès central dans la console d'administration WSUS pour la gestion des appareils et des ordinateurs clients WSUS. Sous ce nœud, vous trouverez les différents groupes que vous avez configurés (ainsi que le groupe par défaut, Ordinateurs non attribués).

## Gestion des ordinateurs clients

La sélection de l'un des groupes d'ordinateurs dans le nœud **Ordinateurs** entraîne l'affichage des ordinateurs de ce groupe dans le volet d'informations. Si un ordinateur est affecté à plusieurs groupes, il apparaît dans les listes de tous les groupes. Si vous sélectionnez un ordinateur dans la liste, vous pouvez voir ses propriétés, qui incluent des détails généraux sur l'ordinateur et l'état des mises à jour le concernant. Vous pouvez filtrer la liste des ordinateurs sous un groupe d'ordinateurs donné par état. Par défaut, seuls sont affichés les ordinateurs pour lesquels des mises à jour sont nécessaires ou qui ont subi des échecs d'installation ; toutefois, vous pouvez filtrer l'affichage par n'importe quel état. Cliquez sur **Actualiser** après avoir modifié le filtre d'état.

Vous pouvez également gérer les groupes d'ordinateurs sur la page des ordinateurs, par exemple créer les groupes et leur attribuer des ordinateurs. Pour plus d'informations sur la gestion des groupes d'ordinateurs, consultez Gestion des groupes d'ordinateurs dans la section suivante de ce guide et la section 1.5. Planifier les groupes d'ordinateurs WSUS de l'Étape 1 : Préparer votre déploiement WSUS du guide de déploiement WSUS.

> ⓘ **Notes**
>
> Vous devez d'abord configurer les ordinateurs clients pour qu'ils contactent le serveur WSUS avant de pouvoir les gérer à partir de ce serveur. Tant que vous n'effectuez pas cette tâche, votre serveur WSUS ne reconnaît pas vos ordinateurs clients et ces derniers ne s'affichent pas dans la liste sur la page des ordinateurs. Pour plus d'informations sur la configuration des ordinateurs clients, consultez la section 1.5. Planifier les groupes d'ordinateurs WSUS de l'Étape 1 : Préparer votre déploiement WSUS et l'Étape 3 : Configurer WSUS dans le guide de déploiement WSUS.

# Contrôle du moment où les ordinateurs clients WSUS installent les mises à jour

Il existe deux méthodes pour contrôler quand les ordinateurs clients WSUS installent les mises à jour :

- Approbation avec échéances : les échéances imposent de manière stricte à quel moment une mise à jour est installée
- Stratégies de groupe WSUS : les stratégies de groupe contrôlent à quel moment l'agent Windows Update analyse et installe les mises à jour

  Pour plus d'informations, consultez Étape 5 : Configurer les paramètres de stratégie de groupe pour les mises à jour automatiques, dans le guide de déploiement WSUS.

# Gestion des groupes d'ordinateurs

WSUS vous permet de cibler les mises à jour vers des groupes d'ordinateurs clients afin que vous puissiez vous assurer que des ordinateurs spécifiques obtiennent toujours les mises à jour adéquates au moment le plus approprié. Par exemple, si tous les ordinateurs d'un service (tel que l'équipe Comptabilité) ont une configuration spécifique, vous pouvez configurer un groupe pour cette équipe, décider des mises à jour dont leurs ordinateurs ont besoin et l'heure à laquelle elles doivent être installées, puis utiliser les rapports WSUS pour évaluer les mises à jour pour l'équipe.

Les ordinateurs sont toujours affectés au groupe **Tous les ordinateurs** et restent affectés au groupe **d'ordinateurs non attribués** jusqu'à ce que vous les affectiez à un autre groupe. Les ordinateurs peuvent appartenir à plusieurs groupes.

Les groupes d'ordinateurs peuvent être configurés en hiérarchies (par exemple, le groupe Traitement des paies et le groupe Compte fournisseurs sous le groupe Comptabilité). Les mises à jour qui sont approuvées pour un groupe supérieur sont automatiquement déployées sur les groupes inférieurs ainsi que sur le groupe supérieur lui-même. Ainsi, si vous approuvez Update1 pour le groupe Comptabilité, la mise à jour est déployée sur tous les ordinateurs du groupe Comptabilité, tous les ordinateurs du groupe Traitement des paies et tous les ordinateurs du groupe Compte fournisseurs.

Dans la mesure où les ordinateurs peuvent être affectés à plusieurs groupes, il est possible pour une seule mise à jour d'être approuvée plusieurs fois pour le même ordinateur. Toutefois, la mise à jour ne sera déployée qu'une seule fois et tous les conflits seront résolus par le serveur WSUS. Pour poursuivre avec l'exemple ci-dessus, si ComputerA est affecté à la fois au

groupe Traitement des paies et au groupe Compte fournisseurs, et si Update1 est approuvée pour les deux groupes, elle n'est déployée qu'une seule fois.

Vous pouvez affecter les ordinateurs à des groupes d'ordinateurs en adoptant l'une des deux méthodes, à savoir le ciblage côté serveur ou le ciblage côté client. Avec le ciblage côté serveur, vous déplacez manuellement un ou plusieurs ordinateurs clients vers un groupe d'ordinateurs à la fois. Avec le ciblage côté client, vous utilisez la stratégie de groupe ou modifiez les paramètres du Registre sur les ordinateurs clients afin d'activer ces ordinateurs pour qu'ils soient automatiquement ajoutés dans les groupes d'ordinateurs précédemment créés. Ce processus peut faire l'objet d'un script afin d'être déployé sur de nombreux ordinateurs à la fois. Vous devez spécifier la méthode de ciblage que vous utiliserez sur le serveur WSUS en sélectionnant l'une des deux options de la section **Ordinateurs** de la page **Options** .

> ⓘ **Notes**
>
> Si un serveur WSUS est exécuté en mode Réplica, il n'est pas possible de créer des groupes d'ordinateurs sur ce serveur. Tous les groupes d'ordinateurs nécessaires pour les clients du serveur de réplication doivent être créés sur le serveur WSUS qui est la racine de la hiérarchie de serveurs WSUS. Pour plus d'informations sur le mode Réplica, consultez **Mode Réplica pour l'exécution du serveur WSUS** et pour plus d'informations sur le ciblage côté serveur et côté client, consultez la section **1.5. Planifier les groupes d'ordinateurs WSUS** de l'Étape 1 : Préparer votre déploiement WSUS dans le guide de déploiement WSUS.

# Affichage et gestion des mises à jour

16/08/2025

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

Vous pouvez utiliser la console WSUS pour afficher et gérer les mises à jour.

## Affichage des mises à jour

Dans la page **Mises à jour** , vous pouvez effectuer les opérations suivantes :

- Afficher les mises à jour. La vue d'ensemble des mises à jour affiche les mises à jour qui ont été synchronisées à partir de la source de mise à jour vers votre serveur WSUS et qui sont disponibles pour approbation.
- Filtrez les mises à jour. Dans la vue par défaut, vous pouvez filtrer les mises à jour par état d'approbation et état d'installation. Le paramètre par défaut concerne les mises à jour non approuvées dont certains clients ont besoin ou dont l'installation a échoué sur certains clients. Vous pouvez modifier cette vue en modifiant l'état d'approbation et les filtres d'état d'installation, puis en cliquant sur **Actualiser**.
- Créer des vues de mise à jour. Dans le volet **Actions** , sélectionnez **Nouveau mode Mise à jour**. Vous pouvez filtrer les mises à jour par classification, produit, groupe pour lequel elles ont été approuvées et date de synchronisation. Vous pouvez trier la liste en cliquant sur l'en-tête de colonne approprié dans la barre de titre.
- Rechercher des mises à jour. Vous pouvez rechercher une mise à jour individuelle ou un ensemble de mises à jour par titre, description, article de la Base de connaissances ou numéro du Centre de réponse aux problèmes de sécurité Microsoft pour la mise à jour.
- Afficher les détails, l'état et l'historique des révisions pour chaque mise à jour.
- Approuver ou refuser des mises à jour.

### Pour afficher les mises à jour

1. Dans la console d'administration WSUS, développez **Mises à jour**, puis sélectionnez **Toutes les mises à jour**.
2. Par défaut, les mises à jour s'affichent avec leurs titre, classification, pourcentage d'installation ou de non-applicabilité et état d'approbation. Si vous souhaitez afficher des

propriétés de mise à jour supplémentaires ou différentes, cliquez avec le bouton droit sur la barre d'en-tête de colonne et sélectionnez les colonnes appropriées.

3. Pour trier selon différents critères, tels que l'état du téléchargement, le titre, la classification, la date de publication ou l'état d'approbation, sélectionnez l'en-tête de colonne approprié.

## Pour filtrer la liste des mises à jour affichées dans la page Mises à jour

1. Dans la console d'administration WSUS, développez **Mises à jour**, puis sélectionnez **Toutes les mises à jour**.

2. Dans le volet central en regard **de l'approbation**, sélectionnez l'état d'approbation souhaité, puis en regard de **Status** , sélectionnez l'état d'installation souhaité. Sélectionnez **Actualiser**.

## Pour créer une vue de mise à jour sur WSUS

1. Dans la console d'administration WSUS, développez **Mises à jour**, puis sélectionnez **Toutes les mises à jour**.

2. Dans le volet **Actions** , sélectionnez **Nouveau mode Mise à jour**.

3. Dans la fenêtre Ajouter une vue **Mise à jour** , sous **l'étape 1 : Sélectionnez les propriétés**, sélectionnez les propriétés dont vous avez besoin pour filtrer l'affichage de mise à jour :

    - Sélectionnez **Mises à jour dans une classification spécifique** pour filtrer les mises à jour appartenant à une ou plusieurs classifications de mises à jour.

    - Sélectionnez **Mises à jour pour un produit spécifique** à filtrer sur les mises à jour d'un ou de plusieurs produits ou familles de produits.

    - Sélectionnez **Les mises à jour sont approuvées pour un groupe spécifique** pour filtrer les mises à jour approuvées pour un ou plusieurs groupes d'ordinateurs.

    - Sélectionnez **Mises à jour synchronisées dans une période spécifique** pour filtrer les mises à jour synchronisées à un moment spécifique.

    - Sélectionnez **Mises à jour WSUS** pour filtrer les mises à jour WSUS.

4. Sous **l'étape 2 : Modifiez les propriétés**, sélectionnez les mots soulignés pour sélectionner les valeurs souhaitées.

5. Sous **l'étape 3 : spécifiez un nom, donnez** à votre nouvel affichage un nom.

6. Cliquez sur **OK**.

Votre nouvelle vue s'affiche dans l'arborescence sous Mises à jour. Comme les vues standard, elle s'affiche dans le volet central quand vous la sélectionnez.

## Pour rechercher une mise à jour

1. Sélectionnez le nœud **Mises à jour** (ou n'importe quel nœud sous celui-ci).

2. Dans le volet **Actions** , sélectionnez **Rechercher**.

3. Dans la fenêtre **Recherche** , sous l'onglet **Mises à jour** , entrez vos critères de recherche. Vous pouvez utiliser du texte à partir des champs **de** numéro d'article titre, **description** et **base de connaissances Microsoft .** . Chacun de ces éléments est une propriété répertoriée sous l'onglet **Détails** dans les propriétés de mise à jour.

## Pour afficher les propriétés d'une mise à jour

1. Dans la console d'administration WSUS, développez **Mises à jour**, puis sélectionnez **Toutes les mises à jour**.

2. Dans la liste des mises à jour, sélectionnez la mise à jour que vous souhaitez afficher.

3. Dans le volet inférieur, vous verrez les différentes sections de propriété :

    - La barre de titre affiche le titre de la mise à jour ; par exemple, *Mise à jour de sécurité pour le lecteur Windows Media 9 (KB911565)*.

    - La section État affiche l'état d'installation de la mise à jour. Par exemple, les ordinateurs sur lesquels elle a été installée, installation nécessaire ou installée avec des erreurs. La section État affiche également les ordinateurs qui n'ont pas signalé l'état de la mise à jour, qui ne sont pas applicables ainsi que des informations générales (date de publication des numéros de Base de connaissances et du MSRC, etc.).

    - La section Description affiche une brève description de la mise à jour.

    - La section des détails supplémentaires affiche les informations suivantes :

        - Le comportement d'installation de la mise à jour (si elle est amovible ou non, demande un redémarrage, nécessite une entrée utilisateur ou doit être installée exclusivement).

    - Indique si la mise à jour a des termes du contrat de licence logiciel Microsoft
    - Produits auxquels la mise à jour s'applique
    - Mises à jour qui remplacent cette mise à jour
    - Mises à jour remplacées par cette mise à jour
    - Langues prises en charge par la mise à jour
    - ID de mise à jour

Vous ne pouvez effectuer cette procédure que sur une seule mise à jour à la fois. Si vous sélectionnez plusieurs mises à jour, seule la première mise à jour de la liste s'affiche dans le volet **Propriétés** .

# Gestion des mises à jour avec WSUS

Les mises à jour sont utilisées pour mettre à jour des logiciels installés sur un ordinateur ou fournir un remplacement de fichiers complet pour ces derniers. Chaque mise à jour disponible sur Microsoft Update comprend deux composants :

- Métadonnées : fournit des informations sur la mise à jour. Par exemple, les métadonnées fournissent des informations sur les propriétés d'une mise à jour, qui vous permet de savoir l'utilité de la mise à jour. Les métadonnées incluent également les Termes du contrat de licence logiciel Microsoft. Le package de métadonnées téléchargé pour une mise à jour est généralement plus petit que le package des fichiers de mise à jour.
- Fichiers de mise à jour : fichiers réels requis pour installer une mise à jour sur un ordinateur.

Lorsque les mises à jour sont synchronisées sur votre serveur WSUS, les fichiers de mise à jour et les métadonnées sont stockés à deux endroits différents. Les métadonnées sont stockées dans la base de données WSUS. Les fichiers de mise à jour peuvent être stockés soit sur votre serveur WSUS, soit sur des serveurs Microsoft Update, en fonction de la manière dont vous avez configuré vos options de synchronisation. Si vous choisissez d'utiliser des serveurs Microsoft Update comme emplacement de mise à jour, seules les métadonnées sont téléchargées au moment de la synchronisation. Quand vous approuvez les mises à jour via la console WSUS, les ordinateurs clients obtiennent les fichiers de mise à jour directement de Microsoft Update au moment de l'installation. Pour plus d'informations sur les options de stockage des mises à jour, consultez la section 1.3. Choisissez une stratégie de stockage WSUS de l'étape 1 : Préparer votre déploiement WSUS, dans le guide de déploiement WSUS.

Vous allez configurer et exécuter des synchronisations, ajouter des ordinateurs et des groupes d'ordinateurs, et déployer des mises à jour régulièrement. La liste suivante fournit des exemples de tâches générales que vous pouvez entreprendre dans le cadre de la mise à jour d'ordinateurs avec WSUS.

- Déterminer un plan global de gestion des mises à jour en fonction de la topologie et de la bande passante de votre réseau, des besoins de l'entreprise et de la structure organisationnelle.
    - Nécessité ou non de configurer une hiérarchie de serveurs WSUS et structuration de cette hiérarchie.
    - Groupes d'ordinateurs à créer et comment leur attribuer des ordinateurs (ciblage côté serveur ou côté client).
    - Base de données à utiliser pour les métadonnées de mise à jour (par exemple, base de données interne Windows, SQL Server).
    - Nécessité ou non de synchroniser automatiquement les mises à jour et moment auquel la synchronisation doit intervenir.
- Définir les options de synchronisation, telles que la source de mise à jour, la classification des produits et des mises à jour, la langue, les paramètres de connexion, l'emplacement de stockage et la planification de la synchronisation.
- Obtenir les mises à jour et les métadonnées associées sur votre serveur WSUS par le biais de la synchronisation à partir de Microsoft Update ou d'un serveur WSUS en amont.
- Approuver ou refuser des mises à jour. Vous avez la possibilité d'autoriser les utilisateurs à installer les mises à jour eux-mêmes (s'ils sont administrateurs locaux sur leurs ordinateurs clients).
- Configurer les approbations automatiques. Vous pouvez également configurer si vous souhaitez activer l'approbation automatique des révisions des mises à jour existantes ou approuver manuellement les révisions. Si vous choisissez d'approuver manuellement les révisions, votre serveur WSUS continue d'utiliser l'ancienne version jusqu'à ce que vous approuviez manuellement la nouvelle révision.
- Vérifier l'état des mises à jour. Vous pouvez afficher l'état d'une mise à jour, imprimer un rapport d'état ou configurer un e-mail pour les rapports d'état standard.

# Produits et classifications des mises à jour

Les mises à jour disponibles sur Microsoft Update sont différenciées par produit (ou famille de produits) et par classification.

Un produit est une édition spéciale d'un système d'exploitation ou d'une application, par exemple, Windows Server 2012. Une famille de produits est le système de d'exploitation ou l'application de base d'où sont issus les produits individuels. Par exemple, Microsoft Windows est une famille de produits dont Windows Server 2012 fait partie. Vous pouvez sélectionner les produits ou les familles de produits pour lesquels vous souhaitez que votre serveur synchronise les mises à jour. Vous pouvez spécifier une famille de produits ou des produits distincts au sein de la famille. La sélection d'un produit ou d'une famille de produits permet d'obtenir les mises à jour pour les versions actuelles et futures du produit.

Les classifications de mises à jour représentent le type de mise à jour. Pour tout produit ou toute famille de produits, les mises à jour peuvent être disponibles parmi plusieurs classifications de mises à jour (par exemple, Mises à jour critiques pour la famille Windows 7 et Mises à jour de sécurité). Le tableau suivant liste les classifications de mises à jour.

Agrandir le tableau

| Mettre à jour les classifications | Description |
|---|---|
| Mises à jour critiques | Correctifs largement diffusés pour des problèmes spécifiques remédiant à des bogues critiques non liés à la sécurité. |
| Mises à jour de définition | Mises à jour de fichiers de définition de virus ou autre. |
| Ensembles de pilotes | Packages de modules logiciels conçus pour prendre en charge le matériel d'un modèle spécifique d'appareil informatique. |
| Drivers | Composants logiciels conçus pour prendre en charge un nouveau matériel. |
| Packs de fonctionnalités | Nouvelles versions de fonctionnalités, généralement intégrées aux produits à la prochaine version. |
| Hotfix | Package unique composé d'un ou plusieurs fichiers utilisés pour résoudre un problème dans un produit. Correctifs logiciels qui traitent une situation spécifique signalée par un ou plusieurs clients et qui ne sont pas largement disponibles. La classification s'affiche uniquement lorsque vous importez un correctif logiciel à partir du catalogue Microsoft Update.<br><br>Les correctifs logiciels ont été publiés uniquement pour Windows 8.1, Windows Server 2012 R2 et versions antérieures. |
| Mises à jour de sécurité | Correctifs largement diffusés pour des produits spécifiques, remédiant à des problèmes de sécurité. |

| Mettre à jour les classifications | Description |
| --- | --- |
| Service Packs | Ensembles cumulés de tous les correctifs logiciels, mises à jour de sécurité, mises à jour critiques et mises à jour créées depuis la publication du produit. Les Service Packs peuvent également contenir un nombre limité de fonctionnalités ou de modifications de conception demandées par les clients. |
| Tools | Utilitaires ou fonctionnalités qui permettent d'accomplir une tâche ou un ensemble de tâches. |
| Correctifs cumulatifs | Ensemble cumulé de correctifs logiciels, de mises à jour de sécurité, de mises à jour critiques et d'autres mises à jour packagés ensemble de façon à en faciliter le déploiement. Un cumul cible généralement une zone spécifique, telle que la sécurité, ou un composant spécifique, tel qu'Internet Information Services (IIS). |
| Updates | Correctifs largement diffusés pour des problèmes spécifiques remédiant à des bogues non critiques et non liés à la sécurité. |
| Upgrades | Nouvelles versions du produit mettant à niveau un appareil vers la version suivante. Les mises à niveau contiennent des correctifs de bogues, des modifications de conception et d'autres fonctionnalités. |

# Icônes utilisées pour les mises à jour dans Windows Server Update Services

Les mises à jour dans WSUS sont représentées par l'une des icônes suivantes. Pour afficher ces icônes, vous devez activer la colonne Remplacement dans la console Update Services.

## Aucune icône

La mise à jour n'a aucune relation de remplacement avec toute autre mise à jour.

**Préoccupations opérationnelles :**

Il n'existe aucun problème opérationnel.

## Icône de superseding

 Cette mise à jour remplace d'autres mises à jour.

**Préoccupations opérationnelles :**

Il n'existe aucun problème opérationnel.

## Icône d’une mise à jour remplacée et de remplacement

 Cette mise à jour est remplacée par une autre mise à jour et remplace d’autres mises à jour.

**Préoccupations opérationnelles :**

Remplacez ces mises à jour par les mises à jour de remplacement si possible.

## Icône remplacée

 Cette mise à jour est remplacée par une autre mise à jour.

**Préoccupations opérationnelles :**

Remplacez ces mises à jour par les mises à jour de remplacement si possible.

# WSUS et le catalogue Microsoft Update

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

Le catalogue Microsoft Update est un service qui fournit une liste des mises à jour qui peuvent être distribuées sur un réseau d'entreprise. Vous pouvez utiliser le catalogue pour trouver des informations sur les mises à jour logicielles, les pilotes et les correctifs logiciels Microsoft. WSUS inclut actuellement une option permettant d'importer des mises à jour à partir du catalogue Microsoft Update. Toutefois, l'action **Importer les mises à jour** dans WSUS a été créée à l'aide d'ActiveX, qui est désormais déconseillée. Cette fonctionnalité d'importation dans WSUS a été remplacée par un script PowerShell. Le script vous permet d'importer une mise à jour unique ou plusieurs mises à jour dans WSUS. Cet article fournit des informations sur le catalogue, le script d'importation et la façon d'utiliser le script.

## Conditions préalables pour l'importation de mises à jour dans WSUS

Les conditions préalables suivantes sont requises pour importer des mises à jour dans WSUS avec le script PowerShell :

- Tout ordinateur sur lequel la console administrative WSUS est installée, qu'il s'agisse ou non d'un serveur WSUS, peut être utilisé pour importer des mises à jour.
  - Lors de l'importation à partir d'un serveur WSUS, utilisez un compte membre du groupe Administrateurs WSUS ou du groupe Administrateurs locaux.
  - Lors de l'importation à partir d'un ordinateur distant, utilisez un compte membre du groupe Administrateurs WSUS et disposez d'autorisations d'administration sur l'ordinateur local. Les ordinateurs distants doivent être en mesure d'atteindre le serveur WSUS sur le réseau.

## Le catalogue Microsoft Update

Le catalogue Microsoft Update vous permet de rechercher sur différents champs et catégories de mise à jour. Ces champs de mise à jour sont les suivants :

- Mettre à jour le titre
- Description
- Produits applicables
- Classifications
- Numéros d'articles de la Base de connaissances au format `KB1234567`

Lorsque vous recherchez des mises à jour matérielles ou des pilotes, vous pouvez également rechercher les champs suivants :

- Modèle de pilote
- Manufacturer
- Class
- L'identifiant matériel à quatre parties, de type `PCI\VEN_14E4&DEV_1677&SUBSYS_01AD1028`.

Vous pouvez limiter l'étendue de votre recherche en ajoutant des termes de recherche supplémentaires. Pour rechercher une chaîne spécifique, utilisez des guillemets doubles.

> ⓘ **Note**
>
> Le catalogue vous permet également de télécharger des mises à jour directement à partir du site à l'aide du bouton de téléchargement. Toutefois, les mises à jour téléchargées de cette façon sont au `.MSU` format. WSUS ne peut pas importer de mises à jour au `.MSU` format. Ce type de fichier est couramment utilisé par le **programme d'installation autonome de Windows Update**, **DISM** ou d'autres outils de mise à jour. Certains outils nécessitent que vous extrayiez les fichiers du `.MSU` avant qu'ils puissent être utilisés.

# Importer des mises à jour dans WSUS à l'aide de PowerShell

Utilisez les instructions suivantes pour importer des mises à jour dans WSUS :

1. Copiez à partir de cet article le script PowerShell pour importer des mises à jour dans WSUS dans un éditeur de texte et enregistrez-le sous `ImportUpdateToWSUS.ps1`. Utilisez un emplacement auquel vous pouvez facilement accéder, par exemple `C:\temp`.

2. Ouvrez le catalogue Microsoft Update, https://catalog.update.microsoft.com dans un navigateur.

3. Recherchez une mise à jour que vous souhaitez importer dans WSUS.

4. Dans la liste retournée, sélectionnez la mise à jour que vous souhaitez importer dans WSUS. La page détails de la mise à jour s'ouvre.

5. Utilisez le bouton **Copier** dans la page détails de la mise à jour pour copier **l'ID de mise à jour**.

6. Le script peut être utilisé pour importer une mise à jour unique ou plusieurs mises à jour.

- Pour importer plusieurs mises à jour dans WSUS, collez les ID de mise à jour pour chaque mise à jour que vous souhaitez importer dans un fichier texte. Répertoriez un updateID par ligne. Enregistrez le fichier texte lorsque vous avez terminé. Utilisez un emplacement auquel vous pouvez facilement accéder, par exemple `C:\temp\UpdateIDs.txt`.
- Pour importer une seule mise à jour, vous devez uniquement copier l'ID de mise à jour unique.

7. Pour importer des mises à jour, ouvrez une console PowerShell en tant qu'administrateur et exécutez le script avec la syntaxe suivante, en utilisant les paramètres nécessaires :

```
PowerShell
C:\temp\ImportUpdateToWSUS.ps1 [-WsusServer] <String> [-PortNumber] <Int32> [-
UseSsl] [-UpdateId] <String> [-UpdateIdFilePath] <string> [<CommonParameters>]
```

**Exemple 1** : Importez une mise à jour unique dans un serveur WSUS en spécifiant le nom du serveur et le numéro de port :

```
PowerShell
.\ImportUpdateToWSUS.ps1 -WsusServer WSUSServer.contoso.com -PortNumber 8530 -
UpdateId 12345678-90ab-cdef-1234-567890abcdef
```

**Exemple 2** : À l'aide d'un ordinateur distant, importez plusieurs mises à jour dans un serveur WSUS à l'aide de SSL avec la syntaxe suivante :

```
PowerShell
.\ImportUpdateToWSUS.ps1 -WsusServer WSUSServer.contoso.com -PortNumber 8531 -
UseSsl -UpdateIdFilePath C:\temp\UpdateIDs.txt
```

8. Les fichiers de mise à jour pour les mises à jour importées sont téléchargés en fonction des paramètres de vos **fichiers de mise à jour** . Par exemple, si vous utilisez l'option **Télécharger les fichiers de mise à jour sur ce serveur uniquement lorsque les mises à jour sont approuvées**, les fichiers de mise à jour sont téléchargés lorsque la mise à jour est approuvée. Pour plus d'informations sur les options de stockage des mises à jour, consultez la version 1.3 Choisir une stratégie de stockage WSUS.

# Script PowerShell pour importer des mises à jour dans WSUS

```
```

PowerShell

```
<#
.SYNOPSIS
PowerShell script to import an update, or multiple updates, into WSUS based on the
UpdateID from the catalog.

.DESCRIPTION
This script takes user input and attempts to connect to the WSUS server.
Then it tries to import the update by using the provided UpdateID from the catalog.

.INPUTS
The script takes WSUS server Name/IP, WSUS server port, SSL configuration option,
and UpdateID as inputs. UpdateID can be viewed and copied from the update details
page for any update in the catalog, https://catalog.update.microsoft.com.

.OUTPUTS
Writes logging information to standard output.

.EXAMPLE
# Use with remote server IP, port, and SSL.
.\ImportUpdateToWSUS.ps1 -WsusServer 127.0.0.1 -PortNumber 8531 -UseSsl -UpdateId
12345678-90ab-cdef-1234-567890abcdef

.EXAMPLE
# Use with remote server Name, port, and SSL.
.\ImportUpdateToWSUS.ps1 -WsusServer WSUSServer1.us.contoso.com -PortNumber 8531 -
UseSsl -UpdateId 12345678-90ab-cdef-1234-567890abcdef

.EXAMPLE
# Use with remote server IP, defaultport, and no SSL.
.\ImportUpdateToWSUS.ps1 -WsusServer 127.0.0.1  -UpdateId 12345678-90ab-cdef-1234-
567890abcdef

.EXAMPLE
# Use with localhost default port.
.\ImportUpdateToWSUS.ps1 -UpdateId 12345678-90ab-cdef-1234-567890abcdef

.EXAMPLE
# Use with localhost default port, file with updateIDs.
.\ImportUpdateToWSUS.ps1 -UpdateIdFilePath .\file.txt


.NOTES
# On error, try enabling TLS: https://learn.microsoft.com/mem/configmgr/core/plan-
design/security/enable-tls-1-2-client.

# Sample registry add for the WSUS server from command line. Restarts the
WSUSService and IIS after adding:
reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 /V
SchUseStrongCrypto /T REG_DWORD /D 1

## Sample registry add for the WSUS server from PowerShell. Restarts WSUSService and
IIS after adding:
$registryPath = "HKLM:\Software\Microsoft\.NETFramework\v4.0.30319"
```

```
$Name = "SchUseStrongCrypto"
$value = "1"
if (!(Test-Path $registryPath)) {
    New-Item -Path $registryPath -Force | Out-Null
}
New-ItemProperty -Path $registryPath -Name $name -Value $value -PropertyType DWORD -
Force | Out-Null
Restart-Service WsusService, w3svc

# Update import logs/errors are under %ProgramFiles%\Update
Services\LogFiles\SoftwareDistribution.log.

#>

param(
    [Parameter(Mandatory = $false, HelpMessage = "Specifies the name of a WSUS
server, if not specified connects to localhost")]
    # Specifies the name of a WSUS server. If name isn't specified, connects to
localhost.
    [string]$WsusServer,

    [Parameter(Mandatory = $false, HelpMessage = "Specifies the port number to use
to communicate with the upstream WSUS server, default is 8530")]
    # Specifies the port number to use to communicate with the upstream WSUS server.
Default is 8530.
    [ValidateSet("80", "443", "8530", "8531")]
    [int32]$PortNumber = 8530,

    [Parameter(Mandatory = $false, HelpMessage = "Specifies that the WSUS server
should use Secure Sockets Layer (SSL) via HTTPS to communicate with an upstream
server")]
    # Specifies that the WSUS server should use Secure Sockets Layer (SSL) via HTTPS
to communicate with an upstream server.
    [Switch]$UseSsl,

    [Parameter(Mandatory = $true, HelpMessage = "Specifies the update Id we should
import to WSUS", ParameterSetName = "Single")]
    # Specifies the update ID to import to WSUS.
    [ValidateNotNullOrEmpty()]
    [String]$UpdateId,

    [Parameter(Mandatory = $true, HelpMessage = "Specifies path to a text file
containing a list of update ID's on each line", ParameterSetName = "Multiple")]
    # Specifies the path to a text file containing update IDs on each line.
    [ValidateNotNullOrEmpty()]
    [String]$UpdateIdFilePath
)

Set-StrictMode -Version Latest

# Set server options.
$serverOptions = "Get-WsusServer"
if ($psBoundParameters.containsKey('WsusServer')) { $serverOptions += " -Name
$WsusServer -PortNumber $PortNumber" }
if ($UseSsl) { $serverOptions += " -UseSsl" }
```

```
# Empty updateID list.
$updateList = @()

# Get update IDs.
if ($UpdateIdFilePath) {
    if (Test-Path $UpdateIdFilePath) {
        foreach ($id in (Get-Content $UpdateIdFilePath)) {
            $updateList += $id.Trim()
        }
    }
    else {
        Write-Error "[$UpdateIdFilePath]: File not found"
        return
    }
}
else {
    $updateList = @($UpdateId)
}

# Get WSUS server.
Try {
    Write-Host "Attempting WSUS Connection using $serverOptions... " -NoNewline
    $server = invoke-expression $serverOptions
    Write-Host "Connection Successful"
}
Catch {
    Write-Error $_
    return
}

# Empty file list.
$FileList = @()

# Call ImportUpdateFromCatalogSite on WSUS.
foreach ($uid in $updateList) {
    Try {
        Write-Host "Attempting WSUS update import for Update ID: $uid... " -
NoNewline
        $server.ImportUpdateFromCatalogSite($uid, $FileList)
        Write-Host "Import Successful"
    }
    Catch {
        Write-Error "Failed. $_"
    }
}
```

## Paramètres de script

**WsusServer** : <chaîne>

Spécifie le nom d'un serveur WSUS. Si le nom n'est pas spécifié, le script se connecte à

localhost.

- **Obligatoire** : false
- **Valeur par défaut** : localhost

**PortNumber** : <Int32>
Spécifie le numéro de port à utiliser pour communiquer avec le serveur WSUS en amont.

- **Obligatoire** : false
- **Valeur par défaut** : 8530
- **Valeurs autorisées** : 80, 443, 8530, 8531

**UseSsl** : <switch>
spécifie si SSL via HTTPS doit être utilisé pour communiquer avec le serveur WSUS. Si ce nom de paramètre est présent, le paramètre teste `$true` et la connexion est établie au serveur WSUS à l'aide de SSL. Sinon, `false`. Lorsque vous utilisez le paramètre **USeSSL** , définissez **portNumber** sur 443 ou 8531.

- **Obligatoire** : false

**UpdateId** : <chaîne>
spécifie l'ID de mise à jour que vous souhaitez importer dans WSUS. Ce paramètre est requis si vous importez une mise à jour unique. **UpdateId** ne peut pas être utilisé avec **UpdateIdFilePath**.

- **Obligatoire** : true lors de l'importation d'un seul updateID spécifié en tant que paramètre de script.

**UpdateIdFilePath** : <chaîne>
Spécifie le chemin d'accès à un fichier texte contenant des ID de mise à jour sur chaque ligne. Ce paramètre est requis si vous importez plusieurs mises à jour. **UpdateIdFilePath** ne peut pas être utilisé avec **UpdateId**.

- **Obligatoire** : true lors de l'utilisation d'un fichier texte pour importer plusieurs mises à jour.

**CommonParameters** :
Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable et OutVariable. Pour plus d'informations, consultez about_CommonParameters.

# Restriction de l'accès aux correctifs logiciels

Les administrateurs WSUS peuvent envisager de restreindre l'accès aux correctifs logiciels qu'ils ont téléchargés à partir du catalogue Microsoft Update. Pour restreindre les correctifs logiciels

disponibles, procédez comme suit :

1. Démarrez la console du Gestionnaire des services Internet (IIS).
2. Accédez au nœud **contenu** sous le site web **Administration WSUS** .
3. Dans le volet **Accueil du contenu** , double-cliquez sur l'option **Authentification** .
4. Sélectionnez **Authentification anonyme** , puis **sélectionnez Désactiver** dans le volet **Actions** à droite.
5. Sélectionnez **Authentification Windows** , puis **activez** le volet **Actions** à droite.
6. Dans la console d'administration WSUS, créez un groupe cible WSUS pour les ordinateurs qui ont besoin du correctif logiciel et ajoutez-les au groupe. Pour plus d'informations sur les ordinateurs et les groupes, consultez Gestion des ordinateurs clients WSUS et des groupes d'ordinateurs WSUS dans ce guide, et Configurer des groupes d'ordinateurs WSUS dans le guide de déploiement WSUS.
7. Téléchargez les fichiers du correctif logiciel.
8. Définissez les autorisations de ces fichiers afin que seuls les comptes d'ordinateur de ces machines puissent les lire. Vous devez également autoriser le compte de service réseau à accéder entièrement aux fichiers.
9. Approuvez le correctif logiciel pour le groupe cible WSUS créé à l'étape 2.

> ⓘ **Note**
>
> Vous pouvez supprimer les mises à jour importées du catalogue Microsoft Update qui sont définies comme **non approuvées** ou **refusées** en exécutant l'Assistant Nettoyage du serveur WSUS. Vous pouvez réimporter les mises à jour qui ont été précédemment supprimées de vos systèmes WSUS.

# Importation de mises à jour dans différentes langues

Le catalogue inclut des mises à jour qui prennent en charge plusieurs langues.

> ⓘ **Important**
>
> Mettre en correspondance les langues prises en charge par le serveur WSUS avec les langues prises en charge par les mises à jour importées.

Si le serveur WSUS ne prend pas en charge toutes les langues incluses dans la mise à jour, la mise à jour ne sera pas déployée sur les ordinateurs clients. Si une mise à jour prenant en charge plusieurs langues a été téléchargée sur le serveur WSUS, mais pas encore déployée sur

les ordinateurs clients et qu'un administrateur désélectionne l'une des langues incluses dans la mise à jour, la mise à jour ne sera pas déployée sur les clients.

# Troubleshooting

Le ". La section NOTES » du script peut être utilisée pour résoudre les problèmes qui peuvent se produire lorsque vous exécutez le script.

- Si vous recevez une erreur, essayez d'activer TLS (Transport Layer Security) 1.2. Pour plus d'informations, consultez Comment activer TLS 1.2 sur les clients.

- Vous pouvez utiliser la commande suivante pour automatiser le processus d'ajout d'une valeur de Registre liée à l'utilisation de chiffrement fort. Redémarrez manuellement le service Windows Server Update Services et le service World Wide Web Publishing après avoir ajouté la valeur du Registre.

  command

  ```
  reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 /V
  SchUseStrongCrypto /T REG_DWORD /D 1
  ```

- Exécutez le script PowerShell suivant pour automatiser le processus d'ajout d'une valeur de Registre liée à l'utilisation de chiffrement fort. Redémarrez ensuite le service Windows Server Update Services et le service de publication World Wide Web.

  PowerShell

  ```
  $registryPath = "HKLM:\Software\Microsoft\.NETFramework\v4.0.30319"
  $Name = "SchUseStrongCrypto"
  $value = "1"
  if (!(Test-Path $registryPath)) {
     New-Item -Path $registryPath -Force | Out-Null
  }
  New-ItemProperty -Path $registryPath -Name $name -Value $value -PropertyType
  DWORD -Force | Out-Null
  Restart-Service WsusService, w3svc
  ```

- L'activité et/ou les erreurs liées à l'importation des mises à jour se trouvent dans **%ProgramFiles%\Update Services\LogFiles\SoftwareDistribution.log** du serveur WSUS où les mises à jour sont importées.

---

Last updated on 01/12/2025

# Opérations de mise à jour

08/08/2025

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

Une fois les mises à jour synchronisées avec votre serveur WSUS, elles sont analysées automatiquement pour vérifier leur pertinence avec les ordinateurs clients du serveur. Mais vous devez approuver les mises à jour avant leur déploiement sur les ordinateurs de votre réseau. Lorsque vous approuvez une mise à jour, vous indiquez essentiellement à WSUS ce qu'il faut faire (vos choix sont **Installer** ou **Refuser** pour une nouvelle mise à jour). Vous pouvez approuver les mises à jour du groupe **Tous les ordinateurs** ou des sous-groupes. Si vous n'approuvez pas de mise à jour, son état d'approbation reste **Non approuvé** et votre serveur WSUS permet aux clients d'évaluer s'ils ont besoin de la mise à jour ou non.

Si votre serveur WSUS s'exécute en mode de réplica, vous ne pourrez pas approuver les mises à jour sur votre serveur WSUS. Pour plus d'informations sur le mode de réplica, consultez Mode de réplica WSUS en cours d'exécution.

## Approbation des mises à jour

Vous pouvez approuver l'installation des mises à jour pour tous les ordinateurs de votre réseau WSUS ou pour différents groupes d'ordinateurs. Après avoir approuvé une mise à jour, vous pouvez effectuer une (ou plusieurs) des opérations suivantes :

- Appliquer cette approbation aux groupes enfants, le cas échéant.
- Définir un délai pour l'installation automatique. Lorsque vous sélectionnez cette option, vous définissez des heures et des dates spécifiques pour installer les mises à jour, en remplaçant tous les paramètres sur les ordinateurs clients. En outre, vous pouvez spécifier une date passée pour le délai si vous souhaitez approuver une mise à jour immédiatement (pour être installé la prochaine fois que les ordinateurs clients contactent le serveur WSUS).
- Supprimer une mise à jour installée si cette mise à jour prend en charge la suppression.

Il existe deux éléments IMPORTANTS à garder à l'esprit :

- Tout d'abord, vous ne pouvez pas définir de délai pour l'installation automatique d'une mise à jour si l'intervention de l'utilisateur est requise (par exemple, spécifier un paramètre pertinent pour la mise à jour). Pour déterminer si une mise à jour nécessite une intervention de l'utilisateur, examinez le champ **Peut nécessiter l'intervention de l'utilisateur** dans les propriétés d'une mise à jour affichée sur la page **Mises à jour**.

Vérifiez également un message dans la zone **Approuver les mises à jour** qui indique que **la mise à jour sélectionnée nécessite une entrée utilisateur et ne prend pas en charge une échéance d'installation**.

- S'il existe des mises à jour du composant serveur WSUS, vous ne pouvez pas approuver d'autres mises à jour des systèmes clients tant que la mise à jour WSUS n'est pas approuvée. Ce message d'avertissement s'affiche dans la boîte de dialogue Approuver les mises à jour : certaines mises à jour WSUS n'ont pas été approuvées. Vous devez approuver les mises à jour WSUS avant d'approuver cette mise à jour. Dans ce cas, vous devez sélectionnez le nœud Mises à jour WSUS et vous assurer que toutes les mises à jour de cette vue ont été approuvées avant de revenir aux mises à jour générales.

## Pour approuver des mises à jour

1. Dans la console d'administration WSUS, sélectionnez **Mises à jour** , puis toutes **les mises à jour**.
2. Dans la liste des mises à jour, sélectionnez la mise à jour que vous souhaitez approuver, cliquez avec le bouton droit (ou accédez au volet Actions), puis, dans la boîte de dialogue Approuver les mises à jour, sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez approuver la mise à jour, et sélectionnez la flèche en regard de celle-ci.
3. Sélectionnez **Approuvée pour l'installation**, puis **Approuver**.
4. La fenêtre **Progression de** l'approbation affiche la progression vers la fin de l'approbation. Une fois le processus terminé, le bouton **Fermer** s'affiche. Sélectionnez **Fermer**.
5. Vous pouvez sélectionner une échéance en cliquant avec le bouton droit sur la mise à jour, en sélectionnant le groupe d'ordinateurs approprié, en sélectionnant la flèche en regard de celle-ci, puis en sélectionnant **Échéance**.
    - Vous pouvez sélectionner l'une des échéances standard (une semaine, deux semaines, un mois) ou vous pouvez sélectionner **Personnalisé** pour spécifier une date et une heure.
    - Si vous souhaitez qu'une mise à jour soit installée dès que les ordinateurs clients contactent le serveur, sélectionnez **Personnalisé**, puis définissez une date et une heure sur la date et l'heure actuelles ou sur une autre dans le passé.

## Pour approuver plusieurs mises à jour

1. Dans la console d'administration WSUS, sélectionnez **Mises à jour** , puis toutes **les mises à jour**.

2. Pour sélectionner plusieurs mises à jour contiguës, **appuyez sur la touche Maj** tout en sélectionnant les mises à jour. Pour sélectionner plusieurs mises à jour non incohérentes, appuyez longuement sur **Ctrl** enfoncée lors de la sélection des mises à jour.

3. Cliquez avec le bouton droit sur la sélection, puis sélectionnez **Approuver**. La boîte de dialogue **Approuver les mises à jour** s'ouvre avec **l'état Approbation** défini pour **conserver les approbations existantes** et le bouton **OK** désactivé.

4. Vous pouvez modifier les approbations des groupes individuels, mais cela n'affectera pas les approbations enfants. Sélectionnez le groupe pour lequel vous souhaitez modifier l'approbation, puis sélectionnez la flèche à gauche. Dans le menu contextuel, sélectionnez **Approuvé pour l'installation**.

5. La validation pour le groupe sélectionné change pour **Installer**. S'il existe des groupes enfants, leur approbation conserve l'état **Conserver l'approbation existante**. Pour modifier l'approbation des groupes enfants, sélectionnez le groupe, puis la flèche à gauche. Dans le menu contextuel, sélectionnez **Appliquer aux enfants**.

6. Pour définir un enfant spécifique afin d'hériter de l'approbation du parent, sélectionnez l'enfant puis la flèche à gauche. Dans le menu contextuel, sélectionnez **Identique au parent**. Si vous définissez un enfant pour hériter des approbations, mais que vous ne modifiez pas les approbations parentes, l'enfant héritera des approbations existantes du parent.

7. Si vous souhaitez que le comportement d'approbation change pour tous les enfants, approuvez **tous les ordinateurs**, puis choisissez **Appliquer aux enfants**.

8. Sélectionnez **OK** après avoir défini toutes vos approbations. La fenêtre **Progression de** l'approbation affiche la progression vers la fin de l'approbation. Une fois le processus terminé, le bouton **Fermer** est disponible. Sélectionnez **Fermer**.

# Baisse des mises à jour

Si vous sélectionnez cette option, la mise à jour est supprimée de la liste par défaut des mises à jour disponibles et le serveur WSUS n'offre pas la mise à jour aux clients, à des fins d'évaluation ou d'installation. Vous pouvez accéder à cette option en sélectionnant une mise à jour ou un groupe de mises à jour, puis en cliquant avec le bouton droit ou en accédant au volet Actions. Les mises à jour refusées s'affichent dans la liste des mises à jour uniquement si vous sélectionnez **Refusé** dans la liste d'approbations lors de la spécification du filtre de la liste de mises à jour sous **Affichage**.

## Pour refuser des mises à jour

1. Dans la console d'administration WSUS, sélectionnez **Mises à jour**, puis sélectionnez **Toutes les mises à jour**.
2. Dans la liste des mises à jour, sélectionnez une ou plusieurs mises à jour que vous souhaitez refuser.
3. sélectionnez **Refuser**, puis sélectionnez **Oui** dans le message de confirmation.

# Nettoyage des mises à jour refusées

Les mises à jour refusées continuent de consommer certaines ressources serveur WSUS. Vous devez exécuter l'Assistant de nettoyage du serveur pour supprimer les mises à jour refusées de la base de données WSUS. Pour plus d'informations, consultez Assistant de nettoyage du serveur.

# Rétablissement des mises à jour refusées

Une fois qu'une mise à jour a été refusée, vous pouvez quand même la rétablir.

## Pour rétablir les mises à jour refusées

1. Dans la console d'administration WSUS, sélectionnez **Mises à jour** , puis toutes **les mises à jour**.
2. Changer **'Approbation'** en **'Refus'** et sélectionner **Actualiser**. La liste des mises à jour refusées se charge.
3. Dans la liste des mises à jour, sélectionnez une ou plusieurs mises à jour refusées que vous souhaitez rétablir.
4. Pour rétablir une mise à jour particulière, sélectionnez avec le bouton droit sur la mise à jour, puis sélectionnez **Approuver**. Dans la boîte de dialogue **Approuver les mises à jour** , sélectionnez **OK** pour appliquer à nouveau l'état d'approbation non approuvé par défaut. La mise à jour s'affiche dans la liste comme **Non approuvée** au lieu de Refusé.

Une fois qu'une mise à jour refusée a été nettoyée à l'aide de l'Assistant de nettoyage du serveur WSUS, elle est supprimée du serveur WSUS et n'apparaît plus dans l'affichage Toutes les mises à jour. Vous pouvez réimporter les mises à jour refusées et nettoyées à partir du catalogue Microsoft Update. Pour plus d'informations, consultez WSUS et le site du catalogue.

# Changer une mise à jour approuvée en non approuvée

Si une mise à jour a été approuvée et que vous décidez de ne pas l'installer pour l'instant et que vous souhaitez plutôt l'enregistrer pour une prochaine fois, vous pouvez modifier la mise à jour en changeant son état sur Non approuvé. Cela signifie que la mise à jour restera dans la liste par défaut des mises à jour disponibles et indiquera la conformité du client, mais elle ne sera pas installée sur les clients.

### Pour changer une mise à jour approuvée en non approuvée

1. Dans la console d'administration WSUS, sélectionnez **Mises à jour**, puis sélectionnez **Toutes les mises à jour**.

2. Dans la liste des mises à jour, sélectionnez une ou plusieurs mises à jour approuvées pour lesquelles vous souhaitez définir l'état sur Non approuvé.

3. Dans le menu contextuel ou le volet **Actions** , sélectionnez **Non approuvé**, puis sélectionnez **Oui** dans le message de confirmation.

# Approbation de mises à jour à supprimer

Vous pouvez approuver une mise à jour à supprimer (autrement dit, pour désinstaller une mise à jour déjà installée). Cette option est disponible uniquement si la mise à jour est déjà installée et peut être supprimée. Vous pouvez spécifier un délai pour la désinstallation de la mise à jour, ou spécifier une date passée pour le délai si vous souhaitez supprimer la mise à jour immédiatement (la prochaine fois que les ordinateurs clients contactent le serveur WSUS).

Il est IMPORTANT de mentionner que toutes les mises à jour, telles que les mises à jour UUP, ne prennent pas en charge la suppression. Vous pouvez voir si une mise à jour prend en charge la suppression en sélectionnant une mise à jour individuelle et en examinant le volet **d'informations** . Sous **plus d'informations**, vous verrez la catégorie **amovible** . Si la mise à jour ne peut pas être supprimée via WSUS, dans certains cas, elle peut être supprimée avec **l'ajout ou la suppression de programmes** du **Panneau de configuration**.

### Pour approuver des mises à jour à supprimer

1. Dans la console d'administration WSUS, sélectionnez **Mises à jour** , puis toutes **les mises à jour**.

2. Dans la liste des mises à jour, sélectionnez une ou plusieurs mises à jour que vous souhaitez approuver pour la suppression et cliquez avec le bouton droit sur ces mises à jour (ou accédez au volet **Actions** ).

3. Dans la boîte de dialogue **Approuver les mises à jour** , sélectionnez le groupe d'ordinateurs à partir duquel vous souhaitez supprimer la mise à jour, puis sélectionnez la flèche en regard de celle-ci.

4. Sélectionnez **Approuvé pour la suppression**, puis sélectionnez le bouton **Supprimer**.

5. Une fois l'approbation supprimée, vous pouvez sélectionner un délai en cliquant avec le bouton droit sur la mise à jour, en sélectionnant le groupe d'ordinateurs approprié, puis en cliquant sur la flèche en regard de celle-ci. Sélectionnez **Échéance**. Vous pouvez sélectionner l'une des échéances standard (une semaine, deux semaines, un mois) ou sélectionner **Personnalisé** pour sélectionner une date et une heure spécifiques.

6. Si vous souhaitez supprimer une mise à jour dès que les ordinateurs clients contactent le serveur, sélectionnez **Personnalisé** et définissez une date dans le passé.

# Approuver automatiquement les mises à jour

Vous pouvez configurer votre serveur WSUS pour approuver automatiquement certaines mises à jour. Vous pouvez également spécifier l'approbation automatique des révisions de mises à jour existantes à mesure qu'elles deviennent disponibles. Cette option est sélectionnée par défaut. Une révision est une version d'une mise à jour qui a apporté des modifications à celle-ci (par exemple, elle a peut-être expiré ou ses règles d'applicabilité ont peut-être changé). Si vous ne choisissez pas d'approuver automatiquement la version révisée d'une mise à jour, WSUS utilisera l'ancienne version et vous devez approuver manuellement la révision de la mise à jour.

Vous pouvez créer des règles que votre serveur WSUS applique automatiquement lors de la synchronisation. Vous spécifiez les mises à jour que vous souhaitez approuver automatiquement pour l'installation, par classification des mises à jour, par produit et par groupe d'ordinateurs. Cette règle s'applique uniquement aux nouvelles mises à jour, et non pas aux mises à jour révisées. Vous pouvez également spécifier un délai d'approbation de mise à jour, qui définit un certain nombre de jours et une heure spécifique d'offre avant l'installation de la mise à jour approuvée. Ces paramètres sont disponibles dans le volet **Options** , sous **Approbations automatiques**.

## Pour approuver automatiquement les mises à jour

1. Dans la console d'administration WSUS, sélectionnez **Options**, puis **sélectionnez Approbations automatiques**.

2. Dans **Règles de mise à jour**, sélectionnez **Nouvelle règle**.

3. Dans la boîte de dialogue **Ajouter une règle** , sous **l'étape 1 : sélectionnez les propriétés**, indiquez si **une mise à jour se trouve dans une classification spécifique** ou **lorsqu'une mise à jour se trouve dans un produit spécifique** (ou les deux) comme critères. Si vous le souhaitez, indiquez s'il **faut définir un délai** pour l'approbation.

    - Lorsque vous sélectionnez la classification **des mises à niveau** , sachez que les mises à jour des fonctionnalités Windows publiées tous les mois sont également classées comme **mises à niveau**. L'approbation automatique de ces mises à jour peut entraîner la mise à niveau du système d'exploitation des appareils. Les appareils Windows 10 applicables peuvent par exemple être mis à niveau vers Windows 11. En outre, les mises à jour de fonctionnalité nécessitent un espace disque supplémentaire. Pour plus d'informations, veuillez consulter la section Considérations relatives à UUP lors de la planification de votre déploiement WSUS.

4. À **l'étape 2 : modifiez les propriétés**, sélectionnez les propriétés soulignées pour sélectionner les classifications, les produits et les groupes d'ordinateurs pour lesquels vous souhaitez des approbations automatiques, le cas échéant. Si vous le souhaitez, choisissez le délai d'approbation de la mise à jour (jour et heure).

5. À **l'étape 3 : spécifiez un nom**, tapez un nom unique pour la règle.

6. Cliquez sur **OK**.

Les règles d'approbation automatiques ne s'appliquent pas aux mises à jour nécessitant un contrat de licence utilisateur final (CLUF) qui n'a pas encore été accepté sur le serveur. Si vous constatez que l'application d'une règle d'approbation automatique n'entraîne pas l'approbation de toutes les mises à jour pertinentes, vous devez manuellement approuver ces mises à jour.

## Approuver automatiquement les révisions de mises à jour et refuser les mises à jour expirées

La section Approbations automatiques du volet Options contient une option par défaut pour approuver automatiquement les révisions de mises à jour approuvées. Vous pouvez également configurer votre serveur WSUS pour refuser automatiquement les mises à jour expirées. Si vous choisissez de ne pas approuver automatiquement la version révisée d'une mise à jour, votre serveur WSUS utilisera l'ancienne révision et vous devez approuver manuellement la révision de la mise à jour.

> ⓘ **Notes**

Une révision est une version d'une mise à jour qui a changé (par exemple, elle a peut-être expiré ou comporte des règles d'applicabilité mises à jour).

### Pour approuver automatiquement les révisions de mises à jour et refuser les mises à jour expirées

1. Dans la console d'administration WSUS, sélectionnez **Options**, puis **sélectionnez Approbations automatiques**.
2. Sous l'onglet **Avancé** , veillez à **approuver automatiquement les nouvelles révisions des mises à jour approuvées** et **à refuser automatiquement les mises à jour lorsqu'une nouvelle révision les amène à expirer** sont sélectionnées.
3. Cliquez sur OK.

   ⓘ **Notes**

   Conserver les valeurs par défaut pour ces options vous permet de maintenir de bonnes performances sur votre réseau WSUS. Si vous ne souhaitez pas que les mises à jour expirées soient automatiquement refusées, vous devez veiller à les refuser manuellement de façon périodique.

## Refus automatique des mises à jour remplacées

Lorsque vous approuvez une nouvelle mise à jour qui remplace une mise à jour existante automatiquement approuvée, la mise à jour remplacée devient non applicable à un ordinateur ou un appareil une fois la mise à jour plus récente installée. Vous pouvez vérifier dans la console WSUS qu'une mise à jour n'est pas applicable à tous les ordinateurs. Dans ce cas, la mise à jour peut être refusée en toute sécurité. De plus, la mise à jour peut être automatiquement refusée lorsque vous exécutez l'Assistant de nettoyage du serveur WSUS.

Pour rechercher les mises à jour remplacées, vous pouvez sélectionner la colonne de l'indicateur Remplacé dans l'affichage Toutes les mises à jour et trier selon cette colonne. Quatre groupes s'affichent :

- Mises à jour qui n'ont jamais été remplacées (icône vide).
- Mises à jour qui ont été remplacées, mais qui n'ont jamais remplacé une autre mise à jour (icône avec un carré bleu en bas).

- Mises à jour qui ont été remplacées et qui ont remplacé une autre mise à jour (icône avec un carré bleu au milieu).
- Mises à jour qui ont remplacé une autre mise à jour (icône avec un carré bleu en haut).

Il n'existe aucune fonctionnalité dans Windows Server Update Services permettant de refuser automatiquement les mises à jour remplacées lors de l'approbation d'une mise à jour plus récente. Il est recommandé de définir d'abord l'approbation sur Non approuvé, puis d'utiliser l'Assistant de nettoyage du serveur pour refuser automatiquement la mise à jour lorsque toutes les conditions pertinentes sont réunies. Pour plus d'informations, consultez l'Assistant de nettoyage du serveur.

## Approbation de mises à jour de remplacement ou qui ont été remplacées

En général, une mise à jour qui remplace d'autres mises à jour entraîne un ou plusieurs des résultats suivants :

- Optimise, améliore ou s'ajoute au correctif fourni par une ou plusieurs mises à jour précédemment publiées.
- Améliore l'efficacité de son package de fichiers de mise à jour, qui est installé sur les ordinateurs clients si la mise à jour est approuvée pour l'installation. Par exemple, la mise à jour remplacée peut contenir des fichiers qui ne sont plus pertinents au correctif ou aux systèmes d'exploitation pris en charge par la nouvelle mise à jour, de sorte que ces fichiers ne sont plus inclus dans le package de fichiers de la mise à jour de remplacement.
- Met à jour les versions plus récentes des systèmes d'exploitation. Il est également IMPORTANT de noter que la mise à jour de remplacement peut ne pas prendre en charge les versions antérieures des systèmes d'exploitation.

Inversement, une mise à jour qui est remplacée par une autre mise à jour entraîne les résultats suivants :

- Résout un problème semblable à celui résolu par la mise à jour qui la remplace. Toutefois, la mise à jour qui la remplace peut améliorer le correctif fourni par la mise à jour remplacée.
- Met à jour les versions antérieures des systèmes d'exploitation. Dans certains cas, ces versions des systèmes d'exploitation ne sont plus mises à jour par la mise à jour de remplacement.

Dans le volet de détails d’une mise à jour individuelle, une icône d’information et un message en haut indiquent que cette mise à jour remplace ou est remplacée par une autre mise à jour. En outre, vous pouvez déterminer quelles mises à jour remplacent ou sont remplacées par la mise à jour en examinant les entrées **Mises à jour prioritaires sur cette mise à jour** et **Mises à jour remplacées par cette mise à jour** dans la section **Détails supplémentaires** de la fenêtre **Propriétés**. Le volet des détails d’une mise à jour s’affiche sous la liste des mises à jour.

WSUS ne refuse pas automatiquement les mises à jour remplacées et il est recommandé de ne pas supposer que les mises à jour remplacées doivent être refusées au profit de la nouvelle mise à jour de remplacement. Avant de refuser une mise à jour remplacée, assurez-vous qu'elle n'est plus nécessaire sur vos ordinateurs clients. Voici quelques exemples de scénarios dans lesquels vous devrez peut-être installer une mise à jour remplacée :

- Si une mise à jour de remplacement prend en charge uniquement les versions les plus récentes du système d'exploitation, et certains de vos ordinateurs clients exécutent des versions antérieures du système d'exploitation
- Si une mise à jour de remplacement a une mise en application plus limitée que la mise à jour remplacée, ce qui la rendrait inappropriée pour certains ordinateurs clients
- Lorsqu'une mise à jour ne remplace plus une mise à jour précédemment publiée en raison de nouvelles modifications. Il est possible que grâce aux modifications apportées à chaque version, une mise à jour ne remplace plus une mise à jour qu’elle a précédemment remplacée dans une version antérieure. Dans ce scénario, le message relatif à la mise à jour remplacée s'affiche toujours, même si la mise à jour qui la remplace a été substituée par une mise à jour qui ne la remplace pas.
- Maintenez la synchronisation des mises à jour de qualité et de fonctionnalités. Cela signifie que si une mise à jour de fonctionnalité date d’un mois, la mise à jour qualité doit également l’être. Si la mise à jour des fonctionnalités date de deux mois et que la mise à jour qualité est d’un mois, le module linguistique et l’acquisition des fonctionnalités à la demande ne fonctionneront pas

# Assistant de nettoyage du serveur

Article • 06/05/2025 •

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

S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

L'Assistant Nettoyage du serveur est intégré à l'interface utilisateur pour vous aider à gérer votre espace disque. L'Assistant de nettoyage du serveur peut effectuer les opérations suivantes :

- Supprimer les mises à jour inutilisées et les révisions de mise à jour.
- Supprimez toutes les anciennes mises à jour et révisions de mises à jour qui n'ont pas été approuvées.
- Supprimez tous les ordinateurs clients qui n'ont pas contacté le serveur en 30 jours ou plus.
- Supprimez tous les fichiers de mise à jour qui ne sont pas nécessaires par les mises à jour ou par les serveurs en aval.
- Refuser toutes les mises à jour de Microsoft qui sont expirées.
- Refuser toutes les mises à jour qui répondent à tous les critères suivants :
  - La mise à jour remplacée n'est pas obligatoire.
  - La mise à jour remplacée a été effectuée sur le serveur pendant 30 jours ou plus.
  - La mise à jour remplacée n'est actuellement signalée comme nécessaire par aucun client.
  - La mise à jour remplacée n'a pas été déployée explicitement sur un groupe d'ordinateurs pendant 90 jours ou plus.
  - La mise à jour de remplacement doit être approuvée pour l'installation sur un groupe d'ordinateurs.

> ⚠ **Avertissement**
>
> Dans une hiérarchie WSUS, il est fortement recommandé d'exécuter le processus de nettoyage sur le serveur WSUS en aval/réplica le plus bas, puis de monter dans la hiérarchie. L'exécution incorrecte du nettoyage sur n'importe quel serveur en amont

avant d'exécuter le nettoyage sur chaque serveur en aval peut entraîner une incompatibilité entre les données présentes dans les bases de données en amont et les bases de données en aval. L'incompatibilité des données peut entraîner des échecs de synchronisation entre les serveurs en amont et en aval.

> **ⓘ Important**
>
> Si vous supprimez du contenu inutile à l'aide de l'Assistant Nettoyage du serveur, tous les fichiers de mise à jour privée que vous avez téléchargés à partir du site catalogue Microsoft Update sont également supprimés. Vous devez réimporter ces fichiers après avoir exécuté l'Assistant Nettoyage du serveur.

Si les mises à jour sont approuvées à l'aide d'une règle d'approbation automatique, elles peuvent rester dans un état approuvé et ne seront pas supprimées par l'Assistant Nettoyage du serveur. Pour supprimer les mises à jour approuvées automatiquement dans un état approuvé, l'administrateur WSUS doit au minimum définir manuellement l'état d'approbation des mises à jour remplacées sur Non approuvé. Définir manuellement statut d'approbation des mises à jour remplacées sur Non approuvé rend les mises à jour éligibles à la déclinaison par l'Assistant Nettoyage du serveur. L'Assistant de nettoyage du serveur s'assure qu'une mise à jour plus récente est approuvée et qu'aucun système client ne signale ces mises à jour comme étant nécessaires avant de la marquer comme Refusée.

# Mode de réplica WSUS en cours d'exécution

Article • 30/03/2025 •

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

Un serveur WSUS s'exécutant en mode Réplica hérite des approbations de mise à jour et des groupes d'ordinateurs créés sur un serveur d'administration. Dans un scénario qui utilise le mode Réplica, vous disposez généralement d'un serveur d'administration unique et d'un ou plusieurs serveurs WSUS de réplication subordonnés répartis dans toute l'organisation, en fonction de la topographie de cette dernière ou du site. Vous approuvez les mises à jour et créez des groupes d'ordinateurs sur le serveur d'administration, que les serveurs en mode Réplica vont ensuite refléter. Les serveurs en mode Réplica peuvent être configurés uniquement lors de l'installation de WSUS et, si vous avez implémenté ce scénario, cela est probablement dû au fait qu'il est important dans votre organisation que les approbations et les groupes d'ordinateurs soient gérés de manière centralisée.

Si votre serveur WSUS s'exécute en mode Réplica, vous ne pouvez exécuter que des fonctionnalités d'administration limitées sur le serveur, qui, pour l'essentiel, sont les suivantes :

- Ajout et suppression d'ordinateurs de groupes d'ordinateurs. L'appartenance aux groupes d'ordinateurs n'est pas distribuée aux serveurs de réplication, mais uniquement aux groupes d'ordinateurs eux-mêmes. Ainsi, sur un serveur en mode Réplica, vous héritez des groupes d'ordinateurs que vous avez créés sur le serveur d'administration. Toutefois, les groupes d'ordinateurs sont vides. Vous devez ensuite affecter les ordinateurs clients qui se connectent au serveur de réplication aux groupes d'ordinateurs.
- Définition d'une planification de la synchronisation
- Spécification des paramètres du serveur proxy
- Spécification de la source de mise à jour. Il peut s'agir d'un serveur autre que le serveur d'administration
- Affichage des mises à jour disponibles
- Supervision de la mise à jour, de la synchronisation, de l'état de l'ordinateur et des paramètres WSUS sur le serveur

- Exécution de tous les rapports WSUS standard disponibles sur les serveurs en mode Réplica

---

## Commentaires

**Cette page a-t-elle été utile ?** Yes No

# Conseils de dépannage et messages WSUS

S'applique à: ✅ Supported versions of Windows Server

Cet article contient des informations sur les messages WSUS suivants :

- L'ordinateur n'a pas signalé d'état
- ID de message 6703 - Échec de la synchronisation WSUS
- Erreur 0x80070643 : Erreur irrécupérable lors de l'installation
- Certains services ne fonctionnent pas. Vérifiez les services suivants [...]

## L'ordinateur n'a pas signalé d'état

Ce message est généré dans la console WSUS quand un ordinateur client WSUS n'envoie pas d'informations au serveur WSUS pour indiquer son état de mise à jour actuel. Ce problème est généralement dû à l'ordinateur client WSUS, et non au serveur WSUS.

Les raisons les plus courantes sont les suivantes :

- L'ordinateur a perdu la connectivité au réseau :
  - Le câble réseau est déconnecté.
  - Un câble réseau intermédiaire est défectueux.
  - L'ordinateur dispose d'une carte réseau défaillante.
  - Le port réseau auquel l'ordinateur se connecte a été désactivé.
  - L'adaptateur sans fil n'est pas en mesure de s'associer et de se connecter au point d'accès sans fil d'entreprise.
- L'ordinateur est désactivé. (Il a été arrêté ou est en mode veille ou veille prolongée.)

## ID de message 6703 - Échec de la synchronisation WSUS

**Event**

```
Message: The request failed with HTTP status 503: Service Unavailable.
Source: Microsoft.UpdateServices.Administration.AdminProxy.createUpdateServer.
```

Quand vous tentez d'ouvrir Update Services sur le serveur WSUS, vous recevez l'erreur suivante :

**Event**

```
Error: Connection Error
An error occurred trying to connect to the WSUS server. This error can happen for a
number of reasons. Please contact your network administrator if the problem persists.
Click the reset Server Node to connect to the server again.
```

Les tentatives d'accès à l'URL du site web d'administration WSUS, par exemple `http://WSUS01:8530`, échouent avec l'erreur :

`HTTP Error 503. The service is unavailable`

Dans ce cas, la cause la plus probable est que le pool d'applications WsusPool dans IIS est dans un état arrêté.

En outre, la limite de la mémoire privée (KO) du pool d'applications est probablement définie sur la valeur par défaut de 1843200 Ko. Si vous rencontrez ce problème, augmentez la limite de la mémoire privée à 4 Go (4 000 000 Ko) et redémarrez le pool d'applications. Pour augmenter la mémoire, procédez comme suit :

1. Ouvrez la console du **Gestionnaire des services Internet (IIS)**.
2. Sélectionnez **Pools d'applications** dans le volet **Connexions** , puis sélectionnez **WsusPool**, cliquez avec le bouton droit et sélectionnez **Paramètres avancés**.
3. Définissez la **Limite de la mémoire privée (Ko)** sur *4000000*.
4. Sélectionnez **OK** pour appliquer le paramètre.

Si l'environnement l'exige, il peut s'avérer nécessaire d'augmenter la limite de la mémoire privée à 8 Go (8 000 000 Ko) ou plus.

## Erreur 0x80070643 : Erreur irrécupérable lors de l'installation

Si WSUS a été configuré en utilisant Microsoft SQL Server, ce problème est lié au fait que l'utilisateur qui exécute le programme d'installation de WSUS ne dispose pas des autorisations d'administrateur système dans SQL Server. Pour résoudre ce problème, accordez des autorisations d'administrateur système à un compte d'utilisateur ou à un compte de groupe dans SQL Server, puis réexécutez le programme d'installation de WSUS.

## Certains services ne fonctionnent pas

Vérifiez que les services suivants sont en cours d'exécution :

- **Autoupdate :** Consultez Les mises à jour automatiques doivent être mises à jour pour plus d'informations sur la résolution des problèmes du service Selfupdate.
- **WSSUService.exe:** Ce service facilite la synchronisation. Si vous rencontrez des problèmes de synchronisation, accédez à WSUSService.exe en cliquant sur **Démarrer**, en pointant sur **Outils d'administration**, en cliquant sur **Services**, puis en recherchant **le service Windows Server Update** dans la liste des services. Une fois que vous avez trouvé le service :
  - Vérifiez que ce service est en cours d'exécution. Sélectionnez **Démarrer** s'il est arrêté ou **redémarré** pour actualiser le service.
  - Utilisez l'Observateur d'événements pour vérifier les journaux des événements **Application**, **Securit**y et **System** pour voir s'il existe des événements susceptibles d'indiquer un problème.
- **Services web :** les services web sont hébergés dans IIS. S'ils ne sont pas en cours d'exécution, vérifiez qu'IIS est en cours d'exécution (ou démarré). Vous pouvez également essayer de réinitialiser le service Web en tapant **iisreset** à l'invite de commandes.
- **Service SQL :** Chaque service à l'exception du service libre-mise à jour nécessite que le service SQL s'exécute. Si l'un des fichiers journaux indique des problèmes de connexion SQL, vérifiez d'abord le service SQL. Pour accéder au service SQL, sélectionnez **Démarrer**, pointez sur **Outils d'administration**, sélectionnez **Services**, puis recherchez l'une des options suivantes :
  - **MSSQLSERVER** (si vous utilisez WMSDE ou MSDE, ou si vous utilisez SQL Server et utilisez le nom d'instance par défaut pour le nom de l'instance)
  - **MSSQL$WSUS** (si vous utilisez une base de données SQL Server et que vous avez nommé votre instance de base de données WSUS)

    Cliquez avec le bouton droit sur le service, puis sélectionnez **Démarrer** si le service n'est pas en cours d'exécution, ou **Redémarrez** pour actualiser le service s'il est en cours d'exécution.

## Impossible d'ajouter une entrée de collection en double de type mimeMap

Si vous avez précédemment ajouté des types MIME manuellement, vous pouvez rencontrer des erreurs concernant les entrées en double en raison de modifications apportées à WSUS pour

prendre en charge UUP. Si vous recevez une erreur similaire à `Cannot add duplicate collection entry of type 'mimeMap' with unique key attribute 'fileExtension' set to '.wim'`, le type MIME n'a peut-être pas été défini au niveau approprié. Pour résoudre ce problème, vous devez modifier le fichier web.config afin de supprimer le type MIME du niveau où il a été défini à l'origine.

Recherchez le fichier *web.config* où le type MIME a été défini :

1. Ouvrez **les types MIME** à chaque niveau et **recherchez où le type d'entrée** est répertorié comme `local` pour les `.wim` types MIME. `.msu`
    - Par exemple, vous pouvez constater qu'elle `.wim` est définie `local` au niveau du site *d'administration WSUS* ou au niveau du service web *APIRemoting30* . Ces deux types MIME doivent uniquement être définis sur `local` au niveau du serveur.
2. Une fois que vous avez localisé l'emplacement où les types MIME sont définis `local` sur , à partir de ce même emplacement, dans le volet d'action, sélectionnez **Explorer** pour ouvrir l'emplacement du dossier.
3. Ouvrez le fichier *web.config* avec le Bloc-notes ou un autre éditeur de texte.
4. Recherchez les entrées de mappage MIME pour `.wim` et `.msu`. Les entrées doivent ressembler à `<mimeMap fileExtension=".msu" mimeType="application/octect-stream" />`.
5. Dans la ligne située juste au-dessus de l'entrée de fichier, insérez une suppression pour le type tel que `<remove fileExtension=".msu" />`. Si les deux types de fichiers ont été répertoriés, le fichier *web.config* doit ressembler à l'entrée suivante :

    XML

    ```xml
    <configuration>
      <system.webServer>
        <staticContent>
          <remove fileExtension=".wim" />
          <mimeMap fileExtension=".wim" mimeType="application/x-ms-wim" />
          <remove fileExtension=".msu" />
          <mimeMap fileExtension=".msu" mimeType="application/octect-stream" />
        </staticContent>
      </system.webServer>
    </configuration>
    ```

6. Enregistrez la modification dans le fichier *web.config* , puis fermez-le.

Dernière mise à jour : 12/02/2026

# Prise en charge par les ISV de la distribution des mises à jour Express

14/08/2025

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

Les téléchargements de Windows 10 Update peuvent être volumineux car, à des fins de cohérence et de simplicité, chaque package contient l'ensemble des correctifs précédemment publiés.

Depuis la version 7, Windows a pu réduire la taille des téléchargements de Windows Update avec une fonctionnalité appelée Express, et bien que les appareils grand public le prennent en charge par défaut, les appareils Windows 10 entreprise nécessitent windows Server Update Services (WSUS) pour tirer parti d'Express.

## Prise en charge de la fonctionnalité Express par Microsoft

- **Express sur WSUS en tant qu'application autonome**

  La distribution de mises à jour Express est déjà disponible sur toutes les versions de WSUS prises en charge.

- **Fonctionnalité Express sur des appareils directement connectés à Windows Update**

  Les appareils grand public prennent en charge le téléchargement de la fonctionnalité Express : ils utilisent le client Windows Update (WU) pour analyser, télécharger et installer les mises à jour. Pendant la phase de téléchargement, le client WU demande des packages Express et télécharge les plages d'octets appropriées.

- **Les appareils d'entreprise gérés à l'aide de Windows Update for Business** bénéficient également de la distribution de mises à jour Express sans aucun changement de configuration.

## Avantages de la fonctionnalité Express pour les éditeurs de logiciels indépendants

Les éditeurs de logiciels indépendants peuvent utiliser WSUS et le client WU pour prendre en charge la distribution des mises à jour Express. Microsoft recommande les trois étapes

suivantes. Chaque étape est traitée plus en détail plus loin dans l'article.

1. **Configurer WSUS**

   Le serveur WSUS est requis pour l'analyse et les synchronisations de mises à jour (pour plus d'informations, consultez Configuration des synchronisations de mises à jour).

2. **Spécifier et remplir un cache de fichiers ISV**

   Il est recommandé d'utiliser un cache de fichiers ISV pour héberger le contenu de la mise à jour, qui comprend la mise à jour des fichiers CAB (fichiers.cab) et les packages Express (fichiers.psf).

3. **Configurer un agent client ISV pour diriger les opérations du client WU**

> ⓘ **Notes**
>
> Nécessite l'installation de la mise à jour cumulative de la version 1607 de Windows 10 sortie en janvier 2017 (ou après) (KB3213986 [build de système d'exploitation 14393.693]).

- L'agent client ISV détermine quelles mises à jour doivent être approuvées et quand les télécharger et les installer.
- Le client WU détermine les plages d'octets à télécharger et lance la demande de téléchargement

## Étape 1 : Configurer WSUS

WSUS est l'interface de Windows Update et gère toutes les métadonnées décrivant les packages Express à télécharger. Si vous devez effectuer un déploiement, consultez Windows Server Update Services (WSUS). Une fois le WSUS déployé, la première chose à faire et de décider si vous souhaitez stocker le contenu des mises à jour localement sur le serveur WSUS. Lors de la configuration de WSUS, nous vous recommandons de ne pas stocker les mises à jour localement. Cela suppose que vous disposez déjà d'un logiciel dirigeant le déploiement de ces packages dans votre environnement. Pour plus d'informations sur la configuration du stockage local de WSUS, consultez Stockage des mises à jour de WSUS.

## Étape 2 : Spécifier et remplir un cache de fichiers ISV

### Spécifier le cache des fichiers ISV

Les nouveaux paramètres de stratégie de groupe et de gestion des appareils mobiles (GAM) côté client détaillés dans la référence du fournisseur de services de configuration définissent l'emplacement du cache des fichiers ISV.

Agrandir le tableau

| Name | Description |
|---|---|
| Configurer un autre emplacement de téléchargement pour les mises à jour. | Spécifie un autre serveur intranet permettant d'héberger les mises à jour de Microsoft Update. Vous pouvez ensuite utiliser ce service de mise à jour pour procéder à la mise à jour automatique des ordinateurs de votre réseau. |

Vous pouvez choisir entre deux options lors de la configuration de l'autre emplacement de téléchargement pour le cache des fichiers ISV :

1. **Spécifiez un nom d'hôte de serveur HTTP ISV**, qui correspond au cache de fichiers ISV.

   Cette approche configure le client WU pour qu'il effectue des demandes de téléchargement auprès du serveur HTTP indiqué dans la stratégie.

2. **Spécifier localhost**

   Cette approche configure le client WU pour qu'il effectue des demandes de téléchargement auprès du localhost. Cela permet à l'agent client ISV de gérer ces requêtes et de les acheminer comme il convient pour répondre à la demande de téléchargement.

> **Important**
>
> Le cache des fichiers ISV requiert les éléments suivants :
>
> - Le serveur doit être conforme à la norme HTTP 1.1 pour chaque RFC : https://www.rfc-editor.org/rfc/rfc9110.html.
>
>   Plus précisément, le serveur web doit prendre en charge les requêtes HEAD et GET
> - Requêtes de plages partielles
> - Keep-alive
> - Ne pas utiliser Transfer-Encoding:chunked

## Remplir le cache des fichiers ISV

Le cache des fichiers ISV doit être rempli avec les fichiers associés aux mises à jour devant être installées sur les clients gérés.

**Pour remplir le cache des fichiers ISV :**

1. Utilisez les API WSUS pour accéder au chemin d'accès du fichier et au nom de fichier de la mise à jour pour le service MU.

   Les métadonnées de chaque mise à jour effectuée sur le serveur WSUS contiennent le chemin et le nom de fichier de la mise à jour sur Microsoft Update (nom d'hôte Microsoft Update suivi du chemin et du nom de fichier), `https://<microsoft_update_hostname>/<file_path>/<filename>`. Par exemple : `https://download.windowsupdate.com/c/msdownload/update/software/updt/2016/09/windows10.0-kb3195781-x64_0c06079bccc35cba35a48bd2b1ec46f818bd2e74.msu`.

2. Téléchargez des fichiers à partir de Microsoft Update et stockez-les dans le cache de fichiers ISV en utilisant l'une de ces deux méthodes :

   - Stocker des fichiers à l'aide du **même chemin d'accès au dossier que celui du service MU**
   - Stocker des fichiers à l'aide d'un **chemin d'accès au dossier défini par ISV**

     Avoir un serveur HTTP (ou localhost) redirige les requêtes **HTTP GET** , qui référencent le chemin du dossier MU et le nom de fichier, à l'emplacement du fichier ISV.

## Étape 3 : Configurer un agent client ISV pour diriger les opérations du client WU

L'agent client ISV gère le téléchargement et l'installation des mises à jour approuvées à l'aide du flux de travail suivant recommandé :

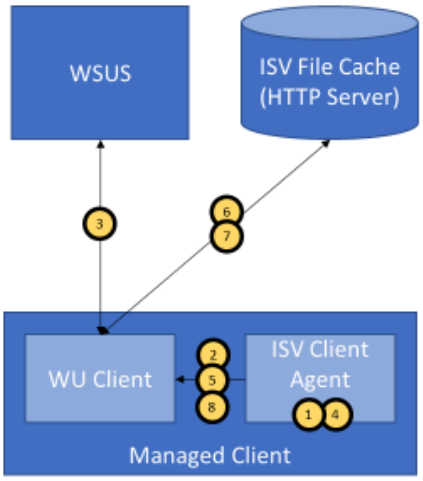
1. L'agent client ISV demande au client WU d'analyser le serveur WSUS
2. L'analyse renvoie l'ensemble des mises à jour applicables au client WU.
3. Le client ISV détermine quelles mises à jour doivent être approuvées et quand les télécharger et les installer.
4. L'agent client ISV demande au client WU de télécharger les mises à jour approuvées
5. Une fois les mises à jour téléchargées, l'agent client ISV demande au client WU pour installer les mises à jour approuvées.

Pour plus d'informations sur l'utilisation du client WU pour l'analyse, le téléchargement et l'installation des mises à jour, Consultez la section Recherche, téléchargement et installation des mises à jour.

## Télécharger les options de flux de travail

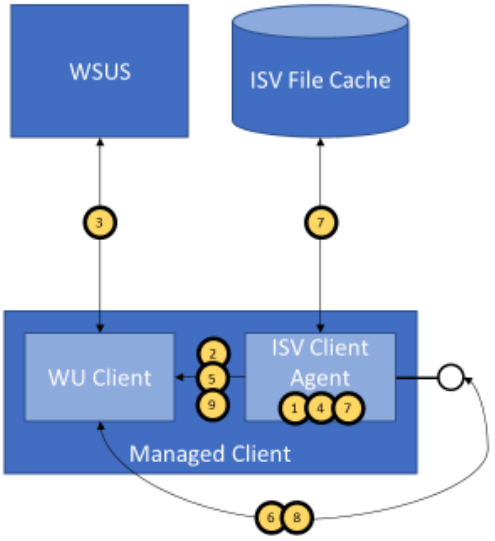
Voici deux illustrations des options de téléchargement de flux de travail à partir d'un cache de fichiers ISV :

### Download from ISV file cache using HTTP server




1. ISV client agent sets alternate download location policy
2. ISV client agent calls WU client to scan for updates
3. WU client scans against WSUS server
4. ISV client agent approves updates
5. ISV client agent calls WU client to download updates
6. WU client uses hostname from alternate download location policy & makes multiple HTTP GET requests to ISV file cache
7. Content downloaded to WU client
8. ISV client agent calls WU client to install updates

### Download from ISV file cache using localhost & ISV client agent




1. ISV client agent sets alternate download location policy (localhost)
2. ISV client agent calls WU client to scan for updates
3. WU client scans against WSUS server
4. ISV client agent approves updates
5. ISV client agent calls WU client to download updates
6. WU client uses hostname from alternate download location policy & makes multiple HTTP GET requests to ISV client agent using localhost
7. ISV client agent gets content from ISV file cache
8. Content downloaded to WU client
9. ISV client agent calls WU client to install updates

## Principe de fonctionnement du téléchargement Express

- Pour les mises à jour du système d'exploitation qui prennent en charge la fonctionnalité Express, deux versions de la charge utile de fichier sont stockées sur le service :
    - **Version complète du fichier :** remplacement des versions locales des fichiers binaires de mise à jour.
    - **Version Express** : contenant les deltas nécessaires pour corriger les fichiers binaires existants sur l'appareil.

      La version complète du fichier et la version Express sont référencées dans les métadonnées de la mise à jour qui ont été téléchargées vers le client lors de la phase d'analyse.

      **Le téléchargement Express fonctionne comme suit :**

      Le client WU tente dans un premier temps de télécharger la version Express et, dans certains cas, il bascule sur la version complète si besoin. Par exemple, le fait de passer par un proxy qui ne prend pas en charge les requêtes de plages d'octets entraîne un basculement vers le téléchargement du fichier complet.

      1. Lorsque le client WU lance un téléchargement Express, **le client WU télécharge tout d'abord un stub** qui fait partie du package Express.
      2. **Le client WU transmet ce stub au programme Windows Installer** qui l'utilise pour générer un inventaire local, en comparant les deltas du fichier sur le périphérique avec ce qui est nécessaire pour accéder à la dernière version du fichier proposé.
      3. Le **programme Windows Installer demande ensuite au client WU de télécharger les plages**, comme déterminé à l'étape précédente.
      4. **Le client WU télécharge ces plages et les transmet au programme Windows Installer**. Ce dernier les applique et détermine ensuite si davantage de plages sont nécessaires. Le client WU répète cette étape jusqu'à ce que le programme Windows Installer indique au client WU que toutes les plages nécessaires ont été téléchargées.

    À ce stade, le téléchargement est terminé et la mise à jour peut être installée.

## Comment l'optimisation de la distribution réduit la consommation de bande passante

L'optimisation de la distribution est une solution de cache distribué avec organisation automatique pour les entreprises cherchant à réduire la consommation de bande passante pour les mises à jour et les mises à niveau du système d'exploitation ainsi que pour les applications. L'optimisation de la distribution permet aux clients de télécharger ces éléments à partir d'autres sources (comme d'autres pairs sur le réseau) avec l'emplacement de téléchargement spécifié (le cache des fichiers ISV dans ce scénario).

Par défaut, dans Windows 10 Entreprise et Windows 10 Education, l'optimisation de la distribution autorise le partage de pair à pair uniquement sur le réseau de l'organisation, mais vous pouvez la configurer différemment en utilisant les paramètres de stratégie de groupe et de gestion des appareils mobiles (GAM).

Pour plus d'informations sur l'optimisation de la distribution, consultez Configurer l'optimisation de la distribution pour les mises à jour de Windows 10.

# Prise en charge par les ISV de la mise à jour delta mensuelle sans WSUS

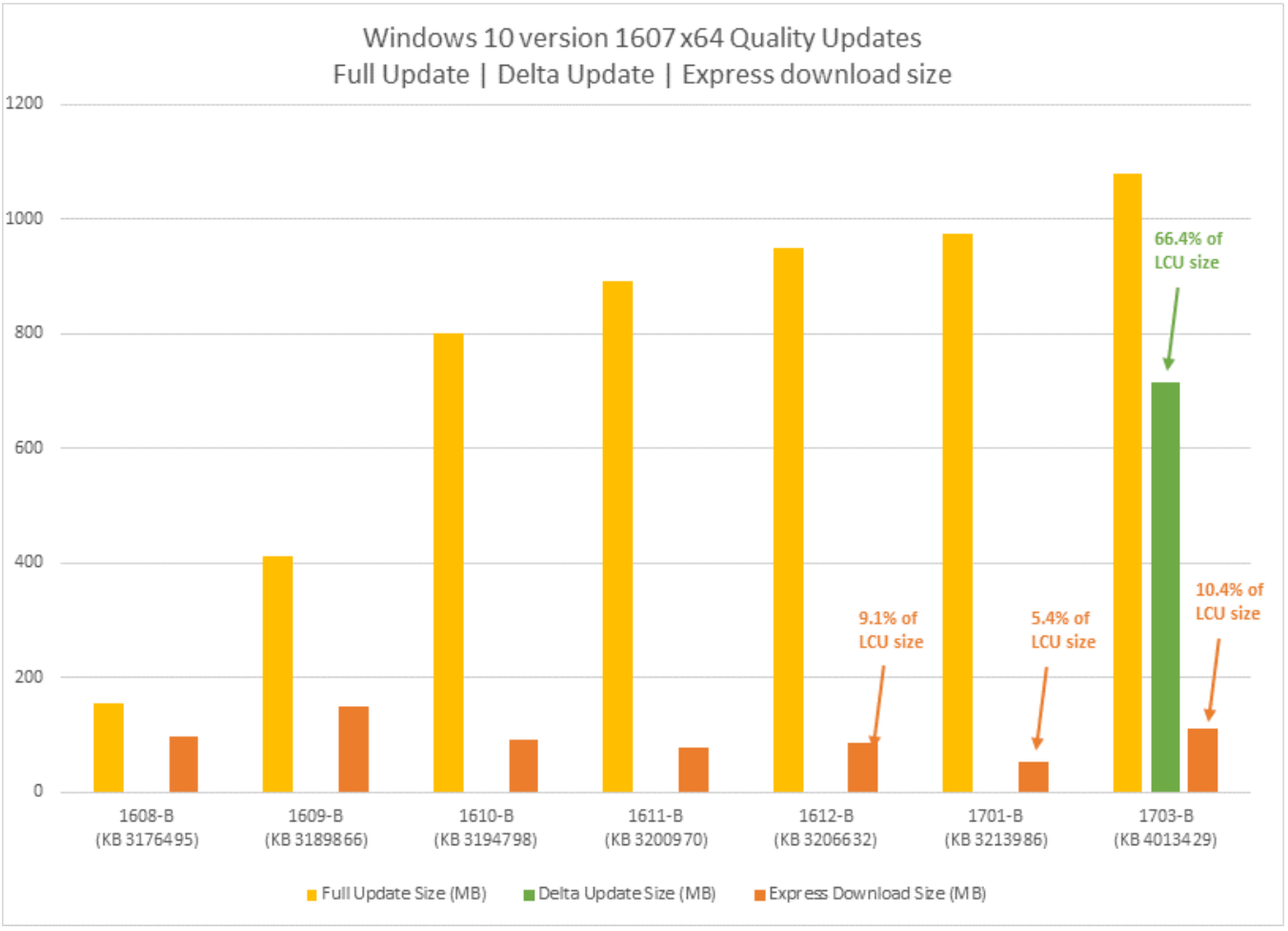
16/08/2025

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

Les téléchargements de Windows 10 Update peuvent être volumineux car, à des fins de cohérence et de simplicité, chaque package contient l'ensemble des correctifs précédemment publiés.

Depuis la version 7, Windows a pu réduire la taille des téléchargements de Windows Update avec une fonctionnalité appelée Express, et bien que les appareils grand public le prennent en charge par défaut, les appareils Windows 10 entreprise nécessitent windows Server Update Services (WSUS) pour tirer parti d'Express. Si Windows Server Update Services (WSUS) est disponible, voir Prise en charge par les ISV de la distribution des mises à jour Express. Nous vous recommandons de l'utiliser pour activer la distribution des mises à jour Express.

Si vous n'avez pas encore installé WSUS mais avez besoin de tailles de package de mise à jour plus petites en attendant, vous pouvez utiliser la mise à jour delta mensuelle. La mise à jour delta réduit considérablement les tailles de package, mais pas autant que la distribution de mises à jour Express WSUS. Nous vous recommandons de déployer la distribution de mises à jour Express WSUS chaque fois que c'est possible pour une plus grande réduction des tailles de package. Vous trouverez ci-dessous un graphique comparatif des tailles de téléchargement delta, cumulative et rapide pour Windows 10 version 1607 :




# Qu’est-ce que la mise à jour delta mensuelle ?

Il existe deux variantes de la mise à jour de sécurité mensuelle : delta et cumulative.

La mise à jour delta mensuelle est une nouveauté et une solution provisoire pour les éditeurs de logiciels indépendants qui ne disposent pas de WSUS pour réduire les tailles de package de mise à jour.

> ⓘ **Important**
>
> **La mise à jour Delta est disponible pour la maintenance de Windows 10, version 1607 (mise à jour anniversaire), version 1703 (Creators Update) et version 1709 (Fall Creators Update).** Pour les mises en production postérieures à la version 1709, vous devez implémenter une infrastructure de déploiement qui prend en charge la distribution de mises à jour pour continuer à profiter des mises à jour incrémentielles.

Avec un mise à jour delta mensuelle, les packages ne contiennent que les mises à jour d’un mois. Une mise à jour cumulative mensuelle contient toutes les mises à jour jusqu’à cette mise en production de mise à jour. Elle produit ainsi un fichier volumineux dont la taille augmente chaque mois. Les mises à jour Delta et mensuelles sont publiées le deuxième mardi de chaque

mois. On les appelle aussi « Update Tuesday ». Le tableau suivant compare les mises à jour delta et cumulatives :

Agrandir le tableau

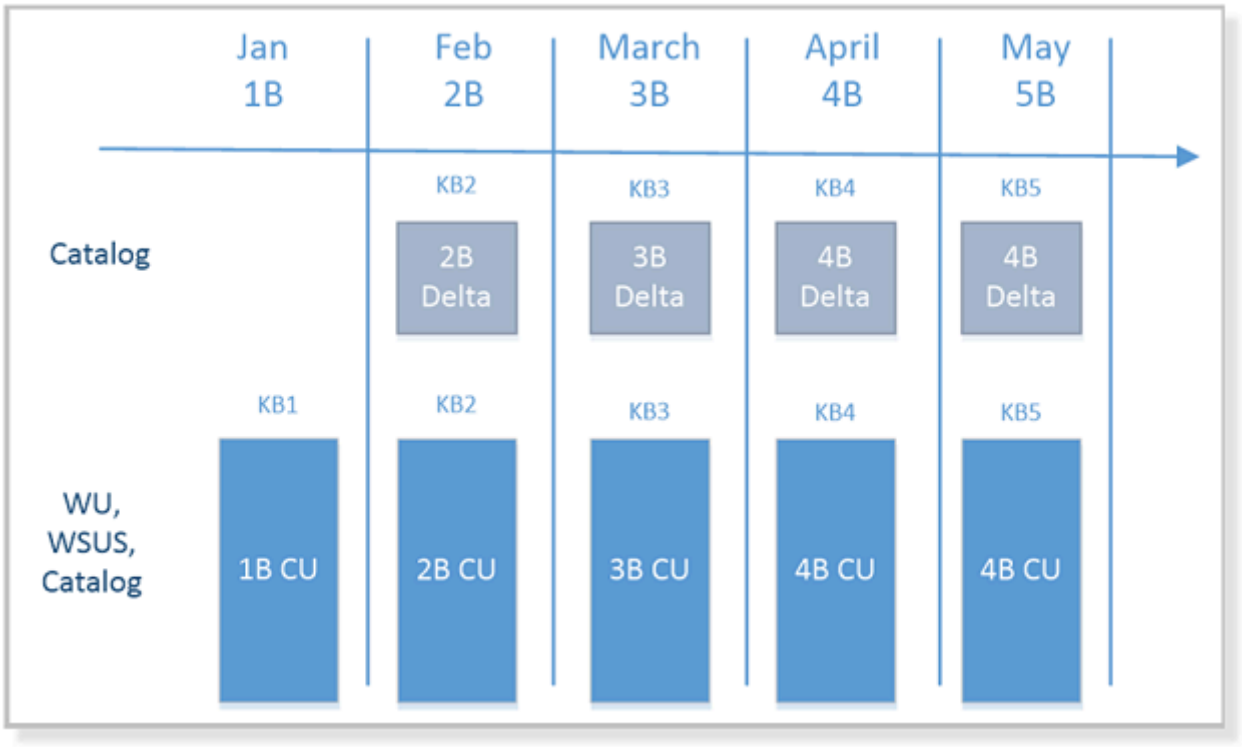
| | **Mise à jour** delta **mensuelle** | **Mise à jour** cumulative **mensuelle** |
|---|---|---|
| **Scope** | Mise à jour unique avec **seulement quelques nouveaux correctifs pour ce mois** | Mise à jour unique avec tous les nouveaux correctifs pour ce mois et tous les mois précédents |
| **Application** | Ne peut être appliqués que si la mise à jour (cumulative ou delta) du mois précédent a été appliquée | Peut être appliquée à tout moment |
| **Delivery** | **Publiée uniquement dans le Catalogue Windows Update** d'où vous pouvez la télécharger pour l'utilisé avec d'autres outils ou processus. Non proposée aux PC connectés à Windows Update | Publiée sur Windows Update (à partir où tous les PC grand public l'installent), dans WSUS et dans le Catalogue Windows Update |

Les mises à jour delta et cumulative ont le même numéro de base de connaissances, avec les mêmes classification et même version en même temps. Vous pouvez différencier les mises à jour par leur titre dans le catalogue ou par le nom de fichier MSU :

- 2017-02 *__*Mise à jour delta*__* pour Windows 10 version 1607 pour systèmes x64 (KB1234567)
- 2017-02 *__*Mise à jour cumulative*__* pour Windows 10 version 1607 pour systèmes x86 (KB1234567)

## Quand utiliser la mise à jour delta mensuelle

Si la taille de la mise à jour de l'appareil client est un souci, nous vous recommandons d'utiliser la mise à jour delta sur des appareils qui disposent de la mise à jour du mois précédent, et la mise à jour cumulative sur des appareils en retard de mise à jour. De cette façon, tous les appareils ne requièrent qu'une seule mise à jour. Cela nécessite un petit ajustement du processus global de gestion des mises à jour, car vous devrez déployer différentes mises à jour en fonction du niveau de mise à jour des appareils dans l'organisation :




## Empêcher le déploiement de mises à jour delta et cumulative au cours du même mois

Étant donné que les mises à jour delta et cumulative sont disponibles en même temps, il est important de comprendre ce qui se passe si vous déployez les deux mises à jour le même mois.

Si vous approuvez et déployez la même version de mises à jour delta cumulative, non seulement vous générez du trafic réseau supplémentaire, car les deux mises à jour sont téléchargées sur le PC, mais il se peut que vous ne puissiez plus redémarrer votre ordinateur sous Windows après le redémarrage.

Si les deux mises à jour delta et cumulative sont installées par inadvertance et que votre ordinateur n'est plus en cours de démarrage, vous pouvez rattraper l'erreur en procédant comme suit :

1. Démarrez dans l'invite de commandes WinRE
2. Répertoriez les packages en état d'attente :

   `x:\windows\system32\dism.exe /image:<drive letter for windows directory> /Get-Packages >> <path to text file>`

   > **Exemple** : `x:\windows\system32\dism.exe /image:c:\ /Get-Packages >> c:\temp\packages.txt`

3. Ouvrez le fichier texte dans lequel vous avez redirigé **get-packages**. Si vous voyez des correctifs en attente d'installation, exécutez **remove-package** pour chaque nom de package :

   ```
   dism.exe /image:<drive letter for windows directory> /remove-package /packagename:<package name>
   ```

   > **Exemple** : `x:\windows\system32\dism.exe /image:c:\ /remove-package /packagename:Package_for_KB4014329~31bf3856ad364e35~amd64~~10.0.1.0`

   > ⓘ **Notes**
   >
   > Ne supprimez pas les correctifs de désinstallation en attente.

> ⓘ **Important**
>
> **La mise à jour Delta est disponible pour la maintenance de Windows 10, version 1607 (mise à jour anniversaire), version 1703 (Creators Update) et version 1709 (Fall Creators Update).** Pour les mises en production postérieures à la version 1709, vous devez implémenter une infrastructure de déploiement qui prend en charge la distribution de mises à jour pour continuer à profiter des mises à jour incrémentielles.

# Migration de la base de données WSUS de WID vers SQL

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

Utilisez les étapes suivantes pour migrer la base de données WSUS (SUSDB) d'une instance Base de données interne Windows vers une instance locale ou distante de SQL Server.

## Prerequisites

- Instance SQL. Il peut s'agir de **MSSQLServer** ou d'une instance personnalisée par défaut.
- SQL Server Management Studio
- WSUS avec le rôle WID installé
- IIS (normalement inclus lorsque vous installez WSUS via le Gestionnaire de serveur). Si ce n'est pas déjà installé, il faut le faire.

## Migration de la base de données WSUS

### Arrêter les services IIS et WSUS sur le serveur WSUS

À partir de PowerShell (avec élévation de privilèges), exécutez :

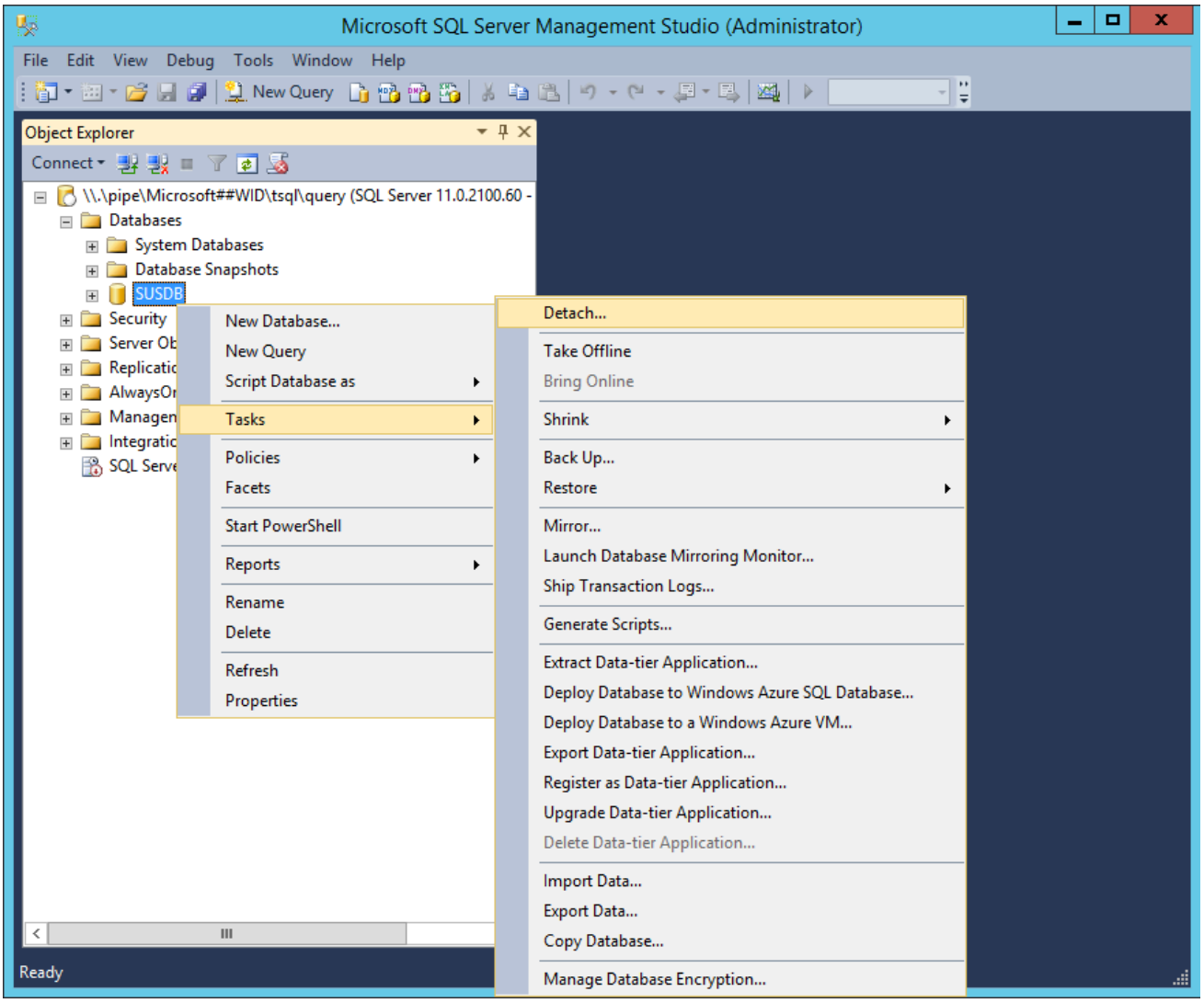
**PowerShell**

```
Stop-Service IISADMIN
Stop-Service WsusService
```

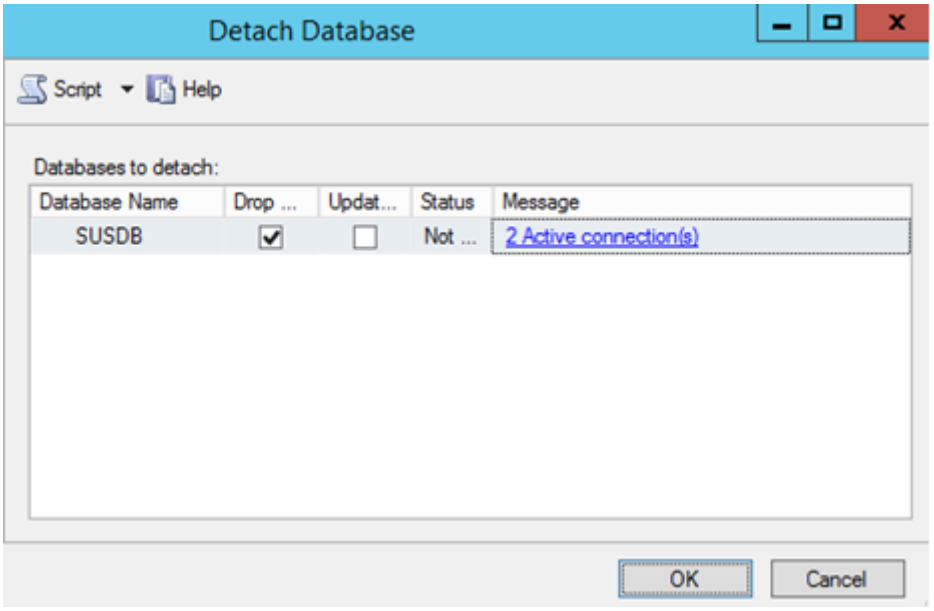
### Détacher SUSDB de la Base de données interne Windows

#### À l'aide de SQL Management Studio

1. Cliquez avec le bouton droit sur **SUSDB** -> -> Cliquez sur **Détacher** :




2. Cochez **Supprimer les connexions existantes**, puis cliquez sur **OK** (facultatif, si des connexions actives existent).




## Utilisation de l'invite de commandes

> **Important**
>
> Ces étapes montrent comment détacher la base de données WSUS (SUSDB) de l'instance de base de données interne Windows à l'aide de l'utilitaire **sqlcmd** . Pour plus d'informations sur l'utilitaire **sqlcmd** , consultez l'utilitaire sqlcmd.
>
> 1. Ouvrez une invite de commandes avec élévation de privilèges
> 2. Exécutez la commande SQL suivante pour détacher la base de données WSUS (SUSDB) de l'instance de base de données interne Windows à l'aide de l'utilitaire **sqlcmd** :

batchfile

```
sqlcmd -S \\.\pipe\Microsoft##WID\tsql\query
use master
GO
alter database SUSDB set single_user with rollback immediate
GO
sp_detach_db SUSDB
GO
```

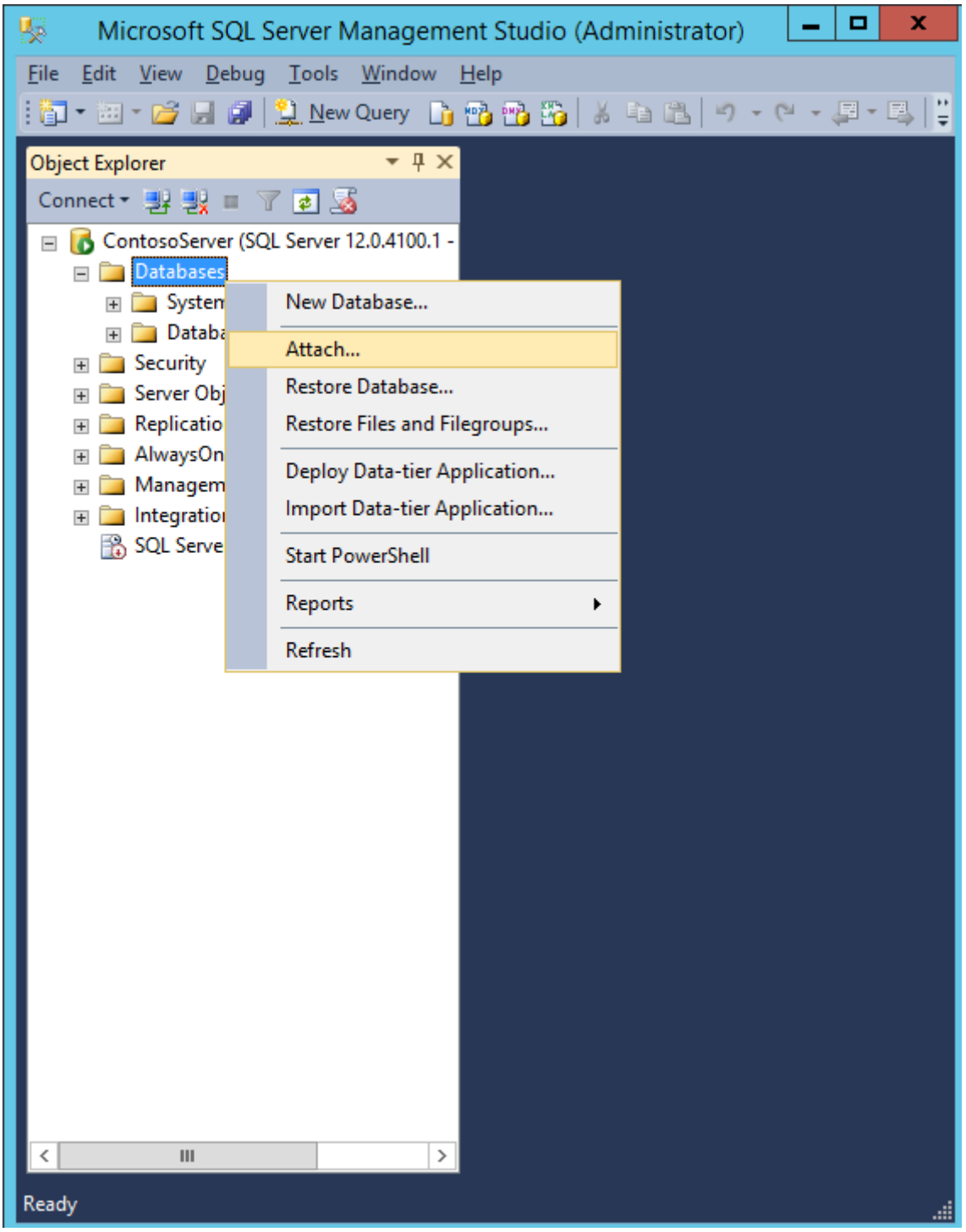
## Copier les fichiers SUSDB sur SQL Server

1. Copiez **SUSDB.mdf** et **SUSDB_log.ldf** à partir du dossier de données WID (**%SystemDrive%\Windows\WID\Data**) dans le dossier de données de l'instance SQL.

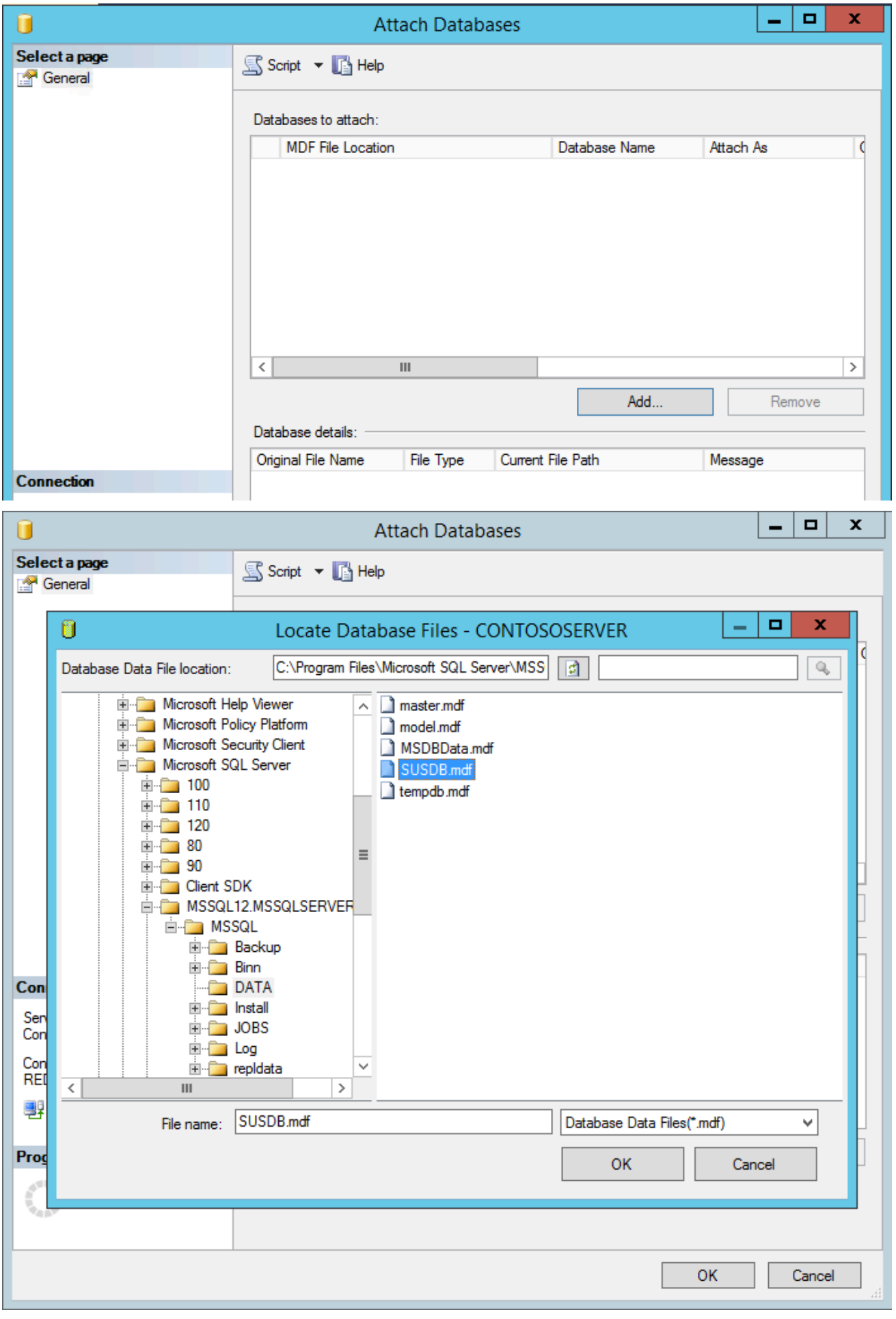
> **Conseil**
>
> Par exemple, si votre dossier d'instance SQL est **C:\Program Files\Microsoft SQL Server\MSSQL12. MSSQLSERVER\MSSQL** et que le dossier de données WID est **C:\Windows\WID\Data,** copiez les fichiers SUSDB à partir de **C:\Windows\WID\Data** vers **C:\Program Files\Microsoft SQL Server\MSSQL12. MSSQLSERVER\MSSQL\Data**

## Attacher SUSDB à l'instance SQL

1. Dans **SQL Server Management Studio**, sous le nœud **Instance**, cliquez avec le bouton droit sur **Bases de données**, puis cliquez sur **Attacher**.




2. Dans la zone **Attacher des bases de données** , sous **Bases de données à joindre**, cliquez sur le bouton **Ajouter** et recherchez le fichier **SUSDB.mdf** (copié à partir du dossier WID), puis cliquez sur **OK**.


Attach Databases
Select a page
General
Script
Help
Databases to attach:
MDF File Location
Database Name
Attach As
Add...
Remove
Database details:
Original File Name
File Type
Current File Path
Message
Connection
Attach Databases
Select a page
General
Script
Help
Locate Database Files - CONTOSOSERVER
Database Data File location:
C:\Program Files\Microsoft SQL Server\MSS
Microsoft Help Viewer
Microsoft Policy Platform
Microsoft Security Client
Microsoft SQL Server
100
110
120
80
90
Client SDK
MSSQL12.MSSQLSERVER
MSSQL
Backup
Binn
DATA
Install
JOBS
Log
repldata
master.mdf
model.mdf
MSDBData.mdf
SUSDB.mdf
tempdb.mdf
File name:
SUSDB.mdf
Database Data Files(*.mdf)
OK
Cancel
OK
Cancel

## Conseil

Cela peut également être effectué à l'aide de Transact-Sql. Consultez la documentation SQL pour attacher une base de données afin de découvrir les instructions appropriées.

Exemple (en utilisant des chemins d'accès de l'exemple précédent) :

SQL

```
   USE master;
   GO
   CREATE DATABASE SUSDB
   ON
       (FILENAME = 'C:\Program Files\Microsoft SQL
Server\MSSQL12.MSSQLSERVER\MSSQL\Data\SUSDB.mdf'),
       (FILENAME = 'C:\Program Files\Microsoft SQL
Server\MSSQL12.MSSQLSERVER\MSSQL\Log\SUSDB_Log.ldf')
       FOR ATTACH;
   GO
```

# Vérifier les autorisations et les connexions pour SQL Server et Base de données

## Autorisations de connexion pour SQL Server

Après avoir attaché SUSDB, vérifiez que **NT AUTHORITY\NETWORK SERVICE** dispose des autorisations de connexion à l'instance de SQL Server en procédant comme suit :

1. Accédez à SQL Server Management Studio
2. Ouvrez l'instance
3. Cliquez sur **Sécurité**
4. Cliquez sur **Connexions**

Le compte **NT AUTHORITY\NETWORK SERVICE** doit être répertorié. Si ce n'est pas le cas, vous devez l'ajouter en utilisant Nouveau nom de connexion.

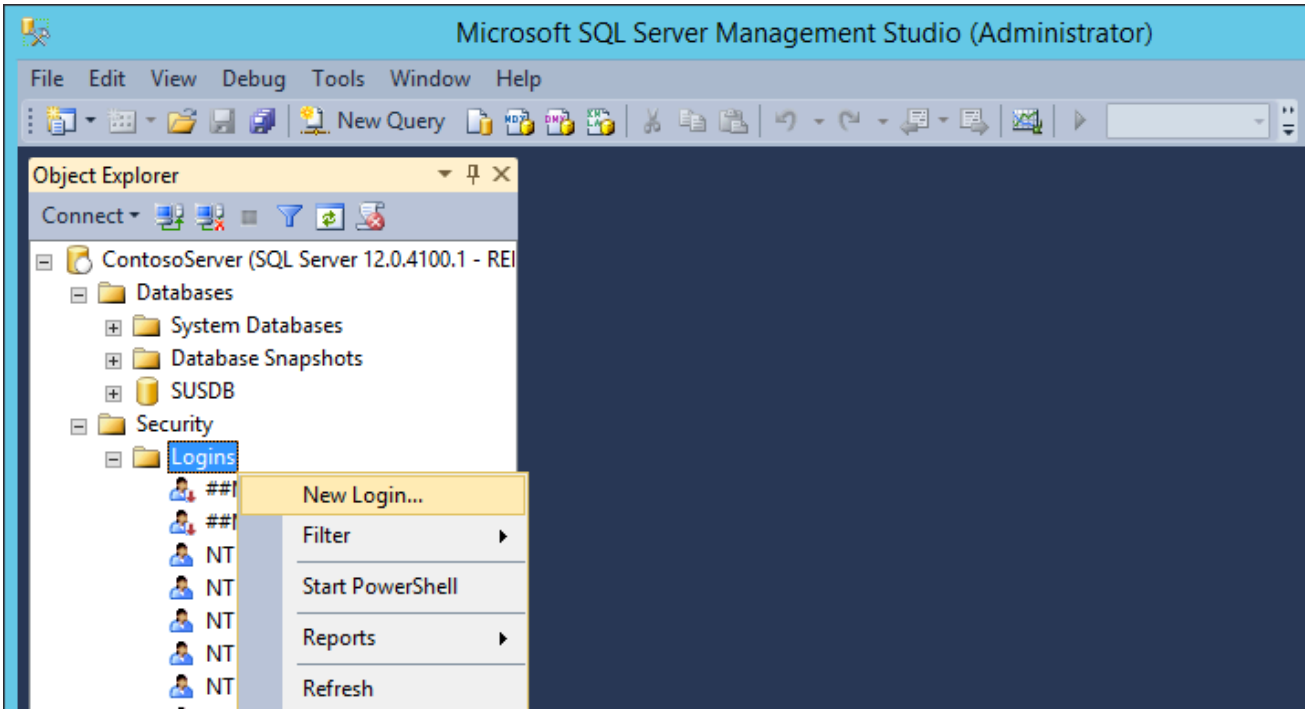
**ⓘ Important**

Si l'instance SQL se trouve sur un ordinateur différent de WSUS, le compte d'ordinateur du serveur WSUS doit être répertorié au format **[FQDN]\[WSUSComputerName]$**. Si ce n'est pas le cas, utilisez les étapes ci-dessous pour l'ajouter, en remplaçant **NT AUTHORITY\NETWORK SERVICE** par le compte d'ordinateur du serveur WSUS (**[FQDN]**

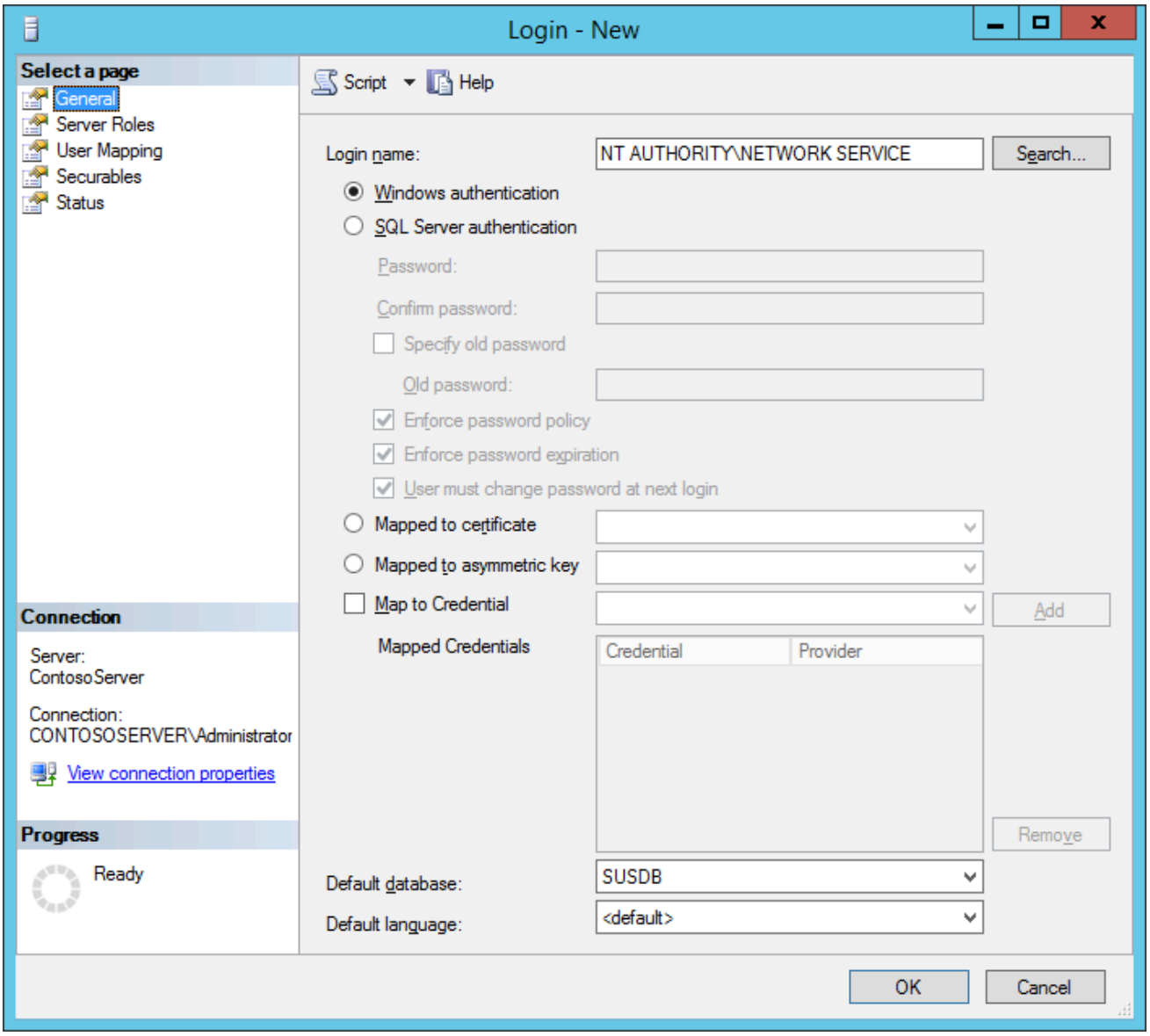
**[WSUSComputerName]$**). Cette procédure ***s'ajoute*** à l'octroi de droits à **NT AUTHORITY\NETWORK SERVICE**

## Ajout de NT AUTHORITY\NETWORK SERVICE et octroi de droits

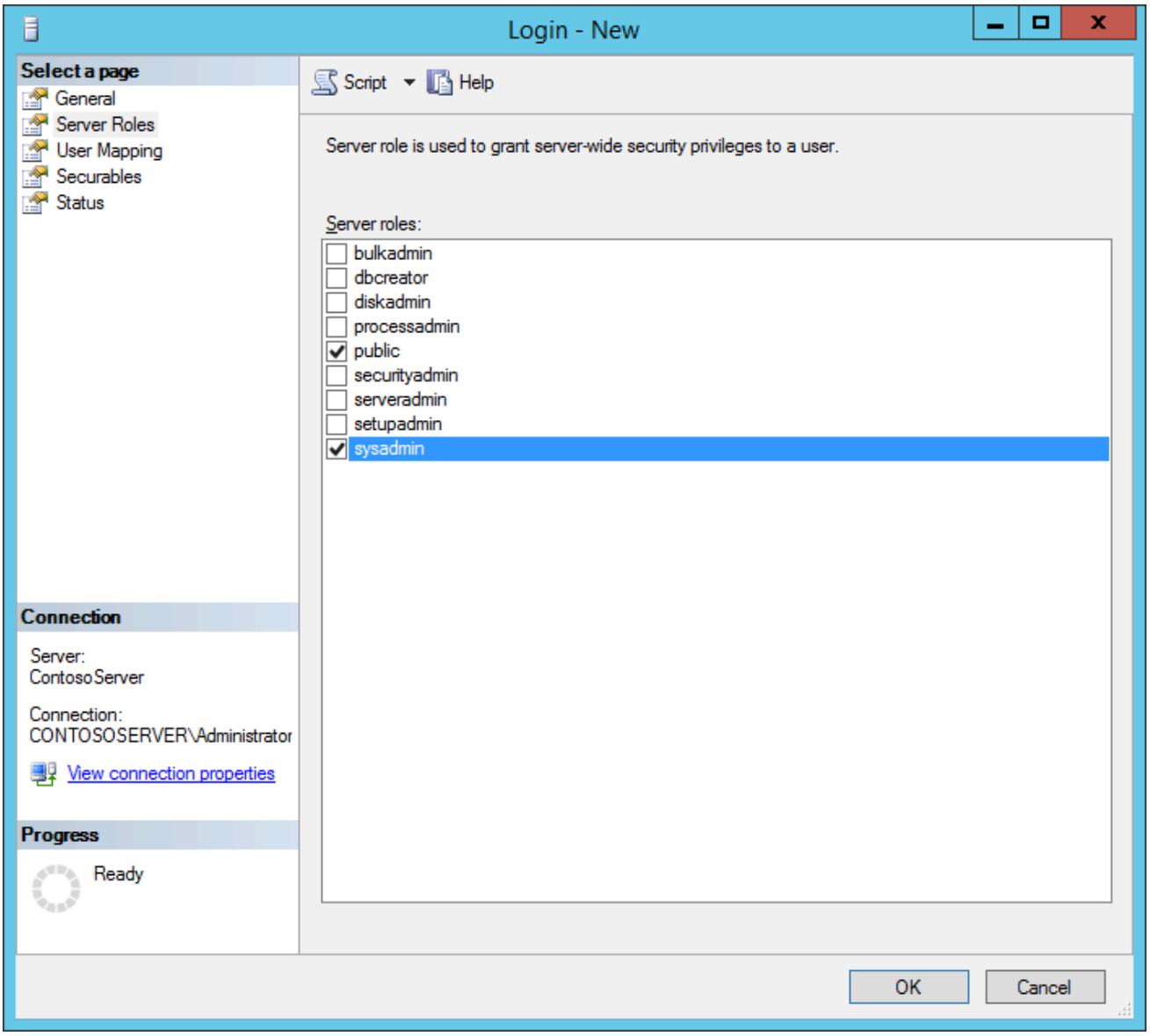
1. Cliquez avec le bouton droit sur **Connexions** , puis cliquez sur **Nouvelle connexion...**




2. Dans la page **Général** , renseignez le **nom** de connexion (**NT AUTHORITY\NETWORK SERVICE**) et définissez la **base de données par défaut** sur SUSDB.




3. Dans la page **Rôles de serveur** , vérifiez que **les administrateurs publics** et **sysadmin** sont sélectionnés.

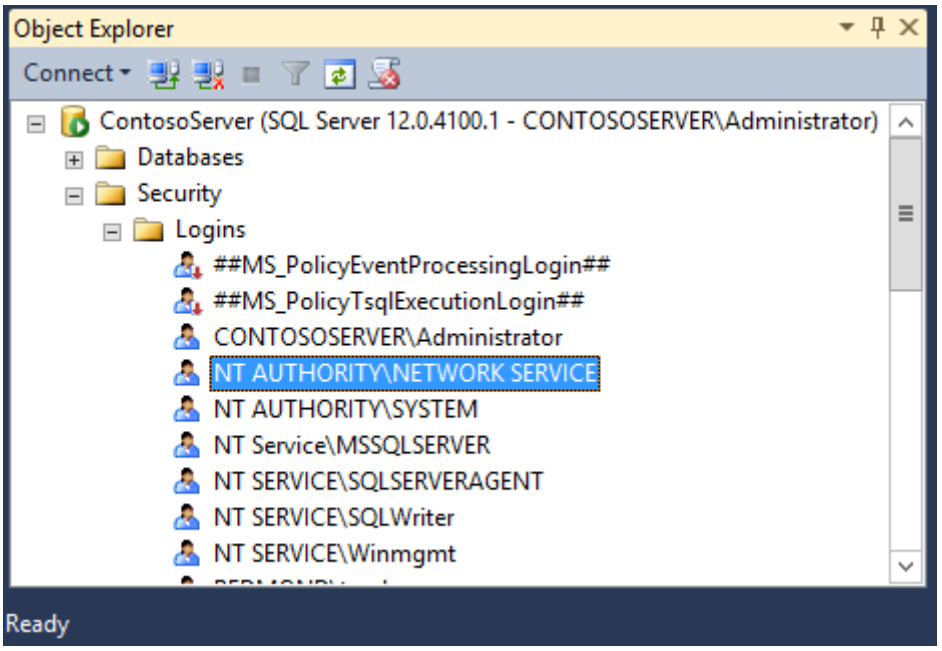



4. Sur la page **Mappage des utilisateurs** :

   - Sous **Utilisateurs mappés à cette connexion** : sélectionnez **SUSDB**
   - Sous **Appartenance au rôle de base de données pour : SUSDB**, vérifiez que les éléments suivants sont cochés :
     - **public**
     - **webService**Capture d'écran de la page Mappage des utilisateurs de la boîte de dialogue Connexion montrant les options publiques et **webService** sélectionnées.

5. Cliquez sur **OK**

Vous devez maintenant voir **NT AUTHORITY\NETWORK SERVICE** sous Connexions.




## Autorisations de base de données

1. Cliquez avec le bouton droit sur SUSDB
2. Sélectionner **les propriétés**
3. Cliquez sur **Autorisations**

Le compte **NT AUTHORITY\NETWORK SERVICE** doit être répertorié.

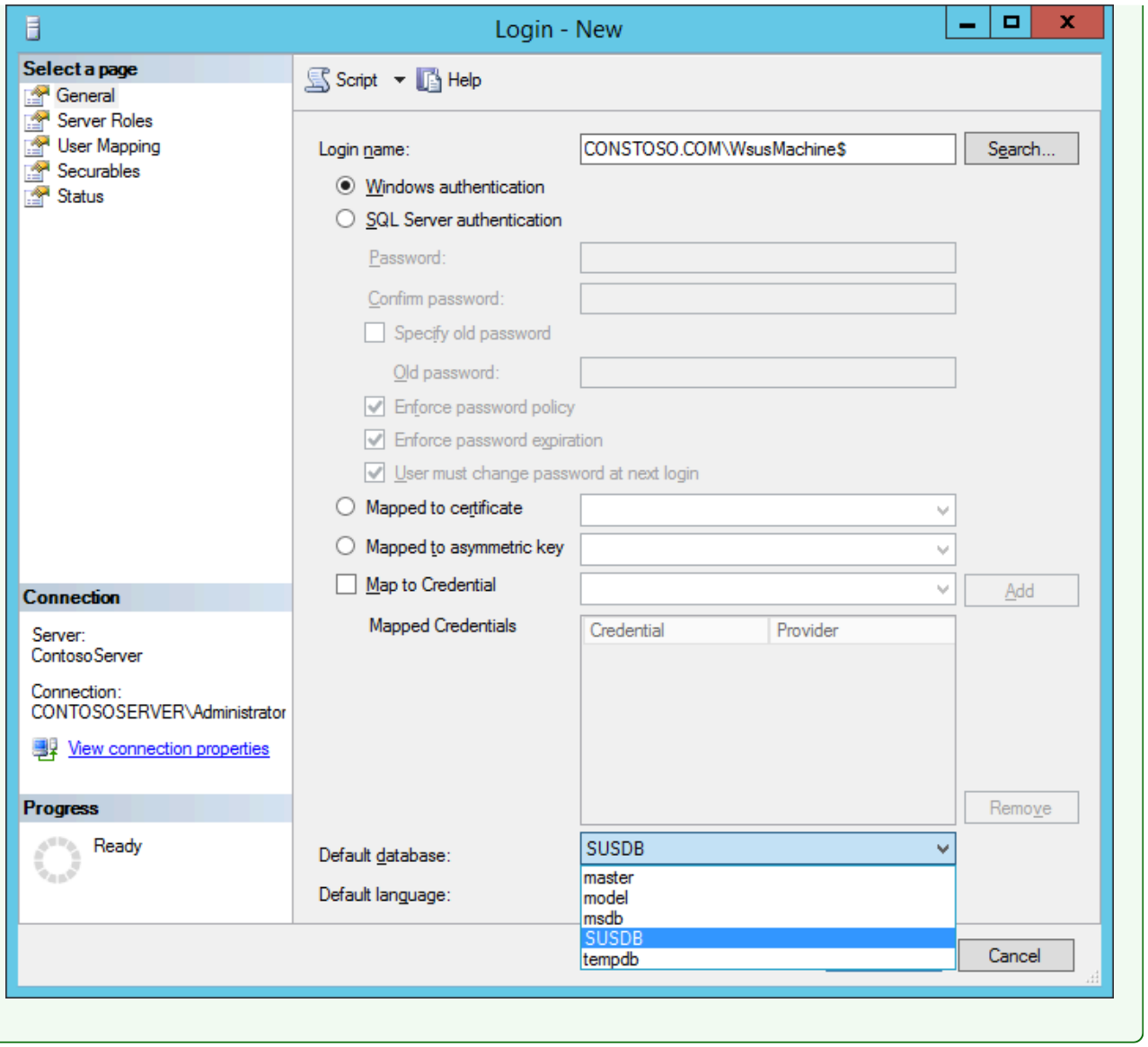
1. Si ce n'est pas le cas, ajoutez le compte.

2. Dans la zone de texte Nom de la connexion, entrez l'ordinateur WSUS au format suivant :

   > [**FQDN]\[WSUSComputerName]$**

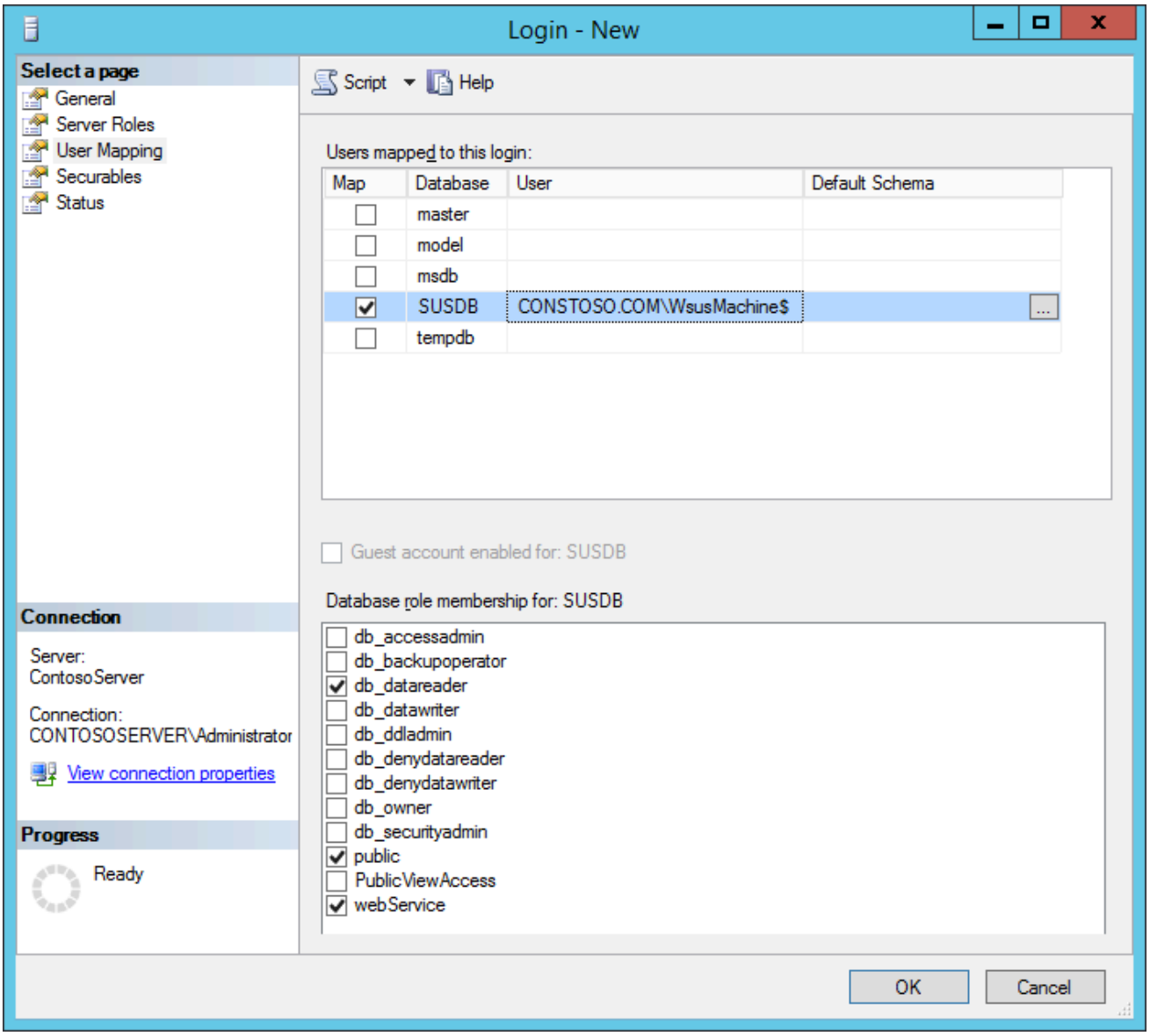
3. Vérifiez que la **base de données par défaut** est définie sur **SUSDB**.

   > **Conseil**
   >
   > Dans l'exemple suivant, le nom de domaine complet est Contosto.com et le nom **de** l'ordinateur WSUS est **WsusMachine** :




4. Dans la page **Mappage des utilisateurs**, sélectionnez la base de données **SUSDB** sous **Utilisateurs associés à cette connexion**

5. Cochez **webService** sous **l'appartenance au rôle de base de données pour : SUSDB** :




6. Cliquez sur **OK** pour enregistrer les paramètres.

> ⓘ **Remarque**
>
> Vous devrez peut-être redémarrer le service SQL pour que les modifications soient appliquées.

## Modifier le registre pour pointer WSUS sur l'instance SQL Server

> ⓘ **Important**
>
> Suivez attentivement les étapes décrites dans cette section. En effet, toute erreur de modification peut être à l'origine de problèmes graves. Avant de le modifier, sauvegardez le

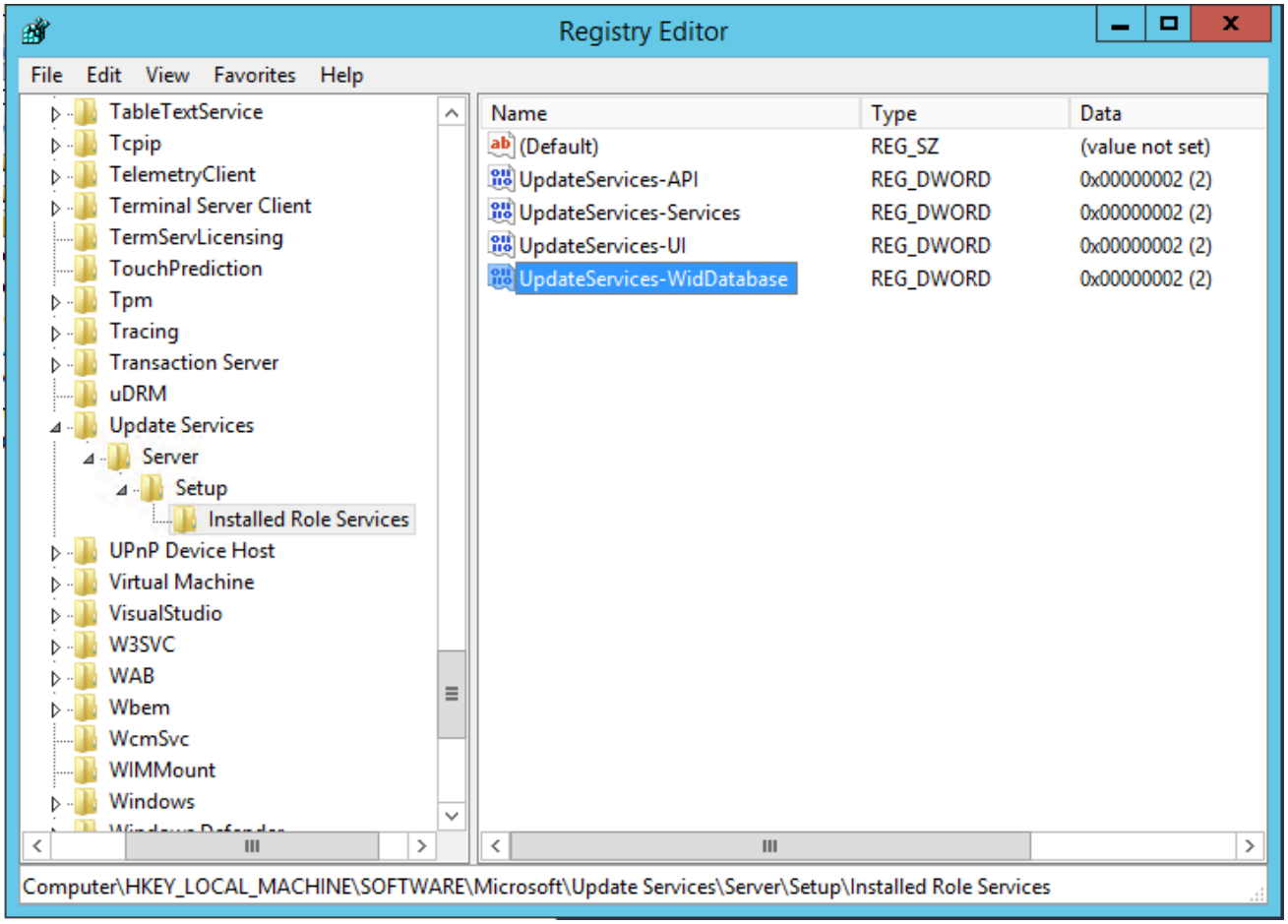
Registre afin de pouvoir le restaurer en cas de problème.

1. Cliquez sur **Démarrer**, sur **Exécuter**, tapez **regedit**, puis cliquez sur **OK**.

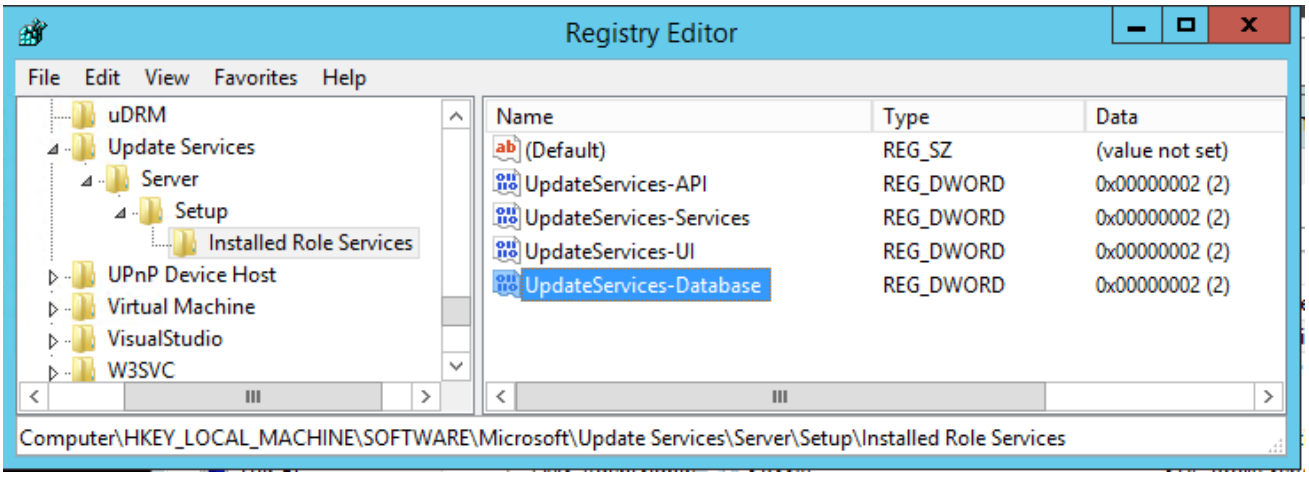
2. Recherchez la clé suivante : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\UpdateServices\Server\Setup\SqlServerName**

3. Dans la zone de texte **Valeur** , tapez **[ServerName]\[InstanceName]**, puis cliquez sur **OK**. Si le nom de l'instance est l'instance par défaut, tapez **[ServerName]**.

4. Recherchez la clé suivante : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Update Services\Server\Setup\Installed Role Services\UpdateServices-WidDatabase**



5. Renommez la clé en **UpdateServices-Database**




> ⓘ **Remarque**
>
> Si vous ne mettez pas à jour cette clé, **WsusUtil** tente de traiter le WID plutôt que l'instance SQL vers laquelle vous avez migré.

## Démarrer les services IIS et WSUS sur le serveur WSUS

À partir de PowerShell (avec élévation de privilèges), exécutez :

**PowerShell**

```
Start-Service IISADMIN
Start-Service WsusService
```

> ⓘ **Remarque**
>
> Si vous utilisez la console WSUS, fermez-la et redémarrez-la.

Si vous avez migré la base de données WSUS vers un SQL Server distant, sécurisez la connexion en activant SQL Server Extended Protection for Authentication (EPA). Pour plus d'informations, voir Sécuriser la connexion SQL Server.

# Désinstallation du rôle WID (non recommandée)

> ⚠ **Avertissement**

La suppression du rôle WID supprime également un dossier de base de données (**%SystemDrive%\Program Files\Update Services\Database**) qui contient les scripts requis par WSUSUtil.exe pour les tâches post-installation. Si vous choisissez de désinstaller le rôle WID, veillez à sauvegarder le dossier **%SystemDrive%\Program Files\Update Services\Database** au préalable.

Utilisation de PowerShell :

**PowerShell**

```powershell
Uninstall-WindowsFeature -Name 'Windows-Internal-Database'
```

Une fois le rôle WID supprimé, vérifiez que la clé de registre suivante est présente : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Update Services\Server\Setup\Installed Role Services\UpdateServices-Database**

---

Last updated on 28/07/2026

# Modifications apportées à la console Windows dans Windows Server

08/08/2025

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

À compter de Windows Server 2016, l'hôte de la console (le code sous-jacent qui prend en charge toutes les applications en mode caractère, notamment l'invite de commandes Windows et l'invite Windows PowerShell, entre autres) a été mis à jour de plusieurs manières pour ajouter un grand nombre de nouvelles fonctionnalités.

## Contrôle des nouvelles fonctionnalités

La nouvelle fonctionnalité est activée par défaut, mais vous pouvez activer et désactiver chacune des nouvelles fonctionnalités ou revenir à l'hôte de console précédent via l'interface Propriétés (principalement sous l'onglet **Options** ) ou avec ces clés de Registre (toutes les clés sont des valeurs DWORD sous `HKEY_CURRENT_USER\Console`) :

Agrandir le tableau

| Clé du Registre | Description |
|---|---|
| ForceV2 | 1 active toutes les nouvelles fonctionnalités de la console ; 0 désactive toutes les nouvelles fonctionnalités. Remarque : Cette valeur n'est pas stockée dans les raccourcis, mais uniquement dans cette clé de Registre. |
| LineSelection | 1 active la sélection de ligne ; 0 pour utiliser uniquement le mode bloc |
| FilterOnPaste | 1 active le nouveau comportement de collage |
| LineWrap | 1 renvoie le texte à la ligne quand vous redimensionnez les fenêtres de la console |
| CtrlKeyShortcutsDisabled | 0 active de nouveaux raccourcis ; 1 les désactive |
| Clés étenduesEdit | 1 active l'ensemble des touches de sélection ; 0 les désactive |
| TrimLeadingZeros | 1 supprime les zéros non significatifs dans les sélections effectuées par un double-clic ; 0 conserve les zéros non significatifs |
| WindowsAlpha | Définit la valeur d'opacité entre 30 % et 100 %. Utilisez 0x4C à 0xFF ou 76 à 255 pour spécifier la valeur |
| WordDelimiters | Définit le caractère qui est utilisé pour passer d'un mot à l'autre quand vous sélectionnez un texte par mot entier à l'aide de Ctrl+Maj+touche de direction |

| Clé du Registre | Description |
| --- | --- |
| | (la valeur par défaut est l'espace). Définissez cette valeur REG_SZ pour contenir tous les caractères qui doivent être traités comme délimiteurs. Remarque : Cette valeur n'est pas stockée dans les raccourcis, mais uniquement dans cette clé de Registre. |

Ces paramètres sont stockés par titre de chaque fenêtre dans le Registre sous HKCU\Console. Les fenêtres de la console ouvertes par un raccourci ont ces paramètres stockés dans le raccourci ; si le raccourci est copié vers un autre ordinateur, les paramètres sont aussi déplacés vers le nouvel ordinateur. Les paramètres des raccourcis remplacent tous les autres paramètres, dont les valeurs par défaut et les paramètres globaux. Toutefois, si vous revenez à la console d'origine à l'aide de l'option **Utiliser l'ancienne console** sous l'onglet **Options**, ce paramètre est global et conservé pour toutes les fenêtres par la suite, notamment après le redémarrage de l'ordinateur.

Vous pouvez préconfigurer ces paramètres ou créer des scripts pour ceux-ci en configurant le Registre de manière appropriée dans un fichier d'installation sans assistance ou avec Windows PowerShell.

Les applications 16 bits NTVDM reviennent toujours à l'hôte de la console plus ancien.

> ⓘ **Notes**
>
> Si vous rencontrez des problèmes avec les nouveaux paramètres de la console et que vous ne pouvez pas les résoudre avec les options spécifiques répertoriées ici, vous pouvez toujours revenir à la console d'origine en affectant la valeur 0 à ForceV2 ou en utilisant **Utiliser l'ancienne console** sous l'onglet **Options**.

# Comportement de la console

Vous pouvez désormais redimensionner la fenêtre de console à volonté en saisissant un bord à l'aide de la souris et en le faisant glisser. Les barres de défilement s'affichent uniquement si vous définissez manuellement les dimensions de la fenêtre (à l'aide de l'onglet **Disposition** dans **Propriétés**) ou si la ligne de texte la plus longue dans la mémoire tampon est plus large que la taille actuelle de la fenêtre.

La nouvelle fenêtre de console prend désormais en charge le retour automatique à la ligne. Toutefois, si vous avez utilisé les API de console pour modifier le texte dans une mémoire tampon, la console laisse le texte tel qu'il a été inséré.

Les fenêtres de console peuvent maintenant être semi-transparentes (pour une transparence minimale de 30 %). Vous pouvez ajuster la transparence dans le menu Propriétés ou avec les commandes de clavier suivantes :

Agrandir le tableau

| Pour ce faire : | Utilisez cette combinaison de touches : |
|---|---|
| Augmenter la transparence | Ctrl+Maj+signe plus (+) ou Ctrl+Maj+défilement vers le haut avec la souris |
| Réduire la transparence | Ctrl+Maj+signe moins (-) ou Ctrl+Maj+défilement vers le bas avec la souris |
| Activer/désactiver le mode plein écran | Alt+Entrée |

# Selection

Il existe de nombreuses nouvelles options pour la sélection de texte et des lignes, ainsi que pour le marquage de texte et l'utilisation de l'historique de la mémoire tampon. La console tente d'éviter les conflits avec les applications qui peuvent utiliser les mêmes touches.

## Pour les développeurs

si un conflit se produit, vous pouvez généralement contrôler le comportement de l'application quand elle utilise l'entrée de ligne, l'entrée traitée et les modes d'entrée d'écho avec l'API SetConsoleMode(). Si le mode d'exécution est l'entrée traitée, les raccourcis ci-dessous s'appliquent mais, dans d'autres modes, votre application doit les gérer. Les combinaisons de touches non répertoriées ici fonctionnent comme dans les versions précédentes de la console. Vous pouvez également essayer de résoudre les conflits avec différents paramètres sous l'onglet **Options** . Si tout le reste échoue, vous pouvez toujours revenir à la console d'origine.

Vous pouvez maintenant utiliser la sélection « cliquer et faire glisser » en dehors du mode d'édition rapide et cette sélection permet de sélectionner du texte sur plusieurs lignes, comme dans le Bloc-notes, et non juste un bloc rectangulaire. Les opérations de copie ne nécessitent plus de supprimer les sauts de ligne. En plus de la sélection « cliquer et faire glisser », les combinaisons de touches suivantes sont disponibles :

## Sélection de texte

Agrandir le tableau

| **Pour ce faire :** | **Utilisez cette combinaison de touches :** |
|---|---|
| Déplacer le curseur d'un caractère vers la gauche, ce qui étend la sélection | Maj+Flèche gauche |
| Déplacer le curseur d'un caractère vers la droite, ce qui étend la sélection | Maj+Flèche droite |
| Sélectionner le texte ligne par ligne vers le haut à partir du point d'insertion | Maj+Flèche vers le haut |
| Étendre la sélection de texte d'une ligne vers le bas à partir du point d'insertion | Maj+Flèche vers le bas |
| Si le curseur se trouve sur la ligne en cours de modification, utilisez une fois cette commande pour étendre la sélection jusqu'au dernier caractère de la ligne d'entrée. Utilisez-la une deuxième fois pour étendre la sélection jusqu'à la marge droite. | SHIFT+END |
| Si le curseur **n'est pas** dans la ligne en cours de modification, utilisez cette commande pour sélectionner tout le texte du point d'insertion vers la marge droite. | SHIFT+END |
| Si le curseur se trouve sur la ligne en cours de modification, utilisez une fois cette commande pour étendre la sélection jusqu'au caractère immédiatement après l'invite de commandes. Utilisez-la une deuxième fois pour étendre la sélection jusqu'à la marge droite. | SHIFT+HOME |
| Si le curseur **n'est pas** dans la ligne en cours de modification, utilisez cette commande pour étendre la sélection à la marge gauche. | SHIFT+HOME |
| Étendre la sélection d'un écran vers le bas | MAJ+PAGE VERS LE BAS |
| Étendre la sélection d'un écran vers le haut | MAJ+PAGE PRÉCÉDENTE |
| Étendre la sélection d'un mot vers la droite. (Vous pouvez définir les délimiteurs de mot avec la clé de Registre WordDelimiters.) | Ctrl+Maj+Droite |
| Étendre la sélection d'un mot vers la gauche | CTRL+SHIFT+HOME |
| Étendre la sélection au début de la mémoire tampon d'écran | CTRL+SHIFT+END |
| Sélectionner tout le texte après l'invite, si le curseur se trouve sur la ligne active et que la ligne n'est pas vide | CTRL+A |
| Sélectionnez l'intégralité de la mémoire tampon, si le curseur **n'est pas** dans la ligne actuelle | CTRL+A |

## Modification du texte

Vous pouvez copier et coller du texte dans la console à l'aide des commandes du clavier. Ctrl+C remplit maintenant deux fonctions. Si aucun texte n'est sélectionné quand vous l'utilisez, cette combinaison envoie la commande BREAK comme d'habitude. Si du texte est sélectionné, la première utilisation copie le texte et efface la sélection ; la deuxième utilisation envoie BREAK. Voici les autres commandes de modification :

Agrandir le tableau

| **Pour ce faire :** | **Utilisez cette combinaison de touches :** |
|---|---|
| Coller du texte dans la ligne de commande | CTRL+V |
| Copier le texte sélectionné dans le Presse-papiers | Ctrl+Ins |
| Copier le texte sélectionné dans le Presse-papiers ; envoyer BREAK | CTRL+C |
| Coller du texte dans la ligne de commande | Maj+Ins |

## Mode de marquage

Pour entrer le mode marque à tout moment, cliquez avec le bouton droit n'importe où dans la barre de titre de la console, pointez sur **Modifier**, puis sélectionnez **Marquer** dans le menu qui s'ouvre. Vous pouvez également utiliser Ctrl+M. En mode marquage, utilisez la touche Alt pour identifier le début d'une sélection du retour automatique à la ligne. (Si l'option **Activer la sélection du retour automatique à la ligne** est désactivée, le mode marquage sélectionne le texte dans un bloc.) En mode marquage, utilisez Ctrl+Maj+touche de direction pour une sélection par caractère et non par mot comme en mode normal. Outre les touches de sélection de la section **Édition de texte** , ces combinaisons sont disponibles en mode marque :

Agrandir le tableau

| **Pour ce faire :** | **Utilisez cette combinaison de touches :** |
|---|---|
| Passer en mode marquage pour déplacer le curseur dans la fenêtre | CTRL+M |
| Commencer la sélection du retour automatique à la ligne en mode marquage, avec d'autres combinaisons de touches | ALT |
| Déplacer le curseur dans la direction spécifiée | Touches de direction |
| Déplacer le curseur d'une page dans la direction spécifiée | Touches Page |
| Déplacer le curseur au début de la mémoire tampon | CTRL+HOME |

| Pour ce faire : | Utilisez cette combinaison de touches : |
| --- | --- |
| Déplacer le curseur à la fin de la mémoire tampon | CTRL+END |

## Navigation dans l'historique

Agrandir le tableau

| Pour ce faire : | Utilisez cette combinaison de touches : |
| --- | --- |
| Monter d'une ligne dans l'historique de sortie | CTRL+FLÈCHE DU HAUT |
| Descendre d'une ligne dans l'historique de sortie | CTRL+FLÈCHE DU BAS |
| Déplacer la fenêtre d'affichage en haut de la mémoire tampon (si la ligne de commande est vide) ou supprimer tous les caractères à gauche du curseur (si la ligne de commande n'est pas vide) | CTRL+HOME |
| Déplacer la fenêtre d'affichage vers la ligne de commande (si la ligne de commande est vide) ou supprimer tous les caractères à droite du curseur (si la ligne de commande n'est pas vide) | CTRL+END |

## Commandes de clavier supplémentaires

Agrandir le tableau

| Pour ce faire : | Utilisez cette combinaison de touches : |
| --- | --- |
| Ouvrir la boîte de dialogue Rechercher | CTRL+F |
| Fermer la fenêtre de la console | ALT+F4 |

# Qu’est-ce que System Insights ?

16/08/2025S’applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

System Insights apporte des analyses prédictives à Windows Server, ce qui vous permet de prévoir et de gérer les ressources du serveur de manière proactive. En analysant les données système locales avec des modèles Machine Learning, System Insights vous aide à anticiper les problèmes potentiels et à optimiser l’utilisation des ressources, ce qui réduit la nécessité de résoudre les problèmes réactifs. Cette vue d’ensemble explique comment System Insights fonctionne, ses fonctionnalités clés et comment vous pouvez l’utiliser pour améliorer la gestion des serveurs.

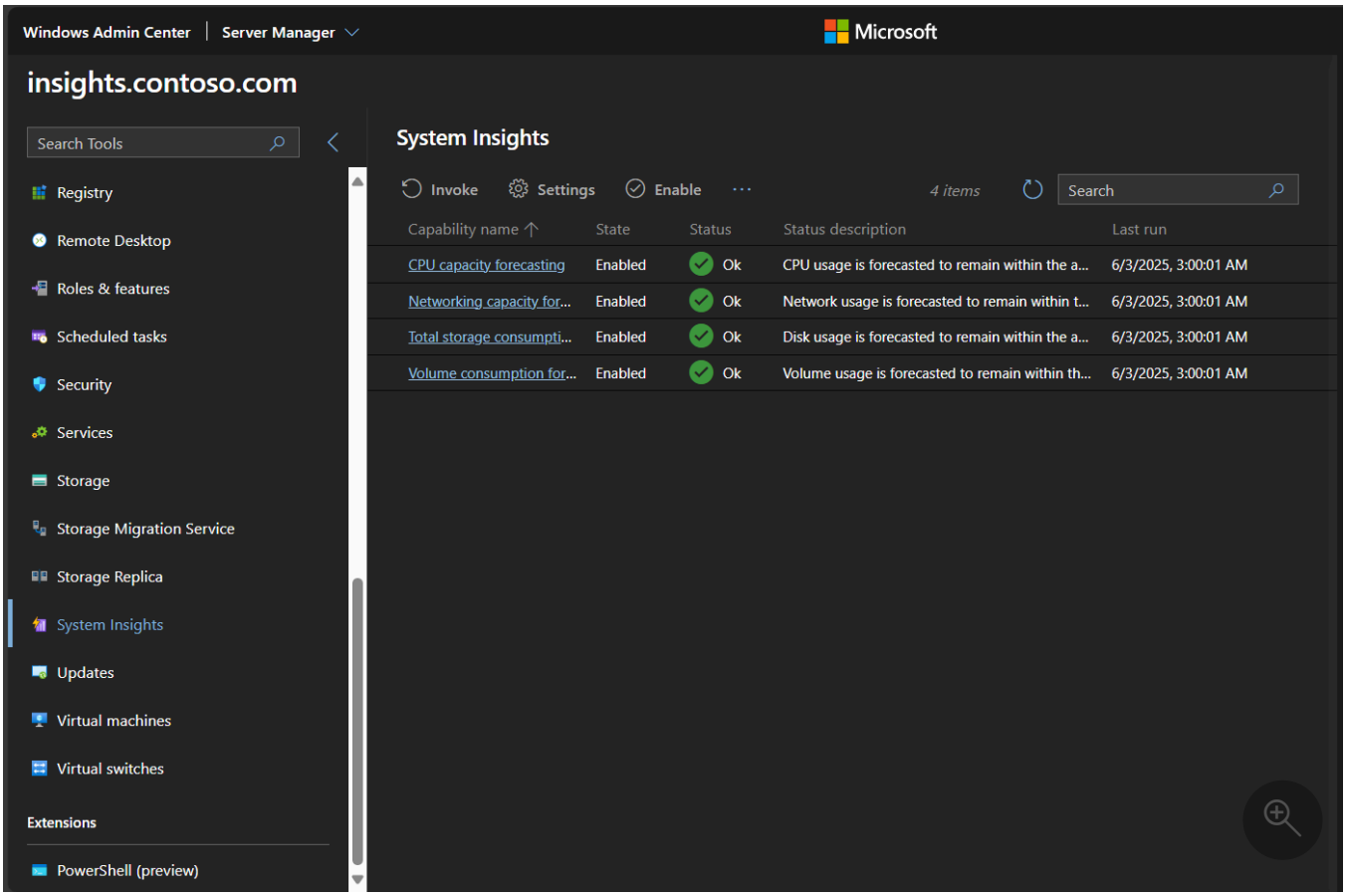
System Insights est disponible sur Windows Server 2019 et versions ultérieures. Il s’exécute sur des ordinateurs hôtes et invités, sur n’importe quel hyperviseur et dans n’importe quel cloud.

System Insights est préinstallé sur Windows Server.

## Fonctionnalités disponibles

System Insights fournit quatre fonctionnalités activées par défaut :

- Prévision de la capacité du processeur : prévision de l’utilisation du processeur.
- Prévision de la capacité de mise en réseau : prévision de l’utilisation du réseau pour chaque carte réseau.
- Prévision totale de la consommation de stockage : prévision de la consommation totale de stockage sur tous les lecteurs locaux.
- Prévision de la consommation en volume : prévision de la consommation de stockage pour chaque volume.




System Insights dispose également d'une infrastructure extensible, de sorte que Microsoft et les tiers peuvent ajouter de nouvelles fonctionnalités prédictives à System Insights sans mettre à jour le système d'exploitation.

## Gérer System Insights

Vous pouvez gérer System Insights via Windows Admin Center ou directement via PowerShell. Configurez chaque fonctionnalité prédictive séparément en fonction des besoins de votre déploiement. Tous les résultats de prédiction sont publiés dans le journal des événements. Vous pouvez donc utiliser Azure Monitor ou System Center Operations Manager pour agréger et afficher facilement les prédictions sur un groupe de machines.

## Fonctionnalités locales de System Insights

System Insights s'exécute complètement localement sur Windows Server. Toutes vos données sont collectées, conservées et analysées directement sur votre machine, afin que vous puissiez réaliser des fonctionnalités d'analyse prédictive sans aucune connectivité cloud.

Vos données système sont stockées sur votre machine, et ces données sont analysées par des fonctionnalités prédictives qui ne nécessitent pas de reformation dans le cloud. Avec System Insights, vous pouvez conserver vos données sur votre machine et bénéficier toujours des fonctionnalités d'analytique prédictive.

# Contenu connexe

Pour en savoir plus sur Insights système, utilisez les ressources suivantes :

- Comprendre les fonctionnalités
- Gérer les fonctionnalités
- Ajouter et développer des fonctionnalités
- System Insights FAQ

# Fonctionnalités System Insights dans Windows Server

16/08/2025S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

Les fonctionnalités System Insights de Windows Server utilisent l'analytique prédictive pour aider les administrateurs à prévoir l'utilisation des ressources et à optimiser les performances du serveur. Cet article explique les fonctionnalités par défaut, les modèles de prédiction et comment interpréter leurs résultats.

Cet article décrit également les sources de données, les chronologies de prédiction et les états de prédiction utilisés pour les fonctionnalités par défaut.

## Vue d'ensemble des fonctionnalités System Insights

Une fonctionnalité System Insights est un modèle d'apprentissage automatique ou de statistiques qui analyse les données système pour vous donner plus d'informations sur votre déploiement. System Insights inclut un ensemble de fonctionnalités par défaut et vous pouvez ajouter de nouvelles fonctionnalités dynamiquement sans mettre à jour le système d'exploitation.

Les quatre fonctionnalités par défaut disponibles sont les suivantes :

- **Prévision de la capacité du processeur**
- **Prévision de la capacité de mise en réseau**
- **Prévision totale de la consommation de stockage**
- **Prévision de la consommation en volume**

Chaque fonctionnalité s'exécute localement sur une instance Windows Server, et vous pouvez gérer chaque fonctionnalité individuellement.

Chaque fonctionnalité analyse les données historiques pour prédire l'utilisation future, et **toutes les fonctionnalités de prévision sont conçues pour prévoir les tendances à long terme plutôt que les comportements à court terme**, ce qui aide les administrateurs à approvisionner correctement le matériel et à régler leurs charges de travail afin d'éviter les conflits de ressources futurs. Étant donné que ces fonctionnalités se concentrent sur l'utilisation à long terme, elles analysent les données quotidiennes.

## Sorties de capacité

Lorsque vous exécutez une fonctionnalité, elle fournit une sortie qui explique le résultat de son analyse ou de sa prédiction. Chaque sortie inclut un **état** et une **description d'état** pour décrire la prédiction. Chaque résultat peut également inclure des données spécifiques aux capacités liées à la prédiction. La **description de l'état** donne un contexte pour **l'état** et les fonctionnalités indiquent un état **OK**, **Avertissement** ou **Critique** . Une fonctionnalité peut également utiliser un état **d'erreur** ou **aucun** s'il n'effectue pas de prédiction. Voici les états des fonctionnalités et leurs significations de base :

- **Ok** - Tout semble bon.
- **Avertissement** - Aucune attention immédiate requise, mais vous devez regarder.
- **Critique** - Vous devriez bientôt jeter un coup d'œil.
- **Erreur** : un problème inconnu a provoqué l'échec de la fonctionnalité.
- **Aucun** - Aucune prédiction n'a été faite. Cela peut être dû à un manque de données ou à toute autre raison spécifique à une fonctionnalité qui n'effectue pas de prédiction.

Toutes les données spécifiques aux fonctionnalités du résultat sont enregistrées dans un fichier JSON accessible par l'utilisateur. Vous trouverez le chemin d'accès au fichier à l'aide de PowerShell. Pour plus d'informations, consultez les résultats de capacité de récupération.

# Modèle de prévision

Les fonctionnalités par défaut utilisent un modèle de prévision pour prédire l'utilisation future, et pour chaque prédiction, le modèle est entraîné localement sur les données de votre ordinateur. Ce modèle est conçu pour vous aider à détecter les tendances à plus long terme, et le réentraînement sur chaque instance Windows Server permet de s'adapter au comportement et aux nuances spécifiques de l'utilisation de chaque machine.

> **Notes**
>
> Déterminer le type de modèle à utiliser nécessite de tester de nombreux modèles à l'aide d'un jeu de données contenant des dizaines de milliers de machines. Après avoir analysé et ajusté ces modèles, nous avons décidé d'utiliser un modèle de prévision autorégressif, car il produit des prédictions très précises et visuellement intuitives tout en ne nécessitant pas trop de temps pour effectuer l'apprentissage. Toutefois, ce modèle nécessite trois semaines de données d'entraînement, de sorte que chaque fonctionnalité utilise une tendance linéaire de base jusqu'à ce que trois semaines de données soient disponibles.

# Chronologies de prévision

Les fonctionnalités par défaut prévoient quelques jours à l'avenir en fonction du nombre de jours pour lesquels les données ont été collectées. Le tableau suivant présente les chronologies de prédiction de ces fonctionnalités :

Agrandir le tableau

| Taille des données d'entrée | Longueur de prévision |
|---|---|
| 0 à 5 jours | Aucune prédiction n'est effectuée. |
| 6 à 180 jours | 1/3 * taille des données d'entrée |
| 180 à 365 jours | 60 jours |

# Données de prévision

Chaque fonctionnalité analyse les données quotidiennes pour prédire l'utilisation future. Toutefois, l'utilisation du processeur, de la mise en réseau et même du stockage peut fréquemment changer tout au long de la journée, en s'adaptant dynamiquement aux charges de travail sur l'ordinateur. Étant donné que l'utilisation n'est pas constante tout au long de la journée, il est important de représenter correctement l'utilisation quotidienne dans un point de données unique. Le tableau ci-dessous détaille les points de données spécifiques et la façon dont les données sont traitées :

Agrandir le tableau

| Nom de la fonctionnalité | Sources de données | Logique de filtrage |
|---|---|---|
| Prévision de la consommation de volume | Taille du volume | Maximum quotidien |
| Prévision de la consommation totale de stockage | Somme des tailles de volume, somme des tailles de disque | Utilisation quotidienne maximale |
| Prévision de la capacité processeur | % temps processeur | Moyenne maximale de 2 heures par jour |
| Prévision de la capacité de mise en réseau | Nombre total d'octets/s | Moyenne maximale de 2 heures par jour |

Lors de l'évaluation de la logique de filtrage, il est important de noter que chaque fonctionnalité cherche à informer les administrateurs lorsque l'utilisation future dépassera significativement les capacités disponibles. Même si le CPU atteint momentanément une utilisation de 100%, l'utilisation du processeur ne provoquera peut-être pas de dégradation notable des performances ou de conflit de ressources. Pour le processeur et la mise en réseau,

il doit y avoir une utilisation élevée plutôt que des pics momentanés. Quelques heures d'utilisation élevée du processeur ou de la mise en réseau peuvent avoir un impact significatif sur les performances de vos charges de travail critiques. La moyenne maximale de 2 heures par jour évite ces extrêmes et produit toujours des données significatives pour chaque capacité d'analyse.

Toutefois, pour le volume et l'utilisation totale du stockage, l'utilisation du stockage ne peut pas dépasser la capacité disponible, même momentanément, de sorte que l'utilisation quotidienne maximale est utilisée pour ces fonctionnalités.

# État de prévision

Toutes les fonctionnalités System Insights doivent générer un état associé à chaque prédiction. Chaque fonctionnalité par défaut utilise la logique suivante pour définir chaque état de prédiction :

- **OK** : la prévision ne dépasse pas la capacité disponible.
- **Avertissement** : La prévision dépasse la capacité disponible au cours des 30 prochains jours.
- **Critique** : la prévision dépasse la capacité disponible au cours des 7 prochains jours.
- **Erreur** : la fonctionnalité a rencontré une erreur inattendue.
- **Aucun** : il n'y a pas suffisamment de données pour effectuer une prédiction. Cela peut être dû à un manque de données ou parce qu'aucune donnée n'est signalée récemment.

> **Notes**
>
> Si une fonctionnalité fait des prédictions sur plusieurs instances (par exemple plusieurs volumes ou cartes réseau), l'état reflète l'état le plus grave de toutes les instances. Les états individuels de chaque volume ou carte réseau sont visibles dans Windows Admin Center ou dans les données contenues dans la sortie de chaque fonctionnalité. Pour obtenir des instructions sur l'analyse de la sortie JSON des fonctionnalités par défaut, consultez ce blog.

# Contenu connexe

Pour plus d'informations sur les insights système, consultez les ressources suivantes :

- Vue d'ensemble de System Insights
- Gérer les fonctionnalités
- Ajouter et développer des fonctionnalités

- Consulter les questions fréquentes (FAQ) sur System Insights

# Gérer les fonctionnalités System Insights dans Windows Admin Center

16/08/2025S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

Les fonctionnalités System Insights peuvent être gérées et configurées pour répondre à vos besoins de déploiement. Cet article explique comment ajuster les paramètres pour chaque fonctionnalité à l'aide de **PowerShell** ou **de Windows Admin Center**, avec des exemples et des captures d'écran pas à pas.

## Afficher les fonctionnalités

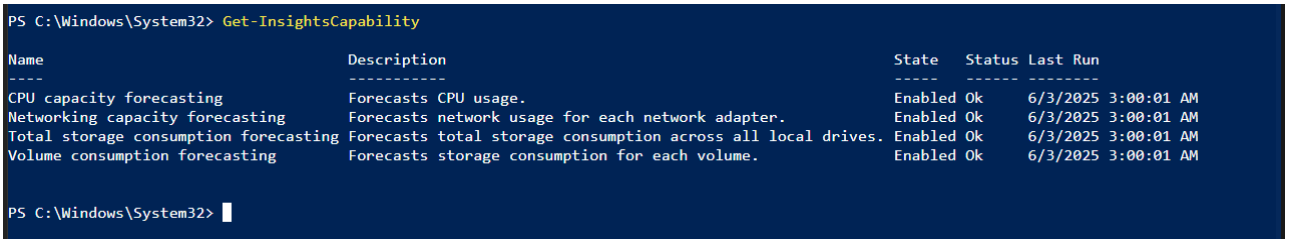
PowerShell

Vous pouvez répertorier toutes les fonctionnalités disponibles à l'aide de l'applet de commande Get-InsightsCapability :

1. Ouvrez PowerShell. Entrez la commande suivante :

PowerShell

```
Get-InsightsCapability
```




## Activer et désactiver une fonctionnalité

Chaque fonctionnalité peut être activée ou désactivée. La désactivation d'une fonctionnalité empêche de l'appeler. Pour les fonctionnalités autres que les fonctionnalités par défaut, la désactivation d'une fonctionnalité arrête la collecte de données pour cette fonctionnalité. Par défaut, toutes les fonctionnalités sont activées et vous pouvez vérifier l'état d'une fonctionnalité avant de la modifier.

PowerShell

Pour activer une fonctionnalité, utilisez l'applet **de commande Enable-InsightsCapability** :

1. Ouvrez PowerShell et entrez la commande suivante en remplaçant le nom de la fonctionnalité par la fonctionnalité de votre choix.

```
PowerShell
```

```
Enable-InsightsCapability -Name "CPU capacity forecasting"
```

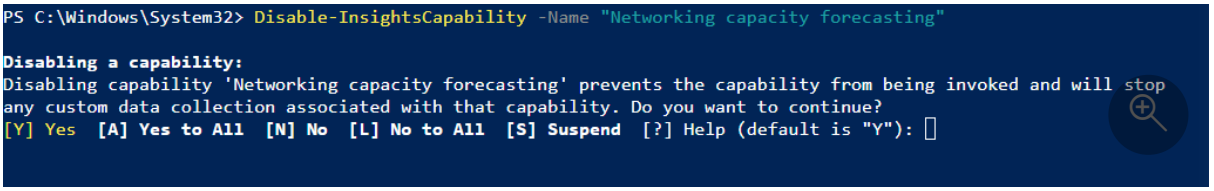
Pour désactiver une fonctionnalité, utilisez l'applet **de commande Disable-InsightsCapability** :

1. Ouvrez PowerShell et entrez la commande suivante en remplaçant le nom de la fonctionnalité par la fonctionnalité de votre choix.

```
PowerShell
```

```
Disable-InsightsCapability -Name "Networking capacity forecasting"
```

2. Vous êtes invité à confirmer la fonctionnalité que vous désactivez.




## Appeler une fonctionnalité

L'appel d'une fonctionnalité exécute immédiatement la fonctionnalité permettant de récupérer une prédiction, et les administrateurs peuvent appeler une fonctionnalité à tout moment dans Windows Admin Center ou à l'aide de l'applet de commande **Invoke-InsightsCapability** . Pour vous assurer que l'appel d'une fonctionnalité n'entre pas en conflit avec des opérations critiques sur votre ordinateur, vous pouvez planifier les prédictions pendant les heures creuses.

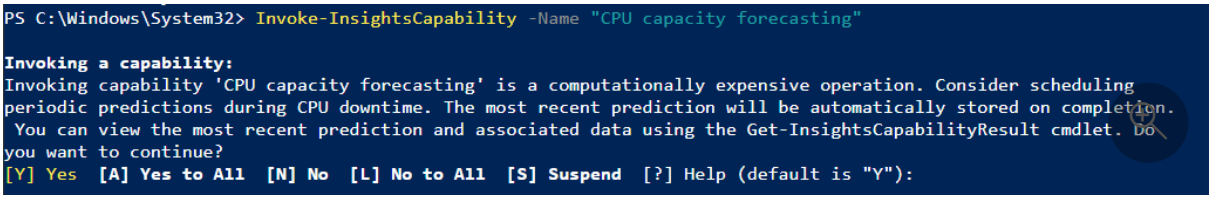
PowerShell

1. Ouvrez PowerShell et entrez la commande suivante en remplaçant le nom de la fonctionnalité par la fonctionnalité de votre choix.

```
PowerShell
```

```
Invoke-InsightsCapability -Name "CPU capacity forecasting"
```

2. Vérifiez que vous souhaitez appeler la fonctionnalité.




# Récupérer les résultats de la fonctionnalité

PowerShell

Une fois qu'une fonctionnalité est appelée, les résultats les plus récents sont visibles à l'aide de **Get-InsightsCapability** ou **Get-InsightsCapabilityResult**. Ces cmdlets génèrent les valeurs **État** et **Description d'état** les plus récentes de chaque fonctionnalité, ce qui correspond au résultat de chaque prédiction. Les champs **État** et **Description de l'état** sont décrits en détail dans le document de présentation des fonctionnalités.

En outre, vous pouvez utiliser la cmdlet **Get-InsightsCapabilityResult** pour afficher les 30 derniers résultats de prédiction et récupérer les données associées à la prédiction :

PowerShell

```
# Specify the History parameter to see the last 30 prediction results.
Get-InsightsCapabilityResult -Name "CPU capacity forecasting" -History

# Use the Output field to locate and then show the results of "CPU capacity
forecasting."
# Specify the encoding as UTF8, so that Get-Content correctly parses non-
English characters.
$Output = Get-Content (Get-InsightsCapabilityResult -Name "CPU capacity
forecasting").Output -Encoding UTF8 | ConvertFrom-Json
$Output.ForecastingResults
```

## Utiliser le journal des événements pour récupérer les résultats des fonctionnalités

Insights système journalise un événement chaque fois qu'une fonctionnalité termine une prédiction. Ces événements sont visibles dans le canal **Microsoft-Windows-System-Insights/Admin**. La fonctionnalité Insights système publie un ID d'événement différent pour chaque état :

Agrandir le tableau

| État de prédiction | ID de l'événement |
|---|---|
| OK | 151 |
| Avertissement | 148 |
| Critique | 150 |
| Error | 149 |
| Aucun | 1:32 |

Utilisez Azure Monitor ou System Center Operations Manager pour agréger ces événements et afficher les résultats de prédiction d'un groupe de machines.

# Définir une planification de capacité

En plus des prédictions à la demande, vous pouvez configurer des prédictions périodiques pour chaque fonctionnalité afin que la fonctionnalité spécifiée soit appelée automatiquement selon une planification prédéfinie. Chaque fonctionnalité par défaut est planifiée pour s'exécuter tous les jours à 3 h 00. Toutefois, vous pouvez créer des planifications personnalisées pour chaque fonctionnalité, et System Insights prend en charge différents types de planification.

PowerShell

Utilisez l'applet **de commande Get-InsightsCapabilitySchedule** pour afficher les planifications des fonctionnalités. Utilisez le pipeline `|` dans PowerShell pour afficher des informations sur toutes les fonctionnalités retournées par l'applet **de commande Get-InsightsCapability** .

PowerShell

```
Get-InsightsCapability | Get-InsightsCapabilitySchedule
```

Les prédictions périodiques sont activées par défaut, mais elles peuvent être désactivées à tout moment à l'aide des cmdlets **Enable-InsightsCapabilitySchedule** et **Disable-InsightsCapabilitySchedule** :

PowerShell

```
Enable-InsightsCapabilitySchedule -Name "Total storage consumption
forecasting"
Disable-InsightsCapabilitySchedule -Name "Volume consumption forecasting"
```

Vous pouvez créer des planifications personnalisées pour chaque fonctionnalité à l'aide de l'applet de commande **Set-InsightsCapabilitySchedule** :

PowerShell

```
Set-InsightsCapabilitySchedule -Name "CPU capacity forecasting" -Daily -
DaysInterval 2 -At 4:00PM
Set-InsightsCapabilitySchedule -Name "Networking capacity forecasting" -Daily
-DaysOfWeek Saturday, Sunday -At 2:30AM
Set-InsightsCapabilitySchedule -Name "Total storage consumption forecasting" -
Hourly -HoursInterval 2 -DaysOfWeek Monday, Wednesday, Friday
Set-InsightsCapabilitySchedule -Name "Volume consumption forecasting" -Minute
-MinutesInterval 30
```

Étant donné que les fonctionnalités par défaut analysent les données quotidiennes, des planifications quotidiennes sont recommandées pour ces fonctionnalités. En savoir plus sur les fonctionnalités par défaut.

# Créer des actions de correction

La fonctionnalité Insights système permet de lancer des scripts de correction personnalisés selon le résultat d'une fonctionnalité. Pour chaque fonctionnalité, vous pouvez configurer un script PowerShell personnalisé correspondant à chaque état de prédiction, ce qui permet aux administrateurs d'effectuer des actions correctives automatiquement sans intervention manuelle.

Voici quelques exemples d'actions de correction : exécution du nettoyage de disque, extension d'un volume, exécution de la déduplication, migration dynamique des machines virtuelles et configuration d'Azure File Sync.

PowerShell

Vous pouvez afficher les actions pour chaque fonctionnalité à l'aide de la cmdlet **Get-InsightsCapabilityAction** :

PowerShell

```
Get-InsightsCapability | Get-InsightsCapabilityAction
```

Vous pouvez créer des actions ou supprimer des actions existantes à l'aide des cmdlets **Set-InsightsCapabilityAction** et **Remove-InsightsCapabilityAction**. Chaque action est exécutée à l'aide des informations d'identification spécifiées dans le paramètre **ActionCredential**.

PowerShell

```
$Cred = Get-Credential
Set-InsightsCapabilityAction -Name "CPU capacity forecasting" -Type Warning -
Action "C:\Users\Public\WarningScript.ps1" -ActionCredential $Cred
Set-InsightsCapabilityAction -Name "CPU capacity forecasting" -Type Critical -
Action "C:\Users\Public\CriticalScript.ps1" -ActionCredential $Cred

Remove-InsightsCapabilityAction -Name "CPU capacity forecasting" -Type Warning
```

# Contenu connexe

Pour en savoir plus sur Insights système, utilisez les ressources suivantes :

- Documentation PowerShell System Insights
- Vue d'ensemble des insights système
- Présentation des fonctionnalités
- Ajout et développement de fonctionnalités
- Questions fréquentes sur les insights système

# Ajouter et développer des fonctionnalités dans System Insights

16/08/2025S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

La fonctionnalité Insights système vous permet d'ajouter de nouvelles capacités prédictives au module Insights système, sans nécessiter de mises à jour du système d'exploitation. Cela permet aux développeurs, aussi bien ceux de Microsoft et des tiers, de créer et de fournir de nouvelles capacités en milieu de version pour répondre aux scénarios qui vous intéressent.

Toute nouvelle capacité peut s'intégrer à l'infrastructure Insights système existante et l'étendre :

- De nouvelles fonctionnalités peuvent **spécifier n'importe quel compteur de performances ou événement système**, qui sont collectés, conservés localement et retournés à la fonctionnalité d'analyse lorsque la fonctionnalité est appelée.
- De nouvelles fonctionnalités peuvent **utiliser les plans de gestion Windows Admin Center et PowerShell existants**. Non seulement les nouvelles fonctionnalités sont détectables dans System Insights, elles bénéficient également de planifications personnalisées et d'actions de correction.

## Gérer les nouvelles capacités

- Découvrez comment ajouter, supprimer et mettre à jour des fonctionnalités à l'aide de PowerShell.

## Développer une capacité

Utilisez les ressources suivantes pour commencer à écrire vos propres capacités personnalisées :

- Découvrez les sources de données que vous pouvez collecter.
- Téléchargez le package NuGet System Insights, qui contient les classes et interfaces dont vous avez besoin pour écrire une fonctionnalité.
- Lisez la documentation de l'API pour en savoir plus sur les classes et interfaces System Insights.
- Utilisez l'exemple de fonctionnalité System Insights pour vous aider à commencer. Il vous montre comment inscrire une capacité, comment spécifier les sources de données à collecter et comment commencer à analyser les données système.

## Contenu connexe

Pour plus d’informations sur les insights système, consultez les ressources suivantes :

- Vue d’ensemble des insights système
- Comprendre les fonctionnalités
- Gérer les fonctionnalités
- Ajouter, supprimer et mettre à jour des fonctionnalités
- Questions fréquentes (FAQ) sur la fonctionnalité Insights système

# Ajouter, supprimer et mettre à jour des fonctionnalités dans System Insights

16/08/2025S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

System Insights vous permet de créer de nouvelles fonctionnalités qui utilisent la fonctionnalité existante de collecte et de gestion des données. Néanmoins, il reste tout aussi important, une fois ces capacités créées, de disposer également de la prise en charge de la plateforme pour gérer leurs ajouts, suppressions et mises à jour.

Cette rubrique décrit les fonctionnalités générales permettant d'ajouter, de supprimer et de mettre à jour des capacités dans les insights système.

## Ajouter une fonctionnalité

System Insights vous permet d'ajouter de nouvelles fonctionnalités à tout moment à l'aide de l'applet **de commande Add-InsightsCapability** . **Add-InsightsCapability** vous oblige à spécifier un nom de fonctionnalité et la bibliothèque de fonctionnalités. La bibliothèque de la capacité contient la description, les sources de données et la logique de prédiction de la capacité.

PowerShell

```
Add-InsightsCapability -Name Sample capability -Library C:\SampleCapability.dll
```

Une fois qu'une fonctionnalité est ajoutée à System Insights, vous pouvez appeler et gérer immédiatement la fonctionnalité à l'aide de PowerShell ou de Windows Admin Center.

## Mettre à jour une fonctionnalité

System Insights vous permet de mettre à jour une fonctionnalité à l'aide de l'applet **de commande Update-InsightsCapability** .

PowerShell

```
Update-InsightsCapability -Name Sample capability -Library
C:\SampleCapabilityv2.dll
```

La mise à jour d'une capacité vous permet de spécifier une nouvelle bibliothèque de capacité, et donc de modifier la description de la capacité, les sources de données et la logique de prédiction associée. Plus important encore, vous conservez ainsi toutes les informations de

configuration et d'historique de cette capacité, notamment les planifications personnalisées, les actions et les résultats de prédiction passés.

# Supprimer une fonctionnalité

Vous pouvez supprimer des fonctionnalités dans System Insights à l'aide de l'applet **de commande Remove-InsightsCapability** .

```PowerShell
Remove-InsightsCapability -Name Sample capability
```

> **Notes**
>
> Les capacités de prévision par défaut ne peuvent pas être supprimées.

La suppression d'une capacité a pour effet de la supprimer définitivement la capacité et toutes les informations associées, y compris la planification, les actions de correction et les résultats de prédiction passés.

Envisagez de désactiver une fonctionnalité plutôt que de la supprimer si vous vous inquiétez de supprimer définitivement toutes les informations associées à la fonctionnalité.

# Contenu connexe

Pour plus d'informations sur les insights système, consultez les ressources suivantes :

- Vue d'ensemble des insights système
- Présentation des fonctionnalités
- Gestion des fonctionnalités
- Ajout et développement de fonctionnalités
- FAQ sur les insights système

# Sources de données Insights système

15/08/2025S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

La fonctionnalité Insights système introduit des fonctionnalités de collecte de données extensibles. Lors de l'écriture d'une nouvelle capacité, vous pouvez spécifier des sources de données existantes ou nouvelles à collecter localement et à analyser. Cette rubrique décrit les sources de données que vous pouvez choisir lors de l'inscription d'une nouvelle capacité.

## Sources de données

Lors de l'écriture d'une nouvelle capacité, vous devez identifier les sources de données spécifiques à collecter pour chaque capacité. Les sources de données que vous spécifiez sont collectées et conservées directement sur votre ordinateur, et vous pouvez choisir parmi trois types de sources de données :

- **Compteurs de performances** : spécifiez le chemin d'accès, le nom et les instances du compteur, et System Insights collecte les données pertinentes signalées par ces compteurs de performances.
- **Événements système** : spécifiez le nom du canal et l'ID d'événement, et System Insights indique combien de fois cet événement s'est produit.
- **Série connue** : System Insights collecte certaines informations de base sur votre ordinateur pour quelques ressources bien définies. Ces séries sont utilisées pour les capacités par défaut, mais elles peuvent également être utilisées par n'importe quelle capacité personnalisée. Celles-ci collectent les informations suivantes :
  - **Disk**:
    - *Propriétés* : Guid
    - *Données* : Taille
  - **Volume**:
    - *Propriétés* : UniqueId, DriveLetter, FileSystemLabel, Size
    - *Données* : Taille utilisée
  - **Carte réseau** :
    - *Propriétés* : InterfaceGuid, InterfaceDescription, Speed
    - *Données* : Octets reçus/s, Octets envoyés/s, Nombre total d'octets/s
  - **CPU**:
    - *Propriétés* : -
    - *Données* : temps processeur %

- Spécifiez une série connue et System Insights retourne les données collectées par cette série.

# Chronologies de conservation et intervalles de collecte

Les sources de données ont des chronologies de rétention et des intervalles de collecte différents. Le tableau suivant indique la durée et la fréquence à laquelle chaque source de données est collectée :

Agrandir le tableau

| Source de données | Chronologie de rétention | Intervalle de collecte |
|---|---|---|
| Compteurs de performance | 3 mois | 15 minutes |
| Événements système | 3 mois | 15 minutes |
| Série connue | 1 an | 1 heure |

## Types d'agrégation

Étant donné que chaque série n'enregistre qu'un seul point de données pour chaque intervalle de collecte, chaque série a un type d'agrégation associé. Pour les compteurs de performances, vous avez le choix entre différents types d'agrégation.

Le tableau suivant décrit la source de données et le type d'agrégation correspondant :

Agrandir le tableau

| Source de données | Types d'agrégation |
|---|---|
| Compteurs de performance | Somme, moyenne, max, min |
| Événements système | Count |
| Séries de disques connues | Dernière (dernière valeur dans l'intervalle de collecte) |
| Séries de volumes connues | Dernière (dernière valeur dans l'intervalle de collecte) |
| Séries de processeurs connues | Average |
| Séries de réseaux connues | Average |

# Empreinte des données

La fonctionnalité Insights système collecte toutes les données localement sur votre lecteur C (C:). En général, l'empreinte des données Insights système est modeste. Elle dépend directement du type et du nombre de sources de données spécifiées par chaque fonctionnalité, et le tableau suivant détaille l'utilisation du stockage pour chaque type de données :

Agrandir le tableau

| Source de données | Empreinte maximale |
|---|---|
| Compteurs de performance | 240 Ko |
| Événements système | 200 kB |
| Séries de disques connues | 200 Ko par disque |
| Séries de volumes connues | 300 Ko par volume |
| Séries de processeurs connues | 100 Ko |
| Séries de réseaux connues | 300 Ko par carte réseau |

Pour les fonctionnalités de prévision par défaut, l'empreinte maximale doit être inférieure à 10 Mo pour la plupart des machines autonomes.

# Contenu connexe

Pour plus d'informations sur les insights système, consultez les ressources suivantes :

- Vue d'ensemble des insights système
- Présentation des fonctionnalités
- Gestion des fonctionnalités
- Ajout et développement de fonctionnalités
- FAQ sur les insights système

# Questions fréquentes (FAQ) sur la fonctionnalité Insights système

16/08/2025S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

## Comment utiliser Insights système avec Azure Monitor ou System Center Operations Manager ?

Azure Monitor et System Center Operations Manager fournissent des informations opérationnelles sur vos déploiements pour vous aider à gérer votre infrastructure. Insights système, en revanche, est une fonctionnalité Windows Server qui introduit des capacités d'analytique prédictive locale. Ensemble, la fonctionnalité Insights système et Azure Monitor ou SCOM peuvent faciliter la mise en évidence des prédictions sur une population d'appareils :

Azure Monitor ou SCOM peuvent s'appuyer sur les événements créés par la fonctionnalité Insights système, car celle-ci génère le résultat de chaque prédiction dans le journal des événements. Ils peuvent faire apparaître ces prédictions spécifiques à une machine sur une flotte de serveurs Windows Server, ce qui vous permet d'avoir une vue unifiée de ces prédictions sur un groupe d'instances de serveur.

Consultez les ID de canal et d'événement pour chaque prédiction dans les résultats de la fonctionnalité de récupération.

## Quel est le lien entre la fonctionnalité Insights système et Windows ML ?

Windows ML est une plateforme qui permet aux développeurs d'importer et de noter des modèles Machine Learning préentraînés sur des appareils Windows. Ces modèles bénéficient de l'accélération matérielle et peuvent être notés localement.

Insights système est une fonctionnalité de Windows Server 2019 qui offre des capacités prédictives locales ainsi qu'une expérience de gestion complète, ce qui inclut l'intégration de PowerShell et de Windows Admin Center.

## Puis-je utiliser Insights système pour mon cluster ?

Yes. La fonctionnalité Insights système peut s'exécuter indépendamment sur chaque nœud de cluster de basculement individuel, et le comportement par défaut d'Insights système prévoit l'utilisation dans le stockage local, le volume, le processeur et la mise en réseau. **Vous pouvez également activer les prévisions pour le stockage en cluster**, de sorte que les capacités de prévision de stockage prédisent l'utilisation des volumes et du stockage en cluster. Vous pouvez gérer ces paramètres dans Windows Admin Center ou PowerShell.

## Quel est le coût d'exécution des capacités par défaut ?

Chaque capacité par défaut est peu coûteuse à exécuter. Chaque fonctionnalité prend plus de temps à s'exécuter lorsque vous collectez plus de données, mais elles doivent généralement s'exécuter en quelques secondes.

## Contenu connexe

Pour plus d'informations sur les insights système, consultez les ressources suivantes :

- Vue d'ensemble des insights système
- Présentation des fonctionnalités
- Gestion des fonctionnalités
- Ajout et développement de fonctionnalités

# Prise en main de la collecte d'événements de configuration et de démarrage

15/08/2025

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

## Overview

La collecte des événements de configuration et de démarrage est une nouvelle fonctionnalité dans Windows Server 2016 qui vous permet de désigner un ordinateur « collecteur » capable de rassembler divers événements importants qui se produisent sur d'autres ordinateurs lors de leur démarrage ou de leur processus de configuration. Vous pouvez ensuite analyser les événements collectés avec l'observateur d'événements, l'analyseur de messages, Wevtutil ou les applets de commande Windows PowerShell.

Auparavant, ces événements étaient impossibles à surveiller, car l'infrastructure nécessaire pour les collecter n'existe pas tant qu'un ordinateur n'est pas déjà configuré. Les types d'événements d'installation et de démarrage que vous pouvez surveiller sont les suivants :

- Chargement des modules et pilotes de noyau
- Énumération des appareils et initialisation de leurs pilotes (y compris les périphériques tels que le type de processeur)
- Vérification et montage de systèmes de fichiers
- Démarrage des fichiers exécutables
- Démarrage et saisie semi-automatique des mises à jour du système
- Les points lorsque le système devient disponible pour l'ouverture de session, établissent la connexion avec un contrôleur de domaine, l'achèvement du démarrage du service et la disponibilité des partages réseau

L'ordinateur collecteur doit exécuter Windows Server 2016 (il peut être en mode Server with Desktop Experience ou Server Core). L'ordinateur cible doit exécuter Windows 10 ou Windows Server 2016. Vous pouvez également exécuter ce service sur une machine virtuelle hébergée sur un ordinateur qui **n'exécute pas** Windows Server 2016. Les combinaisons suivantes d'ordinateurs collecteurs et cibles virtualisés sont connues pour fonctionner :

Agrandir le tableau

| Hôte de virtualisation | Machine virtuelle du collecteur | Machine virtuelle cible |
|---|---|---|
| Windows 8.1 | yes | yes |
| Windows 10 | yes | yes |
| Windows Server 2016 | yes | yes |
| Windows Server 2012 R2 | yes | no |

# Installer le service de collecteur

À compter de Windows Server 2016, le service collecteur d'événements est disponible en tant que fonctionnalité facultative. Dans cette version, vous pouvez l'installer à l'aide de DISM.exe avec cette commande à une invite de Windows PowerShell avec élévation de privilèges :

```
dism /online /enable-feature /featurename:SetupAndBootEventCollection
```

Cette commande crée un service appelé BootEventCollector et le démarre avec un fichier de configuration vide.

Vérifiez que l'installation a réussi en vérifiant `get-service -displayname *boot*`. Le collecteur d'événements de démarrage doit être en cours d'exécution. Il s'exécute sous le compte de service réseau et crée un fichier de configuration vide (Active.xml) dans **%SystemDrive%\ProgramData\Microsoft\BootEventCollector\Config**.

Vous pouvez également installer le service de collecte d'événements d'installation et de démarrage avec l'Assistant Ajout de rôles et de fonctionnalités dans Gestionnaire de serveur.

# Configuration

Vous devez configurer deux éléments pour collecter les événements d'installation et de démarrage.

- Sur les ordinateurs cibles qui envoient les événements (c'est-à-dire les ordinateurs dont vous souhaitez surveiller l'installation et le démarrage), activez le transport KDNET/EVENT-NET et activez le transfert des événements.
- Sur l'ordinateur collecteur, spécifiez les ordinateurs à partir desquels accepter les événements et où les enregistrer.

> ⓘ **Notes**

Vous ne pouvez pas configurer un ordinateur pour envoyer les événements de démarrage ou de démarrage à lui-même. Mais si vous souhaitez surveiller deux ordinateurs, vous pouvez les configurer pour qu'ils s'envoient les événements l'un à l'autre.

## Configurer un ordinateur cible

Sur chaque ordinateur cible, vous activez d'abord le transport KDNET/EVENT-NET, puis vous activez l'envoi d'événements ETW via le transport, puis redémarrez l'ordinateur cible. EVENT-NET est un protocole de transport dans le noyau qui est similaire à KDNET (le protocole de débogueur du noyau). EVENT-NET transmet uniquement les événements et n'autorise pas l'accès au débogueur. Ces deux protocoles s'excluent mutuellement; vous ne pouvez activer qu'un seul d'entre eux à la fois.

Vous pouvez activer le transport d'événements à distance (avec Windows PowerShell) ou localement.

### Pour activer le transport d'événements à distance

1. Si vous avez déjà configuré Communication à distance Windows PowerShell sur l'ordinateur cible, passez à l'étape 3. Si ce n'est pas le cas, sur l'ordinateur cible, ouvrez une invite de commandes et exécutez la commande suivante :

   winrm quickconfig

2. Répondez aux invites, puis redémarrez l'ordinateur cible. Si les ordinateurs cibles ne se trouvent pas dans le même domaine que l'ordinateur collecteur, vous devrez peut-être les définir en tant qu'hôtes approuvés. Pour ce faire :

3. Sur l'ordinateur collecteur, exécutez l'une des commandes suivantes :

   - Dans une invite Windows PowerShell : `Set-Item -Force WSMan:\localhost\Client\TrustedHosts <target1>,<target2>,...`, suivi de `Set-Item -Force WSMan:\localhost\Client\AllowUnencrypted true` où <target1>, etc. sont les noms ou adresses IP des ordinateurs cibles.

   - Ou dans une invite de commandes : **winrm set winrm/config/client @{TrustedHosts=<target1,target2><>,...; AllowUnencrypted=true}**

     > **ⓘ Important**

> Cela configure la communication non chiffrée. Ne le faites donc pas en dehors d'un environnement de laboratoire.

4. Testez la connexion à distance en accédant à l'ordinateur collecteur et en exécutant l'une de ces commandes Windows PowerShell :

   Si l'ordinateur cible se trouve dans le même domaine que l'ordinateur collecteur, exécutez `New-PSSession -Computer <target> | Remove-PSSession`

   Si l'ordinateur cible n'est pas dans le même domaine, exécutez `New-PSSession -Computer <target> -Credential Administrator | Remove-PSSession`, qui vous invite à entrer des informations d'identification.

   Si la commande ne retourne rien, la communication à distance a réussi.

5. Sur l'ordinateur cible, ouvrez une invite de Windows PowerShell avec élévation de privilèges et exécutez cette commande :

   `Enable-SbecBcd -ComputerName <target_name> -CollectorIP <ip> -CollectorPort <port> -Key <a.b.c.d>`

   Ici <, target_name> est le nom de l'ordinateur cible, <ip> est l'adresse IP de l'ordinateur collecteur. <port> est le numéro de port où le collecteur s'exécutera. La clé <a.b.c.d> est une clé de chiffrement requise pour la communication, comprenant quatre chaînes alphanumériques séparées par des points. Cette même clé est utilisée sur l'ordinateur collecteur. Si vous n'entrez pas de clé, le système génère une clé aléatoire ; vous en aurez besoin pour l'ordinateur collecteur, alors prenez-en note.

6. Si vous avez déjà configuré un ordinateur collecteur, mettez à jour le fichier de configuration sur l'ordinateur collecteur avec les informations du nouvel ordinateur cible. Pour plus d'informations, consultez la section Configuration de l'ordinateur collecteur.

### Pour activer le transport d'événements localement sur l'ordinateur cible

1. Démarrez une invite de commandes avec élévation de privilèges, puis exécutez les commandes suivantes :

   **bcdedit /event yes**

   **bcdedit /eventsettings net hostip :1.2.3.4 port :50000 key :a.b.c.d**

   Ici 1.2.3.4 est un exemple ; remplacez ceci par l'adresse IP de l'ordinateur collecteur. Remplacez également 50000 par le numéro de port où le collecteur s'exécutera et a.b.c.d

par la clé de chiffrement requise pour la communication. Cette même clé est utilisée sur l'ordinateur collecteur. Si vous n'entrez pas de clé, le système génère une clé aléatoire ; vous en aurez besoin pour l'ordinateur collecteur, alors prenez-en note.

2. Si vous avez déjà configuré un ordinateur collecteur, mettez à jour le fichier de configuration sur l'ordinateur collecteur avec les informations du nouvel ordinateur cible. Pour plus d'informations, consultez la section Configuration de l'ordinateur collecteur.

**Maintenant que le transport d'événements lui-même est activé, vous devez autoriser le système à envoyer des événements ETW via ce transport.**

### Pour activer l'envoi d'événements ETW via le transport à distance

1. Sur l'ordinateur collecteur, ouvrez une invite de Windows PowerShell avec élévation de privilèges.

2. Exécutez `Enable-SbecAutologger -ComputerName <target_name>`, où <target_name> est le nom de l'ordinateur cible.

Si vous n'êtes pas en mesure de configurer Communication à distance Windows PowerShell, vous pouvez toujours activer l'envoi d'événements directement sur l'ordinateur cible.

### Pour activer l'envoi d'événements ETW via le transport localement

1. Sur l'ordinateur cible, démarrez Regedit.exe et recherchez cette clé de Registre :

   **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger**. Différentes sessions de journal sont répertoriées en tant que sous-clés sous cette clé. **La plateforme d'installation**, **l'enregistreur d'événements NT** et **le programme d'installation de Microsoft-Windows** sont des choix possibles pour une utilisation avec le programme d'installation et la collecte d'événements de démarrage, mais l'option recommandée est **EventLog-System**. Ces clés sont détaillées dans Configuration et démarrage d'une session de journal automatique.

2. Dans la clé EventLog-System, remplacez la valeur de **LogFileMode** de **0x10000180** par **0x10080180**. Pour plus d'informations sur les détails de ces paramètres, consultez Constantes du mode de journalisation.

3. De manière facultative, vous pouvez également activer le transfert des données de vérification des bogues vers l'ordinateur collecteur. Pour ce faire, recherchez la clé de Registre HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager et créez la clé **Filtre d'impression de débogage** avec la valeur **0x1**.

4. Redémarrer l'ordinateur cible.

## Choix de la carte d'adaptateur

Si l'ordinateur cible a plusieurs adaptateurs réseau, le pilote KDNET choisit le premier adaptateur pris en charge répertorié. Vous pouvez spécifier un adaptateur réseau spécifique à utiliser pour le transfert des événements d'installation en procédant comme suit :

### Pour spécifier un adaptateur réseau

1. Sur l'ordinateur cible, ouvrez Device Manager, développez **cartes réseau**, recherchez la carte réseau que vous souhaitez utiliser, puis cliquez dessus avec le bouton droit.

2. Dans le menu qui s'ouvre, cliquez sur **Propriétés**, puis sur l'onglet **Détails** . Développez le menu dans le champ **Propriété** , faites défiler pour rechercher les **informations d'emplacement** (la liste n'est probablement pas dans l'ordre alphabétique), puis cliquez dessus. La valeur est une chaîne de la forme **pci bus X, appareil Y, fonction Z**. Notez X.Y.Z ; il s'agit des paramètres de bus dont vous avez besoin pour la commande suivante.

3. Exécutez l'une de ces commandes :

   À partir d'une invite Windows PowerShell avec élévation de privilèges : `Enable-SbecBcd -ComputerName <target_name> -CollectorIP <ip> -CollectorPort <port> -Key <a.b.c.d> -BusParams <X.Y.Z>`

   À partir d'une invite de commandes avec élévation de privilèges : **bcdedit /eventsettings net hostip:aaa port:50000 key:bbb busparams:X.Y.Z**

## Valider la configuration de l'ordinateur cible

Pour vérifier les paramètres sur l'ordinateur cible, ouvrez une invite de commandes avec élévation de privilèges et exécutez **bcdedit /enum**. Une fois cette opération terminée, exécutez **bcdedit /eventsettings**. Vous pouvez vérifier les valeurs suivantes :

- Key
- Debugtype = NET
- Hostip = <adresse IP du collecteur>
- Port = <numéro de port que vous avez spécifié pour le collecteur à utiliser>
- DHCP = oui

Vérifiez également que vous avez activé **bcdedit /event**, car **/debug** et **/event** sont mutuellement exclusifs. Vous ne pouvez exécuter que l'un ou l'autre. De même, vous ne pouvez pas combiner /eventsettings avec /debug ou /dbgsettings avec /event.

Notez également que la collecte d'événements ne fonctionne pas si vous la définissez sur un port série.

## Configuration de l'ordinateur collecteur

Le service collecteur reçoit les événements et les enregistre dans des fichiers ETL. Ces fichiers ETL peuvent ensuite être lus par d'autres outils, tels que les applets de Event Viewer, Message Analyzer, Wevtutil et Windows PowerShell.

Étant donné que le format ETW ne vous permet pas de spécifier le nom de l'ordinateur cible, les événements de chaque ordinateur cible doivent être enregistrés dans un fichier distinct. Les outils d'affichage peuvent afficher un nom d'ordinateur, mais il s'agit du nom de l'ordinateur sur lequel l'outil s'exécute.

Plus précisément, un anneau de fichiers ETL est affecté à chaque ordinateur cible. Chaque nom de fichier inclut un index compris entre 000 et une valeur maximale que vous configurez (jusqu'à 999). Lorsque le fichier atteint la taille maximale configurée, il bascule les événements d'écriture vers le fichier suivant. Après le fichier le plus élevé possible, il revient à l'index de fichier 000. De cette façon, les fichiers sont automatiquement recyclés, ce qui limite l'utilisation de l'espace disque. Vous pouvez également définir des stratégies de rétention externe supplémentaires pour limiter davantage l'utilisation du disque ; par exemple, vous pouvez supprimer des fichiers antérieurs à un nombre défini de jours.

Les fichiers ETL collectés sont généralement conservés dans le répertoire **c :\ProgramData\Microsoft\BootEventCollector\Etl** (qui peut avoir des sous-répertoires supplémentaires). Vous pouvez trouver le fichier journal le plus récent en le triant par heure de la dernière modification. Il existe également un journal d'état (généralement dans **c :\ProgramData\Microsoft\BootEventCollector\Logs**), qui enregistre chaque fois que le collecteur change d'écriture dans un nouveau fichier.

Il existe également un journal du collecteur, qui enregistre des informations sur le collecteur lui-même. Vous pouvez conserver ce journal au format ETW (dans lequel les événements sont signalés au service de journal Windows ; il s'agit de la valeur par défaut) ou dans un fichier (normalement dans **c :\ProgramData\Microsoft\BootEventCollector\Logs**). L'utilisation d'un fichier peut être utile si vous souhaitez activer des modes détaillés qui produisent beaucoup de données. Vous pouvez également définir le journal pour écrire dans une sortie standard en exécutant le collecteur à partir de la ligne de commande.

**Création du fichier de configuration du collecteur**

Lorsque vous activez le service, trois fichiers de configuration XML sont créés et stockés dans **c :\ProgramData\Microsoft\BootEventCollector\Config** :

- **Active.xml** Ce fichier contient la configuration active actuelle du service collecteur. Juste après l'installation, ce fichier a le même contenu que Empty.xml. Lorsque vous définissez une nouvelle configuration de collecteur, vous l'enregistrez dans ce fichier.
- **Empty.xml** Ce fichier contient les éléments de configuration minimaux nécessaires avec leurs valeurs par défaut définies. Ceci n'active aucune collection, mais permet uniquement au service collecteur de démarrer en mode inactif.
- **Example.xml** Ce fichier fournit des exemples et des explications des éléments de configuration possibles.

**Choix d'une limite de taille de fichier**

L'une des décisions que vous devez prendre consiste à définir une limite de taille de fichier. La limite de taille de fichier maximale dépend du volume attendu d'événements et de l'espace disque disponible. Les fichiers plus petits sont plus pratiques du point de vue du nettoyage des anciennes données. Toutefois, chaque fichier comporte la surcharge d'un en-tête de 64 Ko et la lecture de nombreux fichiers pour obtenir l'historique combiné peut être peu pratique. La limite de taille de fichier minimale absolue est de 256 Ko. Une limite de taille de fichier pratique raisonnable doit être supérieure à 1 Mo, et 10 Mo est probablement une bonne valeur typique. Une limite plus élevée peut être raisonnable si vous attendez de nombreux événements.

Il existe plusieurs détails à garder à l'esprit concernant le fichier de configuration :

- Adresse de l'ordinateur cible. Vous pouvez utiliser son adresse IPv4, une adresse MAC ou un GUID SMBIOS. Gardez ces facteurs à l'esprit lorsque vous choisissez l'adresse à utiliser :
    - L'adresse IPv4 fonctionne mieux avec l'affectation statique des adresses IP. Toutefois, même les adresses IP statiques doivent être disponibles via DHCP.
    - Une adresse MAC ou un GUID SMBIOS est pratique lorsqu'ils sont connus à l'avance, mais que les adresses IP sont attribuées dynamiquement.
    - Les adresses IPv6 ne sont pas prises en charge par le protocole EVENT-NET.
    - Il est possible de spécifier plusieurs façons d'identifier l'ordinateur. Par exemple, si le matériel physique est sur le point d'être remplacé, vous pouvez entrer à la fois l'ancienne et la nouvelle adresse MAC, et l'une ou l'autre sera acceptée.
- Clé de chiffrement utilisée pour la communication avec l'ordinateur collecteur

- Nom de l'ordinateur cible. Vous pouvez utiliser l'adresse IP, le nom d'hôte ou tout autre nom comme nom d'ordinateur.
- Le nom du fichier ETL à utiliser et la configuration de la taille d'anneau pour celui-ci

### Pour créer un fichier de configuration

1. Ouvrez une invite de Windows PowerShell avec élévation de privilèges et remplacez les répertoires par %SystemDrive%\ProgramData\Microsoft\BootEventCollector\Config.
2. Tapez `notepad .\newconfig.xml`, puis appuyez sur ENTRÉE.
3. Copiez cet exemple de configuration dans la fenêtre Bloc-notes :

```
<collector configVersionMajor=1
statuslog=c:\ProgramData\Microsoft\BootEventCollector\Logs\statuslog.xml>
  <common>
    <collectorport value=50000/>
    <forwarder type=etl>
      <set name=file value=c:\ProgramData\Microsoft\BootEventCollector\Etl\
{computer}\{computer}_{#3}.etl/>
      <set name=size value=10mb/>
      <set name=nfiles value=10/>
      <set name=toxml value=none/>
    </forwarder>
    <target>
      <ipv4 value=192.168.1.1/>
      <key value=a.b.c.d/>
      <computer value=computer1/>
    </target>
    <target>
      <ipv4 value=192.168.1.2/>
      <key value=d1.e2.f3.g4/>
      <computer value=computer2/>
    </target>
  </common>
</collector>
```

> ⓘ **Notes**
>
> Le nœud racine est <collector>. Ses attributs spécifient la version de la syntaxe du fichier de configuration et le nom du fichier journal d'état.
>
> L'élément <commun> regroupe plusieurs cibles en spécifiant les éléments de configuration communs, tout comme un groupe d'utilisateurs peut être utilisé pour spécifier les autorisations communes pour plusieurs utilisateurs.

L'élément <collectorport> définit le numéro de port UDP où le collecteur écoutera les données entrantes. Il s'agit du même port que celui spécifié dans l'étape de configuration cible pour Bcdedit. Le collecteur ne prend en charge qu'un seul port et toutes les cibles doivent se connecter au même port.

L'élément <redirecteur> spécifie comment les événements ETW reçus des ordinateurs cibles seront transférés. Il n'existe qu'un seul type de redirecteur, qui les écrit dans les fichiers ETL. Les paramètres spécifient le modèle de nom de fichier, la limite de taille pour chaque fichier dans l'anneau et la taille de l'anneau pour chaque ordinateur. Le paramètre toxml spécifie que les événements ETW seront écrits au format binaire à mesure qu'ils ont été reçus, sans conversion au format XML. Consultez la section conversion d'événements XML pour plus d'informations sur la décision de conférer ou non les événements au format XML. Le modèle de nom de fichier contient les substitutions suivantes : {computer} pour le nom de l'ordinateur et {#3} pour l'index du fichier dans l'anneau.

Dans cet exemple de fichier, deux ordinateurs cibles sont définis avec l'élément <cible>. Chaque définition spécifie l'adresse IP avec <ipv4>, mais vous pouvez également utiliser l'adresse MAC (par exemple, `<mac value=11:22:33:44:55:66/>` ou `<mac value=11-22-33-44-55-66/>`) ou le GUID SMBIOS (par exemple, `<guid value={269076F9-4B77-46E1-B03B-CA5003775B88}/>`) pour identifier l'ordinateur cible. Notez également la clé de chiffrement (identique à celle qui a été spécifiée ou générée avec Bcdedit sur l'ordinateur cible) et le nom de l'ordinateur.

4. Entrez les détails de chaque ordinateur cible en tant qu'élément <cible> distinct dans le fichier de configuration, puis enregistrez Newconfig.xml et fermez le Bloc-notes.

5. Appliquez la nouvelle configuration avec `$result = (Get-Content .\newconfig.xml | Set-SbecActiveConfig); $result`. La sortie doit retourner avec le champ Réussite « true ». Si vous obtenez un autre résultat, consultez la section Résolution des problèmes de cette rubrique.

Vous pouvez toujours vérifier la configuration active actuelle avec `(Get-SbecActiveConfig).text`.

Vous pouvez effectuer une vérification de validité sur le fichier de configuration avec `$result = (Get-Content .\newconfig.xml | Check-SbecConfig); $result`.

Bien que la commande Windows PowerShell pour appliquer une nouvelle configuration met automatiquement à jour le service sans vous obliger à le redémarrer, vous pouvez toujours redémarrer le service vous-même avec l'une des commandes suivantes :

- Avec Windows PowerShell : `Restart-Service BootEventCollector`
- Dans une invite de commandes ordinaire : **sc stop BootEventCollector; sc start BootEventCollector**

# Configuration de Nano Server en tant qu'ordinateur cible

L'interface minimale offerte par Nano Server peut parfois rendre difficile le diagnostic des problèmes. Vous pouvez configurer votre image Nano Server pour participer automatiquement à la collecte d'événements d'installation et de démarrage, en envoyant des données de diagnostic à un ordinateur collecteur sans intervention supplémentaire de votre part. Pour cela, procédez comme suit :

## Pour configurer Nano Server en tant qu'ordinateur cible

1. Créer votre image Nano Server de base. Voir Prise en main de Nano Server pour plus d'informations.
2. Configurez un ordinateur collecteur comme dans la section Configuration de l'ordinateur collecteur de cette rubrique.
3. Ajoutez des clés de registre AutoLogger pour activer l'envoi de messages de diagnostic. Pour ce faire, vous montez le disque dur virtuel Nano Server créé à l'étape 1, chargez la ruche du registre, puis ajoutez certaines clés de registre. Dans cet exemple, l'image Nano Server est en C:\NanoServer ; votre chemin d'accès peut être différent, donc ajustez les étapes en conséquence.

   a. Sur l'ordinateur collecteur, copiez **le fichier .. \Windows\System32\WindowsPowerShell\v1.0\Modules\BootEventCollector** et collez-le dans le **fichier .. \Windows\System32\WindowsPowerShell\v1.0\Modules** sur l'ordinateur que vous utilisez pour modifier le disque dur virtuel Nano Server.

   b. Démarrez une console Windows PowerShell avec des autorisations élevées et exécutez `Import-Module BootEventCollector`.

   c. Mettez à jour le registre du disque dur virtuel Nano Server pour activer autologgers. Pour cela, exécutez `Enable-SbecAutoLogger -Path C:\NanoServer\Workloads\IncludingWorkloads.vhd`. Cette opération ajoute une liste de base des événements d'installation et de démarrage les plus courants ; vous pouvez rechercher d'autres personnes dans le Contrôle des sessions de suivi d'événements.

4. Mettez à jour les paramètres BCD dans l'image Nano Server pour activer l'indicateur Événements et définissez l'ordinateur collecteur pour vous assurer que les événements de diagnostic sont envoyés au serveur approprié. Notez l'adresse IPv4, le port TCP et la clé de chiffrement de l'ordinateur collecteur que vous avez configurés dans le fichier Active.XML du collecteur (décrits ailleurs dans cette rubrique). Utilisez cette commande dans une console Windows PowerShell avec des autorisations élevées : `Enable-SbecBcd -Path C:\NanoServer\Workloads\IncludingWorkloads.vhd -CollectorIp 192.168.100.1 -CollectorPort 50000 -Key a.b.c.d`

5. Mettez à jour l'ordinateur collecteur pour recevoir l'événement envoyé par l'ordinateur Nano Server en ajoutant la plage d'adresses IPv4, l'adresse IPv4 spécifique ou l'adresse MAC de Nano Server au fichier Active.XML sur l'ordinateur collecteur (voir la section Configuration de l'ordinateur collecteur de cette rubrique).

# Démarrage du service collecteur d'événements

Une fois qu'un fichier de configuration valide est enregistré sur l'ordinateur collecteur et qu'un ordinateur cible est configuré, dès que l'ordinateur cible est redémarré, la connexion au collecteur est établie et les événements sont collectés.

Le journal du service collecteur lui-même (qui est distinct des données d'installation et de démarrage collectées par le service) se trouve sous Microsoft-Windows-BootEvent-Collector/Administration. Pour une interface graphique pour les événements, utilisez l'observateur d'événements. Créez une vue ; développez **Journaux des applications et des services**, puis **Microsoft**, puis **Windows**. Recherchez **BootEvent-Collector, développez-le** et **recherchez l'administrateur**.

- Avec Windows PowerShell : `Get-WinEvent -LogName Microsoft-Windows-BootEvent-Collector/Admin`
- Dans une invite de commandes ordinaire : **wevtutil qe Microsoft-Windows-BootEvent-Collector/Administration**

# Troubleshooting

## Résolution des problèmes d'installation de la fonctionnalité

Agrandir le tableau

| Error | Description de l'erreur | Symptom | Problème potentiel |
|---|---|---|---|
| Dism.exe | 87 | L'option feature-name n'est pas reconnue dans ce contexte | Cela peut se produire si vous avez mal orthographié le nom de la fonctionnalité. Vérifiez que vous disposez de l'orthographe correcte, puis réessayez. Vérifiez que cette fonctionnalité est disponible sur la version du système d'exploitation que vous utilisez. Dans Windows PowerShell, exécutez `dism /online /get-features | ?{$_ -match boot}`. Si aucune correspondance n'est retournée, vous exécutez probablement une version qui ne prend pas en charge cette fonctionnalité. |
| Dism.exe | 0x800f080c | La fonctionnalité `<name>` est inconnue. | Identique à ce qui précède |

## Résolution des problèmes du collecteur

**Exploitation forestière:** Le collecteur enregistre ses propres événements en tant que fournisseur ETW Microsoft-Windows-BootEvent-Collector. C'est le premier endroit où vous devez rechercher la résolution des problèmes avec le collecteur. Vous pouvez les trouver dans l'observateur d'événements sous Journaux des applications et des services > Microsoft > Windows > BootEvent-Collector > Administration, ou vous pouvez les lire dans une fenêtre de commande avec l'une des commandes suivantes :

Dans une invite de commandes ordinaire : **wevtutil qe Microsoft-Windows-BootEvent-Collector/Administration**

Dans une invite Windows PowerShell : `Get-WinEvent -LogName Microsoft-Windows-BootEvent-Collector/Admin` (vous pouvez ajouter `-Oldest` pour retourner la liste dans l'ordre chronologique avec d'abord les événements les plus anciens)

Vous pouvez ajuster le niveau de détail dans les journaux à partir de l'erreur, en passant par l'avertissement, les informations (valeur par défaut), les commentaires et le débogage. Les niveaux plus détaillés que les informations sont utiles pour diagnostiquer les problèmes liés aux ordinateurs cibles qui ne se connectent pas, mais ils peuvent générer une grande quantité de données. Utilisez-les donc avec précaution.

Vous définissez le niveau de journalisation minimal dans l'élément <collecteur> du fichier de configuration. Par exemple : <collector configVersionMajor=1 minlog=verbose>.

Le niveau détaillé consigne un enregistrement pour chaque paquet reçu au fur et à mesure de son traitement. Le niveau de débogage ajoute plus de détails de traitement et sauvegarde également le contenu de tous les paquets ETW reçus.

Au niveau du débogage, il peut être utile d'écrire le journal dans un fichier plutôt que d'essayer de l'afficher dans le système de journalisation habituel. Pour ce faire, ajoutez un élément supplémentaire dans l'élément <collecteur> du fichier de configuration :

<collector configVersionMajor=1 minlog=debug
log=c :\ProgramData\Microsoft\BootEventCollector\Logs\log.txt>

**Une approche suggérée pour résoudre les problèmes liés au collecteur :**

1. Tout d'abord, vérifiez que le collecteur a reçu la connexion de la cible (il crée le fichier uniquement lorsque la cible commence à envoyer les messages) avec

   ```
   Get-SbecForwarding
   ```

   S'il retourne qu'il y a une connexion à partir de cette cible, le problème peut se trouver dans les paramètres de l'autologger. S'il ne retourne rien, le problème est lié à la connexion KDNET avec laquelle commencer. Pour diagnostiquer les problèmes de connexion KDNET, essayez de vérifier la connexion à partir des deux extrémités (c'est-à-dire à partir du collecteur et de la cible).

2. Pour afficher les diagnostics étendus à partir du collecteur, ajoutez ceci à l'élément <collecteur> du fichier de configuration : <collecteur ... minlog=verbose>. Cela permet d'activer les messages relatifs à chaque paquet reçu.

3. Vérifiez si des paquets sont reçus. Si vous le souhaitez, vous pouvez écrire le journal en mode détaillé directement dans un fichier plutôt que via ETW. Pour ce faire, ajoutez ceci à l'élément <collector> du fichier de configuration : <collector ... minlog=verbose log=c:\ProgramData\Microsoft\BootEventCollector\Logs\log.txt>

4. Vérifiez dans les journaux des événements les messages concernant les paquets reçus. Vérifiez si des paquets sont reçus. Si les paquets sont reçus mais incorrects, vérifiez les messages d'événement pour plus d'informations.

5. Du côté cible, KDNET écrit des informations de diagnostic dans le registre. Recherchez les messages dans **HKLM\SYSTEM\CurrentControlSet\Services\kdnet** . KdInitStatus (DWORD) = 0 en cas de réussite et affiche un code d'erreur sur l'erreur KdInitErrorString = explication de l'erreur (contient également des messages d'information si aucune erreur)

6. Exécutez Ipconfig.exe sur la cible et recherchez le nom de l'appareil qu'il signale. Si KDNET a été correctement chargé, le nom de l'appareil doit ressembler à kdnic au lieu du nom de la carte du fournisseur d'origine.

7. Vérifiez si DHCP est configuré pour la cible. KDNET nécessite absolument DHCP.

8. Vérifiez que le collecteur se trouve sur le même réseau que la cible. Si ce n'est pas le cas, vérifiez si le routage est correctement configuré, en particulier le paramètre de passerelle par défaut pour DHCP.

**État de la connexion**

Vous pouvez consulter la liste actuelle des connexions établies et des informations sur l'emplacement où les données sont transférées avec `Get-SbecForwarding`.

Vous pouvez également obtenir l'historique récent des modifications d'état dans les connexions avec `Get-SbecHistory`.

## Résolution des problèmes liés à la définition d'une nouvelle configuration

Si vous avez appliqué la configuration avec la commande `$result = (Get-Content .\newconfig.xml | Set-SbecActiveConfig); $result` Windows PowerShell `$result`, la variable contient des informations sur le déploiement. Vous pouvez interroger cette variable pour en obtenir différentes informations :

Obtient des informations sur des erreurs avec `$result.ErrorString`. Si des erreurs sont signalées ici, la nouvelle configuration n'a pas été appliquée et l'ancienne configuration reste inchangée.

Obtenez des avertissements avec `$result.WarningString`.

Obtenez des informations sur les détails de la configuration avec `$result.InfoString`.

Vous pouvez obtenir le résultat complet avec `$result | fl *`. Sinon, si vous ne souhaitez pas enregistrer le résultat dans une variable, vous pouvez utiliser `Get-Content .\newconfig.xml | Set-SbecActiveConfig | fl *`.

## Résolution des problèmes liés aux ordinateurs cibles

Agrandir le tableau

| Error | Description de l'erreur | Problème potentiel |
|---|---|---|
| Ordinateur cible | La cible ne se connecte pas au | L'ordinateur cible n'a pas été redémarré après sa configuration. Redémarrer l'ordinateur cible. L'ordinateur cible a des paramètres |

| Error | Description de l'erreur | Problème potentiel |
| --- | --- | --- |
| | collecteur | BCD incorrects. Vérifiez les paramètres dans la section Valider les paramètres de l'ordinateur cible. Corrigez si nécessaire, puis redémarrez l'ordinateur cible.<br>Le pilote KDNET/EVENT-NET n'a pas pu se connecter à un adaptateur réseau ou à l'adaptateur réseau incorrect. Dans Windows PowerShell, exécutez et vérifiez `gwmi Win32_NetworkAdapter` la sortie d'une carte **réseau** ServiceName. Si l'adaptateur réseau incorrect est sélectionné, effectuez à nouveau les étapes décrites dans Pour spécifier un adaptateur réseau. Si l'adaptateur réseau n'apparaît pas du tout, il se peut que le pilote ne prend en charge aucun de vos adaptateurs réseau.<br><br>**Voir aussi :** Une approche suggérée pour résoudre les problèmes du collecteur ci-dessus, en particulier les étapes 5 à 8. |
| Collector | Je ne vois plus d'événements après la migration de la machine virtuelle sur laquelle mon collecteur est hébergé. | Vérifiez que l'adresse IP de l'ordinateur collecteur n'a pas changé. Si c'est le cas, consultez Pour activer l'envoi d'événements ETW via le transport à distance. |
| Collector | Les fichiers ETL ne sont pas créés. | `Get-SbecForwarding` indique que la cible s'est connectée, sans erreur, mais que les fichiers ETL ne sont pas créés.<br><br>L'ordinateur cible n'a probablement pas encore envoyé de données ; les fichiers ETL sont créés uniquement lorsque des données sont reçues. |
| Collector | Un événement n'apparaît pas dans le fichier ETL. | L'ordinateur cible a envoyé un événement, mais lorsque le fichier ETL est lu avec l'observateur d'événements de Message Analyzer, l'événement n'est pas présent. L'événement pourrait encore se trouver dans la mémoire tampon. Les événements ne sont pas écrits dans le fichier ETL tant qu'une mémoire tampon complète de 64 Ko n'est pas collectée ou tant qu'un délai d'expiration d'environ 10 à 15 secondes sans aucun nouvel événement ne s'est produit. Attendez la fin du délai d'expiration ou videz les mémoires tampons avec `Save-SbecInstance`.<br><br>Le manifeste d'événement n'est pas disponible sur l'ordinateur collecteur ou l'ordinateur sur lequel l'observateur d'événements ou l'analyseur de messages s'exécute. Dans ce cas, le collecteur peut ne pas être en mesure de traiter l'événement (consultez le journal du collecteur) ou l'observateur peut ne pas être en mesure de l'afficher. Il est recommandé d'installer tous les manifestes sur |

| Error | Description de l'erreur | Problème potentiel |
| --- | --- | --- |
| | | l'ordinateur collecteur et d'installer les mises à jour sur l'ordinateur collecteur avant de les installer sur les ordinateurs cibles. |

# Commencer avec la journalisation de l'inventaire logiciel

15/08/2025

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

La journalisation de l'inventaire logiciel regroupe les données d'inventaire logiciel Microsoft par serveur. Avant d'utiliser la journalisation de l'inventaire logiciel avec Windows Server 2012 R2, assurez-vous que les 3000850 de la base de connaissances Windows Update et les 3060681 de base de connaissances sont installées sur chaque système qui sera inventorié. Aucune mise à jour Windows Update n'est requise pour Windows Server 2016. En outre, si vous souhaitez utiliser la fonctionnalité SIL pour transférer des données vers un serveur d'agrégation, assurez-vous que vous disposez de certificats SSL valides pour votre réseau.

## Description de la fonctionnalité

La journalisation de l'inventaire logiciel dans Windows Server est une fonctionnalité comprenant des applets de commande PowerShell qui permettant aux administrateurs de serveurs de récupérer la liste des logiciels qui sont installés sur ces derniers. De plus, elle collecte et transmet ces données régulièrement à un serveur web cible via le réseau, à l'aide du protocole HTTPS, à des fins d'agrégation. La gestion de cette fonctionnalité, principalement pour la collecte et le transfert quotidiens, est également assurée par des commandes PowerShell.

> ⓘ **Notes**
>
> Un serveur d'agrégation exécutant un service web peut être configuré séparément. En savoir plus sur Agrégateur de journalisation de l'inventaire logiciel.

> ⓘ **Important**
>
> Aucune des données collectées par la journalisation de l'inventaire logiciel n'est envoyée à Microsoft dans le cadre du mode de fonctionnement de la fonctionnalité.

## Applications pratiques

La journalisation de l'inventaire logiciel vise à réduire les coûts d'exploitation liés à la récupération d'informations précises concernant les logiciels Microsoft déployés localement sur un serveur, mais plus particulièrement sur de nombreux serveurs d'un environnement informatique (en supposant qu'elle est déployée et activée dans l'environnement informatique). La possibilité de transférer ces données à un serveur d'agrégation (s'il est configuré séparément par un administrateur) permet une collecte centralisée des données par un processus uniforme et automatique. Même s'il est possible d'obtenir le même résultat en interrogeant directement les interfaces, la journalisation de l'inventaire logiciel, à l'aide d'une architecture de transmission (via le réseau) mise en œuvre par chaque serveur, permet de relever les défis liés à la découverte des ordinateurs, défis typiques de nombreux scénarios de gestion des actifs et des inventaires logiciels. Le protocole SSL est utilisé pour sécuriser la transmission des données par HTTPS au serveur d'agrégation d'un administrateur. La centralisation des données (sur un serveur) facilite l'analyse et la manipulation des données, ainsi que la création de rapports sur celles-ci. Il est important de noter qu'aucune de ces données n'est envoyée à Microsoft dans le cadre du mode de fonctionnement de la fonctionnalité. Les fonctions et données de la journalisation de l'inventaire logiciel sont réservées aux administrateurs et au propriétaire titulaire d'une licence du logiciel serveur.

La journalisation de l'inventaire logiciel peut aider les administrateurs des serveurs à exécuter les tâches suivantes :

- Récupération à distance et à la demande des informations d'inventaire logiciel et serveur depuis les serveurs Windows.
- Agrégation des informations d'inventaire logiciel et serveur pour un large éventail de scénarios de gestion des actifs logiciels en activant la fonctionnalité Journalisation de l'inventaire logiciel de chaque serveur et en choisissant un URI cible de serveur web et une empreinte numérique du certificat pour l'authentification.

# Voir aussi

Agrégateur de journalisation de l'inventaire logiciel
Gérer la journalisation de l'inventaire logiciel
Cmdlets de journalisation de l'inventaire logiciel dans Windows PowerShell
Microsoft Assessment and Planning Toolkit Outil Gestion de l'activation en volume

# Gérer la journalisation de l’inventaire logiciel

16/08/2025

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

Ce document explique comment gérer la journalisation de l’inventaire logiciel, une fonctionnalité qui permet aux administrateurs de centres de données de consigner facilement les données de gestion des ressources logicielles Microsoft pour leur déploiement au fil du temps. Ce document explique comment gérer la journalisation de l’inventaire logiciel. Avant d’utiliser la journalisation de l’inventaire logiciel avec Windows Server 2012 R2, vérifiez que les mises à jour Windows KB 3000850 et KB 3060681 sont installées sur chaque système à inventorier. Aucune mise à jour Windows Update n’est nécessaire pour Windows Server 2016. Cette fonctionnalité s’exécute localement sur chaque serveur à inventorier. Elle ne collecte pas de données depuis des serveurs distants.

La fonctionnalité Journalisation de l'inventaire logiciel peut également être ajoutée à deux versions de Windows Server antérieures à Windows Server 2012 R2. Vous pouvez installer les mises à jour suivantes pour ajouter la fonctionnalité Journalisation de l’inventaire logiciel à Windows Server 2012 et Windows Server 2008 R2 SP1 :

- **Windows Server 2012 (Standard ou Datacenter Edition)**

> ⓘ **Notes**
>
> Assurez-vous d’avoir installé WMF 4.0 avant d’appliquer le package de mise à jour ci-dessous.

- Package de mise à jour de WMF 4.0 pour Windows Server 2012 : KB 3119938

- **Windows Server 2008 R2 SP1**

> ⓘ **Notes**
>
> Assurez-vous d’avoir installé WMF 4.0 avant d’appliquer le package de mise à jour ci-dessous.

- Nécessite .NET Framework 4.5

- Package de mise à jour de WMF 4.0 pour Windows Server 2008 R2 : KB 3109118

Il existe deux méthodes principales pour l'inventaire à l'aide de cette fonctionnalité :

1. Démarrage de la fonctionnalité de journalisation SIL pour collecter à partir de sources de données SIL et transmettre la charge utile par le réseau vers une cible spécifiée (URI) toutes les heures.

2. Interrogation manuelle des données SIL à l'aide de PowerShell ou WMI à n'importe quel intervalle.

Le démarrage de la journalisation SIL implique une planification et une prévoyance, mais présente des avantages importants par rapport à l'interrogation manuelle des données. L'utilisation de la journalisation SIL présente trois principaux avantages pour les administrateurs de centre de données :

- Un historique permanent (journal) peut être collecté au fil du temps, générant des rapports flexibles et complets à partir d'une source unique.

- Les défis relatifs à la découverte des ordinateurs typiques de nombreux outils d'inventaire peuvent être surmontés.

- Les défis relatifs aux délimitations d'approbation et la nécessité de privilèges utilisateur élevés typiques de nombreux outils d'inventaire peuvent être surmontés tout en conservant un niveau de sécurité, dans la mesure où les données sont chiffrées sur HTTPS avec SSL.

La journalisation de l'inventaire logiciel est installée par défaut, mais elle ne démarre par défaut. La configuration de la journalisation de l'inventaire logiciel est effectuée avec les applets de commande PowerShell. Seules quelques options de configuration sont disponibles pour la journalisation de l'inventaire logiciel. Ce document décrit ces options et leur objectif, ainsi que les applets de commande destinées à la collection de données (si vous utilisez la deuxième méthode ci-dessus).

**Dans ce document**

Les options de configuration traitées dans ce document incluent :

- Démarrage et arrêt de la journalisation de l'inventaire logiciel

- Journalisation de l'inventaire logiciel au fil du temps

- Affichage des données de journalisation de l'inventaire logiciel

- Suppression des données consignées par la journalisation de l'inventaire logiciel

- [Sauvegarde et restauration des données consignées par la journalisation de l'inventaire logiciel]manage-software-inventory-logging.md#BKMK_Step5)

- Lecture des données consignées et publiées par la journalisation de l'inventaire logiciel
- Sécurité de la journalisation de l'inventaire logiciel
- Utilisation des paramètres de date et d'heure dans la journalisation de l'inventaire logiciel Windows Server
- Activation et configuration de la journalisation de l'inventaire logiciel dans un disque dur virtuel monté
- Vue d'ensemble de l'utilisation de la journalisation de l'inventaire logiciel dans Windows Server 2012 R2 sans KB 3000850
- Utilisation de la journalisation de l'inventaire logiciel dans un environnement Windows Server 2012 R2 Hyper-V sans KB 3000850

> ⓘ **Notes**
>
> Cette rubrique inclut des exemples d'applets de commande Windows PowerShell que vous pouvez utiliser pour automatiser certaines des procédures décrites. Pour plus d'informations, consultez l'utilisation des cmdlets.

# Démarrage et arrêt de la journalisation de l'inventaire logiciel

La journalisation quotidienne de l'inventaire des logiciels et sa transmission sur le réseau doivent être activées sur un ordinateur exécutant Windows Server 2012 R2 pour consigner l'inventaire des logiciels.

> ⓘ **Notes**
>
> Vous pouvez utiliser l'applet de commande PowerShell **Get-SilLogging** pour récupérer des informations sur le service de journalisation de l'inventaire logiciel, notamment s'il est en cours d'exécution ou arrêté.

## Pour démarrer la journalisation de l'inventaire logiciel

1. Connectez-vous au serveur avec un compte disposant des privilèges d'administrateur local.
2. Ouvrez PowerShell en tant qu'administrateur.

3. À l'invite de PowerShell, tapez **Start-SilLogging**

> ⓘ **Notes**
>
> Il est possible de définir la cible sans définir d'empreinte de certificat, mais si vous le faites, les transferts échoueront et les données seront stockées localement pour une durée par défaut maximale de 30 jours (après quoi elles sont supprimées). Une fois qu'un hachage de certificat valide a été défini pour la cible (et qu'un certificat valide correspondant a été installé dans le magasin LocalMachine/Personal), les données stockées localement sont transmises à la cible, tant que celle-ci est configurée pour accepter ces données avec ce certificat (pour plus d'informations, voir Software Inventory Logging Aggregator ).

### Pour arrêter la journalisation de l'inventaire logiciel

1. Connectez-vous au serveur avec un compte disposant des privilèges d'administrateur local.
2. Ouvrez PowerShell en tant qu'administrateur.
3. À l'invite de PowerShell, tapez **Stop-SilLogging**

## Configuration de la journalisation de l'inventaire logiciel

Il existe trois étapes de configuration de la journalisation de l'inventaire logiciel pour transmettre des données à un serveur d'agrégation dans le temps :

1. Utilisez **Set-SilLogging –TargetUri** pour spécifier l'adresse web de votre serveur d'agrégation (elle doit commencer par « https:// »).
2. Utilisez **Set-SilLogging –CertificateThumbprint** pour spécifier le hachage d'empreinte de votre certificat SSL valide à utiliser pour authentifier les transmissions de données vers votre serveur d'agrégation (celui-ci devra être configuré pour accepter le hachage).
3. Installez un certificat SSL valide (pour votre réseau) dans le **magasin Local Machine/Personal** (ou **/LocalMachine/MY**) du serveur local à partir duquel transférer des données.

Il est préférable d'effectuer ces étapes avant d'utiliser **Start-SilLogging**. Si vous souhaitez les utiliser après l'utilisation de **Start-SilLogging**, vous devez simplement arrêter et redémarrer SIL.

Vous pouvez également utiliser l'applet de commande Publish-SilData pour vérifier que le serveur d'agrégation dispose d'un ensemble complet des données pour ce serveur.

Pour obtenir un guide complet sur la configuration de l'infrastructure SIL dans son ensemble, voir Software Inventory Logging Aggregator. En particulier, si **Publish-SilData** génère une erreur ou que la journalisation SIL échoue par ailleurs, voir la section de dépannage.

# Journalisation de l'inventaire logiciel au fil du temps

Si un administrateur a démarré la journalisation de l'inventaire logiciel, la collection toutes les heures et le transfert des données vers le serveur d'agrégation (URI cible) commencent. Le premier transfert de données sera un ensemble de données complet des mêmes données que Get-SilData récupère et affiche sur la console à un moment donné. Par la suite, à chaque intervalle, SIL effectue une vérification des données et transfère uniquement un petit justificatif d'identification au serveur cible d'agrégation si les données n'ont pas changé depuis la dernière collecte. Si une valeur a changé, SIL envoie à nouveau un jeu de données complet.

> ⓘ **Important**
>
> Si, à n'importe quel intervalle, l'URI cible est inaccessible ou le transfert des données sur le réseau a échoué pour une raison quelconque, les données collectées sont stockées localement pour une durée par défaut maximale de 30 jours (après quoi elles sont supprimées). Lors du transfert suivant des données au serveur cible d'agrégation, toutes les données stockées localement sont transférées et les données mises en cache locales sont supprimées.

# Affichage des données de journalisation de l'inventaire logiciel

Outres les applets de commande PowerShell décrites dans la section précédente, six autres applets de commande peuvent être utilisées pour collecter des données de journalisation de l'inventaire logiciel :

- **Get-SilComputer** : affiche les valeurs à un moment donné pour des données relatives à un serveur et à un système d'exploitation spécifiques, ainsi que le nom de domaine complet ou le nom de l'hôte physique, si disponible.

- **Get-SilComputerIdentity (KB 3000850)** : affiche les identificateurs utilisés par SIL pour des serveurs individuels.
- **Get-SilData** : affiche une collection à un moment donné de toutes les données de journalisation de l'inventaire logiciel.
- **Get-SilSoftware** : affiche l'identité à un moment donné de tous les logiciels installés sur l'ordinateur.
- **Get-SilUalAccess** : affiche le nombre total de demandes de périphérique client et de demandes d'utilisateur client uniques au serveur à partir de deux jours antérieurs.
- **Get-SilWindowsUpdate** : affiche la liste à un moment donné de toutes les mises à jour de Windows installées sur l'ordinateur.

Un cas d'utilisation typique des cmdlets de journalisation de l'inventaire logiciel consiste pour un administrateur à interroger la journalisation de l'inventaire logiciel pour obtenir une collecte instantanée de toutes les données de journalisation de l'inventaire logiciel à l'aide de Get-SilSoftware.

**Exemple de sortie**

```
PS C:\> Get-SilData

ID                 : 961FF8A1-8549-4BEC-8DF6-3B3E32C26FFA
UUID               : B49ACB4C-7D9C-4806-9917-AE750BB3DA84
VMGUID             : E84CCCBD-0D0F-486B-A424-9780C7CF92E4
Name               : Server01Guest.Test.Contoso.com
HypervisorHostName : Server01.Test.Contoso.com

ID          : {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}
Name        : Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219
InstallDate : 12/5/2013
Publisher   : Microsoft Corporation
Version     : 10.0.40219

ID          : {89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}
Name        : Microsoft Silverlight
InstallDate : 3/20/2014
Publisher   : Microsoft Corporation
Version     : 5.1.30214.0

ChassisSerialNumber       : 4452-0564-0284-2290-0113-6804-05
CollectedDateTime         : 10/27/2014 4:01:33 PM
Model                     : Virtual Machine
Name                      : Server01Guest.Test.Contoso.com
NumberOfCores             : 1
NumberOfLogicalProcessors : 1
```

```
NumberOfProcessors        : 1
OSName                    : Microsoft Windows Server 2012 R2 Datacenter
OSSku                     : 8
OSSuite                   : 400
OSSuiteMask               : 400
OSVersion                 : 6.3.9600
ProcessorFamily           : 179
ProcessorManufacturer     : GenuineIntel
ProcessorName             : Intel(R) Xeon(R) CPU           E5440  @ 2.83GHz
SystemManufacturer        : Microsoft Corporation
```

> ⓘ **Notes**
>
> La sortie de cette applet de commande est la même que celle de toutes les autres applets de commande **Get-Sil** pour cette fonctionnalité combinée, mais elle est fournie à la console de façon asynchrone. De ce fait, l'ordre des objets peut ne pas toujours être le même.
>
> Il n'est pas nécessaire d'avoir commencé à utiliser la journalisation de l'inventaire logiciel pour utiliser les applets de commande **Get-Sil**.

# Suppression des données consignées par la journalisation de l'inventaire logiciel

La journalisation de l'inventaire logiciel n'est pas destinée à être un composant essentiel. Elle a été conçue pour affecter le moins possible les opérations système locales tout en maintenant un haut niveau de fiabilité. Elle permet également à l'administrateur de supprimer manuellement la base de données de la journalisation de l'inventaire logiciel et les fichiers associés (chaque fichier présent dans le répertoire \Windows\System32\LogFiles\SIL) pour répondre aux besoins opérationnels.

## Pour supprimer les données consignées par la journalisation de l'inventaire logiciel

1. Dans PowerShell, arrêtez la journalisation de l'inventaire logiciel avec la commande Stop-SilLogging .
2. Ouvrez l'Explorateur Windows.
3. Accédez au dossier **\Windows\System32\Logfiles\SIL**.
4. Supprimez tous les fichiers de ce dossier.

# Sauvegarde et restauration des données consignées par la journalisation de l'inventaire logiciel

La journalisation de l'inventaire logiciel stocke temporairement les collections de données effectuées toutes les heures si le transfert sur le réseau échoue. Les fichiers journaux sont stockés dans le répertoire \Windows\System32\LogFiles\SIL\. Les sauvegardes des données de journalisation de l'inventaire logiciel peuvent être effectuées avec vos sauvegardes planifiées du serveur.

> **ⓘ Important**
>
> Si, pour une raison quelconque, une réparation de l'installation ou une mise à niveau du système d'exploitation est nécessaire, tous les fichiers journaux stockés localement seront perdus.  Si ces données sont importantes pour les opérations, il est recommandé de les sauvegarder avant l'installation du nouveau système d'exploitation. Après la réparation ou la mise à niveau, restaurez simplement les données au même emplacement.

> **ⓘ Notes**
>
> Si, pour une raison quelconque, la gestion de la durée de rétention des données enregistrées localement par SIL devient importante, elle peut être configurée en modifiant la valeur de Registre : \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SoftwareInventoryLogging. La valeur par défaut est « 30 » pour 30 jours.

# Lecture des données consignées et publiées par la journalisation de l'inventaire logiciel

Les données enregistrées par SIL mais stockées localement (si le transfert vers l'URI cible échoue) ou les données transférées au serveur cible d'agrégation sont stockées dans un fichier binaire (pour les données de chaque jour). Pour afficher ces données dans PowerShell, utilisez l'applet de commande Import-BinaryMiLog.

# Sécurité de la journalisation de l'inventaire logiciel

Des privilèges d'administrateur sur le serveur local sont requis pour récupérer les données à partir des API WMI et PowerShell de la journalisation de l'inventaire logiciel.

Pour exploiter correctement la fonctionnalité complète de journalisation de l'inventaire logiciel afin de transférer des données vers un point d'agrégation en permanence au fil du temps (à des intervalles d'une heure), un administrateur doit utiliser des certificats clients pour garantir des sessions SSL sécurisées pour le transfert de données via le protocole HTTPS. Vous trouverez ici une vue d'ensemble de l'authentification HTTPS : Authentification HTTPS.

Toutes les données stockées localement sur un serveur Windows (se produit uniquement si la fonctionnalité est démarrée mais la cible est inaccessible pour une raison quelconque) ne sont accessibles qu'avec des privilèges d'administrateur sur le serveur local.

# Utilisation des paramètres de date et d'heure dans la journalisation de l'inventaire logiciel Windows Server 2012 R2

- Lorsque vous utilisez Set-SilLogging - TimeOfDay pour définir le moment auquel la journalisation SIL s'exécute, vous devez spécifier une date et une heure. La date du calendrier est définie et la journalisation n'a pas lieu tant que la date n'est pas atteinte, en heure locale du système.

- Lorsque vous utilisez Get-SilSoftware ou Get-SilWindowsUpdate, « InstallDate » affiche toujours 12:00:00 AM, une valeur sans signification.

- Lorsque vous utilisez Get-SilUalAccess, « SampleDate » affiche toujours 11:59:00 PM, une valeur sans signification.  La date est la donnée pertinente pour ces requêtes d'applet de commande.

# Activation et configuration de la journalisation de l'inventaire logiciel dans un disque dur virtuel monté

La journalisation de l'inventaire logiciel prend également en charge la configuration et l'activation sur des ordinateurs virtuels hors connexion. Les utilisations pratiques couvrent les paramètres « d'image gold » pour le déploiement à grande échelle entre les centres de données, ainsi que la configuration des images des utilisateurs finals, qu'il s'agisse d'un déploiement de site local ou de cloud.

Pour prendre en charge ces utilisations, la journalisation de l'inventaire logiciel comporte des entrées de Registre associées à chaque option configurable. Vous trouverez ces valeurs de Registre sous \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SoftwareInventoryLogging.

Agrandir le tableau

| Fonction | Nom de la valeur | Données | Applet de commande correspondante (disponible uniquement dans le système d'exploitation en cours d'exécution) |
|---|---|---|---|
| Fonctionnalité de démarrage/d'arrêt | CollectionState | 1 ou 0 | Démarrer-SilLogging, Arrêter-SilLogging |
| Spécifie le point d'agrégation cible sur le réseau | TargetUri | chaîne | Set-SilLogging - TargetURI |
| Spécifie l'empreinte du certificat ou le hachage du certificat utilisé pour l'authentification SSL pour le serveur web cible | CertificateThumbprint | chaîne | Set-SilLogging - CertificateThumbprint |
| Spécifie la date et l'heure auxquelles la fonctionnalité débute (si la valeur définie est dans le futur selon l'heure système locale) | Heure de collecte | Par défaut : 2000-01-01T03:00:00 | Set-SilLogging -TimeOfDay |

Pour modifier ces valeurs sur un disque dur virtuel hors connexion (système d'exploitation de l'ordinateur inactif), un disque dur virtuel doit tout d'abord être monté, et ensuite les commandes suivantes peuvent être utilisées pour apporter des modifications :

- Chargement reg
- Suppression du Registre
- Reg add
- Déchargement reg

La journalisation de l'inventaire logiciel vérifie ces valeurs lorsque le système d'exploitation démarre et s'exécute en conséquence.

# Vue d'ensemble de l'utilisation de la journalisation de l'inventaire logiciel dans Windows Server 2012 R2 sans KB 3000850

Les modifications suivantes des paramètres par défaut et de la fonctionnalité de journalisation de l'inventaire logiciel ont été effectuées avec KB 3000850 :

- L'intervalle par défaut pour la collecte et le transfert sur le réseau lorsque la journalisation SIL démarre est passé de quotidien à chaque heure (au hasard à l'intérieur de chaque heure).
- La charge utile de données par défaut a été réduite pour inclure uniquement les objets provenant de SilComputer, Get-SilComputerIdentity et Get-SilSoftware.
- L'invité pour la communication de canal hôte dans les environnements Hyper-V a été supprimé.

# Utilisation de la journalisation de l'inventaire logiciel dans un environnement Windows Server 2012 R2 Hyper-V sans KB 3000850

> **Notes**
>
> Cette fonctionnalité est supprimée avec l'installation de la mise à jour KB 3000850 .

Lorsque vous utilisez la journalisation de l'inventaire logiciel sur un hôte Hyper-V Windows Server 2012 R2, il est possible d'extraire des données SIL des invités Windows Server 2012 R2 qui s'exécutent localement, si la journalisation SIL a été démarrée dans le ou les invités. Cependant, cette possibilité n'existe que lorsque vous utilisez les applets de commande Powershell Get-SilData et Publish-SilData, et seulement avec Windows Server 2012 R2 dans l'hôte et l'invité.  Cette fonctionnalité vise à permettre aux administrateurs de centre de données qui fournissent des ordinateurs virtuels invités aux locataires ou autres entités d'une grande entreprise, de capturer des données d'inventaire logiciel sur l'hôte hyperviseur et, par la suite, de transférer toutes ces données à un agrégateur (ou un URI cible).

Voici deux exemples de ce à quoi peut ressembler la sortie dans la console PowerShell (très abrégés) sur un hôte Hyper-V Windows Server 2012 R2 exécutant une VM invitée Windows Server 2012 R2 lorsque la journalisation SIL est démarrée.  Vous remarquerez que le premier exemple, qui utilise Get-SilData seul, affiche toutes les données de l'hôte comme prévu.  Toutes

les données SIL de l'invité sont également incluses, mais dans un format réduit.  Pour développer et afficher ces données à partir de l'invité, coupez et collez simplement l'extrait de code utilisé dans le deuxième exemple ci-dessous.  Les objets de données SIL de l'invité auront toujours le GUID de l'ordinateur virtuel associé au sein de l'objet.

> ⓘ **Notes**
>
> Les données SIL étant une sortie sur la console, lors de l'utilisation de l'applet de commande Get-SilData, dans des flux de données, les objets ne sortiront pas systématiquement dans l'ordre prévu.  Dans les deux exemples ci-dessous, le texte a été codé par couleur (bleu pour les données de l'hôte physique et vert pour les données de l'invité virtuel) uniquement comme outil d'illustration de ce document.

# Voir aussi

Prise en main de la journalisation de l'inventaire logicielAgrégateur de la journalisation de l'inventaire logicielApplets de commande de la journalisation de l'inventaire logiciel dans Windows PowerShellImport-BinaryMiLogExport-BinaryMiLog

# Agrégateur de journalisation de l'inventaire logiciel

Article • 09/03/2023

> S'applique à : Windows Server 2022, Windows Server 2019, Windows Server 2012 R2

## Qu'est-ce que Software Inventory Logging Aggregator ?

Software Inventory Logging Aggregator (SILA) reçoit, compile et produit des rapports simples sur le nombre et le type de logiciels professionnels Microsoft installés sur les serveurs Windows d'un centre de données.

SILA est un logiciel que vous installez sur Windows Server, mais qui n'est pas inclus dans l'installation de Windows Server. Pour installer le logiciel, commencez par le télécharger gratuitement à partir du Centre de téléchargement Windows : Software Inventory Logging Aggregator 1.0 pour Windows Server

L'infrastructure de la Journalisation de l'inventaire logiciel permet de réduire les coûts de fonctionnement lors de l'inventaire des logiciels Microsoft déployés sur les nombreux serveurs d'un environnement informatique. Ce framework est constitué de deux composants, le logiciel SIL Aggregator et la fonctionnalité Journalisation de l'inventaire logiciel (SIL) Windows Server, introduite dans Windows Server 2012 R2. Software Inventory Logging Aggregator 1.0 s'installe sur un seul serveur et reçoit des données d'inventaire des serveurs Windows Server configurés pour lui transférer des données via SIL. La conception du logiciel permet aux administrateurs de centre de données d'activer SIL dans des images Windows Server maîtres destinées à une large distribution au sein de leur environnement. Ce package logiciel est le point cible que les clients installent localement pour faciliter la journalisation des données d'inventaire au fil du temps. Ce logiciel permet également de créer régulièrement des rapports d'inventaire simples dans Microsoft Excel. Les rapports Software Inventory Logging Aggregator 1.0 indiquent le nombre d'installations de Windows Server, System Center et SQL Server.

> **ⓘ Important**
>
> Aucune donnée n'est envoyée à Microsoft dans le cadre de l'utilisation de ce logiciel.

## Données collectées par SIL au fil du temps

Une fois le logiciel déployé correctement, les données suivantes peuvent être consultées dans SIL Aggregator :

- Installations uniques de Windows Server dans votre centre de données
- FQDN
- GUID d'identification
- Nombre de processeurs et de cœurs physiques
- Nombre de processeurs virtuels (dans le cas d'une machine virtuelle)
- Modèle et type des processeurs physiques
- Si l'Hyper-Threading est activé ou non sur les processeurs physiques
- Numéro de série du châssis
- Borne haute et identité des machines virtuelles Windows Server s'exécutant simultanément (dans le cas d'un hôte exécutant un hyperviseur) sur chaque hôte, au fil du temps
- Borne haute et nom d'hôte des machines virtuelles Windows Server gérées (agent System Center présent) s'exécutant simultanément sur chaque hôte, au fil du temps
- Nom des agents System Center installés sur les machines virtuelles comptabilisées dans la borne haute gérée
- Nombre et emplacement des installations de SQL Server au fil du temps (uniquement les références et éditions qui nécessitent une licence)
- Listes des logiciels installés dans Ajout/Suppression de programmes

## Qui utilise SIL ?

- **Les professionnels de l'informatique ou les administrateurs de centre de données**, qui recherchent une méthode économique pour collecter des données d'inventaire logiciel précieuses, automatiquement, au fil du temps.
- **Les directeurs informatiques et les contrôleurs financiers**, qui ont besoin de signaler l'utilisation de logiciels d'entreprise Microsoft dans les déploiements informatiques de leur entreprise.

# Mise en route

### Composants requis

Software Inventory Logging Aggregator (SIL Aggregator) installé sur au moins un serveur pour l'agrégation et les rapports, dans une machine virtuelle ou sur du matériel physique :

- **Windows Server 2012 R2** (édition Standard ou Datacenter)
- **Rôle serveur IIS** avec .NET Framework 4.5, les services WCF et l'activation HTTP dans la même arborescence de sélection dans l'**Assistant Ajout de rôles et de fonctionnalités**.
- **SQL Server** 2012 SP2 Standard Edition ou SQL Server 2014 Standard Edition
- **Microsoft Excel 64 bits** 2013 (facultatif pour l'installation, mais nécessaire pour la création de rapports)
- Facultatif : **VMware PowerCLI 5.5.0.5836** (nécessaire dans les environnements VMware)

> ⓘ **Notes**
>
> Quand vous utilisez le Windows Management Framework, il existe un problème de compatibilité connu avec WMF version 5.1, sur SIL Aggregator uniquement. Il n'est pas nécessaire d'aller au-delà de la version 4.0 de WMF sur les serveurs sur lesquels SIL Aggregator est installé.

La journalisation de l'inventaire logiciel (SIL) existe dans les versions de Windows Server disposant des mises à jour suivantes :

- **Windows Server 2016** ou version ultérieure
- **Windows Server 2012 R2** (édition Standard ou Datacenter)
  - Mise à jour de Windows Server 2012 R2 **KB3000850** (novembre 2014)
  - Mise à jour de Windows Server 2012 R2 **KB3060681** (juin 2015) (peut apparaître comme une mise à jour facultative sur Windows Update)

## Sécurité et types de comptes

### Certificats requis

SIL et SIL Aggregator utilisent des certificats SSL pour la communication authentifiée. Pour cela, il suffit généralement d'installer SIL Aggregator avec un certificat (le nom de serveur et le nom de certificat doivent correspondre) pour héberger le service web qui reçoit les données d'inventaire. Ensuite, les serveurs Windows qui doivent être inventoriés à l'aide de la fonctionnalité SIL utilisent un autre certificat client, pour transmettre des données à SIL Aggregator. Une applet de commande PowerShell (Set-SilAggregator, plus d'informations ci-dessous) doit être utilisée pour ajouter des empreintes numériques de certificat à la liste de certificats approuvés de SIL Aggregator à partir desquels l'Aggregator accepte les données associées. SIL Aggregator effectue le traitement et l'insertion dans sa base de données après l'authentification de chaque charge utile de données avec un certificat. Consultez la section **Détails des applets de commande SIL Aggregator** pour plus d'informations sur le fonctionnement.

## Configuration du compte d'interrogation

Quand vous ajoutez des informations d'identification à SIL Aggregator pour activer les opérations d'interrogation, vous devez configurer un compte avec le moins de privilèges possibles. Pour des raisons de sécurité, vous ne devez pas utiliser les mêmes informations d'identification pour plusieurs hôtes dans un centre de données ou un autre déploiement informatique.

Sur l'hôte Windows Server que vous voulez configurer pour qu'il soit interrogé par SIL Aggregator et afin d'éviter le recours à un utilisateur du groupe Administrateurs, procédez comme suit pour accorder l'accès minimum à un compte d'utilisateur :

### Pour configurer un compte d'interrogation

1. Sur l'hôte Hyper-V Windows Server que vous voulez interroger avec SIL Aggregator, créez un compte d'utilisateur local à l'aide de **Gestion de l'ordinateur** dans Windows (veillez à décocher la case qui oblige à modifier le mot de passe lors de la première ouverture de session).

2. Ajoutez cet utilisateur au groupe **Utilisateurs de gestion à distance**.

3. Ajoutez cet utilisateur au groupe **Administrateurs Hyper-V**.

4. Ouvrez **WMIMgmt.msc** avec **Démarrer**->**Exécuter**.

5. Cliquez sur **Autres actions** dans la section **Actions** et sélectionnez **Propriétés**.

6. Cliquez sur **Sécurité**.

7. Sélectionnez l'**espace de noms cimv2** dans l'affichage de l'arborescence **Espace de noms**.
8. Cliquez sur le bouton **Sécurité**.
9. Ajoutez le groupe **Utilisateurs de gestion à distance** au format **nom_ordinateur\nom_groupe**
10. Cliquez sur **OK**.
11. Dans la fenêtre Sécurité de **root\cimv2**, sélectionnez les **Utilisateur de gestion à distance**.
12. Dans la section des autorisations en bas, vérifiez que la case **Appel à distance autorisé** est cochée.
13. Cliquez sur **Appliquer**, puis sur **OK**.
14. Cliquez sur **OK** dans la fenêtre **Propriétés** .

## Installation de SIL Aggregator

Vous devez vérifier les points suivants avant d'installer SIL Aggregator sur un serveur Windows Server :

- **Vous disposez d'un certificat SSL valide** que vous voulez utiliser pour héberger le service web de ce logiciel.
    - Le certificat doit être au format **.pfx**
    - Le nom du serveur Windows et le nom du certificat doivent correspondre.
- **SQL Server Standard Edition est installé** ou est installé sur un serveur distant que vous comptez utiliser avec ce logiciel.
    - SIL Aggregator fonctionne avec SQL Server 2012 SP2 et SQL Server 2014. Aucune configuration particulière de SQL Server n'est nécessaire.
    - Le compte utilisé pour installer SIL Aggregator doit être un rôle administrateur système sur SQL pour pouvoir créer la base de données pendant l'installation.
    - Le compte utilisé pour installer SIL Aggregator doit être ajouté en tant qu'administrateur sur SQL Analysis Services avant d'installer SIL Aggregator.
    - Une fois installé, SQL Server Agent doit être configuré pour s'exécuter automatiquement.

- **Le rôle serveur IIS est ajouté** avec le .Net Framework 4.5, les Services WCF et l'activation HTTP dans la même arborescence de sélection dans l'**Assistant Ajout de rôles et de fonctionnalités**.
- Vous êtes **connecté au serveur avec un compte disposant de privilèges d'administrateur** sur le serveur.
- Vous êtes **connecté au serveur avec un compte disposant des privilèges d'administrateur système sur le serveur SQL Server**, si vous voulez appliquer l'authentification Windows

  OR

  Si vous voulez utiliser l'authentification SQL, **vous disposez du mot de passe pour un compte disposant des privilèges d'administrateur SQL**.

## Pour installer Software Inventory Logging Aggregator

1. Double-cliquez sur **Setup.exe** pour démarrer l'installation.
2. Cliquez sur **Suivant** dans la fenêtre d'accueil.
3. Si vous acceptez le CLUF, cochez la case pour accepter le contrat, puis cliquez sur **Suivant**.
4. Dans **Choisir des fonctionnalités**, sélectionnez **Installer Sofware Inventory Logging Aggregator et le module Rapports**, puis cliquez sur **Suivant**.

   Pour plus d'informations sur l'installation du module Rapports uniquement, consultez `Publish-SilReport` dans la section **Détails des applets de commande SIL Aggregator**.
5. Une fois toutes les conditions préalables vérifiées, cliquez sur **Suivant**.
6. Dans **Choisir un type de compte**, sélectionnez **utilisateur local** ou **gMSA**, selon votre préférence.

   L'option de compte utilisateur local crée un utilisateur local avec un mot de passe fort généré automatiquement. Ce compte est utilisé pour tous les services et opérations de tâches de SIL Aggregator sur le serveur local. L'utilisation des comptes gMSA (comptes de service administrés de groupe) est recommandée si l'Aggregator fait partie d'un domaine Active Directory (Windows Server 2012 et versions ultérieures). Pour plus d'informations sur les comptes gMSA, consultez : Vue d'ensemble des comptes de service administrés de groupe

- L'option de compte gMSA doit être utilisée si vous prévoyez d'exécuter la base de données SQL Server sur un serveur distinct que celui sur lequel SIL Aggregator est installé.
- N'oubliez pas de redémarrer le serveur après l'ajout du compte d'ordinateur au groupe de sécurité gMSA dans Active Directory.

7. Dans **Choisir un serveur SQL Server**, entrez le serveur SQL Server sur lequel votre instance SQL est installée, ou **localhost**, si elle est installée sur le serveur local.

   Un seul SIL Aggregator est pris en charge par instance SQL.

8. Sélectionnez le type d'authentification et cliquez sur **Vérifier SQL**.
9. Cliquez sur **Suivant**, puis sélectionnez un numéro de port dans **Détails du serveur IIS**, ou conservez la valeur par défaut.
10. Accédez à l'emplacement du fichier **.pfx**, tapez son mot de passe, puis cliquez sur **Suivant**.
11. Le dernier écran affiche la progression de l'installation. Une fois terminé, cliquez sur **Terminer**.

# Désinstallation de SIL Aggregator

## Pour désinstaller Software Inventory Logging Aggregator

1. Ouvrez **PowerShell** en tant qu'administrateur, puis tapez `Stop-SilAggregator`. Au retour de l'invite, SIL Aggregator est arrêté.

   Par conception, SIL Aggregator traite les fichiers au bout de 20 minutes ou une fois que 100 fichiers ont été reçus. Dans les environnements à grande échelle, ce scénario ne se produit jamais, mais à petite échelle, certains fichiers peuvent ne pas avoir encore été traités à l'arrêt de l'Aggregator. Utilisez le paramètre `-Force` si vous n'avez pas besoin de conserver ces fichiers et données.

2. Accédez au **Panneau de configuration**, cliquez sur **Programmes et fonctionnalités**, sur **Désinstaller des programmes**, sur **Software Inventory Logging Aggregator**, puis sur **Désinstaller**.

   Software Inventory Logging Aggregator ouvre une fenêtre pour vous inviter à choisir entre la suppression ou la conservation de toutes les données de la base de données. La sélection par défaut est de les conserver (si une réinstallation est

nécessaire, vous pouvez attacher la base de données pour reprendre là où l'Aggregator s'était arrêté).

3. Sélectionnez **Conserver** ou **Supprimer**, puis cliquez sur **Suivant**.

4. Une fois la barre de progression terminée, cliquez sur **Terminer**.

# Commencer à utiliser SIL et SIL Aggregator

## Présentation des applets de commande PowerShell SIL Aggregator

Les commandes suivantes peuvent être exécutées à partir de la console Windows PowerShell en tant qu'administrateur.

| **Applet de commande Windows PowerShell** | **Fonction** |
|---|---|
| `Start-SilAggregator` | Démarre tous les services et tâches de Software Inventory Logging Aggregator. Cette commande permet à l'Aggregator de recevoir des données sur HTTPS à partir de serveurs sur lesquels la journalisation SIL a démarré. |
| `Stop-SilAggregator` | Arrête tous les services et tâches de Software Inventory Logging Aggregator. Si des tâches ou des services se trouvent au milieu d'une opération, cette commande peut s'exécuter après un certain délai. |
| `Set-SilAggregator` | Permet à l'administrateur de modifier la configuration de Software Inventory Logging Aggregator. |
| `Add-SilVmHost` | Utilisée pour ajouter des noms d'hôte spécifiques ou un tableau de noms d'hôte à interroger selon un intervalle régulier (la valeur par défaut est une heure). |
| `Remove-SilVmHost` | Utilisée pour supprimer des noms d'hôte spécifiques ou un tableau de noms d'hôte à interroger selon un intervalle régulier. |
| `Get-SilVMHost` | Utilisée pour récupérer la liste des hôtes physiques auxquels Software Inventory Logging Aggregator doit demander les données d'état d'exécution des machines virtuelles. |
| `Get-SILAggregatorData` | Utilisée pour récupérer des données de la base de données dans la console PowerShell. |

| Applet de commande Windows PowerShell | Fonction |
| --- | --- |
| `Publish-SilReport` | Permet de créer des rapports de base de données sur les données de journalisation de l'inventaire logiciel. **Remarque :** Le traitement du cube sur l'Aggregator ne se produit qu'une fois par jour. Par conséquent, les données capturées au niveau de l'Aggregator n'apparaissent dans les rapports que le jour suivant. |

## Ordre de démarrage suggéré

Une fois que vous avez installé Software Inventory Logging Aggregator sur votre serveur, ouvrez PowerShell en tant qu'administrateur.

- Sur votre SIL Aggregator :
  - Exécutez `Start-SilAggregator`

    Cette opération est nécessaire pour que votre Aggregator reçoive activement sur HTTPS les données des serveurs que vous avez configurés pour l'inventaire. Notez que même si vous avez activé vos serveurs pour qu'ils commencent à effectuer le transfert vers l'Aggregator, cela ne pose pas de problème, car ils mettent en cache leurs charges utiles de données localement pendant 30 jours. Une fois que l'Aggregator, leur « targeturi », est en cours d'exécution, toutes les données mises en cache sont transférées en même temps à l'Aggregator et toutes les données sont traitées.

  - Exécutez `Add-SilVMHost`

    Exemple : `add-silvmhost –vmhostname contoso1 –hostcredential get-credential`

    - Dans cet exemple, **contoso1** est le nom de réseau (ou adresse IP) du serveur hôte physique que votre Aggregagor doit interroger pour consulter les mises à jour régulières concernant les machines virtuelles en cours d'exécution, afin d'assurer le suivi de ces données au fil du temps. Get-Credential invite l'utilisateur connecté à entrer le compte à utiliser pour commencer à interroger cet hôte. L'exécution de la même commande sur le même hôte vous permet de mettre à jour le compte utilisé à tout moment. Soyez attentif aux modifications de mot de passe de compte et aux délais d'expiration dans le temps. Si les informations d'identification sont modifiées ou expirent, l'interrogation sur l'hôte échoue.

    - Par défaut, l'interrogation s'effectue toutes les heures et commence une heure après l'exécution de `Start-SilAggregator` ou une heure après qu'un hôte a été ajouté à la liste d'interrogation. L'intervalle d'interrogation peut être modifié à l'aide de `Set-SilAggregator cmdlet`.

    - Cette applet de commande détecte automatiquement dans une liste prédéfinie d'options (consultez la section **Détails des applets de commande SIL Aggregator**), les valeurs HostType et HyperVisorType appropriées pour l'hôte que vous ajoutez. Si elle ne parvient pas à reconnaître ces options ou si les informations d'identification indiquées sont incorrectes, une invite s'affiche. Si vous acceptez avec une entrée **Y**, l'hôte est ajouté, répertorié comme **Inconnu**, mais il n'est pas interrogé.

  - Exécutez `Set-SilAggregator –AddCertificateThumbprint` « l'empreinte numérique du certificat de votre client »

    Cette commande permet de recevoir des données sur HTTPS des serveurs Windows sur lesquels la journalisation SIL est activée. L'empreinte numérique est ajoutée à la liste des empreintes numériques à partir desquelles SIL Aggregator accepte les données. SIL Aggregator est conçu pour accepter les certificats valides d'authentification client d'entreprise. Le certificat utilisé doit être installé dans le magasin **\localmachine\MY (Ordinateur Local -> Personnel**) sur le serveur qui transfère les données.

- Sur vos serveurs Windows à inventorier, ouvrez PowerShell en tant qu'administrateur et exécutez les commandes suivantes :

  - Exécutez `Set-SilLogging –TargetUri "https://contososilaggregator" –CertificateThumbprint "your client certificate's thumbprint"`

    - Cette commande indique à SIL dans Windows Server l'emplacement où envoyer les données d'inventaire et le certificat à utiliser pour l'authentification.

      > **ⓘ Important**
      >
      > Vérifiez que « https:// » est inclus dans la valeur TargetUri.

    - Vous devez installer le certificat client d'entreprise avec cette empreinte numérique dans **\localmachine\MY** ou utiliser **certmgr.msc** pour installer le certificat dans le magasin **Ordinateur Local -> Personnel**.

> **ⓘ Important**
>
> Si ces valeurs ne sont pas correctes ou si le certificat n'est pas installé dans le magasin approprié (ou n'est pas valide), les transferts vers la cible échouent quand la journalisation SIL est lancée. Les données sont mises en cache localement pendant 30 jours.

- Exécutez `Start-SilLogging`

  Cette commande démarre la journalisation SIL. Toutes les heures, à des intervalles aléatoires, SIL transfère ses données d'inventaire à l'Aggregator spécifié avec le paramètre `-targeturi` . Le premier transfert est un jeu de données complet. Chaque transfert suivant s'apparente davantage à une « pulsation » qui identifie si les données ont changé. Si le jeu de données a été modifié, un autre jeu de données complet est transféré.

- Exécutez `Publish-SilData`

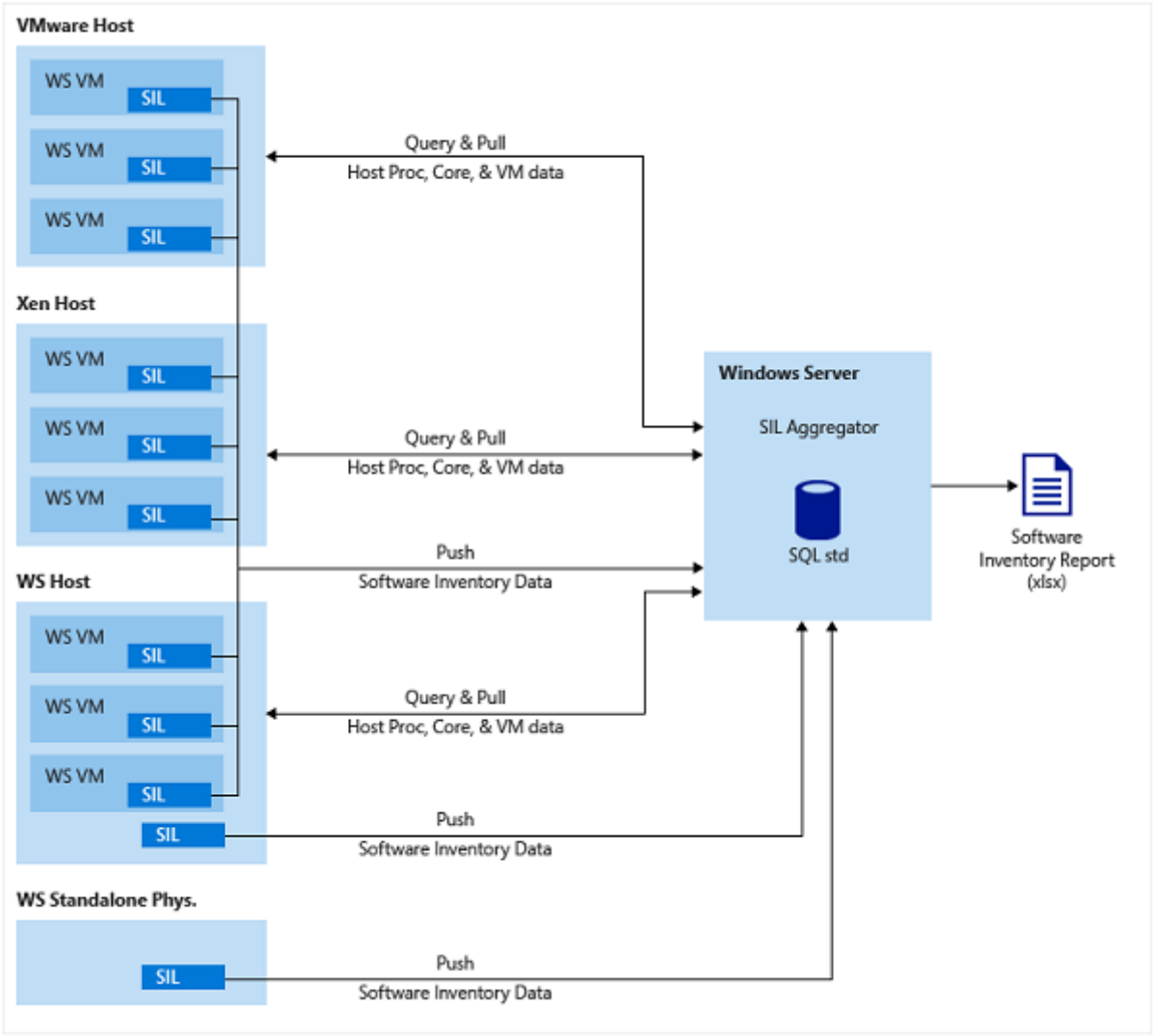
  - La première fois que SIL est activé pour la journalisation, cette étape est facultative.
  - Il s'agit d'un transfert manuel unique d'un jeu complet de données.
  - Si la journalisation SIL a été démarrée depuis un certain temps et qu'un nouveau SIL Aggregator est désigné par `Set-SilLogging`, vous devez exécuter cette applet de commande, une seule fois, pour envoyer un jeu complet de données au nouvel Aggregator.

Une fois que vous avez suivi ces étapes pour ajouter des hôtes physiques exécutant des machines virtuelles Windows Server, ET que vous avez activé la journalisation de l'inventaire logiciel (ou journalisation SIL) au sein de ces serveurs Windows, vous pouvez exécuter `Publish-SilReport -OpenReport` à tout moment sur SIL Aggregator (nécessite Excel 2013). Notez toutefois que le cube SQL Server Analysis Services cube effectue le traitement une fois par jour, les données ne sont donc pas disponibles dans les rapports le jour-même.

# Présentation de l'architecture

La journalisation SIL fonctionne en mode par envoi et par extraction et est constituée de deux composants qui fonctionnent en parallèle : la fonctionnalité de journalisation de l'inventaire logiciel (SIL) dans Windows Server et le MSI téléchargeable Software

Inventory Logging Aggregator (SILA). Les serveurs à inventorier envoient des données d'inventaire logiciel sur HTTPS, à l'aide de la journalisation SIL, à SIL Aggregator (toutes les heures à des points aléatoires au sein de chaque heure). L'Aggregator, à son tour, interroge les hôtes hyperviseur physiques pour extraire des données d'inventaire matériel toutes les heures. Les modes par envoi et par extraction doivent être configurés correctement pour activer toutes les fonctionnalités de SIL. Ils peuvent être configurés dans n'importe quel ordre. Toutefois, le traitement du cube sur l'Aggregator se produit une seule fois par jour, les données capturées sur l'Aggregator, par envoi ou par extraction, n'apparaissent donc pas dans les rapports avant le jour suivant.




> **ⓘ Important**
>
> Aucune donnée n'est envoyée à Microsoft dans le cadre de l'utilisation de ce logiciel.

# Activer SIL sur plusieurs serveurs

Il existe plusieurs façons d'activer SIL dans une infrastructure de serveurs distribués, comme un cloud privé de machines virtuelles. Voici un exemple de la manière de configurer des images Windows Server pour qu'elles envoient automatiquement des données d'inventaire à SIL Aggregator quand elles démarrent sur le réseau pour la première fois.

Exécutez les applets de commande suivantes dans la console PowerShell en tant qu'administrateur sur chaque machine virtuelle ou appareil/ordinateur physique où Windows Server est installé (voir la section **Conditions préalables**) :

Vous devez disposer d'un certificat SSL client valide au format .pfx pour effectuer ces étapes. Vous devez ajouter l'empreinte numérique de ce certificat à SIL Aggregator à l'aide de l'applet de commande `Set-SILAggregator –AddCertificateThumbprint`. Ce certificat client n'a pas besoin de correspondre au nom du SIL Aggregator.

- `$secpasswd = ConvertTo-SecureString "<password for the account with permissions to the network location holding your client pfx file>" -AsPlainText –Force`
- `$mycreds = New-Object System.Management.Automation.PSCredential ("<user account with permissions to the network location holding your client pfx file>", $secpasswd)`
- `$driveLetters = ([int][char]'C')..([int][char]'Z') | % {[char]$_}`
- `$occupiedDriveLetters = Get-Volume | % DriveLetter`
- `$availableDriveLetters = $driveLetters | ? {$occupiedDriveLetters -notcontains $_}`
- `$firstAvailableDriveLetter = $availableDriveLetters[0]`
- `New-PSDrive -Name $firstAvailableDriveLetter -PSProvider filesystem -root <\\server\path to share which holds your pfx certificate file> -credential $mycreds`
- `Copy-Item ${firstAvailableDriveLetter}:\<certificatename.pfx file in directory of new drive> c:\<location of your choice>`
- `Remove-PSDrive –Name $firstAvailableDriveLetter`
- `$mypwd = ConvertTo-SecureString -String "<password for the certificate pfx file>" -Force –AsPlainText`

- `Import-PfxCertificate -FilePath c:\<location\\certificatename.pfx> cert:\localMachine\my -Password $mypwd`
- `Set-sillogging –targeturi "https://<machinename of your SIL Aggregator>" –certificatethumbprint`

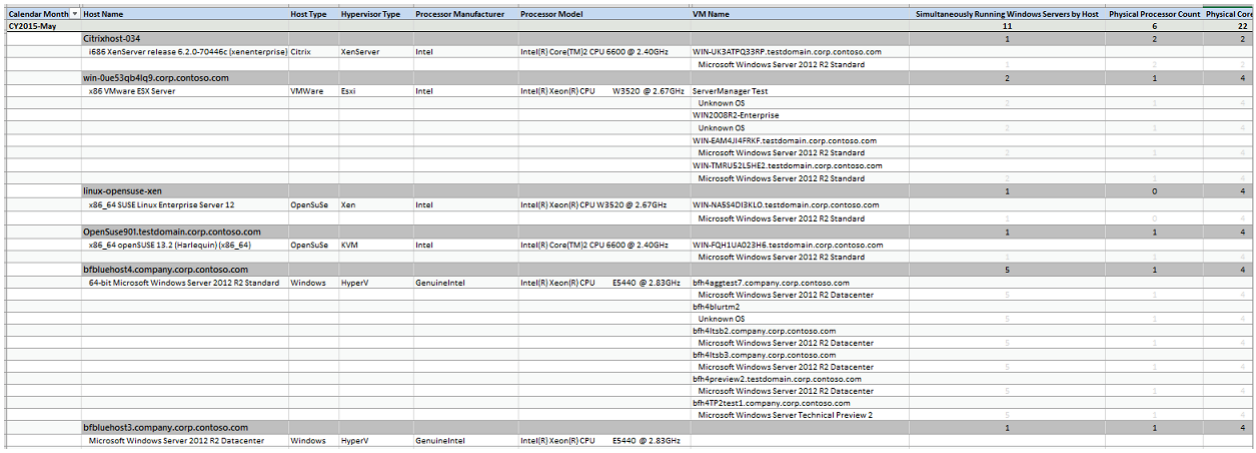
> ⓘ Notes
>
> Utilisez l'empreinte numérique du certificat de votre fichier pfx client ajoutée à SIL Aggregator avec l'applet de commande **Set-SilAggregator `-AddCertificateThumbprint**.

- `Start-sillogging`

Chaque fois que SIL Aggregator n'est pas accessible, les données d'inventaire SIL sont mises en cache localement sur les serveurs Windows pendant 30 jours. Une fois l'envoi correctement effectué à l'Aggregator, toutes les données mises en cache sont transférées.

Ajoutez `Publish-SilData` à la liste ci-dessus si vous envoyez des données SIL à un nouveau SIL Aggregator après avoir réussi plusieurs envois à un ancien Aggregator (cette commande envoie un complément de données SIL dont le nouvel Aggregator a besoin pour cet ordinateur).

# Rapports Software Inventory Logging Aggregator



| Calendar Month | Host Name | Host Type | Hypervisor Type | Processor Manufacturer | Processor Model | VM Name | Simultaneously Running Windows Servers by Host | Physical Processor Count | Physical Core |
|---|---|---|---|---|---|---|---|---|---|
| CY2015-May | | | | | | | 11 | 6 | 22 |
| | Citrixhost-034 | | | | | | 1 | 2 | 2 |
| | i686 XenServer release 6.2.0-70446c (xenenterprise) | Citrix | XenServer | Intel | Intel(R) Core(TM)2 CPU 6600 @ 2.40GHz | WIN-UK3ATPQ33RP.testdomain.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Standard | 1 | 2 | 2 |
| | win-0ue53qb4lq9.corp.contoso.com | | | | | | 2 | 1 | 4 |
| | x86 VMware ESX Server | VMWare | Esxi | Intel | Intel(R) Xeon(R) CPU W3520 @ 2.67GHz | ServerManager Test | | | |
| | | | | | | Unknown OS | 1 | 1 | 4 |
| | | | | | | WIN2008R2-Enterprise | | | |
| | | | | | | Unknown OS | 1 | 1 | 4 |
| | | | | | | WIN-EAM4JI4FRKF.testdomain.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Standard | 1 | 1 | 4 |
| | | | | | | WIN-TMRUS2LSHE2.testdomain.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Standard | 1 | 1 | 4 |
| | linux-opensuse-xen | | | | | | 1 | 0 | 4 |
| | x86_64 SUSE Linux Enterprise Server 12 | OpenSuSe | Xen | Intel | Intel(R) Xeon(R) CPU W3520 @ 2.67GHz | WIN-NA5S4DI3KL0.testdomain.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Standard | 1 | 0 | 4 |
| | OpenSuse901.testdomain.corp.contoso.com | | | | | | 1 | 1 | 4 |
| | x86_64 openSUSE 13.2 (Harlequin) (x86_64) | OpenSuSe | KVM | Intel | Intel(R) Core(TM)2 CPU 6600 @ 2.40GHz | WIN-FQH1UA023H6.testdomain.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Standard | 1 | 1 | 4 |
| | bfbluehost4.company.corp.contoso.com | | | | | | 5 | 1 | 4 |
| | 64-bit Microsoft Windows Server 2012 R2 Standard | Windows | HyperV | GenuineIntel | Intel(R) Xeon(R) CPU E5440 @ 2.83GHz | bfh4aggtest7.company.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Datacenter | 5 | 1 | 4 |
| | | | | | | bfh4blurtm2 | | | |
| | | | | | | Unknown OS | 5 | 1 | 4 |
| | | | | | | bfh4ltsb2.company.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Datacenter | 5 | 1 | 4 |
| | | | | | | bfh4ltsb3.company.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Datacenter | 5 | 1 | 4 |
| | | | | | | bfh4preview2.testdomain.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server 2012 R2 Datacenter | 5 | 1 | 4 |
| | | | | | | bfh4TP2test1.company.corp.contoso.com | | | |
| | | | | | | Microsoft Windows Server Technical Preview 2 | 5 | 1 | 4 |
| | bfbluehost3.company.corp.contoso.com | | | | | | 1 | 1 | 4 |
| | Microsoft Windows Server 2012 R2 Datacenter | Windows | HyperV | GenuineIntel | Intel(R) Xeon(R) CPU E5440 @ 2.83GHz | | | | |

## Traitement du cube

Dans Software Inventory Logging Aggregator, le cube SQL Server Analysis Services est traité une fois par jour à 3:00:00 AM, heure du système local. Les rapports reflètent toutes les données jusqu'à cette heure, mais aucune après cette heure le même jour.

## Borne haute

Un aspect fondamental des rapports Software Inventory Logging Aggregator est la capture de ce qui est communément appelé une « borne haute » des serveurs Windows qui s'exécutent de manière simultanée. Cela s'applique au nombre d'installations de Windows Server et System Center dans ces rapports. Pour Windows Server, chaque hôte physique a un point dans le temps (indépendamment du type du système d'exploitation sur l'hôte), au cours d'un mois, où la plupart des machines virtuelles Windows Server s'exécutent simultanément. Il s'agit de la borne haute du mois. En outre, pour System Center, il existe un point dans le temps dans le mois où la plupart des serveurs Windows gérés s'exécutent simultanément pour chaque hôte physique (un serveur géré est identifié quand un ou plusieurs agents System Center sont présents). Seule la borne haute la plus récente pour un hôte physique est affichée dans le rapport. Aucune donnée après la borne haute n'est affichée. Et on peut supposer que le nombre machines virtuelles Windows Server (onglets WS) ou de machines virtuelles Windows Server gérées (onglets SC), se trouve en dessous de la borne haute au-delà de ce point. Ce mode de suivi et de représentation de l'utilisation doit permettre de planifier la capacité et de s'aligner avec les modèles de licence de ces produits.

Sous les onglets relatifs à SQL dans le rapport, les installations de SQL Server sont comptabilisées de manière cumulative et non par rapport à la borne haute. Les totaux représentent le nombre d'installations de SQL Server en cours d'exécution.

> ⓘ **Notes**
>
> L'utilisation de la journalisation de l'inventaire logiciel ne remplace pas l'obligation de signaler précisément l'utilisation des logiciels Microsoft dans le cadre des termes du contrat de licence applicable.

## Date et heure d'interrogation

Quand vous utilisez Software Inventory Logging Aggregator, l'agrégation des valeurs de borne haute est pilotée par l'interrogation. En d'autres termes, une borne haute ne peut être capturée que par l'interrogation de l'hôte physique sous-jacent. Les valeurs de borne haute sont donc directement associées à une « date et heure d'interrogation » correspondante. Même si l'intervalle d'interrogation est réglable, la fidélité des bornes

hautes capturées est impactée si une valeur d'intervalle supérieure est utilisée. Plus l'intervalle est grand, moins les données sont représentatives de l'utilisation réelle.

## Les rapports sont effectués mois par mois

Tous les rapports, y compris les rapports annuels, sont représentés sous forme de rapports mois par mois. Les bornes hautes, les totaux et les données de l'ordinateur sont réinitialisées au début de chaque mois calendaire.

Les données de rapport suivantes, entre autres, sont affectées par le passage à un nouveau mois :

- Toutes les bornes hautes de tous les hôtes sont réinitialisées au début d'un nouveau mois.
- Si l'Aggregator reçoit au moins une charge utile complète d'une machine virtuelle (sur HTTPS), mais ne reçoit plus de pulsations, toutes les interrogations de l'hôte sous-jacent dans le mois interprètent l'association entre l'hôte, la machine virtuelle et les données de machine virtuelle comme si la machine virtuelle était en cours d'exécution ou arrêtée pendant tout le mois. Au début du nouveau mois, cette association est effacée jusqu'à ce qu'une charge utile complète ou une pulsation soit reçue de la part de cette machine virtuelle.

## Remarques supplémentaires sur le comportement du rapport

- Les onglets Résumé sont des listes de référence rapide de l'inventaire. Les hôtes et leurs machines virtuelles sont répertoriés dans la même colonne.
- Ignorez toutes les valeurs qui sont grisées ou faibles. Il s'agit d'artefacts de la création de rapports à partir du cube SSAS.
- Si une machine virtuelle est listée sous « Système d'exploitation inconnu », cela signifie que l'Aggregator n'a pas reçu de charge utile de données complète de cette machine virtuelle via SIL sur HTTPS.
- Les machines virtuelles listées sous « Hôte inconnu » sont des machines virtuelles Windows Server qui transfèrent correctement les données d'inventaire sur HTTPS à l'Aggregator, mais l'Aggregator n'interroge pas activement ou correctement l'hôte sous-jacent pour cette machine virtuelle. Le décompte sera toujours de zéro pour ces entrées, car l'hôte sous-jacent est inconnu. Utilisez l'applet de commande `Add-SilVMHost`, avec des informations d'identification correctes, pour ajouter l'hôte (ou

tous les hôtes) à SIL Aggregator pour l'interrogation. Une fois l'interrogation correctement activée, les données de la machine virtuelle et de l'hôte sont associées sur les rapports.

- Toutes les dates et heures sont locales par rapport à l'heure et aux paramètres régionaux système de SIL Aggregator. Cela inclut les données d'inventaire reçues des systèmes SIL sur HTTPS. Quand ces fichiers sont traités (pas plus de 20 minutes après la réception) les données sont insérées dans la base de données avec l'heure système locale.

- La mention « SIL Aggregator » est indiquée sur tous les serveurs sur lesquels Software Inventory Logging Aggregator est installé.

- Si la quantité de mémoire physique ou le nombre de processeurs est modifié sur un hôte physique, une nouvelle ligne s'affiche dans le rapport en plus de l'ancienne ligne. L'interrogation des mises à jour cesse sur l'ancienne ligne et continue sur la nouvelle comme s'il s'agissait d'un hôte récemment ajouté.

- Sous les onglets **Résumé** et **Détails** , le total des colonnes Serveurs Windows exécutés simultanément ou serveurs Windows gérés indique le total de toutes les bornes hautes pour tous les hôtes répertoriés. Cela inclut les serveurs Windows qui ne sont pas des hôtes hyperviseur et n'ont aucune machine virtuelle en cours d'exécution ainsi que les serveurs qui peuvent avoir des machines virtuelles en cours d'exécution, mais qui sont « Inconnus », car aucune donnée n'est reçue de la machine virtuelle à partir de SIL via HTTPS. Ceux-ci sont totalisés pour des raisons pratiques.

- Dans la section **SQL Server** de l'onglet **Tableau de bord**, le nombre total d'installations de SQL Server est un résumé de tous les totaux de l'édition dans le tableau de bord. Il peut y avoir une incohérence entre le total de l'onglet **Détails SQL** dans le cas où plusieurs éditions de SQL sont installées sur un seul serveur. Le tableau de bord les compte séparément sur chaque serveur, contrairement à l'onglet **Détails**. Plusieurs éditions SQL installées sur un serveur Windows Server sont toujours comptabilisées comme une seule édition, par contrat de licence.

- Dans la section **Windows Server** de l'onglet **Tableau de bord**, les lignes **Autres hôtes hyperviseur** et **Nombre total d'hôtes hyperviseur** incluent les hôtes Windows Server physiques qui peuvent ou NON exécuter Hyper-V.

## Description des colonnes

Voici la description de chaque colonne de l'onglet **Détails de Windows Server** dans le rapport Excel créé par SIL Aggregator. Les autres onglets de données sont identiques ou

représentent un sous-ensemble de ces colonnes. La seule exception est la colonne « Nombre d'installations » sous les onglets SQL Server (consultez la section **Borne haute**).

| En-tête de colonne | Description |
|---|---|
| Calendar Month | Les données des rapports sont regroupées par mois, en commençant par le plus récent. Les données du mois ne sont pas affichées dans un ordre spécifique. |
| Nom d'hôte | Nom de réseau ou nom de domaine complet de l'hôte physique que SIL Aggregator parvient à interroger.<br>Utilisez l'applet de commande Get-SilVMHost pour rechercher les hôtes qui ont été ajoutés, mais ne sont pas ou plus correctement interrogés. La dernière interrogation réussie est affichée. |
| Type d'hôte | Fabricant du système d'exploitation de l'hôte physique. |
| Type d'hyperviseur | Fabricant de l'hyperviseur de l'hôte physique. |
| Fabricant du processeur | Fabricant des processeurs de l'hôte physique. |
| Modèle de processeur | Modèle des processeurs de l'hôte physique. |
| L'Hyper-Threading est-il activé ? | Affiche True ou False selon que l'Hyper-Threading est activé ou non sur les processeurs de l'hôte physique. |
| Nom de la machine virtuelle | Nom de réseau ou nom de domaine complet de la machine virtuelle Windows Server. Si l'Aggregator n'a pas reçu de données de cet ordinateur sur HTTPS, le nom convivial de la machine virtuelle dans l'hyperviseur est indiqué. |
| Machines virtuelles Windows Server s'exécutant simultanément, par hôte | Nombre de machines virtuelles Windows Server s'exécutant simultanément sur l'hôte. Le nombre le plus élevé du mois pour cet hôte est la borne haute indiquée et capturée à cet instant précis.<br>Consultez la section **Borne haute** de cette documentation.<br><br>Les hôtes physiques sur lesquels Windows Server est installé, ou sur lesquels Windows Server est installé et aucune machine virtuelle Windows Server connue ne s'exécute, sont comptabilisés comme un seul hôte. Si au moins une machine virtuelle Windows Server connue est en cours d'exécution sur l'hôte et que Windows Server est en cours d'exécution sur l'hôte lui-même, le système d'exploitation de l'hôte n'est pas comptabilisé. |
| Nombre de processeurs physiques | Nombre de processeurs physiques installés sur l'hôte physique. |

| En-tête de colonne | Description |
| --- | --- |
| Nombre de cœurs physiques | Nombre de cœurs de processeur physiques installés sur l'hôte physique. |
| Nombre de processeurs virtuels | Nombre de processeurs virtuels que Windows reconnaît dans la machine virtuelle. Cette valeur est fournie uniquement à partir des données transférées sur HTTPS à l'aide de SIL dans un serveur Windows Server. |
| Date et heure d'interrogation | Date et heure du dernier point de borne haute des machines virtuelles Windows Server s'exécutant simultanément sur cet hôte physique.<br>Consultez la section **Date et heure d'interrogation** de cette documentation. |
| Date et heure du dernier affichage de la machine virtuelle | Date et heure auxquelles l'Aggregator a reçu le dernier inventaire des données sur HTTPS de la part de cette machine virtuelle Windows Server. |
| Date et heure du dernier affichage de l'hôte | Date et heure auxquelles l'Aggregator a reçu le dernier inventaire des données sur HTTPS de la part de cet hôte physique Windows Server.<br>L'activation de SIL et le transfert des données d'inventaire sur HTTPS à un SIL Aggregator sont pris en charge sur des hôtes physiques exécutant Windows Server et Hyper-V. |

# Détails des applets de commande SIL Aggregator

Voici les détails des applets de commande SIL Aggregator. Pour obtenir la documentation complète des applets de commande, consultez : Applets de commande PowerShell SIL Aggregator

## Publish-SilReport

- Cette applet de commande, utilisée en l'état, crée un rapport de journalisation de l'inventaire logiciel et le place dans le répertoire Documents de l'utilisateur connecté (Excel 2013 est nécessaire sur l'ordinateur sur lequel est exécutée l'applet de commande).
- Utilisée avec le paramètre `-OpenReport`, elle crée le rapport et l'ouvre dans Excel pour consultation.

- Notez que lors de l'installation de SIL Aggregator, vous avez la possibilité d'installer uniquement le module Rapports. Vous pouvez installer le module Rapports sur un système d'exploitation client Windows, tel que Windows 8.1 ou Windows 10. Cela permet à un client léger, comme un PC portable ou une tablette, de se connecter à un serveur de base de données SIL Aggregator pour publier directement des rapports SIL.

    - L'exemple suivant vous invite à indiquer les informations d'identification à utiliser, se connecte à un serveur de base de données SIL Aggregator nommé SILContoso, et crée et ouvre un rapport SIL sur l'ordinateur local.

      ```
      Publish-SilReport -DBServerName "SILContoso" -DBServerCredential Get-Credential –OpenReport
      ```

    - Avant de vous connecter pour la première fois, dans la plupart des cas vous devez ouvrir un port dans le pare-feu sur le serveur de base de données SIL Aggregator pour autoriser les connexions. Les professionnels de l'informatique peuvent configurer ce port à l'avance pour permettre à leurs contrôleurs financiers ou autres gestionnaires d'inventaire de créer leurs propres rapports. Pour savoir comment procéder, consultez le lien ci-dessous. Le port par défaut généralement utilisé pour SQL Server Analysis Services est 2383.

## Add-SilVMHost

Les types d'hôtes et versions d'hyperviseur suivants sont pris en charge quand vous utilisez l'applet de commande `Add-SilVMHost` . Notez qu'il n'est pas nécessaire de les spécifier. L'applet de commande `Add-SilVMHost` détecte automatiquement une combinaison prise en charge. Dans le cas contraire ou si les informations d'identification indiquées sont incorrectes, une invite s'affiche. Si l'utilisateur accepte avec une entrée « Y », l'hôte est ajouté, mais n'est pas interrogé. Il est ajouté comme « Inconnu ».

| **Version d'hyperviseur** | **Valeur HostType SIL Aggregator** | **SIL Aggregator Valeur HypervisorType** |
|---|---|---|
| Windows Server, 2012 R2 | Windows | Hyper-V |
| VMware 5.5 | VMware | Esxi |
| Xen 4.x | Ubuntu, OpenSuse ou CentOS | Xen |
| XenServer 6.2 | Citrix | XenServer |
| KVM | Ubuntu, OpenSuse ou CentOS | KVM |

D’autres versions de ces types et plateformes d’hyperviseur peuvent également fonctionner. SIL Aggregator inclut la version sshnet ci-dessous. Elle est utilisée pour communiquer avec les plateformes de virtualisation Linux.

```
sshnet 2014.4.6-beta1
https://sshnet.codeplex.com/releases/view/120504
Copyright (c) 2010, RENCI
```

## Get-SilAggregator

`Get-SilAggregator` fournit des informations de configuration pour votre application Software Inventory Logging Aggregator. L’exemple de sortie suivant affiche les informations suivantes :

- L’application est en cours d’exécution
- L’intervalle d’interrogation est toutes les heures (peut être modifié en incréments d’heure)
- Heure de début de l’interrogation
- URI cible que les autres ordinateurs doivent définir pour transférer des données à cet Aggregator
- Empreintes numériques de certificat dont cet Aggregator accepte des données
- Type de compte spécifié à l’installation

  `PS C:\Windows\system32> Get-SilAggregator`

  ``

  `State : Running HostPollIntervalInHours : Every 1 Hour(s)`

  `PollStartTime : 8/24/2015 5:07:33 AM`

  `TargetURI : https://SilContoso`

  `CertificateThumbprint : 3efc6b8ce7d5eefba5107ede9d1caca550417452, 2dc4ea8bfb64b1246a8c1ffa1b701cd1042a3412`

  `UserProfile : Local`

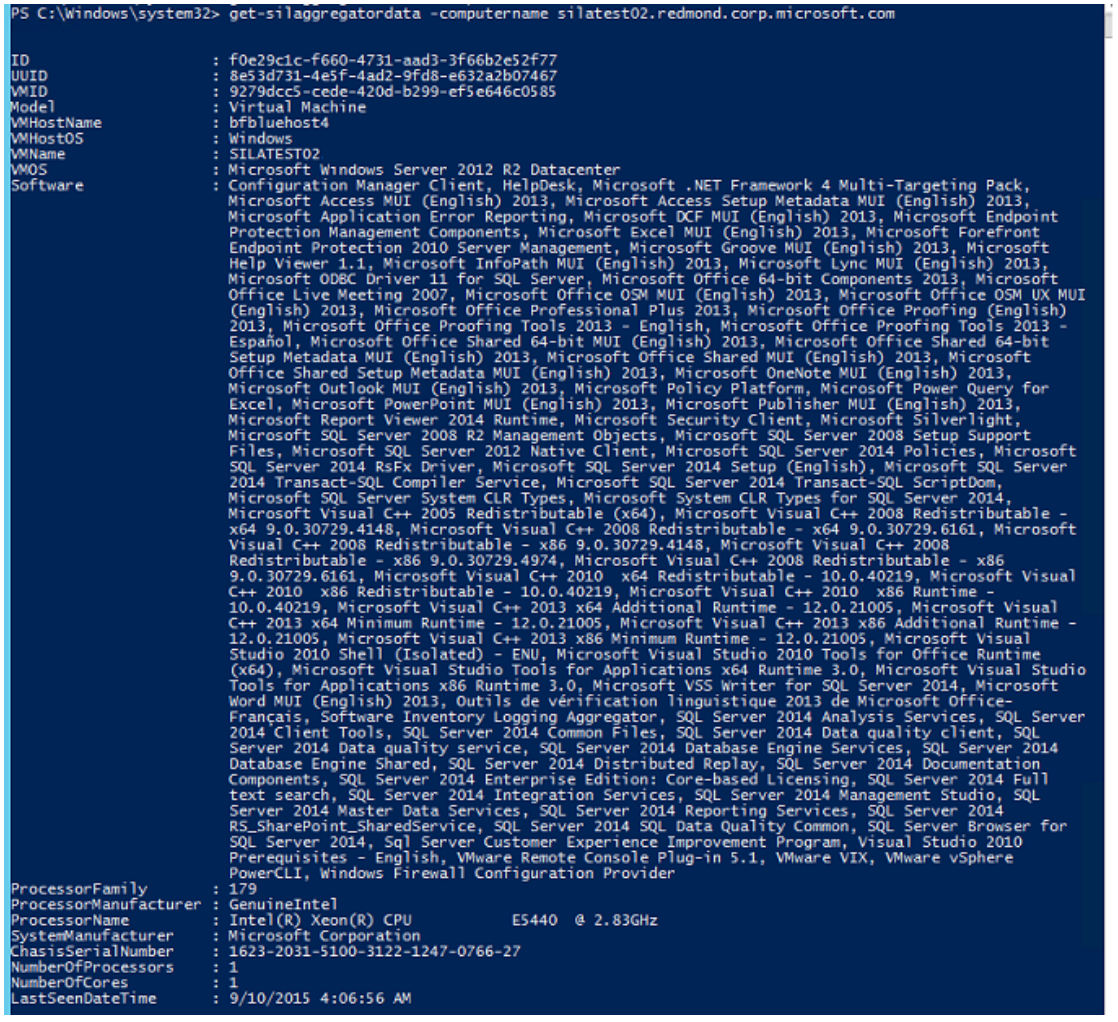
## Set-SilAggregator

Avec l'applet de commande `Set-SilAggregator`, vous pouvez :

- Modifier l'intervalle horaire de l'interrogation.
- Modifier la date et l'heure de début de l'interrogation pour démarrer à l'intervalle spécifié.
- Ajouter ou supprimer des empreintes numériques de certificat dont SIL Aggregator accepte des données ou qui sont associées à ce dernier.

## Get-AggregatorData

- Utilisée seule, cette applet de commande affiche le contenu de l'onglet Détail des serveurs Windows d'un rapport Excel SIL Aggregator.
- Utilisée avec des paramètres, cette applet de commande récupère les données directement de la base de données destinée à permettre des utilisations personnalisées de la solution SIL globale.
- Notez que les paramètres `-StartTime` et `-Endtime` affichent des données de rapport à partir du premier jour du mois de la date de début et du dernier jour du mois de la date de fin.



## Get-SilVMHost

- Cette applet de commande renvoie la liste des hôtes physiques que SIL Aggregator doit interroger, la date et l'heure de la dernière interrogation réussie et les valeurs HostType (fabricant du système d'exploitation) et HypervisorType (fabricant de l'hyperviseur). Consultez les détails d'Add-SilVMHost pour plus d'informations sur HostType et HypervisorType.

  Si un hôte n'a aucune date et heure d'interrogation, mais qu'il a des valeurs HostType et HypervisorType prises en charge, cela signifie que l'interrogation n'a pas encore commencé ou n'a pas encore été réussie.

- Cette applet de commande affiche également la liste des noms d'hôte qui ont été ajoutés par l'intermédiaire des données provenant des machines virtuelles elles-mêmes, si elles sont disponibles dans la machine virtuelle. Celles-ci s'affichent dans la liste, mais n'ont pas de valeur HostType ou HypervisorType. Ces données peuvent permettre de mettre en correspondance les machines virtuelles et les hôtes qui ne sont peut-être pas configurés pour l'interrogation.

- Utilisez les paramètres `-StartTime` et `-EndTime` pour mieux comprendre à quel moment les hôtes ont été ajoutés pour la première fois ou interrogés pour la dernière fois.

## Remove-SilVMHost

- Cette applet de commande supprime tout hôte de la liste des hôtes à interroger. Si un hôte est supprimé, il est possible qu'une machine virtuelle sur l'hôte rajoute ce dernier à la liste, mais l'hôte n'est pas interrogé avec les informations d'identification correctes spécifiées à l'aide de l'applet de commande `Add-SilVMHost`.

- Si un hôte est supprimé, il n'est pas interrogé, mais n'est pas supprimé des rapports. En revanche, comme il n'est pas interrogé, il n'apparaîtra pas dans les rapports du mois suivant.

- Utilisez les paramètres `-StartTime` et`-EndTime` individuellement pour supprimer des groupes d'hôtes correctement interrogés jusqu'à une date, ou correctement interrogé à partir d'une date.

# Éviter les erreurs et problèmes suivants avec SIL et SIL Aggregator (Guide de résolution des

# problèmes)

- Éléments à vérifier en cas d'échec de l'applet de commande `SilLogging` ou `Publish-Sildata`, ou en cas d'erreur :
    - Vérifiez que **targeturi** contient **https://** dans l'entrée.
    - Vérifiez que toutes les mises à jour nécessaires pour Windows Server sont installées (consultez la section Conditions préalables pour SIL). Pour une vérification rapide, recherchez les mises à jour avec l'applet de commande suivante : `Get-SilWindowsUpdate *3060*, *3000*`
    - Vérifiez que le certificat utilisé pour l'authentification auprès de l'Aggregator est installé dans le magasin approprié sur le serveur local à inventorier avec SilLogging (consultez la section Prise en main).
    - Dans SIL Aggregator, vérifiez que l'empreinte numérique du certificat utilisé pour l'authentification auprès de l'Aggregator est ajoutée à la liste à l'aide de l'applet de commande `Set-SilAggregator –AddCertificateThumbprint` (consultez la section Prise en main).
    - Si vous utilisez des certificats d'entreprise, vérifiez que le serveur sur lequel SIL est activé est joint au domaine pour lequel le certificat a été créé, ou qu'il peut être vérifié avec une autorité racine. Si un certificat n'est pas approuvé sur l'ordinateur local qui tente de transférer/envoyer des données à un Aggregator, cette action échoue avec une erreur.
    - Si tous les éléments ci-dessus ont été vérifiés, vous pouvez vérifier que le certificat utilisé pour installer SIL Aggregator est intègre et qu'il correspond au nom du serveur SIL Aggregator lui-même (cette étape est inutile si d'autres ordinateurs parviennent à transférer correctement des données au même SIL Aggregator).
    - Vous pouvez vérifier dans l'emplacement suivant la présence de fichiers SIL mis en cache sur le serveur qui tente de transférer/d'envoyer des données, \Windows\System32\Logfiles\SIL. Si `SilLogging` a démarré et s'exécute depuis plus d'une heure, ou que `Publish-SilData` a été exécuté récemment et qu'il n'existe aucun fichier dans ce répertoire, la journalisation dans l'Aggregator a réussi.
- Vérifiez que l'utilisateur connecté dispose d'un accès à la base de données SQL et à Analysis Services.

    - Cela est nécessaire pour l'installation de SIL Aggregator.
    - Cela est nécessaire lors de l'utilisation de PowerShell à distance pour gérer SIL Aggregator.
- Pour publier des rapports SIL Aggregator à partir d'un système d'exploitation de bureau client.
    - Utilisez l'option permettant d'installer uniquement le module Rapports sur votre client Windows (8.1/10).
    - Si vous rencontrez des problèmes quand vous tentez de créer un rapport à l'aide de PowerShell à distance, vous devez probablement ouvrir un port de pare-feu sur le SIL Aggregator auquel vous essayez de vous connecter (consultez l'applet de commande `Publish-SilReport` dans la section Détails des applets de commande SIL Aggregator).
- Quand vous utilisez l'option gMSA :
    - N'oubliez pas de redémarrer le serveur après l'avoir joint au groupe d'ordinateurs gMSA dans Active Directory.
    - Dans le processus d'installation, n'utilisez pas le nom de domaine complet pour l'entrée domaine\utilisateur. Par exemple, utilisez **mydomain\gmsaaccount**. N'entrez pas **mydomain.com\gmsaaccount**.
- Quand vous utilisez le Windows Management Framework dans votre environnement :
    - Assurez-vous que WMF 5.1 n'est pas installé sur le ou les serveurs sur lesquels SILA est installé. Il est possible d'obtenir une erreur dans le journal des événements concernant la DLL « **mpunits.dll** ». Cela empêchera le bon fonctionnement. SILA nécessite uniquement WMF 4.0.

# Gestion de SIL dans le temps

## Désinstaller/réinstaller SIL Aggregator

Si vous devez désinstaller, puis réinstaller SIL Aggregator, vous pouvez le faire sans perdre les données d'inventaire existantes et historiques. Désinstallez simplement le logiciel (en suivant les étapes décrites dans cette documentation) et sélectionnez l'option permettant de conserver la base de données de journalisation de l'inventaire logiciel. Ensuite, réinstallez SIL Aggregator (en suivant les étapes décrites dans cette

documentation), puis sélectionnez l'option permettant d'attacher une base de données existante.

Après avoir effectué cette opération, vous devez mettre à jour les informations d'identification à l'aide de l'applet de commande `Add-SilVMHost` sur tous les hôtes qui ont été précédemment interrogés par SIL Aggregator (en supposant que vous vouliez continuer à collecter des données sur ces hôtes). En outre, pour éviter les doublons d'entrées pour le même hôte dans les rapports, vous devez rajouter des hôtes pour l'interrogation à l'aide de la même adresse réseau que celle ajoutée à l'origine. Voici les trois types de vmhostname pris en charge qui peuvent être utilisés pour ajouter un hôte à l'aide de l'applet de commande `Add-SilVMHost` :

- Adresse IP
- Nom de domaine complet (FQDN)
- Nom NetBIOS

## Modification de SIL Aggregators

Quand vous voulez démarrer l'inventaire des serveurs de votre environnement avec un autre SIL Aggregator, utilisez simplement l'applet de commande SIL sur ces serveurs pour modifier le targeturi (et l'empreinte numérique du certificat, si nécessaire), `Set-SilLogging –TargetUri`. Notez que vous devez ensuite utiliser l'applet de commande `Publish-SilData` au moins une fois pour transférer un inventaire complet au SIL Aggregator nouvellement spécifié.

## Modification ou mise à jour des certificats

**ÉTAPES IMPORTANTES POUR ÉVITER LA PERTE DE DONNÉES :** si vous devez modifier le certificat que les serveurs utilisent pour transférer des données à un SIL Aggregator, mais que l'Aggregator cible reste le même, procédez comme suit pour éviter de perdre des données en transit vers l'Aggregator :

- Sur le SIL Aggregator, utilisez l'applet de commande `Set-SilAggregator –AddCertificateThumbprint` pour ajouter la nouvelle empreinte numérique du SIL Aggregator.
- Sur TOUS les serveurs qui transfèrent des données, installez le nouveau certificat à utiliser dans **\LOCALMACHINE\MY** à l'aide de la méthode de votre choix.

- Sur TOUS les serveurs qui transfèrent des données, utilisez l'applet de commande `Set-SilLogging –CertificateThumbprint` pour mettre à jour l'empreinte numérique du nouveau certificat.
- **REMARQUE IMPORTANTE : une fois seulement que vous avez mis à jour tous les serveurs qui transfèrent des données, supprimez l'ancienne empreinte numérique** du SIL Aggregator à l'aide de l'applet de commande `Set-SilAggregator –RemoveCertificateThumbprint`. Si un serveur qui transfère des données continue à le faire à l'aide d'un ancien certificat qui a été supprimé du SIL Aggregator, **des données seront perdues** et ne seront pas insérées dans la base de données de l'Aggregator. Cela impacte uniquement les scénarios dans lesquels un serveur a déjà correctement transféré des données à un SIL Aggregator, puis que le certificat est supprimé de la liste d'empreintes numériques du SIL Aggregator.

# Notes de publication

- Le fait que SIL Aggregator ne gère ni ne signale la présence de l'installation de SQL Server Standard Edition est un problème connu. Pour le résoudre, effectuez les étapes suivantes :
    1. Ouvrez SQL Server Management Studio sur SIL Aggregator.
    2. Connectez-vous au Moteur de base de données.
    3. Développez la base de données SoftwareInventoryLogging puis Tables dans l'arborescence de sélection.
    4. Cliquez avec le bouton droit sur **dbo.SqlServerEdition**, puis sélectionnez « **Modifier les 200 lignes du haut** ».
    5. Remplacez PropertyNumValue à côté de « Standard Edition » par **2760240536** (à partir de-1534726760).
    6. Fermez la requête pour enregistrer la modification.
    7. Il sera peut-être nécessaire d'exécuter une fois l'applet de commande `Publish-SilData` sur tous les serveurs qui exécutent SIL et qui ont déjà journalisé des données sur cet Aggregator pour que celui-ci gère correctement la présence de SQL Server Standard Edition.
- Dans les rapports SIL générés, le total des cœurs de processeur inclut le nombre de threads si l'Hyper-Threading est activé sur le serveur physique. Pour obtenir le

nombre réel de cœurs physiques sur les serveurs sur lesquels l'Hyper-Threading est activé, vous devez réduire ce nombre de moitié.

- Le total des lignes (sous l'onglet **Tableau de bord**) et des colonnes (sous les onglets **Résumé et Détails**) intitulées « **Simultanément en cours d'exécution**... » pour Windows Server et System Center n'est pas exactement identique d'un emplacement à l'autre. Sous l'onglet **Tableau de bord**, vous devez ajouter la valeur « **Appareils Windows Server (sans machine virtuelle connue**) » à la valeur « **Simultanément en cours d'exécution**... » pour retrouver le total des onglets **Résumé et Détail**.

- Consultez **ÉTAPES IMPORTANTES POUR ÉVITER LA PERTE DE DONNÉES** lors de la modification ou mise à jour des certificats, dans la section **Gestion de SIL au fil du temps** de cette documentation.

- S'il est possible d'ajouter des hôtes Windows Server 2008 R2 et Windows Server 2012 à la liste d'hôtes à interroger, cette version (1.0) de SIL Aggregator prend uniquement en charge l'interrogation de Windows Server 2012 R2, pour des hôtes Windows/Hyper-V, afin que toutes les fonctionnalités soient disponibles. En particulier, nous savons que lors de l'interrogation d'hôtes Windows Server 2008 R2, les machines virtuelles et les hôtes peuvent ne pas correspondre dans les rapports SIL Aggregator.

# Voir aussi

Software Inventory Logging Aggregator 1.0 pour Windows Server
Applets de commande PowerShell SIL Aggregator
Applets de commande PowerShell SIL
Vue d'ensemble de SIL
Gestion de SIL

# Bien démarrer avec la journalisation des accès utilisateur

14/08/2025

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

La journalisation des accès utilisateur est une fonctionnalité proposée dans Windows Server qui permet de regrouper les données d'utilisation client par rôle et par produit sur un serveur local. Elle aide les administrateurs de serveur Windows à quantifier les demandes effectuées par des ordinateurs clients concernant les rôles et les services d'un serveur local.

UAL est installé et activé par défaut, et collecte les données quasiment en temps réel. Aucune configuration pour l'administrateur n'est requise, bien que la journalisation des accès utilisateur (UAL) puisse être désactivée ou activée. Pour plus d'informations, voir Gérer la journalisation des accès utilisateur. Le service de journalisation des accès utilisateur regroupe les données d'utilisation client par rôle et par produit dans les fichiers des bases de données locales. Les administrateurs informatiques peuvent ensuite utiliser les applets de commande WMI et Windows PowerShell pour récupérer les quantités et les instances par rôle de serveur (ou produit logiciel), par utilisateur, par périphérique, par serveur local et par date.

> ⓘ **Notes**
>
> UAL prend en charge le Microsoft Assessment and Planning Toolkit.

## Applications pratiques

UAL regroupe les événements des périphériques clients uniques et les événements liés aux demandes des utilisateurs, consignés dans une base de données locale. Ces enregistrements sont accessibles (via une requête d'un administrateur de serveur) pour récupérer les quantités et les instances par rôle de serveur, par utilisateur, par périphérique, par serveur local et par date. De plus, la journalisation des accès utilisateur a été étendue pour permettre aux développeurs de logiciels non-Microsoft d'instrumenter les événements de journalisation des accès utilisateur qui doivent être regroupés par Windows Server.

UAL peut effectuer les tâches suivantes :

- quantifier les demandes d'utilisateurs clients pour les serveurs virtuels ou physiques locaux ;

- quantifier les demandes d’utilisateurs clients pour les produits logiciels installés sur un ordinateur physique local ou un ordinateur virtuel ;
- récupérer des données sur un serveur local exécutant Hyper-V pour identifier les périodes de faible et de forte demande sur un ordinateur virtuel Hyper-V ;
- Récupérer les données UAL à partir de plusieurs serveurs distants.

En outre, les développeurs de logiciels peuvent instrumenter des événements UAL qui peuvent ensuite être regroupés et récupérés avec les interfaces WMI et Windows PowerShell.

Les rôles de serveur et services suivants sont pris en charge par la journalisation des accès utilisateur :

- Services de certificats Active Directory (AD CS)
- Services AD RMS (Active Directory Rights Management Services)
- BranchCache
- DNS (Domain Name System)

  > ⓘ **Notes**
  >
  > UAL collecte des données DNS toutes les 24 heures, et il existe un cmdlet UAL distinct pour ce scénario.

- Protocole DHCP (Dynamic Host Configuration Protocol)
- Serveur de télécopie
- Services de fichiers
- Serveur FTP
- Hyper-V

  > ⓘ **Notes**
  >
  > UAL collecte des données Hyper-V toutes les 24 heures, et il existe un cmdlet UAL distinct pour ce scénario.

- Serveur Web (IIS)

> ⚠ **Avertissement**
>
> Pour utiliser UAL avec IIS, vous devez utiliser iisual.exe. Pour plus d'informations, voir Analyse des données d'utilisation client avec la journalisation des accès utilisateur IIS.

- Services de Microsoft Message Queue (MSMQ)
- Services de stratégie réseau et d'accès
- Services d'impression et de numérisation de document
- Service Routage et accès à distance
- Services de déploiement Windows (WDS)
- Windows Server Update Services (WSUS)

> ⓘ **Important**
>
> La journalisation des accès utilisateur (UAL) n'est pas recommandée pour les serveurs connectés directement à Internet, tels que les serveurs web situés dans un espace d'adressage accessible à Internet. Elle est également déconseillée dans les scénarios où des performances extrêmement élevées constituent la fonction principale du serveur (par exemple, dans les environnements de calcul haute performance - HPC). La journalisation des accès utilisateur est principalement destinée à des scénarios mettant en jeu un intranet d'entreprise de petite ou moyenne taille, dans lesquels un volume élevé est prévu, mais pas aussi élevé que dans les déploiements servant un volume de trafic Internet de façon régulière.

# Fonctionnalités importantes

Le tableau suivant décrit les fonctions clés de l'UAL et leur valeur potentielle.

Agrandir le tableau

| Functionality | Value |
|---|---|
| Collecter et regrouper les données d'événements de demandes client quasiment en temps réel | L'équivalent de trois ans de données peut être enregistré. **Important:** Les administrateurs doivent appliquer la conformité des données collectées et des périodes de |

| Functionality | Value |
| --- | --- |
| | rétention des données avec la politique de confidentialité de l'organisation et les réglementations locales. |
| Utiliser des requêtes de journalisation des accès utilisateur via l'interface WMI ou Windows PowerShell pour récupérer les données de demande client sur un serveur local ou distant | UAL permet une vue unique des données d'utilisation en cours. Les administrateurs de serveurs et d'entreprises peuvent récupérer ces données et collaborer avec les administrateurs commerciaux pour optimiser l'utilisation de leurs licences de logiciels en volume. |
| Option activée par défaut. | Les administrateurs de serveur n'ont pas besoin de configurer cette fonctionnalité pour que toutes les fonctionnalités principales soient disponibles et opérationnelles. |

# Données enregistrées avec UAL

Les données liées aux utilisateurs suivantes sont enregistrées par UAL.

Agrandir le tableau

| Data | Description |
| --- | --- |
| **UserName** | Nom d'utilisateur du client qui accompagne les entrées UAL provenant des rôles et produits installés, le cas échéant. |
| **ActivityCount** | Nombre de fois qu'un utilisateur accède à un rôle ou un service. |
| **FirstSeen** | Date et heure auxquelles un utilisateur accède pour la première fois à un rôle ou un service. |
| **LastSeen** | Date et heure auxquelles un utilisateur accède pour la dernière fois à un rôle ou un service. |
| **ProductName** | Nom du produit parent du logiciel, tel que Windows, qui fournit les données UAL. |
| **RoleGUID** | Le GUID attribué ou enregistré par l'UAL qui représente le rôle du serveur ou le produit installé. |
| **RoleName** | Nom du rôle, du composant ou du sous-produit qui fournit les données UAL. "Cet élément est également associé à ProductName et RoleGUID." |
| **TenantIdentifier** | GUID unique du client d'un rôle ou d'un produit installé qui accompagne les données de journalisation des accès utilisateur, le cas échéant. |

Les données liées aux appareils suivantes sont enregistrées avec UAL.

Agrandir le tableau

| Data | Description |
|---|---|
| **IPAddress** | Adresse IP d'un périphérique client qui est utilisé pour accéder à un rôle ou un service. |
| **ActivityCount** | Nombre de fois qu'un utilisateur accède à un rôle ou un service. |
| **FirstSeen** | Date et heure auxquelles une adresse IP est utilisée pour la première fois pour accéder à un rôle ou un service. |
| **LastSeen** | Date et heure auxquelles une adresse IP est utilisée pour la dernière fois pour accéder à un rôle ou un service. |
| **ProductName** | Nom du produit parent du logiciel, tel que Windows, qui fournit les données UAL. |
| **RoleGUID** | GUID affecté ou inscrit par la journalisation des accès utilisateur, et qui représente le rôle de serveur ou le produit installé. |
| **RoleName** | Nom du rôle, du composant ou du sous-produit qui fournit les données UAL. "Cet élément est également associé à ProductName et RoleGUID." |
| **TenantIdentifier** | GUID unique du client d'un rôle ou d'un produit installé qui accompagne les données de journalisation des accès utilisateur, le cas échéant. |

# Configuration logicielle requise

UAL peut être utilisée sur n'importe quel ordinateur exécutant une version de Windows Server postérieure à Windows Server 2012.

# Références supplémentaires

Journalisation des accès utilisateur sur MSDN. Gérer la journalisation des accès utilisateur

# Gérer la journalisation des accès utilisateur

14/08/2025

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

Ce document explique comment gérer la journalisation des accès utilisateur (UAL, User Access Logging).

La journalisation des accès utilisateur est une fonctionnalité qui peut aider les administrateurs de serveur à quantifier le nombre de demandes client uniques de rôles et services sur un serveur local.

La journalisation des accès utilisateur est installée et activée par défaut et collecte les données quasiment en temps réel. Seules quelques options de configuration sont disponibles pour la journalisation des accès utilisateur. Ce document décrit ces options et leur effet escompté.

Pour en savoir plus sur les avantages de la journalisation des accès utilisateur, voir Bien démarrer avec la journalisation des accès utilisateur.

**Dans ce document**

Les options de configuration traitées dans ce document incluent :

- Désactivation et activation du service de journalisation des accès utilisateur
- Collecte et suppression de données
- Suppression des données consignées par la journalisation des accès utilisateur
- Gestion de la journalisation des accès utilisateur dans des environnements de grand volume
- Récupération à partir d'un état endommagé
- Activation du suivi des licences d'utilisation Dossiers de travail

## Désactivation et activation du service de journalisation des accès utilisateur

La journalisation des accès utilisateur est activée et s'exécute par défaut lorsqu'un ordinateur exécutant Windows Server 2012 ou une version ultérieure est installé et démarré pour la première fois. Les administrateurs peuvent arrêter et désactiver la journalisation des accès utilisateur pour respecter les exigences de confidentialité ou d'autres besoins opérationnels.

Vous pouvez arrêter la journalisation des accès utilisateur à l'aide de la console Services, à partir de la ligne de commande ou en utilisant des applets de commande PowerShell. Toutefois, pour s'assurer que la journalisation des accès utilisateur ne s'exécutera pas à nouveau au prochain démarrage de l'ordinateur, vous devez également désactiver le service. Les procédures suivantes décrivent comment arrêter et désactiver la journalisation des accès utilisateur.

> ⓘ **Notes**
>
> Vous pouvez utiliser l'applet de commande PowerShell `Get-Service UALSVC` pour récupérer des informations sur le service de journalisation des accès utilisateur, y compris les informations indiquant si le service est en cours d'exécution ou arrêté, et s'il est activé ou désactivé.

## Pour arrêter et désactiver le service de journalisation des accès utilisateur à l'aide de la console Services

1. Connectez-vous au serveur avec un compte disposant des privilèges d'administrateur local.
2. Dans le Gestionnaire de serveur, pointez sur **Outils**, puis cliquez sur **Services**.
3. Faites défiler l'affichage et sélectionnez **Service de journalisation des accès utilisateur**. Cliquez sur **Arrêter le service**.
4. Cliquez avec le bouton droit sur le nom du service et sélectionnez **Propriétés**. Sous l'onglet **Général** , remplacez le **type de démarragepar Désactivé**, puis cliquez sur **OK**.

## Pour arrêter et désactiver la journalisation des accès utilisateur à partir de la ligne de commande

1. Connectez-vous au serveur avec un compte disposant des privilèges d'administrateur local.
2. Appuyez sur le logo Windows + R, puis tapez **cmd** pour ouvrir une fenêtre d'invite de commandes.

   > ⓘ **Important**
   >
   > Si la boîte de dialogue **Contrôle de compte d'utilisateur** s'affiche, vérifiez que l'action affichée est celle que vous voulez, puis cliquez sur **Oui**.

3. Tapez **net stop ualsvc**, et appuyez sur ENTRÉE.

4. Tapez **netsh ualsvc set opmode mode=disable**, puis appuyez sur ENTRÉE.

L'applet ou les applets de commande Windows PowerShell suivantes remplissent la même fonction que la procédure précédente. Entrez chaque applet de commande sur une seule ligne, même si elles peuvent apparaître comme renvoyées sur plusieurs lignes ici en raison de contraintes de mise en forme.

Vous pouvez également arrêter et désactiver la journalisation des accès utilisateur en utilisant les commandes Windows PowerShell Stop-service et Disable-Ual.

```
Stop-service ualsvc
```

```
Disable-ual
```

Si vous souhaitez redémarrer et réactiver la journalisation des accès utilisateur ultérieurement, vous pouvez le faire à l'aide des procédures décrites ci-dessous.

## Pour démarrer et activer le service de journalisation des accès utilisateur à l'aide de la console Services

1. Connectez-vous au serveur avec un compte disposant des privilèges d'administrateur local.

2. Dans le Gestionnaire de serveur, pointez sur **Outils**, puis cliquez sur **Services**.

3. Faites défiler l'affichage et sélectionnez **Service de journalisation des accès utilisateur**. Cliquez sur **Démarrer le service** .

4. Cliquez avec le bouton droit sur le nom du service et sélectionnez **Propriétés**. Sous l'onglet **Général** , remplacez le **type de démarragepar Automatique**, puis cliquez sur **OK**.

## Pour démarrer et activer la journalisation des accès utilisateur à partir de la ligne de commande

1. Connectez-vous au serveur avec des informations d'identification d'administrateur local.

2. Appuyez sur le logo Windows + R, puis tapez **cmd** pour ouvrir une fenêtre d'invite de commandes.

   > **ⓘ Important**
   >
   > Si la boîte de dialogue **Contrôle de compte d'utilisateur** s'affiche, vérifiez que l'action affichée est celle que vous voulez, puis cliquez sur **Oui**.

3. Tapez **net start ualsvc**, puis appuyez sur ENTRÉE.

4. Tapez **netsh ualsvc set opmode mode=enable**, puis appuyez sur ENTRÉE.

L'applet ou les applets de commande Windows PowerShell suivantes remplissent la même fonction que la procédure précédente. Entrez chaque applet de commande sur une seule ligne, même si elles peuvent apparaître comme renvoyées sur plusieurs lignes ici en raison de contraintes de mise en forme.

Vous pouvez également démarrer et réactiver la journalisation des accès utilisateur en utilisant les commandes Windows PowerShell Start-service et Enable-Ual.

```
Enable-ual
```

```
Start-service ualsvc
```

# Collecte des données de journalisation des accès utilisateur

Outres les applets de commande PowerShell décrites dans la section précédente, 12 autres applets de commande supplémentaires permettent de collecter les données de journalisation des accès utilisateur :

- **Get-UalOverview** : fournit les détails liés à l'UAL et l'historique des produits et des rôles installés.
- **Get-UalServerUser** : fournit des données d'accès utilisateur client pour le serveur local ou ciblé.

- **Get-UalServerDevice** : fournit des données d'accès aux appareils clients pour le serveur local ou ciblé.
- **Get-UalUserAccess** : fournit des données d'accès utilisateur client pour chaque rôle ou produit installé sur le serveur local ou ciblé.
- **Get-UalDeviceAccess** : fournit des données d'accès aux appareils clients pour chaque rôle ou produit installé sur le serveur local ou ciblé.
- **Get-UalDailyUserAccess** : fournit des données d'accès utilisateur client pour chaque jour de l'année.
- **Get-UalDailyDeviceAccess** : fournit des données d'accès aux appareils clients pour chaque jour de l'année.
- **Get-UalDailyAccess** : fournit des données d'accès utilisateur et d'appareil client pour chaque jour de l'année.
- **Get-UalHyperV** : fournit des données de machine virtuelle pertinentes pour le serveur local ou ciblé.
- **Get-UalDns** : fournit des données spécifiques au client DNS du serveur DNS local ou ciblé.
- **Get-UalSystemId** : fournit des données spécifiques au système pour identifier de manière unique le serveur local ou ciblé.

L'applet de commande `Get-UalSystemId` est censée fournir un profil unique d'un serveur pour toutes les autres données issues de ce serveur à mettre en corrélation.  Si un serveur connaît une modification quelconque d'un des paramètres de `Get-UalSystemId` , un nouveau profil est créé.  L'applet de commande `Get-UalOverview` est censée fournir à l'administrateur la liste des rôles installés et en cours d'utilisation sur le serveur.

> ⓘ **Notes**
>
> Les fonctionnalités élémentaires des services d'impression et de numérisation de document et des services de fichiers sont installées par défaut. Par conséquent, les administrateurs peuvent s'attendre à toujours voir les informations relatives à ces fonctionnalités affichées comme si les rôles complets étaient installés. Des applets de commande de journalisation des accès utilisateur distinctes sont incluses pour Hyper-V et DNS en raison des données uniques que la journalisation des accès utilisateur collecte pour ces rôles serveur.

Un cas d'usage standard des applets de commande de journalisation des accès utilisateur correspond au scénario dans lequel un administrateur interroge le service de journalisation des accès utilisateur au sujet des accès client uniques sur une plage de dates donnée. Cette opération peut être réalisée de différentes façons. La méthode ci-dessous est recommandée pour obtenir les accès par des périphériques uniques sur une plage de dates.

```
PS C:\Windows\system32>Gwmi -Namespace "root\AccessLogging" -query "SELECT * FROM
MsftUal_DeviceAccess WHERE LastSeen >='1/01/2013' and LastSeen <='3/31/2013'"
```

Ceci retourne une liste détaillée de tous les périphériques client uniques, classés par adresse IP, qui ont effectué des demandes auprès du serveur dans cette plage de dates.

'ActivityCount' pour chaque client unique est limité à 65 535 par jour. En outre, l'appel à WMI à partir de PowerShell est requis uniquement lorsque vous effectuez une requête par date.  Tous les autres paramètres des applets de commande de journalisation des accès utilisateur peuvent être utilisés au sein des requêtes PowerShell comme prévu, comme dans l'exemple suivant :

```
PS C:\Windows\system32> Get-UalDeviceAccess -IPAddress "10.36.206.112"

ActivityCount    : 1
FirstSeen        : 6/23/2012 5:06:50 AM
IPAddress        : 10.36.206.112
LastSeen         : 6/23/2012 5:06:50 AM
ProductName      : Windows Server 2012 Datacenter
RoleGuid         : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName         : File Server
TenantIdentifier : 00000000-0000-0000-0000-000000000000
PSComputerName
```

La journalisation des accès utilisateur conserve jusqu'à deux années d'historique. Pour permettre la récupération des données d'UAL par un administrateur lorsque le service est en cours d'exécution, l'UAL effectue une copie du fichier de base de données actif, current.mdb, dans un fichier nommé *GUID.mdb* toutes les 24 heures pour l'utilisation du fournisseur WMI.

Le premier jour de l'année, l'UAL créera une *nouvelle GUID.mdb*. L'ancienne *GUID.mdb* est conservée en tant qu'archive pour l'utilisation du fournisseur. Après deux ans, la *GUID.mdb* originale sera remplacée.

> ⓘ **Important**

La procédure suivante doit être exécutée uniquement par un utilisateur avancé et serait communément utilisée par un développeur testant sa propre instrumentation des interfaces de programmation d'application de journalisation des accès utilisateur...

### Pour ajuster l'intervalle par défaut de 24 heures pour rendre les données visibles au fournisseur WMI

1. Connectez-vous au serveur avec un compte disposant des privilèges d'administrateur local.
2. Appuyez sur le logo Windows + R, puis tapez **cmd** pour ouvrir une fenêtre d'invite de commandes.
3. Ajoutez la valeur de Registre : **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WMI\AutoLogger\Sum\PollingInterval (REG_DWORD)**.

   > ⚠ **Avertissement**
   >
   > Une modification incorrecte du Registre peut endommager gravement votre système. Avant d'apporter des modifications au Registre, il est conseillé de sauvegarder les données importantes stockées sur l'ordinateur.

   L'exemple suivant montre comment ajouter un intervalle de deux minutes (non recommandé comme état d'exécution à long terme) : **REG ADD HKLM\System\CurrentControlSet\Control\WMI\AutoLogger\Sum /v PollingInterval /t REG_DWORD /d 120000 /F**

   Les valeurs temporelles sont exprimées en millisecondes. La valeur minimale est de 60 secondes, la valeur maximale de sept jours et la valeur par défaut de 24 heures.
4. Utilisez la console Services pour arrêter et redémarrer le service de journalisation des accès utilisateur.

## Suppression des données consignées par la journalisation des accès utilisateur

La journalisation des accès utilisateur n'a pas pour vocation d'être un composant essentiel. Elle a été conçue pour affecter le moins possible les opérations système locales tout en maintenant un haut niveau de fiabilité. Ceci permet à l'administrateur de supprimer manuellement la base

de données de journalisation des accès utilisateur et les fichiers associés (chaque fichier présent dans le répertoire \Windows\System32\LogFiles\SUM\) pour répondre aux besoins opérationnels.

### Pour supprimer les données consignées par la journalisation des accès utilisateur

1. Arrêtez le service de journalisation des accès utilisateur.
2. Ouvrez l'Explorateur Windows.
3. Accédez à **\Windows\System32\Logfiles\SUM**.
4. Supprimez tous les fichiers de ce dossier.

## Gestion de la journalisation des accès utilisateur dans des environnements de grand volume

Cette section décrit ce à quoi un administrateur peut s'attendre lorsque la journalisation des accès utilisateur est utilisée sur un serveur à grand volume client :

Le nombre maximal d'accès pouvant être consignés par le biais de la journalisation des accès utilisateur est de 65 535 par jour.  Il n'est pas recommandé d'utiliser la journalisation des accès utilisateur sur des serveurs connectés directement à Internet, tels que des serveurs Web connectés directement à Internet, ni dans des scénarios où des performances extrêmement élevées constituent l'objectif principal du serveur (par exemple, dans les environnements HPC). La journalisation des accès utilisateur est principalement destinée à des scénarios mettant en jeu un intranet d'entreprise de petite ou moyenne taille, dans lesquels un volume élevé est prévu, mais pas aussi élevé qu'un grand nombre de déploiements servant un volume de trafic Internet de façon régulière.

**Journalisation des accès utilisateur dans la mémoire** : comme la journalisation des accès utilisateur utilise la méthode ESE (Extensible Storage Engine), la mémoire requise augmentera au fil du temps (ou en fonction de la quantité des demandes client). En revanche, la mémoire sera libérée lorsque le système en aura besoin pour réduire l'impact sur les performances système.

**Journalisation des accès utilisateur sur le disque**: les capacités approximatives de disque dur requises par la journalisation des accès utilisateur sont indiquées ci-dessous :

- 0 enregistrement client unique : 22 Mo
- 50 000 enregistrements client unique : 80 Mo

- 500 000 enregistrements client unique : 384 Mo
- 1 000 000 enregistrements client unique : 729 Mo

## Récupération à partir d'un état endommagé

Cette section traite de l'utilisation par la journalisation des accès utilisateur de la méthode ESE (Extensible Storage Engine) à un niveau élevé et de ce que peut faire un administrateur si les données de journalisation des accès utilisateur sont endommagées ou irrécupérables.

La journalisation des accès utilisateur utilise ESE pour optimiser l'utilisation des ressources système et pour renforcer leur résistance à l'endommagement. Pour plus d'informations sur les avantages que procure ESE, voir ESE (Extensible Storage Engine) sur MSDN.

Chaque fois que le service de journalisation des accès utilisateur démarre, ESE effectue une récupération logicielle. Pour plus d'informations, voir Fichiers ESE (Extensible Storage Engine) sur MSDN.

En cas de problème lié à la récupération logicielle, ESE effectue une récupération sur incident. Pour plus d'informations, consultez La fonction JetInit sur MSDN.

Si la journalisation des accès utilisateur ne peut toujours pas démarrer avec l'ensemble existant de fichiers ESE, elle supprimera tous les fichiers présents dans le répertoire \Windows\System32\LogFiles\SUM\. Une fois ces fichiers supprimés, le service de journalisation des accès utilisateur redémarrera et de nouveaux fichiers seront créés. Le service de journalisation des accès utilisateur reprendra son exécution comme s'il se trouvait sur un ordinateur nouvellement configuré.

> ⓘ **Important**
>
> Les fichiers présents dans le répertoire de la base de données de journalisation des accès utilisateur ne doivent jamais être déplacés ni modifiés. Tout manquement à cette règle initiera la procédure de récupération, dans laquelle s'inscrit la routine de nettoyage décrite dans cette section. Si des sauvegardes du répertoire \Windows\System32\LogFiles\SUM\ sont requises, tous les fichiers de ce répertoire doivent être sauvegardés ensemble pour qu'une opération de restauration fonctionne comme prévu.

## Activation du suivi des licences d'utilisation Dossiers de travail

Le serveur Dossiers de travail peut utiliser la journalisation des accès utilisateur pour faire état de l'utilisation du client. Contrairement à la journalisation des accès utilisateur, la journalisation des dossiers de travail n'est pas activée par défaut. Vous pouvez l'activer en modifiant la clé de Registre suivante :

```
Reg add HKLM\Software\Microsoft\Windows\CurrentVersion\SyncShareSrv /v
EnableWorkFoldersUAL /t REG_DWORD /d 1
```

Après avoir ajouté la clé de Registre, vous devez redémarrer le service SyncShareSvc sur le serveur, pour activer la journalisation.

Une fois la journalisation activée, 2 événements à caractère informatif sont consignés dans le canal Journaux Windows\Application chaque fois qu'un client se connecte au serveur. Pour Dossiers de travail, chaque utilisateur peut avoir un ou plusieurs périphériques clients se connectant au serveur et recherchant des mises à jour de données toutes les 10 minutes. Dans le cas d'un serveur gérant 1 000 utilisateurs, dotés de 2 périphériques chacun, les journaux d'applications sont remplacés toutes les 70 minutes, ce qui complique la résolution des problèmes non associés. Pour éviter ce problème, vous pouvez désactiver temporairement le service de journalisation des accès utilisateur ou augmenter la taille du canal Journaux Windows\Application du serveur.

# Voir aussi

- Bien démarrer avec la journalisation des accès utilisateur

# Guide d’optimisation des performances pour Windows Server 2022

15/08/2025

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

Lorsque vous exécutez un système de serveur dans votre organisation, les paramètres de serveur par défaut ne sont peut-être pas adaptés aux besoins de votre entreprise. Par exemple, vous pourriez avoir besoin de la consommation d'énergie la plus basse possible, ou du temps de latence le plus bas possible, ou du débit maximum possible sur votre serveur. Ce guide fournit un ensemble d’instructions utiles pour régler les paramètres serveur dans Windows Server 2022 et obtenir des gains de performance ou d’efficacité énergétique, en particulier lorsque la nature de la charge de travail varie peu au fil du temps.

Il est important que vos changements de paramètres tiennent compte du matériel, de la charge de travail, des budgets énergétiques et des objectifs de performance de votre serveur. Ce guide décrit chaque paramètre et ses effets potentiels pour vous aider à prendre une décision éclairée quant à sa pertinence par rapport à votre système, à votre charge de travail, à vos performances et à vos objectifs d'utilisation d'énergie.

> ⚠ **Avertissement**
>
> Les paramètres du Registre et les paramètres d’optimisation ont considérablement changé entre les différentes versions de Windows Server. Veillez à utiliser les recommandations d’optimisation les plus récentes pour éviter des résultats inattendus.

## Contenu de ce guide

Ce guide fournit des conseils sur les performances et l’optimisation de Windows Server 2022, qui s’articulent autour de trois catégories :

Agrandir le tableau

| Matériel serveur | Rôle serveur | Sous-système de serveur |
|---|---|---|
| Considérations relatives aux performances du matériel | Serveurs Active Directory | Gestion de la mémoire et du cache |
| Considérations relatives à la puissance du matériel | Serveurs de fichiers | Sous-système de mise en réseau |

| Matériel serveur | Rôle serveur | Sous-système de serveur |
|---|---|---|
| | Serveurs Hyper-V | Espaces de stockage direct |
| | Services Bureau à distance | Mise en réseau SDN (Software Defined Networking) |
| | Serveurs Web | |
| | Conteneurs Windows Server | |

# Modifications de cette version

## Sections ajoutées

- Mise en réseau SDN (Software Defined Networking) et recommandations relatives à la configuration de passerelle HNV et SLB
- Espaces de stockage direct
- HTTP1.1 et HTTP2
- Conteneurs Windows Server

## Sections modifiées

- Mises à jour de la section Recommandations relatives à Active Directory
- Mises à jour de la section Recommandations relatives aux serveurs de fichiers
- Mises à jour de la section Recommandations relatives aux serveur Web
- Mises à jour de la section Recommandations relatives à la puissance du matériel
- Mises à jour de la section Recommandations relatives à l'optimisation de PowerShell
- Mises à jour significatives de la section guide Hyper-V
- Section *Optimisation des performances pour les charges de travail supprimée*, liens vers les ressources pertinentes ajoutés à l'article Ressources d'optimisation supplémentaires
- *Suppression de sections dédiées au stockage*, en faveur de la nouvelle section Espaces de stockage directs et du contenu canonique de Technet
- *Suppression de la section réseau dédiée*, en faveur du contenu canonique de Technet

# Machines virtuelles dans Azure

**S'applique à :** ✔ Machines virtuelles Linux ✔ Machines virtuelles Windows ✔ Jeux d'échelle flexibles

Les machines virtuelles Azure sont l'un des types de ressources informatiques évolutives à la demande qu'Azure offre. En règle générale, une machine virtuelle convient bien si vous avez besoin de davantage de contrôle de votre environnement informatique. Cet article vous informe sur les points à prendre en compte avant de créer une machine virtuelle, sur sa création et sur sa gestion.

Une machine virtuelle Azure vous offre la flexibilité de la virtualisation sans avoir à acheter et à maintenir le matériel physique qui l'exécute. Vous devez cependant toujours assurer la maintenance de la machine virtuelle en effectuant des tâches comme la configuration, la mise à jour corrective et l'installation des logiciels qui s'exécutent sur celle-ci.

Azure machines virtuelles peuvent être utilisées de différentes manières. Quelques exemples :

- **Development et test** : Azure machines virtuelles offrent un moyen rapide et facile de créer un ordinateur avec des configurations spécifiques requises pour coder et tester une application.
- **Applications dans le cloud** : étant donné que la demande de votre application peut varier, il peut être judicieux de l'exécuter sur une machine virtuelle dans Azure. Vous payez pour des machines virtuelles supplémentaires quand vous en avez besoin et vous les arrêtez le reste du temps.
- centre de données étendu – les machines virtuelles d'un réseau virtuel Azure de Microsoft se connectent facilement au réseau de votre organisation.

## À quoi dois-je penser avant de créer une machine virtuelle ?

Il existe toujours une multitude de considérations de conception lorsque vous générez une infrastructure d'application dans Azure. Il est important de réfléchir à ces aspects des machines virtuelles avant de commencer :

- Les désignations de vos ressources
- l'emplacement de stockage des ressources,
- la taille de la machine virtuelle ;

- le nombre maximal de machines virtuelles qui peuvent être créées ;
- le système d'exploitation exécuté sur la machine virtuelle ;
- la configuration de la machine virtuelle après son démarrage ;
- les ressources liées dont a besoin la machine virtuelle.

> **Remarque**
>
> Trusted Launch par défaut (TLaD) est désormais disponible de manière générale pour les nouvelles machines virtuelles (VM) Generation 2. Avec TLaD, toutes les nouvelles machines virtuelles de génération 2 créées à l'aide d'outils clients sont par défaut configurées avec Trusted Launch, le démarrage sécurisé et le vTPM activés. Inscrivez-vous au TLaD pour implémenter les modifications par défaut dans votre ou vos environnements respectifs.

## Les éléments constituant une machine virtuelle et leur modèle de facturation

Lorsque vous déployez une machine virtuelle, vous générez également les ressources nécessaires à son bon fonctionnement. Ces ressources impliquent un coût qu'il convient de prendre en considération.

Les ressources par défaut associées à une machine virtuelle et leurs modalités de facturation sont décrites dans le tableau ci-après :

Agrandir le tableau

| Ressource | Descriptif | Coût |
|---|---|---|
| Réseau virtuel | Pour permettre à votre machine virtuelle d'échanger avec d'autres ressources | Tarification du réseau virtuel |
| Une carte d'interface réseau (NIC) virtuelle | Pour établir la connexion au réseau virtuel | Aucun coût additionnel n'est appliqué pour les cartes NIC. Cependant, le nombre de cartes NIC utilisables dépend de la taille de votre machine virtuelle. Adaptez la taille de votre machine virtuelle en conséquence et consultez les tarifs correspondants. |
| Une adresse IP privée et, dans certains cas, une adresse IP publique. | Pour assurer la communication et le transfert de données au sein de votre réseau ainsi qu'avec des réseaux externes | Tarifs des adresses IP |

| Ressource | Descriptif | Coût |
| --- | --- | --- |
| Groupe de sécurité réseau (NSG) | Pour organiser la gestion du trafic réseau entrant et sortant de votre machine virtuelle. Par exemple, vous pouvez devoir autoriser l'accès au port 22 pour SSH tout en souhaitant restreindre le trafic destiné au port 80. Le contrôle de l'ouverture ou du blocage des ports s'effectue via le NSG. | Il n'y a pas de frais supplémentaires pour les groupes de sécurité réseau dans Azure. |
| Un disque du système d'exploitation et, si nécessaire, des disques séparés pour vos données. | Il est recommandé de conserver vos données sur un disque distinct de celui du système d'exploitation. Ainsi, en cas de défaillance de la machine virtuelle, vous pouvez détacher le disque de données et le rattacher à une nouvelle instance. | Toutes les nouvelles machines virtuelles disposent d'un disque système et d'un disque local.<br>Azure ne facture pas le stockage sur disque local.<br>Le disque du système d'exploitation, généralement d'une capacité de 127 Gio mais parfois plus réduit selon les images, est facturé selon le tarif standard des disques.<br>Vous pouvez voir le coût de l'attachement de disques Premium (SSD) et Standard (HDD) à vos machines virtuelles sur la page de tarification des disques managés. |
| Dans certaines situations, une licence de système d'exploitation | Pour permettre à votre machine virtuelle d'exécuter le système d'exploitation | Le coût varie en fonction du nombre de cœurs de votre machine virtuelle, ce qui implique d'ajuster la taille de celle-ci de manière appropriée. Le coût peut être réduit par le biais du Azure Hybrid Benefit. |

Vous pouvez également choisir d'avoir Azure pouvez créer et stocker des clés SSH publiques et privées , Azure utilise la clé publique dans votre machine virtuelle et vous utilisez la clé privée lorsque vous accédez à la machine virtuelle via SSH. Dans le cas contraire, un nom d'utilisateur et un mot de passe sont requis.

Par défaut, ces ressources sont créées dans le même groupe de ressources que la machine virtuelle.

## Emplacements

Il existe plusieurs régions géographiques partout dans le monde où vous pouvez créer des ressources Azure. En règle générale, la région est appelée **emplacement** quand vous créez une

machine virtuelle. Pour une machine virtuelle, l'emplacement définit la zone de stockage des disques durs virtuels.

Ce tableau présente quelques moyens d'obtenir la liste des emplacements disponibles.

Agrandir le tableau

| Méthode | Descriptif |
|---|---|
| portail Azure | Sélectionnez un emplacement dans la liste lorsque vous créez une machine virtuelle. |
| Azure PowerShell | Utilisez la commande Get-AzLocation. |
| API REST | Utilisez l'opération Lister les emplacements. |
| Azure CLI | Utilisez l'opération az account list-locations. |

# Disponibilité

Il existe plusieurs options pour gérer la disponibilité de vos machines virtuelles dans Azure.

- **Zones de disponibilité** sont des zones physiquement séparées dans une région Azure. Les Zones de Disponibilité garantissent la connectivité des machines virtuelles avec au moins une instance au moins 99,99% du temps lorsque vous avez deux instances ou plus déployées sur au moins deux Zones de Disponibilité dans la même région Azure.
- **Virtual Machine Scale Sets** vous permet de créer et de gérer un groupe de machines virtuelles à charge équilibrée. Le nombre d'instances de machine virtuelle peut augmenter ou diminuer automatiquement en fonction d'une demande ou d'un calendrier défini. Les groupes identiques offrent une haute disponibilité à vos applications, et vous permettent de gérer, configurer et mettre à jour de manière centralisée de nombreuses machines virtuelles. Les machines virtuelles d'un groupe identique peuvent également être déployées dans plusieurs zones de disponibilité, dans une seule zone de disponibilité ou dans une région.

Pour plus d'informations, consultez les options Availability pour les machines virtuelles Azure et SLA pour les machines virtuelles Azure.

# Tailles et tarification

La taille de la machine virtuelle que vous utilisez est déterminée par la charge de travail que vous souhaitez exécuter. La taille que vous choisissez détermine ensuite des facteurs comme la puissance de traitement, la mémoire, la capacité de stockage et la bande passante du réseau.

Azure offre une grande variété de tailles pour prendre en charge de nombreux types d'utilisations.

Azure facture un prix hourly en fonction de la taille et du système d'exploitation de la machine virtuelle. Pendant des heures partielles, Azure frais uniquement pour les minutes utilisées. Le stockage est facturé séparément.

## Mise à l'échelle vers plusieurs machines virtuelles

Le nombre de machines virtuelles utilisées par votre application peut varier (montée en puissance et augmentation de la charge) pour répondre à vos besoins. Azure offre plusieurs systèmes de mise à l'échelle automatique et types d'instances en fonction de la taille de votre charge de travail. Pour plus d'informations sur la mise à l'échelle, comparez les produits de calcul basés sur des machines virtuelles.

## Limites du nombre total de cœurs des machines virtuelles

Votre abonnement comporte des limites de quota par défaut qui peuvent avoir un impact négatif sur le déploiement d'un grand nombre de machines virtuelles pour votre projet. La limite est de 20 cœurs de machine virtuelle au total par région et par abonnement. Les limites peuvent être levées en déposant un ticket de support demandant une augmentation du quota. La vérification du quota et de la capacité est effectuée séparément pendant le déploiement. Même avec un quota approuvé, le déploiement peut toujours échouer s'il n'y a pas suffisamment de capacité dans la région cible ou la zone de disponibilité.

## Disques gérés

Les disques managés s'occupent de la création et de la gestion des comptes stockage Azure en arrière-plan pour vous et garantissent que vous n'avez pas à vous soucier des limites de scalabilité du compte de stockage. Vous spécifiez la taille du disque et le niveau de performances (Standard ou Premium) et Azure crée et gère le disque. Quand vous ajoutez des disques ou effectuez un scale-up ou un scale-down de la machine virtuelle, vous n'avez pas à vous soucier du stockage utilisé. Si vous créez de nouvelles machines virtuelles, utilisez le Azure CLI ou le portail Azure pour créer des machines virtuelles avec le système d'exploitation managé et les disques de données. Si vous avez des machines virtuelles avec des disques non managés, vous pouvez convertir vos machines virtuelles en sauvegarde avec des disques managés.

Vous pouvez également gérer vos images personnalisées dans un compte de stockage par région Azure et les utiliser pour créer des centaines de machines virtuelles dans le même abonnement. Pour plus d'informations sur les disques managés, consultez la vue d'ensemble des disques managés.

## Distributions

Microsoft Azure prend en charge diverses distributions Linux et Windows. Vous trouverez des distributions disponibles dans le marketplace, le portail Azure ou en interrogeant les résultats à l'aide de l'interface CLI, de PowerShell et des API REST.

Ce tableau présente différents moyens de trouver les informations d'une image.

Agrandir le tableau

| Méthode | Descriptif |
|---|---|
| portail Azure | Les valeurs sont spécifiées automatiquement pour vous lorsque vous sélectionnez une image à utiliser. |
| Azure PowerShell | Get-AzVMImagePublisher -Location *emplacement*<br>Get-AzVMImageOffer -Location *emplacement* -Publisher *nomDuÉditeur*<br>Get-AzVMImageSku -Location *location* -Publisher *publisherName* -Offer *offerName* |
| API REST | Lister les éditeurs d'images<br>Lister les offres d'images<br>Liste des SKU des images |
| Azure CLI | az vm image list-publishers --emplacement *location*<br>az vm image list-offers --emplacement *location* --éditeur *publisherName*<br>az vm image list-skus --emplacement *location* --éditeur *publisherName* --offre *offerName* |

Microsoft collabore étroitement avec les partenaires pour vous assurer que les images disponibles sont mises à jour et optimisées pour un runtime Azure. Pour plus d'informations sur les offres partenaires Azure, consultez le Place de marché Azure

## Cloud-Init

Azure prend en charge cloud-init dans la plupart des distributions Linux qui le prennent en charge. Nous collaborons activement avec nos partenaires Linux afin de rendre disponibles dans Place de marché Azure des images compatibles cloud-init. Ces images permettent à vos déploiements et configurations cloud-init de fonctionner de manière fluide avec des machines virtuelles et des groupes de machines virtuelles identiques.

Pour plus d'informations, consultez Utilisant cloud-init sur Azure machines virtuelles Linux.

# Stockage

- Introduction à Microsoft stockage Azure
- Ajouter un disque à une machine virtuelle Linux avec l'interface de ligne de commande Azure
- Comment attacher un disque de données à une machine virtuelle Linux dans le portail Azure

## Stockage temporaire local

Certaines tailles de machine virtuelle Azure incluent le stockage temporaire local, avec certaines des tailles les plus récentes utilisant disques NVMe locaux temporaires. Le stockage temporaire local utilise des disques supplémentaires approvisionnés directement en tant que stockage local sur un hôte de machine virtuelle Azure, plutôt que sur des stockage Azure distants. Ce type de stockage convient le mieux aux données qui n'ont pas besoin d'être conservées définitivement, telles que les caches, les mémoires tampons et les fichiers temporaires. Étant donné que les données stockées sur ces disques ne sont pas sauvegardées, elles sont perdues lorsque la machine virtuelle est libérée ou supprimée. Le stockage éphémère est recréé au démarrage. Les disques éphémères locaux sont différents des disques de système d'exploitation éphémères.

Les disques temporaires locaux sont présents comme d'autres stockages distants tels que les disques SSD Premium v2, mais ont ajouté des avantages en matière de performances et ne sont pas comptabilisés par rapport aux IOPS et aux limites de débit de la machine virtuelle.

Les éléments suivants répertorient les principales caractéristiques du stockage éphémère local :

- **Latence ultra-faible** : les opérations de lecture/écriture se produisent sur le matériel physiquement colocalisé avec les ressources de calcul de la machine virtuelle, réduisant ainsi les tronçons réseau et activant les temps de réponse en sous-millisecondes.
- **IOPS et débit supérieurs** : les performances sont mises à l'échelle avec le stockage local sous-jacent, offrant souvent 8 à 10 fois plus d'E/S par seconde que les disques HDD Standard lors de l'utilisation de SSD Premium comme base, avec des limites liées à la taille de la machine virtuelle (jusqu'à la capacité du disque NVMe, limitée à 2 040 Gio).

Azure tailles de machine virtuelle comportant un « d » dans leur convention d'affectation de noms, comme les séries Da***d***sv6, Ea***d***sv6 et FXm***d***sv2, qui incluent un stockage NVMe local dédié. Ces tailles permettent de placer des fichiers temporaires, de l'espace d'échange ou des

composants à fort taux d'E/S, tels que les fichiers de base de données de SQL Server `tempdb`, sur le disque éphémère afin d'améliorer les performances.

## Réseau

- Vue d'ensemble Réseau virtuel
- Adresses IP dans Azure
- Ouverture de ports pour une machine virtuelle Linux dans Azure
- Créer un nom de domaine complet dans le portail Azure

## Disruptions de service

À Microsoft, nous travaillons dur pour nous assurer que nos services sont toujours disponibles lorsque vous en avez besoin. Il arrive parfois que des phénomènes incontrôlables entraînent des interruptions de service non planifiées.

Microsoft fournit un contrat de niveau de service (SLA) pour ses services en tant qu'engagement pour le temps d'activité et la connectivité. Vous trouverez le contrat SLA pour les services de Azure individuels à Azure Contrats de niveau de service.

Azure dispose déjà de nombreuses fonctionnalités de plateforme intégrées qui prennent en charge les applications hautement disponibles. Pour plus d'informations sur ces services, lisez Récupération après sinistre et haute disponibilité pour les applications Azure.

Cet article aborde un scénario réel de récupération d'urgence, dans lequel une région entière connaît une panne en raison d'une catastrophe naturelle majeure ou d'une interruption de service importante. Bien que ces cas soient rares, vous devez envisager l'éventualité d'une panne affectant l'ensemble d'une région. Si une région entière est confrontée à une interruption de service, les copies localement redondantes de vos données sont temporairement indisponibles. Si vous avez activé la géoréplication, trois copies supplémentaires de vos objets blob et tables stockage Azure sont stockées dans une autre région. En cas de panne régionale complète ou de sinistre dans lequel la région primaire n'est pas récupérable, Azure remapise toutes les entrées DNS dans la région géorépliquée.

Dans le cas d'une interruption de service de l'ensemble de la région où votre application de machine virtuelle Azure est déployée, nous fournissons les instructions suivantes pour Azure machines virtuelles.

## Option 1 : Lancer un basculement à l'aide d'Azure Site Recovery

Vous pouvez configurer Azure Site Recovery pour vos machines virtuelles afin de pouvoir récupérer votre application en un seul clic en quelques minutes. Vous pouvez répliquer vers la région Azure de votre choix sans être limité à des régions appairées. Vous pouvez commencer par répliquer vos machines virtuelles. Vous pouvez créer un plan de récupération pour pouvoir automatiser la totalité du processus de basculement de votre application. Vous pouvez tester vos basculements à l'avance sans affecter l'application de production ou la réplication en cours. En cas d'indisponibilité de la région principale, vous devez simplement lancer un basculement et mettre votre application dans la région cible.

## Option 2 : Attendre la récupération

Dans ce cas, aucune action n'est requise de votre part. Soyez assuré que nous nous employons activement à la restauration de la disponibilité du service. Vous pouvez voir l'état actuel du service sur notre tableau de bord Azure Service Health.

Cette option est la meilleure si vous ne configurez pas Azure Site Recovery, le stockage géoredondant avec accès en lecture ou le stockage géoredondant avant l'interruption. Si vous avez configuré le stockage géoredondant ou le stockage géoredondant avec accès en lecture pour le compte de stockage où sont stockés les disques durs virtuels de vos machines virtuelles, vous pouvez essayer de récupérer le disque dur virtuel de l'image de base et l'utiliser pour tenter d'approvisionner une nouvelle machine virtuelle. Cette option n'est pas conseillée, car aucune garantie n'assure la synchronisation des données, ce qui compromet son bon fonctionnement.

> **Remarque**
>
> N'oubliez pas que vous n'avez aucun contrôle sur ce processus et qu'il ne se produit que pour des interruptions de service au niveau régional. Ainsi, vous devez également vous appuyer sur d'autres stratégies de sauvegarde propres à l'application pour atteindre le plus haut niveau de disponibilité. Pour plus d'informations, consultez la section consacrée aux stratégies de données pour une récupération d'urgence.

## Ressources pour les interruptions de service

- Démarrer la protection de vos applications s'exécutant sur des machines virtuelles Azure avec d'Azure Site Recovery
- Pour en savoir plus sur l'implémentation d'une stratégie de récupération d'urgence et de haute disponibilité, consultez Disaster recovery and high availability for Azure applications.

- Pour développer une compréhension technique détaillée des fonctionnalités d'une plateforme cloud, consultez Azure conseils techniques de résilience.
- Si les instructions ne sont pas claires ou si vous souhaitez Microsoft effectuer les opérations en votre nom, contactez Customer Support.

## Résidence des données

Dans Azure, la fonctionnalité permettant de stocker des données client dans une seule région est actuellement disponible uniquement dans la région Asie Sud-Est (Singapour) de la région Asie-Pacifique Asie-Pacifique et Brésil Sud (État de Sao Paulo) du Brésil Géo. Pour toutes les autres régions, les données client sont stockées dans Zone géographique. Pour plus d'informations, consultez le Centre de gestion de la confidentialité.

## Étapes suivantes

Créez votre première machine virtuelle !

- Portail
- Service de contrôle d'accès Azure (CLI)
- PowerShell

---

Dernière mise à jour : 10/04/2026

# Meilleures pratiques Azure Automanage pour les machines – Windows

> ⊗ **Attention**
>
> Le 30 septembre 2027, le service Meilleures pratiques Azure Automanage sera mis hors service. Par conséquent, toute tentative de création d'un profil de configuration ou d'intégration d'un nouvel abonnement au service entraînera une erreur. Pour en savoir plus sur les modalités de migration vers Azure Policy avant cette date, cliquez **ici** .

> ⊗ **Attention**
>
> À compter du 1er février 2025, Azure Automanage commencera à déployer les modifications pour cesser la prise en charge et l'application de tous les services dépendant de l'agent Microsoft Monitoring Agent (MMA) déconseillé. Pour continuer à utiliser Change Tracking and Management, Insights de machine virtuelle, Update Management et Azure Automation, **migrez vers le nouvel agent Azure Monitor (AMA)** .

Ces services Azure sont automatiquement intégrés pour vous lorsque vous utilisez les meilleures pratiques d'Automanage pour les machines sur une machine virtuelle Windows Server. Ils sont essentiels pour notre livre blanc sur les meilleures pratiques, que vous pouvez trouver dans notre Cloud Adoption Framework.

Nous allons intégrer et configurer automatiquement tous ces services, superviser leur fonctionnement et apporter les corrections nécessaires en cas de dérive. Pour en savoir plus, consultez Azure Automanage pour machines virtuelles.

## Versions de Windows Server prises en charge

Automanage prend en charge les versions suivantes de Windows :

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

- Windows Server 2022 Azure Edition
- Windows 10

# Services participant

Agrandir le tableau

| Service | Descriptif | Profil de configuration[1] |
|---|---|---|
| Supervision des insights de machines | Azure Monitor pour les machines surveille les performances et l'intégrité de vos machines virtuelles, y compris de leurs processus en cours d'exécution et de leurs dépendances vis-à-vis d'autres ressources. | Production |
| Sauvegarde | Sauvegarde Azure fournit des sauvegardes indépendantes et isolées pour vous protéger contre la destruction involontaire des données sur vos machines. Les frais sont calculés en fonction du nombre et de la taille des machines virtuelles protégées. | Production |
| Microsoft Defender pour le cloud | Microsoft Defender pour le cloud est un système de gestion de la sécurité de l'infrastructure unifié qui renforce la posture de sécurité de vos centres de données et fournit une protection avancée contre les menaces pour vos charges de travail hybrides dans le cloud. Automanage configure l'abonnement dans lequel votre machine virtuelle réside en offre de niveau gratuit de Microsoft Defender pour le cloud (Sécurité renforcée désactivée). Si votre abonnement est déjà intégré à Microsoft Defender pour le cloud, Automanage ne le reconfigure pas. | Production, développement/test |
| Microsoft Antimalware | Microsoft Antimalware pour Azure offre une protection en temps réel qui permet d'identifier et de supprimer les virus, logiciels espions et autres logiciels malveillants. Il fournit des alertes lorsqu'un logiciel malveillant ou indésirable connu essaye de s'installer ou de s'exécuter sur vos systèmes Azure. **Remarque :** pour fonctionner correctement, Microsoft Antimalware requiert qu'aucun autre logiciel anti-programme malveillant ne soit installé. | Production, développement/test |
| Gestion des mises à jour | Vous pouvez utiliser la solution Update Management d'Azure Automation pour gérer les mises à jour du système d'exploitation de vos machines. Vous pouvez rapidement évaluer l'état des mises à jour disponibles sur toutes les machines d'agent et gérer le processus d'installation des mises à jour nécessaires pour les serveurs. | Production, développement/test |
| Suivi des modifications et inventaire | La fonctionnalité Suivi des modifications et inventaire combine les fonctions de suivi des modifications et d'inventaire pour vous permettre d'effectuer le suivi des modifications apportées à l'infrastructure des machines virtuelles et des serveurs. Le service | Production, développement/test |

| Service | Descriptif | Profil de configuration[1] |
| --- | --- | --- |
| | prend en charge le suivi des modifications sur les services, les démons, les logiciels, le registre et les fichiers de votre environnement pour vous aider à diagnostiquer les changements indésirables et à déclencher des alertes. La prise en charge de l'inventaire vous permet d'interroger les ressources intégrées pour voir les applications installées et d'autres éléments de configuration. | |
| Configuration de l'ordinateur | La stratégie de configuration d'une machine est utilisée pour superviser la configuration de la machine et indiquer sa conformité. Le service de Gestion automatique installe les lignes de base de sécurité Windows à l'aide de l'extension de la configuration invité. Pour les machines Windows, le service de configuration des machines installe la base de référence en mode d'audit uniquement. Vous pouvez voir à quel niveau votre machine virtuelle n'est pas conforme à la base de référence. Toutefois, la non-conformité n'est pas automatiquement corrigée. En savoir plus. Pour modifier le mode d'audit pour les machines Windows, utilisez un profil personnalisé pour choisir votre paramètre de mode d'audit. En savoir plus | Production, développement/test |
| Diagnostics de démarrage | Les diagnostics de démarrage sont une fonctionnalité de débogage pour les machines virtuelles Azure qui permet de diagnostiquer les échecs de démarrage de machine virtuelle. Les diagnostics de démarrage permettent à un utilisateur d'observer l'état de la machine virtuelle lors de son démarrage en collectant des informations de journal série et des captures d'écran. Cette fonctionnalité est activée uniquement pour les machines qui utilisent des disques managés. | Production, développement/test |
| Windows Admin Center | Utilisez Windows Admin Center (préversion) dans le portail Azure pour gérer le système d'exploitation Windows Server au sein d'une machine virtuelle Azure. Cette fonctionnalités n'est prise en charge que pour les machines utilisant Windows Server version 2016 ou ultérieure. Automanage configure Windows Admin Center via une adresse IP privée. Si vous souhaitez vous connecter à Windows Admin Center via une adresse IP publique, ouvrez une règle de port entrant pour le port 6516. Automanage intègre Windows Admin Center pour le profil Dev/Test par défaut. Utilisez les préférences pour activer ou désactiver Windows Admin Center pour les environnements de Production et de Dev/Test. | Production, développement/test |
| Compte Azure Automation | Azure Automation prend en charge la gestion tout au long du cycle de vie de votre infrastructure et des applications. | Production, développement/test |

| Service | Descriptif | Profil de configuration[1] |
| --- | --- | --- |
| Espace de travail Log Analytics | Azure Monitor stocke des données de journal dans un espace de travail Log Analytics, qui est une ressource Azure et un conteneur où les données sont collectées, agrégées, et qui sert de limite d'administration. | Production, développement/test |

[1] La sélection de profil de configuration est disponible lorsque vous activez Automanage. Vous pouvez également créer votre propre profil personnalisé avec l'ensemble des services et paramètres Azure dont vous avez besoin.

# Étapes suivantes

Essayez d'activer le service Automanage pour machines dans le portail Azure.

Activer le service Automanage pour machines dans le portail Azure

---

Dernière mise à jour : 07/05/2025

# Vue d’ensemble de la sécurité des machines virtuelles Azure

Cet article fournit une vue d’ensemble des principales fonctionnalités de sécurité Azure pour les machines virtuelles.

Machines virtuelles Azure vous aide à déployer une large gamme de solutions informatiques de manière agile. Le service prend en charge Microsoft Windows, Linux, Microsoft SQL Server, Oracle, IBM, SAP et Azure BizTalk Services. Vous pouvez déployer n’importe quelle charge de travail et n’importe quelle langue sur presque n’importe quel système d’exploitation.

Les machines virtuelles Azure offrent la flexibilité de la virtualisation sans acheter et maintenir du matériel physique. Vous pouvez créer et déployer des applications avec l’assurance que vos données sont protégées dans des centres de données hautement sécurisés.

Azure vous aide à construire des solutions conformes et renforcées en sécurité qui :

- Protégez les machines virtuelles contre les virus et les malwares.
- Chiffrez les données sensibles.
- Sécurisent le trafic réseau.
- Identifient et détectent les menaces.
- Répondez aux exigences de conformité.

## Lancement sécurisé

Le démarrage sécurisé est la valeur par défaut pour les machines virtuelles Azure de génération 2 nouvellement créées et les ensembles de machines virtuelles identiques. Le lancement approuvé protège contre les techniques d’attaque avancées et persistantes, notamment les kits de démarrage, les rootkits et les programmes malveillants au niveau du noyau.

Le lancement sécurisé fournit :

- **Démarrage sécurisé** : Protège contre l’installation de rootkits et kits de démarrage basés sur des malwares en garantissant que seuls les systèmes d’exploitation et pilotes signés peuvent démarrer.
- **vTPM (Virtual Trusted Platform Module)** : Un coffre-fort sécurisé dédié pour les clés et les mesures qui permet l’attestation et la vérification de l’intégrité du démarrage.

- **Surveillance de l'intégrité du démarrage** : Utilise l'attestation via Microsoft Defender for Cloud pour vérifier l'intégrité de la chaîne de démarrage et alerter en cas de défaillance.

Vous pouvez activer le lancement sécurisé sur les machines virtuelles existantes et les groupes de machines virtuelles à mise à l'échelle. Pour plus d'informations, consultez Lancement approuvé pour les machines virtuelles Azure.

## Informatique confidentielle

L'informatique confidentielle Azure protège les données lors de l'utilisation via des environnements d'exécution approuvés basés sur le matériel. Les machines virtuelles confidentielles utilisent la technologie AMD SEV-SNP pour créer une limite matérielle appliquée entre votre application et la pile de virtualisation.

Les machines virtuelles confidentielles fournissent :

- **Isolation matérielle** : entre les machines virtuelles, l'hyperviseur et le code de gestion de l'hôte.
- **Chiffrement de disque du système d'exploitation confidentiel** : lie les clés de chiffrement de disque au module TPM de la machine virtuelle, ce qui rend le contenu du disque accessible uniquement à la machine virtuelle.
- **Version de clé sécurisée** : liaison de chiffrement entre l'attestation de plateforme et les clés de chiffrement de machine virtuelle.
- **Attestation** : stratégies personnalisables pour garantir la conformité de l'hôte avant le déploiement.

Pour plus d'informations, consultez machines virtuelles confidentielles Azure.

## Chiffrement du disque de machine virtuelle

> **ⓘ Important**
>
> Azure Disk Encryption est prévu pour la mise hors service le **15 septembre 2028**. Jusqu'à cette date, vous pouvez continuer à utiliser Azure Disk Encryption sans interruption. Le 15 septembre 2028, les charges de travail compatibles avec ADE continueront d'être exécutées, mais les disques chiffrés ne pourront pas être déverrouillés après le redémarrage de la machine virtuelle, ce qui entraîne une interruption du service.
>
> Utilisez le chiffrement sur l'hôte pour les nouvelles machines virtuelles ou tenez compte des tailles de machine virtuelle confidentielle avec le chiffrement de disque du système

d'exploitation pour les charges de travail d'informatique confidentielle. Toutes les machines virtuelles compatibles ADE (y compris les sauvegardes) doivent migrer vers le chiffrement à l'hôte avant la date de mise hors service pour éviter toute interruption de service. Pour plus d'informations, consultez Migrer d'Azure Disk Encryption vers le chiffrement sur l'hôte .

Azure propose plusieurs options de chiffrement pour les disques managés :

- **Chiffrement côté serveur (SSE)** : également appelé chiffrement au repos ou chiffrement stockage Azure, SSE est toujours activé et chiffre automatiquement les données sur des disques managés Azure (disques de système d'exploitation et de données) lors de la conservation des clusters de stockage. SSE chiffre les données de manière transparente grâce au chiffrement AES 256 bits, conforme à la norme FIPS 140-2. SSE n'affecte pas les performances du disque et n'a aucun coût supplémentaire. Toutefois, SSE ne chiffre pas les disques temporaires ou les caches de disque.

- **Chiffrement sur l'hôte** : améliore SSE en chiffrant les disques temporaires et les caches de disque au repos, avec des données qui circulent de manière chiffrée vers des clusters de stockage. Ce chiffrement fournit un chiffrement de bout en bout pour vos données de machine virtuelle. Le chiffrement sur l'hôte n'utilise pas l'UC de votre machine virtuelle et n'affecte pas les performances. Les disques temporaires et les disques de système d'exploitation éphémères sont chiffrés avec des clés gérées par la plateforme. Les caches de disque de données et de système d'exploitation sont chiffrés avec des clés gérées par le client ou gérées par la plateforme, en fonction du type de chiffrement de disque.

- **Chiffrement de disque confidentiel** : pour les machines virtuelles confidentielles, ce chiffrement lie les clés de chiffrement de disque au module TPM de la machine virtuelle, ce qui rend le contenu de disque protégé accessible uniquement à la machine virtuelle.

Par défaut, les disques gérés utilisent des clés gérées par la plateforme sans configuration supplémentaire. Pour les clés gérées par le client, vous pouvez utiliser Azure Key Vault, Azure Key Vault Managed HSM ou Azure Cloud HSM pour contrôler et gérer vos propres clés de chiffrement.

Pour plus d'informations, consultez Vue d'ensemble des options de chiffrement de disque managé et du chiffrement côté serveur du stockage disque Azure.

## Gestion des clés

Azure Key Vault fournit un stockage sécurisé pour les clés de chiffrement, les secrets et les certificats. Azure offre plusieurs solutions de gestion de clés avec différents niveaux de sécurité :

- **Azure Key Vault Standard** : FIPS 140-2 Niveau 1 validé, service multilocataire avec des clés protégées par logiciel.
- **Azure Key Vault Premium** : FIPS 140-3 Niveau 3 validé, service multilocataire avec des clés protégées par HSM.
- **Azure Key Vault Managed HSM** : FIPS 140-3 Niveau 3 validé, service monolocataire qui fournit un contrôle client total sur le HSM et la souveraineté des clés.

Pour les machines virtuelles, ces services peuvent stocker :

- **Clés de chiffrement de** disque : clés gérées par le client pour chiffrer les disques managés via des jeux de chiffrement de disque.
- **Clés de chiffrement SQL Server** : clés pour le chiffrement transparent des données sur les machines virtuelles SQL Server.
- **Secrets d'application** : clés et secrets utilisés par les applications s'exécutant sur vos machines virtuelles.

Vous gérez les autorisations et l'accès aux éléments protégés via l'ID Microsoft Entra. Vous pouvez auditer l'utilisation des clés et conserver un contrôle total sur vos clés de chiffrement.

Pour plus d'informations, consultez Qu'est-ce qu'Azure Key Vault ?, Qu'est-ce qu'Azure Key Vault Managed HSM ? et la gestion des clés dans Azure.

## Sauvegarde de machine virtuelle

Sauvegarde Azure est une solution évolutive qui protège vos données de machine virtuelle avec un investissement en capital nul et des coûts d'exploitation minimes. Les erreurs d'application peuvent endommager vos données, et les erreurs humaines peuvent introduire des bogues. Avec Sauvegarde Azure, vos machines virtuelles exécutant Windows et Linux sont protégées.

Sauvegarde Azure fournit :

- **Sauvegardes indépendantes et isolées** : Le coffre-fort des services de récupération stocke les sauvegardes et assure une gestion intégrée des points de récupération. Il protège également contre la destruction accidentelle des données.
- **Points de récupération cohérents avec l'application** : Capture l'état des données applicatives au moment de la sauvegarde pour l'exécution des machines virtuelles.

- **Aucune connectivité sortante explicite requise** : Toute la communication et le transfert de données se font sur le réseau dorsale Azure.
- **Protection contre la suppression progressive** : conserve les données de sauvegarde supprimées pendant 14 jours supplémentaires, afin que vous puissiez récupérer sans perte de données.
- **Restauration inter-régions** : Restaurez les VM Azure dans une région secondaire Azure pairée pour les scénarios de reprise après sinistre.

Pour plus d'informations, consultez La faq sur la sauvegarde Azure et le service Sauvegarde Azure.

## Azure Site Recovery (Récupération de site Azure)

Azure Site Recovery permet d'orchestrer la réplication, le basculement et la récupération des charges de travail et des applications afin qu'elles soient disponibles à partir d'un emplacement secondaire si votre emplacement principal tombe en panne.

Site Recovery :

- **Simplifie la stratégie BCDR** : facilite la gestion de la réplication, du basculement et de la récupération de plusieurs charges de travail et applications métier depuis un seul endroit.
- **Offre une réplication flexible** : Répliquer des charges de travail fonctionnant sur Hyper-V VM, VMware VM et serveurs physiques Windows/Linux.
- **Prend en charge le basculement et la reprise** : Permet d'effectuer des basculements de test dans le cadre d'exercices de reprise après sinistre sans affecter les environnements de production.
- **Élimine les centres de données secondaires** : Répliquer sur Azure, éliminant ainsi le coût et la complexité de la maintenance d'un site secondaire.

Pour plus d'informations, consultez Présentation d'Azure Site Recovery ?, Fonctionnement d'Azure Site Recovery et quelles charges de travail sont protégées par Azure Site Recovery ?

## Réseau virtuel

Les machines virtuelles nécessitent une connectivité réseau. Azure nécessite que les machines virtuelles soient connectées à un réseau virtuel Azure.

Un réseau virtuel Azure est une construction logique basée sur le réseau physique Azure. Chaque réseau virtuel logique Azure est isolé des autres réseaux virtuels Azure. Cette isolation permet de

s'assurer que le trafic réseau dans vos déploiements n'est pas accessible à d'autres clients Microsoft Azure.

Pour plus d'informations, consultez vue d'ensemble de la sécurité réseau Azure et Vue d'ensemble du réseau virtuel.

## Gestion des stratégies de sécurité

Microsoft Defender pour Cloud vous aide à prévenir, détecter et répondre aux menaces. Defender pour le cloud offre une visibilité et un contrôle complets sur la sécurité de vos ressources Azure. Defender for Cloud offre une surveillance intégrée de la sécurité et une gestion des politiques sur l'ensemble de vos abonnements Azure.

Defender pour Cloud vous aide à optimiser et à surveiller la sécurité des machines virtuelles en :

- Fournir des recommandations de sécurité pour les machines virtuelles.
- Surveillance de l'état de vos machines virtuelles.
- Fournir Microsoft Defender pour serveurs avec une protection avancée contre les menaces.

Microsoft Defender pour serveurs inclut les éléments suivants :

- Intégration de Microsoft Defender for Endpoint pour la détection et réponse sur les points de terminaison.
- Évaluation des vulnérabilités pour identifier les faiblesses de sécurité.
- Accès juste-à-temps aux machines virtuelles pour réduire la surface d'attaque.
- Surveillance de l'intégrité des fichiers pour détecter les modifications des fichiers critiques.
- Contrôles adaptatifs des applications pour les applications approuvées.

Pour plus d'informations, consultez Présentation de Microsoft Defender pour cloud, Microsoft Defender pour serveurs et Microsoft Defender pour cloud forum aux questions.

## Conformité

Les offres de conformité de Microsoft et les rapports d'audit identifient quels services cloud sont visés pour chaque audit formel tiers. La portée peut varier selon l'offre, utilisez donc les offres actuelles de conformité Microsoft et la documentation d'audit au lieu d'une liste de certification statique pour Machines virtuelles Azure.

Pour plus d'informations, consultez les offres de conformité Microsoft, Azure et autres services cloud Microsoft dans le périmètre d'audit de conformité, Microsoft Trust Center : Conformité, et la documentation sur la conformité Azure.

# Étapes suivantes

Découvrez les meilleures pratiques de sécurité pour les machines virtuelles et les systèmes d'exploitation.

ⓘ**Remarque :** L'auteur a créé cet article avec l'aide de l'IA. En savoir plus

---

Dernière mise à jour : 21/07/2026

# Vue d’ensemble des mises à jour de l’invité et de la maintenance de l’hôte

**S’applique à :** ✔ Machines virtuelles Linux ✔ Machines virtuelles Windows ✔ Ensembles de mise à l’échelle flexibles ✔ Ensembles de mise à l’échelle uniformes

Cet article présente les options de mise à jour de l’invité et de maintenance de l’hôte pour les machines virtuelles Azure (VM).

Azure met régulièrement à jour son infrastructure pour améliorer la fiabilité et les performances et la sécurité, ou pour lancer de nouvelles fonctionnalités. La plupart des mises à jour sont transparentes pour vous. Pour intégrer ces mises à jour, Azure utilise une infrastructure robuste qui comprend des paires de régions et des zones de disponibilité combinées à de nombreux outils et fonctionnalités.

Azure vous offre également la possibilité de contrôler les mises à jour sur les machines Azure telles que les jeux d’échelle de machines virtuelles, les machines hôtes, les machines virtuelles invitées et les extensions attachées aux machines virtuelles. Ce contrôle est possible grâce à des configurations de maintenance, que vous pouvez utiliser pour définir des planifications récurrentes aux moments où vous souhaitez que les mises à jour disponibles de la plateforme aient lieu.

Avec les mises à jour de l’infrastructure Azure, vous pouvez :

- Mettre à niveau les composants du réseau.
- Retirer le matériel du réseau.
- Corriger les composants logiciels dans les environnements d’hébergement.
- Mettez à jour le logiciel du système d’exploitation invité sur les machines virtuelles.

Pour effectuer ces mises à jour, utilisez les outils disponibles dans Azure.

La plateforme de maintenance vise à vous fournir une *expérience de maintenance unifiée* pour toutes les ressources Azure qui sont affectées pendant la maintenance. L’expérience de maintenance est disponible pour les ressources hôte (Azure Dedicated Host et machines virtuelles isolées) et les ressources invitées (machines virtuelles et machines virtuelles Azure Arc), Azure Kubernetes Service, Salesforce Marketing Cloud (SFMC) et les passerelles de réseau (Passerelle VPN Azure, Azure ExpressRoute et les passerelles de réseau virtuel dans Azure). Pour le déploiement, utilisez le portail Azure, PowerShell ou le CLI Azure.

Le contrôle de maintenance vous offre la possibilité d'ignorer ou de reporter certaines mises à jour et de les planifier uniquement pendant le créneau de maintenance de votre choix. Dans des circonstances exceptionnelles, lorsqu'un problème de sécurité de gravité élevée survient et peut potentiellement compromettre les services aux clients, Azure se réserve le droit de contourner ces calendriers pour mettre en œuvre des modifications urgentes. Cette mesure est prise uniquement pour garantir la sécurité et l'intégrité des services clients. Elle est utilisée uniquement lorsque les mises à jour n'ont aucun effet sur les ressources client. Ces instances sont peu fréquentes et sont appelées uniquement en dernier recours pour protéger les ressources.

# Maintenance de l'hôte

La maintenance des hôtes est effectuée sur les hôtes physiques où se trouvent les machines virtuelles et est généralement transparente pour vous. Certaines mises à jour peuvent avoir un effet sur les hôtes que vous pouvez tolérer. Pendant ces mises à jour, les machines virtuelles allouées sur les hôtes peuvent être gelées (*mises à jour sans redémarrage*), redémarrées (*mises à jour avec redémarrage*) ou migrer en direct vers un autre hôte mis à jour. Azure choisit le mécanisme de mise à jour qui affecte vos machines virtuelles le moins.

## Hôtes dédiés, machines virtuelles isolées et hôtes partagés

L'expérience de maintenance des hôtes est disponible pour les hôtes dédiés, les machines virtuelles isolées et les hôtes partagés. Les hôtes dédiés sont des hôtes dans lesquels un client possède toutes les machines virtuelles. Les hôtes partagés sont des hôtes dans lesquels les machines virtuelles de plusieurs clients résident ensemble. Les machines virtuelles isolées sont de grandes machines virtuelles isolées d'un type de matériel spécifique et dédié à un client unique.

Sur les hôtes dédiés, la fonctionnalité de maintenance de l'hôte est disponible pour toutes les mises à jour. Vous pouvez opter pour le contrôle de la maintenance et programmer une fenêtre de maintenance en fonction de vos besoins dans les 35 jours suivant la date de la dernière maintenance. Les machines virtuelles isolées bénéficient de la fonctionnalité de contrôle de maintenance, au même titre que les hôtes dédiés.

Vous pouvez utiliser contrôle de maintenance pour :

- Appliquer toutes les mises à jour ensemble.
- Attendre jusqu'à 35 jours avant d'appliquer les mises à jour au machines hôtes.
- Configurer un calendrier de maintenance ou utiliser Azure Functions pour automatiser les mises à jour des plateformes.
- Configurer la maintenance des abonnements et des groupes de ressources.

Sur les hôtes partagés, l'expérience de maintenance est disponible pour les mises à jour avec redémarrage ou les mises à jour à fort impact. Actuellement, l'expérience de contrôle de maintenance n'est pas disponible pour les mises à jour qui prennent moins de 30 secondes.

## Notifications de maintenance

Azure fournit des notifications avant, pendant et après les opérations de maintenance. Événements planifiés fournissent des notifications avant qu'un événement ne commence et pendant son déroulement afin que votre application puisse réagir automatiquement. Les événements Flash Health fournissent des informations que vous pouvez exploiter pour analyser les alertes et les tendances en matière de disponibilité des machines virtuelles, pour l'établissement de rapports et l'analyse des causes profondes.

### Événements planifiés

Événements planifiés vous informent à l'avance des incidences à venir sur la disponibilité afin que vous puissiez préparer votre application à l'avance. Elles sont envoyées directement à la machine virtuelle concernée et à toutes les machines virtuelles du même groupe de placement pour une résilience automatisée. Pour plus d'informations sur les événements planifiés, consultez Événements planifiés pour les machines virtuelles Windows et Événements planifiés pour Linux

### Événements de santé Flash

Les événements d'état de santé Flash fournissent des informations en quasi-temps réel concernant les impacts passés sur la disponibilité afin que vous puissiez réagir rapidement et atténuer facilement les incidents. Les informations Flash sont disponibles dans Azure Monitor, AzureResource Graph ou Azure Event Grid pour s'intégrer à vos systèmes et processus.

# Mises à jour des invités

Cette section explique les options de mise à jour d'invité(e).

## Mise à niveau d'image de système d'exploitation

Les mises à niveau automatiques du système d'exploitation sont disponibles pour les groupes identiques de machines virtuelles. Une mise à niveau fonctionne en remplaçant le disque du système d'exploitation d'une machine virtuelle par un nouveau disque qui a été créé à l'aide de la dernière version de l'image. Les extensions et scripts de données personnalisés configurés sont exécutés sur le disque du système d'exploitation, tandis que les disques de données sont

conservés. Pour réduire le temps d'arrêt de l'application, les mises à niveau ont lieu par lots. Pas plus de 20 % des machines virtuelles du groupe identique ne sont mises à niveau à un moment donné.

Le contrôle de la maintenance est également disponible pour les mises à niveau d'images du système d'exploitation. Vous pouvez choisir de participer à cette expérience en utilisant les configurations de maintenance pour planifier le moment où ces mises à jour d'images doivent être appliquées. Pour utiliser cette fonctionnalité, les groupes identiques doivent avoir les mises à niveau automatiques du système d'exploitation activées. Vous pouvez définir une récurrence pour une durée maximale d'une semaine (sept jours). Un minimum de cinq heures est nécessaire pour la fenêtre de maintenance.

## Application de correctifs aux machines virtuelles invitées

Mise à jour corrective automatique des invités de machine virtuelle est intégrée au Gestionnaire de mise à jour Azure. Vous pouvez enregistrer des planifications de déploiement récurrents pour installer des mises à jour pour vos machines Windows Server et Linux dans Azure, dans des environnements locaux et dans d'autres environnements cloud qui sont connectés à l'aide de serveurs utilisant Azure Arc.

## Mises à niveau des extensions invitées

La mise à niveau automatique des extensions est disponible pour les machines virtuelles Azure et les groupes de machines virtuelles identiques Azure. Lorsque la mise à niveau automatique des extensions est activée sur une machine virtuelle ou un groupe identique, l'extension est automatiquement mise à niveau chaque fois que l'éditeur de l'extension publie une nouvelle version pour cette extension. Le processus de mise à niveau de l'extension remplace la version existante de l'extension sur une VM par la nouvelle version de la même extension.

L'intégrité de la machine virtuelle est analysée après l'installation de la nouvelle extension. Si la machine virtuelle n'est pas dans un état sain dans les cinq minutes suivant la fin de la mise à niveau, la version précédente de l'extension du navigateur est restaurée. Le contrôle de la maintenance des extensions n'est actuellement disponible que via le CLI et PowerShell. Vous pouvez définir une récurrence pour une durée maximale d'une semaine (sept jours). Un minimum de cinq heures est nécessaire pour la fenêtre de maintenance.

## Correctif à chaud

Hotpatching est une nouvelle méthode d'installation des mises à jour sur les nouvelles machines virtuelles Windows Server Azure Edition, sans nécessiter de redémarrage après l'installation. La mise à jour corrective à chaud pour les machines virtuelles Windows Server Azure Edition offre les avantages suivants :

- Réduction de l'effet sur la charge de travail et diminution du nombre de redémarrages.
- Déploiement plus rapide des mises à jour, car les packages sont plus petits, s'installent plus rapidement et offrent une orchestration des patchs plus facile à mettre en œuvre avec Update Manager
- Meilleure protection, car les packages de mise à jour Hotpatch se limitent à l'étendue des mises à jour de sécurité Windows, qui s'installent plus rapidement et sans redémarrage

## Gestion des mises à jour Azure

Vous pouvez utiliser Update Manager dans Azure Automation pour gérer les mises à jour système de vos machines virtuelles Windows et Linux dans Azure, dans des environnements locaux et dans d'autres environnements cloud. Vous pouvez rapidement évaluer l'état des mises à jour disponibles sur toutes les machines d'agent et gérer le processus d'installation des mises à jour nécessaires pour les serveurs.

## Gestionnaire de mises à jour

Gestionnaire des mises à jour est un service unifié dans Azure qui vous aide à gérer et à contrôler les mises à jour (Windows et Linux), aussi bien localement que sur d'autres plateformes cloud, dans des environnements hybrides, depuis un tableau de bord unique. La nouvelle fonctionnalité offre une expérience native et prête à l'emploi avec des contrôles d'accès granulaires. Vous avez la possibilité de créer des planifications ou d'agir maintenant et la possibilité de vérifier automatiquement les mises à jour. La fonctionnalité améliorée garantit aux administrateurs une visibilité sur l'intégrité de tous les systèmes de l'environnement. Pour plus d'informations, consultez avantages clés.

# Contenu connexe

Pour plus d'informations sur les moyens d'augmenter la disponibilité de vos applications et services, voir Options de disponibilité pour les machines virtuelles Azure.

---

Dernière mise à jour : 27/09/2026

# Surveiller Machines virtuelles Azure

Cet article aborde les points suivants :

- Types de données de monitoring que vous pouvez collecter pour ce service.
- Méthodes d'analyse de ces données.

> ⓘ **Remarque**
>
> Si vous connaissez déjà ce service et/ou Azure Monitor et que vous voulez simplement savoir comment analyser les données de monitoring, consultez la section **Analyser** vers la fin de cet article.

Quand vous avez des applications critiques et des processus métier qui s'appuient sur des ressources Azure, vous devez monitorer votre système et obtenir des alertes. Le service Azure Monitor collecte et agrège les métriques et les journaux de chaque composant de votre système. Azure Monitor vous fournit une vue de la disponibilité, des performances et de la résilience, et vous avertit des problèmes. Vous pouvez utiliser le portail Azure, PowerShell, Azure CLI, l'API REST ou des bibliothèques de client pour configurer et visualiser les données de monitoring.

- Pour plus d'informations sur Azure Monitor, consultez la vue d'ensemble d'Azure Monitor.
- Pour plus d'informations sur le monitoring des ressources Azure en général, consultez Monitorer les ressources Azure avec Azure Monitor.

Cet article fournit une vue d'ensemble de la façon de surveiller l'intégrité et les performances des machines virtuelles Azure.

> ⓘ **Remarque**
>
> Cet article fournit des informations de base pour vous aider à prendre en main la surveillance de Machines virtuelles Azure. Pour obtenir un guide complet sur la surveillance de l'ensemble de votre environnement de machines virtuelles Azure et de machines virtuelles hybrides, consultez le **Guide de surveillance du déploiement de machines virtuelles**.

# Vue d’ensemble : surveiller les métriques et les journaux d’hôte et d’invité de machines virtuelles

Vous pouvez collecter des métriques et des journaux à partir de :

- **Hôte de la machine virtuelle** : ces données concernent la session Hyper-V qui gère les systèmes d’exploitation invités et comprennent des informations sur l’utilisation du processeur, du réseau et du disque.
- **Invité de la machine virtuelle** : ces données concernent le système d’exploitation et les applications s’exécutant dans la machine virtuelle.

Les données au niveau de l’hôte vous donnent une compréhension des performances et de la charge globales de la machine virtuelle, tandis que les données au niveau de l’invité vous donnent une visibilité sur les applications, les composants et les processus s’exécutant sur l’ordinateur, ainsi que leurs performances et leur intégrité. Par exemple, si vous êtes en train de résoudre un problème de performances, vous pouvez commencer par des métriques d’hôte pour voir quelle machine virtuelle est sous une charge importante, puis utiliser les métriques invitées pour explorer les détails du système d’exploitation et des performances de l’application.

## Données de l’hôte de machine virtuelle

Les données d’hôte de machine virtuelle sont disponibles sans configuration supplémentaire.

Agrandir le tableau

| Scénario | Détails | Collecte de données | Données disponibles | Recommandations |
|---|---|---|---|---|
| **Métriques et journaux de l’hôte de machine virtuelle** | Surveillez la stabilité, l’intégrité et l’efficacité de l’hôte physique sur lequel la machine virtuelle est en cours d’exécution. Effectuez un scale-up ou un scale-down en fonction de la charge sur votre application. | Disponible par défaut sans aucune configuration supplémentaire. | • Métriques de performance de l’hôte<br>• Journaux d’activité<br>• Diagnostics de démarrage | Permettez aux règles d’alerte recommandées d’être averties lorsque les métriques de l’hôte clé s’écartent de leurs valeurs de base attendues. |

# Données invitées de machine virtuelle

Les données invitées de machine virtuelle vous permettent d'analyser et de dépanner les performances et l'efficacité opérationnelle des charges de travail exécutées sur vos machines virtuelles. Pour surveiller les données invitées de machine virtuelle, vous devez installer l'agent Azure Monitor sur la machine virtuelle et configurer une règle de collecte de données (DCR). La fonctionnalité VM Insights installe automatiquement l'agent Azure Monitor sur votre machine virtuelle et configure une règle de collecte de données par défaut pour une intégration rapide et simple.

Agrandir le tableau

| Scénario | Détails | Collecte de données | Données disponibles | Recommandations |
|---|---|---|---|---|
| **Surveillance de base : indicateurs de performances clés** | Identifiez les problèmes liés aux performances du système d'exploitation, notamment l'utilisation du processeur et du disque , la mémoire disponible et les performances réseau en collectant un ensemble prédéfini et de base de compteurs de performances clés. | Activer VM Insights | Ensemble prédéfini de compteurs de performances invités clés | • Utilisez-le comme point de départ.<br>• Activez les alertes de référence Azure Monitor recommandées pour les machines virtuelles.<br>• Ajoutez des compteurs de performances invités d'intérêt et des journaux de système d'exploitation recommandés, selon les besoins. |
| **Surveillance de base : mappage de composants d'application** | Mappez les composants d'application sur une machine virtuelle particulière et entre les machines | Activer la fonctionnalité Map de VM Insights | Dépendances entre les composants d'application s'exécutant sur la machine virtuelle | |

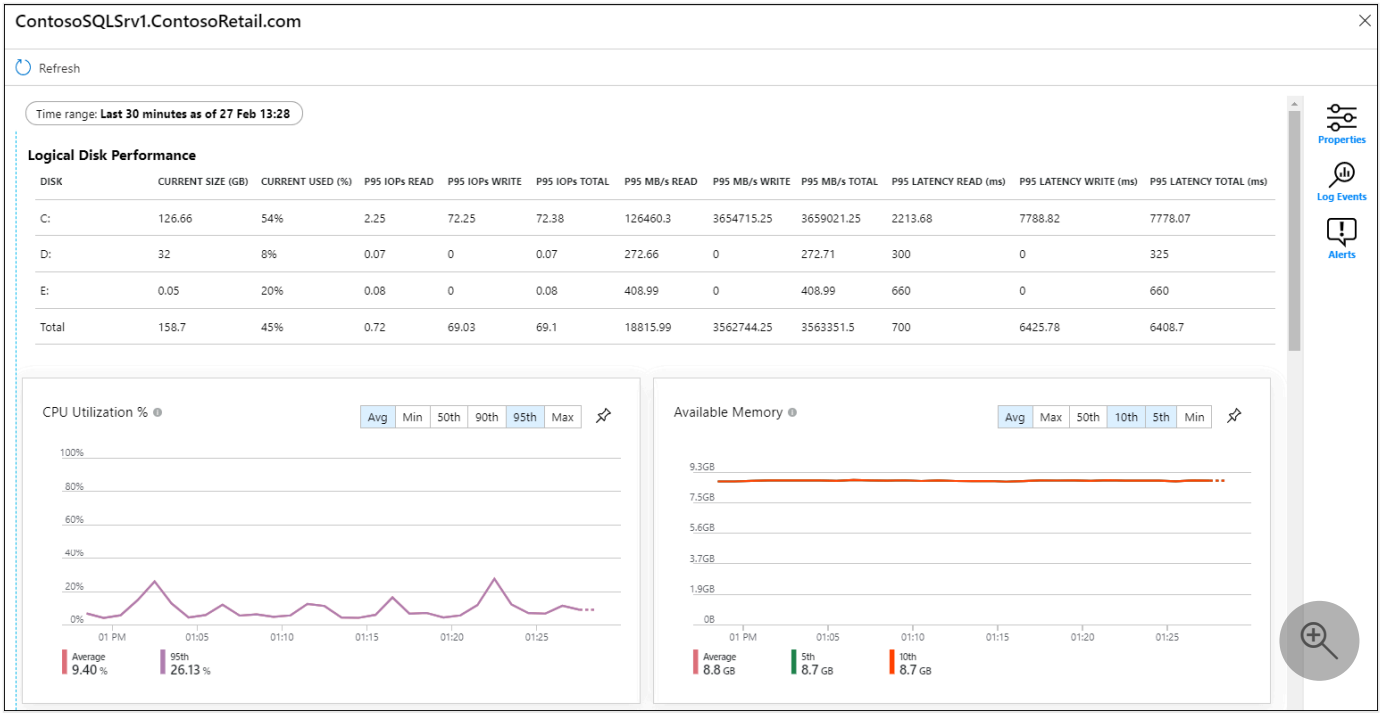
| Scénario | Détails | Collecte de données | Données disponibles | Recommandations |
| --- | --- | --- | --- | --- |
| | virtuelles et découvrez les dépendances qui existent entre les composants d'application.<br><br>Ces informations sont importantes pour la résolution des problèmes, l'optimisation des performances et la planification des modifications ou des mises à jour apportées à l'infrastructure d'application. | | | |
| **Métriques et journaux du système d'exploitation de machine virtuelle (recommandé)** | Surveillez les performances et les événements des applications, la consommation des ressources par des applications et des processus spécifiques ainsi que les performances et les événements au niveau du système d'exploitation. | Installez l'agent Azure Monitor sur la machine virtuelle et configurez une règle de collecte de données. | • Compteurs de performances de l'invité<br>• Événements Windows<br>• Événements Syslog | • Dans Windows, collectez les journaux d'application aux niveaux **Critique**, **Erreur** et **Avertissement** .<br>• Dans Linux, collectez les journaux d'activité des installations **LOG_SYSLOG** au niveau **LOG_WARNING** . |

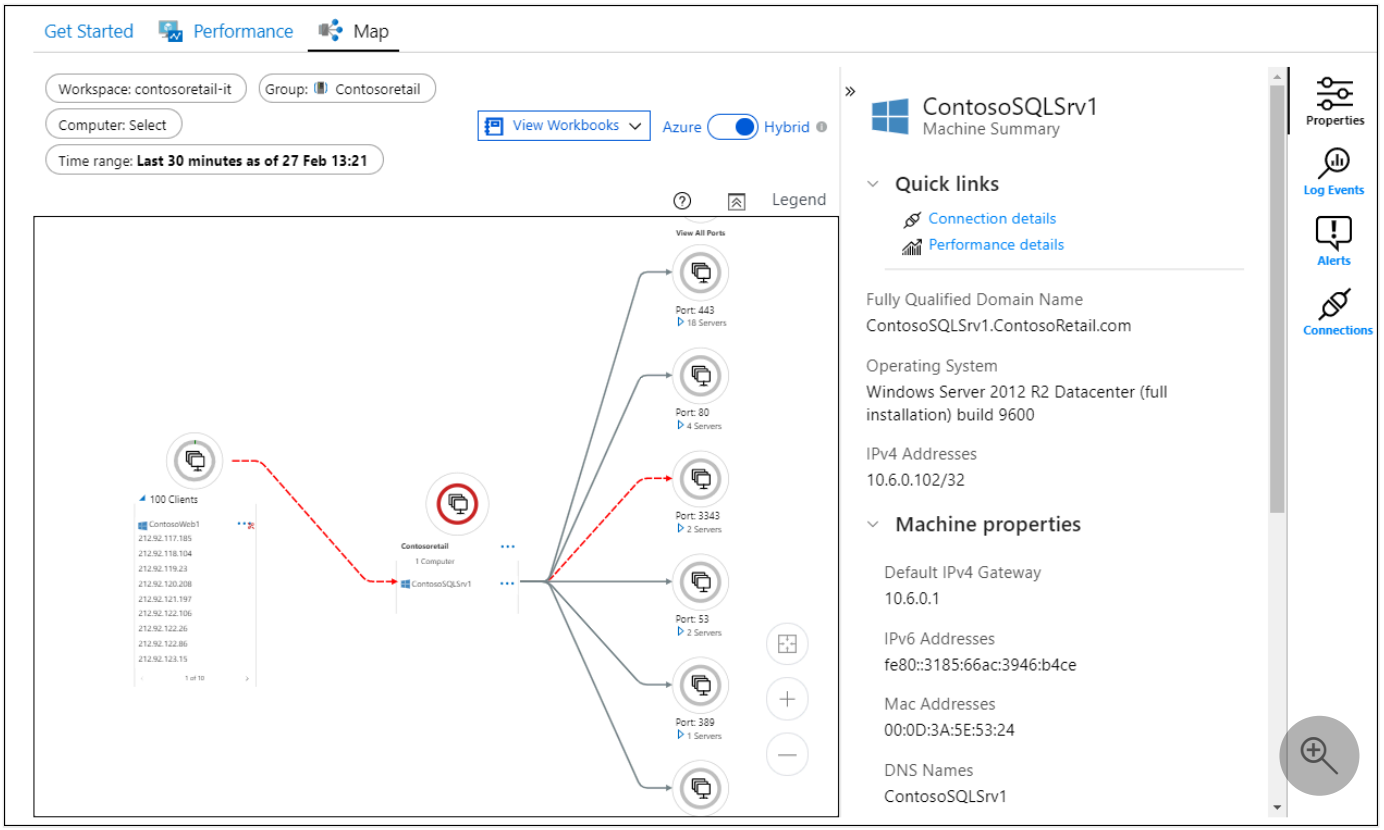
| Scénario | Détails | Collecte de données | Données disponibles | Recommandations |
| --- | --- | --- | --- | --- |
| | Ces données sont importantes pour résoudre les problèmes spécifiques à une application, optimiser l'utilisation des ressources dans les machines virtuelles et garantir des performances optimales pour les charges de travail s'exécutant dans les machines virtuelles. | | | |
| **Données de l'invité de machine virtuelle avancées/personnalisées** | Surveillance des serveurs web, des appliances Linux et des types de données que vous voulez collecter auprès d'une machine virtuelle. | Installez l'agent Azure Monitor sur la machine virtuelle et configurez une règle de collecte de données. | • Journaux d'activité IIS<br>• Interruptions SNMP<br>• Les données écrites dans un fichier texte ou JSON | |

# VM Insights

Insights de machine virtuelle surveille vos machines virtuelles Azure et vos machines virtuelles hybrides dans une même interface. Insights de machine virtuelle offre les avantages suivants, pour la surveillance des machines virtuelles dans Azure Monitor :

- Intégration simplifiée de l’agent Azure Monitor et de Dependency Agent afin de pouvoir superviser le système d’exploitation invité et les charges de travail d’une machine virtuelle.
- Règles de collecte de données prédéfinies qui collectent l’ensemble de données de performances le plus courant.
- Classeurs et graphiques prédéfinis des tendances des performances, qui vous permettent d’analyser les principales métriques de performances du système d’exploitation invité de la machine virtuelle.
- Carte de dépendances qui affiche les processus en cours d’exécution sur chaque machine virtuelle, et les composants interconnectés avec d’autres machines et sources externes.






Pour obtenir un tutoriel sur l'activation de VM Insights pour une machine virtuelle, consultez Activer la supervision avec VM Insights pour la machine virtuelle Azure. Pour obtenir des informations générales sur l'activation des insights et différentes méthodes d'intégration de machines virtuelles, consultez Activer la vue d'ensemble de VM Insights.

Si vous activez VM Insights, l'agent Azure Monitor est installé et commence à envoyer un ensemble prédéfini de données de performances aux journaux Azure Monitor. Vous pouvez créer d'autres règles de collecte de données pour collecter des événements et d'autres données de performances. Pour savoir comment installer l'agent Azure Monitor et créer une règle de collecte de données qui définit les données à collecter, consultez Tutoriel : Collecter les journaux et les métriques d'invité auprès d'une machine virtuelle Azure.

Dans les insights de machine virtuelle, vous pouvez utiliser la fonctionnalité Azure Monitor Map pour afficher les composants d'application s'exécutant dans Azure ou votre environnement. L'extension de machine virtuelle Dependency Agent est disponible pour Windows et Linux.

# Stockage des données

Pour Azure Monitor :

- Les données de métriques sont stockées dans la base de données des métriques Azure Monitor.

- Les données de journal sont stockées dans le magasin de journaux Azure Monitor. Log Analytics est un outil du portail Azure qui peut interroger ce magasin.
- Le journal d'activité Azure est un magasin distinct avec sa propre interface dans le portail Azure.

Vous pouvez choisir d'acheminer les données des métriques et des journaux d'activité vers le magasin des journaux d'activité Azure Monitor. Vous pouvez ensuite utiliser Log Analytics pour interroger les données et les mettre en corrélation avec d'autres données de journal.

De nombreux services peuvent utiliser les paramètres de diagnostic pour envoyer les données des métriques et des journaux vers d'autres emplacements de stockage en dehors d'Azure Monitor. Par exemple, le Stockage Azure, les systèmes partenaires hébergés et les systèmes partenaires non-Azure, en utilisant Event Hubs.

Pour plus d'informations sur la façon dont Azure Monitor stocke les données, consultez Plateforme de données Azure Monitor.

## Métriques de plateforme Azure Monitor

Azure Monitor fournit des métriques de plateforme pour la plupart des services. Ces mesures sont :

- Définies individuellement pour chaque espace de noms.
- Stockées dans la base de données de métriques de série chronologique Azure Monitor.
- Légères et capables de prendre en charge les alertes en quasi-temps réel.
- Utilisées pour suivre les performances d'une ressource au fil du temps.

**Collecte :** Azure Monitor collecte automatiquement les métriques de plateforme. Aucune configuration n'est requise.

**Routage :** vous pouvez également acheminer certaines mesures de plateforme vers Azure Monitor Logs/Log Analytics afin de pouvoir les interroger avec d'autres données de journal. Vérifiez le paramètre d'**exportation DS** pour chaque métrique pour voir si vous pouvez utiliser un paramètre de diagnostic pour router la métrique vers les journaux Azure Monitor / Log Analytics.

- Pour plus d'informations, consultez le paramètre de diagnostic des métriques.
- Pour configurer les paramètres de diagnostic d'un service, consultez Créer des paramètres de diagnostic dans Azure Monitor.

Pour obtenir la liste de toutes les métriques qu'il est possible de collecter pour toutes les ressources dans Azure Monitor, consultez Métriques prises en charge dans Azure Monitor.

Les métriques de plateforme pour les machines virtuelles Azure incluent des *métriques d'hôte* importantes, comme l'utilisation du processeur, du réseau et du disque. Les métriques du système d'exploitation hôte sont liées à la session Hyper-V qui héberge une session du système d'exploitation invité.

Les métriques du *système d'exploitation invité* qui s'exécute dans une machine virtuelle doivent être collectées via un ou plusieurs agents, comme l'agent Azure Monitor, qui s'exécutent sur ou dans le cadre du système d'exploitation invité. Les métriques du système d'exploitation invité comprennent les compteurs de performances, qui effectuent le suivi du pourcentage de processeur et d'utilisation de mémoire du système invité, lesquels sont fréquemment utilisés pour la mise à l'échelle automatique et les alertes. Pour plus d'informations, consultez Métriques du système d'exploitation invité et du système d'exploitation hôte.

Pour plus d'informations sur la façon dont l'agent Azure Monitor collecte les données de surveillance des machines virtuelles, consultez Surveiller les machines virtuelles avec Azure Monitor : Collecter des données.

Pour obtenir la liste des métriques disponibles pour les machines virtuelles, consultez Informations de référence sur les données de surveillance des machines virtuelles.

## Journal des activités Azure

Le journal d'activité contient des événements au niveau de l'abonnement qui suivent les opérations sur chaque ressource Azure qui sont vues comme extérieures à cette ressource, par exemple la création d'une ressource ou le démarrage d'une machine virtuelle.

**Collection :** les événements du journal d'activité sont automatiquement générés et collectés dans un magasin distinct pour être affichés dans le Portail Azure.

**Routage :** vous pouvez envoyer les données de journal d'activité aux journaux Azure Monitor afin de pouvoir les analyser en même temps que d'autres données de journal. D'autres emplacements comme le Stockage Azure, Azure Event Hubs et certains partenaires de monitoring de Microsoft sont également disponibles. Pour plus d'informations sur le routage du journal d'activité, consultez Vue d'ensemble du journal d'activité Azure.

## Règles de collecte des données

Les règles de collecte de données définissent la collecte de données de l'agent Azure Monitor et sont stockées dans votre abonnement Azure. Pour les machines virtuelles, les règles de collecte de données définissent les données à collecter, comme des événements et des compteurs de

performances, et spécifient les emplacements où envoyer les données, comme des espaces de travail Log Analytics. Une machine virtuelle peut être associée à plusieurs règles de collecte de données, et une règle de collecte de données peut être associée à plusieurs machines virtuelles.

## Règle de collecte de données d'Insights de machine virtuelle

Insights de machine virtuelle crée une règle de collecte de données qui collecte des compteurs de performances courants pour le système d'exploitation client et les envoie à la table InsightsMetrics dans l'espace de travail Log Analytics. Pour obtenir la liste des compteurs de performances collectés, consultez Comment interroger les journaux des insights de machine virtuelle. Vous pouvez utiliser cette règle de collecte de données avec d'autres machines virtuelles au lieu de créer une règle de collecte de données pour chaque machine virtuelle.

Vous pouvez également activer la collecte de processus et de dépendances, qui stocke ses données dans les tableaux suivants et active la fonctionnalité Carte des insights de machine virtuelle.

- VMBoundPort : Trafic pour les ports serveur ouverts sur l'ordinateur
- VMComputer : Données d'inventaire pour la machine
- VMConnection : Trafic pour les connexions entrantes et sortantes vers et depuis l'ordinateur
- VMProcess : Processus en cours d'exécution sur la machine

# Analyser les données de surveillance

Il existe de nombreux outils pour analyser les données de surveillance.

## Outils Azure Monitor

Azure Monitor prend en charge les outils de base suivants :

- Metrics Explorer, un outil du portail Azure qui vous permet de voir et d'analyser les métriques des ressources Azure. Pour plus d'informations, consultez Analyser les métriques avec l'Explorateur de métriques Azure Monitor.

- Log Analytics, un outil du portail Azure qui vous permet d'interroger et d'analyser les données de journal en utilisant le langage de requête Kusto (KQL). Pour plus d'informations, voir Bien démarrer avec les requêtes de journal dans Azure Monitor.

- Le journal d'activité, qui a une interface utilisateur dans le portail Azure pour la consultation et les recherches de base. Pour effectuer une analyse plus approfondie, vous devez router

les données vers les journaux Azure Monitor et exécuter des requêtes plus complexes dans Log Analytics.

Les outils qui permettent une visualisation plus complexe sont notamment :

- Les tableaux de bord, qui vous permettent de combiner différentes sortes de données dans un même volet du portail Azure.
- Classeurs, rapports personnalisables que vous pouvez créer dans le portail Azure. Les workbooks peuvent inclure du texte, des métriques et des requêtes de journal.
- Grafana, un outil de plateforme ouvert, parfait pour les tableaux de bord opérationnels. Vous pouvez utiliser Grafana pour créer des tableaux de bord à partir de données de plusieurs sources autres qu'Azure Monitor.
- Power BI, un service d'analyse métier qui fournit des visualisations interactives pour diverses sources de données. Vous pouvez configurer Power BI pour importer automatiquement les données de journal à partir d'Azure Monitor afin de tirer parti de ces visualisations supplémentaires.

## Outils d'exportation Azure Monitor

Vous pouvez extraire des données d'Azure Monitor dans d'autres outils en utilisant les méthodes suivantes :

- **Métriques :** utilisez l'API REST pour les métriques pour extraire les données de métriques de la base de données de métriques Azure Monitor. L'API prend en charge les expressions de filtre pour affiner les données récupérées. Pour plus d'informations, consultez Informations de référence sur l'API REST Azure Monitor.
- **Journaux :** utilisez l'API REST ou les bibliothèques de client associées.
- Une autre option est l'exportation des données d'espace de travail.

Pour bien démarrer avec l'API REST pour Azure Monitor, consultez Procédure pas à pas de l'API REST d'analyse Azure.

# Requêtes Kusto

Vous pouvez analyser les données de surveillance dans les journaux d'activité Azure Monitor ou le magasin Log Analytics en utilisant le langage de requête Kusto (KQL).

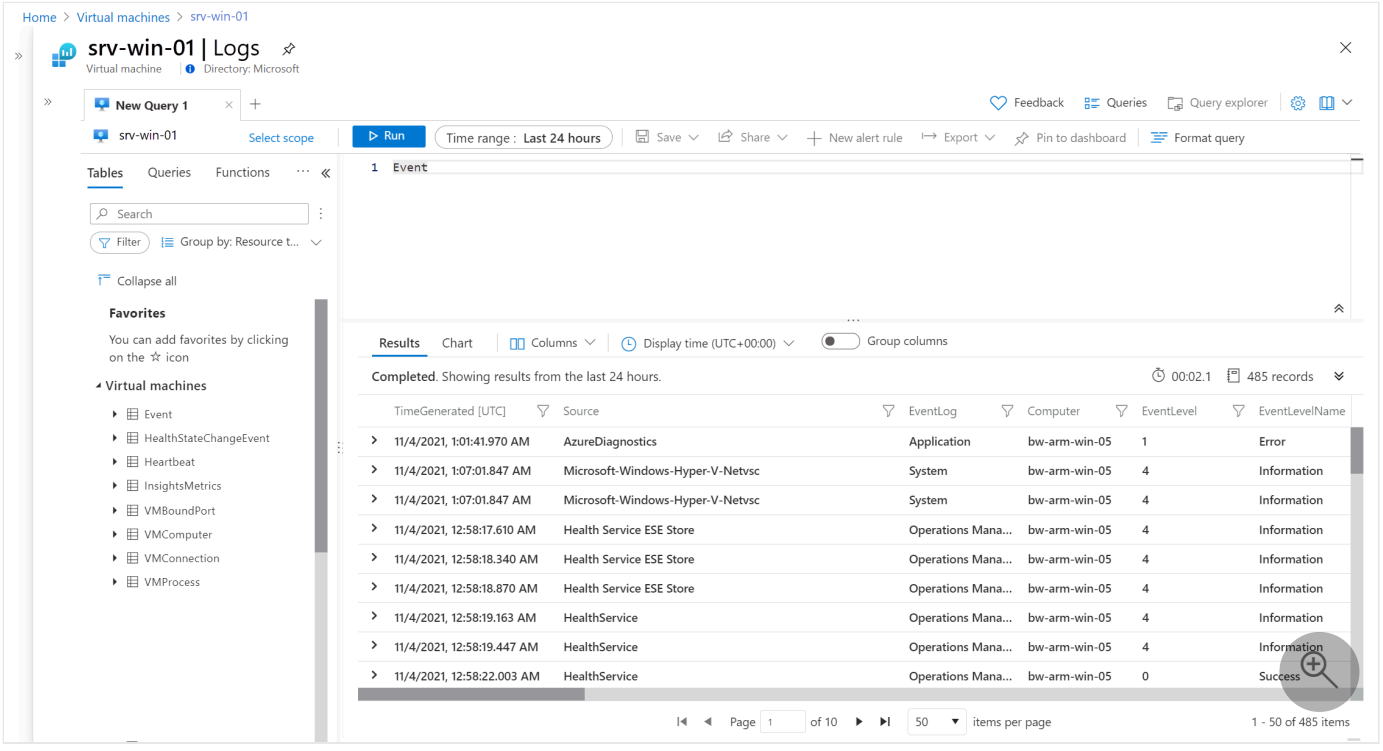
> ⓘ **Important**

Quand vous sélectionnez **Journaux d'activité** dans le menu du service dans le portail, Log Analytics s'ouvre avec l'étendue de requête définie sur le service actuel. Cette étendue signifie que les requêtes de journal ont seulement des données de ce type de ressource. Si vous voulez exécuter une requête qui comprend des données d'autres services Azure, sélectionnez **Journaux** dans le menu **Azure Monitor**. Pour plus d'informations, consultez [Étendue de requête de journal et intervalle de temps dans la fonctionnalité Log Analytics d'Azure Monitor](#).

Pour obtenir la liste des requêtes courantes pour n'importe quel service, consultez l'Interface de requêtes Log Analytics.

Pour analyser les données de journal que vous collectez auprès de vos machines virtuelles, vous pouvez utiliser des requêtes de journal dans Log Analytics. Plusieurs requêtes prédéfinies sont disponibles, et vous pouvez aussi créer vos propres requêtes. Vous pouvez travailler de manière interactive avec les résultats de ces requêtes, les inclure dans un classeur pour les mettre à la disposition d'autres utilisateurs, ou générer des alertes en fonction de leurs résultats.

Pour accéder aux requêtes Kusto prédéfinies pour votre machine virtuelle, sélectionnez **Journaux** dans la section **Surveillance** de la navigation de gauche sur la page du portail Azure de votre machine virtuelle. Dans la page **Journaux**, sélectionnez l'onglet **Requêtes**, puis sélectionnez la requête à exécuter.




# Alertes

Azure Monitor vous alerte de façon proactive quand des conditions spécifiques sont détectées dans vos données de monitoring. Les alertes permettent d'identifier et de résoudre les problèmes affectant votre système avant que vos clients ne les remarquent. Pour plus d'informations, consultez Alertes Azure Monitor.

Il existe de nombreuses sources d'alertes courantes pour les ressources Azure. Pour obtenir des exemples d'alertes courantes pour les ressources Azure, consultez Exemples de requêtes d'alerte de journal. Le site Azure Monitor Baseline Alerts (AMBA) fournit une méthode semi-automatisée de mise en œuvre des alertes, des tableaux de bord et des recommandations concernant les métriques de plateforme. Le site s'applique à un sous-ensemble des services Azure en constante expansion, y compris tous les services qui font partie de la zone d'atterrissage Azure (ALZ).

Le schéma d'alerte commun standardise la consommation de notifications d'alerte pour Azure Monitor. Pour plus d'informations, consultez Schéma d'alerte courant.

## Types d'alertes

Vous pouvez définir une alerte sur n'importe quelle source de données de métrique ou de journal dans la plateforme de données Azure Monitor. Il existe de nombreux types d'alertes différents en fonction des services que vous monitorez et des données de monitoring que vous collectez. Les différents types d'alertes ont divers avantages et inconvénients. Pour plus d'informations, consultez Choisir le bon type d'alerte de monitoring.

La liste suivante décrit les types d'alertes Azure Monitor que vous pouvez créer :

- Les alertes de métrique évaluent les métriques de ressource à intervalles réguliers. Les métriques peuvent être des métriques de plateforme, des métriques personnalisées, des journaux provenant d'Azure Monitor convertis en métriques ou des métriques Application Insights. Les alertes de métriques peuvent également appliquer plusieurs conditions et seuils dynamiques.
- Les alertes de journal permettent aux utilisateurs d'utiliser une requête Log Analytics pour évaluer les journaux de ressource à une fréquence prédéfinie.
- Les alertes de journal d'activité sont déclenchées quand un nouvel événement de journal d'activité correspond à des conditions définies. Les alertes Resource Health et les alertes Service Health sont des alertes de journal d'activité qui concernent l'intégrité de votre service et de vos ressources.

Certains services Azure prennent également en charge les alertes de détection intelligente, les alertes Prometheus ou les règles d'alerte recommandées.

Pour certains services, vous pouvez opérer une surveillance à grande échelle en appliquant la même règle d'alerte de métrique à plusieurs ressources du même type qui existent dans la même région Azure. Les notifications individuelles sont envoyées pour chaque ressource supervisée. Pour connaître les services et clouds Azure pris en charge, consultez Monitorer plusieurs ressources avec une seule règle d'alerte.

Vous pouvez créer une seule règle d'alerte multiressource qui s'applique à toutes les machines virtuelles d'un groupe de ressources ou d'un abonnement particulier dans la même région. Pour obtenir un didacticiel à l'aide de la métrique de disponibilité, consultez Créer une règle d'alerte de disponibilité pour une machine virtuelle Azure (préversion).

## Règles d'alerte recommandées

Pour certains services Azure, vous pouvez activer des règles d'alerte recommandées prêtes à l'emploi.

Le système compile une liste de règles d'alerte recommandées en fonction des éléments suivants :

- La connaissance par le fournisseur de la ressource des signaux et des seuils importants pour la surveillance de la ressource.
- Données qui indiquent ce sur quoi les clients alertent généralement pour cette ressource.

> ⓘ **Remarque**
>
> Les règles d'alerte recommandées sont disponibles pour :
>
> - Machines virtuelles
> - Ressources Azure Kubernetes Service (AKS)
> - Espaces de travail Log Analytics

Les règles d'alerte recommandées pour les machines virtuelles Azure incluent la métrique de disponibilité de machine virtuelle, qui alerte quand une machine virtuelle cesse de s'exécuter.

Pour plus d'informations, consultez Tutoriel : Activer les règles d'alerte recommandées pour une machine virtuelle Azure.

## Règles d'alerte courantes

Pour voir les règles d'alerte courantes du journal des machines virtuelles dans le portail Azure, accédez au volet **Requêtes** dans Log Analytics. Pour **Type de ressource**, entrez **Machines virtuelles** et, pour **Type**, entrez **Alertes**.

Pour obtenir une liste et une explication des règles d'alerte courantes des machines virtuelles, consultez Règles d'alerte courantes.

### Recommandations d'Advisor

Pour certains services, si des conditions critiques ou des changements imminents se produisent durant les opérations relatives aux ressources, une alerte s'affiche dans la page **Vue d'ensemble** du service au sein du portail. Vous trouverez plus d'informations ainsi que les correctifs recommandés pour l'alerte dans **Recommandations Advisor**, sous **Supervision** dans le menu de gauche. Pendant les opérations normales, aucune recommandation Advisor ne s'affiche.

Pour plus d'informations sur Azure Advisor, consultez Vue d'ensemble d'Azure Advisor.

## Autres options de surveillance des machines virtuelles

Les machines virtuelles Azure ont les options de surveillance non-Azure Monitor suivantes :

### Diagnostics de démarrage

Les diagnostics de démarrage sont une fonctionnalité de débogage pour les machines virtuelles Azure qui vous permet de diagnostiquer les échecs de démarrage des machines virtuelles en collectant des informations de journal en série et des captures d'écran d'une machine virtuelle lors du démarrage. Quand vous créez une machine virtuelle dans le portail Azure, les diagnostics de démarrage sont activés par défaut. Pour plus d'informations, consultez Diagnostics de démarrage Azure.

### Résoudre les problèmes de performances VM avec Performance Diagnostics

L'outil Performance Diagnostics permet de résoudre les problèmes de performances sur les machines virtuelles Windows ou Linux en diagnostiquant rapidement les problèmes trouvés sur vos machines et en fournissant des insights sur ces problèmes. Deux modes différents sont pris en charge :

- **Diagnostics continus (préversion)** ce mode collecte des données toutes les cinq secondes et signale des insights actionnables sur l'utilisation élevée des ressources toutes les cinq

minutes.

- **Diagnostics à la demande** ce mode vous aide à résoudre un problème de performances continu avec des données, des insights et des recommandations plus approfondis en fonction des données collectées à un moment donné.

Pour plus d'informations, consultez Résoudre les problèmes de performances sur les machines virtuelles Azure à l'aide des Diagnostics de performances.

## Contenu connexe

- Pour obtenir les informations de référence sur les métriques, les journaux et d'autres valeurs importantes pour les machines virtuelles, consultez Informations de référence sur les données de surveillance des machines virtuelles.
- Pour obtenir des informations générales sur la surveillance des ressources Azure, consultez Surveiller des ressources Azure avec Azure Monitor.
- Pour de l'aide basée sur les cinq piliers d'Azure Well-Architected Framework, consultez Meilleures pratiques pour la surveillance des machines virtuelles dans Azure Monitor.
- Pour bien démarrer avec Insights de machine virtuelle, consultez Vue d'ensemble d'Insights de machine virtuelle.
- Pour savoir comment collecter et analyser les métriques et les journaux d'hôte et de client de machine virtuelle, consultez le cours de formation Surveiller vos machines virtuelles Azure avec Azure Monitor.
- Pour obtenir un guide complet sur la surveillance des machines virtuelles Azure et des machines virtuelles hybrides, consultez le Guide de surveillance du déploiement de machines virtuelles.

---

Dernière mise à jour : 17/06/2026

# Options de sauvegarde et de restauration pour les machines virtuelles dans Azure

**S'applique à :** ✔ Machines virtuelles Linux ✔ Machines virtuelles Windows ✔ Ensembles de mise à l'échelle flexible

Vous pouvez protéger vos données en effectuant des sauvegardes à intervalles réguliers. Il existe plusieurs options de sauvegarde disponibles pour les machines virtuelles, en fonction de votre cas d'utilisation.

## Sauvegarde Azure

Vous utiliserez Sauvegarde Azure pour la plupart des cas d'usage impliquant des opérations de sauvegarde sur des machines virtuelles Azure exécutant des charges de travail de production. La sauvegarde Azure prend en charge des sauvegardes cohérentes avec les applications pour les machines virtuelles Linux et Windows. Azure Backup crée des points de récupération stockés dans des coffres de récupération géoredondants. Quand vous effectuez une restauration à partir d'un point de récupération, vous pouvez restaurer une machine virtuelle entière ou des fichiers spécifiques.

Pour une introduction simple et pratique de Sauvegarde Azure pour les machines virtuelles Azure, consultez le démarrage rapide de Sauvegarde Azure.

Pour plus d'informations sur le fonctionnement de la sauvegarde Azure, consultez Planification de votre infrastructure de sauvegarde de machines virtuelles dans Azure.

## Azure Site Recovery

Azure Site Recovery protège vos machines virtuelles en cas de catastrophe majeure. Ces scénarios peuvent inclure des interruptions de service généralisées ou des pannes régionales causées par des catastrophes naturelles. Vous pouvez configurer Azure Site Recovery pour vos machines virtuelles afin de pouvoir récupérer vos applications en quelques minutes d'un simple clic. Vous pouvez répliquer vers une région Azure de votre choix, car la récupération n'est pas limitée aux régions appariées.

Vous pouvez effectuer des exercices de récupération d'urgence avec des tests de basculement à la demande, sans affecter vos charges de travail de production ni la réplication continue. Créez

des plans de reprise pour orchestrer le basculement et le retour à l'état initial de l'intégralité de l'application fonctionnant sur plusieurs machines virtuelles. La fonctionnalité du plan de récupération est intégrée à des runbooks Azure Automation.

Vous pouvez commencer par répliquer vos machines virtuelles.

## Captures instantanées gérées

Dans les environnements de développement et de test, les instantanés constituent une option simple et rapide pour sauvegarder les machines virtuelles qui utilisent des disques managés. Un instantané managé est une copie complète, en lecture seule, d'un disque managé. Les instantanés existent indépendamment de leurs disques d'origine.

Les instantanés peuvent être utilisés pour créer des disques managés lorsqu'une machine virtuelle est régénérée. Ils sont facturés en fonction de la partie utilisée du disque. Par exemple, si vous créez une capture instantanée d'un disque géré avec une capacité approvisionnée de 64 Go et une taille des données utilisées réelle de 10 Go, la capture instantanée sera facturée uniquement pour la taille des données utilisées de 10 Go.

Pour plus d'informations sur la création de captures instantanées, consultez :

- Créer une copie de VHD stocké en tant que disque managé

## Points de restauration de machine virtuelle

À ce stade, vous pouvez utiliser les API REST d'Azure pour sauvegarder et restaurer vos machines virtuelles. Cette approche est le plus souvent utilisée par les éditeurs de logiciels indépendants ou les organisations ayant un nombre relativement faible de machines virtuelles à gérer.

Vous pouvez utiliser l'API pour créer une collection de points de restauration de machine virtuelle. La collection de points de restauration proprement dite contient des points de restauration individuels pour des machines virtuelles spécifiques. Chaque point de restauration stocke la configuration d'une machine virtuelle et un instantané pour chaque disque managé attaché. Pour économiser de l'espace et de l'argent, vous pouvez exclure des disques de vos points de restauration VM.

Une fois créés, les points de restauration de machine virtuelle peuvent être utilisés pour restaurer des disques individuels. Pour restaurer une machine virtuelle, restaurez tous les disques pertinents et attachez-les à une nouvelle machine virtuelle.

En savoir plus sur l'utilisation des points de restauration de machine virtuelle et sur l'API de collecte des points de restauration.

## Étapes suivantes

Vous pouvez tester Sauvegarde Azure en suivant le démarrage rapide de Sauvegarde Azure.

Vous pouvez également planifier et implémenter la fiabilité de configuration de votre machine virtuelle. Pour plus d'informations, consultez Fiabilité des machines virtuelles.

---

Dernière mise à jour : 02/04/2026

# Utiliser des outils d’automatisation de l’infrastructure avec des machines virtuelles dans Azure

**S’applique à :** ✔ Machines virtuelles Linux ✔ Machines virtuelles Windows ✔ Groupes d'échelle flexibles ✔ Groupes d'échelle uniformes

Pour créer et gérer des machines virtuelles Azure de manière cohérente à grande échelle, une certaine forme d’automatisation est généralement souhaitée. Il existe de nombreux outils et solutions qui vous permettent d’automatiser le cycle de vie complet du déploiement et de la gestion de l’infrastructure Azure. Cet article présente certains des outils d’automatisation de l’infrastructure que vous pouvez utiliser dans Azure. Ces outils s’intègrent généralement à l’une des approches suivantes :

- Automatiser la configuration des machines virtuelles
  - Les outils incluent Ansible, Chef, Puppet, Bicep et le modèle Azure Resource Manager.
  - Les outils spécifiques à la personnalisation de la machine virtuelle incluent cloud-init pour les machines virtuelles Linux, PowerShell Desired State Configuration (DSC) et l’extension de script personnalisé Azure pour toutes les machines virtuelles Azure.
- Automatiser la gestion de l’infrastructure
  - Les outils incluent Packer pour automatiser les builds d’images de machine virtuelle personnalisées et Terraform pour automatiser le processus de génération d’infrastructure.
  - Azure Automation peut effectuer des actions sur votre infrastructure Azure et locale.
- Automatiser le déploiement et la remise des applications
  - Les exemples incluent Azure DevOps Services et Jenkins.

## Terraform

Terraform est un outil d’automatisation qui vous permet de définir et de créer une infrastructure Azure entière avec un seul langage de format de modèle , le langage HCL (HashiCorp Configuration Language). Avec Terraform, vous définissez des modèles qui automatisent le processus pour créer des ressources réseau, de stockage et de machine virtuelle pour une solution d’application donnée. Vous pouvez utiliser vos modèles Terraform existants

pour d'autres plateformes avec Azure pour garantir la cohérence et simplifier le déploiement de l'infrastructure sans avoir à effectuer de conversion en modèle Azure Resource Manager.

Découvrez comment :

- Installez et configurez Terraform avec Azure.
- Créez une infrastructure Azure avec Terraform.

## Azure Automation

Azure Automation utilise des runbooks pour traiter un ensemble de tâches sur les machines virtuelles que vous ciblez. Azure Automation est utilisé pour gérer les machines virtuelles existantes plutôt que pour créer une infrastructure. Azure Automation peut s'exécuter sur des machines virtuelles Linux et Windows, ainsi que sur des machines virtuelles ou physiques locales avec un Runbook Worker hybride. Les runbooks peuvent être stockés dans un référentiel de contrôle de code source, tel que GitHub. Ces runbooks peuvent ensuite être exécutés manuellement ou selon un calendrier défini.

Azure Automation fournit également un service DSC (Desired State Configuration) qui vous permet de créer des définitions pour la façon dont un ensemble donné de machines virtuelles doit être configuré. DSC garantit ensuite que la configuration requise est appliquée et que la machine virtuelle reste cohérente. Azure Automation DSC s'exécute sur des machines Windows et Linux.

Découvrez comment :

- Créer un runbook PowerShell.
- Utilisez Hybrid Runbook Worker pour gérer les ressources locales.
- Utilisez Azure Automation DSC.

## Azure DevOps Services

Azure DevOps Services est une suite d'outils qui vous aident à partager et suivre du code, à utiliser des builds automatisées et à créer un pipeline d'intégration et de développement continu (CI/CD). Azure DevOps Services s'intègre à Visual Studio et à d'autres éditeurs pour simplifier l'utilisation. Azure DevOps Services peut également créer et configurer des machines virtuelles Azure, puis déployer du code sur ces machines virtuelles.

Pour en savoir plus :

- Azure DevOps Services.

# Modèle Azure Resource Manager

Azure Resource Manager est le service de déploiement et de gestion pour Azure. Il fournit une couche de gestion qui vous permet de créer, mettre à jour et supprimer des ressources dans votre abonnement Azure. Vous utilisez des fonctionnalités de gestion, telles que le contrôle d'accès, les verrous et les étiquettes, pour sécuriser et organiser vos ressources après le déploiement.

Découvrez comment :

- Déployez des machines virtuelles Spot à l'aide d'un modèle Resource Manager.
- Créez une machine virtuelle Windows à partir d'un modèle Resource Manager.
- Téléchargez le modèle pour une machine virtuelle.
- Créez un modèle Azure Image Builder.

# Bicep

Bicep est un langage spécifique à un domaine (DSL) qui utilise la syntaxe déclarative pour déployer des ressources Azure. Dans un fichier Bicep, vous définissez l'infrastructure que vous voulez déployer sur Azure, puis utilisez ce fichier tout au long du cycle de vie de développement pour déployer votre infrastructure à plusieurs reprises. Vos ressources sont déployées de manière cohérente.

Commencez par le démarrage rapide.

# Cloud-Init

Cloud-init est une méthode largement utilisée pour personnaliser une machine virtuelle Linux lors de son premier démarrage. Vous pouvez utiliser cloud-init pour installer des packages et écrire des fichiers, ou encore pour configurer des utilisateurs ou des paramètres de sécurité. Étant donné que cloud-init est appelé pendant le processus de démarrage initial, il n'existe aucune étape supplémentaire ni aucun agent requis pour appliquer votre configuration. Pour plus d'informations sur la mise en forme correcte de vos `#cloud-config` fichiers, consultez le site de documentation cloud-init. Les fichiers `#cloud-config` sont des fichiers texte encodés en base64.

Cloud-init fonctionne aussi sur les différentes distributions. Par exemple, vous n'utilisez pas **apt-get install** ou **yum install** pour installer un package. Au lieu de cela, vous pouvez définir une liste

des packages à installer, après quoi cloud-init se charge d'utiliser automatiquement l'outil de gestion de package natif correspondant à la distribution que vous sélectionnez.

Nous travaillons activement avec nos partenaires de distribution Linux afin de mettre des images compatibles cloud-init à disposition sur Place de marché Azure. Ces images permettent à vos déploiements et configurations cloud-init de fonctionner de manière fluide avec les machines virtuelles et les ensembles de machines virtuelles. En savoir plus sur cloud-init sur Azure :

- Prise en charge de cloud-init pour les machines virtuelles Linux dans Azure
- Essayez un didacticiel sur la configuration automatisée des machines virtuelles à l'aide de cloud-init.

## DSC PowerShell

PowerShell Desired State Configuration (DSC) est une plateforme de gestion pour définir la configuration des machines cibles. DSC peut également être utilisé sur Linux via le serveur OMI (Open Management Infrastructure).

Les configurations DSC définissent ce qu'il faut installer sur un ordinateur et comment configurer l'hôte. Un moteur Local Configuration Manager (LCM) s'exécute sur chaque nœud cible qui traite les actions demandées en fonction des configurations push. Un serveur collecteur est un service web qui s'exécute sur un hôte central pour stocker les configurations DSC et les ressources associées. Le serveur collecteur communique avec le moteur LCM sur chaque hôte cible pour fournir les configurations requises et signaler la conformité.

Découvrez comment :

- Créez une configuration DSC de base.
- Configurez un serveur collecteur DSC.
- Utilisez DSC pour Linux.

## Extension de script personnalisé Azure

L'extension de script personnalisé Azure pour Linux ou Windows télécharge et exécute des scripts sur des machines virtuelles Azure. Vous pouvez utiliser l'extension lorsque vous créez une machine virtuelle ou à tout moment après l'utilisation de la machine virtuelle.

Les scripts peuvent être téléchargés à partir du stockage Azure ou de n'importe quel emplacement public tel qu'un dépôt GitHub. Avec l'extension de script personnalisé, vous pouvez écrire des scripts dans n'importe quel langage qui s'exécute sur la machine virtuelle source. Ces

scripts peuvent être utilisés pour installer des applications ou configurer la machine virtuelle comme vous le souhaitez. Pour sécuriser les informations d'identification, des informations sensibles telles que des mots de passe peuvent être stockées dans une configuration protégée. Ces informations d'identification sont uniquement déchiffrées à l'intérieur de la machine virtuelle.

Découvrez comment :

- Créez une machine virtuelle Linux avec Azure CLI et utilisez l'extension de script personnalisé.
- Créez une machine virtuelle Windows avec Azure PowerShell et utilisez l'extension de script personnalisé.

## Ansible

Ansible est un moteur d'automatisation pour la gestion de la configuration, la création de machines virtuelles ou le déploiement d'applications. Ansible utilise un modèle sans agent, généralement avec des clés SSH, pour authentifier et gérer les machines cibles. Les tâches de configuration sont définies dans les playbooks, avec plusieurs modules Ansible disponibles pour effectuer des tâches spécifiques. Pour plus d'informations, consultez Le fonctionnement d'Ansible.

Découvrez comment :

- Installez et configurez Ansible sur Linux pour une utilisation avec Azure.
- Créez une machine virtuelle Linux.
- Gérer une machine virtuelle Linux.

## Chef

Chef est une plateforme d'automatisation qui permet de définir la façon dont votre infrastructure est configurée, déployée et gérée. Certains composants incluent Chef Habitat pour l'automatisation du cycle de vie des applications plutôt que l'infrastructure, et Chef InSpec qui permet d'automatiser la conformité aux exigences de sécurité et de stratégie. Les clients Chef sont installés sur des machines cibles, avec un ou plusieurs serveurs Chef centraux qui stockent et gèrent les configurations. Pour plus d'informations, consultez Une vue d'ensemble de Chef.

Découvrez comment :

- Déployez Chef Automate à partir de la Place de marché Azure.
- Installez Chef sur Windows et créez des machines virtuelles Azure.

# Puppet

Puppet est une plateforme d'automatisation prête pour l'entreprise qui gère le processus de distribution et de déploiement des applications. Les agents sont installés sur des machines cibles pour permettre à Puppet Master d'exécuter des manifestes qui définissent la configuration souhaitée de l'infrastructure et des machines virtuelles Azure. Puppet peut s'intégrer à d'autres solutions telles que Jenkins et GitHub pour un workflow devops amélioré. Pour plus d'informations, consultez Fonctionnement de Puppet.

Découvrez comment :

- Déployer Puppet.

# Emballeur

Packer automatise le processus de génération lorsque vous créez une image de machine virtuelle personnalisée dans Azure. Vous utilisez Packer pour définir le système d'exploitation et exécuter des scripts post-configuration qui personnalisent la machine virtuelle pour vos besoins spécifiques. Une fois configurée, la machine virtuelle est ensuite capturée en tant qu'image de disque managé. Packer automatise le processus pour créer la machine virtuelle source, le réseau et les ressources de stockage, exécuter des scripts de configuration, puis créer l'image de machine virtuelle.

Découvrez comment :

- Utilisez Packer pour créer une image de machine virtuelle Linux dans Azure.
- Utilisez Packer pour créer une image de machine virtuelle Windows dans Azure.

# Jenkins

Jenkins est un serveur d'intégration continu qui permet de déployer et de tester des applications, et de créer des pipelines automatisés pour la remise de code. Il existe des centaines de plug-ins pour étendre la plateforme Jenkins principale, et vous pouvez également intégrer de nombreux autres produits et solutions via des webhooks. Vous pouvez installer manuellement Jenkins sur une machine virtuelle Azure, exécuter Jenkins à partir d'un conteneur Docker ou utiliser une image prédéfini de la Place de marché Azure.

Découvrez comment :

- Créez une infrastructure de développement sur une machine virtuelle Linux dans Azure avec Jenkins, GitHub et Docker.

## Étapes suivantes

Il existe de nombreuses options différentes pour utiliser des outils d'automatisation de l'infrastructure dans Azure. Vous avez la liberté d'utiliser la solution qui convient le mieux à vos besoins et à votre environnement. Pour commencer et essayer certains des outils intégrés à Azure, découvrez comment automatiser la personnalisation d'une machine virtuelle Linux ou Windows .

---

Dernière mise à jour : 07/05/2025

# Vue d’ensemble des disques managés Azure

**S’applique aux :** ✔ Machines virtuelles Linux ✔ Machines virtuelles Windows ✔ Groupes de mise à l'échelle flexibles ✔ Groupes de mise à l'échelle uniformes

Les disques managés Azure sont des volumes de stockage de niveau bloc gérés par Azure et utilisés avec des machines virtuelles Azure. Les disques managés sont comme les disques physiques sur un serveur local, mais ils sont virtualisés. Avec les disques managés, vous devez uniquement spécifier le type de disque et la taille du disque, puis approvisionner le disque. Une fois que vous avez approvisionné le disque, Azure s’occupe du reste.

Il existe cinq types de disques managés : Disques Ultra, disques SSD Premium (SSD) v2, SSD Premium, SSD Standard et disques durs Standard (HDD). Pour en savoir plus sur chaque type de disque et décider qui correspond à vos besoins, consultez les types de disques managés Azure.

Une alternative consiste à utiliser Azure Elastic SAN comme stockage pour votre machine virtuelle. Avec Elastic SAN, vous pouvez consolider le stockage de toutes vos charges de travail dans un seul back-end de stockage. Le san élastique peut être plus rentable si vous avez de nombreuses charges de travail à grande échelle, des charges de travail intensives en E/S et des bases de données de niveau supérieur. Pour en savoir plus, consultez Qu’est-ce qu’Azure Elastic SAN ?.

## Durabilité et disponibilité des disques managés Azure

Les disques managés sont conçus pour la disponibilité de 99,999%. Pour atteindre cette disponibilité, les disques managés fournissent trois réplicas de vos données. Si une ou deux copies rencontrent des difficultés, les copies restantes garantissent la persistance de vos données et une tolérance élevée aux défaillances.

Cette architecture permet à Azure de fournir de façon cohérente une durabilité élevée pour les disques IaaS (infrastructure as a service), avec un taux de défaillance annuel de 0 %. Les disques de stockage localement redondant (LRS) fournissent au moins 99,999999999 % (11 9) de durabilité sur une année. Les disques de stockage redondant interzone (ZRS) fournissent au moins 99,9999999999 % (12 9) de durabilité sur une année.

## Faire évoluer les déploiements de machines virtuelles Azure avec des disques managés

Avec les disques managés, vous pouvez créer jusqu'à 50 000 disques de chaque type de disque dans un abonnement par région. Vous pouvez ensuite créer des milliers de machines virtuelles dans un même abonnement.

Les disques managés augmentent la scalabilité des groupes de machines virtuelles identiques. Vous pouvez créer jusqu'à 1000 machines virtuelles dans un groupe de machines virtuelles identiques à l'aide d'une image de la Place de marché Azure ou d'une image Azure Compute Gallery avec des disques managés.

# Isolation des pannes des disques managés Azure

## Isoler les disques managés à l'aide de groupes à haute disponibilité

Les disques managés sont intégrés aux groupes à haute disponibilité afin d'aider à garantir que les disques des machines virtuelles d'un groupe à haute disponibilité sont suffisamment isolés les uns des autres pour éviter un point de défaillance unique.

Les disques sont automatiquement placés dans différentes unités d'échelle de stockage (horodatages). Si un horodatage est mis en échec en raison d'une défaillance matérielle ou logicielle, seules les instances de machine virtuelle possédant des disques sur ces horodatages sont mises en échec.

Par exemple, supposons que vous disposez d'une application s'exécutant sur cinq machines virtuelles qui se trouvent dans un groupe à haute disponibilité. Les disques de ces machines virtuelles ne sont pas tous stockés dans la même unité d'échelle. Par conséquent, si une unité d'échelle tombe en panne, les autres instances de l'application continuent à s'exécuter.

## Protéger les disques managés avec des zones de disponibilité

Les disques managés prennent en charge les zones de disponibilité, qui aident à protéger vos applications contre les pannes du centre de données. Les Zones de disponibilité sont des emplacements physiques uniques au sein d'une région Azure. Chaque zone est composée d'un ou de plusieurs centres de données équipés d'une alimentation, d'un système de refroidissement et d'un réseau indépendants. Pour garantir la résilience, un minimum de trois zones distinctes sont activées dans toutes les régions.

Pour plus d'informations sur le contrat de niveau de service (SLA) en matière de durée de bon fonctionnement des machines virtuelles avec les zones de disponibilité, consultez la page relative aux contrats SLA Azure.

# Options de performance des disques managés Azure

Les demandes et les besoins de votre charge de travail peuvent changer au fil du temps, soit en raison d'une forte demande pendant un congé, de rafales soudaines de trafic, soit d'un scale-up pour répondre aux besoins des clients. Les disques managés Azure disposent de plusieurs fonctionnalités qui vous permettent d'améliorer leurs performances et de répondre aux besoins changeants de vos charges de travail. Différents types de disques offrent différentes fonctionnalités, certains types de disques ont des fonctionnalités que vous pouvez utiliser pour garantir que leurs performances changent automatiquement pour répondre aux demandes changeantes de votre charge de travail, d'autres nécessitent un ajustement manuel, et d'autres types de disques ne peuvent pas faire non plus.

Pour en savoir plus sur les options dont dispose chaque type de disque, consultez Vue d'ensemble des options permettant d'améliorer les performances des disques managés Azure

# Options de sauvegarde et de reprise d'activité après sinistre pour les disques managés Azure

Les disques managés prennent en charge plusieurs options de sauvegarde et de récupération d'urgence. Ces options incluent des options de redondance intégrées (stockage localement redondant et stockage redondant interzone), Sauvegarde Azure, captures instantanées de disque managé, points de restauration et Azure Site Recovery. La configuration idéale des options de sauvegarde et de récupération d'urgence pour vos besoins peut varier. Pour déterminer ce qui convient le mieux à vos besoins, consultez Sauvegarde et récupération d'urgence pour les disques managés Azure.

## Captures instantanées de disque managé

La capture instantanée d'un disque managé est une copie en lecture seule et cohérente en cas d'incident d'un disque managé, qui est stockée comme disque managé standard par défaut. Avec des captures instantanées, vous pouvez sauvegarder vos disques managés à tout moment dans le temps. Ces captures instantanées existent indépendamment du disque source, et vous pouvez les utiliser pour créer des disques managés.

Pour savoir comment créer des instantanés de disque managé, consultez Créer un instantané d'un disque dur virtuel.

## Images managées pour les machines virtuelles Azure

Les disques managés prennent en charge la création d'images personnalisées managées. Vous pouvez créer une image à partir de votre disque dur virtuel (VHD) personnalisé dans un compte de stockage ou directement à partir d'une machine virtuelle généralisée (par le biais de Sysprep). L'image contient tous les disques managés associés à une machine virtuelle, y compris les disques de données et les disques du système d'exploitation. Une image personnalisée managée vous permet de créer des centaines de machines virtuelles sans avoir à copier ou à gérer des comptes de stockage.

Pour plus d'informations sur la création d'images, consultez Créer une image managée héritée d'une machine virtuelle généralisée dans Azure.

## Comparer les images managées et les instantanés de disque managé

Les images managées et les captures instantanées de disque managé diffèrent dans leur source, leur étendue et leur utilisation prévue :

Agrandir le tableau

| Caractéristique | Image gérée | Instantané de disque managé |
|---|---|---|
| Source | Une machine virtuelle généralisée que vous avez désallouée | Copie instantanée d'un disque géré |
| Scope | Inclut tous les disques managés attachés à la machine virtuelle, y compris le système d'exploitation et les disques de données | Contient une copie d'un disque managé |
| Usage prévu | Créer des machines virtuelles à partir d'une image réutilisable | Sauvegarder un disque ou créer un disque managé |
| Comportement sur plusieurs disques | Capture les disques attachés à la machine virtuelle généralisée dans une seule image | Ne coordonne pas les captures instantanées entre plusieurs disques, il ne convient donc pas aux scénarios nécessitant des copies coordonnées, comme l'agrégation par bandes de disques |

Si une machine virtuelle ne possède qu'un disque de système d'exploitation et qu'aucun disque de données n'est disponible, vous pouvez créer une machine virtuelle à partir d'une image de cette machine virtuelle ou d'un instantané du disque du système d'exploitation.

# Télécharger des VHD et des VHDX vers des disques managés Azure

Vous pouvez réduire les coûts en chargeant directement les données sur des disques managés, sans les attacher à des machines virtuelles. Avec le chargement direct, vous pouvez charger des VHD d'une taille maximale de 32 Tio. Pour savoir comment télécharger votre VHD sur Azure, consultez les articles Azure CLI ou Azure PowerShell.

# Sécurité des disques gérés Azure

## Contrôler l'accès aux importations et exportations de disques managés

Vous avez plusieurs options pour protéger vos disques managés contre l'importation ou l'exportation. Vous pouvez créer un rôle de contrôle d'accès en fonction du rôle Azure personnalisé (RBAC) avec un jeu d'autorisations limité, vous pouvez utiliser l'ID Microsoft Entra, Private Links, Azure Policy ou configurer le `NetworkAccessPolicy` paramètre sur vos ressources de disque. Pour plus d'informations, consultez Restreindre les disques gérés pour qu'ils ne soient pas importés ou exportés.

## Options de chiffrement des disques managés Azure

Plusieurs types de chiffrement sont disponibles pour vos disques managés, notamment Server-Side Encryption (SSE), Azure Disk Encryption (ADE), le chiffrement sur l'hôte et le chiffrement de disque confidentiel. Vous pouvez utiliser des clés gérées par la plateforme ou des clés gérées par le client avec ces options de chiffrement. Pour en savoir plus sur vos options de chiffrement, consultez Vue d'ensemble des options de chiffrement de disque managé

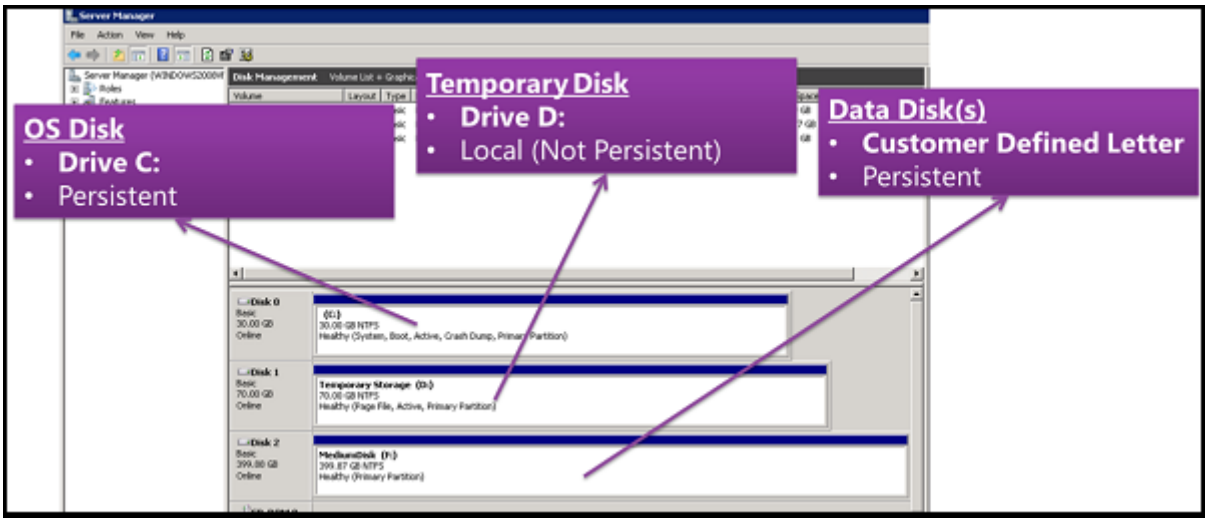
# Partager des disques managés sur des machines virtuelles Azure

Pour une utilisation avec des applications de cluster, vous pouvez attacher un disque managé individuel à plusieurs machines virtuelles simultanément, ce qui vous permet de déployer des applications en cluster nouvelles ou de migrer des applications en cluster existantes vers Azure. Cette configuration nécessite un gestionnaire de cluster, tel que Windows Server Failover Cluster (WSFC) ou Pacemaker, qui gère la communication entre les nœuds du cluster et le verrouillage d'écriture. Pour en savoir plus sur cette configuration, consultez Partager un disque managé Azure.

# rôles de disque de machine virtuelle Azure

Il existe trois rôles de disque principaux dans Azure : le disque de système d'exploitation, le disque de données et le disque temporaire. Ces rôles sont mappés à des disques qui sont attachés à votre machine virtuelle.

Les performances de chaque rôle de disque fonctionnent différemment. Pour en savoir plus sur le fonctionnement des performances pour chaque rôle, consultez allocation de disque et performances.




## Disque de système d'exploitation

À chaque machine virtuelle est attaché un disque de système d'exploitation. Ce disque a un système d'exploitation préinstallé, que vous avez sélectionné lors de la création de la machine virtuelle. Ce disque contient le volume de démarrage.

> ⓘ **Remarque**
>
> Le 8 septembre 2028, la possibilité d'utiliser des disques durs Standard en tant que disques de système d'exploitation sera retirée. Pour plus d'informations, consultez Migrer vos disques de système d'exploitation HDD Standard d'après le 8 septembre 2028.

En règle générale, vous devez stocker uniquement vos informations de système d'exploitation sur le disque du système d'exploitation. Le disque de données est l'endroit où vous devez stocker toutes les applications et toutes les données. Si le coût est un problème, vous pouvez utiliser le disque du système d'exploitation au lieu de créer un disque de données.

Le disque de système d'exploitation a une capacité maximale de 4 095 gibioctets (Gio). Cependant, de nombreux systèmes d'exploitation sont partitionnés avec des enregistrements de démarrage principaux (MBR) par défaut. Un MBR limite la taille utilisable à 2 To. Si vous avez besoin de plus de 2 Tio, créez et attachez des disques de données et utilisez-les pour le stockage des données. Si vous devez stocker des données sur le disque du système d'exploitation et que vous avez besoin de plus d'espace, convertissez-le en table de partitionnement GUID (GPT). Pour en savoir plus sur les différences entre un MBR et une GPT sur les déploiements Windows, consultez la FAQ sur Windows et GPT.

Sur les machines virtuelles Windows Azure, le lecteur C est votre disque de système d'exploitation, et il correspond à un stockage persistant, sauf si vous utilisez des disques de système d'exploitation éphémères.

## Disque de données

Un disque de données est un disque managé attaché à une machine virtuelle pour stocker des données d'application ou d'autres données. Les disques de données sont enregistrés en tant que disques SCSI et sont nommés avec la lettre de votre choix. La taille et le type de la machine virtuelle déterminent le nombre de disques de données que vous pouvez attacher à la machine virtuelle et les types de disques que vous pouvez utiliser avec la machine virtuelle.

En règle générale, vous devez utiliser des disques de données pour stocker vos applications et vos données, au lieu de les stocker sur un disque de système d'exploitation. Le stockage des applications et des données sur des disques de données plutôt que sur des disques de système d'exploitation offre les avantages suivants :

- Amélioration de la sauvegarde et de la récupération d'urgence
- Augmentation de la flexibilité et de la scalabilité
- Isolation des performances
- Maintenance plus facile
- Amélioration de la sécurité et du contrôle d'accès

Pour plus d'informations sur ces avantages, consultez Pourquoi dois-je utiliser le disque de données pour stocker des applications et des données au lieu du disque du système d'exploitation ?.

## Disque temporaire

La plupart des machines virtuelles contiennent un disque temporaire qui n'est pas un disque managé. Le disque temporaire fournit un stockage à court terme pour les applications et les

processus. Il est destiné à stocker uniquement des données telles que des fichiers de pagination, des fichiers d'échange ou des fichiers tempdb SQL Server.

Les données présentes sur le disque temporaire peuvent être perdues lors d'un événement de maintenance, quand vous redéployez une machine virtuelle ou quand vous arrêtez la machine virtuelle. Lors d'un redémarrage standard réussi de la machine virtuelle, les données présentes sur le disque temporaire sont conservées. Pour plus d'informations sur les machines virtuelles sans disques temporaires, consultez Tailles de machine virtuelle Azure sans disque temporaire local.

Sur les machines virtuelles Linux Azure, le disque temporaire est généralement */dev/disk/azure/resource*. Sur les machines virtuelles Windows, le disque temporaire est par défaut le lecteur D. Le disque temporaire n'est pas chiffré, sauf si :

- Vous utilisez une machine virtuelle Azure en version 5 ou ultérieure (telle que Dsv5 ou Dsv6). Les machines virtuelles Azure de version 5 et ultérieure chiffrent automatiquement leurs disques temporaires et (s'ils sont utilisés) leurs disques de système d'exploitation éphémères avec le chiffrement au repos.
- Pour le chiffrement côté serveur, vous activez le chiffrement sur l'hôte.
- Pour Azure Disk Encryption, vous définissez le paramètre `VolumeType` sur All sur Windows ou EncryptFormatAll sur Linux.

## Contenu de disque managé associé Azure

- En savoir plus sur les types de disques individuels qu'Azure propose, quel type correspond à vos besoins et à leurs objectifs de performances, consultez Sélectionner un type de disque pour les machines virtuelles IaaS
- En savoir plus sur le fonctionnement des performances des machines virtuelles et des disques
- Découvrez les meilleures pratiques pour atteindre la haute disponibilité avec des machines virtuelles Azure et des disques managés
- En savoir plus sur la facturation des disques managés, consultez Présentation de la facturation du stockage sur disque Azure

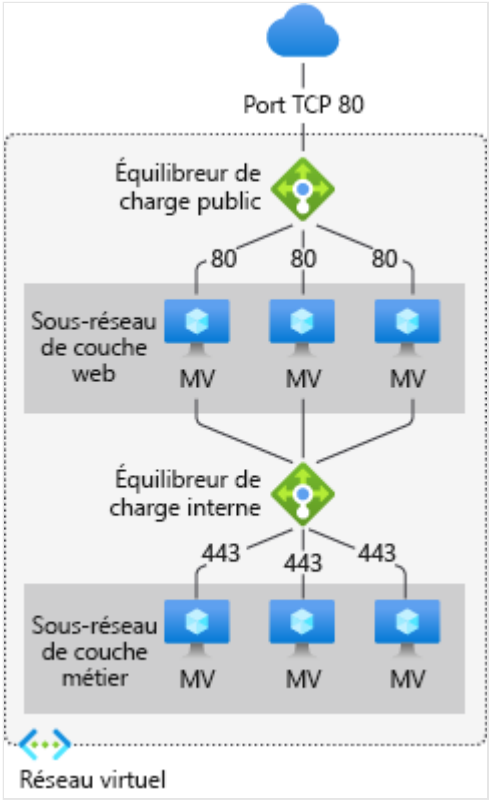
---

Dernière mise à jour : 20/08/2026

# Réseaux virtuels et machines virtuelles dans Azure

Lorsque vous créez une machine virtuelle Azure, vous créez un réseau virtuel ou en utilisez un existant. Déterminez la façon dont vos machines virtuelles doivent être accessibles sur le réseau virtuel. Il est essentiel de planifier les choses avant de créer des ressources et de vous assurer que vous connaissez les limites des ressources réseau.

Dans l'illustration suivante, les machines virtuelles sont représentées en tant que serveurs web et serveurs d'applications. Chaque ensemble de machines virtuelles est affecté à des sous-réseaux distincts dans le réseau virtuel.




Vous pouvez créer un réseau virtuel avant de créer une machine virtuelle, ou vous pouvez créer le réseau virtuel lors de la création d'une machine virtuelle.

Vous créez ces ressources pour prendre en charge la communication avec une machine virtuelle :

- Interfaces réseau
- Adresses IP
- Réseau virtuel et sous-réseaux

Tenez également compte des ressources facultatives suivantes :

- Groupes de sécurité réseau
- Équilibreurs de charge

## Interfaces réseau

Une carte d'interface réseau (NIC) est l'interconnexion entre une machine virtuelle et un réseau virtuel. Une machine virtuelle doit posséder au moins une carte d'interface réseau. Une machine virtuelle peut avoir plusieurs cartes d'interface réseau, en fonction de la taille de la machine virtuelle que vous créez. Pour en savoir plus sur le nombre de cartes réseau prises en charge par chaque taille de machine virtuelle, consultez tailles de machine virtuelle.

Vous pouvez créer une machine virtuelle avec plusieurs cartes réseau et ajouter ou supprimer des cartes réseau tout au long du cycle de vie d'une machine virtuelle. Plusieurs cartes réseau permettent à une machine virtuelle de se connecter à différents sous-réseaux.

Chaque carte d'interface réseau attachée à une machine virtuelle doit se trouver dans le même emplacement et abonnement que la machine virtuelle. Chaque carte d'interface réseau doit être connectée à un réseau virtuel existant dans les mêmes emplacement et abonnement Azure que la carte d'interface réseau. Le sous-réseau auquel une machine virtuelle est connectée peut être modifié une fois la machine virtuelle créée. Vous ne pouvez pas modifier le réseau virtuel. Chaque carte d'interface réseau attachée à une machine virtuelle est attribuée à une adresse MAC qui ne change pas jusqu'à ce que la machine virtuelle soit supprimée.

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer une interface réseau.

Agrandir le tableau

| Méthode | Description |
|---|---|
| portail Azure | Lorsque vous créez une machine virtuelle dans le Portail Azure, une interface réseau est automatiquement créée pour vous. Le portail crée une machine virtuelle avec une seule carte d'interface réseau. Si vous souhaitez créer une machine virtuelle avec plusieurs cartes d'interface réseau, vous devez la créer en suivant une autre méthode. |
| Azure PowerShell | Utilisez New-AzNetworkInterface avec le paramètre `-PublicIpAddressId` pour fournir l'identificateur de l'adresse IP publique que vous avez créée précédemment. |
| Azure CLI | Pour fournir l'identificateur de l'adresse IP publique que vous avez créée précédemment, utilisez az network nic create avec le paramètre `--public-ip-address`. |

| Méthode | Description |
| --- | --- |
| Modèle | Pour plus d'informations sur le déploiement d'une interface réseau à l'aide d'un modèle, consultez Interface de réseau dans un Réseau virtuel avec une Adresse IP publique. |

# Adresses IP

Vous pouvez attribuer ces types d'adresses IP à une interface réseau dans Azure :

- **Adresses IP publiques** : utilisées pour la communication entrante et sortante (sans traduction d'adresses réseau [NAT]) avec Internet et d'autres ressources Azure non connectées à un réseau virtuel. L'attribution d'une adresse IP publique à une carte d'interface réseau est facultative. Les adresses IP publiques ont un coût nominal et il existe une limite maximum d'adresses IP publiques pouvant être utilisées par abonnement.
- **Adresses IP privées** : utilisées pour la communication au sein d'un réseau virtuel, avec votre réseau local et Internet (sans NAT). Au moins une adresse IP privée doit être affectée à une machine virtuelle. Pour en savoir plus sur le NAT (traduction d'adresses réseau) dans Azure, consultez Comprendre les connexions sortantes dans Azure.

Vous pouvez affecter des adresses IP publiques aux :

- Machines virtuelles
- Équilibreurs de charge publics

Vous pouvez affecter des adresses IP privées aux :

- Machines virtuelles
- Équilibreurs de charge interne

Vous attribuez des adresses IP à une machine virtuelle à l'aide d'une interface réseau.

Azure affecte dynamiquement des adresses IP par défaut. Une adresse IP n'est pas affectée lors de la création, mais elle est affectée lorsque vous créez ou démarrez une machine virtuelle arrêtée. L'adresse IP est libérée lorsque vous arrêtez ou supprimez la machine virtuelle.

Pour conserver l'adresse IP de la machine virtuelle de la même façon, définissez la méthode d'allocation sur statique. L'adresse IP est attribuée immédiatement et ne se libère que si vous supprimez la machine virtuelle ou modifiez sa méthode d'allocation en mode dynamique.

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer une adresse IP.

Agrandir le tableau

| Méthode | Description |
| --- | --- |
| portail Azure | Par défaut, les adresses IP publiques sont dynamiques. L'adresse IP peut changer lorsque la machine virtuelle est arrêtée ou supprimée. Pour vous assurer que la machine virtuelle utilise toujours la même adresse IP publique, créez une adresse IP publique statique. Par défaut, le portail attribue une adresse IP privée dynamique à une carte d'interface réseau lors de la création d'une machine virtuelle. Vous pouvez modifier cette adresse IP statique après la création de la machine virtuelle. |
| Azure PowerShell | Vous utilisez New-AzPublicIpAddress avec le paramètre `-AllocationMethod` en tant que Dynamique ou Statique. |
| Azure CLI | Vous utilisez az network public-ip create avec le paramètre `--allocation-method` défini sur la valeur Dynamique ou Statique. |
| Modèle | Pour plus d'informations sur le déploiement d'une adresse IP publique à l'aide d'un modèle, consultez Interface réseau dans un Réseau virtuel avec une Adresse IP publique. |

Après avoir créé une adresse IP publique, vous pouvez l'associer à une machine virtuelle en l'attribuant à une carte d'interface réseau.

> **Remarque**
>
> Azure fournit une adresse IP d'accès sortant par défaut pour les machines virtuelles qui n'ont pas d'adresse IP publique ou qui se trouvent dans le pool de back-ends d'un équilibreur de charge Azure de base interne. Le mécanisme d'adresse IP d'accès sortant par défaut fournit une adresse IP sortante qui n'est pas configurable.
>
> L'adresse IP de l'accès sortant par défaut est désactivée quand l'un des événements suivants se produit :
>
> - Une adresse IP publique est affectée à la machine virtuelle.
> - La machine virtuelle est placée dans le pool principal d'un équilibreur de charge standard, avec ou sans règles de trafic sortant.
> - Une ressource Azure NAT Gateway est attribuée au sous-réseau de la machine virtuelle.
>
> Les machines virtuelles que vous créez en utilisant des ensembles de machines virtuelles en mode d'orchestration flexible n'ont pas d'accès sortant par défaut.
>
> Pour plus d'informations sur les connexions sortantes dans Azure, consultez Accès sortant par défaut dans Azure et Utiliser SNAT (Source Network Address Translation) pour les

connexions sortantes.

## Réseau virtuel et sous-réseaux

Un sous-réseau est une plage d'adresses IP dans votre réseau virtuel. Vous pouvez diviser un réseau virtuel en plusieurs sous-réseaux pour plus de sécurité et une meilleure organisation. Chaque carte d'interface réseau dans une machine virtuelle est connectée à un sous-réseau dans un réseau virtuel. Les cartes d'interface réseau connectées aux sous-réseaux (identiques ou différents) au sein d'un réseau virtuel peuvent communiquer entre elles sans aucun besoin de configuration supplémentaire.

Lorsque vous configurez un réseau virtuel, vous spécifiez la topologie, y compris les sous-réseaux et les espaces d'adressage disponibles. Sélectionnez des plages d'adresses qui ne se chevauchent pas si le réseau virtuel est connecté à d'autres réseaux virtuels ou à des réseaux locaux. Les adresses IP sont privées et ne sont pas accessibles à partir d'Internet. Azure traite toute plage d'adresses dans le cadre de l'espace d'adressage IP du réseau virtuel privé. La plage d'adresses est accessible uniquement au sein du réseau virtuel, au sein de réseaux virtuels interconnectés et à partir de votre emplacement local.

Si vous travaillez au sein d'une organisation dans laquelle une autre personne est responsable des réseaux internes, vous devez discuter avec elle avant de sélectionner votre espace d'adressage. Assurez-vous qu'il n'y a pas de chevauchement dans l'espace d'adressage. Indiquez-lui l'espace que vous souhaitez utiliser afin qu'elle n'essaie pas d'utiliser la même plage d'adresses IP que vous.

Il n'existe pas de limites de sécurité par défaut entre les sous-réseaux. Les machines virtuelles de chacun de ces sous-réseaux peuvent communiquer. Si votre déploiement requiert des limites de sécurité, utilisez des **Groupes de sécurité réseau (NSG)** , qui contrôlent le flux du trafic vers et depuis les sous-réseaux et les machines virtuelles.

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer un réseau virtuel et des sous-réseaux.

Agrandir le tableau

| Méthode | Description |
| --- | --- |
| portail Azure | Si vous autorisez Azure à créer un réseau virtuel lors de la création d'une machine virtuelle, le nom attribué sera une combinaison du nom du groupe de ressources qui contient le réseau |

| Méthode | Description |
| --- | --- |
| | virtuel et de `-vnet` . L'espace d'adressage est 10.0.0.0/24, le nom du sous-réseau nécessaire est **default**, et la plage d'adresses de sous-réseau est 10.0.0.0/24. |
| Azure PowerShell | Vous utilisez New-AzVirtualNetworkSubnetConfig et New-AzVirtualNetwork pour créer un sous-réseau et un réseau virtuel. Vous pouvez également utiliser Add-AzVirtualNetworkSubnetConfig pour ajouter un sous-réseau à un réseau virtuel existant. |
| Azure CLI | Le sous-réseau et le réseau virtuel sont créés en même temps. Fournissez un paramètre `--subnet-name` à az network vnet create avec le nom du sous-réseau. |
| Modèle | Pour plus d'informations sur l'utilisation d'un modèle pour créer un réseau virtuel et des sous-réseaux, consultez Réseau virtuel avec deux sous-réseaux . |

## Préfixes d'adresses multiples sur un sous-réseau

Plusieurs préfixes d'adresse sur un sous-réseau sont une fonctionnalité qui offre la possibilité de modifier des espaces d'adressage IP sur un sous-réseau. Avec cette solution, les clients utilisant des machines virtuelles et des groupes de machines virtuelles identiques peuvent ajouter et supprimer des préfixes d'adresses IP pour répondre à leurs exigences de mise à l'échelle.

**Limitations :**

- Les clients ne peuvent utiliser qu'une seule configuration d'adresse client (CA) par carte d'interface réseau (NIC).
- Les clients ne peuvent l'utiliser que sur des sous-réseaux de machines virtuelles et de groupes de machines virtuelles identiques. Les sous-réseaux délégués ne sont pas pris en charge.

**Tarification** : plusieurs préfixes d'adresse sur un sous-réseau sont proposés gratuitement.

Nous vous invitons à partager vos commentaires sur cette fonctionnalité dans cette enquête rapide .

> **Important**
>
> La prise en charge des préfixes multiples pour les sous-réseaux de réseau virtuel Azure est actuellement en préversion publique. Cette préversion n'a pas de contrat de niveau de service et n'est pas recommandée pour les charges de travail de production. Certaines fonctionnalités peuvent ne pas être prises en charge ou avoir des fonctionnalités limitées.

Pour plus d'informations, consultez Conditions d'Utilisation Supplémentaires relatives aux Évaluations Microsoft Azure.

Pour plus d'informations sur la configuration de préfixes d'adresses multiples sur un sous-réseau, consultez Créer des préfixes multiples pour un sous-réseau.

**Important**

Il existe deux propriétés de sous-réseau pour l'espace d'adressage, **AddressPrefix** (chaîne) et **AddressPrefixes** (liste). La distinction et l'utilisation sont expliquées ci-dessous.

- La propriété de type tableau a été introduite pour prendre en charge la double pile. La propriété est également utilisée pour les scénarios avec plusieurs préfixes de sous-réseau, comme indiqué précédemment.
- Dans le cadre de la mise à jour de l'expérience client du portail Azure, **AddressPrefixes** est la propriété par défaut de l'espace d'adressage du sous-réseau lorsqu'un sous-réseau est créé via le portail.
  - Par défaut, tout nouveau sous-réseau créé via le portail utilise le paramètre de la liste **AddressPrefixes**.
- Si les clients utilisent la double pile dans leur réseau virtuel ou ont plusieurs préfixes de sous-réseau, leur configuration est mise à jour pour utiliser la propriété de type liste.
  - Pour les déploiements existants utilisant la chaîne, le comportement actuel est conservé, sauf s'il existe des modifications explicites dans votre réseau virtuel pour utiliser la propriété de liste pour les préfixes d'adresses de sous-réseau (par exemple en cas d'ajout d'un espace d'adressage IPv6 ou d'un autre préfixe au sous-réseau).
- Nous recommandons aux clients de rechercher les deux propriétés dans le sous-réseau, le cas échéant.

## Groupes de sécurité réseau

Un groupe de sécurité réseau contient une liste des règles de liste de contrôle d'accès qui autorise ou rejette le trafic réseau vers les sous-réseaux, les cartes d'interface réseau ou les deux. Des groupes de sécurité réseau peuvent être associés à des sous-réseaux ou à des cartes d'interface réseau connectées à un sous-réseau. Lorsqu'un groupe de sécurité réseau est associé à un sous-réseau, les règles de liste de contrôle d'accès s'appliquent à toutes les machines virtuelles présentes dans ce sous-réseau. Le trafic vers une carte d'interface réseau peut être limité par l'association directe d'un groupe de sécurité réseau à une carte d'interface réseau.

Les NSG contiennent deux ensembles de règles : les règles de trafic entrant et les règles de trafic sortant. La priorité d'une règle doit être unique dans chaque ensemble.

Chaque règle a des propriétés de :

- Protocole
- Plages de ports source et de destination
- Préfixes d'adresse
- Direction du trafic
- Priorité
- Type d'accès

Tous les groupes de sécurité réseau contiennent un ensemble de règles par défaut. Vous ne pouvez pas supprimer ou remplacer ces règles par défaut, car elles ont la priorité la plus faible et les règles que vous créez ne peuvent pas les remplacer.

Lorsque vous associez un groupe de sécurité réseau à une carte réseau, les règles d'accès réseau de ce groupe sont appliquées uniquement à cette carte réseau. Si un groupe de sécurité réseau est appliqué à une seule carte d'interface réseau sur une machine virtuelle comprenant plusieurs cartes d'interface réseau, celui-ci n'affecte pas le trafic lié aux autres cartes d'interface réseau. Vous pouvez associer différents groupes de sécurité réseau à une carte d'interface réseau (ou une machine virtuelle, selon le modèle de déploiement) et au sous-réseau auquel une carte d'interface réseau ou une machine virtuelle est liée. La priorité est donnée en fonction de la direction du trafic.

Veillez à planifier vos groupes de sécurité réseau lorsque vous planifiez vos machines virtuelles et votre réseau virtuel.

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer un groupe de sécurité réseau.

Agrandir le tableau

| Méthode | Description |
| --- | --- |
| portail Azure | Lorsque vous créez une machine virtuelle dans le portail Azure, un NSG est automatiquement créé et associé à l'interface réseau créée par le portail. Le nom du groupe de sécurité réseau est une combinaison du nom de la machine virtuelle et de `-nsg` .<br>Ce groupe de sécurité réseau contient une règle de trafic entrant : |

| Méthode | Description |
| --- | --- |
| | avec une priorité de 1 000.<br>Le service est configuré pour RDP.<br>Le protocole est défini sur TCP.<br>Le port est défini sur 3 389.<br>L'action est définie sur **Autoriser**.<br>Si vous souhaitez autoriser tout autre trafic entrant vers la machine virtuelle, créez une ou plusieurs règles. |
| Azure PowerShell | Utilisez New-AzNetworkSecurityRuleConfig et fournissez les informations de la règle requise. Utilisez New-AzNetworkSecurityGroup pour créer le groupe de sécurité réseau. Utilisez Set-AzVirtualNetworkSubnetConfig pour configurer le groupe de sécurité réseau du sous-réseau. Utilisez Set-AzVirtualNetwork pour ajouter le groupe de sécurité réseau au réseau virtuel. |
| Azure CLI | Utilisez az network nsg create pour créer initialement le groupe de sécurité réseau. Utilisez az network nsg rule create pour ajouter des règles à un groupe de sécurité réseau. Utilisez az network vnet subnet update pour ajouter le NSG au sous-réseau. |
| Modèle | Utilisez Create a Network Security Group comme guide pour le déploiement d'un groupe de sécurité réseau à l'aide d'un modèle. |

# Équilibreurs de charge

Azure Load Balancer offre une haute disponibilité et des performances réseau élevées pour vos applications. Un équilibreur de charge peut être configuré pour équilibrer le trafic Internet entrant vers des machines virtuelles ou équilibrer le trafic entre les machines virtuelles d'un réseau virtuel. Un équilibrage de charge peut également équilibrer le trafic entre les machines virtuelles et les ordinateurs locaux d'un réseau intersite ou transférer le trafic externe vers une machine virtuelle spécifique.

L'équilibreur de charge mappe le trafic entrant et sortant entre :

- L'adresse IP publique et le port sur le serveur de répartition de charge.
- L'adresse IP privée et le port de la machine virtuelle.

Lorsque vous créez un équilibrage de charge, vous devez également prendre en compte les éléments de configuration suivants :

- **Configuration d'une adresse IP frontale** : un équilibrage de charge peut inclure une ou plusieurs adresses IP frontales. Ces adresses IP servent d'entrée pour le trafic.
- **Pool d'adresses principal** : adresses IP qui sont associées à la carte d'interface réseau vers laquelle la charge est distribuée.

- **Réacheminement de port** : définit la manière dont le trafic entrant transite via l'adresse IP frontale et est distribué à l'adresse IP principale en utilisant des règles NAT de trafic entrant.
- **Règles d'équilibrage de charge** : mappent une combinaison donnée d'adresses IP et de ports frontaux vers un ensemble de combinaisons d'adresses IP et de port principaux. Un même équilibreur de charge peut avoir plusieurs règles d'équilibrage de charge. Chaque règle est une combinaison d'une adresse IP et d'un port frontaux et d'une adresse IP et d'un port principaux associés aux machines virtuelles.
- **Sondes** : surveillent l'intégrité des machines virtuelles. Lorsqu'une sonde ne répond pas, l'équilibrage de charge n'envoie plus de nouvelles connexions aux machines virtuelles défaillantes. Les connexions existantes ne sont pas affectées et les nouvelles connexions sont envoyées aux machines virtuelles saines.
- **Règles de trafic sortant** - Une règle de trafic sortant configure la traduction d'adresses réseau (NAT) du trafic sortant pour que toutes les machines virtuelles ou instances identifiées par le pool de back-ends de votre équilibreur de charge Standard soient traduites vers le front-end.

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer un équilibrage de charge accessible sur Internet.

Agrandir le tableau

| Méthode | Description |
|---|---|
| Portail Azure | Vous pouvez équilibrer la charge du trafic Internet sur les machines virtuelles avec le portail Azure. |
| Azure PowerShell | Utilisez New-AzLoadBalancerFrontendIpConfig avec le paramètre `-PublicIpAddress` pour fournir l'identificateur de l'adresse IP publique que vous avez créée précédemment. Utilisez New-AzLoadBalancerBackendAddressPoolConfig pour créer la configuration du pool d'adresses principal. Utilisez New-AzLoadBalancerInboundNatRuleConfig pour créer des règles NAT de trafic entrant associées à la configuration IP frontale que vous avez créée. Utilisez New-AzLoadBalancerProbeConfig pour créer les sondes dont vous avez besoin. Utilisez New-AzLoadBalancerRuleConfig pour créer la configuration d'équilibrage de charge. Utilisez New-AzLoadBalancer pour créer l'équilibrage de charge. |
| Azure CLI | Utilisez az network lb create pour créer la configuration d'équilibrage de charge initiale. Utilisez az network lb frontend-ip create pour ajouter l'adresse IP publique que vous avez créée précédemment. Utilisez az network lb address-pool create pour ajouter la configuration du pool d'adresses principal. Utilisez az network lb inbound-nat-rule create pour ajouter des règles NAT. Utilisez az network lb rule create pour ajouter les règles d'équilibrage de charge. Utilisez az network lb probe create pour ajouter les sondes. |

| Méthode | Description |
| --- | --- |
| Modèle | Utilisez 3 machines virtuelles dans un équilibreur de charge comme guide pour le déploiement d'un équilibrage de charge à l'aide d'un modèle. |

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer un équilibrage de charge interne.

Agrandir le tableau

| Méthode | Description |
| --- | --- |
| Portail Azure | Vous pouvez équilibrer la charge du trafic interne avec un équilibreur de charge sur le portail Azure. |
| Azure PowerShell | Pour fournir une adresse IP privée dans le sous-réseau du réseau, utilisez New-AzLoadBalancerFrontendIpConfig avec le paramètre `-PrivateIpAddress`. Utilisez New-AzLoadBalancerBackendAddressPoolConfig pour créer la configuration du pool d'adresses principal. Utilisez New-AzLoadBalancerInboundNatRuleConfig pour créer des règles NAT de trafic entrant associées à la configuration IP frontale que vous avez créée. Utilisez New-AzLoadBalancerProbeConfig pour créer les sondes dont vous avez besoin. Utilisez New-AzLoadBalancerRuleConfig pour créer la configuration d'équilibrage de charge. Utilisez New-AzLoadBalancer pour créer l'équilibrage de charge. |
| Azure CLI | Utilisez la commande az network lb create pour créer la configuration d'équilibrage de charge initiale. Pour définir l'adresse IP privée, utilisez az network lb frontend-ip create avec le paramètre `--private-ip-address`. Utilisez az network lb address-pool create pour ajouter la configuration du pool d'adresses principal. Utilisez az network lb inbound-nat-rule create pour ajouter des règles NAT. Utilisez az network lb rule create pour ajouter les règles d'équilibrage de charge. Utilisez az network lb probe create pour ajouter les sondes. |
| Modèle | Utilisez 2 machines virtuelles dans un équilibreur de charge comme guide pour le déploiement d'un équilibrage de charge à l'aide d'un modèle. |

# Machines virtuelles

Les machines virtuelles peuvent être créées dans le même réseau virtuel et se connecter les unes aux autres à l'aide d'adresses IP privées. Les machines virtuelles peuvent se connecter si elles se trouvent dans des sous-réseaux différents. Elles se connectent sans avoir besoin de configurer de passerelle ou d'utiliser d'adresses IP publiques. Pour placer des machines virtuelles dans un réseau virtuel, vous devez créer le réseau virtuel. Lorsque vous créez chaque machine virtuelle, vous l'affectez au réseau virtuel et au sous-réseau. Les machines virtuelles acquièrent leurs paramètres réseau lors du déploiement ou du démarrage.

Une adresse IP est affectée aux machines virtuelles lorsqu'elles sont déployées. Lorsque vous déployez plusieurs machines virtuelles dans un réseau virtuel ou un sous-réseau, des adresses IP leur sont attribuées lorsqu'elles démarrent. Vous pouvez également allouer une adresse IP statique à une machine virtuelle. Si vous allouez une adresse IP dynamique statique, vous devez envisager d'utiliser un sous-réseau spécifique afin d'éviter de réutiliser accidentellement l'adresse IP statique pour une autre machine virtuelle.

Si vous créez une machine virtuelle et que vous voulez la migrer plus tard vers un réseau virtuel, il ne s'agit pas d'une modification de configuration simple. Redéployez la machine virtuelle dans le réseau virtuel. Pour la redéployer, le plus simple consiste à supprimer la machine virtuelle (mais pas les disques attachés à celle-ci), puis à recréer la machine virtuelle à l'aide des disques d'origine dans le réseau virtuel.

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer une machine virtuelle dans un réseau virtuel.

Agrandir le tableau

| Méthode | Description |
|---|---|
| portail Azure | Utilise les paramètres de réseau par défaut qui ont été mentionnés précédemment pour créer une machine virtuelle avec une seule carte d'interface réseau. Pour créer une machine virtuelle avec plusieurs cartes d'interface réseau, vous devez utiliser une autre méthode. |
| Azure PowerShell | Inclut l'utilisation de Add-AzVMNetworkInterface pour ajouter la carte d'interface réseau que vous avez créée précédemment pour la configuration de la machine virtuelle. |
| Azure CLI | Créez une machine virtuelle et connectez-la à un réseau virtuel, à un sous-réseau et à une carte d'interface réseau, en procédant par étapes individuelles. |
| Modèle | Utilisez Very simple deployment of a Windows VM comme guide pour le déploiement d'une machine virtuelle à l'aide d'un modèle. |

# NAT Gateway

Azure NAT Gateway simplifie la connectivité Internet sortante uniquement pour les réseaux virtuels. Quand il est configuré sur un sous-réseau, toute la connectivité sortante utilise vos adresses IP publiques statiques spécifiées. Une connectivité sortante est possible sans équilibreur de charge ni adresses IP publiques directement attachées aux machines virtuelles. NAT est complètement managé et hautement résilient.

Une connectivité sortante peut être définie pour chaque sous-réseau avec NAT. Plusieurs sous-réseaux au sein du même réseau virtuel peuvent avoir différents services NAT. Un sous-réseau est

configuré en spécifiant la ressource de passerelle NAT à utiliser. Tous les flux sortants UDP et TCP en provenance de toute instance de machine virtuelle utilisent une passerelle NAT. NAT est compatible avec les ressources d'adresse IP publique standard ou les ressources de préfixe d'adresse IP publique ou une combinaison des deux. Vous pouvez utiliser directement un préfixe d'adresse IP publique ou distribuer les adresses IP publiques du préfixe entre plusieurs ressources de passerelle NAT. NAT nettoie tout le trafic vers la plage d'adresses IP du préfixe. Le filtrage de toute adresse IP de vos déploiements est simple.

La passerelle NAT traite automatiquement tout le trafic sortant sans configuration client. Les routes définies par l'utilisateur ne sont pas nécessaires. NAT est prioritaire sur les autres scénarios de trafic sortant et remplace la destination Internet par défaut d'un sous-réseau.

Les groupes de machines virtuelles identiques qui créent des machines virtuelles en mode d'orchestration flexible n'ont pas d'accès sortant par défaut. La passerelle NAT Azure est la méthode d'accès sortant recommandée pour les ensembles de machines virtuelles en mode d'orchestration flexible.

Pour plus d'informations sur Azure NAT Gateway, consultez Qu'est-ce que Azure NAT Gateway ?

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer une ressource de passerelle NAT.

Agrandir le tableau

| Méthode | Description |
|---|---|
| portail Azure | Crée un réseau virtuel, un sous-réseau, une adresse IP publique, une passerelle NAT et une machine virtuelle pour tester la ressource de passerelle NAT. |
| Azure PowerShell | Inclut l'utilisation de New-AzNatGatewaypour créer une ressource de passerelle NAT. Crée un réseau virtuel, un sous-réseau, une adresse IP publique, une passerelle NAT et une machine virtuelle pour tester la ressource de passerelle NAT. |
| Azure CLI | Inclut l'utilisation de az network nat gateway createpour créer une ressource de passerelle NAT. Crée un réseau virtuel, un sous-réseau, une adresse IP publique, une passerelle NAT et une machine virtuelle pour tester la ressource de passerelle NAT. |
| Modèle | Crée un réseau virtuel, un sous-réseau, une adresse IP publique et une ressource de passerelle NAT. |

## Azure Bastion

Azure Bastion est déployé pour fournir une connectivité de gestion sécurisée aux machines virtuelles dans un réseau virtuel. Le service Azure Bastion vous permet d'établir une connexion RDP et SSH sécurisée et fluide aux machines virtuelles de votre réseau virtuel. Azure Bastion active les connexions sans exposer d'adresse IP publique sur la machine virtuelle. Les connexions sont établies directement à partir du portail Azure, sans qu'un client/agent ou logiciel supplémentaire ne soit nécessaire. Azure Bastion prend en charge les adresses IP publiques standard.

Le tarif horaire commence à partir du moment où Bastion est déployé, quelle que soit l'utilisation des données sortantes. Pour plus d'informations, consultez Tarifications et Références SKU. Si vous déployez Bastion dans le cadre d'un tutoriel ou d'un test, nous vous recommandons de supprimer cette ressource après l'avoir utilisée.

Pour plus d'informations sur Azure Bastion, consultez Présentation d'Azure Bastion.

Ce tableau répertorie les méthodes que vous pouvez utiliser pour créer le déploiement d'un Bastion Azure.

Agrandir le tableau

| Méthode | Description |
|---|---|
| portail Azure | Crée un réseau virtuel, des sous-réseaux, une adresse IP publique, un hôte bastion et des machines virtuelles. |
| Azure PowerShell | Crée un réseau virtuel, des sous-réseaux, une adresse IP publique et un hôte bastion. Inclut l'utilisation de New-AzBastion pour créer l'hôte bastion. |
| Azure CLI | Crée un réseau virtuel, des sous-réseaux, une adresse IP publique et un hôte bastion. Inclut l'utilisation de az network bastion create pour créer l'hôte bastion. |
| Modèle | Pour obtenir un exemple de modèle de déploiement intégrant un hôte Azure Bastion, consultez Démarrage rapide : créer un équilibreur de charge public pour équilibrer la charge des machines virtuelles à l'aide d'un modèle ARM. |

# Étapes suivantes

Pour connaître les étapes spécifiques aux machines virtuelles concernant la gestion des réseaux virtuels Azure pour les machines virtuelles, consultez les didacticiels Windows ou Linux.

Il existe également des guides de démarrage rapide sur l'équilibrage de charge des machines virtuelles et la création d'applications à haute disponibilité en utilisant le CLI ou le PowerShell

- Découvrez comment configurer les connexions de réseau virtuel à réseau virtuel.

- Découvrez comment résoudre les problèmes relatifs aux itinéraires.
- En savoir plus sur la bande passante réseau des machines virtuelles

---

Last updated on 15/04/2025

# Options de disponibilité pour machines virtuelles Azure

**S'applique aux :** ✔ Machines virtuelles Linux ✔ Machines virtuelles Windows ✔ Groupes identiques flexibles ✔ Groupes identiques uniformes

Cet article fournit une vue d'ensemble des options de disponibilité pour machines virtuelles Azure.

## Zones de disponibilité

Les zones de disponibilité élargissent le niveau de contrôle dont vous disposez pour maintenir la disponibilité des applications et des données sur vos machines virtuelles. Une zone de disponibilité est une zone physiquement séparée au sein d'une région Azure. On distingue trois zones de disponibilité par région Azure prise en charge.

Chaque zone de disponibilité possède une source d'alimentation, un réseau et un système de refroidissement propres. En concevant vos solutions de manière à utiliser des machines virtuelles répliquées dans des zones, vous pouvez protéger vos applications et vos données de la perte d'un centre de données. Si une zone est compromise, les applications et données répliquées sont instantanément rendues disponibles dans une autre zone.

> ⓘ **Remarque**
>
> Les ressources régionales peuvent exister ou non dans une zone de disponibilité. De plus, il n'est pas possible de savoir dans quelle zone physique ou logique se trouve une ressource régionale. Une défaillance dans l'une des zones de disponibilité d'une région peut entraîner l'arrêt d'une machine virtuelle régionale.

## Groupes de machines virtuelles identiques

Les groupes de machines virtuelles identiques Azure vous permettent de créer et de gérer un groupe de machines virtuelles à charge équilibrée. Le nombre d'instances de machine virtuelle peut augmenter ou diminuer automatiquement en fonction d'une demande ou d'un calendrier défini. Les groupes identiques offrent une haute disponibilité à vos applications, et vous permettent de gérer, configurer et mettre à jour de manière centralisée de nombreuses machines

virtuelles. Le groupe identique proprement dit ne vous coûte rien ; vous payez uniquement pour chaque instance de machine virtuelle que vous créez.

Les machines virtuelles d'un groupe identique peuvent également être déployées dans plusieurs zones de disponibilité, dans une seule zone de disponibilité ou dans une région. Les options de déploiement de la zone de disponibilité peuvent varier en fonction du mode d'orchestration.

## Groupes à haute disponibilité

Un groupe à haute disponibilité est un regroupement logique de machines virtuelles qui permet à Azure de comprendre comment votre application est conçue, afin de garantir la redondance et la disponibilité. Il est recommandé de créer au moins deux machines virtuelles dans un groupe à haute disponibilité, de manière à fournir une application hautement disponible et à répondre aux exigences du niveau de 99,95 % inscrit dans les contrats de niveau de service Azure. Le groupe à haute disponibilité proprement dit ne vous coûte rien ; vous payez uniquement pour chaque instance de machine virtuelle que vous créez.

## Équilibrage de charge

Combinez Azure Load Balancer avec des zones de disponibilité et des groupes identiques pour une meilleure résilience de votre application. L'équilibrage de charge Azure répartit le trafic entre plusieurs machines virtuelles. L'équilibrage de charge Azure est compris pour nos machine virtuelles de niveau Standard. Certains niveaux de machines virtuelles n'intègrent pas Azure Load Balancer. Pour plus d'informations sur l'équilibrage de charge des machines virtuelles, consultez les démarrages rapides Load Balancer à l'aide de CLI ou PowerShell.

## Redondance de Stockage Azure

Le service Stockage Azure stocke toujours plusieurs copies de vos données afin qu'elles soient protégées contre des événements planifiés ou non, notamment des défaillances matérielles temporaires, des pannes de réseau ou de courant et des catastrophes naturelles majeures. La redondance garantit que votre compte de stockage répond à ses objectifs de disponibilité et de durabilité, même en cas de défaillance.

Lorsque vous choisissez l'option de redondance la mieux adaptée à votre scénario, réfléchissez aux compromis possibles entre, d'une part, des coûts réduits et, de l'autre, une disponibilité accrue. Les facteurs déterminant le choix de l'option de redondance sont les suivants :

- Mode de réplication de vos données dans la région primaire

- Réplication éventuelle de vos données vers une deuxième région géographiquement éloignée de la région primaire, afin d'offrir une protection contre des catastrophes régionales
- Nécessité ou non pour l'application d'avoir accès en lecture aux données répliquées dans la région secondaire si la région primaire devient indisponible pour une raison quelconque

Pour plus d'informations, consultez Redondance de Stockage Azure.

## Azure Site Recovery (Récupération de site Azure)

En tant qu'organisation, vous devez adopter une stratégie de continuité d'activité et de reprise d'activité (BCDR) capable de garantir la sécurité de vos données et de maintenir vos applications et vos charges de travail en ligne, lorsque des interruptions planifiées et non planifiées se produisent.

Azure Site Recovery permet d'assurer la continuité de l'activité en maintenant l'exécution des charges de travail et des applications métier lors des interruptions. Site Recovery réplique les charges de travail s'exécutant sur des machines virtuelles et physiques depuis un site principal vers un emplacement secondaire. En cas d'interruption au niveau de votre site principal, vous basculez vers l'emplacement secondaire, depuis lequel vous pouvez accéder aux applications. Quand l'emplacement principal est de nouveau fonctionnel, vous pouvez effectuer une restauration automatique vers celui-ci.

Site Recovery peut gérer la réplication pour :

- Les machines virtuelles Azure qui répliquent des données entre des régions Azure.
- Machines virtuelles locales, machines virtuelles Azure Stack et serveurs physiques.

## Étapes suivantes

- Créer une machine virtuelle dans une zone de disponibilité
- Créer une machine virtuelle dans un groupe à haute disponibilité
- Créer un groupe de machines virtuelles identiques

---

Dernière mise à jour : 05/12/2025

# Qu’est-ce que PowerShell ?

PowerShell est une solution multiplateforme d’automatisation des tâches, composée d’un interpréteur de commandes (shell), d’un langage de script et d’un framework de gestion de la configuration. PowerShell s’exécute sur Windows, Linux et macOS.

## Interpréteur de ligne de commande

PowerShell est un interpréteur de commandes moderne qui comprend les meilleures fonctionnalités d’autres interpréteurs de commandes populaires. Contrairement à la plupart d’entre eux, qui acceptent et retournent uniquement du texte, PowerShell accepte et retourne des objets .NET. L’interpréteur de commandes comprend les fonctionnalités suivantes :

- Historique de lignes de commande robuste
- Saisie semi-automatique par tabulation et prédiction de commandes (cf. about_PSReadLine)
- alias de commandes et de paramètres
- Pipeline pour le chaînage des commandes
- Système d’aide dans la console, similaire aux pages `man` Unix

## Langage de script

En tant que langage de script, PowerShell est souvent utilisé pour automatiser la gestion des systèmes. Il sert également à créer, à tester et à déployer des solutions, souvent dans des environnements CI/CD. PowerShell repose sur le common language runtime (CLR) .NET. Toutes les entrées et sorties sont des objets .NET. Il n’est pas nécessaire d’analyser la sortie texte pour extraire des informations de la sortie. Le langage de script PowerShell comprend les fonctionnalités suivantes :

- Extensibilité au moyen de fonctions, de classes, de scripts et de modules
- Système de mise en forme extensible pour une sortie facile
- Système de type extensible pour la création de types dynamiques
- Prise en charge intégrée des formats de données courants (par exemple CSV, JSON et XML)

## Plateforme d’automatisation

La nature extensible de PowerShell fournit un écosystème de modules PowerShell pour déployer et gérer presque toutes les technologies avec lesquelles vous travaillez. Par exemple :

Modules Microsoft

- Azure
- Windows
- Exchange
- SQL

Modules tiers

- AWS
- VMware
- Oracle Cloud

## Gestion des configurations

PowerShell Desired State Configuration (DSC) est un framework de gestion dans PowerShell qui vous permet de gérer l'infrastructure de votre entreprise avec la configuration sous forme de code :

- Créer des configurations déclaratives et des scripts personnalisés pour des déploiements reproductibles
- Appliquer des paramètres de configuration et signaler la dérive de configuration
- Déployer la configuration suivant des modèles push ou pull

# Manifeste Monad

Jeffrey Snover, l'inventeur de PowerShell, a écrit le Manifeste monad pour expliquer sa vision de PowerShell et comment il changerait la façon dont nous gérons les systèmes. Utilisez le lien suivant pour télécharger une copie du Manifeste Monad.

Ce fichier PDF est une version du manifeste Monad original, qui a énoncé la vision à long terme et a commencé l'effort de développement qui est devenu PowerShell. PowerShell a fourni de nombreux éléments décrits dans ce document.

# Étapes suivantes

## Prise en main

Vous débutez avec PowerShell et vous ne savez pas où commencer ? Consultez les ressources suivantes.

- Installer PowerShell
- Découvrir PowerShell
- PowerShell 101
- Vidéo Microsoft Virtual Academy
- Modules Learn PowerShell

## PowerShell en action

Découvrez comment PowerShell est utilisé dans différents scénarios et sur différentes plateformes.

- Accès distant à PowerShell via SSH
- Prise en main de Azure PowerShell
- Création d'un pipeline CI/CD avec DSC
- Gestion des Microsoft Exchange

---

Last updated on 12/08/2026

# Windows Commands

S'applique à: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10, ✅ Azure Local 2311.2 and later

Toutes les versions prises en charge de Windows et windows Server ont un ensemble de commandes de console Win32 intégrées. Cet ensemble de documentation décrit les commandes Windows que vous pouvez utiliser pour automatiser les tâches à l'aide de scripts ou d'outils de script.

## Command-line shells

Windows a deux interpréteurs de commandes : l'interpréteur de commandes et PowerShell. Chaque interpréteur de commandes est un programme logiciel qui fournit une communication directe entre vous et le système d'exploitation ou l'application, fournissant un environnement pour automatiser les opérations informatiques.

L'interpréteur de commandes était le premier interpréteur de commandes intégré à Windows pour automatiser les tâches de routine, telles que la gestion des comptes d'utilisateur ou les sauvegardes nocturnes, avec des fichiers batch (.bat). Avec l'hôte de script Windows, vous pouvez exécuter des scripts plus sophistiqués dans l'interpréteur de commandes. Pour plus d'informations, consultez cscript ou wscript. Vous pouvez effectuer des opérations plus efficacement à l'aide de scripts que vous pouvez à l'aide de l'interface utilisateur. Les scripts acceptent toutes les commandes disponibles sur la ligne de commande.

PowerShell a été conçu pour étendre les fonctionnalités de l'interpréteur de commandes pour exécuter des commandes PowerShell appelées applets de commande. Les applets de commande sont similaires aux commandes Windows, mais fournissent un langage de script plus extensible. Vous pouvez exécuter des commandes Windows et des applets de commande PowerShell dans PowerShell, mais l'interpréteur de commandes ne peut exécuter que des commandes Windows et non des applets de commande PowerShell.

Pour l'automatisation Windows la plus robuste, up-to-date, nous vous recommandons d'utiliser PowerShell au lieu des commandes Windows ou de l'hôte de script Windows pour l'automatisation Windows.

Vous trouverez une référence de codes de sortie et d'erreur pour les commandes Windows dans les articles des codes d'erreur système de débogage qui peuvent être utiles pour comprendre les erreurs produites. Les commandes Windows incluent également des opérateurs de redirection de commandes. Pour en savoir plus sur leur utilisation, consultez Utilisation des opérateurs de redirection de commandes.

> ⓘ **Remarque**
>
> Vous pouvez également télécharger et installer PowerShell Core, la version open source de PowerShell.

## Saisie semi-automatique du fichier et du nom du répertoire de l'interpréteur de commandes

Vous pouvez configurer l'interpréteur de commandes pour terminer automatiquement les noms de fichiers et de répertoires sur une session d'ordinateur ou d'utilisateur lorsqu'un caractère de contrôle spécifié est enfoncé. Par défaut, ce caractère de contrôle est configuré pour être la touche **tabulation** des noms de fichiers et de répertoires, bien qu'ils puissent être différents. Pour modifier ce caractère de contrôle, exécutez `regedit.exe` et accédez à l'une des clés et entrées de Registre suivantes, selon que vous souhaitez modifier la valeur de l'utilisateur actuel uniquement ou pour tous les utilisateurs de l'ordinateur.

> ⊗ **Attention**
>
> Une modification incorrecte du Registre peut endommager gravement votre système. Avant d'apporter les modifications suivantes au Registre, vous devez sauvegarder les données évaluées sur l'ordinateur.

**registry**

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\PathCompletionChar
```

Définissez ces valeurs sur celle du caractère de contrôle que vous souhaitez utiliser. Consultez les codes de clé virtuelle pour obtenir une liste complète. Pour désactiver un caractère d'achèvement particulier dans le Registre, utilisez la valeur de **l'espace** (0x20) car il n'est pas un caractère de contrôle valide. Le type de valeur de cette entrée de Registre est REG_DWORD et peut également être spécifié par valeur hexadécimale ou décimale.

Vous pouvez également activer ou désactiver la saisie semi-automatique du nom du fichier et du répertoire par instance d'un interpréteur de commandes en exécutant `cmd.exe` le paramètre et le commutateur `/F:ON` ou `/F:OFF`. Si l'achèvement du nom est activé avec le `/F:ON` paramètre et le commutateur, les deux caractères de contrôle utilisés sont `Ctrl-D` utilisés pour la saisie semi-automatique du nom du répertoire et `Ctrl-F` pour la saisie semi-automatique du nom de fichier. Les paramètres spécifiés par l'utilisateur sont prioritaires sur les paramètres de

l'ordinateur et les options de ligne de commande sont prioritaires sur les paramètres du Registre.

# Référence de ligne de commande A-Z

Pour trouver des informations sur une commande spécifique, dans le menu A-Z suivant, sélectionnez la lettre que la commande commence par, puis sélectionnez le nom de la commande.

Un | B | C | D | E | F | G | H | Je | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

## A


- active
- add
- add alias
- add volume
- adprep
- append
- arp
- assign
- assoc
- at
- atmadm
- attach-vdisk
- attrib
- attributes
  - attributes disk
  - attributes volume
- auditpol
  - auditpol backup
  - auditpol clear
  - auditpol get
  - auditpol list
  - auditpol remove
  - auditpol resourcesacl
  - auditpol restore
  - auditpol set
- autochk
- autoconv

- autofmt
- automount

## B

- bcdboot
- bcdedit
- bdehdcfg
  - bdehdcfg driveinfo
  - bdehdcfg newdriveletter
  - bdehdcfg quiet
  - bdehdcfg restart
  - bdehdcfg size
  - bdehdcfg target
- begin backup
- begin restore
- bitsadmin
  - bitsadmin addfile
  - bitsadmin addfileset
  - bitsadmin addfilewithranges
  - bitsadmin cache
    - bitsadmin cache and delete
    - bitsadmin cache and deleteurl
    - bitsadmin cache and getexpirationtime
    - bitsadmin cache and getlimit
    - bitsadmin cache and help
    - bitsadmin cache and info
    - bitsadmin cache and list
    - bitsadmin cache and setexpirationtime
    - bitsadmin cache and setlimit
    - bitsadmin cache and clear
  - bitsadmin cancel
  - bitsadmin complete
  - bitsadmin create
  - bitsadmin examples
  - bitsadmin getaclflags
  - bitsadmin getbytestotal
  - bitsadmin getbytestransferred
  - bitsadmin getclientcertificate
  - bitsadmin getcompletiontime

- bitsadmin getcreationtime
- bitsadmin getcustomheaders
- bitsadmin getdescription
- bitsadmin getdisplayname
- bitsadmin geterror
- bitsadmin geterrorcount
- bitsadmin getfilestotal
- bitsadmin getfilestransferred
- bitsadmin gethelpertokenflags
- bitsadmin gethelpertokensid
- bitsadmin gethttpmethod
- bitsadmin getmaxdownloadtime
- bitsadmin getminretrydelay
- bitsadmin getmodificationtime
- bitsadmin getnoprogresstimeout
- bitsadmin getnotifycmdline
- bitsadmin getnotifyflags
- bitsadmin getnotifyinterface
- bitsadmin getowner
- bitsadmin getpeercachingflags
- bitsadmin getpriority
- bitsadmin getproxybypasslist
- bitsadmin getproxylist
- bitsadmin getproxyusage
- bitsadmin getreplydata
- bitsadmin getreplyfilename
- bitsadmin getreplyprogress
- bitsadmin getsecurityflags
- bitsadmin getstate
- bitsadmin gettemporaryname
- bitsadmin gettype
- bitsadmin getvalidationstate
- bitsadmin help
- bitsadmin info
- bitsadmin list
- bitsadmin listfiles
- bitsadmin makecustomheaderswriteonly
- bitsadmin monitor
- bitsadmin nowrap
- bitsadmin peercaching
  - bitsadmin peercaching and getconfigurationflags

    - bitsadmin peercaching and help
    - bitsadmin peercaching and setconfigurationflags
- bitsadmin peers
    - bitsadmin peers and clear
    - bitsadmin peers and discover
    - bitsadmin peers and help
    - bitsadmin peers and list
- bitsadmin rawreturn
- bitsadmin removeclientcertificate
- bitsadmin removecredentials
- bitsadmin replaceremoteprefix
- bitsadmin reset
- bitsadmin resume
- bitsadmin setaclflag
- bitsadmin setclientcertificatebyid
- bitsadmin setclientcertificatebyname
- bitsadmin setcredentials
- bitsadmin setcustomheaders
- bitsadmin setdescription
- bitsadmin setdisplayname
- bitsadmin sethelpertoken
- bitsadmin sethelpertokenflags
- bitsadmin sethttpmethod
- bitsadmin setmaxdownloadtime
- bitsadmin setminretrydelay
- bitsadmin setnoprogresstimeout
- bitsadmin setnotifycmdline
- bitsadmin setnotifyflags
- bitsadmin setpeercachingflags
- bitsadmin setpriority
- bitsadmin setproxysettings
- bitsadmin setreplyfilename
- bitsadmin setsecurityflags
- bitsadmin setvalidationstate
- bitsadmin suspend
- bitsadmin takeownership
- bitsadmin transfer
- bitsadmin util
    - bitsadmin util and enableanalyticchannel
    - bitsadmin util and getieproxy
    - bitsadmin util and help

        - bitsadmin util and repairservice
        - bitsadmin util and setieproxy
        - bitsadmin util and version
    - bitsadmin wrap
- bootcfg
    - bootcfg addsw
    - bootcfg copy
    - bootcfg dbg1394
    - bootcfg debug
    - bootcfg default
    - bootcfg delete
    - bootcfg ems
    - bootcfg query
    - bootcfg raw
    - bootcfg rmsw
    - bootcfg timeout
- break

## C

- cacls
- call
- cd
- certreq
- certutil
- change
    - change logon
    - change port
    - change user
- chcp
- chdir
- chglogon
- chgport
- chgusr
- chkdsk
- chkntfs
- choice
- cipher
- clean
- cleanmgr

- clip
- cls
- cmd
- cmdkey
- cmstp
- color
- comp
- compact
- compact vdisk
- convert
  - convert basic
  - convert dynamic
  - convert gpt
  - convert mbr
- copy
- create
  - create partition efi
  - create partition extended
  - create partition logical
  - create partition msr
  - create partition primary
  - create volume mirror
  - create volume raid
  - create volume simple
  - create volume stripe
- cscript

## D

- date
- dcdiag
- dcgpofix
- dcpromo
- defrag
- del
- delete
  - delete disk
  - delete partition
  - delete shadows
  - delete volume

- detach vdisk
- detail
  - detail disk
  - detail partition
  - detail vdisk
  - detail volume
- dfsdiag
  - dfsdiag testdcs
  - dfsdiag testdfsconfig
  - dfsdiag testdfsintegrity
  - dfsdiag testreferral
  - dfsdiag testsites
- dfsrmig
- diantz
- dir
- diskcomp
- diskcopy
- diskpart
- diskperf
- diskraid
- diskshadow
- dispdiag
- dnscmd
- doskey
- driverquery
- dtrace

## E

- echo
- edit
- endlocal
- end restore
- erase
- eventcreate
- Evntcmd
- exec
- exit
- expand
- expand vdisk

- expose
- extend
- extract

## F

- fc
- filesystems
- find
- findstr
- finger
- flattemp
- fondue
- for
- forfiles
- format
- freedisk
- fsutil
  - fsutil 8dot3name
  - fsutil behavior
  - fsutil devdrv
  - fsutil dirty
  - fsutil file
  - fsutil fsinfo
  - fsutil hardlink
  - fsutil objectid
  - fsutil quota
  - fsutil repair
  - fsutil reparsepoint
  - fsutil resource
  - fsutil sparse
  - fsutil tiering
  - fsutil transaction
  - fsutil usn
  - fsutil volume
  - fsutil wim
- ftp
  - ftp append
  - ftp ascii
  - ftp bell

- ftp binary
- ftp bye
- ftp cd
- ftp close
- ftp debug
- ftp delete
- ftp dir
- ftp disconnect
- ftp get
- ftp glob
- ftp hash
- ftp lcd
- ftp literal
- ftp ls
- ftp mget
- ftp mkdir
- ftp mls
- ftp mput
- ftp open
- ftp prompt
- ftp put
- ftp pwd
- ftp quit
- ftp quote
- ftp recv
- ftp remotehelp
- ftp rename
- ftp rmdir
- ftp send
- ftp status
- ftp trace
- ftp type
- ftp user
- ftp verbose
- ftp mdelete
- ftp mdir

- ftype
- fveupdate

## G

- getmac
- gettype
- goto
- gpfixup
- gpresult
- gpt
- gpupdate
- graftabl

## H

- help
- helpctr
- hostname

## I

- icacls
- if
- import (shadowdisk)
- import (diskpart)
- inactive
- ipconfig
- ipxroute
- irftp

## J

- jetpack

## K

- klist
- ksetup
  - ksetup addenctypeattr
  - ksetup addhosttorealmmap
  - ksetup addkdc
  - ksetup addkpasswd
  - ksetup addrealmflags
  - ksetup changepassword

- ksetup delenctypeattr
- ksetup delhosttorealmmap
- ksetup delkdc
- ksetup delkpasswd
- ksetup delrealmflags
- ksetup domain
- ksetup dumpstate
- ksetup getenctypeattr
- ksetup listrealmflags
- ksetup mapuser
- ksetup removerealm
- ksetup server
- ksetup setcomputerpassword
- ksetup setenctypeattr
- ksetup setrealm
- ksetup setrealmflags
- ktmutil
- ktpass

## L

- label
- list
  - list providers
  - list shadows
  - list writers
- load metadata
- lodctr
- logman
  - logman create
  - logman create alert
  - logman create api
  - logman create cfg
  - logman create counter
  - logman create trace
  - logman delete
  - logman import and logman export
  - logman query
  - logman start and logman stop
  - logman update

    - logman update alert
    - logman update api
    - logman update cfg
    - logman update counter
    - logman update trace
- logoff
- lpq
- lpr

## M

- macfile
- makecab
- manage bde
    - manage bde status
    - manage bde on
    - manage bde off
    - manage bde pause
    - manage bde resume
    - manage bde lock
    - manage bde unlock
    - manage bde autounlock
    - manage bde protectors
    - manage bde tpm
    - manage bde setidentifier
    - manage bde forcerecovery
    - manage bde changepassword
    - manage bde changepin
    - manage bde changekey
    - manage bde keypackage
    - manage bde upgrade
    - manage bde wipefreespace
- mapadmin
- md
- merge vdisk
- mkdir
- mklink
- mmc
- mode
- more

- mount
- mountvol
- move
- mqbkup
- mqsvc
- mqtgsvc
- msdt
- msg
- msiexec
- msinfo32
- mstsc

## N

- nbtstat
- netcfg
- netdom
  - netdom add
  - netdom computername
  - netdom join
  - netdom move
  - netdom movent4bdc
  - netdom query
  - netdom remove
  - netdom renamecomputer
  - netdom reset
  - netdom resetpwd
  - netdom trust
  - netdom verify
- net print
- net user
- netsh
  - netsh add
  - netsh advfirewall
  - netsh branchcache
  - netsh bridge
  - netsh delete
  - netsh dhcpclient
  - netsh dnsclient
  - netsh dump

    - netsh exec
    - netsh http
    - netsh interface
    - netsh ipsec
    - netsh lan
    - netsh mbn
    - netsh namespace
    - netsh netio
    - netsh nlm
    - netsh ras
    - netsh rpc
    - netsh set
    - netsh show
    - netsh trace
    - netsh wcn
    - netsh wfp
    - netsh winhttp
    - netsh winsock
    - netsh wlan
- netstat
- nfsadmin
- nfsshare
- nfsstat
- nlbmgr
- nltest
- nslookup
    - nslookup exit Command
    - nslookup finger Command
    - nslookup help
    - nslookup ls
    - nslookup lserver
    - nslookup root
    - nslookup server
    - nslookup set
    - nslookup set all
    - nslookup set class
    - nslookup set d2
    - nslookup set debug
    - nslookup set domain
    - nslookup set port
    - nslookup set querytype

    - nslookup set recurse
    - nslookup set retry
    - nslookup set root
    - nslookup set search
    - nslookup set srchlist
    - nslookup set timeout
    - nslookup set type
    - nslookup set vc
    - nslookup view
- ntbackup
- ntcmdprompt
- ntfrsutl

## O

- offline
    - offline disk
    - offline volume
- online
    - online disk
    - online volume
- openfiles

## P

- pagefileconfig
- path
- pathping
- pause
- pbadmin
- pentnt
- perfmon
- ping
- pktmon
- pnpunattend
- pnputil
- popd
- powershell
- powershell ise
- print

- prncnfg
- prndrvr
- prnjobs
- prnmngr
- prnport
- prnqctl
- prompt
- pubprn
- pushd
- pushprinterconnections
- pwlauncher
- pwsh

## Q

- qappsrv
- qprocess
- query
  - query process
  - query session
  - query termserver
  - query user
- quser
- qwinsta

## R

- rd
- rdpsign
- recover
- recover disk group
- refsutil
  - refsutil compression
  - refsutil dedup
  - refsutil fixboot
  - refsutil iometrics
  - refsutil leak
  - refsutil salvage
  - refsutil streamsnapshot
  - refsutil triage

- reg
  - reg add
  - reg compare
  - reg copy
  - reg delete
  - reg export
  - reg import
  - reg load
  - reg query
  - reg restore
  - reg save
  - reg unload
- regini
- regsvr32
- relog
- rem
- remove
- ren
- rename
- repadmin
- repair
  - repair bde
- replace
- rescan
- reset
  - reset session
- retain
- revert
- rexec
- risetup
- rmdir
- robocopy
- route ws2008
- rpcinfo
- rpcping
- rsh
- rundll32
- rundll32 printui
- rwinsta

## S

- san
- sc config
- sc create
- sc delete
- sc query
- schtasks
- scwcmd
  - scwcmd analyze
  - scwcmd configure
  - scwcmd register
  - scwcmd rollback
  - scwcmd transform
  - scwcmd view
- secedit
  - secedit analyze
  - secedit configure
  - secedit export
  - secedit generaterollback
  - secedit import
  - secedit validate
- select
  - select disk
  - select partition
  - select vdisk
  - select volume
- serverceipoptin
- servermanagercmd
- serverweroptin
- set environmental variables
- set shadow copy
  - set context
  - set id
  - setlocal
  - set metadata
  - set option
  - set verbose
- setlocal
- setspn
- setx

- sfc
- shadow
- shift
- showmount
- shrink
- shutdown
- simulate restore
- sort
- start
- subcommand set device
- subcommand set drivergroup
- subcommand set drivergroupfilter
- subcommand set driverpackage
- subcommand set image
- subcommand set imagegroup
- subcommand set server
- subcommand set transportserver
- subcommand set multicasttransmission
- subcommand start namespace
- subcommand start server
- subcommand start transportserver
- subcommand stop server
- subcommand stop transportserver
- subst
- sxstrace
- sysmon
- sysocmgr
- systeminfo

## T

- takeown
- tapicfg
- taskkill
- tasklist
- tcmsetup
- telnet
  - telnet close
  - telnet display
  - telnet open

    - telnet quit
    - telnet send
    - telnet set
    - telnet status
    - telnet unset
- tftp
- time
- timeout
- title
- tlntadmn
- tpmtool
- tpmvscmgr
- tracerpt
- tracert
- tree
- tscon
- tsdiscon
- tsecimp
- tskill
- tsprof
- type
- typeperf
- tzutil

## U

- unexpose
- uniqueid
- unlodctr

## V

- ver
- verifier
- verify
- vol
- vssadmin
    - vssadmin delete shadows
    - vssadmin list shadows
    - vssadmin list writers

    - vssadmin resize shadowstorage

## W

- waitfor
- wbadmin
    - wbadmin delete catalog
    - wbadmin delete systemstatebackup
    - wbadmin disable backup
    - wbadmin enable backup
    - wbadmin get disks
    - wbadmin get items
    - wbadmin get status
    - wbadmin get versions
    - wbadmin restore catalog
    - wbadmin start backup
    - wbadmin start recovery
    - wbadmin start sysrecovery
    - wbadmin start systemstatebackup
    - wbadmin start systemstaterecovery
    - wbadmin stop job
- wdsutil
- wecutil
- wevtutil
- where
- whoami
- winnt
- winnt32
- winrs
- winsat mem
- winsat mfmedia
- wmic
- writer
- wscript

## X

- xcopy

---

Last updated on 26/02/2026