



Guide d'administration

Amazon WorkSpaces



Amazon WorkSpaces: Guide d'administration

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que c'est WorkSpaces ?	1
Connect à l'aide d'une application cliente	3
Apportez votre propre licence (BYOL) de bureau Windows	4
Utilisation des licences de bureau Bring Your Own Windows dans WorkSpaces	5
Vidéos sur le téléchargement et la création d'images BYOL	20
Lier des comptes BYOL dans WorkSpaces	20
Messages d'erreur courants et solutions	21
Liste des messages SysPrep d'erreur et des corrections d'erreurs	28
Utiliser et gérer WorkSpaces Personal	30
WorkSpaces Options personnelles	31
Commencez avec WorkSpaces Personal	31
Créez un Workspace	41
Connectez-vous au Workspace	44
Étapes suivantes	45
Protocoles réseau et accès	46
Protocoles pour Amazon WorkSpaces	46
Exigences du VPC	48
AWS Accélérateur mondial (AGA)	53
Zones de disponibilité pour WorkSpaces	56
Exigences relatives aux adresses IP et aux ports	58
Exigences réseau	162
Appareils approuvés	165
Intégration SAML 2.0	168
Accès à l'identifiant Microsoft Entra	194
Authentification par carte à puce	197
Accès Internet	217
Groupes de sécurité	218
Groupes de contrôles d'accès IP	219
PCoClient IP zéro	223
Configurer Android pour Chromebook	224
Configuration de l'accès Web	224
Configuration d'Amazon WorkSpaces Thin Client	230
Configurer le chiffrement des points de terminaison FIPS	235
Activer les connexions SSH pour Linux WorkSpaces	237

Configuration requise et composants de service	244
Gérez les annuaires pour WorkSpaces	251
Enregistrer un Directory Service annuaire existant	253
Sélection d'une unité d'organisation	255
Configuration des adresses IP automatiques	256
Contrôle de l'accès aux appareils	257
Gestion des autorisations d'administrateur local	257
Mettre à jour le compte du connecteur AD (AD Connector)	258
Authentification multifactorielle (AD Connector)	258
Créer un annuaire	260
Mettre à jour les serveurs DNS pour WorkSpaces	287
Suppression d'un annuaire	295
Configuration de l'administration de l'annuaire	298
Administrer les utilisateurs	301
Gérer les utilisateurs	301
Création de plusieurs WorkSpaces pour un utilisateur	304
Personnalisez la façon dont les utilisateurs se connectent à leur WorkSpaces	305
Activez les fonctionnalités de WorkSpaces gestion en libre-service	308
Activation de l'optimisation audio d'Amazon Connect	311
Activation du chargement des journaux de diagnostic	314
Administrer le WorkSpaces personnel	316
Gérer Windows WorkSpaces	317
Gérez votre Amazon Linux 2 WorkSpaces	377
Gérez votre Ubuntu WorkSpaces	387
Gérez votre Rocky Linux WorkSpaces	396
Gérez votre Red Hat Enterprise Linux WorkSpaces	403
Optimisation pour la communication en temps réel	409
Gestion du mode d'exécution	423
Gestion des applications	426
Modifier un WorkSpace	434
Personnaliser la marque	442
Balisage des ressources	450
Maintenance	452
Chiffré WorkSpaces	454
Redémarrer un WorkSpace	465
Reconstruire un WorkSpace	466

Restaurer un WorkSpace	468
Microsoft 365 BYOL	470
Mettre à niveau Windows BYOL WorkSpaces	473
Migrer un WorkSpace	484
Supprimer un WorkSpace	493
Bundles et images	495
Options d'offres groupées	498
Création d'une image et d'un bundle personnalisés	504
Mise à jour d'un bundle personnalisé	526
Copie d'une image personnalisée	528
Partage ou annulation de partage d'une image personnalisée	531
Suppression d'un bundle ou d'une image personnalisés	534
Moniteur WorkSpaces personnel	535
Moniteur avec tableau CloudWatch de bord automatique	537
Surveiller à l'aide CloudWatch de métriques	539
Surveillez à l'aide d'Amazon EventBridge	554
Comprendre les événements de AWS connexion pour les utilisateurs de cartes à puce	558
Créez des CloudWatch tableaux de bord personnalisés	565
Continuité des activités	572
Redirection entre régions	573
Résilience multirégionale	591
Résolution des problèmes	601
Activation de la journalisation avancée	601
Résolution de problèmes spécifiques	606
Notes de mise à jour	640
Utiliser et gérer les WorkSpaces pools	651
Régions et zones de disponibilité prises en charge	651
Gérer les annuaires	654
Configurer SAML 2.0 et créer un répertoire de pool	655
Mise à jour des informations de l'annuaire	675
Supprimer un répertoire WorkSpaces Pools	679
Mise en réseau et accès	679
Accès Internet	679
Exigences du VPC	681
Configurer le chiffrement des points de terminaison FIPS	695
Points de terminaison d'un VPC Amazon S3	696

Connexions à votre VPC	696
Connexions utilisateur	699
Création d'un WorkSpaces pool	702
Administrer WorkSpaces les pools	705
Mode de course	706
Bundles	707
Modifier un pool	708
Suppression d'un groupe	708
Auto Scaling pour WorkSpaces piscines	708
Utilisation d'Active Directory	721
Domaines Active Directory	722
Avant de commencer	723
Authentification par certificat	725
Administration	733
Plus d'informations	740
Bundles et images	740
Options d'offres groupées	741
Création d'une image et d'un bundle personnalisés	745
Gérez des images et des ensembles personnalisés	761
Utiliser des scripts de session pour gérer l'expérience	762
WorkSpaces Pools de surveillance	773
WorkSpaces Métriques et dimensions des piscines	773
Administrer le stockage permanent	776
Administrer les dossiers de base	776
Activez la persistance des paramètres de l'application pour vos utilisateurs	784
Fonctionnement de la persistance des paramètres de l'application	784
Activer la persistance des paramètres de l'application	787
Gérez les paramètres de l'application VHDs pour vos utilisateurs	788
Codes de notification de dépannage	796
Sécurité	800
Protection des données	801
Chiffrement au repos	802
Chiffrement en transit	802
Gestion des identités et des accès	803
Exemples de politiques	804
Spécifier WorkSpaces les ressources dans une politique IAM	812

Création du rôle workspaces_ DefaultRole	818
Création du rôle AmazonWorkSpaces PCAAccess de service	820
AWS politiques gérées pour WorkSpaces	821
Accès aux instances de streaming WorkSpaces et scripts y afférents	829
Référence des autorisations relatives aux opérations sur Amazon WorkSpaces Console	834
Validation de conformité	842
Résilience	843
Sécurité de l'infrastructure	843
Isolement de réseau	844
Isolation sur les hôtes physiques	844
Credential Guard/Sécurité basée sur la virtualisation (VBS)	844
Autorisation des utilisateurs professionnels	845
Création et diffusion à partir de points de terminaison VPC d'interface	845
Effectuer des demandes d' WorkSpaces API Amazon via un point de terminaison d'interface VPC	850
Création d'une politique de point de terminaison VPC pour Amazon WorkSpaces	852
Connexion de votre réseau privé à votre VPC	853
Gestion des mises à jour	854
Quotas	855
WorkSpaces fin de vie du client	868
Versions du client non prises en charge	870
EOL FAQs	873
J'utilise une version d'un WorkSpaces client qui a atteint son EOL. Que dois-je faire pour passer à une version prise en charge ?	873
Puis-je utiliser une version du WorkSpaces client qui a atteint sa fin de vie avec une version compatible ? Workspace	873
J'utilise une version d'un WorkSpaces client qui a atteint son EOL. Puis-je tout de même signaler des problèmes à son sujet ?	874
J'utilise une version WorkSpaces client prise en charge sur un système d'exploitation qui a atteint sa fin de vie. Puis-je tout de même signaler des problèmes à son sujet ?	874
Guide du développeur du kit SDK d'extension	875
Historique de la documentation	876
Mises à jour antérieures	886
.....	dcccxc

Qu'est-ce qu'Amazon WorkSpaces ?

Amazon vous WorkSpaces permet de fournir des bureaux virtuels basés sur le cloud WorkSpaces destinés à vos utilisateurs. Ces ordinateurs de bureau peuvent exécuter Microsoft Windows, Amazon Linux 2, Ubuntu Linux, Rocky Linux ou Red Hat Enterprise Linux. WorkSpaces élimine le besoin d'acheter et de déployer du matériel ou d'installer des logiciels complexes. Vous pouvez rapidement ajouter ou supprimer des utilisateurs à mesure que vos besoins évoluent. Les utilisateurs peuvent accéder à leurs bureaux virtuels à partir de plusieurs appareils ou navigateurs web.

Amazon vous WorkSpaces permet de choisir entre WorkSpaces Personal et WorkSpaces Pools en fonction des besoins de votre organisation et des utilisateurs.

- **WorkSpaces Personnel** : choisissez WorkSpaces Personnel si vous avez besoin de bureaux virtuels permanents conçus pour les utilisateurs qui ont besoin d'un bureau hautement personnalisé réservé à leur usage exclusif. Cela ressemble à un ordinateur de bureau physique attribué à un individu. Pour de plus amples informations, veuillez consulter [Créez un WorkSpace in WorkSpaces Personal](#).
- **WorkSpaces Pool** : choisissez WorkSpaces Pool pour les bureaux virtuels non persistants conçus pour les utilisateurs qui ont besoin d'accéder à des environnements de bureau hautement sélectionnés hébergés sur une infrastructure éphémère. Pour de plus amples informations, veuillez consulter [Administrer WorkSpaces les pools](#).

Vous pouvez configurer WorkSpaces les ordinateurs de bureau de différentes manières :

- Choisissez parmi une gamme de configurations matérielles, de configurations logicielles et de AWS régions. Pour plus d'informations, consultez [Amazon WorkSpaces Bundles](#) et [the section called "Création d'une image et d'un bundle personnalisés"](#).
- Si vous utilisez Windows, vous pouvez apporter vos propres licences et applications ou les acheter AWS sur le Marketplace for Desktop Apps. WorkSpaces
- Si vous utilisez Windows 10 ou 11, vous pouvez associer votre WorkSpaces identifiant Microsoft Entra afin que vos utilisateurs puissent utiliser leurs informations d'identification Entra ID existantes pour accéder facilement aux applications Microsoft 365 pour entreprises. WorkSpaces Vous pouvez également vous inscrire à Intune pour gérer vos WorkSpaces bureaux virtuels à l'aide d'Intune. Pour de plus amples informations, veuillez consulter [Créez un répertoire Microsoft Entra ID dédié avec WorkSpaces Personal](#). Pour en savoir plus sur l'identifiant Microsoft Entra, voir

[Qu'est-ce que l'identifiant Microsoft Entra ?](#) . Pour en savoir plus sur Microsoft Intune, consultez [Microsoft Intune qui gère en toute sécurité les identités, gère les applications et gère les appareils](#).

- Choisissez un protocole PCo IP ou DCV. Pour de plus amples informations, veuillez consulter [Protocoles pour le WorkSpaces personnel](#).
- Créez un Microsoft Active Directory géré de manière autonome pour vos utilisateurs, ou connectez-vous WorkSpaces à votre Active Directory local afin que vos utilisateurs puissent utiliser leurs informations d'identification existantes pour accéder facilement aux ressources de l'entreprise. Pour de plus amples informations, veuillez consulter [the section called “Gérez les annuaires pour WorkSpaces”](#).
- Utilisez les mêmes outils de gestion WorkSpaces que ceux que vous utilisez pour gérer les bureaux sur site.
- Utilisez l'authentification multifactorielle (MFA) pour plus de sécurité.
- Utilisez AWS Key Management Service (AWS KMS) pour chiffrer les données au repos, les E/S du disque et les instantanés de volume.
- Choisissez les adresses IP que vos utilisateurs sont autorisés à utiliser pour accéder à leurs WorkSpaces.
- Choisissez une facturation mensuelle ou horaire pour WorkSpaces. Pour plus d'informations, consultez [Tarification d'WorkSpaces](#).

Pour plus d'informations sur l'utilisation WorkSpaces, voir :

- [WorkSpacesRessources Amazon](#) : inclut des livres blancs, des articles de blog, des webinaires et des sessions re:Invent
- [Mise en service de bureaux dans le cloud](#)
- [Bonnes pratiques pour le déploiement d'Amazon WorkSpaces](#)
- [Amazon WorkSpaces FAQs](#)
- Pour obtenir WorkSpaces des informations sur les prix et des exemples, consultez la section [WorkSpaces Tarification](#).

Connectez-vous à l' WorkSpaces aide d'une application cliente

Vous pouvez vous connecter à votre en WorkSpaces utilisant l'application client d'un appareil compatible via un navigateur Web compatible sur un système d'exploitation compatible.

Note

Vous ne pouvez pas utiliser de navigateur Web pour vous connecter à Amazon Linux WorkSpaces.

Il existe des applications client pour les appareils suivants :

- Ordinateurs Windows
- Ordinateurs macOS
- Ordinateurs Ubuntu Linux 18.04
- Chromebooks
- iPads
- Appareils Android
- Tablettes Fire
- Aucun appareil client (les appareils clients Teradici zéro ne sont pris en charge qu'avec PCo IP.)

Sous Windows, macOS et Linux PCs, vous pouvez utiliser les navigateurs Web suivants pour vous connecter à Windows et Ubuntu Linux WorkSpaces :

- Chrome 53 et versions ultérieures (Windows et macOS uniquement)
- Firefox 49 et versions ultérieures

Pour plus d'informations, consultez la section [WorkSpaces Clients](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Apportez vos propres licences de bureau Windows WorkSpaces

Si votre contrat de licence avec Microsoft le permet, vous pouvez apporter et déployer votre ordinateur de bureau Windows 10 ou 11 sur votre WorkSpaces. Pour cela, vous devez activer la fonctionnalité Apportez votre propre licence (BYOL) et fournir une licence Windows 10 ou 11 répondant aux exigences ci-dessous. Pour plus d'informations sur l'utilisation des logiciels Microsoft sur AWS, consultez [Amazon Web Services et Microsoft](#).

Pour rester conforme aux conditions de licence Microsoft, AWS exécutez votre BYOL WorkSpaces sur du matériel qui vous est dédié dans le AWS Cloud. En apportant votre propre licence, vous pouvez offrir une expérience cohérente à vos utilisateurs. Pour plus d'informations, consultez [Tarification d'WorkSpaces](#).

Important

La création d'images n'est pas prise en charge sur les systèmes Windows 11 qui ont été mis à niveau d'une version de Windows 11 vers une version plus récente de Windows 11 (mise à niveau des fonctionnalités/versions de Windows). Par exemple, un système Windows 11 23H2 mis à niveau vers 24H2 ne peut pas être utilisé pour créer une image. Toutefois, les mises à jour cumulatives ou de sécurité de Windows sont prises en charge par le processus de WorkSpaces création d'images.

Rubriques

- [Utilisation des licences de bureau Bring Your Own Windows dans WorkSpaces](#)
- [Vidéos sur le téléchargement et la création d'images BYOL](#)
- [Lier des comptes BYOL dans WorkSpaces](#)
- [Messages d'erreur courants et solutions](#)
- [Liste des messages SysPrep d'erreur et des corrections d'erreurs](#)

Utilisation des licences de bureau Bring Your Own Windows dans WorkSpaces

Suivez les étapes ci-dessous pour importer et utiliser votre propre licence de bureau Windows sur Amazon WorkSpaces

Conditions préalables à l'utilisation de Windows BYOL avec Amazon WorkSpaces

Avant de commencer, vérifiez les éléments suivants :

- Votre contrat de licence Microsoft autorise l'exécution de Windows dans un environnement hébergé virtuel.
- Si vous utilisez des non-GPU-enabled offres groupées, assurez-vous d'en utiliser un minimum de 50 WorkSpaces par région, quelle que soit la combinaison AlwaysOn de AutoStop configurations. Ce minimum est requis pour fonctionner WorkSpaces sur du matériel dédié, ce qui est nécessaire pour se conformer aux exigences de licence Microsoft. Le matériel dédié est provisionné par AWS, de sorte que votre VPC peut rester en location par défaut.

Si vous prévoyez d'utiliser des offres dotées d'un processeur graphique, assurez-vous d'exécuter au moins 4 AlwaysOn ou 20 offres AutoStop compatibles GPU par région et WorkSpaces par mois sur du matériel dédié.

Note

Tenez compte des points suivants lors de l'importation d'images BYOL :

- Les forfaits compatibles GPU ne sont pas disponibles dans la région Afrique (Le Cap) et dans la région Israël (Tel Aviv).
- Dans le cadre du processus d'importation d'images, extrait AWS automatiquement les journaux système pour résoudre les erreurs d'importation d'images, fournir une aide au dépannage et fournir des messages d'erreur précis aux utilisateurs.
- Les forfaits compatibles GPU ne sont pas disponibles dans la région Afrique (Le Cap) et dans la région Israël (Tel Aviv).
- Pour courir votre course WorkSpaces dans la région Afrique (Cape Town), vous devez courir un minimum de 400 WorkSpaces dans la région Afrique (Cape Town).
- Les packs Value ne sont pas disponibles pour Windows 11 et WorkSpaces Pools. Pour plus d'informations sur la migration de votre offre groupée de valeur existante, WorkSpaces consultez [Migrer un Workspace dans WorkSpaces Personal](#).

- Pour une expérience de visioconférence optimale, nous vous recommandons d'utiliser des packs Power (4 vCPU, 16 Go de mémoire ou plus).
- WorkSpaces peut utiliser une interface de gestion dans la plage d'adresses IP /16. L'interface de gestion est connectée à un réseau WorkSpaces de gestion sécurisé utilisé pour le streaming interactif. Cela permet WorkSpaces de gérer votre WorkSpaces. Pour de plus amples informations, veuillez consulter [Interfaces réseau](#). À cette fin, vous devez réserver un masque réseau /16 à partir d'au moins l'une des plages d'adresses IP suivantes et vous assurer que la plage d'adresses IP que vous avez choisie n'entre pas en conflit sur votre réseau :
 - 10.0.0.0/8
 - 100.64.0.0/10
 - 172.16.0.0/12
 - 192.168.0.0/16
 - 198.18.0.0/15

 Note

- Au fur et à mesure que vous adoptez le WorkSpaces service, les plages d'adresses IP de l'interface de gestion disponibles changent fréquemment. Pour déterminer les plages actuellement disponibles, exécutez la commande [list-available-management-cidr-ranges](#) AWS Command Line Interface (AWS CLI).
- Outre le bloc CIDR /16 que vous sélectionnez, la plage d'adresses IP 54.239.224.0/20 est utilisée pour le trafic de l'interface de gestion dans toutes les régions. AWS

Accès S3

Si vous utilisez des périmètres de données pour contrôler l'accès à Amazon S3 dans votre environnement, vous devrez peut-être autoriser explicitement l'accès aux compartiments Amazon S3 qui stockent les composants gérés par EC2 Image Builder. Vous pouvez utiliser l'ARN ou l'URL du compartiment pour autoriser la mise en liste de ces compartiments, en fonction de la manière dont vous contrôlez l'accès à Amazon S3.

Accès requis pour les scripts de démarrage de gestion des composants Amazon EC2 Image Builder :

- ARN du compartiment S3 : `arn:<AWS partition>:s3::ec2imagebuilder-managed-resources-<AWS Region>-prod`

- URL du compartiment S3 : `https://ec2imagebuilder-managed-resources-<AWS Region>.s3.<AWS Region>.<AWS partition-specific domain name>`

Accès requis pour les composants gérés par Amazon EC2 Image Builder :

- ARN du compartiment S3 : `arn:<AWS partition>:s3::ec2imagebuilder-toe-<AWS Region>-prod`
- URL du compartiment S3 : `https://ec2imagebuilder-toe-<AWS Region>.s3.<AWS Region>.<AWS partition-specific domain name>`

Connectivité réseau

Si vous utilisez un proxy pour filtrer les communications sortantes (comme AWS Network Firewall) depuis votre compte AWS indiquant que vous importez une image BYOL, assurez-vous que les points de terminaison HTTPS suivants sont accessibles :

Accès requis pour le composant Amazon EC2 Image Builder :

- `ssm.<region>.amazonaws.com`
- `ssmmessages.<region>.amazonaws.com`
- `ec2messages.<region>.amazonaws.com`
- `imagebuilder.<region>.amazonaws.com`
- `ec2.<region>.amazonaws.com`
- `s3.<region>.amazonaws.com`
- `s3.us-east-1.amazonaws.com`
- `tools.amazonworkspaces.com`
- `go.microsoft.com`
- `definitionupdates.microsoft.com`
- `time.windows.com`

La liste ci-dessus n'est pas exhaustive et il est recommandé d'utiliser un VPC disposant d'un accès public à Internet. Le processus d'importation d'images ne prend pas en charge VPCs l'utilisation d'AWS PrivateLink.

Versions Windows prises en charge pour BYOL

Votre machine virtuelle doit être exécutée sur l'une des versions Windows suivantes :

- Windows 10 version 22H2 (mise à jour de novembre 2022)
- Windows 10 Entreprise LTSC 2019 (1809)
- Windows 10 Entreprise LTSC 2021 (21H2)
- Windows 11 Entreprise LTSC 2024 (24H2)
- Windows 11 Enterprise 22H2 (version d'octobre 2022)
- Windows 11 Entreprise 23H2 (version d'octobre 2023)
- Windows 11 Enterprise 24H2 (version d'octobre 2024)
- Windows 11 Enterprise 25H2 (version de septembre 2025)

Vous aurez besoin d'une image de machine virtuelle Windows ou d'un fichier image ISO Windows qui utilise une version compatible du système d'exploitation Windows :

- Téléchargez une image ISO de l'édition Enterprise en vous connectant au [centre d'administration Microsoft 365](#). Connectez-vous à votre abonnement sur le [portail des abonnements Visual Studio pour connaître](#) les téléchargements disponibles. N'utilisez pas de fichier ISO téléchargé depuis le [site Web public de téléchargement de Windows 11](#) qui ne fournit pas d'ISO pour l'édition Enterprise.
- Pour utiliser une image de machine virtuelle personnalisée, [validez votre image](#) avant de l'importer.
- AMIs Les données chiffrées ne sont pas prises en charge dans le processus d'importation. Le chiffrement peut être activé après le provisionnement de WorkSpaces la version finale.
- Le chiffrement EBS par défaut n'est pas pris en charge. Avant d'importer une image, [désactivez le chiffrement par défaut dans la console EC2](#).
- Pour les images Windows 11, le WorkSpaces mode de démarrage UEFI doit être activé. Pour plus d'informations sur la façon dont EC2 Image Builder détecte le mode de démarrage, [consultez la section Types de volumes et systèmes de fichiers pris en charge par VM](#) Import/Export dans le guide de l' Import/Export utilisateur de VM.
- Toutes les versions de système d'exploitation prises en charge prennent en charge tous les types de calcul disponibles dans la AWS région que vous utilisez WorkSpaces. Les versions de Windows qui ne sont plus prises en charge par Microsoft ne sont pas garanties de fonctionner et ne sont pas prises en charge par le AWS Support.

 Note

Les versions Windows 10 N et Windows 11 N ne sont actuellement pas prises en charge pour BYOL.

Étape 1 : Activez votre compte pour BYOL

Après avoir confirmé que vous remplissez les conditions requises pour utiliser Windows BYOL avec WorkSpaces, vous devez autoriser votre compte à utiliser des images BYOL.

1. Dans la WorkSpaces console, accédez à la page Paramètres du compte.
2. Dans la section Bring Your Own License (BYOL), le statut d'activation du BYOL de votre compte est affiché. Si le statut indique que votre compte n'est pas activé, cliquez sur le bouton Commencer avec BYOL.
3. Sur la page BYOL, choisissez Activer le compte pour BYOL.

 Note

L'activation de votre compte pour BYOL ne s'applique qu'à une seule région. Notez dans quelle région vous vous trouvez actuellement, et si vous souhaitez utiliser une autre région, passez à cette région avant d'activer votre compte.

4. Une fenêtre contextuelle apparaît pour confirmer que vous comprenez les exigences minimales pour utiliser le WorkSpaces BYOL. Confirmez que vous avez bien compris les exigences et choisissez Activer le compte.

 Note

Si vous envisagez d'utiliser Graphics WorkSpaces avec BYOL, créez un ticket AWS Support. L'activation du BYOL graphique n'est pas encore prise en charge par le biais de la WorkSpaces console.

5. Dans la plupart des cas, les comptes sont automatiquement activés. Cependant, certains comptes nécessitent un examen supplémentaire. L'état d'activation est affiché sur la page BYOL une fois actualisée.
6. Lorsque votre compte est activé pour BYOL, passez à l'étape suivante.

(Facultatif) Validez votre image avant de l'importer

Note

Cette étape s'applique uniquement aux images de machine virtuelle personnalisées qui vont être importées. Si vous importez une image ISO Windows, vous pouvez ignorer cette étape.

Si vous importez une image de machine virtuelle personnalisée, nous vous recommandons d'exécuter l'outil WorkSpaces Image Checker pour vous assurer que votre machine virtuelle est compatible avec WorkSpaces. L'outil Image Checker exécute une série de tests et peut aider à résoudre les problèmes de compatibilité.

Pour télécharger le script du vérificateur de compatibilité des images

Avant de télécharger et d'exécuter le script Image Compatibility Checker, vérifiez que les dernières mises à jour de sécurité Windows sont installées sur votre machine virtuelle. Au cours de son exécution, ce script désactive le service Windows Update.

1. Téléchargez le fichier .zip du script Image Compatibility Checker depuis le fichier [ImageCompatibilityChecker.zip](#) dans votre dossier. Downloads
2. Dans votre dossier Downloads, créez un dossier BYOL.
3. Récupérez les fichiers dans ImageCompatibilityChecker.zip et copiez-les dans le dossier Downloads\BYOL.
4. Supprimez le dossier Downloads\ImageCompatibilityChecker.zip afin de ne conserver que les fichiers récupérés.

Vérifiez que la machine virtuelle Windows n'est pas activée avec BitLocker.

Assurez-vous que la machine virtuelle Windows n'est pas activée avec BitLocker

1. Ouvrez Powershell en tant qu'administrateur.
2. Exécutez la commande suivante :

```
manage-bde -off DriveLetter:
```

3. Vérifiez l'état de BitLocker en exécutant cette commande :

```
manage-bde -Status DriveLetter:
```

4. Assurez-vous que les valeurs affichées correspondent à celles-ci :

- BitLocker Version — Aucune
- État de la conversion — Entièrement déchiffré
- Pourcentage crypté : 0,0 %
- Méthode de chiffrement — Aucune
- État de protection — Protection désactivée
- État du verrouillage — Déverrouillé

Procédez comme suit pour exécuter le script Image Compatibility Checker.

Pour exécuter le script Image Compatibility Checker

1. Ouvrez Powershell en tant qu'administrateur.
 1. Sélectionnez le bouton Démarrer de Windows.
 2. Cliquez avec le bouton droit sur Windows PowerShell
 3. Choisissez Exécuter en tant qu'administrateur.
 4. Si le Contrôle de compte utilisateur vous le demande, choisissez Oui.
2. À l'invite de PowerShell commande, accédez au répertoire dans lequel se trouve le script Image Compatibility Checker. Par exemple, si le script se trouve dans le répertoire Downloads\BYOL, entrez les commandes suivantes, puis appuyez sur Entrée :

```
cd C:\Users\username\Downloads\BYOL
```

3. Entrez la commande suivante pour mettre à jour la politique PowerShell d'exécution sur l'ordinateur. Cela permet au script Image Compatibility Checker de s'exécuter :

```
Set-ExecutionPolicy AllSigned
```

4. Lorsque vous êtes invité à confirmer si vous souhaitez modifier la politique PowerShell d'exécution, entrez A pour spécifier Oui à tous.
5. Entrez la commande suivante pour exécuter le script Image Compatibility Checker :

```
.\ImageCompatibilityChecker.exe
```

6. Si une notification de sécurité s'affiche, appuyez sur la touche R pour l'exécuter une seule fois.
7. Dans la boîte de dialogue de validation d'WorkSpaces image, choisissez Run Tests.
8. Lorsqu'un test est terminé, vous pouvez en afficher le statut. Si un test affiche le statut FAILED (ÉCHEC), choisissez Info (Informations) pour afficher de plus amples informations sur la manière de résoudre le problème qui a provoqué l'échec. Si des tests affichent le statut WARNING (AVERTISSEMENT), choisissez le bouton Fix all Warnings (Corriger tous les avertissements).
9. Le cas échéant, résolvez l'ensemble des problèmes qui entraînent soit l'échec des tests soit des avertissements, et répétez les étapes [Step 7](#) et [Step 8](#) jusqu'à ce que la machine virtuelle réussisse tous les tests. Tous les échecs et avertissements doivent être résolus avant d'exporter la machine virtuelle.
10. Le contrôleur du script BYOL génère deux fichiers journaux, WorkSpacesImageCompatibilityCheckLog`YYYY-MM-DD_HHmmss`.txt et ImageInfo.txt. Ces fichiers se trouvent dans le répertoire qui contient les fichiers de script du vérificateur de compatibilité des images.

 Tip

Ne supprimez pas ces fichiers. Si un problème se produit, ces fichiers peuvent être utiles pour le résoudre.

11. Une fois que votre machine virtuelle a passé tous les tests, vous obtenez un message Validation Successful (Validation réussie).

Vous serez également invité à exécuter Sysprep. Fermez l'invite et n'exécutez pas encore Sysprep.

12. Arrêtez la machine virtuelle et exportez-la. Pour plus d'informations, voir [Exporter votre machine virtuelle depuis son environnement de virtualisation](#) dans le guide de l'Import/Export utilisateur de la machine virtuelle.
13. (Facultatif) Démarrez la machine virtuelle et exécutez à nouveau le script Image Compatibility Checker. Toutes les validations devraient réussir. Un écran s'affichera à nouveau avec un bouton permettant d'exécuter Sysprep. Choisissez Run Sysprep. Si Sysprep réussit, la machine virtuelle que vous avez exportée à partir de l'étape 12 peut être importée dans Amazon Elastic Compute Cloud (Amazon EC2).

Si Sysprep échoue, consultez les journaux Sysprep dans le %WINDIR%\System32\Sysprep\Panther chemin, revenez à la machine virtuelle exportée à partir de l'étape 12, résolvez les

problèmes signalés et complétez à nouveau l'étape 12 en exportant la machine virtuelle corrigée. Vous exécuterez ensuite à nouveau le script Image Compatibility Checker pour vous assurer que les problèmes ont été résolus.

La raison la plus courante d'une défaillance de Sysprep est que les packages Modern AppX n'ont pas été désinstallés pour tous les utilisateurs. Utilisez l'`Remove-AppxPackage` PowerShell applet de commande pour supprimer les packages AppX.

14. Importez la machine virtuelle que vous avez exportée à l'étape 12 dans Amazon EC2.

Étape 2 : créer une image BYOL à l'aide WorkSpaces de la console

Procédez comme suit pour importer votre image et créer une image WorkSpaces BYOL :

1. Accédez au volet de navigation et choisissez Images, puis Importer une image.
2. Suivez les étapes de la page Importer une image en fonction de l'option d'image de base et du type d'image que vous souhaitez importer :
 - Importation de machine virtuelle — Importe une image de machine virtuelle déjà personnalisée. Vous pouvez importer un OVF fichier VHDXVMDK, ou.
 - Importation ISO — Importe une image ISO Windows que vous avez téléchargée auprès de Microsoft et qui n'a pas été personnalisée.
 - Importation d'AMI — Importe une AMI Amazon EC2 existante à utiliser comme image WorkSpaces BYOL.
3. Effectuez l'une des actions suivantes :
 - Pour l'option d'importation de machines virtuelles, téléchargez votre fichier sur Amazon S3, puis spécifiez l'emplacement du fichier à importer. Notez que le compartiment S3 que vous utilisez doit se trouver dans la même région que celle dans laquelle vous souhaitez déployer BYOL WorkSpaces.
 - Pour l'importation ISO, importez une image ISO Windows que vous avez téléchargée auprès de Microsoft et qui n'a pas été personnalisée. Notez que le compartiment S3 que vous utilisez doit se trouver dans la même région que celle dans laquelle vous souhaitez déployer BYOL WorkSpaces.
 - Pour l'importation d'AMI, spécifiez l'ID de l'AMI.
4. Accédez à Configuration de l'infrastructure.

WorkSpaces crée automatiquement un pipeline Amazon EC2 Image Builder pour créer votre image BYOL. La configuration de l'infrastructure définit la manière dont EC2 Image Builder est configuré pour créer votre image. Vous pouvez le personnaliser à l'aide des paramètres suivants :

- Valeurs par défaut du service : crée et utilise un rôle et une politique IAM par défaut pour créer votre image.
 - Utiliser une configuration d'infrastructure existante : propose une sélection de configurations d'infrastructure personnalisées configurées dans Amazon EC2 Image Builder. Pour plus d'informations, consultez la section [Création d'une configuration d'infrastructure](#) dans le guide de l'utilisateur d'EC2 Image Builder.
5. Accédez aux paramètres avancés et sélectionnez si vous souhaitez mettre fin à l'instance de build EC2 si votre image rencontre des erreurs d'importation.
- Si vous choisissez de mettre fin à l'instance en cas d'échec, vous ne pourrez pas accéder à l'instance pour corriger les erreurs pendant le flux de travail d'importation d'images.
 - Si vous choisissez de ne pas mettre fin à l'instance, celle-ci peut être utilisée pour corriger les erreurs, mais l'exécution de l'instance EC2 peut entraîner des coûts supplémentaires.
6. Accédez à Détails de l'image pour définir les propriétés de votre image : y compris le nom de l'image.
- Nom de l'image — Identifiant unique de votre image.
 - Type de calcul — Spécifiez si cette image doit utiliser du matériel non graphique/de base ou du matériel graphique
 - Version du système d'exploitation — Choisissez la version du système d'exploitation Windows de l'image
 - Version sémantique : définissez une version sémantique pour l'image, qui sera stockée dans EC2 Image Builder. Pour plus d'informations, consultez la section Gestion des [versions sémantiques dans Image Builder](#) dans le guide de l'utilisateur d'EC2 Image Builder

 Note

Au cours du processus d'importation BYOL, les ressources EC2 Image Builder seront créées dans AWS votre compte. Afin de créer l'image, un rôle lié à un service nommé `AWSServiceRoleForImageBuilder` est automatiquement créé s'il n'existe pas déjà. Ce

rôle contiendra la politique AWS gérée [AWSServiceRoleForImageBuilder](#). Vous devez également disposer des [autorisations requises pour que VM Import/Export puisse](#) importer une image de machine virtuelle personnalisée.

Pendant la création de votre image, le statut sur la page Images de la console apparaît comme En attente. Le processus d'ingestion BYOL prend au moins 90 minutes.

Les erreurs survenant lors de l'importation de votre image apparaîtront sur la page Images avec les résolutions suggérées. Les journaux détaillés se trouvent sur Amazon CloudWatch dans le groupe de journaux Image Builder créé lors de l'importation de votre image. Les types d'erreur possibles sont les suivants :

- Erreurs d'image — L'image n'a pas pu être créée par EC2 Image Builder. Corrigez les problèmes dans votre environnement de virtualisation et importez une nouvelle image.
- Erreurs d'Image Builder : une erreur s'est produite lors de la tentative de création de votre image. Consultez les journaux Image Builder sur Amazon CloudWatch pour plus de détails
- Erreurs EC2 : votre image présente des problèmes qui n'ont pas pu être résolus automatiquement. Pour résoudre ces erreurs, vous pouvez vous connecter à l'instance Amazon EC2 si elle a été configurée pour ne pas s'arrêter en cas d'échec de compilation et effectuer directement les corrections. Vous pouvez ensuite réessayer l'importation depuis la page Images.
- Erreurs corrigées automatiquement — Ces problèmes ont été automatiquement corrigés par WorkSpaces Aucune action supplémentaire n'est requise.

Pour obtenir des informations détaillées sur les erreurs courantes, consultez la section [Messages d'erreur courants et leurs solutions](#).

Étape 3 : Choisissez la plage d'adresses IP pour votre interface de gestion BYOL

BYOL WorkSpaces fonctionne sur du matériel dédié afin de respecter les conditions de licence Microsoft. Pour ce faire, une interface de gestion BYOL est créée afin d'établir une connexion sécurisée entre vous WorkSpaces et le réseau de WorkSpaces gestion AWS géré. Pour en savoir plus, consultez [Interfaces réseau](#).

Si vous avez un autre AWS compte activé pour le BYOL dans la même région, vous devez utiliser la même interface de gestion pour tous les comptes afin de réserver moins d'adresses IP. Pour ce faire, ne choisissez pas une plage d'adresses IP d'interface de gestion et consultez la section Lier les comptes BYOL ci-dessous.

Choix d'une plage d'adresses IP d'interface de gestion

1. Retournez à la page BYOL dans les paramètres du compte.
2. Dans la section Choisir une plage d'adresses IP, sélectionnez le bouton Choisir une plage d'adresses IP.
3. Entrez une plage de recherche en fournissant une plage d'adresses IP disponible sur votre réseau. WorkSpaces renvoie les plages d'adresses IP de masque réseau /16 disponibles qui correspondent à votre recherche.
4. Choisissez une plage d'adresses IP disponible (affichée sous forme de blocs CIDR).

Note

Une fois que vous avez choisi la plage d'adresses IP pour votre interface de gestion, elle ne peut pas être modifiée.

Lier des comptes BYOL

Si vous avez un autre AWS compte activé pour le BYOL dans la même région, qui partage le même compte payeur, vous devez utiliser la même interface de gestion pour tous les comptes afin de réserver moins d'adresses IP. Le fait de lier des comptes évite également d'avoir à respecter les exigences BYOL minimales pour chaque compte, car l'exigence minimale est partagée entre les comptes liés. Si aucun autre compte n'est déjà activé pour BYOL sous le même compte payeur, ignorez cette procédure.

Pour créer un lien vers un compte BYOL existant, ne sélectionnez pas de plage d'adresses IP.

Lier des comptes BYOL

1. Connectez-vous au AWS compte qui est déjà activé pour BYOL WorkSpaces.
2. Accédez à la page BYOL dans les paramètres du compte.
3. Dans la section Choisir une plage d'adresses IP, sélectionnez le bouton Envoyer une invitation dans la section Liaison de comptes.
4. Indiquez l'identifiant du AWS compte qui n'est pas activé pour BYOL et vers lequel vous souhaitez créer un lien.

 Note

Les deux comptes doivent utiliser BYOL dans la même région.

5. Une fois l'invitation à créer un lien envoyée, revenez au AWS compte qui n'est pas encore activé pour BYOL. Sur la page des paramètres du compte, vous verrez une bannière de notification indiquant que vous avez une invitation à associer un compte BYOL en attente. Choisissez Afficher l'invitation dans la bannière.
6. Confirmez l'invitation à associer le compte.

Si vous souhaitez utiliser une interface de gestion différente pour deux comptes associés au même compte payeur, contactez le AWS Support pour obtenir de l'aide.

Étape 4 : Créez un bundle personnalisé à partir de l'image BYOL dans WorkSpaces

Après avoir créé votre image BYOL en suivant les instructions de la section, vous pouvez utiliser l'image pour créer un bundle personnalisé. Pour plus d'informations, voir [Création d'une WorkSpaces image personnalisée et d'un bundle pour WorkSpaces Personal](#).

Étape 5 : créer un répertoire dédié pour Amazon WorkSpaces

Pour utiliser des images BYOL pour WorkSpaces, vous devez créer un répertoire à cette fin.

Pour créer un répertoire pour WorkSpaces, voir [Créer un répertoire pour WorkSpaces Personal](#). Assurez-vous de choisir Enable Dedicated WorkSpaces lors de la création du répertoire.

 Important

Si l' WorkSpaces option Enabled Dedicated ne s'affiche pas lors de l'enregistrement de l'annuaire, assurez-vous d'avoir suivi les étapes d'activation du BYOL dans votre compte et dans votre région.

Si vous avez déjà enregistré un annuaire Microsoft AD AWS géré ou un répertoire AD Connector WorkSpaces qui ne s'exécute pas sur du matériel dédié, vous pouvez configurer un nouveau répertoire Microsoft AD AWS géré ou un répertoire AD Connector à cette fin. Vous pouvez également désenregistrer le répertoire, puis le réenregistrer en tant que répertoire dédié. WorkSpaces Pour en savoir plus sur l'enregistrement et le

désenregistrement d'un annuaire de services d' AWS annuaire existant, voir [Enregistrer un annuaire de service d' AWS annuaire existant auprès de Personal. WorkSpaces](#)

Étape 6 : Lancez votre BYOL WorkSpaces

Lancez votre BYOL Personal WorkSpaces

Pour lancer un compte personnel WorkSpaces, voir [Créer un compte Workspace dans WorkSpaces Personnel](#).

Lancez votre pool BYOL WorkSpaces

Pour lancer un WorkSpaces pool, vous devez lancer un pool Workspace, créer une image de celui-ci Workspace, puis utiliser cette image pour lancer un pool.

Pour créer une image pour les pools BYOL WorkSpaces

1. Lancez une image personnelle Workspace avec l'image BYOL que vous souhaitez utiliser pour vos WorkSpaces pools. Pour plus d'informations sur le lancement de WorkSpaces Personnel, voir [Créer un Workspace dans WorkSpaces Personnel](#).
2. Connectez-vous au compte personnel Workspace et assurez-vous que toutes les mises à jour Windows sont installées.
3. Mettez à jour vos configurations Amazon EC2. Pour mettre à jour vos configurations EC2 à l'aide de Windows 10, voir [Installer la dernière version d'EC2Config](#). Pour mettre à jour vos configurations EC2 à l'aide de Windows 11, voir [Installer la dernière version de EC2 Launch](#).
4. Ajoutez une liste d'exclusion de Windows Defender. Pour plus d'informations, voir [Ajouter une exclusion à la sécurité Windows](#).

Ajoutez les dossiers suivants à la liste d'exclusion dans Windows Defender :

- C:\Program Files\Amazon\
- C:\ProgramData\Amazon*
- C:\Program Files\NICE\
- C:\ProgramData\NICE\
- C:\Program Files (x86)\AWS Tools*
- C:\Program Files (x86)\AWS SDK for .NET*
- C:\AWSEUC\ (Ceci est pour le script de session)

5. Désactivez Windows Update au démarrage en saisissant la commande suivante.
6. Ouvrez Powershell en tant qu'administrateur.
 1. Sélectionnez le bouton Démarrer de Windows.
 2. Cliquez avec le bouton droit sur Windows PowerShell
 3. Choisissez Exécuter en tant qu'administrateur.
 4. Si le Contrôle de compte utilisateur vous le demande, choisissez Oui.
7. Exécutez les commandes suivantes :

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Force
```

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Force
```

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU"  
-Name "NoAutoUpdate" -Value 1 -Force
```

8. Redémarrez le WorkSpace. Pour plus d'informations, voir Redémarrer un WorkSpace dans WorkSpaces Personal.

Note

Nous vous recommandons de procéder comme suit avant de commencer à créer une image pour les WorkSpaces pools BYOL.

- Supprimez les applications de démarrage inutiles.
- Supprimez ou désactivez les tâches planifiées inutiles. Ouvrez le menu Démarrer, choisissez Tâches planifiées, sélectionnez les tâches que vous souhaitez désactiver, puis sélectionnez Désactiver.

9. Exécutez le vérificateur d'image après le redémarrage en saisissant la commande suivante.

```
C:\Program Files\Amazon\ImageChecker.exe
```

10. Résolvez toutes les erreurs détectées par le vérificateur d'image. Pour plus d'informations, consultez la section Conseils pour résoudre les problèmes détectés par le vérificateur d'images.
11. Une fois que tous les tests ont passé avec succès le vérificateur d'image, revenez à la WorkSpaces console.

12. Dans le volet de navigation, sous WorkSpaces, choisissez Personnel. Choisissez le BYOL personnel WorkSpaces, puis choisissez Actions, Créer une image.
13. Dans le volet de navigation, choisissez Images. Sous Images, vérifiez si l'image est créée.

Vous pouvez désormais lancer WorkSpaces Pools avec l'image que vous avez créée. Pour plus d'informations sur le lancement de WorkSpaces pools, consultez la section Créer un WorkSpaces pool.

Vidéos sur le téléchargement et la création d'images BYOL

Pour une démonstration sur le téléchargement d'images BYOL, regardez les vidéos suivantes.

Pour une démonstration sur la création d'images BYOL avec Microsoft Hyper-V, regardez la vidéo suivante.

Pour une démonstration sur la création d'images BYOL avec VMware Workstation, regardez la vidéo suivante.

Lier des comptes BYOL dans WorkSpaces

Vous pouvez utiliser la liaison BYOL pour lier des comptes et partager des configurations BYOL. Les configurations BYOL incluent la plage CIDR utilisée par vos comptes et les images que vous utilisez pour créer WorkSpaces avec votre licence Windows. Tous les comptes liés partagent la même infrastructure matérielle sous-jacente.

Le compte activé pour la liaison BYOL est le propriétaire principal de l'infrastructure matérielle sous-jacente et est appelé compte source. Le compte Source gère l'accès à l'infrastructure matérielle sous-jacente. Les comptes cibles sont les comptes liés au compte source.

Important

APIs pour BYOL, les liens entre comptes ne sont pas disponibles dans le AWS GovCloud (US) Region.

 Note

Les AWS comptes auxquels vous souhaitez établir un lien doivent faire partie de votre organisation et appartenir au même compte payeur. Vous ne pouvez associer que des comptes au sein d'une même région.

Pour associer les comptes source et cible

1. Envoyez un lien d'invitation depuis votre compte Source vers le compte Target à l'aide de l'[CreateAccountLinkInvitation](#) API.
2. Acceptez le lien en attente depuis votre compte Target à l'aide de l'[AcceptAccountLinkInvitation](#) API.
3. Vérifiez que le lien a été établi à l'aide de l'[ListAccountLinks](#) API [GetAccountLink](#) or.

Messages d'erreur courants et solutions

L'importation BYOL ne prend pas en charge les systèmes sur lesquels Microsoft Office autonome actif est installé. L'importation BYOL permet uniquement aux applications Microsoft Office 365 d'être présentes sur la source avant de démarrer le processus d'importation.

Microsoft Office autonome (autre que Microsoft Office 365) doit être désinstallé avant l'importation. Pour plus d'informations, consultez [Désinstaller Office d'un PC](#).

L'importation BYOL nécessite un système sans agent PCo IP.

Désinstallez l'agent PCo IP. Pour plus d'informations sur la désinstallation de l'agent PCo IP, voir [Désinstaller le client logiciel Teradici PCo IP pour Mac](#)

L'importation BYOL requiert que les mises à jour Windows soient désactivées.

Désactivez les mises à jour Windows en effectuant les étapes suivantes :

1. Appuyez sur la touche Windows + R. Tapez `services.msc`, puis appuyez sur Entrée.
2. Cliquez avec le bouton droit sur Windows Update, puis sélectionnez Propriétés.
3. Dans l'onglet Général, définissez le type de démarrage à Désactivé.

4. Choisissez Arrêter.
5. Cliquez sur Appliquez, puis sur OK.
6. Redémarrez votre ordinateur.

L'importation BYOL nécessite l'activation du montage automatique.

Vous devez activer le montage automatique. Exécutez la commande suivante dans PowerShell en tant qu'administrateur :

```
C:\> diskpart  
DISKPART> automount enable
```

Le montage automatique de nouveaux volumes est activé.

L'importation BYOL nécessite l'activation du compte WorkSpaces _BYOL

WorkSpacesLe compte _BYOL doit être activé. Pour plus d'informations, consultez [Activer le BYOL pour votre compte BYOL à l'aide de la console Amazon WorkSpaces](#).

L'importation BYOL nécessite que l'interface réseau utilise le protocole DHCP pour attribuer automatiquement une adresse IP. L'interface réseau utilise actuellement une adresse IP statique.

L'interface réseau doit être modifiée pour utiliser le protocole DHCP. Pour plus d'informations, consultez la section [Modifier TCP/IP les paramètres](#).

L'importation BYOL nécessite plus de 20 Go d'espace disponible sur le disque local.

Le disque local doit disposer de suffisamment d'espace. Vous devez donc libérer au moins 20 Go d'espace.

L'importation BYOL nécessite des systèmes disposant d'un seul lecteur local. Il existe des lecteurs locaux, amovibles ou réseau supplémentaires.

Seul le lecteur C peut être présent sur une image machine Amazon utilisée pour importer une WorkSpace image BYOL. Retirez tous les autres lecteurs, y compris les lecteurs virtuels.

L'importation BYOL nécessite Windows 10 ou Windows 11.

Utilisez un système d'exploitation Windows 10 ou Windows 11.

L'importation BYOL nécessite des systèmes qui ne sont pas associés à un domaine AD.

Le système doit être dissocié du domaine AD. Pour plus d'informations, consultez [FAQ sur la gestion des périphériques Azure Active Directory](#).

L'importation BYOL nécessite des systèmes qui ne sont pas associés au domaine Azure.

Le système doit être dissocié du domaine Azure. Pour plus d'informations, consultez [FAQ sur la gestion des périphériques Azure Active Directory](#).

L'importation BYOL nécessite que le pare-feu public Windows soit désactivé.

Le profil de pare-feu public doit être désactivé. Pour plus d'informations, consultez [Activer ou désactiver le pare-feu de Microsoft Defender](#).

L'importation BYOL nécessite un système sans VMware outils.

VMWare les outils doivent être désinstallés. Pour plus d'informations, voir [Désinstaller et installer manuellement des VMware outils dans VMware Fusion \(1014522\)](#).

L'importation BYOL nécessite que la taille du disque local soit inférieure à 80 Go.

La taille du disque doit être inférieure à 80 Go. Réduisez la taille du disque.

L'importation BYOL nécessite moins de 2 partitions sur le disque local. En outre, toutes les partitions Windows 10 doivent être au format MBR et toutes les partitions Windows 11 au format GPT.

Les volumes doivent être partitionnés au format MBR pour Windows 10 et GPT pour Windows 11. Pour en savoir plus, consultez [Gérer les disques](#).

L'importation BYOL nécessite que toutes les mises à jour en attente nécessitant un redémarrage soient terminées.

Installez toutes les mises à jour et redémarrez le système d'exploitation.

L'importation BYOL nécessite que cela **AutoLogon** soit désactivé.

Pour désactiver le AutoLogon registre, procédez comme suit :

1. Appuyez sur la touche Windows + R, puis saisissez `Regedit.exe` dans l'invite de commande.
2. Faites défiler vers le bas jusqu'à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`.
3. Ajoutez une valeur pour `DontDisplayLastUserName`.
4. Pour le champ Type, saisissez `REG_SZ`.
5. Pour le champ Valeur, saisissez `0`.

 Note

- La valeur `DontDisplayLastUserName` détermine si la boîte de dialogue de connexion affiche le nom d'utilisateur du dernier utilisateur connecté au PC.
- La valeur n'existe pas par défaut. S'il existe, vous devez le définir sur `0` sinon la valeur de `DefaultUser` sera effacée et AutoLogon échouera.

L'importation BYOL nécessite l'activation de **RealTimeIsUniversal**.

RealTimeUniversal La clé de registre doit être activée. Pour plus d'informations, consultez [Configurer les paramètres horaires pour Windows Server 2008 et versions ultérieures](#).

L'importation BYOL nécessite un système disposant d'une partition démarrable.

Le nombre de partitions démarrables ne doit pas dépasser une.

Pour supprimer les partitions supplémentaires

1. Appuyez sur les touches Logo Windows + R pour ouvrir la boîte de dialogue Exécuter. Saisissez `msconfig`, puis appuyez sur la touche Entrée du clavier pour ouvrir la boîte de dialogue Configuration du système.
2. Choisissez l'onglet Démarrer, puis vérifiez que le système d'exploitation que vous souhaitez utiliser est défini comme Système d'exploitation actuel ; Système d'exploitation par défaut. Si

ce n'est pas le cas, sélectionnez le système d'exploitation de votre choix, puis choisissez Par défaut.

3. Pour supprimer une autre partition, choisissez-la, puis cliquez sur les boutons Supprimer, Appliquer et OK.

Si l'erreur persiste, démarrez votre ordinateur à partir du disque d'installation ou de réparation, puis procédez comme suit.

1. Ignorez l'écran initial des langues, puis choisissez Réparer votre ordinateur sur l'écran d'installation principal.
2. Dans l'écran Choisir une option, choisissez Dépanner.
3. Dans l'écran Options avancées, choisissez Invites de commande.
4. Dans l'invite de commande, saisissez `bootrec.exe /fixmbr`, puis appuyez sur Entrée.

L'importation BYOL nécessite un système 64 bits.

Une image du système d'exploitation 64 bits doit être utilisée. Pour plus d'informations, consultez [Versions de Windows prises en charge pour BYOL](#).

L'importation BYOL nécessite un système qui n'a pas été mis à niveau sur place. Ce système a été mis à niveau sur place.

Windows ne doit pas avoir été mis à niveau à partir d'une version précédente.

L'importation BYOL nécessite qu'aucun antivirus ne soit installé sur le système.

Vous devez désinstaller votre logiciel antivirus. Exécutez le Vérificateur de compatibilité des images pour obtenir des informations sur le logiciel antivirus à désinstaller.

L'importation BYOL nécessite que les systèmes Windows 10 disposent d'un mode de démarrage hérité.

L'ancien BIOS BootMode doit être utilisé pour Windows 10. Pour plus d'informations, voir [Modes de démarrage](#).

L'importation BYOL nécessite la désactivation de l'état de stockage réservé de Windows

Pour désactiver l'état de stockage réservé

1. Installez toutes les mises à jour de Windows et redémarrez le système d'exploitation.
2. Assurez-vous qu'il n'y a pas de nouvelles mises à jour.
3. Exécutez l'une des commandes suivantes dans Powershell en tant qu'administrateur.

- `Set-WindowsReservedStorageState -State Disabled`
- `DISM.exe /Online /Set-ReservedStorageState /State:Disabled`

4. Redémarrez le système.

Note

Si le stockage réservé est en cours d'utilisation, il est possible qu'il ne soit pas désactivé et le message d'erreur suivant est renvoyé : This operation is not supported when reserved storage is in use. Please wait for any servicing operations to complete and then try again later.

L'importation BYOL utilise une lettre de lecteur restreinte.

Le D: Drive est une lettre de conduite restreinte pour WorkSpaces. Assurez-vous qu'il n'D: est pas utilisé ou qu'il ne sera pas mappé lors du lancement d'une instance à partir de l'image.

L'importation BYOL contient une image du système d'exploitation incompatible avec le protocole de streaming sélectionné.

L'image importée n'est pas prise en charge par le protocole de diffusion choisi, voir [Création d'une image BYOL à l'aide de la WorkSpaces console](#).

L'importation BYOL est incompatible avec l'intégrité de la mémoire.

L'intégrité de la mémoire n'est pas prise en charge lorsque Credential Guard est activé sur le système d'exploitation Windows d'un WorkSpace. L'intégrité de la mémoire a été détectée et ne peut pas

être désactivée lors de l'importation d'images. UEFILock Veuillez importer une image UEFILock désactivée, voir [Désactiver Credential Guard](#).

L'importation BYOL nécessite la désactivation de l'état Bitlocker.

Pour désactiver Bitlocker :

1. Ouvrez Powershell en tant qu'administrateur.
2. Exécutez la commande suivante :

```
manage-bde -off DriveLetter:
```

3. Vérifiez le statut de BitLocker en exécutant la commande ci-dessous :

```
manage-bde -Status DriveLetter:
```

4. Assurez-vous que les valeurs affichées correspondent à celles-ci :

- BitLocker Version — Aucune
- État de la conversion : entièrement déchiffré
- Pourcentage crypté : 0,0 %
- Méthode de chiffrement — Aucune
- État de protection — Protection désactivée
- État du verrouillage — Déverrouillé

WorkSpaces la création échoue en raison de problèmes de synchronisation horaire avec des images personnalisées

Par défaut, les images personnalisées atteignent « time.windows.com » en tant que serveur NTP par défaut. Si le serveur NTP n'est pas joignable, des problèmes de synchronisation horaire peuvent survenir, entraînant des échecs de validation des RDP/Skylight certificats et des problèmes de connexion SSL empêchant WorkSpaces la création.

Si vous rencontrez des problèmes de synchronisation horaire, mettez à jour le serveur NTP pour utiliser le service Amazon Time Sync au 169.254.169.123. Pour plus d'informations, consultez [Configurer l'heure pour votre instance Windows](#).

Liste des messages SysPrep d'erreur et des corrections d'erreurs

Des packages AppX sont installés sur l'AMI que vous importez. Supprimez-les et réimportez l'image.

Des packages AppX modernes peuvent toujours être installés pour vos utilisateurs. Supprimez le package AppX en exécutant le cmdlet Powershell, `Remove-AppxPackage`

Note

Au cours du processus d'importation BYOL, les packages AppX incriminés seront nettoyés et Sysprep sera réessayé. Si le processus d'importation d'image continue d'échouer, cela signifie que les packages AppX devront être nettoyés manuellement.

Le stockage réservé est activé sur l'AMI que vous importez. Désactivez-le après les mises à jour de Windows et réimportez l'image.

Pour désactiver le stockage réservé

1. Ouvrez l'éditeur de registre mais entrez `regedit.exe`.
2. Accédez à la clé de registre `:HKLM\Software\Microsoft\Windows\CurrentVersion\ReserveManager`.
3. Modifiez la valeur du `ShippedWithReserves` paramètre de 1 à 0.
4. Remplacez la valeur de `ActiveScenario` par 0.
5. Désactivez le stockage réservé sous Windows à l'aide de la commande suivante :

```
DISM.exe /Online /Set-ReservedStorageState /State:Disabled
```

Un logiciel antivirus ou anti-spyware est installé sur l'AMI que vous importez. Supprimez-le et réimportez l'image.

Vous devez désinstaller votre logiciel antivirus. Exécutez le vérificateur de compatibilité des images pour obtenir des informations sur le logiciel antivirus à désinstaller. Pour de plus amples informations, veuillez consulter [\(Facultatif\) Validez votre image avant de l'importer](#).

Une erreur inconnue s'est produite dans l'AMI que vous importez pendant l'AMI SysPrep.

SysPrep la raison de l'échec n'a pas pu être déterminée. Contactez le AWS support à l'adresse <https://aws.amazon.com/support>.

Utiliser et gérer WorkSpaces Personal

WorkSpaces Personal propose des bureaux virtuels permanents conçus pour les utilisateurs qui ont besoin d'un poste de travail hautement personnalisé réservé à leur usage exclusif, similaire à un ordinateur de bureau physique attribué à un individu.

Chacun WorkSpace est associé à un cloud privé virtuel (VPC) et à un répertoire pour stocker et gérer les informations pour vous WorkSpaces et les utilisateurs. Pour de plus amples informations, veuillez consulter [the section called “Exigences du VPC”](#). Les annuaires sont gérés soit par le WorkSpaces service, soit via le Directory Service, qui propose les options suivantes : Simple AD, AD Connector ou AWS Directory Service pour Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD. Pour plus d'informations, consultez le [Guide d'administration AWS Directory Service](#).

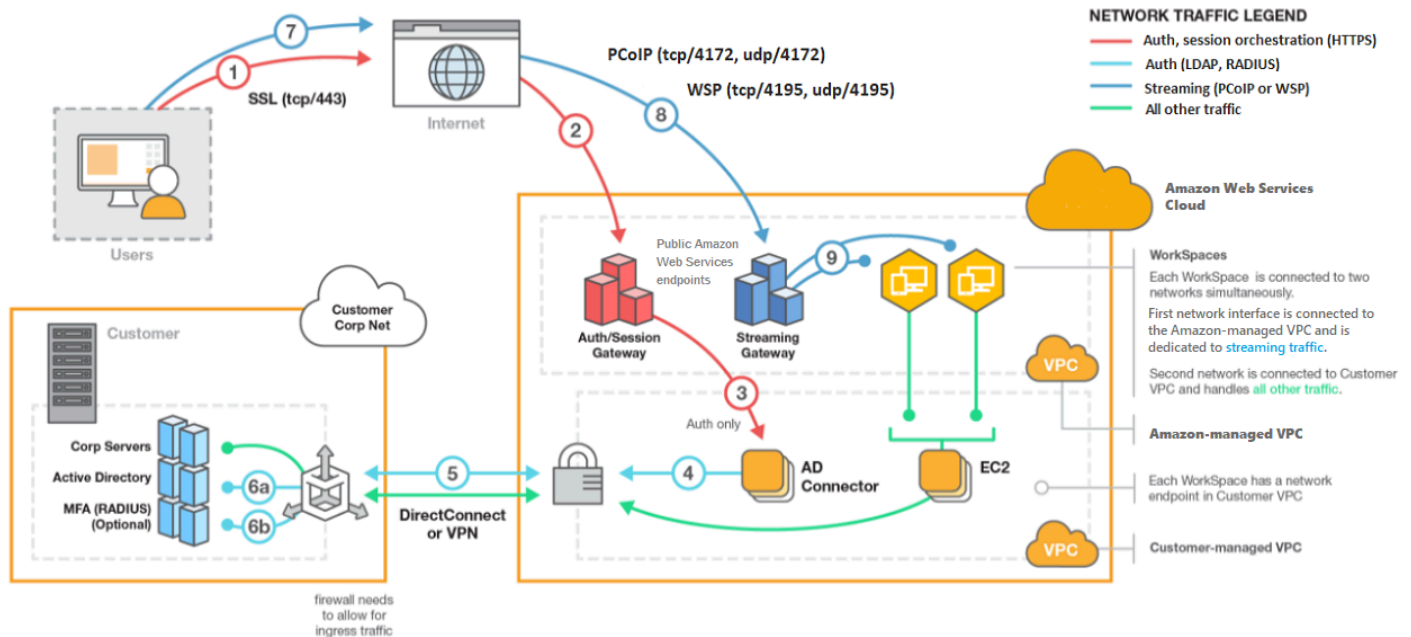
WorkSpaces utilise votre IAM Identity Center (pour les annuaires gérés par Amazon WorkSpaces), Simple AD, AD Connector ou AWS Managed Microsoft AD pour authentifier les utilisateurs. Les utilisateurs y WorkSpaces accèdent à l'aide d'une application cliente à partir d'un appareil compatible ou, pour Windows WorkSpaces, d'un navigateur Web, et ils se connectent à l'aide de leurs informations d'identification d'annuaire. Les informations de connexion sont envoyées à une passerelle d'authentification, qui transmet le trafic vers le répertoire du WorkSpace. Une fois l'utilisateur authentifié, le trafic de streaming est initié via la passerelle de streaming.

Les applications client utilisent HTTPS via le port 443 pour toutes les informations liées à l'authentification et à la session. Les applications clientes utilisent les ports 4172 (PCoIP) et 4195 (DCV) pour le streaming de pixels vers les ports 4172 WorkSpace et 4195 pour les contrôles de santé du réseau. Pour de plus amples informations, veuillez consulter [Ports pour client](#).

WorkSpace Chacune est associée à deux interfaces réseau élastiques : une interface réseau pour la gestion et le streaming (eth0) et une interface réseau principale (eth1). L'interface réseau principale possède une adresse IP fournie par votre VPC, à partir des mêmes sous-réseaux utilisés par l'annuaire. Cela garantit que le trafic en provenance de vous WorkSpace peut facilement atteindre le répertoire. L'accès aux ressources du VPC est contrôlé par les groupes de sécurité affectés à l'interface réseau principale. Pour de plus amples informations, veuillez consulter [Interfaces réseau](#).

Le schéma suivant montre l'architecture de ceux WorkSpaces qui utilisent AD Connector.

Amazon WorkSpaces Architectural Diagram



Options pour créer un WorkSpace avec WorkSpaces Personal

Il existe plusieurs méthodes pour créer un WorkSpace. Vous pouvez utiliser les instructions de configuration rapide, les instructions de configuration avancées ou choisir l'une des options suivantes :

- [Création d'un répertoire Microsoft AD AWS géré pour WorkSpaces Personal](#)
- [Création d'un annuaire Simple AD pour WorkSpaces Personal](#)
- [Création d'un AD Connector pour les WorkSpaces particuliers](#)
- [Créez une relation de confiance entre votre annuaire Microsoft AD AWS géré et votre domaine local pour Personal WorkSpaces](#)
- [Créez un répertoire Microsoft Entra ID dédié avec WorkSpaces Personal](#)
- [Créez un répertoire personnalisé dédié avec WorkSpaces Personal](#)

Commencez avec WorkSpaces Personal

En tant que nouvel WorkSpaces utilisateur, vous pouvez choisir de configurer votre WorkSpaces Personal avec une configuration rapide ou une configuration avancée. Les didacticiels suivants

décrivent comment configurer un poste de travail basé sur le cloud, connu sous le nom d'Workspace, en utilisant WorkSpaces et Directory Service.

 Note

Pour commencer à utiliser WorkSpaces Pools, consultez [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#).

WorkSpaces Configuration rapide personnalisée

Dans ce didacticiel, vous apprendrez à configurer un bureau virtuel basé sur le cloud Microsoft Windows, Amazon Linux 2, Ubuntu Linux, Rocky Linux ou Red Hat Enterprise Linux, connu sous le nom de Workspace, en utilisant WorkSpaces et Directory Service.

Ce didacticiel utilise l'option de configuration rapide pour lancer votre Workspace. Cette option n'est disponible que si vous n'avez jamais lancé de Workspace. Sinon, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

 Note

Cette option de configuration rapide et ce didacticiel ne s'appliquent pas aux WorkSpaces pools.

 Note

La configuration rapide est prise en charge dans les AWS régions suivantes :

- USA Est (Virginie du Nord)
- USA Ouest (Oregon)
- Europe (Irlande)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asia Pacific (Tokyo)

Pour modifier votre région, consultez [Choisir une région](#).

Tâches

- [Avant de commencer](#)
- [En quoi consiste la configuration rapide](#)
- [Étape 1 : Lancez le WorkSpace](#)
- [Étape 2 : Connectez-vous au WorkSpace](#)
- [Étape 3 : Nettoyer \(Facultatif\)](#)
- [Étapes suivantes](#)

Avant de commencer

Avant de commencer, vérifiez que vous respectez les conditions requises suivantes :

- Vous devez disposer d'un AWS compte pour créer ou administrer un WorkSpace. Les utilisateurs n'ont pas besoin de AWS compte pour se connecter et utiliser leur WorkSpaces.
- WorkSpaces n'est pas disponible dans toutes les régions. Vérifiez les régions prises en charge et [sélectionnez une région](#) pour votre WorkSpaces. Pour plus d'informations sur les régions prises en charge, consultez la section [WorkSpaces Tarification par AWS région](#).

Il est également utile de lire et de comprendre les points suivants avant de poursuivre :

- Lorsque vous lancez un WorkSpace, vous devez sélectionner un WorkSpace bundle. Pour plus d'informations, consultez [Amazon WorkSpaces Bundles](#) et [Amazon WorkSpaces Pricing](#).
- Lorsque vous lancez un WorkSpace, vous devez sélectionner le protocole (PCoIP ou DCV) que vous souhaitez utiliser avec votre bundle. Pour de plus amples informations, veuillez consulter [Protocoles pour le WorkSpaces personnel](#).
- Lorsque vous lancez un WorkSpace, vous devez spécifier les informations de profil de l'utilisateur, notamment son nom d'utilisateur et son adresse e-mail. Les utilisateurs achèvent leurs profils en spécifiant un mot de passe. Les informations concernant WorkSpaces et les utilisateurs sont stockées dans un répertoire. Pour de plus amples informations, veuillez consulter [the section called "Gérez les annuaires pour WorkSpaces"](#).

En quoi consiste la configuration rapide

La configuration rapide exécute les tâches suivantes à votre place :

- Crée un rôle IAM pour permettre au WorkSpaces service de créer des interfaces réseau élastiques et de répertorier vos WorkSpaces annuaires. Ce rôle est nommé `workspaces_DefaultRole`.
- Crée un cloud privé virtuel (VPC). Si vous souhaitez plutôt utiliser un VPC existant, assurez-vous qu'il répond aux exigences indiquées dans [Configuration d'un VPC pour le personnel WorkSpaces](#), puis suivez les étapes décrites dans l'un des didacticiels répertoriés dans [Création d'un répertoire pour WorkSpaces Personal](#). Choisissez le didacticiel qui correspond au type d'annuaire Active Directory que vous souhaitez utiliser.
- Configure un répertoire Simple AD dans le VPC et l'active pour. WorkDocs Ce répertoire Simple AD est utilisé pour stocker les utilisateurs et les WorkSpace informations. Le premier Compte AWS créé par la configuration rapide est votre administrateur Compte AWS. † L'annuaire possède également un compte administrateur. Pour plus d'informations, consultez [Ce qui est créé](#) dans le Guide d'administration AWS Directory Service .
- Crée les Comptes AWS données spécifiées et les ajoute au répertoire.
- Crée WorkSpaces. Chacun WorkSpace reçoit une adresse IP publique pour fournir un accès à Internet. Le mode de fonctionnement est AlwaysOn. Pour de plus amples informations, veuillez consulter [Gérer le mode de course dans WorkSpaces Personal](#).
- Envoie des e-mails d'invitation aux utilisateurs spécifiés. Si les utilisateurs ne reçoivent pas les e-mails d'invitation, consultez [Envoi d'un e-mail d'invitation](#).

† Le premier Compte AWS créé par la configuration rapide est votre administrateur Compte AWS. Vous ne pouvez pas le mettre à jour Compte AWS depuis la WorkSpaces console. Ne partagez pas les informations relatives à ce compte avec d'autres personnes. Pour inviter d'autres utilisateurs à l'utiliser WorkSpaces, créez-en un nouveau Comptes AWS pour eux.

Étape 1 : Lancez le Workspace

Grâce à la configuration rapide, vous pouvez lancer votre premier Workspace en quelques minutes.

Pour lancer un Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Configuration rapide. Si ce bouton ne s'affiche pas, cela signifie que vous en avez déjà lancé un Workspace dans cette région ou que vous n'utilisez pas l'une des [régions qui prennent en charge la configuration rapide](#). Dans ce cas, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

Services ▾

Search for services, features, marketplace products, and docs [Option+S]

Customer Account ▾ N. Virginia ▾ Support ▾

End User Computing

Amazon WorkSpaces

Secure, reliable, and scalable access to persistent desktops from any location.

Amazon WorkSpaces is a fully managed desktop virtualization service for Windows and Linux that enables you to access resources from any supported device.

How it works

- Set up your directory with existing network and identity, and then register with the console.
- Choose a WorkSpaces bundle of an Operating System and a compute type of your choice, or use the default.
- Amazon WorkSpaces: Centrally manage your persistent cloud desktops and stream them to users.
- Users securely access their desktops through a browser or native client applications.

Create WorkSpaces

Quick setup

Launch WorkSpaces for an individual or small group of cloud-based users in less than 20 minutes.

Quick setup

Advanced setup

Launch WorkSpaces using advanced options, including your on-premises directory and existing [Amazon VPC](#).

Advanced setup

3. Pour Identifier des utilisateurs, entrez le nom d'utilisateur, prénom nom de famille et l'adresse e-mail. Ensuite, sélectionnez Suivant.

Note

Si c'est la première fois que vous l'utilisez WorkSpaces, nous vous recommandons de vous créer un utilisateur à des fins de test.

Services Search for services, features, marketplace products, and docs [Option+S]

Customer Account N. Virginia Support

WorkSpaces > Get Started

Step 1
Identify users

Step 2
Select bundles

Step 3
Review

Identify users [Info](#)

Add up to 5 users to your WorkSpaces.

Create users

Username	First Name	Last Name	Email	
				Remove
Must contain alphanumeric and numeric characters.	Must contain alphanumeric and numeric characters.	Must contain alphanumeric and numeric characters.	Must be a valid email address	
Create additional users		Save		
Add up to 5 users				

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4. Pour les ensembles, sélectionnez un ensemble (matériel et logiciel) pour l'utilisateur avec le protocole approprié (PCoIP ou DCV). Pour plus d'informations sur les différents forfaits publics disponibles pour Amazon WorkSpaces, consultez [Amazon WorkSpaces Bundles](#).

Select bundles Info

All Amazon Linux bundles come with Firefox, LibreOffice, Evolution, Python, and more. All Windows bundles come with Internet Explorer 11 and Firefox. You can install your own application and packages on your WorkSpaces after it has launched.

Bundle (10/90)

Bundle	Language	Root volume	User volume
☒ Value with Amazon Linux 2 PCoIP	English	80 GiB	10 GiB
☐ Standard with Amazon Linux 2 PCoIP Free tier eligible	English	80 GiB	50 GiB
☐ Performance with Amazon Linux 2 PCoIP	English	80 GiB	100 GiB
☐ Power with Amazon Linux 2 PCoIP	English	175 GiB	100 GiB
☐ PowerPro with Amazon Linux 2 PCoIP	English	175 GiB	100 GiB
☐ Standard with Windows 10 PCoIP Free tier eligible	English	80 GiB	50 GiB
☐ Value with Windows 10 PCoIP	English	80 GiB	10 GiB
☐ Value with Windows 10 and Office 2016 PCoIP	English	80 GiB	10 GiB
☐ Value with Windows 10 PCoIP	English	80 GiB	10 GiB
☐ Performance with Windows 10 PCoIP	English	80 GiB	10 GiB

5. Vérifiez les informations fournies. Ensuite, choisissez Créer WorkSpace.
6. Le lancement prend environ 20 minutes. WorkSpace Pour suivre la progression, accédez au volet de navigation de gauche, puis choisissez Annuaire. Vous verrez un annuaire en cours de création avec le statut initial REQUESTED, qui passera ensuite à CREATING.

Une fois que le répertoire a été créé et que son statut est égal à ACTIVE, vous pouvez choisir WorkSpaces dans le volet de navigation de gauche de suivre la progression du processus de WorkSpace lancement. Le statut initial du WorkSpace est PENDING. Une fois le lancement terminé, le statut passe à AVAILABLE, et une invitation est envoyée à l'adresse e-mail spécifiée pour l'utilisateur. Si les utilisateurs ne reçoivent pas les e-mails d'invitation, consultez [Envoi d'un e-mail d'invitation](#).

Étape 2 : Connectez-vous au WorkSpace

Après avoir reçu l'e-mail d'invitation, vous pouvez vous connecter à l' WorkSpace aide du client de votre choix. Une fois connecté, le client affiche le WorkSpace bureau.

Pour vous connecter au WorkSpace

1. Si vous n'avez pas encore configuré les informations d'identification de l'utilisateur, ouvrez le lien dans l'e-mail d'invitation et suivez les instructions. N'oubliez pas le mot de passe que vous avez spécifié car vous en aurez besoin pour vous connecter à votre WorkSpace.

Note

Les mots de passe sont sensibles à la casse et doivent comporter entre 8 et 64 caractères, inclus. Les mots de passe doivent comporter au moins un caractère appartenant à chacune des catégories suivantes : minuscules (a à z), majuscules (A à Z), chiffres (0 à 9) et le jeu de caractères ~!@#\$%^&* _-+=`|(){}[];:'<>,.?/.

2. Consultez la section [WorkSpacesClients](#) du guide de WorkSpaces l'utilisateur Amazon pour plus d'informations sur les exigences de chaque client, puis effectuez l'une des opérations suivantes :
 - Lorsque vous y êtes invité, téléchargez l'une des applications client ou lancez Web Access.
 - Si vous n'y êtes pas invité et que vous n'avez pas encore installé d'application cliente, ouvrez <https://clients.amazonworkspaces.com/> et téléchargez l'une des applications clientes ou lancez Web Access.

Note

Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter à Amazon Linux WorkSpaces.

3. Lancez le client, saisissez le code d'inscription fourni dans l'e-mail d'invitation et choisissez S'inscrire.
4. Lorsque vous êtes invité à vous connecter, entrez vos informations d'identification, puis choisissez Se connecter.
5. (Facultatif) Lorsque vous êtes invité à enregistrer vos informations d'identification, choisissez Oui.

Pour plus d'informations sur l'utilisation des applications clientes, telles que la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez la section [WorkSpaces Client and Peripheral Device Support](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Étape 3 : Nettoyer (Facultatif)

Si vous avez terminé avec ce WorkSpace que vous avez créé pour ce didacticiel, vous pouvez le supprimer. Pour de plus amples informations, veuillez consulter [the section called "Supprimer un WorkSpace"](#).

Note

Simple AD est mis à votre disposition gratuitement pour une utilisation avec WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire Simple AD pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé auprès d'Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires.AWS Directory Service](#)

Pour supprimer des annuaires vides, consultez [Supprimer un répertoire pour WorkSpaces Personal](#). Si vous supprimez votre répertoire Simple AD, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à l'utiliser WorkSpaces .

Étapes suivantes

Vous pouvez continuer à personnaliser WorkSpace ce que vous venez de créer. Par exemple, vous pouvez installer un logiciel, puis créer un bundle personnalisé à partir de votre WorkSpace. Vous pouvez également effectuer diverses tâches administratives pour votre annuaire WorkSpaces et votre WorkSpaces annuaire. Pour plus d'informations, consultez la documentation suivante.

- [Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal](#)
- [Administrer le WorkSpaces personnel](#)
- [Gérer les annuaires pour WorkSpaces Personal](#)

Pour en créer d'autres WorkSpaces, effectuez l'une des opérations suivantes :

- Si vous souhaitez continuer à utiliser le VPC et le répertoire Simple AD créés par configuration rapide, vous pouvez ajouter des utilisateurs supplémentaires en suivant WorkSpaces les étapes

décrites dans la [Créez un Workspace in WorkSpaces Personal](#) section du didacticiel Lancer une Workspace utilisation de Simple AD.

- Si vous devez utiliser un autre type d'annuaire ou un annuaire Active Directory existant, consultez le didacticiel approprié dans [Création d'un répertoire pour WorkSpaces Personal](#).

Pour plus d'informations sur l'utilisation des applications WorkSpaces clientes, telles que la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez la section [WorkSpaces Client and Peripheral Device Support](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Commencez avec la configuration avancée WorkSpaces personnalisée

Dans ce didacticiel, vous apprendrez à configurer un poste de travail virtuel basé sur le cloud Microsoft Windows, Amazon Linux, Ubuntu Linux ou Red Hat Enterprise Linux, connu sous le nom de Workspace, en utilisant WorkSpaces et Directory Service.

Ce didacticiel utilise l'option de configuration avancée pour lancer votre Workspace.

Note

La configuration avancée est prise en charge dans toutes les régions pour WorkSpaces.

Tâches

- [Avant de commencer](#)
- [Utilisation de la configuration avancée pour lancer votre Workspace](#)

Avant de commencer

Avant de commencer, assurez-vous de disposer d'un AWS compte que vous pouvez utiliser pour créer ou administrer un Workspace. Les utilisateurs n'ont pas besoin de AWS compte pour se connecter et utiliser leur WorkSpaces.

Passez en revue et comprenez les concepts suivants avant de poursuivre :

- Lorsque vous lancez un Workspace, vous devez sélectionner un Workspace bundle. Pour plus d'informations, consultez [Amazon WorkSpaces Bundles](#).

- Lorsque vous lancez un WorkSpace, vous devez sélectionner le protocole (PCoIP ou DCV) que vous souhaitez utiliser avec votre bundle. Pour de plus amples informations, veuillez consulter [Protocoles pour le WorkSpaces personnel](#).
- Lorsque vous lancez un WorkSpace, vous devez spécifier les informations de profil de l'utilisateur, notamment son nom d'utilisateur et son adresse e-mail. Les utilisateurs achèvent leurs profils en spécifiant un mot de passe. Les informations concernant WorkSpaces et les utilisateurs sont stockées dans un répertoire. Pour de plus amples informations, veuillez consulter [the section called "Gérez les annuaires pour WorkSpaces"](#).

Utilisation de la configuration avancée pour lancer votre WorkSpace

Pour utiliser la configuration avancée pour lancer votre WorkSpace :

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez l'un des types d'annuaire suivants, puis cliquez sur Suivant :
 - AWS Microsoft AD géré
 - Simple AD
 - AD Connector
3. Saisissez les informations de l'annuaire.
4. Choisissez deux sous-réseaux au sein d'un VPC dans deux zones de disponibilité différentes. Pour plus d'informations, consultez [Configuration d'un VPC avec des sous-réseaux publics](#).
5. Vérifiez les informations de votre annuaire et choisissez Créer un annuaire.

Créez un WorkSpace in WorkSpaces Personal

WorkSpaces vous permet de fournir des bureaux Windows et Linux virtuels basés sur le cloud à vos utilisateurs, connus sous WorkSpacesle nom de.

Avant de créer un compte personnel WorkSpace, créez un répertoire en effectuant l'une des opérations suivantes :

- Créer un annuaire Simple AD.
- Créez un service d' AWS annuaire pour Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD.

- Connectez-vous à un annuaire Microsoft Active Directory existant à l'aide d'Active Directory Connector.
- Créez une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site.
- Créez un répertoire dédié qui utilise l'identifiant Microsoft Entra comme source d'identité (via IAM Identity Center). WorkSpaces dans le répertoire sont associés à un identifiant Entra natif et inscrits à Microsoft Intune via le mode piloté par l'utilisateur de Microsoft Windows Autopilot.

 Note

Ces répertoires ne prennent actuellement en charge que Windows 10 et 11 Bring Your Own Licenses personal WorkSpaces.

- Créez un répertoire dédié qui utilise le fournisseur d'identité de votre choix comme source d'identité (via IAM Identity Center). WorkSpaces dans le répertoire sont associés à un identifiant Entra natif et inscrits à Microsoft Intune via le mode piloté par l'utilisateur de Microsoft Windows Autopilot.

 Note

Ces répertoires ne prennent actuellement en charge que Windows 10 et 11 Bring Your Own Licenses personal WorkSpaces.

Maintenant que vous avez créé un répertoire, vous êtes prêt à créer un répertoire personnel WorkSpace.

Pour créer un compte personnel WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Choisissez Launch WorkSpaces, Personal.
4. Sélectionnez Create WorkSpaces (Créer).
5. Sous Intégration (facultatif), vous pouvez choisir de me recommander des options en fonction de mon cas d'utilisation pour obtenir des recommandations sur le type que WorkSpace vous souhaitez utiliser. Vous pouvez ignorer cette étape si vous savez que vous souhaitez utiliser le mode personnel WorkSpaces.
6. Choisissez Next. WorkSpaces enregistre votre AD Connector.

7. Sous Configurer WorkSpaces, entrez les informations suivantes :

- Pour Bundle, choisissez parmi les options suivantes le type de bundle que vous souhaitez utiliser pour votre WorkSpaces.
- Utiliser un WorkSpaces pack de base : choisissez l'un des packs dans le menu déroulant. Pour plus d'informations sur le type de bundle que vous avez sélectionné, choisissez Bundle details. Pour comparer les forfaits proposés pour les pools, choisissez Comparer tous les forfaits.
- Utilisez votre propre bundle personnalisé ou BYOL : choisissez un bundle que vous avez créé précédemment. Pour créer un bundle personnalisé, voir [Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal](#).

Note

Passez en revue les utilisations et spécifications recommandées de chaque offre groupée pour vous assurer de sélectionner celle qui convient le mieux aux utilisateurs. Pour plus d'informations sur chaque cas d'utilisation, consultez [Amazon WorkSpaces Bundles](#). Pour plus d'informations sur les spécifications des offres groupées, les utilisations recommandées et les prix, consultez [WorkSpaces les tarifs Amazon](#).

- Pour le mode Running, choisissez l'une des options suivantes pour configurer Workspace la disponibilité immédiate de votre personnel et le mode de paiement (mensuel ou horaire) :
 - AlwaysOn— Facture des frais mensuels pour une utilisation illimitée de votre WorkSpaces. Ce mode est idéal pour les utilisateurs qui utilisent leur poste de travail principal à Workspace plein temps.
 - AutoStop— Des factures à l'heure. Avec ce mode, vous vous WorkSpaces arrêtez après une période de déconnexion spécifiée, et l'état des applications et des données est enregistré.
 - Pour les balises, spécifiez la valeur de paire de clés que vous souhaitez utiliser. Une clé peut être une catégorie générale, telle que « projet », « propriétaire » ou « environnement », avec des valeurs associées spécifiques.
- ## 8. Sous Sélectionner un répertoire, entrez les informations suivantes :
- Choisissez le répertoire que vous avez créé. Pour créer un répertoire, choisissez Create directory. Pour plus d'informations sur la création d'annuaires personnels, consultez [Enregistrer un Directory Service répertoire existant avec WorkSpaces Personal](#).

- Choisissez les utilisateurs du répertoire WorkSpaces pour lesquels vous souhaitez fournir des informations personnelles en procédant comme suit.
 1. Choisissez Créer des utilisateurs.
 2. Entrez le nom d'utilisateur, le prénom, le nom de famille et l'e-mail de l'utilisateur. Pour ajouter des utilisateurs supplémentaires, choisissez Créer un utilisateur supplémentaire et entrez leurs informations.
- 9. Sous Personnalisation (facultatif), vous pouvez personnaliser les ensembles, le chiffrement du volume root et du volume utilisateur, ainsi que le volume utilisateur pour tous les utilisateurs ou pour des utilisateurs spécifiques.
- 10. Choisissez Create WorkSpaces. Le statut initial du Workspace est EN ATTENTE. Lorsque la création est terminée, le statut est DISPONIBLE et une invitation est envoyée à l'adresse e-mail que vous avez spécifiée pour les utilisateurs.
- 11. Envoyez des invitations à l'adresse e-mail de chaque utilisateur. Pour de plus amples informations, veuillez consulter [Envoi d'un e-mail d'invitation](#).

 Note

- Ces invitations ne sont pas envoyées automatiquement si vous utilisez AD Connector ou une relation de confiance.
- Aucun e-mail d'invitation n'est envoyé si l'utilisateur existe déjà dans Active Directory. Assurez-vous d'envoyer manuellement un e-mail d'invitation à l'utilisateur. Pour de plus amples informations, veuillez consulter [Envoi d'un e-mail d'invitation](#).
- Dans toutes les régions, le texte de l'e-mail d'invitation est en anglais (États-Unis). Dans les régions suivantes, le texte anglais est précédé d'une deuxième langue :
 - Asie-Pacifique (Séoul) : coréen
 - Asie-Pacifique (Tokyo) : japonais
 - Canada (centre) : français (canadien)
 - Chine (Ningxia) : chinois simplifié

Connectez-vous au Workspace

Vous pouvez vous connecter à votre Workspace compte en utilisant le client de votre choix. Une fois connecté, le client affiche le Workspace bureau.

Pour vous connecter au Workspace

1. Ouvrez le lien dans l'e-mail d'invitation.
2. Consultez la section [WorkSpaces Clients](#) du guide de WorkSpaces l'utilisateur Amazon pour plus d'informations sur les exigences de chaque client, puis effectuez l'une des opérations suivantes :
 - Lorsque vous y êtes invité, téléchargez l'une des applications client ou lancez Web Access.
 - Si vous n'y êtes pas invité et que vous n'avez pas encore installé d'application cliente, ouvrez <https://clients.amazonworkspaces.com/> et téléchargez l'une des applications clientes ou lancez Web Access.

Note

Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter à Amazon Linux WorkSpaces.

3. Lancez le client, saisissez le code d'inscription fourni dans l'e-mail d'invitation et choisissez S'inscrire.
4. Lorsque vous êtes invité à vous connecter, saisissez les informations d'identification de l'utilisateur, puis choisissez Se connecter.
5. (Facultatif) Lorsque vous êtes invité à enregistrer vos informations d'identification, choisissez Oui.

Note

Étant donné que vous utilisez AD Connector, vos utilisateurs ne pourront pas réinitialiser leurs propres mots de passe. (Le mot de passe oublié ? l'option sur l'écran de connexion de l'application WorkSpaces cliente ne sera pas disponible.) Pour plus d'informations sur la réinitialisation des mots de passe utilisateur, veuillez consulter [Configuration des outils d'administration Active Directory pour le WorkSpaces personnel](#).

Étapes suivantes

Vous pouvez continuer à personnaliser Workspace ce que vous venez de créer. Par exemple, vous pouvez installer un logiciel, puis créer un bundle personnalisé à partir de votre Workspace. Vous

pouvez également effectuer diverses tâches administratives pour votre annuaire WorkSpaces et votre WorkSpaces annuaire. Si vous en avez terminé avec votre WorkSpace, vous pouvez le supprimer. Pour plus d'informations, consultez la documentation suivante.

- [Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal](#)
- [Administrer le WorkSpaces personnel](#)
- [Gérer les annuaires pour WorkSpaces Personal](#)
- [Supprimer un WorkSpace dans WorkSpaces Personal](#)

Pour plus d'informations sur l'utilisation des applications WorkSpaces clientes, telles que la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez la section [WorkSpaces Client and Peripheral Device Support](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Protocoles réseau et accès pour le WorkSpaces personnel

En tant qu' WorkSpace administrateur, vous devez comprendre comment gérer le WorkSpaces réseau et l'accès, en commençant par les protocoles.

Protocoles pour le WorkSpaces personnel

Amazon WorkSpaces prend en charge deux protocoles : PCo IP et DCV. Le protocole que vous choisissez dépend de plusieurs facteurs, tels que le type d'appareil à WorkSpaces partir duquel vos utilisateurs accèderont à leurs données, le système d'exploitation installé sur votre ordinateur WorkSpaces, les conditions du réseau auxquelles ils seront confrontés et la question de savoir si vos utilisateurs ont besoin d'une assistance vidéo bidirectionnelle.

Exigences

Les DCV ne WorkSpaces sont pris en charge que si les exigences minimales suivantes sont remplies.

Exigences concernant l'agent hôte :

- Agent hôte Windows version 2.0.0.312 ou ultérieure
- Agent hôte Ubuntu version 2.1.0.501 ou ultérieure
- Agent hôte Amazon Linux 2 version 2.0.0.596 ou supérieure

- Agent hôte Rocky Linux version 2.1.0.1628 ou supérieure
- Agent hôte Red Hat Enterprise Linux version 2.1.0.1628 ou supérieure

Prérequis du client :

- Client natif Windows version 5.1.0.329 ou supérieure
- Client natif macOS version 5.5.0 ou supérieure
- Client Ubuntu 22.04 version 2024.x ou supérieure
- Amazon WorkSpaces Thin Client (pour plus d'informations, consultez la [documentation Amazon WorkSpaces Thin Client](#))
- Web Access

Pour plus d'informations sur la façon de vérifier la version de votre WorkSpace client et la version de votre agent hôte, consultez la [FAQ](#).

Quand utiliser le DCV

- Si vous avez besoin d'une plus grande loss/latency tolérance pour répondre aux conditions du réseau de votre utilisateur final. Par exemple, vous avez des utilisateurs qui y accèdent WorkSpaces sur des distances internationales ou qui utilisent des réseaux peu fiables.
- Si vous avez besoin que les utilisateurs s'authentifient à l'aide de cartes intelligentes ou les utilisent en cours de session.
- Si vous avez besoin de fonctionnalités de support par webcam en cours de session.
- Si vous devez utiliser Web Access avec le bundle Windows Server 2022 ou Windows Server 2025. WorkSpaces
- Si vous devez utiliser Ubuntu WorkSpaces.
- Si vous devez utiliser Windows 11 BYOL WorkSpaces.
- Si vous devez utiliser des WorkSpaces bundles compatibles GPU avec Windows.
- Si vous devez utiliser des ensembles basés sur un processeur graphique Windows (Graphics.G6, Graphics.G4DN et .g4dn) ou des ensembles basés sur un processeur graphique Ubuntu (Graphics.G4DN et GraphicsPro .g4dn). GraphicsPro
- Si vous avez besoin que vos utilisateurs s'authentifient en cours de session avec des WebAuthn authenticateurs tels que YubiKey Windows Hello.

Quand utiliser l' PCoIP

- Si vous souhaitez utiliser les clients Linux pour iPad ou Android.
- Si vous utilisez des périphériques clients plume Teradici.
- Si vous devez employer un bundle Linux pour des cas d'utilisation autres que les cartes intelligentes.
- Si vous devez l'utiliser WorkSpaces dans la région Chine (Ningxia)

Note

- Un annuaire peut contenir un mélange d' PCoIP et de DCV WorkSpaces .
- Un utilisateur peut avoir à la fois une PCo adresse IP et un DCV à condition Workspace que les deux WorkSpaces soient situés dans des répertoires distincts. Le même utilisateur ne peut pas avoir d' PCoadresse IP et de DCV Workspace dans le même répertoire. Pour plus d'informations sur la création de plusieurs WorkSpaces pour un utilisateur, consultez [Création d'un multiple WorkSpaces pour un utilisateur dans WorkSpaces Personal](#).
- Vous pouvez migrer Workspace entre les deux protocoles à l'aide de la fonctionnalité de WorkSpaces migration, qui nécessite une reconstruction du Workspace. Pour de plus amples informations, veuillez consulter [Migrer un Workspace dans WorkSpaces Personal](#).
- Si vous avez Workspace été créé avec des bundles PCo IP, vous pouvez modifier le protocole de streaming pour migrer entre les deux protocoles sans nécessiter de reconstruction, tout en conservant le volume racine. Pour plus d'informations, voir [Modifier les protocoles](#).
- Pour une expérience de visioconférence optimale, nous vous recommandons d'utiliser uniquement les packs Power PowerPro, GeneralPurpose .4xlarge ou GeneralPurpose .8xlarge.

Les rubriques suivantes fournissent des informations supplémentaires sur la gestion du réseau et de l'accès pour WorkSpaces Personal :

Configuration d'un VPC pour le personnel WorkSpaces

WorkSpaces vous lance WorkSpaces dans un cloud privé virtuel (VPC).

Vous pouvez créer un VPC avec deux sous-réseaux privés pour votre compte WorkSpaces et une passerelle NAT dans un sous-réseau public. Vous pouvez également créer un VPC avec deux sous-réseaux publics pour vous WorkSpaces et associer une adresse IP publique ou une adresse IP élastique à chacun d'eux. WorkSpace

Pour plus d'informations sur les considérations relatives à la conception des VPC, consultez les [meilleures pratiques VPCs et la mise en réseau dans les WorkSpaces déploiements Amazon et les meilleures pratiques pour le déploiement - Conception de WorkSpaces VPC](#).

Table des matières

- [Exigences](#)
- [Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT](#)
- [Configuration d'un VPC avec des sous-réseaux publics](#)

Exigences

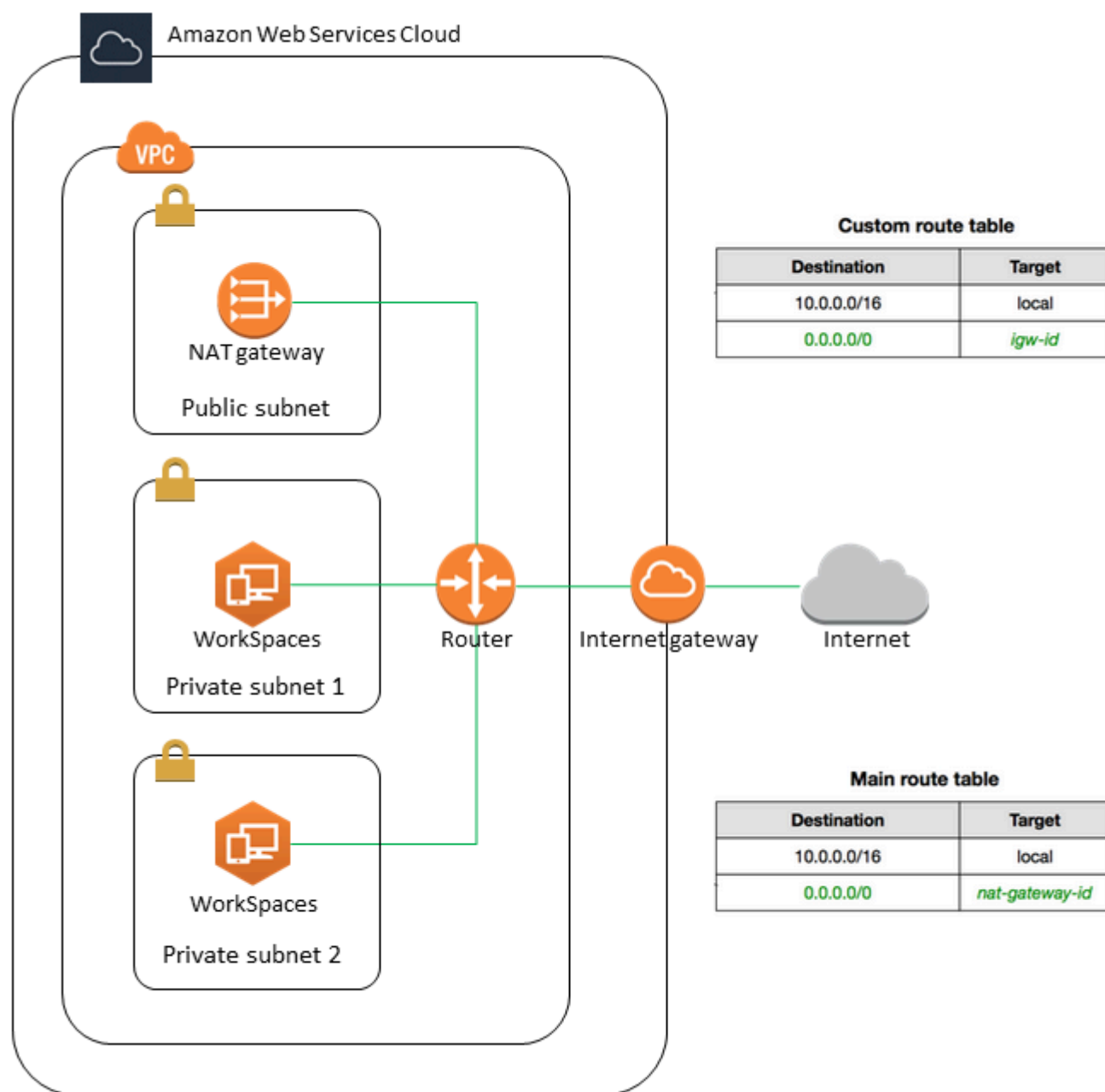
Les sous-réseaux de votre VPC doivent résider dans différentes zones de disponibilité de la région dans laquelle vous le lancez. WorkSpaces Les zones de disponibilité sont des emplacements distincts conçus pour être isolés des défaillances dans d'autres zones de disponibilité. En lançant des instances dans des zones de disponibilité distinctes, vous pouvez protéger vos applications de la défaillance d'un seul emplacement. Chaque sous-réseau doit résider entièrement dans une zone de disponibilité et ne peut pas s'étendre sur plusieurs zones.

Note

Amazon WorkSpaces est disponible dans un sous-ensemble de zones de disponibilité dans chaque région prise en charge. Pour déterminer les zones de disponibilité que vous pouvez utiliser pour les sous-réseaux du VPC que vous utilisez WorkSpaces, consultez. [Zones de disponibilité pour le WorkSpaces personnel](#)

Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT

Si vous créez Directory Service un Microsoft AWS géré ou un Simple AD, nous vous recommandons de configurer le VPC avec un sous-réseau public et deux sous-réseaux privés. Configurez votre répertoire pour le lancer WorkSpaces dans les sous-réseaux privés. Pour fournir un accès Internet WorkSpaces à un sous-réseau privé, configurez une passerelle NAT dans le sous-réseau public.



Pour créer un VPC avec un sous-réseau public et deux sous-réseaux privés

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Sélectionnez Create VPC (Créer un VPC).
3. Sous Resources to create (Ressources à créer), choisissez VPC and more (VPC et autres).
4. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.

5. Pour configurer les sous-réseaux, procédez comme suit :
 - a. Pour Number of Availability Zones (Nombre de zones de disponibilité), choisissez 1 ou 2, selon vos besoins.
 - b. Développez Personnalisez AZs et choisissez vos zones de disponibilité. Sinon, AWS sélectionnez-les pour vous. Pour effectuer une sélection appropriée, consultez [Zones de disponibilité pour le WorkSpaces personnel](#).
 - c. Pour Number of public subnets (Nombre de sous-réseaux publics), assurez-vous de disposer d'un sous-réseau public par zone de disponibilité.
 - d. Pour Nombre de sous-réseaux privés, assurez-vous de disposer d'un sous-réseau privé par zone de disponibilité.
 - e. Entrez un bloc CIDR pour chaque sous-réseau. Pour plus d'informations, voir [Dimensionnement des sous-réseaux](#) dans le Guide de l'utilisateur Amazon VPC.
6. Pour Passerelles NAT, choisissez 1 par AZ.
7. Sélectionnez Create VPC (Créer un VPC).

IPv6 Blocs CIDR

Vous pouvez associer des blocs IPv6 CIDR à votre VPC et à ses sous-réseaux, et configurer ces sous-réseaux pour IPv6 attribuer automatiquement des adresses aux instances nouvellement lancées. Pour les sous-réseaux créés par le client, l'attribution automatique de l'IPv6 adressage est désactivée par défaut. Pour afficher ou mettre à jour ce paramètre dans la console Amazon VPC, choisissez Subnets dans le volet de navigation, sélectionnez le sous-réseau cible, puis choisissez Actions, Modifier les paramètres d'attribution automatique des adresses IP.

Configuration d'un VPC avec des sous-réseaux publics

Si vous préférez, vous pouvez créer un VPC avec deux sous-réseaux publics. Pour fournir un accès Internet WorkSpaces aux sous-réseaux publics, configurez l'annuaire pour attribuer des adresses IP élastiques automatiquement ou manuellement une adresse IP élastique à chacun WorkSpace d'entre eux.

Tâches

- [Étape 1 : Créer un VPC](#)
- [Étape 2 : Attribuez des adresses IP publiques à votre WorkSpaces](#)

Étape 1 : Créer un VPC

Créez un VPC avec un sous-réseau public comme suit.

Pour créer le VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Sélectionnez Create VPC (Créer un VPC).
3. Sous Resources to create (Ressources à créer), choisissez VPC and more (VPC et autres).
4. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
5. Pour configurer les sous-réseaux, procédez comme suit :
 - a. Pour Nombre de zones de disponibilité, choisissez 2.
 - b. Développez Personnalisez AZs et choisissez vos zones de disponibilité. Sinon, AWS sélectionnez-les pour vous. Pour effectuer une sélection appropriée, consultez [Zones de disponibilité pour le WorkSpaces personnel](#).
 - c. Pour Number of public subnets (Nombre de sous-réseaux publics), choisissez 2.
 - d. Pour Number of private subnets (Nombre de sous-réseaux privés), choisissez 0.
 - e. Entrez un bloc CIDR pour chaque sous-réseau public. Pour plus d'informations, voir [Dimensionnement des sous-réseaux](#) dans le Guide de l'utilisateur Amazon VPC.
6. Sélectionnez Create VPC (Créer un VPC).

IPv6 Blocs CIDR

Vous pouvez associer des blocs IPv6 CIDR à votre VPC et à ses sous-réseaux, et configurer ces sous-réseaux pour IPv6 attribuer automatiquement des adresses aux instances nouvellement lancées. Pour les sous-réseaux créés par le client, l'attribution automatique de l'IPv6 adressage est désactivée par défaut. Pour afficher ou mettre à jour ce paramètre dans la console Amazon VPC, choisissez Subnets dans le volet de navigation, sélectionnez le sous-réseau cible, puis choisissez Actions, Modifier les paramètres d'attribution automatique des adresses IP.

Étape 2 : Attribuez des adresses IP publiques à votre WorkSpaces

Vous pouvez attribuer des adresses IP publiques à votre adresse IP WorkSpaces automatiquement ou manuellement. Pour utiliser l'affectation automatique, consultez [the section called "Configuration](#)

des adresses IP automatiques". Pour affecter des adresses IP publiques manuellement, utilisez la procédure suivante.

Pour attribuer une adresse IP publique à WorkSpace un

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Développez la ligne (choisissez l'icône en forme de flèche) pour WorkSpace et notez la valeur de l'WorkSpace adresse IP. Il s'agit de l'adresse IP privée principale du WorkSpace.
4. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
5. Dans le volet de navigation, sélectionnez Elastic IPs. Si aucune adresse IP élastique n'est disponible, choisissez Allouer une adresse IP élastique et choisissez le pool d' IPv4adresses d'Amazon ou le pool d' IPv4adresses appartenant au client, puis choisissez Allouer. Notez la nouvelle adresse IP.
6. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
7. Sélectionnez l'interface réseau de votre WorkSpace. Pour trouver l'interface réseau qui vous convient WorkSpace, entrez la valeur WorkSpace IP (que vous avez notée précédemment) dans le champ de recherche, puis appuyez sur Entrée. La valeur WorkSpace IP correspond à l' IPv4 adresse privée principale de l'interface réseau. Notez que l'ID VPC de l'interface réseau correspond à l'ID de votre WorkSpaces VPC.
8. Choisissez Actions, Gérer les adresses IP. Choisissez Assign new IP (Attribuer une nouvelle adresse IP), puis choisissez Yes, Update (Oui, mettre à jour). Notez la nouvelle adresse IP.
9. Sélectionnez Actions, Associate Address.
10. Sur la page Associate Elastic IP Address (Associer une adresse IP Elastic) choisissez une adresse IP Elastic dans Address (Adresse). Pour Associate to private IP address (Associer à l'adresse IP privée), spécifiez la nouvelle adresse IP privée, puis choisissez Associate Address (Associer l'adresse).

Configurer AWS Global Accelerator (AGA) pour le WorkSpaces personnel

Vous pouvez activer AWS Global Accelerator (AGA) soit au niveau du WorkSpaces répertoire, soit pour l' WorkSpaces exécution individuelle du protocole DCV. Lorsqu'il est activé, le service achemine automatiquement le trafic de streaming vers l'emplacement AWS périphérique le plus proche et sur le réseau AWS mondial, ce qui est redondant et exempt de congestion. Cela permet d'offrir une

expérience de streaming plus réactive et plus stable. Le WorkSpaces service gère entièrement l'utilisation de l'AGA et est soumis à des limites de volume de données sortantes.

Table des matières

- [Prérequis](#)
- [Limites](#)
- [Limites de données sortantes](#)
- [Activer AGA pour un WorkSpaces répertoire](#)
- [Activer AGA pour les particuliers WorkSpaces](#)

Prérequis

- WorkSpaces utilise une série d'IPv4 adresses publiques pour les points de terminaison dédiés à l'accélérateur AWS mondial (AGA). Assurez-vous de configurer vos politiques de pare-feu pour les appareils qui accèdent WorkSpaces via AGA. Si les points de terminaison AGA sont bloqués par le pare-feu, le trafic de WorkSpaces streaming ne sera pas acheminé via AGA. Pour plus d'informations sur les plages d'adresses IP des points de terminaison AGA dans chaque AWS région, consultez [Serveurs de passerelle DCV](#).
- Pour accéder WorkSpaces via AGA, les utilisateurs doivent utiliser la version WorkSpaces client 5.23 ou ultérieure.

Limites

- Vous ne pouvez activer AGA WorkSpaces que pour DCV. Si vous activez AGA au niveau du WorkSpaces répertoire, cela ne s'appliquera qu'au DCV WorkSpaces du répertoire.
- Vous ne pouvez pas activer AGA pour un répertoire (ou pour un répertoire WorkSpaces dans lequel les groupes de contrôle d'accès FIPS et IP sont activés). Vous devez désactiver les groupes de contrôle d'accès FIPS ou IP avant d'activer AGA pour l'annuaire.

Limites de données sortantes

Les limites de volume de données applicables aux WorkSpaces offres groupées sont les suivantes.

- Offres avantageuses, standard et performantes : inclut 20 Go de données sortantes AGA par utilisateur et par mois.

- Forfaits PowerPro d'alimentation et de carte graphique : inclut 50 Go de données sortantes AGA par utilisateur et par mois.

Ces limites de données sortantes visent à couvrir l'utilisation des données par les utilisateurs en streaming depuis leur WorkSpaces. Au-delà de ces limites, le WorkSpaces service peut restreindre l'utilisation de l'AGA et acheminer WorkSpaces le trafic hors de l'AGA sur une case-by-case base donnée.

Activer AGA pour un WorkSpaces répertoire

Vous pouvez configurer les paramètres AGA au niveau du répertoire. Les paramètres s'appliqueront à tous les DCV WorkSpaces du répertoire, sauf si l'individu les remplace. WorkSpaces

Pour activer AGA pour un répertoire

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Dans la colonne ID du répertoire, choisissez l'ID du répertoire pour lequel vous souhaitez configurer les paramètres AGA.
4. Sur la page Détails du répertoire, faites défiler la page jusqu'à la section de configuration de l'accélérateur AWS global (AGA) et choisissez Modifier.
5. Choisissez Activer AGA (automatique).
6. Toujours utiliser le protocole TCP avec AGA est sélectionné par défaut. Si vous le désélectionnez, votre WorkSpaces client déterminera si le protocole TCP ou UDP est utilisé avec AGA en fonction des paramètres du protocole de streaming DCV de vos clients.
7. Choisissez Enregistrer.

Une fois que vous avez activé AGA pour un WorkSpaces répertoire, le DCV WorkSpaces de l'annuaire utilise AGA pour le streaming à partir de la session suivante. Aucun redémarrage n'est nécessaire.

Activer AGA pour les particuliers WorkSpaces

Vous pouvez configurer les paramètres AGA pour chaque individu WorkSpaces, ce qui remplace les paramètres hérités du répertoire auquel WorkSpaces ils sont associés.

Pour activer l'AGA pour les particuliers WorkSpaces

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation WorkSpaces, choisissez Personnel.
3. Dans la colonne WorkSpace ID, choisissez l' WorkSpace ID pour WorkSpace lequel vous souhaitez configurer les paramètres AGA.
4. Sur la page WorkSpaces Détails, faites défiler la page jusqu'à la section de configuration de l'accélérateur AWS global (AGA) et choisissez Modifier.
5. Choisissez Remplacer manuellement les configurations AGA pour cela WorkSpace.
6. Choisissez Activer AGA (automatique).
7. Toujours utiliser le protocole TCP avec AGA est sélectionné par défaut. Si vous le désélectionnez, votre WorkSpaces client déterminera si le protocole TCP ou UDP est utilisé avec AGA en fonction des paramètres du protocole de streaming DCV de vos clients.
8. Choisissez Enregistrer.

Zones de disponibilité pour le WorkSpaces personnel

Lorsque vous créez un cloud privé virtuel (VPC) à utiliser avec Amazon WorkSpaces, les sous-réseaux de votre VPC doivent résider dans différentes zones de disponibilité de la région dans laquelle vous le lancez. WorkSpaces Les zones de disponibilité sont des emplacements distincts conçus pour être isolés des défaillances dans d'autres zones de disponibilité. En lançant des instances dans des zones de disponibilité distinctes, vous pouvez protéger vos applications de la défaillance d'un seul emplacement. Chaque sous-réseau doit résider entièrement dans une zone de disponibilité et ne peut pas s'étendre sur plusieurs zones.

Une zone de disponibilité est représentée par un code de région suivi d'un identifiant à lettre ; par exemple, us-east-1a. Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous associons les zones de disponibilité aux noms de chaque AWS compte de manière indépendante. Par exemple, il se peut que la zone us-east-1a de disponibilité de votre AWS compte ne soit pas la même que celle us-east-1a d'un autre AWS compte.

Pour coordonner les zones de disponibilité entre les comptes, vous devez utiliser un ID de zone de disponibilité, qui représente l'identifiant unique et cohérent d'une zone de disponibilité. Par exemple, use1-az2 il s'agit d'un identifiant AZ pour la us-east-1 région et il a le même emplacement dans tous les AWS comptes.

La visualisation AZ vous IDs permet de déterminer l'emplacement des ressources d'un compte par rapport aux ressources d'un autre compte. Par exemple, si vous partagez avec un autre compte un sous-réseau dans la zone de disponibilité portant l'ID use1-az2, ce sous-réseau est accessible par cet autre compte dans la zone de disponibilité portant également l'ID use1-az2. L'ID de zone de disponibilité de chaque VPC et de chaque sous-réseau s'affiche dans la console Amazon VPC.

Amazon n' WorkSpaces est disponible que dans un sous-ensemble des zones de disponibilité de chaque région prise en charge. Le tableau suivant répertorie l'AZ IDs que vous pouvez utiliser pour chaque région. Pour voir le mappage entre AZ et IDs les zones de disponibilité de votre compte, consultez la section [AZ IDs pour vos ressources](#) dans le guide de AWS RAM l'utilisateur.

Nom de la région	Code région	AZ pris en charge IDs
USA Est (Virginie du Nord)	us-east-1	use1-az2, use1-az4, use1-az6
USA Ouest (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asie-Pacifique (Mumbai)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
Asie-Pacifique (Séoul)	ap-northeast-2	apne2-az1 , apne2-az3
Asie-Pacifique (Singapour)	ap-southeast-1	apse1-az1 , apse1-az2
Asie-Pacifique (Sydney)	ap-southeast-2	apse2-az1 , apse2-az3
Asie-Pacifique (Tokyo)	ap-northeast-1	apne1-az1 , apne1-az4
Canada (Centre)	ca-central-1	cac1-az1, cac1-az2
Europe (Francfort)	eu-central-1	euc1-az2, euc1-az3
Europe (Irlande)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europe (Londres)	eu-west-2	euw2-az2, euw2-az3

Nom de la région	Code région	AZ pris en charge IDs
Europe (Paris)	eu-west-3	euw3-az1, euw3-az2, euw3-az3
Amérique du Sud (São Paulo)	sa-east-1	sae1-az1, sae1-az3
Afrique (Le Cap)	af-south-1	afs1-az1, afs1-az2, afs1-az3
Israël (Tel Aviv)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3
AWS GovCloud (US-Ouest)	us-gov-west-1	usgw1-az1 , usgw1-az2 , usgw1-az3
AWS GovCloud (USA Est)	us-gov-east-1	usge1-az1 , usge1-az2 , usge1-az3

Pour plus d'informations sur les zones de disponibilité et les zones de [disponibilité IDs](#), consultez les [sections Régions, zones de disponibilité et zones locales](#) dans le guide de EC2 l'utilisateur Amazon.

Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal

Pour vous connecter WorkSpaces, le réseau auquel vos WorkSpaces clients sont connectés doit disposer de certains ports ouverts aux plages d'adresses IP des différents AWS services (regroupés en sous-ensembles). Ces plages d'adresses varient selon les AWS régions. De plus, ces mêmes ports doivent être ouverts sur n'importe quel pare-feu qui s'exécute sur le client. Pour plus d'informations sur les plages d'adresses AWS IP des différentes régions, consultez la section [Plages d'adresses AWS IP](#) dans le Référence générale d'Amazon Web Services.

Pour des diagrammes d'architecture supplémentaires, consultez [Best Practices for Deploying Amazon WorkSpaces](#).

Ports pour client

L'application WorkSpaces cliente nécessite un accès sortant sur les ports suivants :

Port 53 (UDP)

Ce port est utilisé pour accéder aux serveurs DNS. Il doit être ouvert sur les adresses IP de votre serveur DNS de manière à permettre au client de résoudre les noms de domaine public. Cette exigence de port est facultative si vous n'utilisez pas de serveurs DNS pour la résolution de noms de domaine.

Port 443 (UDP et TCP)

Ce port est utilisé pour les mises à jour d'application client, l'enregistrement et l'authentification. Les clients de bureau prennent en charge l'utilisation d'un serveur proxy pour le trafic sur le port 443 (HTTPS). Pour activer l'utilisation d'un serveur proxy, ouvrez l'application client, choisissez paramètres Paramètres avancés, sélectionnez Utiliser le serveur proxy, spécifiez l'adresse et le port du serveur proxy et choisissez Enregistrer.

Ce port doit être ouvert aux plages d'adresses IP suivantes :

- Le sous-ensemble AMAZON dans la région GLOBAL.
- Le AMAZON sous-ensemble de la région dans laquelle WorkSpace se trouve le.
- Le sous-ensemble AMAZON dans la région us-east-1.
- Le sous-ensemble AMAZON dans la région us-west-2.
- Le sous-ensemble S3 dans la région us-west-2.

Port 4172 (UDP et TCP)

Ce port est utilisé pour le streaming WorkSpace sur le bureau et les contrôles de santé de l'PCoadresse IP WorkSpaces. Ce port doit être ouvert à la passerelle PCo IP et aux serveurs de contrôle de santé de la région dans laquelle il WorkSpace se trouve. Pour plus d'informations, consultez [Serveur de surveillance de l'état](#) et [PCoServeurs de passerelle IP](#).

Pour l' PCoIP WorkSpaces, les applications clientes de bureau ne prennent pas en charge l'utilisation d'un serveur proxy, ni le déchiffrement TLS ni l'inspection du trafic du port 4172 en UDP (pour le trafic des ordinateurs de bureau). Elles requièrent une connexion directe au port 4172.

Port 4195 (UDP et TCP)

Ce port est utilisé pour le streaming WorkSpace sur le poste de travail et pour les contrôles de santé du DCV WorkSpaces. Ce port doit être ouvert aux plages d'adresses IP de la passerelle DCV et aux serveurs de contrôle de santé de la région dans laquelle elle WorkSpace se trouve.

Pour plus d'informations, consultez [Serveur de surveillance de l'état](#) et [Serveurs de passerelle DCV](#).

Pour le DCV WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et supérieure) et l'application cliente macOS (version 5.4 et supérieure) prennent en charge l'utilisation de serveurs proxy HTTP pour le trafic TCP du port 4195, mais l'utilisation d'un proxy n'est pas recommandée. Le déchiffrement et l'inspection TLS ne sont pas pris en charge. Pour plus d'informations, consultez Configurer les paramètres du serveur proxy de l'appareil pour l'accès à Internet pour [Windows WorkSpaces](#) WorkSpaces, [Amazon Linux](#) et [Ubuntu WorkSpaces](#).

Note

- Si votre pare-feu utilise un filtrage avec état, les ports éphémères (également appelés ports dynamiques) sont automatiquement ouverts pour permettre la communication de retour. Si votre pare-feu utilise un filtrage sans état, vous devez ouvrir les ports éphémères explicitement pour permettre la communication en retour. La plage de ports éphémères requise que vous devez ouvrir varie en fonction de votre configuration.
- La fonction de serveur proxy n'est pas prise en charge pour le trafic UDP. Si vous choisissez d'utiliser un serveur proxy, les appels d'API que l'application client envoie aux WorkSpaces services Amazon sont également transmis par proxy. Les appels d'API et le trafic des espaces de travail doivent passer par le même serveur proxy.
- L'application WorkSpaces cliente tente d'abord de diffuser en utilisant UDP (QUIC) pour des performances optimales. Si le réseau client n'autorise que le protocole TCP, le protocole TCP sera utilisé. Le client WorkSpaces Web se connectera via le port TCP 4195 ou 443. Si le port 4195 est bloqué, le client tentera uniquement de se connecter au port 443.

Ports pour l'accès Web

WorkSpaces Web Access nécessite un accès sortant pour les ports suivants :

Port 53 (UDP)

Ce port est utilisé pour accéder aux serveurs DNS. Il doit être ouvert sur les adresses IP de votre serveur DNS de manière à permettre au client de résoudre les noms de domaine public. Cette

exigence de port est facultative si vous n'utilisez pas de serveurs DNS pour la résolution de noms de domaine.

Port 80 (UDP et TCP)

Ce port est utilisé pour les connexions initiales à `https://clients.amazonworkspaces.com` qui bascule alors vers HTTPS. Il doit être ouvert à toutes les plages d'adresses IP du EC2 sous-ensemble de la région dans laquelle il se Workspace trouve.

Port 443 (UDP et TCP)

Ce port est utilisé pour l'enregistrement et l'authentification avec HTTPS. Il doit être ouvert à toutes les plages d'adresses IP du EC2 sous-ensemble de la région dans laquelle il se Workspace trouve.

Port 4195 (UDP et TCP)

Pour WorkSpaces ce qui est configuré pour le DCV, ce port est utilisé pour diffuser le trafic du WorkSpaces bureau. Ce port doit être ouvert aux plages d'adresses IP de la passerelle DCV. Pour de plus amples informations, veuillez consulter [Serveurs de passerelle DCV](#).

L'accès Web DCV prend en charge l'utilisation d'un serveur proxy pour le trafic TCP du port 4195, mais cela n'est pas recommandé. Pour plus d'informations, consultez Configurer les paramètres du serveur proxy de l'appareil pour l'accès à Internet pour [Windows WorkSpaces](#) WorkSpaces, [Amazon Linux](#) ou [Ubuntu WorkSpaces](#).

Note

- Si votre pare-feu utilise un filtrage avec état, les ports éphémères (également appelés ports dynamiques) sont automatiquement ouverts pour permettre la communication de retour. Si votre pare-feu utilise un filtrage sans état, vous devez ouvrir les ports éphémères explicitement pour permettre la communication en retour. La plage de ports éphémères requise que vous devez ouvrir varie en fonction de votre configuration.
- L'application WorkSpaces cliente tente d'abord de diffuser en utilisant UDP (QUIC) pour des performances optimales. Si le réseau client n'autorise que le protocole TCP, le protocole TCP sera utilisé. Le client WorkSpaces Web se connectera via le port TCP 4195 ou 443. Si le port 4195 est bloqué, le client tentera uniquement de se connecter au port 443.

Généralement, le navigateur Web sélectionne de manière aléatoire un port source dans la plage supérieure à utiliser pour le trafic en continu. WorkSpaces Web Access ne contrôle pas le port sélectionné par le navigateur. Vous devez vérifier que le trafic de retour renvoyé vers ce port est autorisé.

Domaines et adresses IP à ajouter à votre liste d'autorisation

Pour que l'application WorkSpaces cliente puisse accéder au WorkSpaces service, vous devez ajouter les domaines et adresses IP suivants à la liste d'autorisation du réseau à partir duquel le client tente d'accéder au service.

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Domaine ou adresse IP
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/ https://opfcaptcha-prod.s3.cn-north-1.amazonaws.com
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/ - Dans la région AWS GovCloud (ouest des États-Unis) : https://d2td7dqidlhx7.cloudfront.net/prod/pdt/windows/WorkSpacesAppCastx64.xml
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaines (IPv4) : https://skylight-client-ds.us-east-1.amazonaws.com https://skylight-client-ds.us-west-2.amazonaws.com https://skylight-client-ds.ap-south-1.amazonaws.com https://skylight-client-ds.ap-northeast-2.amazonaws.com

Catégorie	Domaine ou adresse IP
	• https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com • https://skylight-client-ds.ap-northeast-1.amazonaws.com • https://skylight-client-ds.ca-central-1.amazonaws.com • https://skylight-client-ds.eu-central-1.amazonaws.com • https://skylight-client-ds.eu-west-1.amazonaws.com • https://skylight-client-ds.eu-west-2.amazonaws.com • https://skylight-client-ds.eu-west-3.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • https://skylight-client-ds.af-south-1.amazonaws.com • https://skylight-client-ds.il-central-1.amazonaws.com • Dans la région AWS GovCloud (ouest des États-Unis) : https://skylight-client-ds.us-gov-west-1.amazonaws.com • Dans la région AWS GovCloud (USA Est) : https://skylight-client-ds.us-gov-east-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	- Dans la région AWS GovCloud (ouest des États-Unis) : https://skylight-client-ds.us-gov-west-1.amazonaws.com - Dans la région AWS GovCloud (USA Est) : https://skylight-client-ds.us-gov-east-1.amazonaws.com Domaines (IPv6) : - skylight-client-dshttps://.eu-west-2.api.aws - skylight-client-dshttps://.eu-west-1.api.aws - skylight-client-dshttps://.us-east-1.api.aws - skylight-client-dshttps://.ap-southeast-1.api.aws - skylight-client-dshttps://.sa-east-1.api.aws - skylight-client-dshttps://.ap-northeast-1.api.aws - skylight-client-dshttps://.us-west-2.api.aws - skylight-client-dshttps://.ap-southeast-2.api.aws - skylight-client-dshttps://.ap-south-1.api.aws - skylight-client-dshttps://.af-south-1.api.aws - skylight-client-dshttps://.eu-central-1.api.aws - skylight-client-dshttps://.ap-northeast-2.api.aws - skylight-client-dshttps://.il-central-1.api.aws - skylight-client-dshttps://.ca-central-1.api.aws - https ://skylight-client-ds. us-gov-east-1.api.aws

Catégorie	Domaine ou adresse IP
	https ://skylight-client-ds. us-gov-west-1.api. aws

Catégorie	Domaine ou adresse IP
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaines (IPv4) : • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com • https://ws-client-service.ap-south-1.amazonaws.com • https://ws-client-service.ap-northeast-2.amazonaws.com • https://ws-client-service.ap-southeast-1.amazonaws.com • https://ws-client-service.ap-southeast-2.amazonaws.com • https://ws-client-service.ap-northeast-1.amazonaws.com • https://ws-client-service.ca-central-1.amazonaws.com • https://ws-client-service.eu-central-1.amazonaws.com • https://ws-client-service.eu-west-1.amazonaws.com • https://ws-client-service.eu-west-2.amazonaws.com • https://ws-client-service.eu-west-3.amazonaws.com • https://ws-client-service.sa-east-1.amazonaws.com • https://ws-client-service.af-south-1.amazonaws.com • https://ws-client-service.il-central-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	- Dans la région AWS GovCloud (ouest des États-Unis) : https://ws-client-service.us-gov-west-1.amazonaws.com - Dans la région AWS GovCloud (USA Est) : https://ws-client-service.us-gov-east-1.amazonaws.com Domaines (IPv6) : - ws-client-servicehttps://.eu-west-2.api.aws - ws-client-servicehttps://.eu-west-1.api.aws - https://ws-client-service.us-east-1.amazonaws.com - ws-client-servicehttps://.ap-southeast-1.api.aws - ws-client-servicehttps://.sa-east-1.api.aws - ws-client-servicehttps://.ap-northeast-1.api.aws - ws-client-servicehttps://.us-west-2.api.aws - ws-client-servicehttps://.ap-southeast-2.api.aws - ws-client-servicehttps://.ap-south-1.api.aws - ws-client-servicehttps://.af-south-1.api.aws - ws-client-servicehttps://.eu-central-1.api.aws - ws-client-servicehttps://.ap-northeast-2.api.aws - ws-client-servicehttps://.il-central-1.api.aws - ws-client-servicehttps://.ca-central-1.api.aws

Catégorie	Domaine ou adresse IP
	• <code>https ://ws-client-service. us-gov-east-1.api. aws</code> • <code>https ://ws-client-service. us-gov-west-1.api. aws</code>

Catégorie	Domaine ou adresse IP
Paramètres d'annuaire	Authentification du client auprès du répertoire et des clients avant de se connecter au WorkSpace : - https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connexions à partir de clients macOS : - https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : - https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : - Hérité : https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID de l'annuaire> - USA Est (Virginie du Nord) : https://d2h1yryv1jxiq.cloudfront.net/ - USA Ouest (Oregon) : https://d1fq42e1gi7rtq.cloudfront.net/ - Asie-Pacifique (Mumbai) : https://d1ctsk4u02kky7.cloudfront.net/ - Asie-Pacifique (Séoul) : https://dyoj3cw6iktvq.cloudfront.net - Asie-Pacifique (Singapour) : https://d1525ef92cauk.cloudfront.net/ - Asie-Pacifique (Sydney) : https://dodwxjr2amr8p.cloudfront.net/

Catégorie	Domaine ou adresse IP
	- Asie-Pacifique (Tokyo) : https://d3v7kcib8ir2e1.cloudfront.net/ - Canada (Centre) : https://d1ebdk07rr01qy.cloudfront.net/ - Europe (Francfort) : https://d39q4y7cndearu.cloudfront.net/ - Europe (Irlande) : https://d2127w6wvrc6l3.cloudfront.net/ - Europe (Londres) : https://df4ahgpxbxqy2.cloudfront.net/ - Europe (Paris) — https://d2kmf63k5sit88.cloudfront.net/ - Amérique du Sud (São Paulo) : https://d2nezqurrjvain.cloudfront.net/ - Afrique (Le Cap) : https://dr6ry0pwao y23.cloudfront.net - Israël (Tel Aviv) — https://d2kmf63k5sit88.cloudfront.net Fichier CSS pour le style des pages de connexion : https://d3s98kk2h6f4oh.cloudfront.net/ https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : - USA Est (Virginie du Nord) : https://d32i4gd7pg4909.cloudfront.net/ - USA Ouest (Oregon) : https://d18af777lco7lp.cloudfront.net/

Catégorie	Domaine ou adresse IP
	• Asie-Pacifique (Mumbai) : https://d78hovzzqqtbsb.cloudfront.net/ • Asie-Pacifique (Séoul) : https://dtyv4uwoh7ynt.cloudfront.net/ • Asie-Pacifique (Singapour) : https://d3qzmd7y07pz0i.cloudfront.net/ • Asie-Pacifique (Sydney) : https://dwcpoxuuza83q.cloudfront.net/ • Asie-Pacifique (Tokyo) : https://d2c2t8mxjhq5z1.cloudfront.net/ • Canada (Centre) : https://d2wfbsypmqjmog.cloudfront.net/ • Europe (Francfort) : https://d1whcm49570jjw.cloudfront.net/ • Europe (Irlande) : https://d3pgffbf39h4k4.cloudfront.net/ • Europe (Londres) : https://d16q6638mh01s7.cloudfront.net/ • Europe (Paris) — https://d1a3pnge9on3sx.cloudfront.net/ • Amérique du Sud (São Paulo) : https://d2lh2qc5bdoq4b.cloudfront.net/ • Afrique (Le Cap) : https://di5ygl2cs0mrh.cloudfront.net/ • Israël (Tel Aviv) — https://d1a3pnge9on3sx.cloudfront.net Dans la région AWS GovCloud (ouest des États-Unis) : • Paramètres d'annuaire de client :

Catégorie	Domaine ou adresse IP
	<a href="https://s3.amazonaws.com/workspaces-client-properties/produit/pdt/<directory ID>">https://s3.amazonaws.com/workspaces-client-properties/produit/pdt/<directory ID> - Graphiques de page de connexion pour le comarquage de niveau annuaire de client : https://workspace-client-assets-pdt.s3-us-gov-west-1.amazonaws.com - Fichier CSS pour le style des pages de connexion : https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css - JavaScript fichier pour les pages de connexion : Non applicable Dans la région AWS GovCloud (USA Est) : - Paramètres d'annuaire de client : <a href="https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID>">https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID> - Graphiques de page de connexion pour le comarquage de niveau annuaire de client : https://workspace-client-assets-pdt.s3-us-gov-east-1.amazonaws.com - Fichier CSS pour le style des pages de connexion : https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css - JavaScript fichier pour les pages de connexion :

Catégorie	Domaine ou adresse IP
	Non applicable
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	• https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-southeast-2.apps.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.ap-northeast-1.apps.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.eu-west-1.apps.signin.aws • https://smartcard.us-east-1.signin.aws • https://smartcard.us-east-1.apps.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.us-west-2.apps.signin.aws • https://smartcard.us-gov-east-1.signin-fips.amazonaws-us-gov.com • https://smartcard.us-gov-east-1.apps.signin-fips.amazonaws-us-gov.com • https://smartcard.us-gov-west-1.signin.amazonaws-us-gov.com • https://smartcard.us-gov-west-1.apps.signin.amazonaws-us-gov.com • https://smartcard.signin.amazonaws-us-gov.com

Catégorie	Domaine ou adresse IP
Pages de connexion utilisateur	• https://af-south-1.signin.aws • https://af-south-1.signin.aws.amazon.com • https://af-south-1.sso.signin.aws • https://af-south-1.apps.signin.aws • https://ap-south-1.signin.aws • https://ap-south-1.signin.aws.amazon.com • https://ap-south-1.sso.signin.aws • https://ap-south-1.apps.signin.aws • https://ap-southeast-1.signin.aws • https://ap-southeast-1.signin.aws.amazon.com • https://ap-southeast-1.sso.signin.aws • https://ap-southeast-1.apps.signin.aws • https://ap-southeast-2.signin.aws • https://ap-southeast-2.signin.aws.amazon.com • https://ap-southeast-2.sso.signin.aws • https://ap-southeast-2.apps.signin.aws • https://ap-northeast-1.signin.aws • https://ap-northeast-1.signin.aws.amazon.com • https://ap-northeast-1.sso.signin.aws • https://ap-northeast-1.apps.signin.aws • https://ap-northeast-2.signin.aws • https://ap-northeast-2.signin.aws.amazon.com • https://ap-northeast-2.sso.signin.aws • https://ap-northeast-2.apps.signin.aws • https://ca-central-1.signin.aws

Catégorie	Domaine ou adresse IP
	• https://ca-central-1.signin.aws.amazon.com • https://ca-central-1.sso.signin.aws • https://ca-central-1.apps.signin.aws • https://eu-central-1.signin.aws • https://eu-central-1.signin.aws.amazon.com • https://eu-central-1.sso.signin.aws • https://eu-central-1.apps.signin.aws • https://eu-west-1.signin.aws • https://eu-west-1.signin.aws.amazon.com • https://eu-west-1.sso.signin.aws • https://eu-west-1.apps.signin.aws • https://eu-west-2.signin.aws • https://eu-west-2.signin.aws.amazon.com • https://eu-west-2.sso.signin.aws • https://eu-west-2.apps.signin.aws • https://eu-west-3.signin.aws • https://eu-west-3.signin.aws.amazon.com • https://eu-west-3.sso.signin.aws • https://eu-west-3.apps.signin.aws • https://il-central-1.signin.aws • https://il-central-1.signin.aws.amazon.com • https://il-central-1.sso.signin.aws • https://il-central-1.apps.signin.aws • https://sa-east-1.signin.aws • https://sa-east-1.signin.aws.amazon.com • https://sa-east-1.sso.signin.aws • https://sa-east-1.apps.signin.aws • https://us-east-1.signin.aws • https://us-east-1.signin.aws.amazon.com

Catégorie	Domaine ou adresse IP
	• https://us-east-1.sso.signin.aws • https://us-east-1.apps.signin.aws • https://us-west-2.signin.aws • https://us-west-2.signin.aws.amazon.com • https://us-west-2.sso.signin.aws • https://us-west-2.apps.signin.aws • https://us-gov-east-1.signin-fips.amazonaws-us-gov.com • https://us-gov-east-1.sso.signin-fips.aws-us-gov.com • https://us-gov-east-1.apps.signin-fips.aws-us-gov.com • https://us-gov-west-1.signin.amazonaws-us-gov.com • https://us-gov-west-1.sso.signin.aws-us-gov.com • https://us-gov-west-1.apps.signin.aws-us-gov.com <i>directory_id</i> https://awsapps.com/  Note L'identifiant du répertoire est le domaine du client. Dans les régions AWS GovCloud (ouest des États-Unis) et AWS GovCloud (est des États-Unis) : https://login.us-gov-home.awsapps.com/directory/<i>directory id</i>/

Catégorie	Domaine ou adresse IP
	 Note L'identifiant du répertoire est le domaine du client.

Catégorie	Domaine ou adresse IP
Agent WS	Domaines (IPv4) : • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com • https://ws-broker-service.ap-south-1.amazonaws.com • https://ws-broker-service.ap-northeast-2.amazonaws.com • https://ws-broker-service.ap-southeast-1.amazonaws.com • https://ws-broker-service.ap-southeast-2.amazonaws.com • https://ws-broker-service.ap-northeast-1.amazonaws.com • https://ws-broker-service.ca-central-1.amazonaws.com • https://ws-broker-service.eu-central-1.amazonaws.com • https://ws-broker-service.eu-west-1.amazonaws.com • https://ws-broker-service.eu-west-2.amazonaws.com • https://ws-broker-service.eu-west-3.amazonaws.com • https://ws-broker-service.sa-east-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	• https://ws-broker-service.af-south-1.amazonaws.com • https://ws-broker-service.il-central-1.amazonaws.com • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com • https://ws-broker-service.us-gov-east-1.amazonaws.com • https://ws-broker-service-fips.us-gov-east-1.amazonaws.com Domaines (IPv6) : • ws-broker-servicehttps://.eu-west-3.api.aws • ws-broker-servicehttps://.eu-west-2.api.aws • ws-broker-servicehttps://.eu-west-1.api.aws • ws-broker-servicehttps://.us-east-1.api.aws • ws-broker-servicehttps://.us-west-2.api.aws • ws-broker-servicehttps://.eu-central-1.api.aws • ws-broker-servicehttps://.ap-northeast-1.api.aws • ws-broker-servicehttps://.ap-northeast-2.api.aws • ws-broker-servicehttps://.ap-southeast-1.api.aws • ws-broker-servicehttps://.ap-southeast-2.api.aws • ws-broker-servicehttps://.sa-east-1.api.aws • ws-broker-servicehttps://.ap-south-1.api.aws

Catégorie	Domaine ou adresse IP
	- ws-broker-servicehttps://.af-south-1.api.aws - ws-broker-servicehttps://.ca-central-1.api.aws - ws-broker-servicehttps://.il-central-1.api.aws - https ://ws-broker-service. us-gov-west-1.api. aws - https ://ws-broker-service. us-gov-east-1.api. aws - ws-broker-service-fipshttps://.us-west-2.api. aws - ws-broker-service-fipshttps://.us-east-1.api. aws - https ://ws-broker-service-fips. us-gov-we st-1.api.aws - https ://ws-broker-service-fips. us-gov-ea st-1.api.aws

Catégorie	Domaine ou adresse IP
WorkSpaces Points de terminaison de l'API	Domaines (IPv4) : • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.eu-west-3.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	• https://workspaces.af-south-1.amazonaws.com • https://workspaces.il-central-1.amazonaws.com • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com • https://workspaces.us-gov-east-1.amazonaws.com • https://workspaces-fips.us-gov-east-1.amazonaws.com Domaines (IPv6) : • https://workspaces.eu-west-3.api.aws • https://workspaces.eu-west-2.api.aws • https://workspaces.eu-west-1.api.aws • https://workspaces.us-east-1.api.aws • https://workspaces.us-west-2.api.aws • https://workspaces.eu-central-1.api.aws • https://workspaces.ap-northeast-1.api.aws • https://workspaces.ap-northeast-2.api.aws • https://workspaces.ap-southeast-1.api.aws • https://workspaces.ap-southeast-2.api.aws • https://workspaces.sa-east-1.api.aws • https://workspaces.ap-south-1.api.aws • https://workspaces.af-south-1.api.aws • https://workspaces.ca-central-1.api.aws • https://workspaces.il-central-1.api.aws • https://workspaces.us-gov-west-1.api.aws

Catégorie	Domaine ou adresse IP
	• https://workspaces.us-gov-east-1.api.aws • https://workspaces-fips.us-west-2.api.aws • https://workspaces-fips.us-east-1.api.aws • https://workspaces-fips.us-gov-west-1.api.aws • https://workspaces-fips.us-gov-east-1.api.aws

Catégorie	Domaine ou adresse IP
WorkSpaces Points de terminaison pour l'authentification unique (SSO) SAML	Domaines: • https://euc-ss0-sm.us-east-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm-fips.us-east-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.us-west-2.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm-fips.us-west-2.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.ap-south-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.ap-northeast-2.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.ap-southeast-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.ap-southeast-2.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.ap-northeast-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.eu-central-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.eu-west-2.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.eu-west-3.amazonaws.com/v1/signaler le rythme cardiaque

Catégorie	Domaine ou adresse IP
	• https://euc-ss0-sm.af-south-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.il-central-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.us-gov-west-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm-fips.us-gov-west-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm.us-gov-east-1.amazonaws.com/v1/signaler le rythme cardiaque • https://euc-ss0-sm-fips.us-gov-east-1.amazonaws.com/v1/signaler le rythme cardiaque

Domaines et adresses IP à ajouter à votre liste d'adresses PCo IP autorisées

Catégorie	Domaine ou adresse IP
PCoPasserelle de session IP (PSG)	PCoServeurs de passerelle IP
Session Broker (PCM)	Domaines (IPv4) : • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	• https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com • https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.eu-west-3.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com • https://skylight-cm.us-gov-east-1.amazonaws.com • https://skylight-cm-fips.us-gov-east-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	Domaines (IPv6) : • https://skylight-cm.us-east-1.api.aws • https://skylight-cm.us-west-2.api.aws • https://skylight-cm.eu-west-3.api.aws • https://skylight-cm.eu-west-2.api.aws • https://skylight-cm.eu-west-1.api.aws • https://skylight-cm.eu-central-1.api.aws • https://skylight-cm.ap-northeast-1.api.aws • https://skylight-cm.ap-northeast-2.api.aws • https://skylight-cm.ap-southeast-1.api.aws • https://skylight-cm.ap-southeast-2.api.aws • https://skylight-cm.ap-south-1.api.aws • https://skylight-cm.sa-east-1.api.aws • https://skylight-cm.af-south-1.api.aws • https://skylight-cm.ca-central-1.api.aws • https://skylight-cm.il-central-1.api.aws • https://skylight-cm.us-gov-west-1.api.aws • https://skylight-cm.us-gov-east-1.api.aws • skylight-cm-fipshttps://.us-west-2.api.aws • skylight-cm-fipshttps://.us-east-1.api.aws • https://skylight-cm-fips.us-gov-west-1.api.aws • https://skylight-cm-fips.us-gov-east-1.api.aws

Catégorie	Domaine ou adresse IP
Serveurs TURN d'accès Web pour PCo IP	Serveurs : • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • L'accès Web n'est actuellement pas disponible dans la région Asie-Pacifique (Mumbai). • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • Web Access n'est actuellement pas disponible dans la région Afrique (Le Cap) • Web Access n'est actuellement pas disponible dans la région Israël (Tel Aviv).

Domaines et adresses IP à ajouter à votre liste d'autorisations pour le DCV

Catégorie	Domaine ou adresse IP
Passerelle de session DCV (WSG)	Serveurs de passerelle DCV
Serveurs TURN d'accès Web pour DCV	Serveurs de passerelle DCV

Serveur de surveillance de l'état

Les applications WorkSpaces clientes effectuent des contrôles de santé sur les ports 4172 et 4195. Ces contrôles permettent de vérifier si le trafic TCP ou UDP circule des WorkSpaces serveurs vers

les applications clientes. Pour que ces surveillances aboutissent, les politiques de pare-feu doivent autoriser le trafic sortant vers les adresses IP des serveurs régionaux de surveillance de l'état PColP suivants.

Région	Nom d'hôte de vérification de l'état	Adresses IP
USA Est (Virginie du Nord)	IPv4:	IPv4:
	drp-iad.amazonworkspaces.com	3.209.215.252
		3.212.50.30
	IPv6:	3.225.55.35
	drp-workspaces.us-east-1.api.aws	3.226.24.234
		34.200.29.95
		52.200.219.150
USA Ouest (Oregon)		IPv6:
		2600:11 de 18:74 ou 9:44:/56
	IPv4:	IPv4:
	drp-pdx.amazonworkspaces.com	34.217.248.177
		52.34.160.80
	IPv6:	54.68.150.54
	drp-workspaces.us-west-2.api.aws	54.185.4.125
		54.188.171.18
		54.244.158.140
		IPv6:
		2600:01 ou 14:27:5700 : /56

Région	Nom d'hôte de vérification de l'état	Adresses IP
Asie-Pacifique (Mumbai)	IPv4: drp-bom.amazonworkspaces.com IPv6: drp-workspaces.ap-south-1.api.aws	IPv4: 13,127,57,82 13,234,250,73 IPv6: 2406:da1a:502 : b800 : :/56
Asie-Pacifique (Séoul)	IPv4: drp-icn.amazonworkspaces.com IPv6: drp-workspaces.ap-northeast-2.api.aws	IPv4: 13.124.44.166 13.124.203.105 52.78.44.253 52.79.54.102 IPv6: 2406:da12:c8c:4900 : :/56
Asie-Pacifique (Singapour)	IPv4: drp-sin.amazonworkspaces.com IPv6: drp-workspaces.ap-southeast-1.api.aws	IPv4: 3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118 IPv6: 2406:de 18:99:04 à 00:/56

Région	Nom d'hôte de vérification de l'état	Adresses IP
Asie-Pacifique (Sydney)	IPv4: drp-syd.amazonworkspaces.com IPv6: drp-workspaces.ap-southeast-2.api.aws	IPv4: 3.24.11.127 13.237.232.125 IPv6: 2406:da1c:9b 5:9 d00 : :/56
Asie-Pacifique (Tokyo)	IPv4: drp-nrt.amazonworkspaces.com IPv6: drp-workspaces.ap-northeast-1.api.aws	IPv4: 18.178.102.247 54.64.174.128 IPv6: 2406:da 14:785:5300 :/56
Canada (Centre)	IPv4: drp-yul.amazonworkspaces.com IPv6: drp-workspaces.ca-central-1.api.aws	IPv4: 52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0 IPv6: 2600:01 ou 11:759:d900 : :/56

Région	Nom d'hôte de vérification de l'état	Adresses IP
Europe (Francfort)	IPv4: drp-fra.amazonworkspaces.com IPv6: drp-workspaces.eu-central-1.api.aws	IPv4: 52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227 IPv6: 2a05:d014:b5c:500 : /56
Europe (Irlande)	IPv4: drp-dub.amazonworkspaces.com IPv6: drp-workspaces.eu-west-1.api.aws	IPv4: 18.200.177.86 52.48.86.38 54.76.137.224 IPv6: 2h05:d 018:10 caf:400 : /56
Europe (Londres)	IPv4: drp-lhr.amazonworkspaces.com IPv6: drp-workspaces.eu-west-2.api.aws	IPv4: 35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36 IPv6: 2a05:d01c:263 : f400 : /56

Région	Nom d'hôte de vérification de l'état	Adresses IP
Europe (Paris)	IPv4: drp-cdg.amazonworkspaces.com IPv6: drp-workspaces.eu-west-3.ap i.aws	IPv4: 51,17,52,90 51,17,109,231 51,16,190,43 IPv6: 2a05:d 012:16:8600 :/56
Amérique du Sud (São Paulo)	IPv4: drp-gru.amazonworkspaces.com IPv6: drp-workspaces.sa-east-1.ap i.aws	IPv4: 18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234 IPv6: 2600:1 f1e:bbf:fa00 : /56
Afrique (Le Cap)	IPv4: drp-cpt.amazonworkspaces.com/ IPv6: drp-workspaces.af-south-1.a pi.aws	IPv4: 13,244,128,155 13,245,205,255 13,245216,116 IPv6: 2406:da 11:685:2400 :/56

Région	Nom d'hôte de vérification de l'état	Adresses IP
Israël (Tel Aviv)	IPv4: drp-tlv.amazonworkspaces.com/ IPv6: drp-workspaces.il-central-1.api.aws	IPv4: 51,17,52,90 51,17,109,231 51,16,190,43 IPv6: 2a05:d025:c78:fc00 : /56
AWS GovCloud (US-Ouest)	IPv4: drp-pdt.amazonworkspaces.com IPv6: espaces de travail en ligne. us-gov-west-1.api.aws	IPv4: 52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88 IPv6: 2600:01 ou 12:28 f:af00 : /56
AWS GovCloud (USA Est)	IPv4: drp-osu.amazonworkspaces.com IPv6: espaces de travail en ligne. us-gov-east-1.api.aws	IPv4: 18,253,251,70 18,254,0,118 IPv6: 2600 : 1 f15 : a 45:3 e00 : /56

PCoServeurs de passerelle IP

WorkSpaces utilise PCoIP pour diffuser la session de bureau aux clients via le port 4172. Pour ses serveurs de passerelle PCoIP, WorkSpaces utilise une petite gamme d'adresses publiques et d'adresses Amazon EC2. IPv4 IPv6 Cela vous permet de définir des stratégies de pare-feu plus précises pour les appareils qui accèdent à WorkSpaces. Notez que le WorkSpaces client donne la priorité aux IPv6 connexions lorsqu'elles sont prises en charge et IPv6 que les passerelles sont accessibles. S'il n' IPv6 est pas disponible, il revient à IPv4.

Région	Code région	Plage d'adresses IP publiques
USA Est (Virginie du Nord)	us-east-1	3.217.228.0 - 3.217.231.255
		3.235.112.0 - 3.235.119.255
		52.23.61.0 - 52.23.62.255
		2600:1 de 32:8000 : :/39
USA Ouest (Oregon)	us-west-2	35,80,88,0 - 35,80,95,255
		44.234.54.0 - 44.234.55.255
		54.244.46.0 - 54.244.47.255
		2600:1 de 32:4000 : :/39
Asie-Pacifique (Mumbai)	ap-south-1	13,126,243,0 - 13,126,243,255
		2406:da32:a000 : :/40
Asie-Pacifique (Séoul)	ap-northeast-2	3.34.37.0 - 3.34.37.255
		3.34.38.0 - 3.34.39.255
		13.124.247.0 - 13.124.247.255
		2406 : à partir de 32:20 : /40
Asie-Pacifique (Singapour)	ap-southeast-1	18.141.152.0 - 18.141.152.255
		18.141.154.0 - 18.141.155.255

Région	Code région	Plage d'adresses IP publiques
		52.76.127.0 - 52.76.127.255 2406:da 32:8:00 :/40
Asie-Pacifique (Sydney)	ap-southeast-2	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255 2406:da32:c000 : /40
Asie-Pacifique (Tokyo)	ap-northeast-1	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255 2406:da 32:40:/40
Canada (Centre)	ca-central-1	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255 2600:1 de 32:1000:/40
Europe (Francfort)	eu-central-1	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255 2a05:d 032:4000 : /40
Europe (Irlande)	eu-west-1	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255 2a05:d 032:8000 : /40

Région	Code région	Plage d'adresses IP publiques
Europe (Londres)	eu-west-2	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255 2a05:d032:c000 : :/40
Europe (Paris)	eu-west-3	51,44,204,0-51,44,207,255
Amérique du Sud (São Paulo)	sa-east-1	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255 2600:1 f32:e000 : :/40
Afrique (Le Cap)	af-south-1	13,246,120,0 - 13,246,123,255 2406 : à partir de 32:100:/40
Israël (Tel Aviv)	il-central-1	51,17,28,0-51,17,31,255 2a05:d 02:5000 : :/40
AWS GovCloud (US-Ouest)	us-gov-west-1	52.61.193.0 - 52.61.193.255 2600:1 de 32:2000 : :/40
AWS GovCloud (USA Est)	us-gov-east-1	18,254,140,0 - 18,254,143,255 2600:1 de 32:5000 : :/40

Serveurs de passerelle DCV

Important

À partir de juin 2020, WorkSpaces diffuse la session de bureau pour DCV WorkSpaces aux clients via le port 4195 au lieu du port 4172. Si vous souhaitez utiliser le DCV WorkSpaces, assurez-vous que le port 4195 est ouvert au trafic.

Note

Pour les WorkSpaces pools non BYOL, les plages d'adresses IP ne sont pas garanties. Vous devez plutôt autoriser la liste des noms de domaine de la passerelle DCV. Pour plus d'informations, consultez la section [Noms de domaine de la passerelle DCV](#).

WorkSpaces utilise une petite plage d'adresses publiques IPv4 et d'IPv6 adresses Amazon EC2 pour ses serveurs de passerelle DCV. Cela vous permet de définir des politiques de pare-feu plus précises pour les appareils qui y accèdent WorkSpaces. WorkSpaces utilise une plage d'IPv4 adresses publiques distincte pour les points de terminaison dédiés à l'accélérateur AWS global (AGA). Assurez-vous de configurer vos politiques de pare-feu pour autoriser la liste des plages d'adresses IP si vous prévoyez d'activer AGA pour votre WorkSpaces. Notez que le WorkSpaces client donne la priorité aux IPv6 connexions lorsqu'elles sont prises en charge et IPv6 que les passerelles sont accessibles. S'il n'IPv6 est pas disponible, il revient à IPv4.

Si vous utilisez AGA + IPv6, vous devez autoriser la liste des plages IPv6 CIDR à partir des GLOBALACCELERATOR plages. Pour plus d'informations, reportez-vous à la section [Emplacement et plages d'adresses IP des serveurs Global Accelerator Edge](#) dans le Guide du développeur de AWS Global Accelerator.

Région	Code région	Plage d'adresses IP publiques
USA Est (Virginie du Nord)	us-east-1	3,227,4,0/22 44,209,84,0/22 93.77.138.0/24 (points de terminaison AGA)

Région	Code région	Plage d'adresses IP publiques
		93.77.139.0/24 (points de terminaison AGA) 2600:1 de 28:34 c : :/48
USA Est (Ohio)	us-east-2	3,146,84,0/22 93.77.130.0/24 (points de terminaison AGA) 93.77.131.0/24 (points de terminaison AGA) 2600:1 de 26:28 : :/48
USA Ouest (Oregon)	us-west-2	34,223,96,0/22 93.77.148.0/24 (points de terminaison AGA) 93.77.149.0/24 (points de terminaison AGA) 2600:11 de 24:34 :/48
Asie-Pacifique (Mumbai)	ap-south-1	65,1156,0/22 93.77.142.0/24 (points de terminaison AGA) 93.77.143.0/24 (points de terminaison AGA) 2406:da2a:14 : :/48
Asie-Pacifique (Séoul)	ap-northeast-2	3,35,160,0/22 93.77.156.0/24 (points de terminaison AGA) 93.77.157.0/24 (points de terminaison AGA) 2406 à 22:44 :/48

Région	Code région	Plage d'adresses IP publiques
Asie-Pacifique (Singapour)	ap-southeast-1	• 13,212,1322,0/22 • 93.77.158.0/24 (points de terminaison AGA) • 93.77.159.0/24 (points de terminaison AGA) • 2406 : à partir de 28:/48
Asie-Pacifique (Sydney)	ap-southeast-2	• 3,25,248,0/22 • 93.77.150.0/24 (points de terminaison AGA) • 93.77.151.0/24 (points de terminaison AGA) • 2406:da2c:24 : :/48
Asie-Pacifique (Malaisie)	ap-southeast-5	• 43,217,232,0/22
Asie-Pacifique (Tokyo)	ap-northeast-1	• 3,1114,164,0/22 • 93.77.134.0/24 (points de terminaison AGA) • 93.77.135.0/24 (points de terminaison AGA) • 2406 : à partir de 24:28 : /48
Canada (Centre)	ca-central-1	• 3,97,20,0/22 • 93.77.128.0/24 (points de terminaison AGA) • 93.77.129.0/24 (points de terminaison AGA) • 26001:21 ou 21:8:/48

Région	Code région	Plage d'adresses IP publiques
Europe (Francfort)	eu-central-1	• 18,2192.216,0/22 • 93.77.154.0/24 (points de terminaison AGA) • 93.77.155.0/24 (points de terminaison AGA) • 2a05:d 02:18:/48
Europe (Irlande)	eu-west-1	• 3,248,176,0/22 • 93.77.132.0/24 (points de terminaison AGA) • 93.77.133.0/24 (points de terminaison AGA) • 2h05:d 028:40:/48
Europe (Londres)	eu-west-2	• 18,134,68,0/22 • 93.77.140.0/24 (points de terminaison AGA) • 93.77.141.0/24 (points de terminaison AGA) • 2a05:d02c:8 : /48
Europe (Paris)	eu-west-3	• 51,44,72,0/22 • 93.77.144.0/24 (points de terminaison AGA) • 93.77.145.0/24 (points de terminaison AGA) • 2a05:d 02:21 c : /48

Région	Code région	Plage d'adresses IP publiques
Amérique du Sud (São Paulo)	sa-east-1	15,228,64,0/22 93.77.146.0/24 (points de terminaison AGA) 93.77.147.0/24 (points de terminaison AGA) 2600:1 f2e:14 : :/48
Afrique (Le Cap)	af-south-1	13,246,108,0/22 93.77.136.0/24 (points de terminaison AGA) 93.77.137.0/24 (points de terminaison AGA) 2406:da21:c : :/48
Israël (Tel Aviv)	il-central-1	51,17,72,0/22 93.77.152.0/24 (points de terminaison AGA) 93.77.153.0/24 (points de terminaison AGA) 2a05:d 025:1000 : :/48
AWS GovCloud (US-Ouest)	us-gov-west-1	3,32,139,0/24 3,30,129,0/24 3,30,130,0/23 2600:11 ou 22:28:/48
AWS GovCloud (USA Est)	us-gov-east-1	18,254,148,0/22 2600:1 de 25:14 : :/48

Noms de domaine de passerelle DCV

Le tableau suivant répertorie les noms de domaine de la WorkSpace passerelle DCV. Ces domaines doivent être joignables pour que l'application WorkSpaces cliente puisse accéder au service WorkSpace DCV.

Région	Domaine
USA Est (Virginie du Nord)	*.prod.us-east-1.highlander.aws.a2z.com (FIPS) *.wsp-fips.prod.us-east-1.highlander.aws.a2z.com
USA Ouest (Oregon)	*.prod.us-west-2.highlander.aws.a2z.com (FIPS) *.wsp-fips.prod.us-west-2.highlander.aws.a2z.com
Asie-Pacifique (Mumbai)	*.prod.ap-south-1.highlander.aws.a2z.com
Asie-Pacifique (Séoul)	*.prod.ap-northeast-2.highlander.aws.a2z.com
Asie-Pacifique (Singapour)	*.prod.ap-southeast-1.highlander.aws.a2z.com
Asie-Pacifique (Sydney)	*.prod.ap-southeast-2.highlander.aws.a2z.com
Asie-Pacifique (Tokyo)	*.prod.ap-northeast-1.highlander.aws.a2z.com
Canada (Centre)	*.prod.ca-central-1.highlander.aws.a2z.com
Europe (Francfort)	*.prod.eu-central-1.highlander.aws.a2z.com
Europe (Irlande)	*.prod.eu-west-1.highlander.aws.a2z.com
Europe (Londres)	*.prod.eu-west-2.highlander.aws.a2z.com
Europe (Paris)	*.prod.eu-west-3.highlander.aws.a2z.com
Amérique du Sud (São Paulo)	*.prod.sa-east-1.highlander.aws.a2z.com
Afrique (Le Cap)	*.prod.af-south-1.highlander.aws.a2z.com

Région	Domaine
Israël (Tel Aviv)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (US-Ouest)	*.prod.us-gov-west-1.highlander.aws.a2z.com (FIPS) *.wsp-fips.prod.us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (USA Est)	*.prod.us-gov-east-1.highlander.aws.a2z.com (FIPS) *.wsp-fips.prod.us-gov-east-1.highlander.aws.a2z.com

Interfaces réseau

Chacune WorkSpace possède les interfaces réseau suivantes :

- L'interface réseau principale (eth1) fournit la connectivité aux ressources de votre VPC et sur Internet, et est utilisée pour WorkSpace les joindre au répertoire.
- L'interface réseau de gestion (eth0) est connectée à un réseau de gestion WorkSpaces sécurisé. Il est utilisé pour le streaming interactif du WorkSpace bureau vers WorkSpaces les clients, et pour WorkSpaces permettre de gérer le WorkSpace.

WorkSpaces sélectionne l'adresse IP de l'interface réseau de gestion parmi différentes plages d'adresses, en fonction de la région dans laquelle WorkSpaces elles sont créées. Lorsqu'un répertoire est enregistré, WorkSpaces testez le CIDR du VPC et les tables de routage de votre VPC pour déterminer si ces plages d'adresses créent un conflit. Si un conflit est détecté dans toutes les plages d'adresses disponibles de la région, un message d'erreur s'affiche et l'annuaire n'est pas enregistré. Si vous modifiez les tables de routage de votre VPC après l'enregistrement de l'annuaire, vous risquez de créer un conflit.

Warning

Ne modifiez ni ne supprimez aucune des interfaces réseau associées à un WorkSpace. Cela pourrait les WorkSpace rendre inaccessibles ou perdre l'accès à Internet. Par exemple, si vous avez [activé l'attribution automatique des adresses IP élastiques](#) au niveau du

répertoire, une [adresse IP élastique](#) (issue du pool fourni par Amazon) vous est attribuée WorkSpace lors de son lancement. Toutefois, si vous associez une adresse IP élastique que vous possédez à un WorkSpace, puis que vous dissociez ensuite cette adresse IP élastique du WorkSpace, celui-ci WorkSpace perd son adresse IP publique et n'en obtient pas automatiquement une nouvelle depuis le pool fourni par Amazon.

Pour associer une nouvelle adresse IP publique provenant du pool fourni par Amazon au WorkSpace, vous devez [reconstruire](#) le WorkSpace. Si vous ne souhaitez pas reconstruire le WorkSpace, vous devez associer une autre adresse IP élastique que vous possédez au WorkSpace.

Plages IP de l'interface de gestion

Le tableau suivant répertorie les plages d'adresses IP utilisées pour l'interface réseau de gestion.

Note

- Si vous utilisez Windows Bring Your Own License (BYOL) WorkSpaces, les plages d'adresses IP indiquées dans le tableau suivant ne s'appliquent pas. PCoIP BYOL WorkSpaces utilise plutôt la plage d'adresses IP 54.239.224.0/20 pour le trafic de l'interface de gestion dans toutes les régions. AWS Pour Windows DCV BYOL WorkSpaces, les plages d'adresses IP 54.239.224.0/20 et 10.0.0.0/8 s'appliquent à toutes les régions. AWS (Ces plages d'adresses IP sont utilisées en plus du bloc CIDR /16 que vous sélectionnez pour le trafic de gestion de votre WorkSpaces BYOL.)
- Si vous utilisez un DCV WorkSpaces créé à partir de bundles publics, la plage d'adresses IP 10.0.0.0/8 s'applique également au trafic de l'interface de gestion dans toutes les AWS régions, en plus des PCoIP/DCV plages indiquées dans le tableau suivant.

Région	Plage d'adresses IP
USA Est (Virginie du Nord)	PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP : 10.0.0.0/8

Région	Plage d'adresses IP
USA Ouest (Oregon)	PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16 et 198.19.0.0/16 WSP : 10.0.0.0/8
Asie-Pacifique (Mumbai)	PCoIP/WSP : 192.168.0.0/16 WSP : 10.0.0.0/8
Asie-Pacifique (Séoul)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Asie-Pacifique (Singapour)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Asie-Pacifique (Sydney)	PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16 et 198.19.0.0/16 WSP : 10.0.0.0/8
Asie-Pacifique (Tokyo)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Canada (Centre)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Europe (Francfort)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Europe (Irlande)	PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16 et 198.19.0.0/16 WSP : 10.0.0.0/8

Région	Plage d'adresses IP
Europe (Londres)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Europe (Paris)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Amérique du Sud (São Paulo)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
Afrique (Le Cap)	PCoIP/WSP : 172.31.0.0/16 et 198.19.0.0/16 WSP : 10.0.0.0/8
Israël (Tel Aviv)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8
AWS GovCloud (US-Ouest)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8 et 192.169.0.0/16
AWS GovCloud (USA Est)	PCoIP/WSP : 198.19.0.0/16 WSP : 10.0.0.0/8

Ports de l'interface de gestion

Les ports suivants doivent tous être ouverts sur l'interface du réseau de gestion WorkSpaces :

- TCP entrant sur le port 4172. Ceci est utilisé pour établir la connexion de streaming sur le protocole PCo IP.
- UDP entrant sur le port 4172. Ceci est utilisé pour diffuser les entrées utilisateur sur le protocole PCo IP.
- TCP entrant sur le port 4489. Utilisé pour les accès à l'aide du client web.
- TCP entrant sur le port 8200. Ceci est utilisé pour la gestion et la configuration du Workspace.

- TCP entrant sur les ports 8201-8250. Ces ports sont utilisés pour établir la connexion de streaming et pour diffuser les entrées utilisateur sur le protocole DCV.
- UDP entrant sur le port 8220. Ce port est utilisé pour établir la connexion de streaming et pour diffuser les entrées utilisateur sur le protocole DCV
- TCP sortant sur les ports 8443 et 9997. Utilisé pour les accès à l'aide du client web.
- UDP sortant sur les ports 3478; 4172 et 4195. Utilisé pour les accès à l'aide du client web.
- UDP sortant sur les ports 50002 et 55002. Utilisé pour le streaming. Si votre pare-feu utilise un filtrage avec état, les ports éphémères 50002 et 55002 sont automatiquement ouverts pour permettre la communication en retour. Si votre pare-feu utilise un filtrage sans état, vous devez ouvrir les ports éphémères 49152 à 65535 pour permettre la communication en retour.
- TCP sortant sur le port 80, tel que défini dans les [plages d'adresses IP de l'interface de gestion](#), vers l'adresse IP 169.254.169.254 pour accéder au service de métadonnées EC2. Tout proxy HTTP qui vous est attribué WorkSpaces doit également exclure 169.254.169.254.
- TCP sortant sur le port 1688 vers les adresses IP 169.254.169.250 et 169.254.169.251 afin de permettre l'accès à Microsoft KMS en vue de l'activation de Windows pour les instances WorkSpaces basées sur des bundles publics. Si vous utilisez Windows Bring Your Own License (BYOL) WorkSpaces, vous devez autoriser l'accès à vos propres serveurs KMS pour l'activation de Windows.
- TCP sortant sur le port 1688 vers l'adresse IP 54.239.236.220 pour autoriser l'accès à Microsoft KMS pour l'activation d'Office pour BYOL. WorkSpaces

Si vous utilisez Office via l'un des ensembles WorkSpaces publics, l'adresse IP pour l'activation de Microsoft KMS pour Office varie. Pour déterminer cette adresse IP, recherchez l'adresse IP de l'interface de gestion du Workspace, puis remplacez les deux derniers octets par 64.250. Par exemple, si l'adresse IP de l'interface de gestion est 192.168.3.5, l'adresse IP pour l'activation de Microsoft KMS Office est 192.168.64.250.

- TCP sortant vers l'adresse IP 127.0.0.2 pour DCV WorkSpaces lorsque l'Workspace hôte est configuré pour utiliser un serveur proxy.
- Communications provenant de l'adresse de bouclage 127.0.0.1.

Dans des circonstances normales, le WorkSpaces service configure ces ports pour votre WorkSpaces. Si un logiciel de sécurité ou de pare-feu est installé sur un port Workspace qui bloque l'un de ces ports, celui-ci Workspace risque de ne pas fonctionner correctement ou d'être inaccessible.

Ports de l'interface principale

Quel que soit le type de répertoire dont vous disposez, les ports suivants doivent tous être ouverts sur l'interface réseau principale WorkSpaces :

- Pour la connectivité Internet, les ports suivants doivent être ouverts en sortie vers toutes les destinations et en provenance du WorkSpaces VPC. Vous devez les ajouter manuellement au groupe de sécurité pour vous WorkSpaces si vous souhaitez qu'ils aient accès à Internet.
 - TCP 80 (HTTP)
 - TCP 443 (HTTPS)
- Pour communiquer avec les contrôleurs de répertoire, les ports suivants doivent être ouverts entre votre WorkSpaces VPC et vos contrôleurs de répertoire. Pour un annuaire Simple AD, le groupe de sécurité créé par Directory Service aura ces ports correctement configurés. Pour un annuaire AD•Connector, vous devrez peut-être ajuster le groupe de sécurité par défaut pour le VPC afin d'ouvrir ces ports.
 - TCP/UDP 53 - DNS
 - TCP/UDP 88 - Authentification Kerberos
 - UDP 123 - NTP
 - TCP 135 - RPC
 - UDP 137-138 - Netlogon
 - TCP 139 - Netlogon
 - TCP/UDP 389 - LDAP
 - TCP/UDP 445 - SMB
 - TCP/UDP 636 - LDAPS (LDAP over TLS/SSL)
 - TCP 1024-65535 - Ports dynamiques pour RPC
 - TTCP 3268-3269 - Catalogue mondial

Si un logiciel de sécurité ou de pare-feu est installé sur un port WorkSpace qui bloque l'un de ces ports, celui-ci WorkSpace risque de ne pas fonctionner correctement ou d'être inaccessible.

Exigences relatives aux adresses IP et aux ports par région

USA Est (Virginie du Nord)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.us-east-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.us-east-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>

Catégorie	Détails
	Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • USA Est (Virginie du Nord) : https://d32i4gd7pg4909.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	https://smartcard.us-east-1.signin.aws
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaines: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com

Catégorie	Détails
WorkSpaces Points de terminaison de l'API	Domaines: https://workspaces.us-east-1.amazonaws.com
Session Broker (PCM)	Domaines: https://skylight-cm.us-east-1.amazonaws.com https://skylight-cm-fips.us-east-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn.*.us-east-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-iad.amazonaws.com
Adresses IP de surveillance de l'état	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
Plage d'adresses IP des serveurs de passerelle DCV	3,227,4,0/22 44,209,84,0/22
Nom de domaine de la passerelle DCV	*.prod.us-east-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 - WSP : 10.0.0.0/8

USA Ouest (Oregon)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.us-west-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.us-west-2.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client :

Catégorie	Détails
	• <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • USA Ouest (Oregon) : https://d18af777lc07lp.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	https://smartcard.us-west-2.signin.aws
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaines: • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com

Catégorie	Détails
WorkSpaces Points de terminaison de l'API	Domaines: - https://workspaces.us-west-2.amazonaws.com - https://workspaces-fips.us-west-2.amazonaws.com
Session Broker (PCM)	Domaines: - https://skylight-cm.us-west-2.amazonaws.com - https://skylight-cm-fips.us-west-2.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.us-west-2.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-pdx.amazonworkspaces.com
Adresses IP de surveillance de l'état	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	35,80,88,0 - 35,80,95,255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255
Plage d'adresses IP des serveurs de passerelle DCV	34,223,96,0/22
Nom de domaine de la passerelle DCV	*.prod.us-west-2.highlander.aws.a2z.com

Catégorie	Détails
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 - WSP : 10.0.0.0/8

Asie-Pacifique (Mumbai)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.ap-south-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.ap-south-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/

Catégorie	Détails
	Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Asie-Pacifique (Mumbai) : https://d78hovzzqqtsb.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)

Catégorie	Détails
Agent WS	Domaine : https://ws-broker-service.ap-south-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.ap-south-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.ap-south-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	L'accès Web n'est actuellement pas disponible dans la région Asie-Pacifique (Mumbai).
Nom d'hôte de vérification de l'état	drp-bom.amazonworkspaces.com
Adresses IP de surveillance de l'état	13,127,57,82 13,234,250,73
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	13,126,243,0 - 13,126,243,255
Plage d'adresses IP des serveurs de passerelle DCV	65,1156,0/22
Nom de domaine de la passerelle DCV	*.prod.ap-south-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 192.168.0.0/16 - WSP : 10.0.0.0/8

Asie-Pacifique (Séoul)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Device Metrics (pour les applications WorkSpaces clientes 1.0 et 2.0 et versions ultérieures)	https://device-metrics-us-2.amazon.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.ap-northeast-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.ap-northeast-2.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire et des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client :

Catégorie	Détails
	• <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Asie-Pacifique (Séoul) : https://dtyv4uwoh7ynt.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : • https://ws-broker-service.ap-northeast-2.amazonaws.com

Catégorie	Détails
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.ap-northeast-2.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.ap-northeast-2.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.ap-northeast-2.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-icn.amazonworkspaces.com
Adresses IP de surveillance de l'état	13.124.44.166 13.124.203.105 52.78.44.253 52.79.54.102
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
Plage d'adresses IP des serveurs de passerelle DCV	3,35,160,0/22
Nom de domaine de la passerelle DCV	*.prod.ap-northeast-2.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 198.19.0.0/16 - WSP : 10.0.0.0/8

Asie-Pacifique (Singapour)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.ap-southeast-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.ap-southeast-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client :

Catégorie	Détails
	• <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Asie-Pacifique (Singapour) : https://d3qzmd7y07pz0i.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : • https://ws-broker-service.ap-southeast-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : • https://workspaces.ap-southeast-1.amazonaws.com

Catégorie	Détails
Session Broker (PCM)	Domaine : https://skylight-cm.ap-southeast-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.ap-southeast-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-sin.amazonworkspaces.com
Adresses IP de surveillance de l'état	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255 52.76.127.0 - 52.76.127.255
Plage d'adresses IP des serveurs de passerelle DCV	13,212,1322,0/22
Nom de domaine de la passerelle DCV	*.prod.ap-southeast-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 198.19.0.0/16 - WSP : 10.0.0.0/8

Asie-Pacifique (Sydney)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/

Catégorie	Détails
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.ap-southeast-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.ap-southeast-2.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire et des clients avant de se connecter au WorkSpace : • <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Asie-Pacifique (Sydney) : https://dwcpxuuza83q.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/

Catégorie	Détails
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	https://smartcard.ap-southeast-2.signin.aws
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : https://ws-broker-service.ap-southeast-2.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.ap-southeast-2.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.ap-southeast-2.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.ap-southeast-2.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-syd.amazonworkspaces.com
Adresses IP de surveillance de l'état	3.24.11.127 13.237.232.125
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255

Catégorie	Détails
Plage d'adresses IP des serveurs de passerelle DCV	3,25,248,0/22
Nom de domaine de la passerelle DCV	*.prod.ap-southeast-2.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16 et 198.19.0.0/16 - WSP : 10.0.0.0/8

Asie-Pacifique (Tokyo)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.ap-northeast-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.ap-northeast-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>

Catégorie	Détails
	Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<régi>on>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<régi>on>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<régi>on>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<régi>on>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Asie-Pacifique (Tokyo) : https://d2c2t8mxjhq5z1.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	https://smartcard.ap-northeast-1.signin.aws
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com

Catégorie	Détails
Pages de connexion utilisateur	https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : https://ws-broker-service.ap-northeast-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.ap-northeast-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.ap-northeast-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.ap-northeast-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-nrt.amazonworkspaces.com
Adresses IP de surveillance de l'état	18.178.102.247 54.64.174.128
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
Plage d'adresses IP des serveurs de passerelle DCV	3,1114,164,0/22
Nom de domaine de la passerelle DCV	*.prod.ap-northeast-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 198.19.0.0/16 - WSP : 10.0.0.0/8

Canada (Centre)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.ca-central-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.ca-central-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client :

Catégorie	Détails
	• <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Canada (Centre) : https://d2wfbsypmqjmog.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : • https://ws-broker-service.ca-central-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : • https://workspaces.ca-central-1.amazonaws.com

Catégorie	Détails
Session Broker (PCM)	Domaine : https://skylight-cm.ca-central-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.ca-central-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-yul.amazonworkspaces.com
Adresses IP de surveillance de l'état	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
Plage d'adresses IP des serveurs de passerelle DCV	3,97,20,0/22
Nom de domaine de la passerelle DCV	*.prod.ca-central-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 198.19.0.0/16 - WSP : 10.0.0.0/8

Europe (Francfort)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/

Catégorie	Détails
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.eu-central-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.eu-central-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire et des clients avant de se connecter au WorkSpace : • <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Europe (Francfort) : https://d1whcm49570jjw.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/

Catégorie	Détails
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : https://ws-broker-service.eu-central-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.eu-central-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.eu-central-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.eu-central-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-fra.amazonworkspaces.com
Adresses IP de surveillance de l'état	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255

Catégorie	Détails
Plage d'adresses IP des serveurs de passerelle DCV	18,2192.216,0/22
Nom de domaine de la passerelle DCV	*.prod.eu-central-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 198.19.0.0/16 - WSP : 10.0.0.0/8

Europe (Irlande)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.eu-west-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.eu-west-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS :

Catégorie	Détails
	• https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Europe (Irlande) : https://d3pgffbf39h4k4.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	https://smartcard.eu-west-1.signin.aws
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com

Catégorie	Détails
Pages de connexion utilisateur	https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : https://ws-broker-service.eu-west-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.eu-west-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.eu-west-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.eu-west-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-dub.amazonworkspaces.com
Adresses IP de surveillance de l'état	18.200.177.86 52.48.86.38 54.76.137.224
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255
Plage d'adresses IP des serveurs de passerelle DCV	3,248,176,0/22
Nom de domaine de la passerelle DCV	*.prod.eu-west-1.highlander.aws.a2z.com

Catégorie	Détails
Plages d'adresses IP de l'interface de gestion	- PCoIP/WSP : 172.31.0.0/16, 192.168.0.0/16 et 198.19.0.0/16 - WSP : 10.0.0.0/8

Europe (Londres)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.eu-west-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.eu-west-2.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/

Catégorie	Détails
	Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Europe (Londres) : https://d16q6638mh01s7.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)

Catégorie	Détails
Agent WS	Domaine : https://ws-broker-service.eu-west-2.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.eu-west-2.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.eu-west-2.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.eu-west-2.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-lhr.amazonworkspaces.com
Adresses IP de surveillance de l'état	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
Plage d'adresses IP des serveurs de passerelle DCV	18,134,68,0/22
Nom de domaine de la passerelle DCV	*.prod.eu-west-2.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	198.19.0.0/16 - WSP : 10.0.0.0/8

Europe (Paris)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/ Client
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.eu-west-3.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.eu-west-3.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>

Catégorie	Détails
	Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d2kmf63k5sit88.cloudfront.net/prod/<region>/<directory ID>">https://d2kmf63k5sit88.cloudfront.net/prod/<region>/<directory ID> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Europe (Paris) — https://d1a3png9on3sx.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : • https://ws-broker-service.eu-west-3.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : • https://workspaces.eu-west-3.amazonaws.com

Catégorie	Détails
Session Broker (PCM)	Domaine : https://skylight-cm.eu-west-3.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : tour :*.eu-west-3.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-cdg.amazonworkspaces.com
Adresses IP de surveillance de l'état	51,17,52,90 51,17,109,231 51,16,190,43
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	51,44,204,0-51,44,207,255 2a05:d 02:00:40
Plage d'adresses IP des serveurs de passerelle DCV	51,17,72,0/22
Nom de domaine de la passerelle DCV	*.prod.eu-west-3.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	198.19.0.0/16 - WSP : 10.0.0.0/8

Amérique du Sud (São Paulo)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/

Catégorie	Détails
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.sa-east-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.sa-east-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire et des clients avant de se connecter au WorkSpace : • <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Amérique du Sud (São Paulo) : https://d2lh2qc5bdoq4b.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/

Catégorie	Détails
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : https://ws-broker-service.sa-east-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.sa-east-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.sa-east-1.amazonaws.com
Serveurs TURN d'accès Web pour PCo IP	Serveur : turn:*.sa-east-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-gru.amazonworkspaces.com
Adresses IP de surveillance de l'état	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255

Catégorie	Détails
Plage d'adresses IP des serveurs de passerelle DCV	15,228,64,0/22
Nom de domaine de la passerelle DCV	*.prod.sa-east-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	• 198.19.0.0/16 • WSP : 10.0.0.0/8

Afrique (Le Cap)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.af-south-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.af-south-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : • <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS :

Catégorie	Détails
	• https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire>">https://d1cbg795sa4g1u.cloudfront.net/prod/<région>/<ID annuaire> Fichier CSS pour le style des pages de connexion : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : • Afrique (Le Cap) : https://di5ygl2cs0mrh.cloudfront.net/
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)

Catégorie	Détails
Agent WS	Domaine : https://ws-broker-service.af-south-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.af-south-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.af-south-1.amazonaws.com
Nom d'hôte de vérification de l'état	drp-cpt.amazonworkspaces.com
Adresses IP de surveillance de l'état	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	13,246,120,0 - 13,246,123,255
Plage d'adresses IP des serveurs de passerelle DCV	15,228,64,0/22
Nom de domaine de la passerelle DCV	*.prod.af-south-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	172.31.0.0/16 et 198.19.0.0/16 - WSP : 10.0.0.0/8

Israël (Tel Aviv)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://d2td7dqidlhx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://skylight-client-ds.il-central-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.il-central-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au Workspace : <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : <a href="https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire>">https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client :

Catégorie	Détails
	Fichier CSS pour le style des pages de connexion : https://d3s98kk2h6f4oh.cloudfront.net/ https://dyqsoz7pkju4e.cloudfront.net/ JavaScript fichier pour les pages de connexion : - Israël (Tel Aviv) ; —
Service de journal Forrester	https://fls-na.amazon.com/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://<id de l'annuaire>.awsapps.com/">https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente le domaine du client)
Agent WS	Domaine : https://ws-broker-service.il-central-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.il-central-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.il-central-1.amazonaws.com

Catégorie	Détails
Serveurs TURN d'accès Web pour PCo IP	Serveur : • tourner :*.il-central-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-tlv.amazonworkspaces.com
Adresses IP de surveillance de l'état	• 51,17,52,90 • 51,17,109,231 • 51,16,190,43
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	• 51,17,28,0-51,17,31,255
Plage d'adresses IP des serveurs de passerelle DCV	51,17,72,0/22
Nom de domaine de la passerelle DCV	*.prod.il-central-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	• 198.19.0.0/16 • WSP : 10.0.0.0/8

AWS GovCloud Région (USA Ouest)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/WorkSpacesAppCast.xml
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/

Catégorie	Détails
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : h https://skylight-client-ds.us-gov-west-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.us-gov-west-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire et des clients avant de se connecter au WorkSpace : • <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://s3.amazonaws.com/workspaces-client-properties/produit/pdt/<directory ID>">https://s3.amazonaws.com/workspaces-client-properties/produit/pdt/<directory ID> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://s3.amazonaws.com/workspaces-client-assets/produit/pdt/<directory ID>">https://s3.amazonaws.com/workspaces-client-assets/produit/pdt/<directory ID> Fichier CSS pour le style des pages de connexion : • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript fichier pour les pages de connexion : • Non applicable
Service de journal Forrester	https://fls-na.amazon.com/

Catégorie	Détails
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	https://smartcard.signin.amazonaws-us-gov.com
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	https://login.us-gov-home.awsapps.com/directory/(où se trouve le domaine du client) <directory id><directory id>
Agent WS	Domaine : - https://ws-broker-service.us-gov-west-1.amazonaws.com - https://ws-broker-service-fips.us-gov-west-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : - https://workspaces.us-gov-west-1.amazonaws.com - https://workspaces-fips.us-gov-west-1.amazonaws.com
Session Broker (PCM)	Domaine : - https://skylight-cm.us-gov-west-1.amazonaws.com - https://skylight-cm-fips.us-gov-west-1.amazonaws.com
Nom d'hôte de vérification de l'état	drp-pdt.amazonworkspaces.com

Catégorie	Détails
Adresses IP de surveillance de l'état	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	• 52.61.193.0 - 52.61.193.255
Plage d'adresses IP des serveurs de passerelle DCV	• 3,32,139,0/24 • 3,30,129,0/24 • 3,30,130,0/23
Nom de domaine de la passerelle DCV	*.prod. us-gov-west-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	• 198.19.0.0/16 • WSP : 10.0.0.0/8 et 192.169.0.0/16

AWS GovCloud Région (USA Est)

Domaines et adresses IP à ajouter à votre liste d'autorisation

Catégorie	Détails
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Mise à jour automatique du client	https://s3.amazonaws.com/workspaces-client-updates/prod/osu/windows/WorkSpacesAppCast.xml
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/

Catégorie	Détails
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : h https://skylight-client-ds.us-gov-east-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : https://ws-client-service.us-gov-east-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire et des clients avant de se connecter au WorkSpace : • <a href="https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire>">https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • <a href="https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID>">https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • <a href="https://s3.amazonaws.com/workspaces-client-assets/prod/osu/<directory ID>">https://s3.amazonaws.com/workspaces-client-assets/prod/osu/<directory ID> Fichier CSS pour le style des pages de connexion : • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript fichier pour les pages de connexion : • Non applicable
Service de journal Forrester	https://fls-na.amazon.com/

Catégorie	Détails
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Points de terminaison d'authentification par carte à puce de présession	https://smartcard.signin.amazonaws-us-gov.com
Dépendance d'enregistrement (pour les clients Web Access et Teradici PCo IP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	<a href="https://login.us-gov-home.awsapps.com/directory/(où se trouve le domaine du client) <directory id><directory id>">https://login.us-gov-home.awsapps.com/directory/(où se trouve le domaine du client) <directory id><directory id>
Agent WS	Domaine : https://ws-broker-service.us-gov-east-1.amazonaws.com https://ws-broker-service-fips.us-gov-east-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : https://workspaces.us-gov-east-1.amazonaws.com https://workspaces-fips.us-gov-east-1.amazonaws.com
Session Broker (PCM)	Domaine : https://skylight-cm.us-gov-east-1.amazonaws.com https://skylight-cm-fips.us-gov-east-1.amazonaws.com
Nom d'hôte de vérification de l'état	drp-osu.amazonworkspaces.com
Adresses IP de surveillance de l'état	18,253,251,70 18,254,0,118

Catégorie	Détails
PCoPlages d'adresses IP publiques des serveurs de passerelle IP	• 18,254,140,0 - 18,254,143,255
Plage d'adresses IP des serveurs de passerelle DCV	18,254,148,0/22
Nom de domaine de la passerelle DCV	*.prod. us-gov-east-1.highlander.aws.a2z.com
Plages d'adresses IP de l'interface de gestion	• 198.19.0.0/16 • WSP : 10.0.0.0/8

Configuration requise pour le réseau client pour WorkSpaces Personal

Vos WorkSpaces utilisateurs peuvent se connecter à leur WorkSpaces compte en utilisant l'application cliente d'un appareil compatible. Ils peuvent également utiliser un navigateur Web pour se connecter et prendre en charge WorkSpaces cette forme d'accès. Pour obtenir la liste des offres WorkSpaces compatibles avec l'accès par navigateur Web, consultez « Quels WorkSpaces forfaits Amazon prennent en charge l'accès Web ? » dans [Accès client, Web Access et expérience utilisateur](#).

Note

Il n'est pas possible d'utiliser un navigateur Web pour se connecter à Amazon Linux WorkSpaces.

Important

À compter du 1er octobre 2020, les clients ne pourront plus utiliser le client Amazon WorkSpaces Web Access pour se connecter à Windows 7 personnalisé WorkSpaces ou à Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Pour offrir à vos utilisateurs une bonne expérience avec leurs appareils WorkSpaces, vérifiez que leurs appareils clients répondent aux exigences réseau suivantes :

- L'appareil client doit être doté d'une connexion Internet haut débit. Nous vous recommandons de planifier un minimum de 1 Mbps par utilisateur simultané regardant une fenêtre vidéo 480p. Selon vos exigences de qualité utilisateur pour la résolution vidéo, plus de bande passante peut être nécessaire.
- Le réseau auquel l'appareil client est connecté, ainsi que le pare-feu de l'appareil client, doivent avoir certains ports ouverts vers les plages d'adresses IP de différents services AWS . Pour de plus amples informations, veuillez consulter [Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal](#).
- Pour des performances optimales en matière d' PCoIP, le temps de trajet aller-retour (RTT) entre le réseau du client et la région dans laquelle il WorkSpaces se trouve doit être inférieur à 100 ms. Si le RTT est compris entre 100 ms et 200 ms, l'utilisateur peut y accéder WorkSpace, mais les performances sont affectées. Si le RTT est compris entre 200 et 375 ms, les performances se dégradent. Si le RTT dépasse 375 ms, la connexion WorkSpaces client est interrompue.

Pour optimiser les performances du DCV, le RTT entre le réseau du client et la région dans laquelle il WorkSpaces se trouve doit être inférieur à 250 ms. Si le RTT est compris entre 250 ms et 400 ms, l'utilisateur peut y accéder WorkSpace, mais les performances sont dégradées.

Pour vérifier le RTT dans les différentes AWS régions depuis votre lieu de résidence, utilisez l'[Amazon WorkSpaces Connection Health Check](#).

- Pour utiliser des webcams avec DCV, nous recommandons une bande passante de téléchargement minimale de 1,7 mégabits par seconde.
- Si les utilisateurs y accèdent WorkSpaces via un réseau privé virtuel (VPN), la connexion doit prendre en charge une unité de transmission maximale (MTU) d'au moins 1 200 octets.

Note

Vous ne pouvez pas y accéder WorkSpaces via un VPN connecté à votre cloud privé virtuel (VPC). Pour accéder à WorkSpaces l'aide d'un VPN, une connexion Internet (via les adresses IP publiques du VPN) est requise, comme décrit dans [Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal](#).

- Les clients ont besoin d'un accès HTTPS aux WorkSpaces ressources hébergées par le service et Amazon Simple Storage Service (Amazon S3). Les clients ne prennent pas en charge la redirection vers un proxy au niveau de l'application. Un accès HTTPS est requis pour que les utilisateurs puissent terminer avec succès leur inscription et accéder à leur WorkSpaces.

- Pour autoriser l'accès depuis des appareils clients PCo IP zéro, vous devez utiliser un bundle de protocoles PCo IP pour WorkSpaces. Vous devez également activer le protocole NTP (Network Time Protocol) dans Teradici. Pour de plus amples informations, veuillez consulter [Configurer des clients PCo IP zéro pour WorkSpaces Personal](#).

Vous pouvez vérifier qu'un appareil client répond aux exigences de mise en réseau de la façon suivante.

Pour vérifier la configuration réseau requise pour les clients 3.0+

1. Ouvrez votre WorkSpaces client. Si vous avez ouvert le client pour la première fois, vous êtes invité à entrer le code d'enregistrement que vous avez reçu dans l'e-mail d'invitation.
2. Selon le client que vous utilisez, effectuez l'une des opérations suivantes.

Si vous utilisez...	Faites ceci
Clients Windows ou Linux	Dans l'angle supérieur droit de l'application client, sélectionnez l'icône Réseau.
Client macOS	Choisissez Connexions (Connexions), Network (Réseau).

L'application client teste la connexion réseau, les ports et la durée du cycle, et indique les résultats de ces tests.

3. Fermez la boîte de dialogue Network (Réseau) pour revenir à la page de connexion.

Pour vérifier la configuration réseau requise pour les clients 1.0+ et 2.0+

1. Ouvrez votre WorkSpaces client. Si vous avez ouvert le client pour la première fois, vous êtes invité à entrer le code d'enregistrement que vous avez reçu dans l'e-mail d'invitation.
2. Choisissez Network (Réseau) en bas à droite de l'application client. L'application client teste la connexion réseau, les ports et la durée du cycle, et indique les résultats de ces tests.
3. Choisissez Ignorer pour revenir à la page de connexion.

Restreindre l'accès aux appareils fiables pour les WorkSpaces particuliers

Par défaut, les utilisateurs peuvent y accéder WorkSpaces depuis n'importe quel appareil compatible connecté à Internet. Si votre entreprise limite l'accès aux données d'entreprise aux appareils fiables (également appelés appareils administrés), vous pouvez restreindre WorkSpaces l'accès aux appareils fiables dotés de certificats valides.

Note

Cette fonctionnalité n'est actuellement disponible que lorsque vos annuaires WorkSpaces personnels sont gérés Directory Service via Simple AD, AD Connector et AWS Managed Microsoft AD directory.

Lorsque vous activez cette fonctionnalité, elle WorkSpaces utilise l'authentification basée sur des certificats pour déterminer si un appareil est fiable. Si l'application WorkSpaces cliente ne parvient pas à vérifier qu'un appareil est fiable, elle bloque les tentatives de connexion ou de reconnexion depuis l'appareil.

Pour chaque annuaire, vous pouvez importer jusqu'à deux certificats racines. Si vous importez deux certificats racines, WorkSpaces présentez-les tous les deux au client et celui-ci trouve le premier certificat valide correspondant à l'un ou l'autre des certificats racines.

Clients pris en charge

- Android, fonctionnant sur Android ou sur des systèmes Chrome OS compatibles avec Android
- macOS
- Windows

Important

Cette fonctionnalité n'est prise en charge que pour les clients suivants :

- WorkSpaces applications clientes pour Linux ou iPad
- Les clients tiers, y compris, mais sans s'y limiter, Teradici PCo IP, les clients RDP et les applications de bureau à distance.

 Note

Lorsque vous activez l'accès pour des clients spécifiques, assurez-vous de bloquer l'accès pour les autres types d'appareils dont vous n'avez pas besoin. Pour plus d'informations sur la procédure à suivre, reportez-vous à l'étape 3.7 ci-dessous.

Étape 1 : Créer des certificats

Cette fonctionnalité nécessite deux types de certificats : les certificats racines générés par une autorité de certification et les certificats clients qui se lient à un certificat racine.

Prérequis

- Les certificats racine doivent être des fichiers encodés en Base64 au format CRT, CERT ou PEM.
- Les certificats racine doivent satisfaire au modèle d'expression régulière suivant, ce qui signifie que chaque ligne codée, à part la dernière, doit comporter exactement 64 caractères : `-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`.
- Les certificats d'appareil doivent inclure un nom commun.
- Les certificats d'appareil doivent inclure les extensions suivantes : Key Usage: Digital Signature et Enhanced Key Usage: Client Authentication.
- Tous les certificats de la chaîne, du certificat d'appareil à l'autorité de certification racine approuvée, doivent être installés sur l'appareil client.
- La longueur maximale de chaîne de certificats prise en charge est 4.
- WorkSpaces ne prend actuellement pas en charge les mécanismes de révocation des appareils, tels que les listes de révocation de certificats (CRL) ou le protocole OCSP (Online Certificate Status Protocol), pour les certificats clients.
- Utilisez un algorithme de chiffrement puissant. Nous vous recommandons SHA256 d'utiliser le RSA, SHA256 l'ECDSA, l'ECDSA SHA384 ou l'ECDSA. SHA512
- Pour macOS, si le certificat de l'appareil se trouve dans le trousseau du système, nous vous recommandons d'autoriser l'application WorkSpaces cliente à accéder à ces certificats. Sinon, les utilisateurs doivent saisir les informations d'identification du trousseau lorsqu'ils se connectent ou se reconnectent.

Étape 2 : Déployer les certificats clients vers les appareils approuvés

Sur les appareils approuvés pour les utilisateurs, vous devez installer un ensemble de certificats qui inclut tous les certificats de la chaîne, du certificat de l'appareil à l'autorité de certification racine approuvée. Vous pouvez utiliser votre solution préférée pour installer des certificats dans votre flotte d'appareils clients ; par exemple, System Center Configuration Manager (SCCM) ou la gestion des périphériques mobiles (MDM). Notez que le SCCM et le MDM peuvent éventuellement effectuer une évaluation du niveau de sécurité afin de déterminer si les appareils répondent aux politiques d'accès de votre entreprise. WorkSpaces

Les applications WorkSpaces clientes recherchent les certificats comme suit :

- Android : accédez à Paramètres, choisissez Sécurité et localisation, Informations d'identification, puis choisissez Installer depuis une carte SD.
- Systèmes Chrome OS compatibles avec Android : ouvrez les paramètres Android et choisissez Sécurité et localisation, Informations d'identification, puis choisissez Installer depuis une carte SD.
- macOS : recherche les certificats clients dans le trousseau.
- Windows : recherche les certificats clients dans les magasins de certificats utilisateur et racine.

Étape 3 : Configurer la restriction

Après avoir déployé les certificats clients sur les appareils approuvés, vous pouvez activer un accès restreint au niveau de l'annuaire. Cela nécessite que l'application WorkSpaces cliente valide le certificat sur un appareil avant d'autoriser un utilisateur à se connecter à un Workspace.

Pour configurer la restriction

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez l'annuaire et choisissez Actions, Mettre à jour les détails.
4. Développez Options de contrôle d'accès.
5. Sous Pour chaque type d'appareil, spécifiez les appareils autorisés à accéder WorkSpaces, puis sélectionnez Appareils sécurisés.
6. Importez jusqu'à deux certificats racines. Pour chaque certificat racine, procédez comme suit :
 - a. Choisissez Importer.
 - b. Copiez le corps du certificat dans le formulaire.

- c. Choisissez Importer.
7. Spécifiez si d'autres types d'appareils ont accès à WorkSpaces.
 - a. Faites défiler la page jusqu'à la section Autres plateformes. Par défaut, les clients WorkSpaces Linux sont désactivés et les utilisateurs peuvent y accéder WorkSpaces depuis leurs appareils iOS, Android, Web Access, Chromebooks et appareils clients PCo IP zéro.
 - b. Sélectionnez les types d'appareils à activer et effacez ceux à désactiver.
 - c. Pour bloquer l'accès à partir de tous les types d'appareils sélectionnés, choisissez Bloc.
8. Choisissez Update and Exit (Mettre à jour et quitter).

Intégrer SAML 2.0 à Personal WorkSpaces

Note

SAML 2.0 n'est disponible que lorsque vos annuaires WorkSpaces personnels sont gérés via Directory Service Simple AD, AD Connector et AWS Managed Microsoft AD directory. Cette fonctionnalité ne s'applique pas aux annuaires gérés par Amazon WorkSpaces, qui utilisent normalement IAM Identity Center pour l'authentification des utilisateurs au lieu de la fédération SAML 2.0.

L'intégration de SAML 2.0 à votre authentification de session WorkSpaces pour ordinateur de bureau permet à vos utilisateurs d'utiliser leurs informations d'identification et leurs méthodes d'authentification de fournisseur d'identité (IdP) SAML 2.0 existantes via leur navigateur Web par défaut. En utilisant votre IdP pour authentifier les utilisateurs WorkSpaces, vous pouvez vous protéger en WorkSpaces utilisant des fonctionnalités IdP telles que l'authentification multifactorielle et les politiques d'accès contextuelles.

Flux de travail d'authentification

Les sections suivantes décrivent le flux de travail d'authentification lancé par l'application WorkSpaces cliente, WorkSpaces Web Access et un fournisseur d'identité (IdP) SAML 2.0 :

- Lorsque le flux est initié par l'IdP. Par exemple, lorsque les utilisateurs choisissent une application sur le portail utilisateur de l'IdP dans un navigateur Web.
- Lorsque le flux est initié par le WorkSpaces client. Par exemple, quand les utilisateurs ouvrent l'application client et se connectent.

- Lorsque le flux est initié par WorkSpaces Web Access. Par exemple, quand les utilisateurs ouvrent Web Access dans un navigateur et se connectent.

Dans ces exemples, les utilisateurs saisissent `user@example.com` pour se connecter à l'IdP. L'IdP dispose d'une application de fournisseur de services SAML 2.0 configurée pour un WorkSpaces annuaire et les utilisateurs sont autorisés à utiliser l'application WorkSpaces SAML 2.0. Les utilisateurs créent un WorkSpace pour leurs noms d'utilisateur `user`, dans un répertoire activé pour l'authentification SAML 2.0. En outre, les utilisateurs installent [l'application WorkSpaces cliente](#) sur leur appareil ou utilisent Web Access dans un navigateur Web.

Flux initié par le fournisseur d'identité (IdP) avec l'application client

Le flux initié par l'IdP permet aux utilisateurs d'enregistrer automatiquement l'application WorkSpaces cliente sur leurs appareils sans avoir à saisir de code d' WorkSpaces enregistrement. Les utilisateurs ne se connectent pas à leur compte en WorkSpaces utilisant le flux initié par l'IdP. WorkSpaces l'authentification doit provenir de l'application cliente.

1. Via leur navigateur Web, les utilisateurs se connectent à l'IdP.
2. Une fois connectés à l'IdP, les utilisateurs choisissent l' WorkSpaces application depuis le portail utilisateur de l'IdP.
3. Les utilisateurs sont redirigés vers cette page dans le navigateur et l'application WorkSpaces cliente s'ouvre automatiquement.



4. L'application WorkSpaces cliente est désormais enregistrée et les utilisateurs peuvent continuer à se connecter en cliquant sur Continuer pour se connecter à WorkSpaces.

Flux initié par le fournisseur d'identité (IdP) avec Web Access

Le flux d'accès Web initié par l'IdP permet aux utilisateurs de les enregistrer automatiquement WorkSpaces via un navigateur Web sans avoir à saisir de code d' WorkSpaces enregistrement. Les utilisateurs ne se connectent pas à leur compte en WorkSpaces utilisant le flux initié par l'IdP. WorkSpaces l'authentification doit provenir de Web Access.

1. Via leur navigateur Web, les utilisateurs se connectent à l'IdP.
2. Une fois connectés à l'IdP, les utilisateurs cliquent sur l' WorkSpaces application depuis le portail utilisateur de l'IdP.
3. Dans le navigateur, les utilisateurs sont redirigés vers cette page. Pour ouvrir WorkSpaces, choisissez Amazon WorkSpaces dans le navigateur.



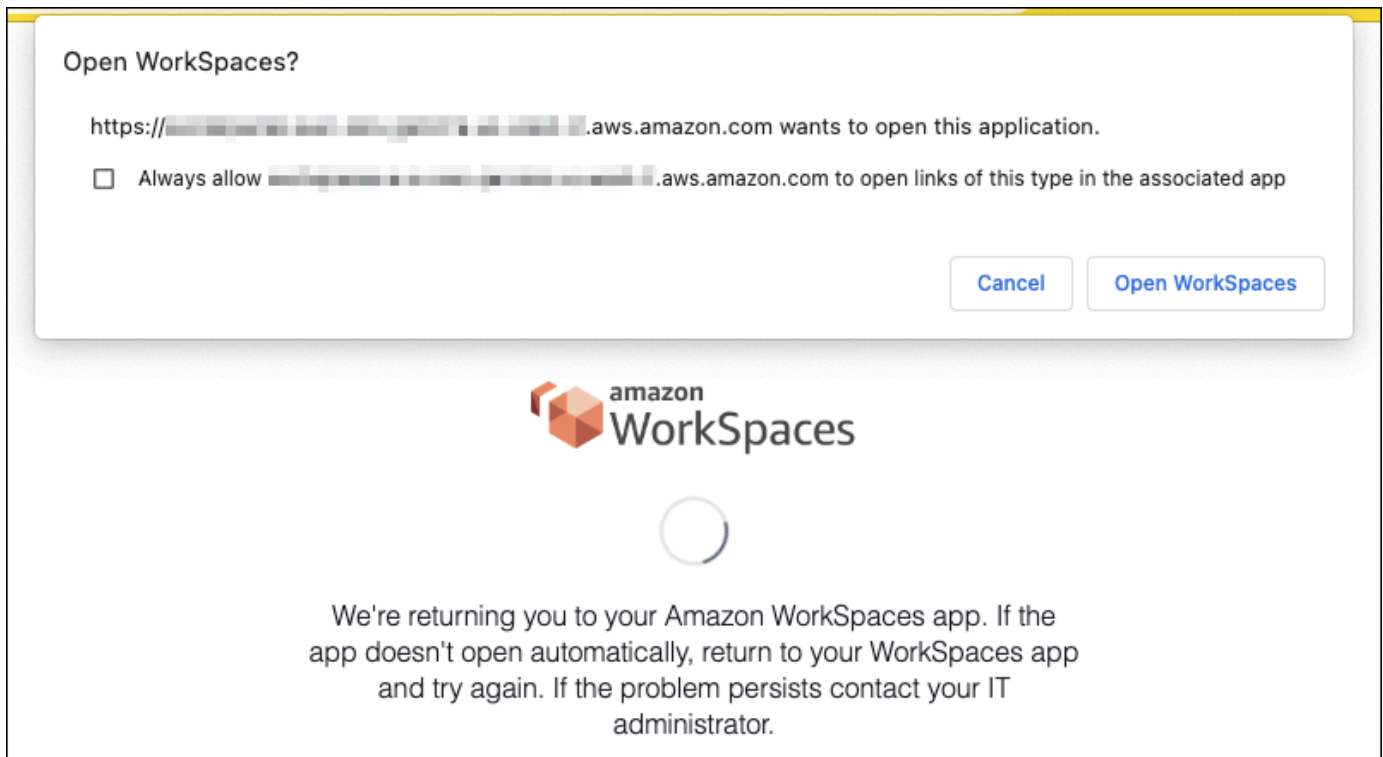
4. L'application WorkSpaces cliente est désormais enregistrée et les utilisateurs peuvent continuer à se connecter via WorkSpaces Web Access.

WorkSpaces flux initié par le client

Le flux initié par le client permet aux utilisateurs de se connecter à leur compte WorkSpaces après s'être connectés à un IdP.

1. Les utilisateurs lancent l'application WorkSpaces cliente (si elle n'est pas déjà en cours d'exécution) et cliquent sur Continuer pour se connecter à WorkSpaces.
2. Les utilisateurs sont redirigés vers leur navigateur Web par défaut pour se connecter à l'IdP. S'ils sont déjà connectés à l'IdP dans leur navigateur, ils n'ont pas besoin de se reconnecter et peuvent ignorer cette étape.

3. Une fois connectés à l'IdP, les utilisateurs sont redirigés vers une fenêtre contextuelle. Suivez les instructions pour autoriser votre navigateur Web à ouvrir l'application client.



4. Les utilisateurs sont redirigés vers l'application WorkSpaces cliente pour terminer la connexion à leur Workspace. WorkSpaces les noms d'utilisateur sont renseignés automatiquement à partir de l'assertion IDP SAML 2.0. Quand vous utilisez l'[authentification par certificat](#), les utilisateurs sont automatiquement connectés.
5. Les utilisateurs sont connectés à leur Workspace.

WorkSpaces Flux initié par Web Access

Le flux initié par Web Access permet aux utilisateurs de se connecter à leur compte WorkSpaces après s'être connectés à un IdP.

1. Les utilisateurs lancent le WorkSpaces Web Access et choisissent Se connecter.
2. Dans le même onglet du navigateur, les utilisateurs sont redirigés vers le portail IdP. S'ils sont déjà connectés à l'IdP dans leur navigateur, ils n'ont pas besoin de se reconnecter et peuvent ignorer cette étape.
3. Une fois connectés à l'IdP, les utilisateurs sont redirigés vers cette page dans le navigateur et cliquent sur Se connecter à. WorkSpaces

4. Les utilisateurs ont été redirigés vers l'application WorkSpaces cliente pour terminer la connexion à leur WorkSpace. WorkSpaces les noms d'utilisateur sont renseignés automatiquement à partir de l'assertion IDP SAML 2.0. Quand vous utilisez l'[authentification par certificat](#), les utilisateurs sont automatiquement connectés.
5. Les utilisateurs sont connectés à leur WorkSpace.

Configurer SAML 2.0 pour le personnel WorkSpaces

Activez l'enregistrement des applications WorkSpaces clientes et la connexion à celles-ci WorkSpaces pour vos utilisateurs à l'aide de leurs identifiants de fournisseur d'identité (IdP) SAML 2.0 et de leurs méthodes d'authentification en configurant la fédération d'identité à l'aide de SAML 2.0. Pour configurer la fédération d'identité à l'aide de SAML 2.0, utilisez un rôle IAM et une URL d'état du relais pour configurer votre IdP et activer AWS. Cela permet à vos utilisateurs fédérés d'accéder à un WorkSpaces annuaire. L'état du relais est le point de terminaison du WorkSpaces répertoire vers lequel les utilisateurs sont redirigés une fois qu'ils se sont connectés avec succès AWS.

Table des matières

- [Exigences](#)
- [Conditions préalables](#)
- [Étape 1 : créer un fournisseur d'identité SAML dans IAM AWS](#)
- [Étape 2 : Créer un rôle IAM de fédération SAML 2.0](#)
- [Étape 3 : Incorporer une politique en ligne pour le rôle IAM](#)
- [Étape 4 : Configurer le fournisseur d'identité SAML 2.0](#)
- [Étape 5 : Créer des assertions pour la réponse de l'authentification SAML](#)
- [Étape 6 : Configurer l'état du relais de votre fédération](#)
- [Étape 7 : Activez l'intégration avec SAML 2.0 dans votre répertoire WorkSpaces](#)

Exigences

- L'authentification SAML 2.0 est disponible dans les régions suivantes :
 - Région USA Est (Virginie du Nord)
 - Région USA Ouest (Oregon)
 - Région Afrique (Le Cap)

- Région Asie-Pacifique (Mumbai)
- Région Asie-Pacifique (Séoul)
- Région Asie-Pacifique (Singapour)
- Région Asie-Pacifique (Sydney)
- Région Asie-Pacifique (Tokyo)
- Région Canada (Centre)
- Région Europe (Frankfurt)
- Région Europe (Irlande)
- Région Europe (Londres)
- Région Amérique du Sud (São Paulo)
- Région Israël (Tel Aviv)
- AWS GovCloud (US-Ouest)
- AWS GovCloud (USA Est)
- Pour utiliser l'authentification SAML 2.0 avec WorkSpaces, l'IdP doit prendre en charge l'authentification unique non sollicitée initiée par l'IdP avec une ressource cible Deep Link ou une URL de point de terminaison d'état relais. IdPs Les exemples incluent ADFS, Azure AD, Duo Single Sign-On, Okta et PingFederate. PingOne Pour plus d'informations, consultez la documentation de votre IdP.
- L'authentification SAML 2.0 fonctionnera si elle est WorkSpaces lancée à l'aide de Simple AD, mais cela n'est pas recommandé car Simple AD ne s'intègre pas à SAML 2.0. IdPs
- L'authentification SAML 2.0 est prise en charge sur les WorkSpaces clients suivants. Les autres versions de clients ne sont pas prises en charge pour l'authentification SAML 2.0. Ouvrez Amazon WorkSpaces [Client Downloads](#) pour trouver les dernières versions :
 - Application client Windows version 5.1.0.3029 ou ultérieure
 - Client macOS version 5.x ou ultérieure
 - Client Linux pour Ubuntu 22.04 version 2024.1 ou ultérieure, Ubuntu 20.04 version 24.1 ou ultérieure
 - Web Access

Les autres versions du client ne pourront pas se connecter à l'authentification SAML 2.0 WorkSpaces activée à moins que la solution de secours ne soit activée. Pour plus d'informations, voir [Activer l'authentification SAML 2.0 sur le WorkSpaces répertoire](#).

Pour step-by-step obtenir des instructions sur WorkSpaces l'intégration de SAML 2.0 à ADFS, Azure AD, Duo Single Sign-On, Okta PingFederate et PingOne pour Enterprise OneLogin, consultez le guide de mise en œuvre de l'authentification [Amazon WorkSpaces SAML](#).

Conditions préalables

Remplissez les conditions préalables suivantes avant de configurer la connexion de votre fournisseur d'identité (IdP) SAML 2.0 à un annuaire. WorkSpaces

1. Configurez votre IdP pour intégrer les identités utilisateur issues du Microsoft Active Directory utilisé avec l' WorkSpaces annuaire. Pour un utilisateur avec a WorkSpace, le AMAccountnom s et les attributs e-mail de l'utilisateur Active Directory et les valeurs de réclamation SAML doivent correspondre pour que l'utilisateur puisse se connecter à l' WorkSpaces aide de l'IdP. Pour plus d'informations sur l'intégration d'Active Directory dans votre IdP, consultez la documentation de votre IdP.
2. Configurez votre fournisseur d'identité pour établir une relation d'approbation avec AWS.
 - Voir [Intégration de fournisseurs de solutions SAML tiers avec des fournisseurs de solutions SAML AWS](#) pour plus d'informations sur la configuration de la AWS fédération. Parmi les exemples pertinents, citons l'intégration d'IdP à AWS IAM pour accéder à la AWS console de gestion.
 - Utilisez votre IdP pour générer et télécharger un document de métadonnées de fédération décrivant votre organisation en tant qu'IdP. Ce document XML signé est utilisé pour établir la relation d'approbation des parties utilisatrices. Enregistrez le fichier dans un emplacement auquel vous pouvez accéder ultérieurement depuis la console IAM.
3. Créez ou enregistrez un répertoire pour à WorkSpaces l'aide de la console WorkSpaces de gestion. Pour plus d'informations, consultez la section [Gérer les annuaires pour WorkSpaces](#). L'authentification SAML 2.0 pour WorkSpaces est prise en charge pour les types de répertoires suivants :
 - AD Connector
 - AWS Microsoft AD géré
4. Créez un WorkSpace pour un utilisateur qui peut se connecter à l'IdP à l'aide d'un type d'annuaire pris en charge. Vous pouvez en créer un WorkSpace à l'aide de la console de WorkSpaces gestion ou de WorkSpaces l'API. AWS CLI Pour plus d'informations, voir [Lancer un bureau virtuel à l'aide de WorkSpaces](#).

Étape 1 : créer un fournisseur d'identité SAML dans IAM AWS

Créez d'abord un IdP SAML dans IAM. AWS Cet IdP définit la relation IdP àAWS confiance de votre organisation à l'aide du document de métadonnées généré par le logiciel IdP de votre organisation. Pour plus d'informations, consultez [Création et gestion d'un fournisseur d'identité SAML \(Console de gestion Amazon Web Services\)](#). Pour plus d'informations sur l'utilisation de SAML IdPs dans AWS GovCloud (US-West) et AWS GovCloud (US-East), consultez [AWS Identity and Access Management](#).

Étape 2 : Créer un rôle IAM de fédération SAML 2.0

Ensuite, créez un rôle IAM de fédération SAML 2.0. Cette étape établit une relation d'approbation entre IAM et l'IdP de votre organisation, ce qui identifie votre IdP comme entité de confiance pour la fédération.

Pour créer un rôle IAM pour l'IdP SAML

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles, puis Créer un rôle.
3. Pour Type de rôle, choisissez Fédération SAML 2.0.
4. Pour Fournisseur SAML, sélectionnez l'IdP SAML que vous avez créé.

Important

Ne choisissez aucune des deux méthodes d'accès SAML 2.0, ni Autoriser l'accès par programmation uniquement, ni Autoriser l'accès par programme et via Amazon Web Services Management Console.

5. Pour Attribut, choisissez SAML:sub_type.
6. Pour le champ Valeur, saisissez `persistent`. Cette valeur restreint l'accès du rôle aux demandes de streaming de l'utilisateur SAML qui incluent une assertion de type d'objet SAML avec une valeur « `persistent` ». Si la valeur de SAML:sub_type est « `persistent` », votre fournisseur d'identité envoie la même valeur unique pour l'élément `NameID` dans toutes les demandes SAML à partir d'un utilisateur particulier. Pour plus d'informations sur l'assertion SAML:sub_TYPE, consultez la section Identification unique des utilisateurs dans une fédération basée sur SAML dans Utilisation de la fédération basée sur SAML [pour l'accès à l'API](#). AWS
7. Passez en revue vos informations d'approbation SAML 2.0 pour confirmer l'entité de confiance et la condition, puis choisissez Suivant : Autorisations.

8. Dans la page Attacher des stratégies d'autorisations, choisissez Suivant : balises.
9. (Facultatif) Saisissez une clé et une valeur pour chaque balise que vous souhaitez ajouter. Pour plus d'informations, consultez [Étiquette d'utilisateurs IAM et Étiquette de rôles IAM](#).
10. Lorsque vous avez terminé, sélectionnez Suivant : vérification. Vous pouvez ultérieurement créer et incorporer une politique en ligne pour ce rôle.
11. Pour Nom du rôle, saisissez un nom vous permettant d'identifier le but de ce rôle. Différentes entités pouvant référencer ce rôle, il n'est pas possible de modifier son nom après sa création.
12. (Facultatif) Dans le champ Description du rôle, saisissez la description du nouveau rôle.
13. Passez en revue les détails du rôle, puis choisissez Créer un rôle.
14. Ajoutez l'TagSession autorisation sts : à la politique de confiance de votre nouveau rôle IAM. Pour plus d'informations, consultez [Transmission des balises de session dans AWS STS](#). Sur la page des détails du nouveau rôle IAM, choisissez l'onglet Relations d'approbation, puis choisissez Modifier la relation d'approbation*. Lorsque l'éditeur de politique Edit Trust Relationship s'ouvre, ajoutez l'autorisation sts : TagSession *, comme suit :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::111122223333:saml-provider/
IDENTITY-PROVIDER"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:aud": "https://signin.aws.amazon.com/saml"
        }
      }
    }
  ]
}
```

Remplacez `IDENTITY-PROVIDER` par le nom de l'IdP SAML que vous avez créé à l'étape 1. Choisissez Mettre à jour la stratégie de confiance.

Étape 3 : Incorporer une politique en ligne pour le rôle IAM

Incorporez ensuite une politique IAM en ligne pour le rôle que vous avez créé. Lorsque vous incorporez une politique en ligne, ses autorisations ne peuvent pas être associées par inadvertance à la mauvaise entité principale. La politique intégrée permet aux utilisateurs fédérés d'accéder à l'WorkSpaces annuaire.

Important

Les politiques IAM permettant de gérer l'accès en AWS fonction de l'adresse IP source ne sont pas prises en charge pour cette `workspaces:Stream` action. Pour gérer les contrôles d'accès IP pour WorkSpaces, utilisez des [groupes de contrôle d'accès IP](#). En outre, lorsque vous utilisez l'authentification SAML 2.0, vous pouvez utiliser les politiques de contrôle d'accès IP si elles sont disponibles auprès de votre IdP SAML 2.0.

1. Dans les détails du rôle IAM que vous avez créé, choisissez l'onglet Autorisations, puis ajoutez les autorisations requises à la politique d'autorisations du rôle. L'assistant Créer une politique démarre.
2. Dans Créer une politique, choisissez l'onglet JSON.
3. Copiez et collez le code JSON suivant dans la fenêtre de l'éditeur de politique. Modifiez ensuite la ressource en saisissant votre code de AWS région, votre identifiant de compte et votre identifiant de répertoire. Dans la politique suivante, `"Action": "workspaces:Stream"` figure l'action qui fournit à vos WorkSpaces utilisateurs les autorisations nécessaires pour se connecter à leurs sessions de bureau dans l'WorkSpaces annuaire.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "workspaces:Stream",
      "Resource": "arn:aws:workspaces:us-east-1:123456789012:directory/DIRECTORY-ID",
    }
  ]
}
```

```
        "Condition": {
            "StringEquals": {
                "workspaces:userId": "${saml:sub}"
            }
        }
    ]
}
```

Remplacez REGION-CODE par la AWS région dans laquelle se trouve votre WorkSpaces répertoire. DIRECTORY-ID Remplacez-le par l'ID du WorkSpaces répertoire, qui se trouve dans la console WorkSpaces de gestion. Pour les ressources en AWS GovCloud (US-West) ou AWS GovCloud (US-East), utilisez le format suivant pour l'ARN : `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`

4. Lorsque vous avez terminé, choisissez Examiner une stratégie. Le programme de [validation de politiques](#) signale les éventuelles erreurs de syntaxe.

Étape 4 : Configurer le fournisseur d'identité SAML 2.0

Ensuite, en fonction de votre IdP SAML 2.0, vous devrez peut-être mettre à jour manuellement votre IdP pour faire AWS confiance en tant que fournisseur de services en téléchargeant `saml-metadata.xml` le fichier `saml-metadata.xml` sur votre IdP. <https://signin.aws.amazon.com/static/>

Cette étape met à jour les métadonnées de votre fournisseur d'identité. Pour certains IdPs, la mise à jour est peut-être déjà configurée. Dans ce cas, passez à l'étape suivante.

Si cette mise à jour n'est pas déjà configurée dans votre IdP, consultez les informations fournies dans la documentation de votre fournisseur d'identité sur la façon de mettre à jour les métadonnées. Certains fournisseurs vous offrent la possibilité d'entrer l'URL, ce qui permet au fournisseur d'identité d'obtenir et d'installer le fichier à votre place. D'autres fournisseurs exigent que vous téléchargiez le fichier à partir de l'URL afin de le fournir en tant que fichier local.

Important

À ce stade, vous pouvez également autoriser les utilisateurs de votre IdP à accéder à l'WorkSpaces application que vous avez configurée dans votre IdP. Les utilisateurs autorisés à accéder à l'WorkSpaces application de votre annuaire n'en ont pas automatiquement Workspace créé un. De même, les utilisateurs qui ont Workspace créé une application pour

eux ne sont pas automatiquement autorisés à accéder à l' WorkSpaces application. Pour se connecter avec succès à une Workspace authentication SAML 2.0, un utilisateur doit être autorisé par l'IdP et doit avoir Workspace créé un.

Note

Si vos utilisateurs finaux passent fréquemment d'une identité WorkSpaces utilisateur à une autre lorsqu'ils utilisent le même fournisseur d'identité (IdP) SAML 2.0, assurez-vous que votre IdP est configuré pour forcer l'authentification ForceAuthn () à chaque tentative de connexion. Cela empêche votre IdP de réutiliser une session SSO existante, ce qui pourrait entraîner des échecs d'authentification lorsque vos utilisateurs passent à une autre. Workspace Reportez-vous à la documentation de votre IdP pour obtenir des conseils sur l'activation du paramètre ForceAuthn (ou équivalent).

Etape 5 : Créer des assertions pour la réponse de l'authentification SAML

Configurez ensuite les informations que votre IdP envoie AWS sous forme d'attributs SAML dans sa réponse d'authentification. En fonction de votre IdP, cela est peut être déjà configuré. Si c'est le cas, ignorez cette étape et passez à l'[Étape 6 : Configurer l'état du relais de votre fédération](#).

Si cette information n'est pas déjà configurée dans votre IdP, fournissez les éléments suivants :

- SAML Subject NameID : identifiant unique de l'utilisateur connecté. La valeur doit correspondre au nom WorkSpaces d'utilisateur et correspond généralement à l'attribut s AMAccount Name de l'utilisateur Active Directory.
- SAML Subject Type (avec une valeur définie à persistent) : définir la valeur à persistent permet de s'assurer que l'IdP envoie la même valeur unique pour l'élément NameID dans toutes les demandes SAML provenant d'un utilisateur particulier. Assurez-vous que votre politique IAM inclut une condition pour autoriser uniquement les requêtes SAML avec un sous-type SAML défini à persistent, comme décrit à l'[Étape 2 : Créer un rôle IAM de fédération SAML 2.0](#).
- Élément **Attribute** avec l'attribut **Name** défini à **<https://aws.amazon.com/SAML/Attributes/Role>** : cet élément contient un ou plusieurs éléments AttributeValue répertoriant le rôle IAM et l'IdP SAML auxquels l'utilisateur est mappé par votre fournisseur d'identité. Le rôle et l'IdP sont spécifiés sous la forme d'une paire séparée par des virgules

de. ARNs Exemple de la valeur attendue : `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME`, `arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`.

- **Attribute** élément dont l'attribut **Name** est défini sur **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** — Cet élément contient un **AttributeValue** élément qui fournit un identifiant pour les informations d'identification AWS temporaires émises pour l'authentification unique. La valeur de l'élément **AttributeValue** doit comporter entre 2 et 64 caractères. Elle ne peut contenir que des caractères alphanumériques, des traits de soulignement et les caractères suivants : `_ . : / = + - @`. Elle ne doit pas comporter d'espace. La valeur est généralement une adresse e-mail ou un nom d'utilisateur principal (UPN). La valeur ne peut pas comporter d'espace, comme dans le nom d'affichage d'un utilisateur.
- Éléments **Attribute** avec l'attribut **Name** défini à **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** : cet élément contient un élément **AttributeValue** qui fournit l'adresse e-mail de l'utilisateur. La valeur doit correspondre à l'adresse e-mail de WorkSpaces l'utilisateur telle que définie dans le WorkSpaces répertoire. Les valeurs des balises peuvent inclure des combinaisons de lettres, chiffres, espaces et les caractères `_ . : / = + - @`. Pour plus d'informations, consultez [Règles de balisage dans IAM et AWS STS](#) dans le Guide de l'utilisateur IAM.
- Éléments **Attribute** avec l'attribut **Name** défini à **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** (facultatif) : cet élément contient un élément **AttributeValue** qui fournit l'élément **userPrincipalName** Active Directory à l'utilisateur qui se connecte. La valeur que vous fournissez doit être au format `username@domain.com`. Ce paramètre est utilisé avec l'authentification par certificat en tant qu'autre nom du sujet dans le certificat utilisateur final. Pour plus d'informations, consultez [Authentification par certificat](#).
- Éléments **Attribute** avec l'attribut **Name** défini à **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** (facultatif) : cet élément contient un élément **AttributeValue** qui fournit l'identifiant de sécurité Active Directory (SID) à l'utilisateur qui se connecte. Ce paramètre est utilisé avec l'authentification par certificat pour permettre un mappage solide vers l'utilisateur Active Directory. Pour plus d'informations, consultez [Authentification par certificat](#).
- Éléments **Attribute** dont l'attribut **Name** est défini à **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** (facultatif) : cet élément contient un élément **AttributeValue** qui fournit un autre format de nom d'utilisateur. Utilisez cet attribut si vous avez des cas d'utilisation qui nécessitent des formats de nom d'utilisateur tels que `corp\usernamecorp.example.com\username`, ou `username@corp.example.com` pour vous

connecter à l'aide du WorkSpaces client. Les clés et valeurs des balises peuvent inclure n'importe quelle combinaison de lettres, chiffres, espaces, et les caractères `_` `:` `.` `+` `=` `@` `-`. Pour plus d'informations, consultez [Règles de balisage dans IAM et AWS STS](#) dans le Guide de l'utilisateur IAM. Pour demander les formats `corp\username` ou `corp.example.com\username`, remplacez `\` par `/` dans l'assertion SAML.

- **Attribute** élément dont l'**Name** attribut est défini sur `https://aws.amazon.com/SAML/Attributes/:DomainPrincipalTag` (facultatif) — Cet élément contient un **AttributeValue** qui fournit le nom de domaine complet (FQDN) DNS Active Directory aux utilisateurs qui se connectent. Ce paramètre est utilisé avec l'authentification par certificat lorsque l'élément **userPrincipalName** Active Directory correspondant à l'utilisateur contient un autre suffixe. La valeur doit être fournie dans `domain.com`, y compris dans tous les sous-domaines.
- **Attribute** élément dont l'**Name** attribut est défini sur `https://aws.amazon.com/SAML/Attributes/SessionDuration` (facultatif) — Cet élément contient un **AttributeValue** élément qui indique la durée maximale pendant laquelle une session de streaming fédérée d'un utilisateur peut rester active avant qu'une nouvelle authentification ne soit requise. La valeur par défaut est de 3600 secondes (60 minutes). Pour plus d'informations, consultez [SessionDurationAttribute SAML](#).

 Note

Bien que l'attribut **SessionDuration** soit facultatif, nous vous recommandons de l'inclure dans la réponse SAML. Si vous ne spécifiez pas cet attribut, la durée de session est définie sur une valeur par défaut de 3 600 secondes (60 minutes). WorkSpaces les sessions de bureau sont déconnectées une fois leur durée de session expirée.

Pour plus d'informations sur la configuration de ces éléments, consultez [Configuration des assertions SAML pour la réponse d'authentification](#) dans le Guide de l'utilisateur IAM. Pour plus d'informations sur les exigences de configuration spécifiques à votre fournisseur d'identité, consultez sa documentation.

Étape 6 : Configurer l'état du relais de votre fédération

Ensuite, utilisez votre IdP pour configurer l'état du relais de votre fédération afin qu'il pointe vers l'URL de l'état du relais de WorkSpaces répertoire. Une fois l'authentification réussie AWS, l'utilisateur est dirigé vers le point de terminaison du WorkSpaces répertoire, défini comme l'état du relais dans la réponse d'authentification SAML.

Le format de URL d'état du relais est le suivant :

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

Construisez l'URL de votre état de relais à partir du code d'enregistrement de votre WorkSpaces répertoire et du point de terminaison de l'état du relais associé à la région dans laquelle se trouve votre répertoire. Le code d'enregistrement se trouve dans la console WorkSpaces de gestion.

Si vous utilisez la redirection entre régions pour WorkSpaces, vous pouvez éventuellement remplacer le code d'enregistrement par le nom de domaine complet (FQDN) associé aux annuaires de votre région principale et de votre région de basculement. Pour plus d'informations, consultez la section Redirection [entre régions pour Amazon WorkSpaces](#). Lors de l'utilisation de la redirection entre régions et de l'authentification SAML 2.0, les annuaires principal et de basculement doivent être activés pour l'authentification SAML 2.0 et configurés indépendamment avec l'IdP en utilisant le point de terminaison d'état du relais associé à chaque région. Cela permettra de configurer correctement le FQDN lorsque les utilisateurs enregistreront leurs applications WorkSpaces clientes avant de se connecter, et permettra aux utilisateurs de s'authentifier lors d'un événement de basculement.

Le tableau suivant répertorie les points de terminaison de l'état du relais pour les régions où l'authentification WorkSpaces SAML 2.0 est disponible.

Régions dans lesquelles l'authentification WorkSpaces SAML 2.0 est disponible

Région	Point de terminaison RelayState
Région USA Est (Virginie du Nord)	- workspaces.euc-sso.us-east-1.aws.amazon.com - espaces de travail (FIPS). euc-sso-fips.us-east-1.aws.amazon.com
Région USA Ouest (Oregon)	- workspaces.euc-sso.us-west-2.aws.amazon.com - espaces de travail (FIPS). euc-sso-fips.us-west-2.aws.amazon.com
Région Afrique (Le Cap)	workspaces.euc-sso.af-south-1.aws.amazon.com

Région	Point de terminaison RelayState
Région Asie-Pacifique (Mumbai)	<code>workspaces.euc-ss0.ap-south-1.aws.amazon.com</code>
Région Asie-Pacifique (Séoul)	<code>workspaces.euc-ss0.ap-northeast-2.amazonaws.com</code>
Région Asie-Pacifique (Singapour)	<code>workspaces.euc-ss0.ap-southeast-1.amazonaws.com</code>
Région Asie-Pacifique (Sydney)	<code>workspaces.euc-ss0.ap-southeast-2.amazonaws.com</code>
Région Asie-Pacifique (Tokyo)	<code>workspaces.euc-ss0.ap-northeast-1.amazonaws.com</code>
Région Canada (Centre)	<code>workspaces.euc-ss0.ca-central-1.amazonaws.com</code>
Région Europe (Francfort)	<code>workspaces.euc-ss0.eu-central-1.amazonaws.com</code>
Région Europe (Irlande)	<code>workspaces.euc-ss0.eu-west-1.amazonaws.com</code>
Région Europe (Londres)	<code>workspaces.euc-ss0.eu-west-2.amazonaws.com</code>
Région Amérique du Sud (São Paulo)	<code>workspaces.euc-ss0.sa-east-1.amazonaws.com</code>
Région Israël (Tel Aviv)	<code>workspaces.euc-ss0.il-central-1.amazonaws.com</code>

Région	Point de terminaison RelayState
AWS GovCloud (US-Ouest)	- espaces de travail.euc-ss0. us-gov-west-1. amazonaws-us-gov.com - espaces de travail (FIPS). euc-ss0-fips. us-gov-west-1. amazonaws-us-gov.com  Note Pour plus d'informations, consultez Amazon WorkSpaces dans le guide de l'utilisateur AWS GovCloud (États-Unis).
AWS GovCloud (USA Est)	- espaces de travail.euc-ss0. us-gov-east-1. amazonaws-us-gov.com - espaces de travail (FIPS). euc-ss0-fips. us-gov-east-1. amazonaws-us-gov.com  Note Pour plus d'informations, consultez Amazon WorkSpaces dans le guide de l'utilisateur AWS GovCloud (États-Unis).

Avec un flux initié par un fournisseur d'identité (IdP), vous pouvez choisir de spécifier le client que vous souhaitez utiliser pour la fédération SAML 2.0. Pour ce faire, spécifiez l'URL de l'état du relais native ou web à la fin de celle-ci, après `&client=`. Lorsque le paramètre est spécifié dans une URL d'état de relais, les sessions correspondantes démarrent automatiquement dans le client spécifié.

Étape 7 : Activez l'intégration avec SAML 2.0 dans votre répertoire WorkSpaces

Vous pouvez utiliser la WorkSpaces console pour activer l'authentification SAML 2.0 sur le WorkSpaces répertoire.

Pour activer l'intégration avec SAML 2.0

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez l'ID du répertoire pour votre WorkSpaces.
4. Sous Authentification, choisissez Modifier.
5. Choisissez Modifier le fournisseur d'identité SAML 2.0.
6. Cochez la case Activer l'authentification SAML 2.0.
7. Pour l'URL d'accès utilisateur et le nom du paramètre de lien profond de l'IdP, entrez les valeurs applicables à votre IdP et à l'application que vous avez configurée à l'étape 1. La valeur par défaut du nom du paramètre de lien profond IdP est RelayState « » si vous omettez ce paramètre. Le tableau suivant répertorie les URL d'accès utilisateur et les noms de paramètres propres aux différents fournisseurs d'identité pour les applications.

Domaines et adresses IP à ajouter à votre liste d'autorisation

Fournisseur d'identité	Paramètre	URL d'accès utilisateur
ADFS	RelayState	<code>https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri></code>
Azure AD	RelayState	<code>https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id></code>
Duo Single Sign-On	RelayState	<code>https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso</code>
Okta	RelayState	<code>https://<sub_domain>.okta.com/app/<a</code>

Fournisseur d'identité	Paramètre	URL d'accès utilisateur
		pp_name>/<app_id>/sso/saml
OneLogin	RelayState	https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>
JumpCloud	RelayState	https://sso.jumpcloud.com/saml2/<app-id>
Auth0	RelayState	https://<DefaultTenantName>.us.auth0.com/samlp/<Client_Id>
PingFederate	TargetResource	https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>
PingOne pour Enterprise	TargetResource	https://sso.connect.pingidentity.com/sso/sp/initssso?saasid=<app_id>&idpid=<idp_id>

L'URL d'accès utilisateur est généralement définie par le fournisseur pour l'authentification unique non sollicitée initiée par un IdP. Un utilisateur peut saisir cette URL dans un navigateur Web pour fédérer directement vers l'application SAML. Pour tester l'URL d'accès utilisateur et les valeurs des paramètres de votre IdP, choisissez Tester. Copiez et collez l'URL de test dans une fenêtre privée de votre navigateur actuel ou d'un autre navigateur pour tester l'ouverture de session SAML 2.0 sans interrompre votre session de console de AWS gestion en cours. Lorsque le flux initié par l'IdP s'ouvre, vous pouvez enregistrer votre WorkSpaces client. Pour plus d'informations, consultez la section [Flux initié par le fournisseur d'identité \(IdP\)](#).

8. Gérez les paramètres de secours en cochant ou en désélectionnant Autoriser les clients qui ne prennent pas en charge le protocole SAML 2.0 à se connecter. Activez ce paramètre pour continuer à permettre à vos utilisateurs d'accéder à WorkSpaces des types de clients ou à des versions qui ne prennent pas en charge le protocole SAML 2.0 ou s'ils ont besoin de temps pour passer à la dernière version du client.

 Note

Ce paramètre permet aux utilisateurs de contourner SAML 2.0 et de se connecter à l'aide de l'authentification par annuaire en utilisant les anciennes versions du client.

9. Pour utiliser SAML avec le client Web, activez Web Access. Pour plus d'informations, consultez [Activer et configurer Amazon WorkSpaces Web Access](#).

 Note

PCoL'adresse IP avec SAML n'est pas prise en charge sur Web Access.

10. Choisissez Enregistrer. Votre WorkSpaces répertoire est désormais activé avec l'intégration de SAML 2.0. Vous pouvez utiliser les flux initiés par l'IDP et par l'application client pour enregistrer les applications WorkSpaces clientes et vous y connecter. WorkSpaces

Authentification basée sur des certificats et authentification personnelle WorkSpaces

Vous pouvez utiliser l'authentification basée sur des certificats WorkSpaces pour supprimer l'invite utilisateur à saisir le mot de passe du domaine Active Directory. En utilisant l'authentification par certificat avec votre domaine Active Directory, vous pouvez :

- vous fier à votre fournisseur d'identité SAML 2.0 pour authentifier l'utilisateur et fournir les assertions SAML qui lui correspondent dans Active Directory ;
- offrir une expérience d'authentification unique avec moins d'invites utilisateur ;
- activer les flux d'authentification sans mot de passe via votre fournisseur d'identité SAML 2.0.

L'authentification par certificat utilise les AWS CA privée ressources de votre AWS compte. AWS CA privée permet de créer des hiérarchies d'autorités de certification (CA) privées, y compris racine et subordonnée CAs. Vous pouvez ainsi créer votre propre hiérarchie d'autorités de certification et

émettre des certificats à l'aide de celle-ci pour authentifier les utilisateurs internes. AWS CA privée

Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Autorité de certification privée](#).

Lorsque vous utilisez AWS CA privée l'authentification basée sur des certificats, WorkSpaces vous demandera automatiquement des certificats pour vos utilisateurs lors de l'authentification de session. Les utilisateurs sont authentifiés auprès d'Active Directory à l'aide d'une carte à puce virtuelle allouée avec les certificats.

L'authentification par certificat est prise en charge avec les offres Windows WorkSpaces on DCV utilisant les dernières applications clientes WorkSpaces Web Access, Windows et macOS. Ouvrez les [téléchargements d'Amazon WorkSpaces Client](#) pour trouver les dernières versions :

- Client Windows version 5.5.0 ou ultérieure
- Client macOS version 5.6.0 ou ultérieure

Pour plus d'informations sur la configuration de l'authentification basée sur des certificats avec Amazon WorkSpaces, consultez [Comment configurer l'authentification basée sur des certificats pour Amazon WorkSpaces et Considérations relatives à la conception dans des environnements hautement réglementés pour l'authentification basée sur des certificats](#) avec des applications et. WorkSpaces WorkSpaces

Conditions préalables

Effectuez les étapes suivantes avant d'activer l'authentification par certificat.

1. Configurez votre WorkSpaces annuaire avec l'intégration SAML 2.0 pour utiliser l'authentification basée sur des certificats. Pour plus d'informations, consultez la section [WorkSpacesIntégration à SAML 2.0](#).
2. Configurez l'attribut `userPrincipalName` dans votre assertion SAML. Pour plus d'informations, consultez [Créer des assertions pour la réponse de l'authentification SAML](#).
3. Configurez l'attribut `ObjectSid` dans votre assertion SAML. Cela est nécessaire pour effectuer un mappage renforcé vers l'utilisateur Active Directory. L'authentification par certificat échoue quand l'attribut ne correspond pas à l'identifiant de sécurité (SID) Active Directory de l'utilisateur spécifié dans l'attribut `NameID SAML_Subject`. Pour plus d'informations, consultez [Créer des assertions pour la réponse de l'authentification SAML](#).

 Note

Selon [Microsoft KB5 014754](#), l'ObjectSidattribut deviendra obligatoire pour l'authentification basée sur des certificats après le 10 septembre 2025.

4. Ajoutez l'TagSessionautorisation [sts](#) : à la politique de confiance de votre rôle IAM utilisée avec votre configuration SAML 2.0 si elle n'est pas déjà présente. Cette autorisation est requise pour utiliser l'authentification par certificat. Pour plus d'informations, consultez [Créer un rôle IAM Fédération SAML 2.0](#).
5. Créez une autorité de certification (CA) privée AWS CA privée si vous n'en avez pas configuré une avec votre Active Directory. AWS CA privée est obligatoire pour utiliser l'authentification basée sur des certificats. Pour plus d'informations, consultez [la section Planification de votre AWS CA privée déploiement](#) et suivez les instructions pour configurer une autorité de certification pour l'authentification basée sur des certificats. Les AWS CA privée paramètres suivants sont les plus courants pour les cas d'utilisation de l'authentification basée sur des certificats :
 - a. Options de type de CA :
 - i. Mode d'utilisation de la CA pour certificat de courte durée (recommandé si vous utilisez la CA uniquement afin d'émettre des certificats utilisateur final pour l'authentification par certificat)
 - ii. Hiérarchie de niveau unique avec CA racine (vous pouvez aussi choisir une CA subordonnée si vous souhaitez intégrer une hiérarchie de CA existante)
 - b. Options d'algorithme principal : RSA 2048
 - c. Options de nom unique du sujet : utilisez n'importe quelle combinaison d'options pour identifier la CA dans votre magasin d'autorités de certification racines de confiance Active Directory.
 - d. Options de révocation des certificats : Distribution de CRL

 Note

L'authentification par certificat nécessite un point de distribution de CRL en ligne accessible depuis les bureaux et le contrôleur de domaine. Cela nécessite un accès non authentifié au compartiment Amazon S3 configuré pour les entrées privées de la CA CRL, ou une CloudFront distribution qui aura accès au compartiment S3 si celui-ci bloque l'accès public. Pour plus d'informations, consultez [Planification d'une liste de révocation de certificats \(CRL\)](#).

6. Balisez votre autorité de certification privée avec une clé autorisée euc-private-ca pour désigner la CA à utiliser avec l'authentification par certificat EUC. La clé ne nécessite pas de valeur. Pour plus d'informations, consultez [Gestion des balises pour votre CA privée](#).
7. L'authentification par certificat utilise des cartes à puce virtuelles pour l'ouverture des sessions. En suivant les [Recommandations pour l'activation de l'ouverture de session de carte à puce auprès d'autorités de certification tierces](#) dans Active Directory, effectuez les opérations suivantes :
 - Configurez les contrôleurs de domaine avec un certificat de contrôleur de domaine pour authentifier les utilisateurs de cartes à puce. Si une CA d'entreprise provenant des services de certificats Active Directory est configurée dans Active Directory, les contrôleurs de domaine sont automatiquement inscrits avec des certificats pour permettre l'ouverture de session par carte à puce. Si vous ne disposez pas des services de certificats Active Directory, consultez [Configuration requise pour les certificats de contrôleur de domaine provenant d'une autorité de certification tierce](#). Vous pouvez créer un certificat de contrôleur de domaine avec AWS CA privée. Dans ce cas, n'utilisez pas une CA privée configurée pour les certificats de courte durée.

 Note

Si vous en utilisez AWS Managed Microsoft AD, vous pouvez configurer les services de certificats sur une EC2 instance afin de satisfaire aux exigences relatives aux certificats de contrôleur de domaine. Voir par [AWS Launch Wizard](#) exemple les déploiements de services de certificats AWS Managed Microsoft AD configurés avec Active Directory. AWS L'autorité de certification privée peut être configurée en tant que subordonnée à l'autorité de certification Active Directory Certificate Services, ou peut être configurée comme sa propre racine lors de l'utilisation AWS Managed Microsoft AD.

Une tâche de configuration supplémentaire associée aux AWS Managed Microsoft AD services de certificats Active Directory consiste à créer des règles de sortie depuis le groupe de sécurité VPC du contrôleur vers l'instance exécutant les services de certificats, en autorisant EC2 les ports TCP 135 et 49152-65535 à activer l'inscription automatique des certificats. En outre, l' EC2 instance en cours d'exécution doit autoriser l'accès entrant sur les mêmes ports depuis les instances de domaine, y compris les contrôleurs de domaine. Pour plus d'informations sur la localisation du groupe de sécurité, AWS Managed Microsoft AD voir [Configurer vos sous-réseaux et groupes de sécurité VPC](#).

- Sur la AWS CA privée console ou à l'aide du SDK ou de la CLI, sélectionnez votre autorité de certification et, sous le certificat de l'autorité de certification, exportez le certificat privé de l'autorité de certification. Pour plus d'informations, consultez [Exportation d'un certificat privé](#).

- Publiez la CA dans Active Directory. Connectez-vous à un contrôleur de domaine ou à un poste associé à un domaine. Copiez le certificat privé de la CA à l'emplacement (<path>\<file>) de votre choix et exécutez les commandes suivantes en tant qu'administrateur de domaine. Vous pouvez également utiliser la stratégie de groupe et l'outil Microsoft PKI Health Tool (PKIView) pour publier l'autorité de certification. Pour plus d'informations, consultez [Instructions de configuration](#).

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f <path>\<file> NTAAuthCA
```

Assurez-vous que les commandes s'exécutent correctement, puis supprimez le fichier de certificat privé. En fonction des paramètres de réplication Active Directory, la publication de la CA sur vos contrôleurs de domaine et instances de bureau peut prendre plusieurs minutes.

Note

- Active Directory doit distribuer automatiquement l'autorité de certification aux autorités de certification Trusted Root et aux NTAAuth magasins Enterprise pour les WorkSpaces ordinateurs de bureau lorsqu'ils sont joints au domaine.

Activation de l'authentification par certificat

Procédez comme suit pour activer l'authentification par certificat.

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez l'ID de répertoire pour votre WorkSpaces.
4. Sous Authentification, cliquez sur Modifier.
5. Cliquez sur Modifier l'authentification par certificat.
6. Cochez la case Activer l'authentification par certificat.
7. Vérifiez que l'ARN (Amazon Resource Name) de votre CA privée est associé dans la liste. L'autorité de certification privée doit se trouver dans le même AWS compte et Région AWS doit être étiquetée avec une clé habilitée euc-private-ca à apparaître dans la liste.
8. Cliquez sur Save Changes (Enregistrer les modifications). L'authentification par certificat est désormais activée.

9. Redémarrez vos packs Windows WorkSpaces on DCV pour que les modifications prennent effet. Pour plus d'informations, voir [Redémarrer un Workspace](#).
10. Après le redémarrage, lorsque les utilisateurs s'authentifient via SAML 2.0 à l'aide d'un client pris en charge, ils ne sont plus invités à saisir le mot de passe de domaine.

Note

Lorsque l'authentification basée sur des certificats est activée pour se connecter WorkSpaces, les utilisateurs ne sont pas invités à utiliser l'authentification multifactorielle (MFA), même si elle est activée dans l'annuaire. Lorsque vous utilisez l'authentification par certificat, la MFA peut être activée via votre fournisseur d'identité SAML 2.0. Pour plus d'informations sur l'AWS Directory Service authentification multifactorielle, consultez [Authentification multifactorielle \(AD Connector\) ou Activer l'authentification multifactorielle](#) pour. AWS Managed Microsoft AD

Gestion de l'authentification par certificat

Certificat d'une autorité de certification (CA)

Dans une configuration typique, le certificat d'une CA privée a une durée de validité de 10 ans. Consultez [Gestion du cycle de vie des CA privées](#) pour plus d'informations sur le remplacement d'une CA privée dont le certificat a expiré, ou la réémission de la CA avec une nouvelle période de validité.

Certificats utilisateur final

Les certificats d'utilisateur final émis par AWS CA privée pour l'authentification WorkSpaces basée sur des certificats ne nécessitent pas de renouvellement ni de révocation. Ces certificats sont de courte durée. WorkSpaces émet automatiquement un nouveau certificat toutes les 24 heures. Ces certificats d'utilisateur final ont une période de validité plus courte qu'une distribution AWS CA privée CRL classique. Par conséquent, les certificats d'utilisateur final n'ont pas besoin d'être révoqués et n'apparaîtront pas dans une CRL.

Rapports d'audit

Vous pouvez créer un rapport d'audit pour répertorier tous les certificats émis ou révoqués par votre autorité de certification privée. Pour plus d'informations, consultez [Utilisation de rapports d'audit avec votre autorité de certification privée](#).

Journalisation et surveillance

Vous pouvez l'utiliser [AWS CloudTrail](#) pour enregistrer les appels d'API vers AWS CA privée by WorkSpaces. Pour plus d'informations, consultez la section [Utilisation CloudTrail](#). Dans [l'historique des CloudTrail événements](#), vous pouvez afficher GetCertificate les noms d'IssueCertificateacm-pca.amazonaws.comévénements provenant de la source d'événements créés par le nom WorkSpaces EcmAssumeRoleSession d'utilisateur. Ces événements seront enregistrés pour chaque demande d'authentification par certificat EUC.

Activer le partage PCA entre comptes

Lorsque vous utilisez le partage entre comptes d'une autorité de certification privée, vous pouvez autoriser d'autres comptes à utiliser une autorité de certification centralisée, ce qui évite d'avoir besoin d'une autorité de certification privée pour chaque compte. L'autorité de certification peut générer et délivrer des certificats en utilisant [AWSResource Access Manager](#) pour gérer les autorisations. Le partage entre comptes CA privés peut être utilisé avec l'authentification WorkSpaces basée sur des certificats (CBA) au sein d'une même région. AWS

Pour utiliser une ressource CA privée partagée avec WorkSpaces CBA

1. Configurez l'autorité de certification privée pour CBA dans un AWS compte centralisé. Pour de plus amples informations, veuillez consulter [Authentification basée sur des certificats et authentification personnelle WorkSpaces](#).
2. Partagez l'autorité de certification privée avec les AWS comptes de WorkSpaces ressources où les ressources utilisent le CBA en suivant les étapes de la section [Comment utiliser la AWS RAM pour partager votre compte ACM Private CA](#) entre plusieurs comptes. Il n'est pas nécessaire de suivre l'étape 3 pour créer un certificat. Vous pouvez partager l'autorité de certification privée avec des AWS comptes individuels ou par le biais d'AWSOrganizations. Pour partager avec des comptes individuels, vous devez accepter l'autorité de certification privée partagée dans votre compte de ressources à l'aide de la console Resource Access Manager (RAM) ou APIs. Lors de la configuration du partage, vérifiez que le partage des ressources RAM de l'autorité de certification privée dans le compte de ressources utilise le modèle d'autorisation AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority gérée. Ce modèle s'aligne sur le modèle PCA utilisé par le rôle de WorkSpaces service lors de l'émission de certificats CBA.
3. Une fois le partage réussi, vous devriez être en mesure de consulter l'autorité de certification privée partagée à l'aide de la console d'autorité de certification privée du compte de ressources.

- Utilisez l'API ou la CLI pour associer l'ARN CA privé au CBA dans les propriétés de votre WorkSpaces répertoire. À l'heure actuelle, la WorkSpaces console ne prend pas en charge la sélection d'une autorité de certification privée partagée ARNs. Exemples de commandes CLI :

```
aws workspaces modify-certificate-based-auth-properties --resource-id <value> --  
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

Accédez à Microsoft Entra ID Joined Personal WorkSpaces

Vous pouvez créer un compte personnel BYOL Windows 10 ou 11 associé à un WorkSpaces identifiant Microsoft Entra et inscrit à Intune. Pour en savoir plus, consultez [Créez un répertoire Microsoft Entra ID dédié avec WorkSpaces Personal](#).

Flux de travail d'authentification

Les sections suivantes décrivent le flux de travail d'authentification lancé par l'application WorkSpaces cliente, WorkSpaces Web Access, et un fournisseur d'identité (IdP) SAML 2.0, Microsoft Entra ID :

- Lorsque le flux est initié par l'IdP. Par exemple, lorsque les utilisateurs choisissent une application dans le portail utilisateur de l'Entra ID dans un navigateur Web.
- Lorsque le flux est initié par le WorkSpaces client. Par exemple, quand les utilisateurs ouvrent l'application client et se connectent.
- Lorsque le flux est initié par WorkSpaces Web Access. Par exemple, quand les utilisateurs ouvrent Web Access dans un navigateur et se connectent.

Dans ces exemples, les utilisateurs saisissent `user@example.onmicrosoft.com` pour se connecter à l'IdP. Sur Entra ID, une application d'entreprise est configurée pour s'intégrer à IAM Identity Center. Les utilisateurs créent un Workspace pour leurs noms d'utilisateur dans un répertoire qui utilise IAM Identity Center comme source d'identité pour se connecter à un tenant Entra ID. En outre, les utilisateurs installent [l'application WorkSpaces cliente](#) sur leur appareil ou utilisent Web Access dans un navigateur Web.

Flux initié par le fournisseur d'identité (IdP) avec l'application client

Le flux initié par l'IdP permet aux utilisateurs d'enregistrer automatiquement l'application WorkSpaces cliente sur leurs appareils sans avoir à saisir de code d' WorkSpaces enregistrement. Les utilisateurs ne se connectent pas à leur compte en WorkSpaces utilisant le flux initié par l'IdP. WorkSpaces l'authentification doit provenir de l'application cliente.

1. À l'aide de leur navigateur Web, les utilisateurs se connectent à l'IdP (Microsoft Entra ID).
2. Une fois connectés à l'IdP, les utilisateurs choisissent l'application AWS IAM Identity Center sur le portail utilisateur de l'IdP.
3. Les utilisateurs sont redirigés vers le portail AWS d'accès dans le navigateur. Ensuite, les utilisateurs choisissent l' WorkSpaces icône.
4. Les utilisateurs sont redirigés vers la page ci-dessous et l'application WorkSpaces cliente s'ouvre automatiquement. Choisissez Open Amazon WorkSpaces app si l'application client ne s'ouvre pas automatiquement.



5. L'application WorkSpaces cliente est désormais enregistrée et les utilisateurs peuvent continuer à se connecter en cliquant sur Continuer pour se connecter à WorkSpaces.

Flux initié par le fournisseur d'identité (IdP) avec Web Access

Le flux d'accès Web initié par l'IdP permet aux utilisateurs de les enregistrer automatiquement WorkSpaces via un navigateur Web sans avoir à saisir de code d' WorkSpaces enregistrement. Les utilisateurs ne se connectent pas à leur compte en WorkSpaces utilisant le flux initié par l'IdP. WorkSpaces l'authentification doit provenir de Web Access.

1. Via leur navigateur Web, les utilisateurs se connectent à l'IdP.
2. Une fois connectés à l'IdP, les utilisateurs cliquent sur l'application AWS IAM Identity Center depuis le portail utilisateur de l'IdP.
3. Les utilisateurs sont redirigés vers le portail AWS d'accès dans le navigateur. Ensuite, les utilisateurs choisissent l'icône WorkSpaces.
4. Dans le navigateur, les utilisateurs sont redirigés vers cette page. Pour ouvrir WorkSpaces, choisissez Amazon WorkSpaces dans le navigateur.



5. L'application WorkSpaces cliente est désormais enregistrée et les utilisateurs peuvent continuer à se connecter via WorkSpaces Web Access.

WorkSpaces flux initié par le client

Le flux initié par le client permet aux utilisateurs de se connecter à leur compte WorkSpaces après s'être connectés à un IdP.

1. Les utilisateurs lancent l'application WorkSpaces cliente (si elle n'est pas déjà en cours d'exécution) et cliquent sur Continuer pour se connecter à WorkSpaces.
2. Les utilisateurs sont redirigés vers leur navigateur Web par défaut pour se connecter à l'IdP. S'ils sont déjà connectés à l'IdP dans leur navigateur, ils n'ont pas besoin de se reconnecter et peuvent ignorer cette étape.
3. Une fois connectés à l'IdP, les utilisateurs sont redirigés vers une fenêtre contextuelle. Suivez les instructions pour autoriser votre navigateur Web à ouvrir l'application cliente.
4. Les utilisateurs sont redirigés vers l'application WorkSpaces cliente, sur l'écran de connexion Windows.

5. Les utilisateurs se connectent à Windows à l'aide de leur nom d'utilisateur et de leurs informations d'identification Entra ID.

WorkSpaces Flux initié par Web Access

Le flux initié par Web Access permet aux utilisateurs de se connecter à leur compte WorkSpaces après s'être connectés à un IdP.

1. Les utilisateurs lancent le WorkSpaces Web Access et choisissent Se connecter.
2. Dans le même onglet du navigateur, les utilisateurs sont redirigés vers le portail IdP. S'ils sont déjà connectés à l'IdP dans leur navigateur, ils n'ont pas besoin de se reconnecter et peuvent ignorer cette étape.
3. Une fois connectés à l'IdP, les utilisateurs sont redirigés vers cette page dans le navigateur et cliquent sur Se connecter à WorkSpaces.
4. Les utilisateurs sont redirigés vers l'application WorkSpaces cliente, sur l'écran de connexion Windows.
5. Les utilisateurs se connectent à Windows à l'aide de leur nom d'utilisateur et de leurs informations d'identification Entra ID.

Première expérience utilisateur

Si vous vous connectez pour la première fois à un système Windows associé à un identifiant Microsoft Entra WorkSpaces, vous devez suivre l'out-of-box expérience (OOBE). Au cours de l'OOBE, WorkSpaces ils sont joints à Entra ID. Vous pouvez personnaliser l'expérience OOBE en configurant le profil de pilote automatique attribué au groupe d'appareils Microsoft Intune que vous créez pour votre WorkSpaces. Pour de plus amples informations, veuillez consulter [Étape 3 : configurer le mode piloté par l'utilisateur de Windows Autopilot](#).

Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal

Les offres Windows et Linux WorkSpaces on DCV autorisent l'utilisation de cartes à puce [CAC \(Common Access Card\)](#) et de [vérification d'identité personnelle \(PIV\)](#) pour l'authentification.

Amazon WorkSpaces prend en charge l'utilisation de cartes à puce à la fois pour l'authentification pré-session et pour l'authentification en cours de session. L'authentification de pré-session fait référence à l'authentification par carte à puce effectuée pendant que les utilisateurs se connectent à

leur WorkSpaces. L'authentification en cours de session fait référence à l'authentification effectuée après la connexion.

Par exemple, les utilisateurs peuvent utiliser des cartes à puce pour l'authentification en cours de session lorsqu'ils travaillent avec des applications et des navigateurs Web. Ou encore, pour les actions nécessitant des autorisations d'administration. Par exemple, si l'utilisateur dispose d'autorisations administratives sur son système Linux WorkSpace, il peut utiliser des cartes à puce pour s'authentifier lors de l'exécution `sudo` et des `sudo -i` commandes.

Table des matières

- [Exigences](#)
- [Limitations](#)
- [Configuration Active Directory](#)
- [Activer les cartes à puce pour Windows WorkSpaces](#)
- [Activez les cartes à puce pour Ubuntu, Rocky Linux et Red Hat Enterprise Linux WorkSpaces](#)
- [Activer les cartes à puce pour Amazon Linux 2 WorkSpaces](#)

Exigences

- Un annuaire Connecteur Active Directory (AD Connector) est requis pour l'authentification pré-session. AD Connector utilise l'authentification mutuelle par certificat (protocole TLS mutuel) pour authentifier les utilisateurs auprès d'Active Directory à l'aide de certificats de carte à puce matériels ou logiciels. Pour plus d'informations sur la façon de configurer AD Connector et l'annuaire sur site, consultez [Configuration Active Directory](#).
- Pour utiliser une carte à puce sous Windows ou Linux WorkSpace, l'utilisateur doit utiliser le client Amazon WorkSpaces Windows version 3.1.1 ou ultérieure, le client WorkSpaces macOS version 3.1.5 ou ultérieure, ou le client WorkSpaces Ubuntu 22.04 version 2024.1 ou ultérieure (l'authentification par carte à puce n'est pas prise en charge avec WorkSpaces le client Ubuntu 20.04). Pour plus d'informations sur l'utilisation des cartes à puce avec les clients Windows et macOS, consultez la section [Support des cartes à puce](#) dans le guide de WorkSpaces l'utilisateur Amazon.
- L'autorité de certification (CA) racine et les certificats de carte à puce doivent répondre à certaines exigences. Pour plus d'informations, consultez [Activer l'authentification mTLS dans AD Connector pour une utilisation avec des cartes à puce](#) dans le Guide d'administration AWS Directory Service et [Exigences de certificat](#) dans la documentation Microsoft.

Outre ces exigences, les certificats utilisateur utilisés pour l'authentification par carte à puce auprès d'Amazon WorkSpaces doivent inclure les attributs suivants :

- Le nom de l'utilisateur AD userPrincipalName (UPN) dans le champ subjectAltName (SAN) du certificat. Nous recommandons d'émettre des certificats de carte à puce pour l'UPN par défaut de l'utilisateur.

 Note

Amazon Linux 2 WorkSpaces s'appuie sur UPN pour le certificate-to-user mappage. Les nouveaux systèmes Linux WorkSpaces, tels qu'Ubuntu, Rocky Linux et Red Hat Enterprise Linux WorkSpaces, prennent en charge des [méthodes de mappage](#) plus sécurisées.

- L'attribut EKU (Extended Key Usage) de l'authentification client (1.3.6.1.5.5.7.3.2).
- L'attribut EKU d'ouverture de session par carte à puce (1.3.6.1.4.1.311.20.2.2).
- Pour l'authentification pré-session, l'OCSP (Online Certificate Status Protocol) est requis pour vérifier la révocation des certificats. Pour l'authentification en cours de session, l'OCSP est recommandé, mais pas obligatoire.

 Note

Ubuntu WorkSpaces, Rocky Linux WorkSpaces et Red Hat Enterprise Linux WorkSpaces nécessitent l'OCSP pour l'authentification en session par défaut, et la vérification OCSP dans ces systèmes nécessite que l'extension NONCE soit activée sur le répondeur OCSP pour empêcher les attaques par rediffusion. Pour désactiver l'extension NONCE, la vérification OCSP en session doit être complètement désactivée. Pour désactiver la vérification OCSP dans Ubuntu, Rocky Linux et Red Hat Enterprise Linux WorkSpaces, créez un nouveau fichier `/etc/sss/conf.d/disable-ocsp.conf` avec le contenu suivant :

```
[sss]
certificate_verification = no_ocsp
```

Limitations

- Seules l'application cliente WorkSpaces Windows version 3.1.1 ou ultérieure, l'application cliente WorkSpaces macOS version 3.1.5 ou ultérieure et l'application client WorkSpaces Ubuntu 22.04 version 2024.1 ou ultérieure sont actuellement prises en charge pour l'authentification par carte à puce. WorkSpaces L'application cliente Ubuntu 20.04 ou antérieure n'est pas prise en charge pour l'authentification par carte à puce.
- L'application cliente WorkSpaces Windows 3.1.1 ou version ultérieure prend en charge les cartes à puce uniquement lorsque le client est exécuté sur une version 64 bits de Windows.
- Seuls les annuaires AD Connector sont aujourd'hui pris en charge pour l'authentification par carte à puce.
- L'authentification en cours de session est disponible dans toutes les régions où le DCV est pris en charge. L'authentification pré-session est disponible dans les régions suivantes :
 - Région Asie-Pacifique (Sydney)
 - Région Asie-Pacifique (Tokyo)
 - Région Europe (Irlande)
 - AWS GovCloud Région (USA Est)
 - AWS GovCloud Région (USA Ouest)
 - Région USA Est (Virginie du Nord)
 - Région USA Ouest (Oregon)
- Pour l'authentification en cours de session et l'authentification de présession sous Linux ou Windows WorkSpaces, une seule carte à puce est actuellement autorisée à la fois. L'utilisation simultanée de plusieurs cartes peut fonctionner, mais elle n'est pas prise en charge.
- Pour l'authentification pré-session, l'activation de l'authentification par carte à puce et de l'authentification par connexion dans le même annuaire n'est actuellement pas prise en charge.
- Seules les cartes CAC et PIV sont prises en charge pour le moment. D'autres types de cartes à puce matérielles ou logicielles peuvent également fonctionner, mais leur utilisation avec le DCV n'a pas encore été entièrement testée.

Configuration Active Directory

Pour activer l'authentification par carte à puce, vous devez configurer votre annuaire AD Connector et votre annuaire sur site de la façon suivante.

Configuration de l'annuaire AD Connector

Avant de commencer, assurez-vous que l'annuaire AD Connector a été configuré conformément aux instructions de la page [Conditions préalables requises pour AD Connector](#) du Guide d'administration AWS Directory Service . En particulier, assurez-vous d'avoir ouvert les ports nécessaires au niveau du pare-feu.

Pour terminer la configuration de votre répertoire AD Connector, suivez les instructions de la page [Activer l'authentification mTLS dans AD Connector pour une utilisation avec des cartes à puce](#) dans le Guide d'administration AWS Directory Service .

Note

L'authentification par carte à puce nécessite une délégation Kerberos contrainte (KCD) pour fonctionner correctement. KCD exige que la partie nom d'utilisateur du compte de service AD Connector corresponde au AMAccount nom s du même utilisateur. Un AMAccount nom ne peut pas dépasser 20 caractères.

Configuration d'annuaire sur site

Outre la configuration de votre répertoire AD Connector :

- Assurez-vous que l'utilisation étendue des clés (EKU) est définie sur les certificats délivrés aux contrôleurs de domaine pour votre annuaire local. Pour ce faire, utilisez le modèle de certificat d'authentification Kerberos par défaut des services de domaine Active Directory (AD DS). N'utilisez pas de modèle de certificat de contrôleur de domaine ni de modèle de certificat d'authentification de contrôleur de domaine, car ces modèles ne contiennent pas les paramètres nécessaires à l'authentification par carte à puce.
- Pour Linux WorkSpaces, assurez-vous que l'extension NONCE est activée sur le répondeur OCSP de l'autorité de certification délivrant les certificats de carte à puce. Si elle ne peut pas être activée, la vérification OCSP en session devra être désactivée dans Ubuntu, Rocky Linux et Red Hat Enterprise Linux. WorkSpaces Pour désactiver la vérification OCSP, créez un nouveau fichier `/etc/sss/conf.d/disable-ocsp.conf` avec le contenu suivant :

```
[sss]  
certificate_verification = no_ocsp
```

Activer les cartes à puce pour Windows WorkSpaces

Pour obtenir des instructions générales sur la manière d'activer l'authentification par carte à puce dans Windows, consultez [Recommandations pour l'activation de l'ouverture de session de carte à puce auprès d'autorités de certification tierces](#) dans la documentation Microsoft.

Pour détecter l'écran de verrouillage Windows et déconnecter la session

Pour permettre aux utilisateurs de déverrouiller WorkSpaces les fenêtres activées pour l'authentification pré-session par carte à puce lorsque l'écran est verrouillé, vous pouvez activer la détection de l'écran de verrouillage Windows dans les sessions des utilisateurs. Lorsque l'écran de verrouillage Windows est détecté, la WorkSpace session est déconnectée et l'utilisateur peut se reconnecter au WorkSpaces client à l'aide de sa carte à puce.

Vous pouvez utiliser les paramètres de stratégie de groupe pour activer la déconnexion de session lorsque l'écran de verrouillage Windows est détecté dans les instances WorkSpaces Windows. Pour plus d'informations, consultez [Configurer la session de déconnexion lors du verrouillage de l'écran pour DCV](#).

Pour activer l'authentification pré-session ou en cours de session

Par défaut, Windows WorkSpaces n'est pas activé pour prendre en charge l'utilisation de cartes à puce pour l'authentification avant ou pendant la session. Si nécessaire, vous pouvez activer l'authentification en session et en présession pour Windows à l'aide des WorkSpaces paramètres de stratégie de groupe. Pour de plus amples informations, veuillez consulter [Configurer la redirection par carte à puce pour DCV](#).

Pour utiliser l'authentification pré-session, outre la mise à jour des paramètres de stratégie de groupe, vous devez également activer l'authentification pré-session via les paramètres de l'annuaire AD Connector. Pour plus d'informations, suivez les instructions de la page [Activer l'authentification mTLS dans AD Connector pour une utilisation avec des cartes à puce](#) dans le Guide d'administration AWS Directory Service .

Pour permettre aux utilisateurs d'utiliser des cartes à puce dans un navigateur

Si les utilisateurs se servent de Chrome comme navigateur, aucune configuration particulière n'est requise pour l'emploi des cartes à puce.

S'ils se servent de Firefox comme navigateur, vous pouvez leur permettre d'utiliser des cartes à puce dans Firefox via une stratégie de groupe. Vous pouvez utiliser ces [modèles de politique de groupe Firefox](#) dans GitHub.

Par exemple, vous pouvez installer la version 64 bits d'[OpenSC](#) pour Windows pour prendre en charge PKCS #11, puis utiliser le paramètre de stratégie de groupe suivant, où **NAME_OF_DEVICE** représente la valeur souhaitée pour identifier PKCS #11 (comme OpenSC), et **PATH_TO_LIBRARY_FOR_DEVICE** le chemin d'accès au module PKCS #11. Ce chemin doit pointer vers une bibliothèque avec une extension .DLL, comme C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll.

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE  
= PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

Si vous utilisez OpenSC, vous pouvez également charger le module pkcs11 OpenSC dans Firefox en exécutant le programme pkcs11-register.exe. Pour exécuter ce programme, double-cliquez sur le fichier C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe, ou ouvrez une fenêtre d'invite de commandes et exécutez la commande suivante :

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

Pour vérifier que le module pkcs11 OpenSC a été chargé dans Firefox, procédez comme suit :

1. Si Firefox est déjà en cours d'exécution, fermez-le.
2. Ouvrez Firefox. Cliquez sur le bouton de menu

dans l'angle supérieur droit, puis choisissez Paramètres.
3. Sur la page about:preferences, dans le volet de navigation de gauche, sélectionnez Vie privée et sécurité.
4. Sous Certificats, choisissez Périphériques de sécurité.
5. Dans la boîte de dialogue Gestionnaire de périphériques, le cadre de cartes à puce OpenSC (0.21) doit être disponible dans le volet de navigation de gauche, et afficher les valeurs suivantes quand vous le sélectionnez :

Module : OpenSC smartcard framework (0.21)

Chemin : C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll

Résolution des problèmes

Pour plus d'informations sur la résolution des problèmes liés aux cartes à puce, consultez [Problèmes de certificat et de configuration](#) dans la documentation Microsoft.

Voici quelques exemples de problèmes courants :

- Mappage incorrect des emplacements aux certificats
- Plusieurs certificats sur la carte à puce qui peuvent correspondre à l'utilisateur Les certificats sont mis en correspondance selon les critères suivants :
 - Autorité de certification racine du certificat
 - Champs <KU> et <EKU> du certificat
 - UPN dans l'objet du certificat
- Plusieurs certificats avec <EKU>msScLogin dans l'utilisation de la clé

Pour l'authentification par carte à puce, il est en général préférable de n'avoir qu'un seul certificat, mappé au tout premier emplacement de la carte.

Les outils de gestion des certificats et des clés de carte à puce (comme la suppression ou le remappage des certificats et des clés) peuvent être spécifiques au fabricant. Pour plus d'informations, consultez la documentation du fabricant de la carte à puce.

Activez les cartes à puce pour Ubuntu, Rocky Linux et Red Hat Enterprise Linux WorkSpaces

Pour permettre l'utilisation de cartes à puce sur Ubuntu, Rocky Linux et Red Hat Enterprise Linux WorkSpaces, vous devez inclure le certificat racine et tous les certificats CA intermédiaires dans l'Workspace image pour toutes les cartes à puce CAs émettrices et pour toutes les CAs émissions de certificats de contrôleur de domaine.

Pour obtenir votre certificat CA : Vous pouvez obtenir votre certificat CA de plusieurs manières :

- Vous pouvez utiliser un ensemble de certificats CA provenant d'une autorité de certification tierce.

- Vous pouvez exporter votre propre certificat CA à l'aide du site Web d'inscription, qui contient `http://ip_address/certsrv` soit `http://fqdn/certsrv` l'adresse IP *ip_address* et le nom de domaine complet (FQDN) du serveur CA, soit où se *fqdn* trouvent. Pour plus d'informations sur l'utilisation du site d'inscription Web, consultez [Comment exporter un certificat d'autorité de certification racine](#) dans la documentation Microsoft.
- Vous pouvez utiliser la procédure suivante pour exporter le certificat CA depuis un serveur CA qui exécute les services de certificats Active Directory (AD CS). Pour plus d'informations sur l'installation d'AD CS, consultez [Installer l'autorité de certification](#) dans la documentation Microsoft.
 1. Connectez-vous au serveur CA à l'aide d'un compte administrateur.
 2. Dans le menu Démarrer Windows, ouvrez une fenêtre d'invite de commandes (Démarrer > Système Windows > Invite de commandes).
 3. Utilisez la commande suivante pour exporter le certificat CA vers un nouveau fichier, où *rootca*.cer figure le nom du nouveau fichier :

```
certutil -ca.cert rootca.cer
```

Pour plus d'informations sur l'exécution de certutil, consultez la page [certutil](#) dans la documentation Microsoft.

4. Utilisez la commande OpenSSL suivante pour convertir le certificat CA exporté du format DER au format PEM, *rootca* où est le nom du certificat. Pour plus d'informations sur OpenSSL, consultez le site <http://www.openssl.org/>.

```
openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
```

Pour ajouter vos certificats CA à votre système Linux WorkSpaces

Pour vous aider à activer les cartes à puce, nous avons ajouté le `enable_smartcard` script à nos packs Linux WorkSpaces DCV. Ce script effectue les actions suivantes :

- Importe vos certificats CA dans un bundle PEM privé qui définit la racine de confiance pour SSSD (sous Linux WorkSpaces).
- Met à jour la configuration SSSD, PAM et Kerberos, qui inclut l'activation PKINIT (authentification Kerberos à l'aide d'un certificat au lieu d'un mot de passe) lors du provisionnement. Workspace

La procédure suivante explique comment utiliser le `enable_smartcard` script pour importer vos certificats CA et activer l'authentification par carte à puce pour votre système Linux WorkSpaces.

1. Créez un nouveau Linux WorkSpace avec le protocole DCV activé. Lorsque vous lancez le WorkSpace dans la WorkSpaces console Amazon, sur la page Select Bundles, assurez-vous de sélectionner DCV pour le protocole, puis sélectionnez l'un des bundles WorkSpaces publics Linux.
2. Sur le `/etc/skylight.conf` fichier nouvellement créé WorkSpace, assurez-vous qu'il y a une `pam_smartcard = true` ligne dans `[features]` la section :

```
[features]
pam_smartcard = true
```

Note

Si tous vos utilisateurs ne sont pas encore configurés pour utiliser `altSecurityIdentities` un mappage de certificats renforcé, vous pouvez également ajouter une `smartcard_weak_mapping = true` ligne dans la même `[features]` section `/etc/skylight.conf` pour prendre en charge les anciennes méthodes de mappage, mais nous vous recommandons de migrer ces utilisateurs pour utiliser des méthodes de mappage robustes dès que possible.

3. Sur le WorkSpace, exécutez la commande suivante en tant qu'utilisateur root *pem-path1*, où se trouvent *pem-path2*, etc., les chemins d'accès aux fichiers, chacun contenant l'un des certificats CA de la chaîne de confiance pour les certificats de carte à puce et de contrôleur de domaine. Tous ces fichiers doivent être au format PEM et contenir un certificat par fichier. Des modèles globulaires peuvent être utilisés (par exemple, `*.pem`)

```
/usr/lib/skylight/enable_smartcard --ca-cert pem-path1 pem-path2 pem-path3 ...
```

Note

Assurez-vous que des packages de dépendance supplémentaires sont installés sur le WorkSpace avant d'exécuter la commande ci-dessus, en utilisant les commandes suivantes en tant qu'utilisateur root.

Pour Rocky Linux et Red Hat Enterprise Linux WorkSpaces :

```
dnf install sssd-dbus libsss_simpleifp sssd-tools krb5-pkinit opensc
```

Pour Ubuntu WorkSpaces :

```
apt install krb5-pkinit opensc
```

4. Effectuez toute personnalisation supplémentaire sur le WorkSpace. Par exemple, vous souhaitez peut-être ajouter une politique à l'échelle du système pour [permettre aux utilisateurs d'utiliser des cartes à puce dans Firefox](#). (Les utilisateurs de Chrome doivent activer eux-mêmes les cartes à puce sur leurs clients. Pour plus d'informations, consultez la section [Support des cartes à puce](#) dans le guide de WorkSpaces l'utilisateur Amazon.)
5. [Créez une WorkSpace image personnalisée et un bundle](#) à partir du WorkSpace.
6. Utilisez le nouveau pack personnalisé WorkSpaces pour le lancer pour vos utilisateurs.

Vous pouvez autoriser vos utilisateurs à utiliser des cartes à puce dans Firefox en ajoutant une SecurityDevices politique à votre WorkSpace image Linux. Pour plus d'informations sur l'ajout de politiques à l'échelle du système à Firefox, consultez les [modèles de politiques de Mozilla](#) sur GitHub.

Pour permettre aux utilisateurs d'utiliser des cartes à puce dans Firefox

1. Sur le fichier WorkSpace que vous utilisez pour créer votre WorkSpace image, créez un nouveau fichier nommé `policies.json` in `PREFIX/firefox/distribution/`, qui se `PREFIX` trouve `/usr/lib64` sur les systèmes basés sur Fedora (Amazon Linux 2, Red Hat Enterprise Linux et Rocky Linux WorkSpaces) et sur les systèmes basés `/usr/lib` sur Debian (Ubuntu). WorkSpaces
2. Dans le fichier JSON, ajoutez la SecurityDevices politique suivante, où se `NAME_OF_DEVICE` trouve la valeur que vous souhaitez utiliser pour identifier le pkcs module. Par exemple, il se peut que vous souhaitiez utiliser une valeur comme `"OpenSC"` :

```
{
  "policies": {
    "SecurityDevices": {
      "NAME_OF_DEVICE": "PREFIX/opensc-pkcs11.so"
    }
  }
}
```

Résolution des problèmes

Le dépannage de l'authentification par carte à puce est facilité lorsque la pré-session est configurée pour utiliser l'authentification par mot de passe. Pendant le provisionnement des sessions, Linux fait WorkSpaces automatiquement passer le mode d'authentification sur l'hôte à un mode basé sur un mot de passe ou à un mode basé sur une carte à puce en fonction de la méthode d'authentification de présession utilisée. En cas de problème d'authentification par carte à puce, la déconnexion et la reconnexion à l'aide de l'authentification de présession par mot de passe réinitialisent l'espace de travail à l'authentification par mot de passe sur l'hôte. Pour passer manuellement de l'WorkSpaces instance Linux à l'authentification par carte à puce, exécutez `/usr/lib/skylight/resume_smartcard` la commande en tant qu'utilisateur root.

Linux WorkSpaces utilise le logiciel OpenSC pour travailler avec des cartes à puce. Ce logiciel est livré avec des outils tels que `pkcs11-tool` et `pkcs15-tool` qui peuvent être utiles pour résoudre les problèmes liés aux cartes à puce. Ces outils peuvent être utilisés pour inspecter les lecteurs de cartes à puce, les jetons individuels et les emplacements ou certificats PIV sur chaque jeton de carte à puce.

Un outil de `openssl` ligne de commande peut être utile pour résoudre les problèmes liés aux chaînes de confiance, aux répondeurs OCSP ou aux indicateurs manquants KUs/EKUs (utilisation des usage/extended clés), en particulier lorsqu'ils sont associés `pkcs15-tool` à la capacité d'extraire des certificats publics d'une carte à puce.

Options de dépannage courantes :

- Extrayez le premier certificat (généralement le slot PIV 9A) de la carte à puce et enregistrez-le sous le nom suivant : `card-cert.pem` `pkcs15-tool --read-certificate 1 > card-cert.pem`
- Validez le certificat extrait par rapport à la base de données de confiance sur WorkSpace : `openssl verify -verbose -CAfile /etc/sssdpki/sssdpki_auth_ca_db.pem -cert card-cert.pem`
- Obtenez l'URL OCSP à partir du certificat de carte à puce extrait : `openssl x509 -noout -ocsp_uri -in card-cert.pem`
- Vérifiez que la réponse OCSP indique que le certificat est valide et inclut NONCE : `openssl ocsp -issuer /etc/sssdpki/sssdpki_auth_ca_db.pem -CAfile /etc/sssdpki/sssdpki_auth_ca_db.pem -cert card-cert.pem -text -url OCSP_URI`, où se `OCSP_URI` trouve l'URL OCSP ci-dessus.

- Vérifiez si le certificat du contrôleur de domaine est considéré comme fiable : `openssl s_client -connect DC_HOSTNAME:636 -showcerts | openssl verify -verbose -CAfile /etc/sssdpki/sssdpki_auth_ca_db.pem`, où **DC_HOSTNAME** est le nom d'hôte de l'un des contrôleurs de domaine de votre domaine Active Directory.
- Vérifiez que le certificat du contrôleur de domaine a défini l'EKU d'authentification KDC (utilisation étendue des clés) : `openssl s_client -connect DC_HOSTNAME:636 -showcerts | openssl x509 -noout -text`
- Essayez le PKINIT manuel pour voir s'il existe des codes d'erreur susceptibles d'être utilisés pour affiner le problème : `KRB5_TRACE=/dev/stdout kinit -X X509_user_identity=PKCS11:opencsc-pkcs11.so:certid=01 -V` où **01** est le numéro de l'un des quatre emplacements PIV principaux de la carte : 01 pour 9A, 02 pour, etc. 9C La plupart des cartes comportent un certificat destiné à l'authentification de l'utilisateur dans l'emplacement 9A.
- Vérifiez si le système est capable de mapper le certificat de carte à puce à un utilisateur AD (exécuter en tant que root) : `dbus-send --print-reply --system --dest=org.freedesktop.sssd.infopipe /org/freedesktop/sssdpki/infopipe/Users org.freedesktop.sssd.infopipe.Users.FindByCertificate string:"$(card-cert.pem)"`. Cela peut être combiné avec l'activation de la journalisation du débogage pour SSSD.

Les problèmes connus les plus courants sont les suivants :

- Chaîne de confiance incomplète pour le certificat de carte à puce : lors de l'importation de certificats à l'aide d'un `enable_smartcard` script, la liste complète de tous les certificats d'autorité de certification racine et intermédiaire doit être fournie. L'`enable_smartcard` affiche une erreur si tous les certificats importés ne sont pas fiables parce qu'ils ne figurent pas dans la liste des certificats d'autorité de certification racine, mais il ne peut pas détecter l'absence d'une chaîne de confiance complète ou du certificat d'autorité de certification intermédiaire le plus interne de l'une des chaînes de confiance. Dans ce cas, il importera les certificats sans erreur, mais un certificat de carte à puce ou un certificat de contrôleur de domaine peuvent toujours être considérés comme non fiables.
- Chaîne de confiance manquante pour les certificats de contrôleur de domaine : si les certificats de contrôleur de domaine sont émis par une autorité de certification différente de celle des cartes à puce (par exemple, dans le cas d'une [carte d'accès commune \(CAC\)](#)), cette chaîne de confiance doit être importée avec la carte à puce émettrice des certificats d'autorité de certification.

- Absence de prise en charge de l'extension NONCE dans le répondeur OCSP - Linux WorkSpaces exige que l'extension NONCE soit activée sur le répondeur OCSP de l'émetteur de la carte à puce. Si elle ne peut pas être activée, la validation OCSP devra être complètement désactivée.
- Les certificats de contrôleur de domaine sont absents (OID 1.3.6.1.5.2.3.1). Pour que l'authentification par carte à puce fonctionne, les certificats de contrôleur de domaine doivent être réémis pour inclure l'`KDC AuthenticationEKU` d'authentification KDC.
- Les certificats de contrôleur de domaine ont expiré. Pour que l'authentification par carte à puce fonctionne, les certificats de contrôleur de domaine doivent être conservés up-to-date.
- Les certificats de carte à puce sont mappés aux utilisateurs dans AD à l'aide de méthodes de mappage faibles. Traditionnellement, le champ UPN dans `subjectAltName` l'attribut était utilisé pour mapper un certificat à un utilisateur dans AD, étant censé correspondre `userPrincipalName` à l'attribut. Cette méthode n'est plus considérée comme une méthode de mappage sécurisée et est interdite par défaut. Il est possible de le réactiver en passant un `--allow-weak-mapping` argument à la `enable_smartcard` commande et en ajoutant une `smartcard_weak_mapping = true` ligne à la `[features]` section du `/etc/skylight.conf` fichier, mais une meilleure solution consiste à utiliser l'une des méthodes de mappage les plus puissantes. Consultez la documentation relative [à l'association de comptes](#) pour plus de détails.

Les outils de gestion des certificats et des clés de carte à puce (comme la suppression ou le remappage des certificats et des clés) peuvent être spécifiques au fabricant. Voici des outils supplémentaires que vous pouvez utiliser pour travailler avec des cartes à puce :

- `opensc-explorer`
- `opensc-tool`
- `pkcs11_inspect`
- `pkcs11_listcerts`
- `pkcs15-tool`

Pour activer la journalisation du débogage

- Ajoutez une `debug_level = LEVEL` ligne `/etc/sss/sss.conf` pour chaque section individuelle, où se **LEVEL** situe le niveau de verbosité souhaité, de 1 à 10. Les journaux de chaque section correspondante peuvent ensuite être trouvés dans le `/var/log/sss/` répertoire. Consultez la documentation SSSD [ici](#) et [ici](#) pour plus de détails.

Activer les cartes à puce pour Amazon Linux 2 WorkSpaces

Note

Amazon Linux 2 WorkSpaces sur DCV présente actuellement les limites suivantes :

- La redirection du presse-papiers, d'entrée audio, d'entrée vidéo et de fuseau horaire n'est pas prise en charge.
- L'utilisation de plusieurs moniteurs n'est pas prise en charge.

Pour permettre l'utilisation de cartes à puce sur Amazon Linux 2 WorkSpaces, vous devez inclure un fichier de certificat CA racine au format PEM dans l' Workspace image.

Pour obtenir votre certificat d'autorité de certification racine : vous pouvez obtenir votre certificat d'autorité de certification racine de plusieurs manières :

- Vous pouvez utiliser un certificat de CA racine géré par une autorité de certification tierce.
- Vous pouvez exporter votre propre certificat de CA racine via le site Web d'inscription, qui est `http://ip_address/certsrv` ou `http://fqdn/certsrv`, où *ip_address* et *fqdn* représentent l'adresse IP et le nom de domaine complet (FQDN) du serveur de certification de la CA racine. Pour plus d'informations sur l'utilisation du site d'inscription Web, consultez [Comment exporter un certificat d'autorité de certification racine](#) dans la documentation Microsoft.
- Vous pouvez utiliser la procédure suivante pour exporter le certificat de CA racine depuis un serveur de certification de CA racine qui exécute les services de certificats Active Directory (AD CS). Pour plus d'informations sur l'installation d'AD CS, consultez [Installer l'autorité de certification](#) dans la documentation Microsoft.
 1. Connectez-vous au serveur de CA racine via un compte administrateur.
 2. Dans le menu Démarrer Windows, ouvrez une fenêtre d'invite de commandes (Démarrer > Système Windows > Invite de commandes).
 3. Utilisez la commande suivante pour exporter le certificat de CA racine vers un nouveau fichier, où *rootca*.cer est le nom du nouveau fichier :

```
certutil -ca.cert rootca.cer
```

Pour plus d'informations sur l'exécution de `certutil`, consultez la page [certutil](#) dans la documentation Microsoft.

4. Utilisez la commande OpenSSL suivante pour convertir le certificat CA racine exporté du format DER au format PEM, `rootca` où est le nom du certificat. Pour plus d'informations sur OpenSSL, consultez le site <http://www.openssl.org/>.

```
openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
```

Pour ajouter votre certificat CA racine à votre Amazon Linux 2 WorkSpaces

Pour vous aider à activer les cartes à puce, nous avons ajouté le `enable_smartcard` script à nos offres Amazon Linux DCV. Ce script effectue les actions suivantes :

- Importation du certificat CA racine dans la base de données des [services de sécurité réseau \(NSS\)](#).
- Installation du module `pam_pkcs11` pour l'authentification PAM (Pluggable Authentication Module).
- Exécute une configuration par défaut, qui inclut l'activation `pkinit` lors du Workspace provisionnement.

La procédure suivante explique comment utiliser le `enable_smartcard` script pour ajouter votre certificat CA racine à votre Amazon Linux 2 WorkSpaces et pour activer les cartes à puce pour votre Amazon Linux 2 WorkSpaces.

1. Créez un nouvel Amazon Linux 2 Workspace avec le protocole DCV activé. Lorsque vous lancez le Workspace dans la WorkSpaces console Amazon, sur la page Select Bundles, assurez-vous de sélectionner DCV pour le protocole, puis sélectionnez l'un des bundles publics Amazon Linux 2.
2. Sur le nouveau Workspace, exécutez la commande suivante en tant qu'utilisateur `root`, où se `pem-path` trouve le chemin d'accès au fichier de certificat de l'autorité de certification racine au format PEM.

```
/usr/lib/skylight/enable_smartcard --ca-cert pem-path
```

 Note

Amazon Linux 2 part du WorkSpaces principe que les certificats figurant sur les cartes à puce sont émis pour le nom d'utilisateur principal (UPN) par défaut de l'utilisateur, par exemple `sAMAccountName@domain`, où se `domain` trouve un nom de domaine complet (FQDN).

Pour utiliser d'autres suffixes UPN, run `/usr/lib/skylight/enable_smartcard --help` pour plus d'informations. Le mappage d'autres suffixes UPN est propre à chaque utilisateur. Par conséquent, ce mappage doit être effectué individuellement sur celui de chaque utilisateur WorkSpace.

3. (Facultatif) Par défaut, tous les services sont activés pour utiliser l'authentification par carte à puce sur Amazon Linux 2 WorkSpaces. Pour limiter l'authentification par carte à puce uniquement à des services spécifiques, vous devez modifier `/etc/pam.d/system-auth`. Supprimer la mise en commentaire de la ligne `auth` pour `pam_succeed_if.so`, et modifiez la liste des services selon les besoins.

Une fois la mise en commentaire supprimée pour la ligne `auth`, vous devez ajouter à la liste le service pour lequel vous souhaitez autoriser l'authentification par carte à puce. Pour qu'un service utilise uniquement l'authentification par mot de passe, vous devez le supprimer de la liste.

4. Procédez à toute personnalisation supplémentaire du WorkSpace. Par exemple, vous souhaitez peut-être ajouter une politique à l'échelle du système pour [permettre aux utilisateurs d'utiliser des cartes à puce dans Firefox](#). (Les utilisateurs de Chrome doivent activer eux-mêmes les cartes à puce sur leurs clients. Pour plus d'informations, consultez la section [Support des cartes à puce](#) dans le guide de WorkSpaces l'utilisateur Amazon.)
5. [Créez une WorkSpace image personnalisée et un bundle](#) à partir du WorkSpace.
6. Utilisez le nouveau pack personnalisé WorkSpaces pour le lancer pour vos utilisateurs.

Vous pouvez autoriser vos utilisateurs à utiliser des cartes à puce dans Firefox en ajoutant une `SecurityDevices` politique à votre WorkSpace image Amazon Linux 2. Pour plus d'informations sur l'ajout de politiques à l'échelle du système à Firefox, consultez les [modèles de politiques de Mozilla](#) sur GitHub.

Pour permettre aux utilisateurs d'utiliser des cartes à puce dans Firefox

1. Sur le fichier WorkSpace que vous utilisez pour créer votre WorkSpace image, créez un nouveau fichier nommé `policies.json` dans `/usr/lib64/firefox/distribution/`.
2. Dans le fichier JSON, ajoutez la SecurityDevices politique suivante, où se `NAME_OF_DEVICE` trouve la valeur que vous souhaitez utiliser pour identifier le pkcs module. Par exemple, il se peut que vous souhaitiez utiliser une valeur comme `"OpenSC"` :

```
{
  "policies": {
    "SecurityDevices": {
      "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
    }
  }
}
```

Résolution des problèmes : pour résoudre les problèmes, nous vous recommandons d'ajouter l'`pkcs11-tool` utilitaire. Il vous permet d'effectuer les actions suivantes :

- Répertorier chaque carte à puce
- Répertorier les emplacements de chaque carte à puce
- Répertorier les certificats sur chaque carte à puce

Voici quelques exemples de problèmes courants :

- Mappage incorrect des emplacements aux certificats
- Plusieurs certificats sur la carte à puce qui peuvent correspondre à l'utilisateur Les certificats sont mis en correspondance selon les critères suivants :
 - Autorité de certification racine du certificat
 - Champs `<KU>` et `<EKU>` du certificat
 - UPN dans l'objet du certificat
- Plusieurs certificats avec `<EKU>msScLogin` dans l'utilisation de la clé

Pour l'authentification par carte à puce, il est en général préférable de n'avoir qu'un seul certificat, mappé au tout premier emplacement de la carte.

Les outils de gestion des certificats et des clés de carte à puce (comme la suppression ou le remappage des certificats et des clés) peuvent être spécifiques au fabricant. Voici des outils supplémentaires que vous pouvez utiliser pour travailler avec des cartes à puce :

- `opensc-explorer`
- `opensc-tool`
- `pkcs11_inspect`
- `pkcs11_listcerts`
- `pkcs15-tool`

Pour activer la journalisation du débogage

Pour résoudre les problèmes liés à la configuration de `pam_pkcs11` et `pam-krb5`, vous pouvez activer la journalisation du débogage.

1. Dans le fichier `/etc/pam.d/system-auth-ac`, modifiez l'action `auth` et faites passer le paramètre `nodebug` de `pam_pkcs11.so` à `debug`.
2. Dans le fichier `/etc/pam_pkcs11/pam_pkcs11.conf`, remplacez `debug = false;` par `debug = true;`. L'option `debug` s'applique séparément à chaque module de mappeur, vous devrez donc peut-être la modifier à la fois sous la section `pam_pkcs11` directement, et aussi sous la section de mappeur appropriée (par défaut, ceci est `mapper generic`).
3. Dans le fichier `/etc/pam.d/system-auth-ac`, modifiez l'action `auth` et ajoutez le paramètre `debug` ou `debug_sensitive` à `pam_krb5.so`.

Une fois que vous avez activé la journalisation du débogage, le système imprime les messages de débogage `pam_pkcs11` directement dans le terminal actif. Les messages de `pam_krb5` sont consignés dans `/var/log/secure`.

Pour vérifier à quel nom d'utilisateur correspond un certificat de carte à puce, utilisez la commande `pklogin_finder` suivante :

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

Lorsque vous y êtes invité, saisissez le code PIN de la carte à puce. `pklogin_finder` sort sur `stdout` le nom d'utilisateur figurant sur le certificat de carte à puce sous la forme ***NETBIOS\username***. Ce nom d'utilisateur doit correspondre au Workspace nom d'utilisateur.

Dans les services de domaine Active Directory (AD DS), le nom de domaine NetBIOS est le nom de domaine antérieur à Windows 2000. Généralement (mais pas toujours), le nom de domaine NetBIOS est le sous-domaine du nom de domaine DNS (Domain Name System). Par exemple, si le nom de domaine DNS est `example.com`, le domaine NetBIOS est généralement `EXAMPLE`. Si le nom de domaine DNS est `corp.example.com`, le domaine NetBIOS est généralement `CORP`.

Par exemple, pour l'utilisateur `mmajor` du domaine `corp.example.com`, le résultat de `pklogin_finder` est `CORP\mmajor`.

Note

Si vous recevez le message `"ERROR:pam_pkcs11.c:504: verify_certificate() failed"`, ceci indique que `pam_pkcs11` a trouvé sur la carte à puce un certificat qui correspond aux critères du nom d'utilisateur, mais qui n'est pas lié à un certificat de CA racine reconnu par la machine. Lorsque cela se produit, `pam_pkcs11` génère le message ci-dessus, puis essaie le certificat suivant. L'authentification n'est autorisée que si un certificat correspondant au nom d'utilisateur et lié à un certificat de CA racine reconnue est trouvé.

Pour résoudre les problèmes de configuration `pam_krb5`, vous pouvez invoquer manuellement `kinit` en mode débogage à l'aide de la commande suivante :

```
KRB5_TRACE=/dev/stdout kinit -V
```

Cette commande devrait réussir à obtenir un ticket d'octroi de tickets (TGT) Kerberos. En cas d'échec, essayez d'ajouter explicitement le nom principal Kerberos approprié à la commande. Par exemple, pour l'utilisateur `mmajor` du domaine `corp.example.com`, utilisez cette commande :

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

Si cette commande aboutit, le problème provient probablement du mappage entre le Workspace nom d'utilisateur et le nom principal Kerberos. Consultez la section `[appdefaults]/pam/mappings` du fichier `/etc/krb5.conf`.

Si cette commande échoue, mais qu'une commande `kinit` basée sur un mot de passe réussit, vérifiez les configurations associées à `pkinit_` dans le fichier `/etc/krb5.conf`. Par exemple, si la carte à puce contient plusieurs certificats, vous devrez peut-être modifier `pkinit_cert_match`.

Fournir un accès à Internet pour les WorkSpaces particuliers

Vos WorkSpaces devez avoir accès à Internet pour pouvoir installer les mises à jour du système d'exploitation et déployer des applications. Vous pouvez utiliser l'une des options suivantes pour autoriser votre accès à Internet WorkSpaces dans un cloud privé virtuel (VPC).

Options

- Lancez vos WorkSpaces sous-réseaux privés et configurez une passerelle NAT dans un sous-réseau public de votre VPC.
- Lancez vos WorkSpaces sous-réseaux publics et attribuez automatiquement ou manuellement des adresses IP publiques à votre WorkSpaces.

Pour plus d'informations sur ces options, consultez les sections correspondantes dans [Configuration d'un VPC pour le personnel WorkSpaces](#).

Avec l'une de ces options, vous devez vous assurer que le groupe de sécurité correspondant WorkSpaces autorise le trafic sortant sur les ports 80 (HTTP) et 443 (HTTPS) vers toutes les destinations (0.0.0.0/0).

Bibliothèque Extras Amazon Linux

Si vous utilisez le référentiel Amazon Linux, votre Amazon Linux WorkSpaces doit avoir accès à Internet ou vous devez configurer des points de terminaison VPC pour ce référentiel et pour le référentiel Amazon Linux principal. Pour plus d'informations, consultez Exemple : autorisation d'accès aux référentiels AMI Amazon Linux dans [Points de terminaison pour Amazon S3](#). Les référentiels AMI Amazon Linux sont des compartiments Amazon S3 dans chaque région. Si vous voulez que des instances dans votre VPC accèdent aux référentiels via un point de terminaison, créez une stratégie de point de terminaison qui autorise l'accès à ces compartiments. La stratégie suivante accorde aux utilisateurs l'accès aux référentiels Amazon Linux.

```
{
  "Statement": [
    {
      "Sid": "AmazonLinux2AMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
```

```
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
    ]
}
]
```

Groupes de sécurité pour WorkSpaces Personal

Lorsque vous enregistrez un répertoire auprès de celui-ci WorkSpaces, il crée deux groupes de sécurité, l'un pour les contrôleurs de répertoire et l'autre pour WorkSpaces le répertoire. Le groupe de sécurité pour les contrôleurs d'annuaire a un nom qui se compose de l'identifiant de répertoire suivi de `_controllers` (par exemple, `d-12345678e1_controllers`). Le nom du groupe de sécurité pour WorkSpaces se compose de l'identifiant du répertoire suivi de `_WorkspacesMembers` (par exemple, `d-123456fc11_WorkspacesMembers`).

Warning

Évitez de modifier, de supprimer ou de détacher les groupes de sécurité `_controllers` et `_WorkspacesMembers`. Soyez prudent quand vous modifiez ou supprimez ces groupes de sécurité, car vous ne pouvez pas les recréer ni les ajouter une fois modifiés ou supprimés. Pour plus d'informations, consultez les [groupes EC2 de sécurité Amazon pour les instances Linux](#) ou les [groupes EC2 de sécurité Amazon pour les instances Windows](#).

Vous pouvez ajouter un groupe WorkSpaces de sécurité par défaut à un répertoire. Une fois que vous avez associé un nouveau groupe de sécurité à un WorkSpaces répertoire, le nouveau groupe de sécurité sera associé au nouveau groupe de sécurité WorkSpaces WorkSpaces que vous lancez ou que vous reconstruisez. Vous pouvez également [ajouter ce nouveau groupe de sécurité par défaut à un groupe existant WorkSpaces sans le reconstruire](#), comme expliqué plus loin dans cette rubrique.

Lorsque vous associez plusieurs groupes de sécurité à un WorkSpaces annuaire, les règles de chaque groupe de sécurité sont efficacement agrégées pour créer un ensemble de règles. Nous vous recommandons de condenser le plus possible vos règles de groupe de sécurité.

Pour plus d'informations sur les groupes de sécurité, consultez [Groupes de sécurité](#) dans le Guide de l'utilisateur Amazon VPC.

Pour ajouter un groupe de sécurité à un WorkSpaces annuaire

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez l'annuaire et choisissez Actions, Mettre à jour les détails.
4. Développez Groupe de sécurité et sélectionnez un groupe de sécurité.
5. Choisissez Update and Exit (Mettre à jour et quitter).

Pour ajouter un groupe de sécurité à un groupe existant WorkSpace sans le reconstruire, vous devez attribuer le nouveau groupe de sécurité à l'Elastic Network Interface (ENI) du WorkSpace.

Pour ajouter un groupe de sécurité à un groupe existant WorkSpace

1. Trouvez l'adresse IP de chacune d'entre elles WorkSpace qui doit être mise à jour.
 - a. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
 - b. Développez chacune WorkSpace d'elles et enregistrez son adresse WorkSpace IP.
2. Trouvez l'ENI correspondant à chacun WorkSpace et mettez à jour son attribution de groupe de sécurité.
 - a. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
 - b. Sous Réseau et sécurité, choisissez Interfaces réseau.
 - c. Recherchez la première adresse IP enregistrée à l'étape 1.
 - d. Sélectionnez l'ENI associé à l'adresse IP, choisissez Actions, puis Modifier les groupes de sécurité.
 - e. Sélectionnez le nouveau groupe de sécurité, puis choisissez Enregistrer.
 - f. Répétez ce processus si nécessaire pour tout autre WorkSpaces.

Groupes de contrôle d'accès IP pour WorkSpaces Personal

Amazon vous WorkSpaces permet de contrôler les adresses IP à partir desquelles vous êtes WorkSpaces accessible. En utilisant des groupes de contrôle basés sur les adresses IP, vous pouvez définir et gérer des groupes d'adresses IP fiables, et autoriser les utilisateurs à accéder à leurs adresses uniquement WorkSpaces lorsqu'ils sont connectés à un réseau fiable.

Un groupe de contrôle d'accès IP agit comme un pare-feu virtuel qui contrôle les adresses IP à partir desquelles les utilisateurs sont autorisés à accéder à leur WorkSpaces. Pour spécifier les plages d'adresses CIDR, ajoutez des règles à votre groupe de contrôle d'accès IP, puis associez le groupe à votre annuaire. Vous pouvez ajouter jusqu'à 30 règles par groupe de contrôle d'accès IP et associer chaque groupe de contrôle d'accès IP à un ou plusieurs annuaires. Vous pouvez créer jusqu'à 140 groupes de contrôle d'accès IP par région et par AWS compte. Toutefois, vous ne pouvez associer qu'un maximum de 35 groupes de contrôle d'accès IP à un seul annuaire.

Un groupe de contrôle d'accès IP par défaut est associé à chaque annuaire. Ce groupe par défaut inclut une règle par défaut qui permet aux utilisateurs d'y accéder WorkSpaces de n'importe où. Vous ne pouvez pas modifier le groupe de contrôle d'accès IP par défaut de votre annuaire. Si vous n'associez aucun groupe de contrôle d'accès IP à votre annuaire, le groupe par défaut est utilisé. Si vous associez un groupe de contrôle d'accès IP à un annuaire, le groupe de contrôle d'accès IP par défaut est dissocié.

Pour spécifier les adresses IP publiques et les plages d'adresses IP de vos réseaux approuvés, ajoutez des règles à vos groupes de contrôle d'accès IP. Si vos utilisateurs y accèdent WorkSpaces via une passerelle NAT ou un VPN, vous devez créer des règles qui autorisent le trafic provenant des adresses IP publiques pour la passerelle NAT ou le VPN.

Note

- Les groupes de contrôle d'accès IP n'autorisent pas l'utilisation d'adresses IP dynamiques pour NATs. Si vous utilisez un NAT, configurez-le pour qu'il utilise une adresse IP statique au lieu d'une adresse IP dynamique. Assurez-vous que le NAT achemine tout le trafic UDP via la même adresse IP statique pendant toute la durée de la WorkSpaces session.
- Les groupes de contrôle d'accès IP contrôlent les adresses IP à partir desquelles les utilisateurs peuvent connecter leurs sessions de streaming WorkSpaces. Les utilisateurs peuvent toujours exécuter des fonctionnalités, telles que le redémarrage, la reconstruction, l'arrêt, à partir de n'importe quelle adresse IP à l'aide d'Amazon WorkSpaces public APIs.
- Les groupes de contrôle d'accès IP ne s'appliquent pas lorsque le point de terminaison VPC pour le streaming est configuré pour un annuaire.
- Lorsque vous modifiez un contrôle d'accès IP, les sessions actives ne sont pas immédiatement interrompues ; les modifications ne seront appliquées qu'aux nouvelles sessions.

Vous pouvez utiliser cette fonctionnalité avec Web Access, les clients PCo IP zéro et les applications clientes pour macOS, iPad, Windows, Chromebook et Android.

Création d'un groupe de contrôles d'accès IP

Vous pouvez créer un groupe de contrôle d'accès IP de la façon suivante. Chaque groupe de contrôle d'accès IP peut contenir jusqu'à 30 règles.

Pour créer un groupe de contrôles d'accès IP

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Contrôles d'accès IP.
3. Choisissez Créer un groupe IP.
4. Dans la boîte de dialogue Créer un groupe IP, entrez le nom et la description du groupe, puis choisissez Créer.
5. Sélectionnez le groupe et choisissez Modifier.
6. Pour chaque adresse IP, choisissez Ajouter une règle. Pour Source, entrez l'adresse IP ou la plage d'adresses IP. Pour Description, entrez une description. Lorsque vous avez fini d'ajouter des règles, choisissez Enregistrer.

Association d'un groupe de contrôle d'accès IP à un annuaire

Vous pouvez associer un groupe de contrôle d'accès IP à un annuaire pour vous assurer qu'WorkSpaces ils ne sont accessibles que depuis des réseaux fiables.

Si vous associez un groupe de contrôle d'accès IP dépourvu de règles à un annuaire, cela bloque tout accès à tous WorkSpaces.

Pour associer un groupe de contrôle d'accès IP à un annuaire

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez l'annuaire et choisissez Actions, Mettre à jour les détails.
4. Développez Groupes de contrôle d'accès IP et sélectionnez un ou plusieurs groupes de contrôle d'accès IP.
5. Choisissez Update and Exit (Mettre à jour et quitter).

Copie d'un groupe de contrôles d'accès IP

Vous pouvez utiliser un groupe de contrôles d'accès IP comme base pour la création d'un nouveau groupe de contrôle d'accès IP.

Pour créer un groupe de contrôles d'accès IP à partir d'un groupe existant

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Contrôles d'accès IP.
3. Sélectionnez le groupe, puis choisissez Actions, Copier vers le nouveau.
4. Dans la boîte de dialogue Copier un groupe IP, entrez le nom et la description du nouveau groupe, puis choisissez Copier un groupe.
5. (Facultatif) Pour modifier les règles copiées à partir du groupe d'origine, sélectionnez le nouveau groupe, puis choisissez Modifier. Ajoutez, mettez à jour ou supprimez des règles en fonction de vos besoins. Choisissez Enregistrer.

Suppression d'un groupe de contrôles d'accès IP

Vous pouvez supprimer une règle d'un groupe de contrôles d'accès IP à tout moment. Si vous supprimez une règle qui a été utilisée pour autoriser une connexion à un WorkSpace, l'utilisateur est déconnecté du WorkSpace.

Avant de supprimer un groupe de contrôle d'accès IP, vous devez le dissocier de tous les annuaires.

Pour supprimer un groupe de contrôles d'accès IP

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Sélectionnez chaque annuaire qui est associé au groupe de contrôle d'accès IP, puis choisissez Actions, Mettre à jour les détails. Développez Groupes de contrôle d'accès IP, désélectionnez la case correspondant au groupe de contrôle d'accès IP, puis choisissez Mettre à jour et quitter.
4. Dans le volet de navigation, choisissez Contrôles d'accès IP.
5. Sélectionnez le groupe cible et choisissez Actions, Supprimer un groupe IP.

Configurer des clients PCo IP zéro pour WorkSpaces Personal

PCoLes clients IP zéro ne sont compatibles qu'avec WorkSpaces les offres groupées utilisant le protocole PCo IP.

Si votre appareil client zéro est doté de la version 6.0.0 ou ultérieure du microprogramme, vos utilisateurs peuvent se connecter WorkSpaces directement à leur Lorsque vos utilisateurs se connectent directement à eux à WorkSpaces l'aide d'un appareil sans client, nous vous recommandons d'utiliser l'authentification multifactorielle (MFA) avec WorkSpaces votre annuaire. Pour plus d'informations sur l'utilisation de la MFA avec votre annuaire, consultez la documentation suivante :

- AWS Managed Microsoft AD : page [Activation de l'authentification multifactorielle \(MFA\) pour AWS Managed Microsoft AD](#) dans le Guide d'administration AWS Directory Service
- AD Connector : page [Activer l'authentification multifactorielle pour AD Connector](#) dans le Guide d'administration AWS Directory Service et section [Authentification multifactorielle \(AD Connector\) pour les particuliers WorkSpaces](#)
- Domaines approuvés : section [Pour activer l'authentification multifactorielle pour AWS Managed Microsoft AD](#) dans le Guide d'administration AWS Directory Service
- Simple AD : Authentification multifactorielle non disponible pour Simple AD

Depuis le 13 avril 2021, PCo IP Connection Manager n'est plus pris en charge pour une utilisation avec aucune version de microprogramme de périphérique client comprise entre 4.6.0 et 6.0.0. Si le microprogramme de votre client zéro n'est pas la version 6.0.0 ou ultérieure, vous pouvez obtenir le dernier microprogramme via un abonnement Desktop Access sur <https://www.teradici.com/desktop-access>.

Important

- Dans l'interface Web d'administration PCo IP de Teradici (AWI) ou dans la console de gestion PCo IP (MC) de Teradici, assurez-vous d'activer le protocole NTP (Network Time Protocol). Pour le nom DNS de l'hôte NTP, utilisez **pool.ntp.org** et définissez le port hôte NTP sur 123. Si le protocole NTP n'est pas activé, les utilisateurs de votre client PCo IP zéro peuvent recevoir des erreurs de certificat, telles que « Le certificat fourni n'est pas valide en raison de l'horodatage ».

- À partir de la version 20.10.4 de l'agent PCo IP, Amazon WorkSpaces désactive la redirection USB par défaut via le registre Windows. Ce paramètre de registre affecte le comportement des périphériques USB lorsque vos utilisateurs utilisent des appareils clients PCo IP zéro pour se connecter à leur WorkSpaces. Pour de plus amples informations, veuillez consulter [Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients PCo IP zéro.](#)

Pour plus d'informations sur la configuration et la connexion à un appareil client PCo IP zéro, consultez la section [PCoIP Zero Client](#) dans le guide de WorkSpaces l'utilisateur Amazon. Pour obtenir la liste des appareils clients PCo IP zéro approuvés, consultez la section [Clients PCo IP Zero](#) sur le site Web de Teradici.

Configurer Android pour Chromebook for Personal WorkSpaces

La version 2.4.13 est la version finale de l'application client Amazon WorkSpaces Chromebook. Étant donné [que Google supprime progressivement le support pour Chrome Apps](#), aucune autre mise à jour ne sera apportée à l'application cliente WorkSpaces Chromebook, et son utilisation n'est pas prise en charge.

Pour les [Chromebooks qui prennent en charge l'installation d'applications Android](#), nous recommandons d'utiliser plutôt l'[application cliente WorkSpaces Android](#).

Certains Chromebooks lancés avant 2019 doivent être activés pour [installer des applications Android](#) avant que les utilisateurs puissent installer l'application cliente Amazon WorkSpaces Android. Pour plus d'informations, consultez [Systèmes Chrome OS prenant en charge les applications Android](#).

Pour gérer à distance l'activation des Chromebooks de vos utilisateurs pour installer des applications Android, veuillez consulter [Configurer Android sur les appareils Chrome](#).

Activer et configurer WorkSpaces Web Access for WorkSpaces Personal

La plupart WorkSpaces des offres sont compatibles avec Amazon WorkSpaces Web Access. Pour obtenir la liste des offres WorkSpaces compatibles avec l'accès par navigateur Web, consultez « Quels WorkSpaces forfaits Amazon prennent en charge l'accès Web ? » dans [Accès client, Web Access et expérience utilisateur](#).

 Note

- Depuis le 7 novembre 2025, Amazon WorkSpaces PCo IP Web Access n'est plus ouvert aux nouveaux clients. La fonctionnalité ne recevra que des mises à jour fonctionnelles et de sécurité critiques à l'avenir. Pour plus d'informations, consultez le [guide de WorkSpaces l'utilisateur Amazon](#).
- L'accès au Web avec DCV pour Windows et Ubuntu WorkSpaces est pris en charge dans toutes les régions où le DCV WorkSpaces est disponible. DCV pour Amazon Linux n' WorkSpaces est disponible qu'en AWS GovCloud (ouest des États-Unis).
- Nous vous recommandons vivement d'utiliser Web Access avec DCV WorkSpaces pour une qualité de streaming et une expérience utilisateur optimales. Les limites suivantes s'appliquent à l'utilisation de Web Access avec PCo IP WorkSpaces :
 - L'accès au Web par PCo IP n'est pas pris en charge en Asie-Pacifique (Mumbai), en Afrique (Le Cap), en Europe (Francfort) et en Israël (Tel Aviv) AWS GovCloud (US) Regions
 - L'accès au Web avec PCo IP n'est pris en charge que pour Windows WorkSpaces, pas avec Amazon Linux ou Ubuntu WorkSpaces.
 - Web Access n'est pas disponible pour certains systèmes Windows 10 WorkSpaces utilisant le protocole PCo IP. Si votre PCo adresse IP WorkSpaces est alimentée par Windows Server 2019 ou 2022, Web Access n'est pas disponible.
 - Les fonctionnalités de l'accès Web via PCo IP sont limitées. Il prend en charge la sortie vidéo, la sortie audio, le clavier et la souris. Il ne prend pas en charge de nombreuses fonctionnalités, notamment l'entrée vidéo, l'entrée audio, la redirection du presse-papiers et les webcams.
- Si vous utilisez macOS sur un VPN et que vous utilisez le navigateur Web Firefox, le navigateur Web ne prendra pas en charge le streaming PCo IP WorkSpaces via WorkSpaces Web Access. Cela est dû à une limitation d'implémentation du protocole WebRTC dans Firefox.

 Important

À compter du 1er octobre 2020, les clients ne pourront plus utiliser le client Amazon WorkSpaces Web Access pour se connecter à Windows 7 personnalisé WorkSpaces ou à Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Étape 1 : Activez l'accès Web à votre WorkSpaces

Vous contrôlez l'accès Web à votre répertoire WorkSpaces au niveau du répertoire. Pour chaque répertoire contenant WorkSpaces auquel vous souhaitez autoriser les utilisateurs à accéder via le client Web Access, procédez comme suit.

Pour activer l'accès Web à votre WorkSpaces

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Dans la colonne ID de l'annuaire, choisissez l'ID de l'annuaire pour lequel vous souhaitez activer l'accès Web.
4. Sur la page Détails de l'annuaire, faites défiler la page jusqu'à la section Autres plateformes et choisissez Modifier.
5. Choisissez Web Access (Accès Web).
6. Choisissez Enregistrer.

 Note

Après avoir activé Web Access, redémarrez votre ordinateur WorkSpace pour que les modifications s'appliquent.

Étape 2 : Configurer l'accès entrant et sortant aux ports pour Web Access

Amazon WorkSpaces Web Access nécessite un accès entrant et sortant pour certains ports. Pour de plus amples informations, veuillez consulter [Ports pour l'accès Web](#).

Étape 3 : Configurer les paramètres de stratégie de groupe et de stratégie de sécurité pour permettre aux utilisateurs de se connecter

Amazon WorkSpaces s'appuie sur une configuration d'écran de connexion spécifique pour permettre aux utilisateurs de se connecter correctement depuis leur client Web Access.

Pour permettre aux utilisateurs de Web Access de se connecter à leur compte WorkSpaces, vous devez configurer un paramètre de stratégie de groupe et trois paramètres de stratégie de sécurité. Si ces paramètres ne sont pas correctement configurés, les utilisateurs peuvent rencontrer de longs délais de connexion ou des écrans noirs lorsqu'ils essaient de se connecter à leur WorkSpaces. Pour configurer ces paramètres, procédez comme suit.

Vous pouvez utiliser les objets de stratégie de groupe (GPOs) pour appliquer des paramètres permettant de gérer Windows WorkSpaces ou les utilisateurs qui font partie de votre WorkSpaces répertoire Windows. Nous vous recommandons de créer une unité organisationnelle pour vos objets WorkSpaces informatiques et une unité organisationnelle pour vos objets WorkSpaces utilisateur.

Pour plus d'informations sur l'utilisation des outils d'administration Active Directory GPOs, consultez la section [Installation des outils d'administration Active Directory](#) dans le Guide d'AWS Directory Service administration.

Pour permettre à l'agent d' WorkSpaces ouverture de session de changer d'utilisateur

Dans la plupart des cas, lorsqu'un utilisateur tente de se connecter à un Workspace, le champ du nom d'utilisateur est prérempli avec le nom de cet utilisateur. Toutefois, si un administrateur a établi une connexion RDP Workspace pour effectuer des tâches de maintenance, le champ du nom d'utilisateur est rempli avec le nom de l'administrateur à la place.

Pour éviter ce problème, désactivez le paramètre de stratégie de groupe Hide entry points for Fast User Switching (Masquer les points d'entrée pour accélérer le changement d'utilisateur). Lorsque vous désactivez ce paramètre, l'agent de WorkSpaces connexion peut utiliser le bouton Changer d'utilisateur pour renseigner le champ du nom d'utilisateur avec le nom correct.

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)
2. Choisissez Action, Edit dans le menu principal.

3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Politiques (Stratégies), Administrative Templates 5Modèle administratifs), System et Logon (Connexion).
4. Ouvrez le paramètre Hide entry points for Fast User Switching (Masquer les points d'entrée pour accélérer le changement d'utilisateur).
5. Dans la boîte de dialogue Hide entry points for Fast User Switching (Masquer les points d'entrée pour accélérer le changement d'utilisateur), choisissez Disabled (Désactivé), puis OK.

Par défaut, la liste des derniers utilisateurs connectés s'affiche à la place du bouton Switch User (Changer d'utilisateur). Selon la configuration du WorkSpace, il est possible que la liste n'affiche pas la vignette Autre utilisateur. Dans ce cas, si le nom d'utilisateur prérempli n'est pas correct, l'agent de WorkSpaces connexion ne peut pas remplir le champ avec le nom correct.

Pour éviter ce problème, activez le paramètre de stratégie de sécurité Interactive logon: Don't display last signed-in (Connexion interactive : Ne pas afficher le dernier connecté) ou Interactive logon: Do not display last user name (Connexion interactive : Ne pas afficher le dernier nom d'utilisateur connecté) (selon la version de Windows que vous utilisez).

Pour masquer le dernier nom d'utilisateur connecté

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)
2. Choisissez Action, Edit dans le menu principal.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Windows Settings (Paramètres Windows), Security Settings (Paramètres de sécurité), Local Policies (Stratégies locales) et Security Options (Options de sécurité).
4. Ouvrez l'un des paramètres suivants :
 - Pour Windows 7 – Ouverture de session interactive : Ne pas afficher le dernier connecté
 - Pour Windows 10 – Ouverture de session interactive : Ne pas afficher le dernier nom d'utilisateur

5. Dans la boîte de dialogue Propriétés (Propriétés) pour le paramètre, choisissez Enabled (Activé), puis OK.

Pour demander d'appuyer sur CTRL+ALT+SUPPR avant que les utilisateurs puissent se connecter

Pour WorkSpaces Web Access, vous devez demander aux utilisateurs d'appuyer sur CTRL+ALT+DEL avant de pouvoir se connecter. Exiger que les utilisateurs appuient sur CTRL+ALT+SUPPR avant de se connecter garantit qu'ils utilisent un chemin de confiance lorsqu'ils entrent leurs mots de passe.

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)
2. Choisissez Action, Edit dans le menu principal.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Windows Settings (Paramètres Windows), Security Settings (Paramètres de sécurité), Local Policies (Stratégies locales) et Security Options (Options de sécurité).
4. Ouvrez le paramètre Interactive logon: Do not require CTRL+ALT+DEL (Connexion interactive: Ne pas exiger CTRL+ALT+SUPPR).
5. Dans l'onglet Local Security Setting (Paramètre de sécurité locale) choisissez Disabled (Désactivé), puis OK.

Pour afficher les informations relatives au domaine et à l'utilisateur lorsque la session est verrouillée

L'agent WorkSpaces de connexion recherche le nom et le domaine de l'utilisateur. Une fois ce paramètre configuré, l'écran de verrouillage affiche le nom complet de l'utilisateur (s'il est spécifié dans Active Directory), son nom de domaine et son nom d'utilisateur.

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)

2. Choisissez Action, Edit dans le menu principal.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Windows Settings (Paramètres Windows), Security Settings (Paramètres de sécurité), Local Policies (Stratégies locales) et Security Options (Options de sécurité).
4. Ouvrez le paramètre Interactive logon: Display user information when the session is locked (Connexion interactive : Afficher les informations utilisateur lorsque la session est verrouillée).
5. Dans l'onglet Local Security Setting (Paramètre de sécurité locale) choisissez User display name, domain and user names (Nom d'affichage de l'utilisateur, noms de domaine et d'utilisateur), puis OK.

Pour appliquer les modifications apportées aux paramètres de stratégie de groupe et de stratégie de sécurité

Les modifications des paramètres de stratégie de groupe et de politique de sécurité prennent effet après la prochaine mise à jour de la stratégie de groupe WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications apportées à la stratégie de groupe et à la stratégie de sécurité dans les procédures précédentes, effectuez l'une des opérations suivantes :

- Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
- À partir d'une invite de commande administrative, entrez `gpupdate /force`.

Configuration du client WorkSpaces léger

La plupart WorkSpaces des offres sont compatibles avec Amazon WorkSpaces Thin Client Access. Pour obtenir la liste des offres WorkSpaces compatibles avec l'accès par navigateur Web, consultez « Quels WorkSpaces forfaits Amazon prennent en charge l'accès client léger ? » dans [Accès client, Web Access et expérience utilisateur](#).

Étape 1 : activer le contrôle d'accès à votre Amazon WorkSpaces Thin Client

Vous contrôlez l'accès des clients légers WorkSpaces à votre répertoire grâce à un contrôle d'accès basé sur l'agent utilisateur. Pour chaque répertoire contenant WorkSpaces auquel vous souhaitez autoriser les utilisateurs à accéder via le client Thin Client Access, procédez comme suit.

Pour activer l'accès des clients légers à votre WorkSpaces

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Dans la colonne ID du répertoire, choisissez l'ID du répertoire pour lequel vous souhaitez activer l'accès client léger.
4. Sur la page Détails de l'annuaire, faites défiler la page jusqu'à la section Autres plateformes et choisissez Modifier.
5. Sélectionnez WorkSpaces Thin Client.
6. Choisissez Enregistrer.

Étape 2 : Configuration de l'accès entrant et sortant aux ports pour l'accès client léger

Amazon WorkSpaces Thin Client Access nécessite un accès entrant et sortant pour certains ports. Pour de plus amples informations, veuillez consulter [Ports pour l'accès Web](#).

Étape 3 : Configurer les paramètres de stratégie de groupe et de stratégie de sécurité pour permettre aux utilisateurs de se connecter

Amazon WorkSpaces s'appuie sur une configuration d'écran de connexion spécifique pour permettre aux utilisateurs de se connecter avec succès depuis leur client Thin Client Access.

1. Pour permettre aux utilisateurs de Thin Client Access de se connecter à leur compte WorkSpaces, vous devez configurer un paramètre de stratégie de groupe et trois paramètres de stratégie de sécurité. Si ces paramètres ne sont pas correctement configurés, les utilisateurs peuvent rencontrer de longs délais de connexion ou des écrans noirs lorsqu'ils essaient de se connecter à leur WorkSpaces. Pour configurer ces paramètres, procédez comme suit.
2. Vous pouvez utiliser les objets de stratégie de groupe (GPOs) pour appliquer des paramètres permettant de gérer Windows WorkSpaces ou les utilisateurs qui font partie de votre WorkSpaces répertoire Windows. Nous vous recommandons de créer une unité organisationnelle pour vos objets WorkSpaces informatiques et une unité organisationnelle pour vos objets WorkSpaces utilisateur.
3. Pour plus d'informations sur l'utilisation des outils d'administration Active Directory GPOs, consultez la section [Installation des outils d'administration Active Directory](#) dans le Guide d'AWS Directory Service administration.

4. Dans la plupart des cas, lorsqu'un utilisateur tente de se connecter à un WorkSpace, le champ du nom d'utilisateur est prérempli avec le nom de cet utilisateur. Toutefois, si un administrateur a établi une connexion RDP WorkSpace pour effectuer des tâches de maintenance, le champ du nom d'utilisateur est rempli avec le nom de l'administrateur à la place.
5. Pour éviter ce problème, désactivez le paramètre de stratégie de groupe Hide entry points for Fast User Switching (Masquer les points d'entrée pour accélérer le changement d'utilisateur). Lorsque vous désactivez ce paramètre, l'agent de WorkSpaces connexion peut utiliser le bouton Changer d'utilisateur pour renseigner le champ du nom d'utilisateur avec le nom correct.

Pour permettre à l'agent d' WorkSpaces ouverture de session de changer d'utilisateur

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)
2. Choisissez Action, Edit dans le menu principal.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Politiques (Stratégies), Administrative Templates 5Modèle administratifs), System et Logon (Connexion).
4. Ouvrez le paramètre Hide entry points for Fast User Switching (Masquer les points d'entrée pour accélérer le changement d'utilisateur).
5. Dans la boîte de dialogue Hide entry points for Fast User Switching (Masquer les points d'entrée pour accélérer le changement d'utilisateur), choisissez Disabled (Désactivé), puis OK.

Par défaut, la liste des derniers utilisateurs connectés s'affiche à la place du bouton Switch User (Changer d'utilisateur). Selon la configuration du WorkSpace, il est possible que la liste n'affiche pas la vignette Autre utilisateur. Dans ce cas, si le nom d'utilisateur prérempli n'est pas correct, l'agent de WorkSpaces connexion ne peut pas remplir le champ avec le nom correct.

Pour éviter ce problème, activez le paramètre de stratégie de sécurité Interactive logon: Don't display last signed-in (Connexion interactive : Ne pas afficher le dernier connecté) ou Interactive logon: Do not display last user name (Connexion interactive : Ne pas afficher le dernier nom d'utilisateur connecté) (selon la version de Windows que vous utilisez).

Pour masquer le dernier nom d'utilisateur connecté

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)
2. Choisissez Action, Edit dans le menu principal.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Windows Settings (Paramètres Windows), Security Settings (Paramètres de sécurité), Local Policies (Stratégies locales) et Security Options (Options de sécurité).
4. Ouvrez l'un des paramètres suivants :
 - Pour Windows 7 – Ouverture de session interactive : Ne pas afficher le dernier connecté
 - Pour Windows 10 – Ouverture de session interactive : Ne pas afficher le dernier nom d'utilisateur
5. Dans la boîte de dialogue Properties (Propriétés) pour le paramètre, choisissez Enabled (Activé), puis OK.

Pour l'accès aux clients WorkSpaces légers, vous devez demander aux utilisateurs d'appuyer sur CTRL+ALT+DEL avant de pouvoir se connecter. Exiger que les utilisateurs appuient sur CTRL+ALT+SUPPR avant de se connecter garantit qu'ils utilisent un chemin de confiance lorsqu'ils entrent leurs mots de passe.

Pour demander d'appuyer sur CTRL+ALT+SUPPR avant que les utilisateurs puissent se connecter

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)
2. Choisissez Action, Edit dans le menu principal.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Windows Settings (Paramètres Windows), Security Settings

(Paramètres de sécurité), Local Policies (Stratégies locales) et Security Options (Options de sécurité).

4. Ouvrez le paramètre Interactive logon: Do not require CTRL+ALT+DEL (Connexion interactive: Ne pas exiger CTRL+ALT+SUPPR).
5. Dans l'onglet Local Security Setting (Paramètre de sécurité locale) choisissez Disabled (Désactivé), puis OK.

L'agent WorkSpaces de connexion recherche le nom et le domaine de l'utilisateur. Une fois ce paramètre configuré, l'écran de verrouillage affiche le nom complet de l'utilisateur (s'il est spécifié dans Active Directory), son nom de domaine et son nom d'utilisateur.

Pour afficher les informations relatives au domaine et à l'utilisateur lorsque la session est verrouillée

1. Ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), accédez à un objet de stratégie de groupe et sélectionnez-le au niveau du domaine ou du contrôleur de domaine de l'annuaire que vous utilisez pour votre WorkSpaces. (Si le [modèle administratif de stratégie de WorkSpaces groupe](#) est installé dans votre domaine, vous pouvez utiliser le WorkSpaces GPO pour les comptes de vos WorkSpaces machines.)
2. Choisissez Action, Edit dans le menu principal.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Windows Settings (Paramètres Windows), Security Settings (Paramètres de sécurité), Local Policies (Stratégies locales) et Security Options (Options de sécurité).
4. Ouvrez le paramètre Interactive logon: Display user information when the session is locked (Connexion interactive : Afficher les informations utilisateur lorsque la session est verrouillée).
5. Dans l'onglet Local Security Setting (Paramètre de sécurité locale) choisissez User display name, domain and user names (Nom d'affichage de l'utilisateur, noms de domaine et d'utilisateur), puis OK.

Les modifications des paramètres de stratégie de groupe et de politique de sécurité prennent effet après la prochaine mise à jour de la stratégie de groupe WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications apportées à la stratégie de groupe et à la stratégie de sécurité dans les procédures précédentes, effectuez l'une des opérations suivantes :

Pour appliquer les modifications apportées aux paramètres de stratégie de groupe et de stratégie de sécurité

1. Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
2. À partir d'une invite de commande administrative, entrez `gpupdate /force`.

Configurer l'autorisation FedRAMP ou la conformité au DoD SRG pour Personal WorkSpaces

Pour vous conformer au [Federal Risk and Authorization Management Program \(FedRAMP\)](#) ou au [Guide des exigences de sécurité du cloud computing \(SRG\) du ministère de la Défense \(DoD\)](#), vous devez configurer WorkSpaces Amazon pour utiliser le chiffrement des terminaux FIPS (Federal Information Processing Standards) au niveau de l'annuaire. Vous devez également utiliser une AWS région des États-Unis agréée par FedRAMP ou conforme aux normes SRG du DoD.

Le niveau d'autorisation FedRAMP (modéré ou élevé) ou le niveau d'impact SRG du DoD (2, 4 ou 5) dépend de la AWS région des États-Unis dans laquelle Amazon est utilisé. WorkSpaces

Pour connaître les niveaux d'autorisation FedRAMP et de conformité au SRG du DoD qui s'appliquent à chaque région, consultez [Services AWS concernés par le programme de conformité](#).

Note

En plus d'utiliser le chiffrement des terminaux FIPS, vous pouvez également chiffrer votre WorkSpaces. Pour de plus amples informations, veuillez consulter [Chiffré WorkSpaces dans WorkSpaces Personal](#).

Prérequis

- Vous devez le créer WorkSpaces dans une [AWS région des États-Unis agréée par FedRAMP ou conforme aux normes SRG du DoD](#).
- Le WorkSpaces répertoire doit être configuré pour utiliser le mode validé FIPS 140-2 pour le chiffrement des terminaux.

 Note

Pour utiliser le paramètre Mode validé FIPS 140-2, le WorkSpaces répertoire doit être nouveau ou tous les répertoires existants WorkSpaces doivent utiliser le mode validé FIPS 140-2 pour le chiffrement des terminaux. Dans le cas contraire, vous ne pouvez pas utiliser ce paramètre. Par conséquent, le paramètre WorkSpaces que vous créez ne sera pas conforme aux exigences de sécurité de FedRAMP ou du DoD.

Reportez-vous à l'[étape 3](#) ci-dessous pour savoir comment vérifier le répertoire.

- Les utilisateurs doivent y accéder WorkSpaces depuis l'une des applications WorkSpaces clientes suivantes :
 - Windows : 2.4.3 ou version ultérieure
 - macOS : 2.4.3 ou version ultérieure pour PCo IP WorkSpaces, et 5.21.0 ou version ultérieure pour DCV WorkSpaces
 - Linux : 3.0.0 ou version ultérieure
 - iOS : 2.4.1 ou version ultérieure
 - Android : 2.4.1 ou version ultérieure
 - Fire Tablet : 2.4.1 ou version ultérieure
 - ChromeOS : 2.4.1 ou version ultérieure
 - Web Access

Pour utiliser le chiffrement des points de terminaison FIPS

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Vérifiez que le répertoire dans lequel vous souhaitez créer un répertoire autorisé par FedRAMP et conforme aux normes SRG du DoD WorkSpaces n'est associé à aucun répertoire existant. WorkSpaces S'ils sont WorkSpaces associés au répertoire et que celui-ci n'est pas déjà activé pour utiliser le mode validé FIPS 140-2, vous pouvez soit le WorkSpaces fermer, soit en créer un nouveau.
4. Choisissez l'annuaire qui répond aux critères ci-dessus, puis choisissez Actions, Update Details (Mettre à jour les détails).
- 5.

Sur la page Update Directory Details (Mettre à jour les détails de l'annuaire) choisissez la flèche pour développer la section Access Control Options (Options de contrôle d'accès) .

6. Pour Chiffrement de point de terminaison, choisissez Mode validation FIPS 140-2 au lieu du Mode de chiffrement TLS (standard).
7. Choisissez Update and Exit (Mettre à jour et quitter).
8. Vous pouvez désormais créer WorkSpaces à partir de ce répertoire des fichiers autorisés par FedRAMP et conformes aux normes SRG du DoD. Pour y accéder WorkSpaces, les utilisateurs doivent utiliser l'une des applications WorkSpaces clientes répertoriées plus haut dans la section [Exigences](#).

Activez les connexions SSH pour votre Linux WorkSpaces dans Personal WorkSpaces

Si vous ou vos utilisateurs souhaitez vous connecter à votre système Linux à l'aide WorkSpaces de la ligne de commande, vous pouvez activer les connexions SSH. Vous pouvez activer les connexions SSH à l'ensemble WorkSpaces d'un répertoire ou à un individu WorkSpaces dans un répertoire.

Pour activer les connexions SSH, vous devez créer un nouveau groupe de sécurité ou mettre à jour un groupe de sécurité existant et ajouter une règle pour autoriser le trafic entrant à cette fin. Les groupes de sécurité font office de pare-feu pour les instances associées, en contrôlant le trafic entrant et le trafic sortant au niveau de l'instance. Après avoir créé ou mis à jour votre groupe de sécurité, vos utilisateurs et d'autres utilisateurs peuvent utiliser PuTTY ou d'autres terminaux pour se connecter depuis leurs appareils à votre système Linux. WorkSpaces Pour de plus amples informations, veuillez consulter [the section called “Groupes de sécurité”](#).

Pour un didacticiel vidéo, voir [Comment puis-je me connecter à mon Amazon Linux WorkSpaces en utilisant SSH ?](#) sur le AWS Knowledge Center. Ce didacticiel concerne Amazon Linux 2 WorkSpaces uniquement.

Table des matières

- [Conditions préalables pour les connexions SSH à Linux WorkSpaces](#)
- [Activer les connexions SSH à tous les systèmes Linux WorkSpaces d'un répertoire](#)
- [Authentification par mot de passe dans WorkSpaces](#)
- [Activer les connexions SSH à un Linux spécifique WorkSpace](#)

- [Se connecter à un système Linux WorkSpace en utilisant Linux ou PuTTY](#)

Conditions préalables pour les connexions SSH à Linux WorkSpaces

- Activation du trafic SSH entrant vers un WorkSpace — Pour ajouter une règle autorisant le trafic SSH entrant vers un ou plusieurs Linux WorkSpaces, assurez-vous de disposer des adresses IP publiques ou privées des appareils nécessitant des connexions SSH à votre WorkSpace. Par exemple, vous pouvez spécifier les adresses IP publiques des appareils situés en dehors de votre cloud privé virtuel (VPC) ou l'adresse IP privée d'une autre instance EC2 dans le même VPC que le vôtre. WorkSpace

Si vous envisagez de vous connecter à un WorkSpace depuis votre appareil local, vous pouvez utiliser la phrase de recherche « quelle est mon adresse IP » dans un navigateur Internet ou utiliser le service suivant : [Vérifier l'adresse IP](#).

- Connexion à un WorkSpace — Les informations suivantes sont requises pour établir une connexion SSH entre un appareil et un système Linux. WorkSpace
 - Le nom NetBIOS du domaine Active Directory auquel vous êtes connecté.
 - Votre nom WorkSpace d'utilisateur.
 - Adresse IP publique ou privée de WorkSpace celle à laquelle vous souhaitez vous connecter.

Privé : si votre VPC est connecté à un réseau d'entreprise et que vous avez accès à ce réseau, vous pouvez spécifier l'adresse IP privée du WorkSpace

Public : si vous avez WorkSpace une adresse IP publique, vous pouvez utiliser la WorkSpaces console pour rechercher l'adresse IP publique, comme décrit dans la procédure suivante.

Pour trouver les adresses IP du système Linux auquel WorkSpace vous souhaitez vous connecter et votre nom d'utilisateur

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Dans la liste des WorkSpaces, choisissez WorkSpace celui pour lequel vous souhaitez activer les connexions SSH.
4. Dans la colonne Mode d'exécution, vérifiez que le WorkSpace statut est Disponible.
5. Cliquez sur la flèche située à gauche du WorkSpace nom pour afficher le résumé intégré et notez les informations suivantes :

- L'Workspace adresse IP. Il s'agit de l'adresse IP privée du Workspace.

L'adresse IP privée est requise pour obtenir l'interface elastic network associée au Workspace. L'interface réseau est requise pour récupérer des informations telles que le groupe de sécurité ou l'adresse IP publique associée au Workspace.

- Le Workspace nom d'utilisateur. Il s'agit du nom d'utilisateur que vous spécifiez pour vous connecter au Workspace.

6. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
7. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
8. Dans le champ de recherche, saisissez l'Workspace adresse IP que vous avez notée à l'étape 5.
9. Sélectionnez l'interface réseau associée à l'Workspace adresse IP.
10. Si vous avez Workspace une adresse IP publique, elle est affichée dans la colonne IP IPv4 publique. Notez cette adresse, le cas échéant.

Pour rechercher le nom NetBIOS du domaine Active Directory auquel vous êtes connecté

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans la liste des annuaires, cliquez sur le lien ID du répertoire correspondant au Workspace.
3. Dans la section Directory details (Détails de l'annuaire) notez le Directory NetBIOS name (Nom NetBIOS de l'annuaire).

Activer les connexions SSH à tous les systèmes Linux WorkSpaces d'un répertoire

Pour activer les connexions SSH à tous les systèmes Linux WorkSpaces d'un répertoire, procédez comme suit.

Pour créer un groupe de sécurité avec une règle autorisant le trafic SSH entrant vers tous les systèmes Linux d'un WorkSpaces répertoire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez Créer un groupe de sécurité.
4. Entrez un nom et une description (facultative) pour votre groupe de sécurité.

5. Pour le VPC, choisissez le VPC qui contient le VPC WorkSpaces auquel vous souhaitez activer les connexions SSH.
6. Dans l'onglet Inbound (Entrant), choisissez Add Rule (Ajouter une règle), puis procédez comme suit :
 - Pour Type, choisissez SSH.
 - Dans Protocol (Protocole), TCP est automatiquement spécifié lorsque vous choisissez SSH.
 - Dans Port Range (Plage de ports), 22 est automatiquement spécifié lorsque vous choisissez SSH.
 - Pour Source, spécifiez la plage CIDR des adresses IP publiques des ordinateurs que les utilisateurs utiliseront pour se connecter à leur WorkSpaces. Par exemple, un réseau d'entreprise ou un réseau domestique.
 - Dans le champ Description (facultatif), saisissez une description pour la règle.
7. Choisissez Créer.
8. Associez ce groupe de sécurité à votre WorkSpaces. Pour plus d'informations sur l'ajout de ce groupe de sécurité à votre WorkSpaces, consultez [Groupes de sécurité pour WorkSpaces Personal](#). Si vous souhaitez associer automatiquement des groupes de sécurité supplémentaires à votre WorkSpaces, consultez ce billet de [blog](#).

Authentification par mot de passe dans WorkSpaces

Pour activer l'authentification par mot de passe sous Linux nouvellement créé WorkSpaces

1. Lancez le WorkSpaces client et connectez-vous à votre Workspace.
2. Ouvrez la fenêtre du terminal.
3. Dans la fenêtre du terminal, exécutez la commande suivante pour activer l'authentification par mot de passe SSH dans cloud-init.

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth: true" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/instance/sem/config_set_passwords && sudo cloud-init single --name set-passwords'
```

Ce script effectuera les opérations suivantes :

- Créez un fichier de configuration dans le répertoire cloud-init. `/etc/cloud/cloud.cfg.d/`

- Modifiez le fichier de configuration pour indiquer à cloud-init d'activer l'authentification par mot de passe SSH.
- Réinitialisez le module set-passwords cloud-init afin qu'il puisse être exécuté à nouveau.
- Exécutez le module set-passwords cloud-init lui-même. Cela va écrire un fichier qui active l'authentification par mot de passe SSH dans le répertoire de configuration SSH/etc/ssh/sshd_config.d/, et redémarrer SSHD afin que le réglage soit effectué immédiatement.

Cela active l'authentification par mot de passe SSH sur votre WorkSpace compte et sera conservée dans les images personnalisées. Si vous activez l'authentification par mot de passe SSH uniquement dans le fichier de configuration SSHD, sans configurer cloud-init, le paramètre ne sera pas conservé lors de l'imagerie sur certains systèmes Linux. WorkSpaces Pour plus d'informations, consultez la section [Définir les mots de passe](#) dans la documentation du module cloud-init.

Pour désactiver l'authentification par mot de passe dans un système Linux existant WorkSpaces

1. Lancez le WorkSpaces client et connectez-vous à votre WorkSpace.
2. Ouvrez la fenêtre du terminal.
3. Dans la fenêtre du terminal, exécutez la commande suivante pour désactiver l'authentification par mot de passe SSH dans cloud-init.

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth: false" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/instance/sem/config_set_passwords && sudo cloud-init single --name set-passwords'
```

Ce script effectuera les opérations suivantes :

- Créez un fichier de configuration dans le répertoire cloud-init. /etc/cloud/cloud.cfg.d/
- Modifiez le fichier de configuration pour indiquer à cloud-init de désactiver l'authentification par mot de passe SSH.
- Réinitialisez le module set-passwords cloud-init afin qu'il puisse être exécuté à nouveau.
- Exécutez le module set-passwords cloud-init lui-même. Cela va écrire un fichier qui active l'authentification par mot de passe SSH dans le répertoire de configuration SSH/etc/ssh/sshd_config.d/, et redémarrer SSHD afin que le réglage soit effectué immédiatement.

Cela désactive immédiatement le SSH dans le Workspace et persistera dans les images personnalisées.

Activer les connexions SSH à un Linux spécifique Workspace

Pour activer les connexions SSH à un système Linux spécifique Workspace, procédez comme suit.

Pour ajouter une règle à un groupe de sécurité existant afin d'autoriser le trafic SSH entrant vers un système Linux spécifique Workspace

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Network & Security (Réseau et sécurité), choisissez Network Interfaces (Interfaces réseau).
3. Dans la barre de recherche, saisissez l'adresse IP privée de Workspace celle à laquelle vous souhaitez activer les connexions SSH.
4. Dans la colonne Security Groups (Groupes de sécurité), cliquez sur le lien du groupe de sécurité.
5. Dans l'onglet Entrant, choisissez Modifier.
6. Choisissez Add Rule (Ajouter une règle) et procédez comme suit :
 - Pour Type, choisissez SSH.
 - Dans Protocol (Protocole), TCP est automatiquement spécifié lorsque vous choisissez SSH.
 - Dans Port Range (Plage de ports), 22 est automatiquement spécifié lorsque vous choisissez SSH.
 - Dans Source, choisissez My IP (Mon adresse IP) ou Custom (Personnalisé), et spécifiez une adresse IP unique ou une plage d'adresses IP dans une notation CIDR. Par exemple, si votre IPv4 adresse est 203.0.113.25, spécifiez 203.0.113.25/32 de répertoirer cette IPv4 adresse unique en notation CIDR. Si votre entreprise alloue des adresses à partir d'une plage, spécifiez la plage complète, telle que 203.0.113.0/24.
 - Dans le champ Description (facultatif), saisissez une description pour la règle.
7. Choisissez Enregistrer.

Se connecter à un système Linux Workspace en utilisant Linux ou PuTTY

Après avoir créé ou mis à jour votre groupe de sécurité et ajouté la règle requise, vos utilisateurs et d'autres utilisateurs peuvent utiliser Linux ou PuTTY pour se connecter depuis leurs appareils au vôtre. WorkSpaces

 Note

Avant d'exécuter l'une des procédures suivantes, assurez-vous de disposer des éléments suivants :

- Le nom NetBIOS du domaine Active Directory auquel vous êtes connecté.
- Le nom d'utilisateur que vous utilisez pour vous connecter au WorkSpace.
- Adresse IP publique ou privée de WorkSpace celle à laquelle vous souhaitez vous connecter.

Pour savoir comment obtenir ces informations, reportez-vous à la section « Conditions requises pour les connexions SSH à Linux WorkSpaces » plus haut dans cette rubrique.

Pour se connecter à un système Linux à WorkSpace l'aide de Linux

1. Ouvrez l'invite de commande en tant qu'administrateur, puis entrez la commande suivante : Pour *NetBIOS nameUsername*, et *WorkSpace IP*, entrez les valeurs applicables.

```
ssh "NetBIOS_NAME\Username"@WorkSpaceIP
```

Voici un exemple de commande SSH où :

- *NetBIOS_NAME* C'est n'importe quelle entreprise
- *Username* C'est Janedoe
- *WorkSpace IP* C'est 203.0.113.25

```
ssh "anycompany\janedoe"@203.0.113.25
```

2. Lorsque vous y êtes invité, entrez le même mot de passe que celui que vous utilisez pour vous authentifier auprès du WorkSpaces client (votre mot de passe Active Directory).

Pour vous connecter à un système Linux à WorkSpace l'aide de PuTTY

1. Ouvrez PuTTY.

2. Dans la boîte de dialogue PuTTY Configuration (Configuration PuTTY), exécutez l'une des actions suivantes :
 - Pour Host Name (or IP address) (Nom d'hôte (ou Adresse IP)), entrez la commande suivante. Remplacez les valeurs par le nom NetBIOS du domaine Active Directory auquel vous êtes connecté, le nom d'utilisateur que vous utilisez pour vous connecter et l'adresse IP du domaine WorkSpace auquel vous souhaitez vous connecter.

```
NetBIOS_NAME\Username@WorkSpaceIP
```

- Pour Port, entrez **22**.
- Pour Connection type (Type de connexion), choisissez SSH.

Pour obtenir un exemple de commande SSH, consultez l'étape 1 de la procédure précédente.

3. Choisissez Ouvrir.
4. Lorsque vous y êtes invité, entrez le même mot de passe que celui que vous utilisez pour vous authentifier auprès du WorkSpaces client (votre mot de passe Active Directory).

Composants de configuration et de service requis pour WorkSpaces Personal

En tant qu'Workspace administrateur, vous devez comprendre ce qui suit à propos de la configuration requise et des composants de service.

- [the section called “Configuration de la table de routage”](#)
- [the section called “Composants pour Windows”](#)
- [the section called “Composants pour Linux”](#)
- [the section called “Composants pour Ubuntu”](#)
- [the section called “Composants pour Rocky Linux ”](#)
- [the section called “Composants pour Red Hat Enterprise Linux ”](#)

Configuration de la table de routage requise

Nous vous recommandons de ne pas modifier la table de routage au niveau du système d'exploitation pour un Workspace. Le WorkSpaces service a besoin des itinéraires préconfigurés

de ce tableau pour surveiller l'état du système et mettre à jour les composants du système. Si des modifications de la table de routage sont nécessaires pour votre organisation, contactez le AWS Support ou l'équipe chargée de votre AWS compte avant d'appliquer les modifications.

Composants de service requis pour Windows

Sous Windows WorkSpaces, les composants de service sont installés aux emplacements suivants. Vous ne devez pas supprimer, modifier, bloquer ni mettre en quarantaine ces objets. Si vous le faites, il ne WorkSpace fonctionnera pas correctement.

Si un logiciel antivirus est installé sur le WorkSpace, assurez-vous qu'il n'interfère pas avec les composants de service installés aux emplacements suivants.

- C:\Program Files\Amazon
- C:\Program Files\NICE
- C:\Program Files\Teradici
- C:\Program Files (x86)\Teradici
- C:\ProgramData\Amazon
- C:\ProgramData\NICE
- C:\ProgramData\Teradici

Si un logiciel antivirus est installé sur le WorkSpaces Core, assurez-vous qu'il n'interfère pas avec les composants de service installés aux emplacements suivants.

- C:\Program Files\Amazon
- C : \ ProgramData \ Amazon

Agent PCo IP 32 bits

Le 29 mars 2021, nous avons mis à jour l'agent PCo IP de 32 bits à 64 bits. Pour Windows WorkSpaces utilisant le protocole PCo IP, cela signifie que l'emplacement des fichiers Teradici est passé de à C:\Program Files (x86)\Teradici. C:\Program Files\Teradici Comme nous avons mis à jour les agents PCo IP pendant les périodes de maintenance régulières, certains d'entre vous ont WorkSpaces peut-être utilisé l'agent 32 bits plus longtemps que d'autres pendant la transition.

Si vous avez configuré des règles de pare-feu, des exclusions de logiciels antivirus (côté client et côté hôte), des paramètres d'objet de stratégie de groupe (GPO) ou des paramètres pour SCCM (Microsoft System Center Configuration Manager), Microsoft Endpoint Configuration Manager ou des outils de gestion de configuration similaires basés sur le chemin complet vers l'agent 32 bits, vous devez également ajouter le chemin complet vers l'agent 64 bits à ces paramètres.

Si vous filtrez les chemins d'accès à des composants PCo IP 32 bits, veillez à ajouter les chemins vers les versions 64 bits des composants. Comme vous n'êtes peut-être pas tous mis à jour en même temps, ne remplacez pas le chemin 32 bits par le chemin 64 bits, sinon certains de vos chemins WorkSpaces risquent de ne pas fonctionner. Par exemple, si vous basez vos exclusions ou filtres de communication sur `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe`, vous devez également ajouter `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`. De même, si vous basez vos exclusions ou filtres de communication sur `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe`, vous devez également ajouter `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe`.

PCoModification du service d'arbitre IP — Sachez que le service d'arbitre PCo IP (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) est supprimé lorsque vous WorkSpaces êtes mis à jour pour utiliser l'agent 64 bits.

PCoClients et périphériques USB à IP zéro : à partir de la version 20.10.4 de l'agent PCo IP, Amazon WorkSpaces désactive la redirection USB par défaut via le registre Windows. Ce paramètre de registre affecte le comportement des périphériques USB lorsque vos utilisateurs utilisent des appareils clients PCo IP zéro pour se connecter à leur WorkSpaces. Pour de plus amples informations, veuillez consulter [Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients PCo IP zéro](#).

Composants de service requis pour Linux

Sur Amazon Linux WorkSpaces, les composants du service sont installés aux emplacements suivants. Vous ne devez pas supprimer, modifier, bloquer ni mettre en quarantaine ces objets. Si vous le faites, il ne Workspace fonctionnera pas correctement.

Note

Si vous apportez des modifications à des fichiers autres que celles `/etc/pcoip-agent/pcoip-agent.conf` susceptibles de vous WorkSpaces empêcher de travailler, vous devrez peut-être les reconstruire. Pour plus d'informations sur la modification du fichier `/etc/`

pcoip-agent/pcoip-agent.conf, consultez [Gérez votre Amazon Linux 2 WorkSpaces en mode WorkSpaces personnel](#).

- /etc/dhcp/dhclient.conf
- /etc/logrotate.d/pcoip-agent
- /etc/logrotate.d/pcoip-server
- /etc/os-release
- /etc/pam.d/pcoip
- /etc/pam.d/pcoip-session
- /etc/pcoip-agent
- /etc/profile.d/system-restart-check.sh
- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /etc/systemd/system/euc-analytic-agent.service
- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf

- `/usr/lib/yum-plugins/halt_os_update_check.py`
- `/usr/sbin/pcoip-agent`
- `/usr/sbin/pcoip-register-host`
- `/usr/sbin/pcoip-support-bundler`
- `/usr/share/doc/pcoip-agent`
- `/usr/share/pcoip-agent`
- `/usr/share/selinux/packages/pcoip-agent.pp`
- `/usr/share/X11`
- `/var/crash/pcoip-agent`
- `/var/lib/pcoip-agent`
- `/var/lib/skylight`
- `/var/log/pcoip-agent`
- `/var/log/skylight`
- `/var/logs/wsp`
- `/var/log/eucanalytics`

Composants de service requis pour Ubuntu

Sur Ubuntu WorkSpaces, les composants du service sont installés aux emplacements suivants. Vous ne devez pas supprimer, modifier, bloquer ni mettre en quarantaine ces objets. Si vous le faites, il ne Workspace fonctionnera pas correctement.

- `/etc/X11/default-display-manager`
- `/etc/dcv`
- `/etc/default/grub.d/zz-hibernation.cfg`
- `/etc/netplan`
- `/etc/os-release`
- `/etc/pam.d/dcv`
- `/etc/pam.d/dcv-graphical-sso`
- `/etc/sss/sss.conf`
- `/etc/wsp`

- `/etc/systemd/system/euc-analytic-agent.service`
- `/lib64/security/pam_self.so`
- `/usr/lib/skylight`
- `/usr/lib/systemd/system/dcvserver.service`
- `/usr/lib/systemd/system/dcvsessionlauncher.service`
- `/usr/lib/systemd/system/skylight-agent.service`
- `/usr/lib/systemd/system/wspdcvhostadapter.service`
- `/usr/share/X11`
- `/usr/bin/euc-analytics-agent`
- `/var/lib/skylight`
- `/var/log/skylight`
- `/var/log/eucanalytics`

Composants de service requis pour Rocky Linux

Sur Red Hat Enterprise Linux WorkSpaces, les composants de service sont installés aux emplacements suivants. Vous ne devez pas supprimer, modifier, bloquer ni mettre en quarantaine ces objets. Si vous le faites, il ne WorkSpace fonctionnera pas correctement.

- `/etc/dcv`
- `/etc/os-release`
- `/etc/pam.d/dcv-graphical-sso`
- `/etc/pam.d/dcv`
- `/etc/systemd/system/euc-analytic-agent.service`
- `/etc/wsp`
- `/usr/bin/euc-analytics-agent`
- `/usr/lib/skylight`
- `/usr/lib/systemd/system/dcvserver.service`
- `/usr/lib/systemd/system/dcvsessionlauncher.service`
- `/usr/lib/systemd/system/skylight-agent.service`
- `/usr/lib/systemd/system/wspdcvhostadapter.service`

- `/usr/lib/systemd/system/xdcv-console.path`
- `/usr/lib/systemd/system/xdcv-console.service`
- `/usr/lib/systemd/system/xdcv-console-update.service`
- `/usr/share/X11`
- `/var/lib/skylight`
- `/var/log/eucanalytics`
- `/var/log/skylight`

Composants de service requis pour Red Hat Enterprise Linux

Sur Red Hat Enterprise Linux WorkSpaces, les composants de service sont installés aux emplacements suivants. Vous ne devez pas supprimer, modifier, bloquer ni mettre en quarantaine ces objets. Si vous le faites, il ne Workspace fonctionnera pas correctement.

- `/etc/dcv`
- `/etc/os-release`
- `/etc/pam.d/dcv-graphical-ss0`
- `/etc/pam.d/dcv`
- `/etc/systemd/system/euc-analytic-agent.service`
- `/etc/wsp`
- `/usr/bin/euc-analytics-agent`
- `/usr/lib/skylight`
- `/usr/lib/systemd/system/dcvserver.service`
- `/usr/lib/systemd/system/dcvsessionlauncher.service`
- `/usr/lib/systemd/system/skylight-agent.service`
- `/usr/lib/systemd/system/wspdcvhostadapter.service`
- `/usr/lib/systemd/system/xdcv-console.path`
- `/usr/lib/systemd/system/xdcv-console.service`
- `/usr/lib/systemd/system/xdcv-console-update.service`
- `/usr/share/X11`
- `/var/log/eucanalytics`

- /var/log/skylight

Gérer les annuaires pour WorkSpaces Personal

WorkSpaces utilise un répertoire pour stocker et gérer des informations pour vos WorkSpaces et pour les utilisateurs. Vous pouvez utiliser l'une des options suivantes :

- AD Connector : utilisez votre annuaire Microsoft Active Directory sur site existant. Les utilisateurs peuvent se connecter à leur compte WorkSpaces à l'aide de leurs informations d'identification locales et accéder aux ressources locales depuis leur WorkSpaces
- AWS Managed Microsoft AD — Créez un Microsoft Active Directory hébergé sur AWS.
- Simple AD — Créez un annuaire compatible avec Microsoft Active Directory, alimenté par Samba 4 et hébergé sur AWS.
- Confiance croisée : créez une relation de confiance entre votre AWS Managed Microsoft AD annuaire et votre domaine local.
- Microsoft Entra ID : créez un répertoire qui utilise l'identifiant Microsoft Entra comme source d'identité (via IAM Identity Center). Les membres du personnel du répertoire sont joints WorkSpaces à l'aide de l'authentification native de Microsoft Entra et sont inscrits dans Microsoft Intune via le mode piloté par l'utilisateur de Microsoft Windows Autopilot. Les annuaires utilisant l'identifiant Microsoft Entra ne prennent en charge que les licences Windows 10 et 11 Bring Your Own WorkSpaces.
- Personnalisé : créez un annuaire utilisant le fournisseur d'identité de votre choix (via IAM Identity Center). WorkSpaces dans le répertoire sont gérés à l'aide de la solution de gestion des appareils de votre choix, telle que JumpCloud. Les annuaires utilisant des fournisseurs d'identité personnalisés ne prennent en charge que les licences Windows 10 et 11 Bring Your Own WorkSpaces.

Pour des didacticiels expliquant comment configurer ces répertoires et les lancer WorkSpaces, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

Tip

Pour une exploration détaillée des considérations relatives à la conception des annuaires et du cloud privé virtuel (VPC) pour différents scénarios de déploiement, consultez [Best Practices for Deploying Amazon](#). WorkSpaces

Après avoir créé un annuaire, vous exécuterez la plupart des tâches d'administration d'annuaire avec des outils comme les outils d'administration Active Directory. Vous pouvez effectuer certaines tâches d'administration d'annuaire à l'aide de la WorkSpaces console et d'autres tâches à l'aide de la stratégie de groupe. Pour de plus amples informations sur la gestion des utilisateurs et des groupes, veuillez consulter [Gérer les utilisateurs dans WorkSpaces Personal](#) et [Configuration des outils d'administration Active Directory pour le WorkSpaces personnel](#).

Note

- Les annuaires partagés ne sont actuellement pas compatibles avec Amazon WorkSpaces.
- Si vous configurez votre annuaire Microsoft AD AWS géré pour une réplication multirégionale, seul le répertoire de la région principale peut être enregistré pour être utilisé auprès d'Amazon WorkSpaces. Les tentatives d'enregistrement du répertoire dans une région répliquée pour une utilisation avec Amazon WorkSpaces échoueront. La réplication multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.
- Simple AD et AD Connector sont mis à votre disposition gratuitement WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire Simple AD ou AD Connector pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé auprès d'Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires.AWS Directory Service](#)

Pour supprimer des annuaires vides, consultez [Supprimer un répertoire pour WorkSpaces Personal](#). Si vous supprimez votre répertoire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à l'utiliser WorkSpaces .

Table des matières

- [Enregistrer un Directory Service répertoire existant avec WorkSpaces Personal](#)
- [Sélectionnez une unité organisationnelle pour WorkSpaces Personnel](#)
- [Configuration des adresses IP publiques automatiques pour WorkSpaces Personal](#)
- [Contrôlez l'accès aux appareils pour WorkSpaces Personal](#)
- [Gérer les autorisations d'administrateur local pour WorkSpaces Personal](#)
- [Mettre à jour le compte AD Connector \(AD Connector\) pour WorkSpaces Personal](#)

- [Authentification multifactorielle \(AD Connector\) pour les particuliers WorkSpaces](#)
- [Création d'un répertoire pour WorkSpaces Personal](#)
- [Mettre à jour les serveurs DNS pour WorkSpaces Personal](#)
- [Supprimer un répertoire pour WorkSpaces Personal](#)
- [Configuration des outils d'administration Active Directory pour le WorkSpaces personnel](#)

Enregistrer un Directory Service répertoire existant avec WorkSpaces Personal

WorkSpaces Pour autoriser l'utilisation d'un Directory Service répertoire existant, vous devez l'enregistrer auprès de WorkSpaces. Après avoir enregistré un répertoire, vous pouvez WorkSpaces le lancer.

Exigences : pour enregistrer un répertoire à utiliser avec WorkSpaces, il doit répondre aux exigences suivantes :

- Si vous utilisez AWS Managed Microsoft AD Simple AD, votre répertoire peut se trouver dans un sous-réseau privé dédié, à condition qu'il ait accès au VPC où il se trouve WorkSpaces .
- Pour plus d'informations sur la conception d'annuaires et de VPC, consultez le livre blanc [Best Practices for Deploying Amazon WorkSpaces](#).

Note

Simple AD et AD Connector sont mis à votre disposition gratuitement WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire Simple AD ou AD Connector pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé auprès d'Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires.AWS Directory Service](#)

Pour supprimer des annuaires vides, consultez [Supprimer un répertoire pour WorkSpaces Personal](#). Si vous supprimez votre répertoire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à l'utiliser WorkSpaces .

Pour enregistrer un annuaire du AWS Directory Service existant

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez Créer un annuaire.
4. Sur la page Créer un répertoire, pour le WorkSpaces type, choisissez Personnel. Pour la gestion des WorkSpace appareils, choisissez AWS Directory Service.
5. Sélectionnez le répertoire que vous souhaitez enregistrer dans le tableau Répertoires dans le Directory Service tableau
6. Sélectionnez deux sous-réseaux de votre VPC qui ne sont pas issus de la même zone de disponibilité. Ces sous-réseaux seront utilisés pour lancer votre WorkSpaces. Pour de plus amples informations, veuillez consulter [Zones de disponibilité pour le WorkSpaces personnel](#).

 Note

Si vous ne savez pas quels sous-réseaux choisir, sélectionnez Aucune préférence.

7. Pour Activer les autorisations en libre-service, choisissez Oui pour permettre à vos utilisateurs de reconstruire leurs autorisations WorkSpaces, de modifier la taille du volume, le type de calcul et le mode d'exécution. L'activation peut avoir un impact sur le montant que vous payez pour Amazon WorkSpaces. Sinon, choisissez No (Non).
8. Choisissez S'inscrire. Initialement la valeur de Membre est REGISTERING. Une fois l'enregistrement terminé, la valeur est Yes.

Après avoir enregistré le Directory Service répertoire, vous pouvez créer un répertoire personnel WorkSpace. Pour de plus amples informations, veuillez consulter [Créez un WorkSpace in WorkSpaces Personal](#).

Lorsque vous avez fini d'utiliser le répertoire avec WorkSpaces, vous pouvez le désenregistrer. Notez que vous devez annuler l'enregistrement d'un annuaire avant de pouvoir le supprimer. Si vous souhaitez désenregistrer et supprimer un répertoire, vous devez d'abord rechercher et supprimer l'ensemble des applications et des services qui sont enregistrés dans le répertoire. Pour plus d'informations, consultez [Supprimer votre annuaire](#) dans le Guide d'administration AWS Directory Service .

Pour annuler l'enregistrement d'un annuaire

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).

3. Sélectionnez l'annuaire.
4. Choisissez Actions, Deregister (Annuler l'enregistrement).
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Confirmer. Une fois la désinscription terminée, le répertoire n'est plus enregistré et est supprimé de la liste.

Sélectionnez une unité organisationnelle pour WorkSpaces Personnel

Note

Cette fonctionnalité n'est disponible que pour les annuaires gérés via AWS Directory Service, notamment AD Connector, AWS Managed Microsoft AD et Simple AD.

WorkSpace les comptes de machine sont placés dans l'unité organisationnelle (UO) par défaut du WorkSpaces répertoire. Initialement, les comptes de machine sont placés dans l'unité d'organisation des ordinateurs de votre annuaire ou l'annuaire auquel votre connecteur AD est connecté. Vous pouvez sélectionner une autre unité d'organisation à partir de votre annuaire ou annuaire connecté, ou spécifier une unité d'organisation dans un autre domaine cible. Notez que vous ne pouvez sélectionner qu'une seule unité d'organisation par annuaire.

Une fois que vous avez sélectionné une nouvelle unité d'organisation, les comptes de machines WorkSpaces correspondant à toutes les unités créées ou reconstruites sont placés dans l'unité d'organisation nouvellement sélectionnée.

Pour sélectionner une unité d'organisation

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez votre répertoire.
4. Sous Domaine cible et unité organisationnelle, choisissez Modifier.
5. Pour trouver une unité d'organisation, sous Cible et unité organisationnelle, vous pouvez commencer à saisir tout ou partie du nom de l'unité organisationnelle et choisir l'unité d'organisation que vous souhaitez utiliser.
6. (Facultatif) Choisissez un nom distinctif d'unité d'organisation pour remplacer l'unité d'organisation sélectionnée par une unité d'organisation personnalisée.

7. Choisissez Enregistrer.
8. (Facultatif) Reconstruisez l'existant WorkSpaces pour mettre à jour l'unité d'organisation. Pour de plus amples informations, veuillez consulter [Reconstituer un Workspace in WorkSpaces Personal](#).

Configuration des adresses IP publiques automatiques pour WorkSpaces Personal

Une fois que vous avez activé l'attribution automatique des adresses IP publiques, chaque adresse IP publique WorkSpace que vous lancez se voit attribuer une adresse IP publique issue du pool d'adresses publiques fourni par Amazon. Un Workspace sous-réseau public peut accéder à Internet via la passerelle Internet s'il possède une adresse IP publique. WorkSpaces qui existaient déjà avant que vous n'activiez l'attribution automatique ne reçoivent pas d'adresses publiques tant que vous ne les avez pas reconstruites.

Notez qu'il n'est pas nécessaire d'activer l'attribution automatique des adresses publiques si vous WorkSpaces utilisez des sous-réseaux privés et que vous avez configuré une passerelle NAT pour le cloud privé virtuel (VPC), ou si WorkSpaces vous vous trouvez dans des sous-réseaux publics et que vous leur avez attribué des adresses IP élastiques. Pour de plus amples informations, veuillez consulter [Configuration d'un VPC pour le personnel WorkSpaces](#).

Warning

Si vous associez une adresse IP élastique que vous possédez à un Workspace, puis que vous dissociez ensuite cette adresse IP élastique du Workspace, celui-ci Workspace perd son adresse IP publique et n'en obtient pas automatiquement une nouvelle dans le pool fourni par Amazon. Pour associer une nouvelle adresse IP publique provenant du pool fourni par Amazon au Workspace, vous devez [reconstituer](#) le Workspace. Si vous ne souhaitez pas reconstruire le Workspace, vous devez associer une autre adresse IP élastique que vous possédez au Workspace.

Pour configurer des adresses IP Elastic

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez le répertoire correspondant à votre WorkSpaces.

4. Choisissez Actions, Mettre à jour les détails.
5. Développez Accès à Internet et sélectionnez Activer ou Désactiver.
6. Choisissez Mettre à jour.

Contrôlez l'accès aux appareils pour WorkSpaces Personal

Vous pouvez spécifier les types d'appareils auxquels vous avez accès en WorkSpaces fonction de la plate-forme de l'appareil. Vous pouvez utiliser des certificats pour restreindre l' WorkSpaces accès aux appareils fiables (également appelés appareils administrés).

Pour contrôler l'accès des appareils à WorkSpaces

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez votre répertoire.
4. Sous Options de contrôle d'accès, choisissez Modifier.
5. Sous Appareils fiables, spécifiez les types d'appareils autorisés à accéder en WorkSpaces sélectionnant Autoriser tout, Appareils fiables ou Refuser tout. Pour de plus amples informations, veuillez consulter [Restreindre l'accès aux appareils fiables pour les WorkSpaces particuliers](#).
6. Choisissez Enregistrer.

Gérer les autorisations d'administrateur local pour WorkSpaces Personal

Note

Cette fonctionnalité n'est disponible que pour les annuaires gérés via AWS Directory Service, notamment AD Connector, AWS Managed Microsoft AD et Simple AD.

Vous pouvez spécifier si les utilisateurs sont des administrateurs locaux sur leur compte WorkSpaces, ce qui leur permet d'installer l'application et de modifier les paramètres de leur WorkSpaces. Les utilisateurs sont les administrateurs locaux par défaut. Si vous modifiez ce paramètre, la modification s'applique à toutes les nouvelles WorkSpaces créations et à toutes celles WorkSpaces que vous reconstruisez.

Pour modifier les autorisations d'administrateur local

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez votre répertoire.
4. Sous Paramètres de l'administrateur local, choisissez Modifier.
5. Pour vous assurer que les utilisateurs sont des administrateurs locaux, choisissez Activer le paramètre d'administrateur local.
6. Choisissez Enregistrer.

Mettre à jour le compte AD Connector (AD Connector) pour WorkSpaces Personal

Vous pouvez mettre à jour le compte AD Connector qui est utilisé pour lire les utilisateurs et les groupes et pour joindre des comptes de WorkSpaces machines à votre répertoire AD Connector.

Pour mettre à jour le compte du connecteur AD

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez votre répertoire, puis choisissez Afficher les détails.
4. Sous Compte du connecteur AD, choisissez Modifier.
5. Entrez les informations d'identification de connexion du nouveau compte.
6. Choisissez Enregistrer.

Authentification multifactorielle (AD Connector) pour les particuliers WorkSpaces

Vous pouvez activer l'authentification multifactorielle (MFA) pour l'annuaire AD Connector. Pour plus d'informations sur l'utilisation de l'authentification multifactorielle avec AWS Directory Service, consultez [Activer l'authentification multifactorielle pour les prérequis d'AD Connector](#) et d'[AD Connector](#).

 Note

- Votre serveur RADIUS peut être hébergé par AWS ou sur site.
- Les noms d'utilisateur doivent correspondre entre Active Directory et le serveur RADIUS.

Pour activer l'authentification multifactorielle

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez votre annuaire et choisissez Actions, Mettre à jour les détails.
4. Développez Authentification multi-facteurs et sélectionnez Activer l'authentification multi-facteurs.
5. Pour Adresse(s) IP du serveur RADIUS, saisissez l'adresse IP des points de terminaison de votre serveur RADIUS séparée par des virgules ou saisissez l'adresse IP de l'équilibreur de charge de votre serveur RADIUS.
6. Pour Port, saisissez le port que votre serveur RADIUS utilise pour les communications. Le réseau sur site doit autoriser le trafic entrant via le port du serveur RADIUS par défaut (UDP : 1812) depuis AD Connector.
7. Pour Code secret partagé et Confirmer le code secret partagé, saisissez le code secret partagé de votre serveur RADIUS.
8. Pour Protocole, choisissez le protocole de votre serveur RADIUS.
9. Pour Délai d'attente du serveur, saisissez le délai d'attente, en secondes, pour que le serveur RADIUS réponde. La valeur doit être comprise entre 1 et 50.
10. Pour Nombre maximum de nouvelles tentatives, saisissez le nombre de tentatives pour communiquer avec le serveur RADIUS. La valeur doit être comprise entre 0 et 10.
11. Choisissez Update and Exit (Mettre à jour et quitter).

L'authentification multifactorielle est disponible lorsque le paramètre Statut RADIUS est Activé. Pendant la configuration de l'authentification multifactorielle, les utilisateurs ne peuvent pas se connecter à leur WorkSpaces.

Création d'un répertoire pour WorkSpaces Personal

WorkSpaces Personal vous permet d'utiliser des annuaires gérés Directory Service pour stocker et gérer des informations pour vous WorkSpaces et pour les utilisateurs. Utilisez les options suivantes pour créer un répertoire WorkSpaces personnel :

- Créer un annuaire Simple AD.
- Créez un service d' AWS annuaire pour Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD.
- Connectez-vous à un annuaire Microsoft Active Directory existant à l'aide d'Active Directory Connector.
- Créez une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site.
- Créez un WorkSpaces répertoire d'identifiants Microsoft Entra dédié.
- Créez un WorkSpaces répertoire personnalisé dédié.

Note

- Les annuaires partagés ne sont actuellement pas pris en charge pour une utilisation avec Amazon WorkSpaces.
- Si vous configurez votre annuaire Microsoft AD AWS géré pour une réplication multirégionale, seul le répertoire de la région principale peut être enregistré pour être utilisé auprès d'Amazon WorkSpaces. Les tentatives d'enregistrement du répertoire dans une région répliquée pour une utilisation avec Amazon WorkSpaces échoueront. La réplication multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.
- Simple AD et AD Connector sont mis à votre disposition gratuitement WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire Simple AD ou AD Connector pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé auprès d'Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires.AWS Directory Service](#)

Avant de créer un répertoire

- WorkSpaces n'est pas disponible dans toutes les régions. Vérifiez les régions prises en charge et sélectionnez une région pour votre WorkSpaces. Pour plus d'informations sur les régions prises en charge, consultez la section [WorkSpaces Tarification par AWS région](#).
- Créez un Virtual Private Cloud avec au moins deux sous-réseaux privés. Pour de plus amples informations, veuillez consulter [Configuration d'un VPC pour le personnel WorkSpaces](#). Le VPC doit être connecté à votre réseau sur site via une connexion réseau privé virtuel (VPN) ou Direct Connect. Pour plus d'informations, consultez [Conditions préalables requises pour AD Connector](#) dans le Guide d'administration AWS Directory Service .
- Fournir un accès à Internet à partir du Workspace. Pour de plus amples informations, veuillez consulter [Fournir un accès à Internet pour les WorkSpaces particuliers](#).

Pour plus d'informations sur la suppression d'un répertoire vide, consultez [Supprimer un répertoire pour WorkSpaces Personal](#). Si vous supprimez votre répertoire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à l'utiliser WorkSpaces .

Table des matières

- [Identifiez le nom de l'ordinateur pour votre répertoire WorkSpaces personnel](#)
- [Création d'un répertoire Microsoft AD AWS géré pour WorkSpaces Personal](#)
- [Création d'un annuaire Simple AD pour WorkSpaces Personal](#)
- [Création d'un AD Connector pour les WorkSpaces particuliers](#)
- [Créez une relation de confiance entre votre annuaire Microsoft AD AWS géré et votre domaine local pour Personal WorkSpaces](#)
- [Créez un répertoire Microsoft Entra ID dédié avec WorkSpaces Personal](#)
- [Créez un répertoire personnalisé dédié avec WorkSpaces Personal](#)

Identifiez le nom de l'ordinateur pour votre répertoire WorkSpaces personnel

La valeur du nom de l'ordinateur affichée pour un Workspace dans la WorkSpaces console Amazon varie en fonction du type d'ordinateur que Workspace vous avez lancé (Amazon Linux, Ubuntu ou Windows). Le nom d'ordinateur d'un Workspace peut être dans l'un des formats suivants :

- Amazon Linux : A- **xxxxxxxxxxxxxx**
- Red Hat Enterprise Linux : R- **xxxxxxxxxxxxxx**

- Rocky Linux : R- **xxxxxxxxxxxxxx**
- Ubuntu : U- **xxxxxxxxxxxxxx**
- Windows : IP-C **xxxxxx** ou WSAMZN- ou AMAZ- **xxxxxx** EC2 **xxxxxx**

Pour Windows WorkSpaces, le format du nom de l'ordinateur est déterminé par le type de bundle, et dans le cas d'un bundle WorkSpaces créé à partir de bundles publics ou à partir de bundles personnalisés basés sur des images publiques, par le moment où les images publiques ont été créées.

À compter du 22 juin 2020, les noms d'ordinateurs Windows WorkSpaces lancés à partir de bundles publics utilisent le **xxxxxx** format WSAMZN- au lieu du format IP-C. **xxxxxx**

Pour les ensembles personnalisés basés sur une image publique, si l'image publique a été créée avant le 22 juin 2020, les noms des ordinateurs sont au format EC2 AMAZ-**xxxxxx**. Si l'image publique a été créée le 22 juin 2020 ou après cette date, les noms des ordinateurs sont au format WSAMZN-**xxxxxx**.

Pour les bundles Bring Your Own License (BYOL), le **xxxxxx** format DESKTOP **xxxxxx** ou EC2 AMAZ- est utilisé par défaut pour les noms d'ordinateurs.

Si vous avez spécifié un format personnalisé pour les noms d'ordinateur dans vos offres groupées personnalisées ou BYOL, votre format personnalisé remplace ces valeurs par défaut. Pour définir un format personnalisé, consultez [Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal](#).

Important

Après avoir créé WorkSpace un, vous pouvez modifier son nom d'ordinateur en toute sécurité. Par exemple, vous pouvez exécuter un PowerShell script avec la commande `Rename-Computer` sur votre ordinateur WorkSpace ou à distance. La valeur du nom d'ordinateur mise à jour sera ensuite affichée pour la WorkSpace dans la WorkSpaces console Amazon.

Création d'un répertoire Microsoft AD AWS géré pour WorkSpaces Personal

Dans ce didacticiel, nous créons un répertoire Microsoft AD AWS géré. Pour des didacticiels qui utilisent les autres options, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

Créez d'abord un répertoire Microsoft AD AWS géré. Directory Service crée deux serveurs d'annuaire, un dans chacun des sous-réseaux privés de votre VPC. Notez qu'aucun utilisateur ne se trouve initialement dans l'annuaire. Vous ajouterez un utilisateur à l'étape suivante lorsque vous lancerez le WorkSpace.

 Note

- Les annuaires partagés ne sont actuellement pas pris en charge pour une utilisation avec Amazon WorkSpaces.
- Si votre annuaire Microsoft AD AWS géré a été configuré pour une réplification multirégionale, seul le répertoire de la région principale peut être enregistré pour être utilisé auprès d'Amazon WorkSpaces. Les tentatives d'enregistrement du répertoire dans une région répliquée pour une utilisation avec Amazon WorkSpaces échoueront. La réplification multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.

Pour créer un annuaire Microsoft AD AWS géré

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez Créer un annuaire.
4. Sur la page Créer un répertoire, pour le WorkSpaces type, choisissez Personnel. Ensuite, pour la gestion des WorkSpace appareils, choisissez AWS Directory Service.
5. Choisissez Create directory, qui ouvre la page Configurer un annuaire sur le AWS Directory Service.
6. Choisissez AWS Managed Microsoft AD, puis Next.
7. Configurez l'annuaire comme suit :
 - a. Dans Nom de l'organisation, entrez un nom d'organisation unique pour votre annuaire (par exemple, my-demo-directory). Ce nom doit comporter au moins quatre caractères, uniquement des caractères alphanumériques et des tirets (-), et commencer ou se terminer par un caractère autre qu'un trait d'union.
 - b. Pour Directory DNS (DNS de l'annuaire), saisissez le nom complet de l'annuaire (par exemple, workspaces.demo.com).

 Important

Si vous devez mettre à jour votre serveur DNS après le lancement de votre WorkSpaces, suivez la procédure [Mettre à jour les serveurs DNS pour WorkSpaces Personal](#) pour vous assurer que WorkSpaces vous êtes correctement mis à jour.

- c. Pour NetBIOS name (Nom NetBIOS), saisissez le nom abrégé de l'annuaire (par exemple, workspaces).
 - d. Pour Admin password (Mot de passe administrateur) et Confirm password (Confirmer le mot de passe), saisissez le mot de passe du compte administrateur de l'annuaire. Pour plus d'informations sur les exigences relatives aux mots de passe, voir [Créer votre répertoire Microsoft AD AWS géré](#) dans le Guide d'AWS Directory Service administration.
 - e. (Facultatif) Dans le champ Description, saisissez une description pour la stratégie.
 - f. Pour VPC, sélectionnez le VPC que vous avez créé.
 - g. Pour Sous-réseaux (subnets), sélectionnez les deux sous-réseaux privés (avec les blocs d'adresse CIDR 10.0.1.0/24 et 10.0.2.0/24).
 - h. Choisissez Étape suivante.
8. Choisissez Créer un annuaire.
 9. Vous serez redirigé vers la page Créer un répertoire sur la WorkSpaces console. Le statut initial de l'annuaire est Requested et ensuite Creating. Une fois l'annuaire créé (cela peut prendre quelques minutes), son statut passe à Active.

Après avoir créé un répertoire Microsoft AD AWS géré, vous pouvez l'enregistrer auprès d'Amazon WorkSpaces. Pour de plus amples informations, veuillez consulter [Enregistrer un Directory Service répertoire existant avec WorkSpaces Personal](#).

Création d'un annuaire Simple AD pour WorkSpaces Personal

Dans ce didacticiel, nous lançons un Workspace logiciel qui utilise Simple AD. Pour des didacticiels qui utilisent les autres options, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

 Note

- Simple AD n'est pas disponible dans toutes les AWS régions. Vérifiez celles prises en charge et [sélectionnez une région](#) pour l'annuaire Simple AD. Pour plus d'informations sur

les régions prises en charge pour Simple AD, consultez [la section Disponibilité des régions pour AWS Directory Service](#).

- Simple AD est mis à votre disposition gratuitement pour une utilisation avec WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire Simple AD pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé auprès d'Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires. AWS Directory Service](#)
- [Simple AD](#) ne prend actuellement en charge que l' IPv4 adressage, ce qui signifie que lors de la création d'un annuaire, le VPC associé sera configuré avec un bloc IPv4 CIDR et ne prend pas en charge les réseaux. IPv6

Lorsque vous créez un annuaire Simple AD. Directory Service crée deux serveurs d'annuaire, un dans chacun des sous-réseaux privés de votre VPC. Au départ, il n'y a aucun utilisateur dans le répertoire. Ajoutez un utilisateur après avoir créé le Workspace. Pour de plus amples informations, consultez [Créez un Workspace in WorkSpaces Personal](#).

Pour créer un annuaire Simple AD

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez Créer un annuaire.
4. Sur la page Créer un répertoire, pour le WorkSpaces type, choisissez Personnel. Ensuite, pour la gestion des Workspace appareils, choisissez AWS Directory Service.
5. Choisissez Create directory, qui ouvre la page Configurer un annuaire sur le AWS Directory Service
6. Choisissez Simple AD, puis Next.
7. Configurez l'annuaire comme suit :
 - a. Dans Nom de l'organisation, entrez un nom d'organisation unique pour votre annuaire (par exemple, my-example-directory). Ce nom doit comporter au moins quatre caractères, uniquement des caractères alphanumériques et des tirets (-), et commencer ou se terminer par un caractère autre qu'un trait d'union.
 - b. Pour DNS du répertoire, saisissez le nom complet de l'annuaire (par exemple, exemple.com).

⚠ Important

Si vous devez mettre à jour votre serveur DNS après le lancement de votre WorkSpaces, suivez la procédure [Mettre à jour les serveurs DNS pour WorkSpaces Personal](#) pour vous assurer que WorkSpaces vous êtes correctement mis à jour.

- c. Par NetBIOS name (Nom NetBIOS), saisissez le nom abrégé de l'annuaire (par exemple, exemple).
 - d. Pour Admin password (Mot de passe administrateur) et Confirm password (Confirmer le mot de passe), saisissez le mot de passe du compte administrateur de l'annuaire. Pour plus d'informations sur les exigences liées au mot de passe, consultez [Création de votre annuaire Microsoft AD](#) dans le Guide d'administration AWS Directory Service.
 - e. (Facultatif) Dans le champ Description, saisissez une description pour la stratégie.
 - f. Pour Taille du répertoire, choisissez Petite.
 - g. Pour VPC, sélectionnez le VPC que vous avez créé.
 - h. Pour Sous-réseaux (subnets), sélectionnez les deux sous-réseaux privés (avec les blocs d'adresse CIDR 10.0.1.0/24 et 10.0.2.0/24).
 - i. Choisissez Suivant.
8. Choisissez Créer un annuaire.
 9. Vous serez redirigé vers la page Créer un répertoire sur la WorkSpaces console. Le statut initial de l'annuaire est Requested et ensuite Creating. Une fois l'annuaire créé (cela peut prendre quelques minutes), son statut passe à Active.

Que se passe-t-il durant la création d'un annuaire ?

WorkSpaces exécute les tâches suivantes en votre nom :

- Crée un rôle IAM pour permettre au WorkSpaces service de créer des interfaces réseau élastiques et de répertorier vos WorkSpaces annuaires. Ce rôle est nommé `workspaces_DefaultRole`.
- Configure un annuaire Simple AD dans le VPC qui est utilisé pour stocker les utilisateurs et WorkSpace les informations. L'annuaire possède un compte administrateur avec le nom d'utilisateur Administrateur et le mot de passe spécifié.
- Crée deux groupes de sécurité, l'un pour les contrôleurs de répertoire et WorkSpaces l'autre pour le répertoire.

Après avoir créé un annuaire Simple AD, vous pouvez l'enregistrer auprès d'Amazon WorkSpaces. Pour de plus amples informations, veuillez consulter [Enregistrer un Directory Service répertoire existant avec WorkSpaces Personal](#).

Création d'un AD Connector pour les WorkSpaces particuliers

Dans ce didacticiel, nous allons créer un AD Connector. Pour des didacticiels qui utilisent les autres options, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

Création d'un AD Connector

Note

AD Connector est mis à votre disposition gratuitement pour une utilisation avec WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire AD Connector pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé par Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires.AWS Directory Service](#)

Pour supprimer des annuaires vides, consultez [Supprimer un répertoire pour WorkSpaces Personal](#). Si vous supprimez votre répertoire AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à l'utiliser WorkSpaces .

Pour créer un connecteur AD

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez Créer un annuaire.
4. Sur la page Créer un répertoire, pour le WorkSpaces type, choisissez Personnel. Ensuite, pour la gestion des WorkSpace appareils, choisissez AWS Directory Service.
5. Choisissez Create directory, qui ouvre la page Configurer un annuaire sur le AWS Directory Service
6. Choisissez AWS Managed Microsoft AD, puis Next.
7. Dans Nom de l'organisation, entrez un nom d'organisation unique pour votre annuaire (par exemple, my-example-directory). Ce nom doit comporter au moins quatre caractères, uniquement des caractères alphanumériques et des tirets (-), et commencer ou se terminer par un caractère autre qu'un trait d'union.

8. Pour Connected directory DNS (DNS de l'annuaire connecté), saisissez le nom complet de votre annuaire sur site (par exemple, exemple.com).
9. Pour Connected directory NetBIOS name (Nom NetBIOS de l'annuaire connecté), saisissez le nom abrégé de votre annuaire sur site (par exemple, exemple).
10. Pour Connector account username (Nom d'utilisateur du compte de connecteur), saisissez le nom d'utilisateur d'un utilisateur de votre annuaire sur site. L'utilisateur doit disposer des autorisations pour lire des utilisateurs et des groupes, créer des objets informatiques et lier des ordinateurs au domaine.
11. Pour Mot de passe du compte du connecteur et Confirmer le mot de passe, saisissez le mot de passe du compte d'utilisateur sur site.
12. Pour DNS address (Adresse DNS), saisissez l'adresse IP d'au moins un serveur DNS de votre annuaire sur site.

 Important

Si vous devez mettre à jour l'adresse IP de votre serveur DNS après avoir lancé votre WorkSpaces, suivez la procédure [Mettre à jour les serveurs DNS pour WorkSpaces Personal](#) pour vous assurer que WorkSpaces vous êtes correctement mis à jour.

13. (Facultatif) Dans le champ Description, saisissez une description pour la stratégie.
14. Conservez la Taille sur Petit.
15. Pour VPC, sélectionnez votre VPC.
16. Pour Sous-réseaux (subnets), sélectionnez vos sous-réseaux. Les serveurs DNS spécifiés doivent être accessibles à partir de chaque sous-réseau.
17. Choisissez Créer un annuaire.
18. Vous serez redirigé vers la page Créer un répertoire sur la WorkSpaces console. Le statut initial de l'annuaire est Requested et ensuite Creating. Une fois l'annuaire créé (cela peut prendre quelques minutes), son statut passe à Active.

Créez une relation de confiance entre votre annuaire Microsoft AD AWS géré et votre domaine local pour Personal WorkSpaces

Dans ce didacticiel, nous créons une relation de confiance entre votre annuaire Microsoft AD AWS géré et votre domaine local. Pour des didacticiels qui utilisent les autres options, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

 Note

Le lancement WorkSpaces Comptes AWS dans un domaine sécurisé distinct fonctionne avec AWS Managed Microsoft AD lorsqu'il est configuré avec une relation d'approbation avec votre annuaire local. Cependant, WorkSpaces l'utilisation de Simple AD ou d'AD Connector ne peut pas être lancée WorkSpaces pour les utilisateurs d'un domaine approuvé.

Pour configurer la relation d'approbation

1. Configurez AWS Managed Microsoft AD dans votre cloud privé virtuel (VPC). Pour plus d'informations, voir [Créer votre répertoire Microsoft AD AWS géré](#) dans le Guide AWS Directory Service d'administration.

 Note

- Les annuaires partagés ne sont actuellement pas pris en charge pour une utilisation avec Amazon WorkSpaces.
- Si votre annuaire Microsoft AD AWS géré a été configuré pour une réplification multirégionale, seul le répertoire de la région principale peut être enregistré pour être utilisé auprès d'Amazon WorkSpaces. Les tentatives d'enregistrement du répertoire dans une région répliquée pour une utilisation avec Amazon WorkSpaces échoueront. La réplification multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.

2. Créez une relation de confiance entre votre AWS Managed Microsoft AD et votre domaine local. Prenez soin de configurer la relation d'approbation en tant que relation d'approbation bidirectionnelle. Pour plus d'informations, voir [Tutoriel : Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre domaine local](#) dans le Guide d'AWS Directory Service administration.

Une confiance unidirectionnelle ou bidirectionnelle peut être utilisée pour gérer et authentifier des utilisateurs et des groupes sur site WorkSpaces, et pour qu'elle WorkSpaces puisse être mise à disposition des utilisateurs et des groupes sur site. Pour plus d'informations, consultez [Déployer Amazon WorkSpaces à l'aide d'un domaine de ressources de confiance unidirectionnel avec AWS Directory Service](#).

 Note

- Red Hat Enterprise Linux, Rocky Linux et Ubuntu WorkSpaces utilisent le System Security Services Daemon (SSSD) pour l'intégration d'Active Directory, et SSSD ne prend pas en charge la confiance dans les forêts. Configurez plutôt une relation d'approbation externe. La confiance bidirectionnelle est recommandée pour Amazon Linux, Ubuntu, Rocky Linux et Red Hat Enterprise Linux. WorkSpaces
- Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter à Linux WorkSpaces.

Créez un répertoire Microsoft Entra ID dédié avec WorkSpaces Personal

Dans ce didacticiel, nous créons des licences personnelles Bring Your Own License (BYOL) pour Windows 10 et 11 WorkSpaces auxquelles un identifiant Microsoft Entra est joint et inscrit à Microsoft Intune. Avant de créer un tel répertoire WorkSpaces, vous devez d'abord créer un répertoire WorkSpaces personnel dédié pour Entra ID-joined WorkSpaces.

 Note

Microsoft Entra join personal WorkSpaces est disponible dans toutes les AWS régions où Amazon WorkSpaces est proposé, à l'exception de l'Afrique (Le Cap), d'Israël (Tel Aviv) et de la Chine (Ningxia).

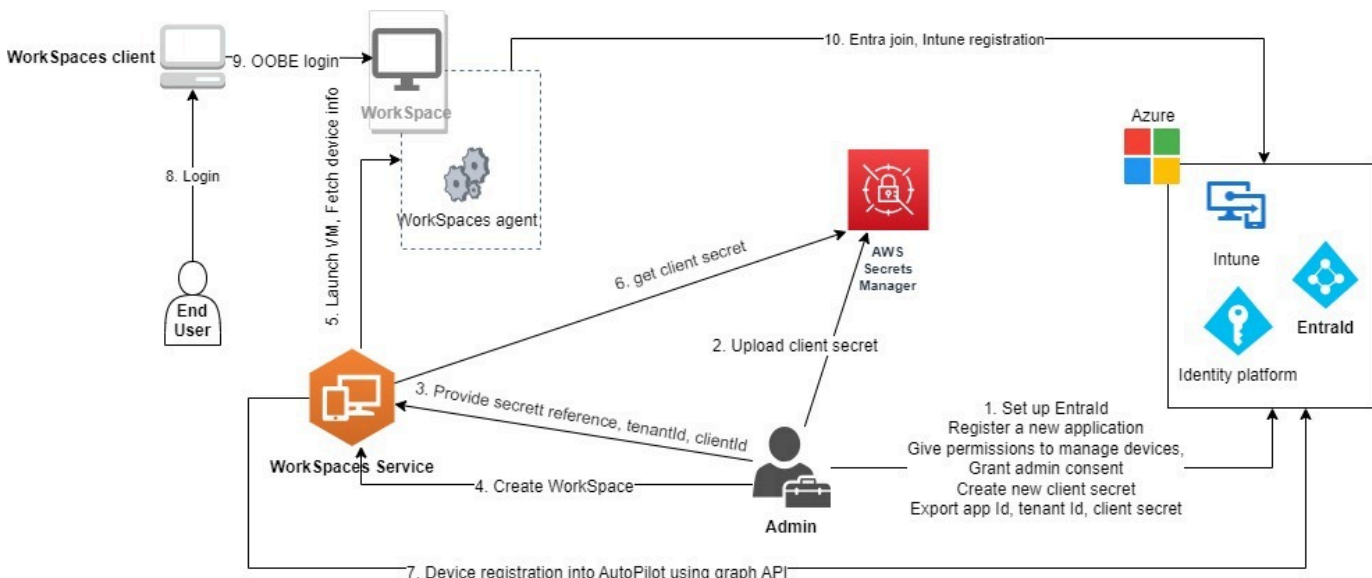
Table des matières

- [Présentation de](#)
- [Exigences et limitations](#)
- [Étape 1 : activer IAM Identity Center et synchroniser avec Microsoft Entra ID](#)
- [Étape 2 : enregistrer une application Microsoft Entra ID pour accorder des autorisations pour Windows Autopilot](#)
- [Étape 3 : configurer le mode piloté par l'utilisateur de Windows Autopilot](#)
- [Étape 4 : Création d'un AWS Secrets Manager secret](#)
- [Étape 5 : Création d'un WorkSpaces répertoire d'identifiants Microsoft Entra dédié](#)

- [Configuration de l'application IAM Identity Center pour un WorkSpaces annuaire \(facultatif\)](#)
- [Création d'une intégration entre régions du centre d'identité IAM \(facultatif\)](#)

Présentation de

Un WorkSpaces répertoire personnel Microsoft Entra ID contient toutes les informations nécessaires au lancement de Microsoft Entra ID joint WorkSpaces qui sont attribuées à vos utilisateurs gérés avec un identifiant Microsoft Entra. Les informations sur les utilisateurs sont mises à disposition WorkSpaces via AWS IAM Identity Center, qui agit en tant que courtier d'identité pour transférer l'identité de votre personnel d'Entra ID à AWS. Le mode piloté par l'utilisateur de Microsoft Windows Autopilot est utilisé pour effectuer l'inscription dans WorkSpaces Intune et l'adhésion à Entra. Le schéma suivant illustre le processus du pilote automatique.



Exigences et limitations

- Forfait Microsoft Entra ID P1 ou supérieur.
 - Microsoft Entra ID et Intune sont activés et comportent des attributions de rôles.
 - Administrateur Intune - Nécessaire pour gérer les profils de déploiement du pilote automatique.
 - Administrateur global : obligatoire pour accorder le consentement de l'administrateur aux autorisations d'API attribuées à l'application créée à l'[étape 3](#). L'application peut être créée sans cette autorisation. Cependant, un administrateur global devra fournir le consentement de l'administrateur sur les autorisations de l'application.
 - Attribuez des licences d'abonnement utilisateur Windows 10/11 VDA E3 ou E5 à vos utilisateurs.
- WorkSpaces

- Les répertoires Entra ID ne prennent en charge que Windows 10 ou 11 Bring Your Own License personal WorkSpaces. Les versions prises en charge sont les suivantes.
 - Windows 10 version 21H2 (mise à jour de décembre 2021)
 - Windows 10 version 22H2 (mise à jour de novembre 2022)
 - Windows 11 Entreprise 23H2 (version d'octobre 2023)
 - Windows 11 Enterprise 22H2 (version d'octobre 2022)
 - Windows 11 Enterprise 24H2 (version d'octobre 2024)
 - Windows 11 Enterprise 25H2 (version de septembre 2025)
- La licence BYOL (Bring Your Own License) est activée pour votre AWS compte et vous avez importé une image BYOL Windows 10 ou 11 valide dans votre compte. Pour de plus amples informations, veuillez consulter [Apportez vos propres licences de bureau Windows WorkSpaces](#).
- Les répertoires Microsoft Entra ID ne prennent en charge que Windows 10 ou 11 BYOL personal WorkSpaces.
- Les annuaires Microsoft Entra ID ne prennent en charge que le protocole DCV.
- Si vous utilisez un pare-feu pour votre WorkSpaces, assurez-vous qu'il ne bloque pas le trafic sortant vers les points de terminaison pour Microsoft Intune et Windows Autopilot. Consultez les exigences relatives aux [points de terminaison réseau pour Microsoft Intune - Microsoft Intune](#) et [Windows Autopilot](#) pour plus de détails.
- Les annuaires Microsoft Entra ID ne prennent pas en charge les clients Microsoft Entra ID dans les environnements Government Community Cloud High (GCCH) et Department of Defense (DoD).

Étape 1 : activer IAM Identity Center et synchroniser avec Microsoft Entra ID

Pour créer des informations personnelles associées à un identifiant Microsoft Entra WorkSpaces et les attribuer aux utilisateurs de votre identifiant Entra, vous devez mettre les informations utilisateur à disposition AWS via IAM Identity Center. IAM Identity Center est le AWS service recommandé pour gérer l'accès des utilisateurs aux AWS ressources. Pour plus d'informations, consultez [Qu'est-ce qu'IAM Identity Center ?](#) . Il s'agit d'une configuration unique.

Si vous ne disposez pas d'une instance IAM Identity Center existante à intégrer à votre WorkSpaces, nous vous recommandons d'en créer une dans la même région que la vôtre WorkSpaces. Si vous avez une instance AWS Identity Center existante dans une autre région, vous pouvez configurer l'intégration entre régions. Pour plus d'informations sur la configuration interrégionale, consultez [the section called "Création d'une intégration entre régions du centre d'identité IAM \(facultatif\)"](#).

 Note

L'intégration entre régions entre WorkSpaces et IAM Identity Center n'est pas prise en charge dans. AWS GovCloud (US) Region

1. Activez IAM Identity Center avec vos AWS Organizations, en particulier si vous utilisez un environnement multi-comptes. Vous pouvez également créer une instance de compte d'IAM Identity Center. Pour en savoir plus, consultez la section [Activation d' AWS IAM Identity Center](#). Chaque WorkSpaces répertoire peut être associé à une instance, une organisation ou un compte IAM Identity Center.

Si vous utilisez une instance d'organisation et que vous essayez de créer un WorkSpaces répertoire dans l'un des comptes membres, assurez-vous de disposer des autorisations IAM Identity Center suivantes.

- "sso:DescribeInstance"
- "sso:CreateApplication"
- "sso:PutApplicationGrant"
- "sso:PutApplicationAuthenticationMethod"
- "sso:DeleteApplication"
- "sso:DescribeApplication"
- "sso:getApplicationGrant"

Pour plus d'informations, consultez [Présentation de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center](#). Assurez-vous également qu'aucune politique de contrôle des services (SCPs) ne bloque ces autorisations. Pour en savoir plus SCPs, consultez la section [Politiques de contrôle des services \(SCPs\)](#).

2. Configurez IAM Identity Center et Microsoft Entra ID pour synchroniser automatiquement les utilisateurs sélectionnés ou tous les utilisateurs de votre tenant Entra ID avec votre instance IAM Identity Center. Pour plus d'informations, voir [Configurer SAML et SCIM avec Microsoft Entra ID et IAM Identity Center et Tutoriel : Configurer AWS IAM Identity Center pour le provisionnement automatique des utilisateurs](#).
3. Vérifiez que les utilisateurs que vous avez configurés sur Microsoft Entra ID sont correctement synchronisés avec l'instance AWS IAM Identity Center. Si un message d'erreur s'affiche dans

Microsoft Entra ID, cela indique que l'utilisateur indiqué dans Entra ID est configuré d'une manière non prise en charge par IAM Identity Center. Le message d'erreur permettra d'identifier ce problème. Par exemple, si l'objet utilisateur dans Entra ID ne contient pas de prénom, de nom de famille, and/or de nom d'affichage, vous recevrez un message d'erreur similaire à "2 validation errors detected: Value at 'name.givenName' failed to satisfy constraint: Member must satisfy regular expression pattern: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r]+; Value at 'name.givenName' failed to satisfy constraint: Member must have length greater than or equal to 1". Pour plus d'informations, voir [Échec de la synchronisation d'utilisateurs spécifiques avec IAM Identity Center à partir d'un fournisseur SCIM externe](#).

Note

WorkSpaces utilise l'attribut Entra ID UserPrincipalName (UPN) pour identifier les utilisateurs individuels et ses limites sont les suivantes :

- UPNs ne peut pas dépasser 63 caractères.
- Si vous modifiez l'UPN après en avoir attribué un WorkSpace à un utilisateur, celui-ci ne pourra pas se connecter à son UPN, WorkSpace sauf si vous redéfinissez l'UPN par rapport à ce qu'il était auparavant.

Étape 2 : enregistrer une application Microsoft Entra ID pour accorder des autorisations pour Windows Autopilot

WorkSpaces Personal utilise le mode piloté par les utilisateurs de Microsoft Windows Autopilot pour s'inscrire WorkSpaces à Microsoft Intune et les associer à l'identifiant Microsoft Entra.

Pour autoriser Amazon WorkSpaces à enregistrer WorkSpaces Personal dans Autopilot, vous devez enregistrer une application Microsoft Entra ID qui accorde les autorisations nécessaires à l'API Microsoft Graph. Pour plus d'informations sur l'enregistrement d'une application Entra ID, voir [Démarrage rapide : enregistrement d'une application auprès de la plateforme d'identité Microsoft](#).

Nous vous recommandons de fournir les autorisations d'API suivantes dans votre application Entra ID.

- Pour créer un nouveau profil WorkSpace qui doit être joint à Entra ID, l'autorisation API suivante est requise.

- `DeviceManagementServiceConfig.ReadWrite.All`
- Lorsque vous résiliez un compte personnel WorkSpace ou que vous le reconstruisez, les autorisations suivantes sont utilisées.

 Note

Si vous ne fournissez pas ces autorisations, elles WorkSpace seront résiliées mais elles ne seront pas supprimées pour vos locataires Intune et Entra ID et vous devrez les supprimer séparément.

- `DeviceManagementServiceConfig.ReadWrite.All`
- `Device.ReadWrite.All`
- `DeviceManagementManagedDevices.ReadWrite.All`
- Ces autorisations nécessitent le consentement de l'administrateur. Pour plus d'informations, voir [Accorder le consentement de l'administrateur à l'ensemble du locataire pour une application](#).

Ensuite, vous devez ajouter un secret client pour l'application Entra ID. Pour plus d'informations, consultez la section [Ajouter des informations d'identification](#). Assurez-vous de vous souvenir de la chaîne secrète du client, car vous en aurez besoin lors de la création du AWS Secrets Manager secret à l'étape 4.

Étape 3 : configurer le mode piloté par l'utilisateur de Windows Autopilot

Assurez-vous de connaître le [didacticiel étape par étape pour la jointure Microsoft Entra dans Intune pilotée par les utilisateurs de Windows Autopilot](#).

Pour configurer votre Microsoft Intune pour le pilote automatique

1. Connectez-vous au centre d'administration Microsoft Intune
2. Créez un nouveau groupe d'appareils de pilote automatique pour le personnel. WorkSpaces
Pour plus d'informations, voir [Création de groupes d'appareils pour Windows Autopilot](#).
 - a. Choisissez Groupes, Nouveau groupe
 - b. Pour Type de groupe, choisissez Sécurité.
 - c. Pour le type d'adhésion, choisissez Dynamic Device.

- d. Choisissez Modifier la requête dynamique pour créer une règle d'adhésion dynamique. La règle doit être au format suivant :

```
(device.devicePhysicalIds -any (_ -eq "[OrderID]:WorkSpacesDirectoryName"))
```

 Important

WorkSpacesDirectoryName doit correspondre au nom du répertoire WorkSpaces personnel Entra ID que vous avez créé à l'étape 5. Cela est dû au fait que la chaîne de nom du répertoire est utilisée comme balise de groupe lors de l'enregistrement des bureaux virtuels dans Autopilot. En outre, le tag de groupe correspond à l'OrderID attribut sur les appareils Microsoft Entra.

3. Choisissez Appareils, Windows, Inscription. Pour les options d'inscription, choisissez Inscription automatique. Pour l'étendue de l'utilisateur MDM, sélectionnez Tout.
4. Créez un profil de déploiement du pilote automatique. Pour plus d'informations, consultez la section [Création d'un profil de déploiement du pilote automatique](#).
 - a. Pour Windows Autopilot, choisissez Profils de déploiement, puis Créer un profil.
 - b. Dans l'écran des profils de déploiement de Windows Autopilot, sélectionnez le menu déroulant Créer un profil, puis sélectionnez Windows PC.
 - c. Dans l'écran Créer un profil, sur la page Sur l' Out-of-box expérience (OOBE). Pour le mode de déploiement, sélectionnez Dirigé par l'utilisateur. Pour Joindre à Microsoft Entra ID, sélectionnez Microsoft Entra joint. Vous pouvez personnaliser les noms d'ordinateur pour votre compte personnel associé à Entra ID en WorkSpaces sélectionnant Oui pour le modèle Appliquer le nom de l'appareil, afin de créer un modèle à utiliser lors de l'inscription d'un appareil.
 - d. Sur la page Attributions, pour Attribuer à, choisissez Groupes sélectionnés. Choisissez Sélectionner les groupes à inclure, puis sélectionnez le groupe d'appareils de pilote automatique que vous venez de créer dans 2.

Étape 4 : Création d'un AWS Secrets Manager secret

Vous devez créer un secret AWS Secrets Manager pour stocker en toute sécurité les informations, y compris l'ID de l'application et le secret du client, pour l'application Entra ID dans laquelle vous avez

créée [Étape 2 : enregistrer une application Microsoft Entra ID pour accorder des autorisations pour Windows Autopilot](#). Il s'agit d'une configuration unique.

Pour créer un AWS Secrets Manager secret

1. Créez une clé gérée par le client sur [AWS Key Management Service](#). La clé sera ensuite utilisée pour chiffrer le AWS Secrets Manager secret. N'utilisez pas la clé par défaut pour chiffrer votre secret, car le WorkSpaces service ne peut pas accéder à la clé par défaut. Suivez les étapes ci-dessous pour créer la clé.
 - a. Ouvrez la AWS KMS console à l'adresse <https://console.aws.amazon.com/kms>.
 - b. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
 - c. Choisissez Create key.
 - d. Sur la page Configurer la clé, pour Type de clé, sélectionnez Symétrique. Pour Utilisation des clés, choisissez Chiffrer et déchiffrer.
 - e. Sur la page de révision, dans l'éditeur de politique clé, assurez-vous d'autoriser l'`workspaces.amazonaws.com` accès principal du WorkSpaces service à la clé en incluant les autorisations suivantes dans la politique clé.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "workspaces.amazonaws.com"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

2. Créez le secret en AWS Secrets Manager utilisant la AWS KMS clé créée à l'étape précédente.
 - a. Ouvrez la console Secrets Manager à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
 - b. Choisissez Store a new secret (Stocker un nouveau secret).

- c. Sur la page Choisir un type de secret, pour Type de secret, sélectionnez Autre type de secret.
- d. Pour les paires clé/valeur, dans le champ clé, entrez « application_id » dans le champ clé, puis copiez l'identifiant de l'application Entra ID de l'[étape 2](#) et collez-le dans le champ valeur.
- e. Choisissez Ajouter une ligne, dans la case clé, entrez « application_password », puis copiez le secret du client de l'application Entra ID de l'[étape 2](#) et collez-le dans le champ de valeur.
- f. Choisissez la AWS KMS clé que vous avez créée à l'étape précédente dans la liste déroulante Clé de chiffrement.
- g. Choisissez Suivant.
- h. Sur la page Configurer le secret, entrez un nom et une description du secret.
- i. Dans la section Autorisations relatives aux ressources, choisissez Modifier les autorisations.
- j. Assurez-vous d'autoriser l'workspaces.amazonaws.com accès principal du WorkSpaces service au secret en incluant le respect de la politique en matière de ressources dans les autorisations relatives aux ressources.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Principal": {
      "Service": [ "workspaces.amazonaws.com" ]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
  } ]
}
```

Étape 5 : Création d'un WorkSpaces répertoire d'identifiants Microsoft Entra dédié

Créez un WorkSpaces répertoire dédié qui stocke les informations relatives aux utilisateurs associés à votre identifiant Microsoft Entra WorkSpaces et à votre identifiant Entra.

Pour créer un WorkSpaces répertoire Entra ID

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sur la page Créer un répertoire, pour le WorkSpaces type, choisissez Personnel. Pour la gestion des WorkSpace appareils, choisissez Microsoft Entra ID.
4. Pour l'ID de locataire Microsoft Entra, entrez l'ID de locataire Microsoft Entra auquel vous WorkSpaces souhaitez associer votre annuaire. Vous ne pourrez pas modifier l'ID du locataire une fois le répertoire créé.
5. Pour l'identifiant et le mot de passe de l'application Entra ID, sélectionnez le AWS Secrets Manager secret que vous avez créé à l'[étape 4](#) dans la liste déroulante. Vous ne pourrez pas modifier le secret associé au répertoire une fois celui-ci créé. Cependant, vous pouvez toujours mettre à jour le contenu du secret, y compris l'identifiant de l'application Entra ID et son mot de passe via la AWS Secrets Manager console à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
6. Si votre instance IAM Identity Center se trouve dans la même AWS région que votre WorkSpaces annuaire, dans Source d'identité utilisateur, sélectionnez l'instance IAM Identity Center que vous avez configurée à l'[étape 1](#) dans la liste déroulante. Vous ne pourrez pas modifier l'instance IAM Identity Center associée à l'annuaire une fois celui-ci créé.

Si votre instance IAM Identity Center se trouve dans une AWS région différente de celle de votre WorkSpaces annuaire, choisissez Activer l'interrégion, puis sélectionnez la région dans la liste déroulante.

Note

Si vous possédez une instance IAM Identity Center existante dans une autre région, vous devez vous inscrire pour configurer une intégration entre régions. Pour plus d'informations sur la configuration interrégionale, consultez [the section called “Création d'une intégration entre régions du centre d'identité IAM \(facultatif\)”](#).

7. Dans Nom du répertoire, entrez un nom unique pour le répertoire (par exemple, WorkSpacesDirectoryName).

 Important

Le nom du répertoire doit correspondre à celui OrderID utilisé pour créer la requête dynamique pour le groupe de périphériques Autopilot que vous avez créé avec Microsoft Intune à l'étape 3. La chaîne du nom du répertoire est utilisée comme balise de groupe lors de l'enregistrement personnel WorkSpaces dans Windows Autopilot. La balise de groupe correspond à l'OrderIDattribut sur les appareils Microsoft Entra.

8. (Facultatif) Dans le champ Description, saisissez une description pour la stratégie.
9. Pour le VPC, sélectionnez le VPC que vous avez utilisé pour lancer votre. WorkSpaces Pour de plus amples informations, veuillez consulter [Configuration d'un VPC pour le personnel WorkSpaces](#).
10. Pour les sous-réseaux, sélectionnez deux sous-réseaux de votre VPC qui ne proviennent pas de la même zone de disponibilité. Ces sous-réseaux seront utilisés pour lancer votre compte personnel WorkSpaces. Pour de plus amples informations, veuillez consulter [Zones de disponibilité pour le WorkSpaces personnel](#).

 Important

Assurez-vous que les entités WorkSpaces lancées dans les sous-réseaux disposent d'un accès Internet, ce qui est nécessaire lorsque les utilisateurs se connectent aux ordinateurs de bureau Windows. Pour de plus amples informations, veuillez consulter [Fournir un accès à Internet pour les WorkSpaces particuliers](#).

11. Pour Configuration, sélectionnez Activer le mode dédié Workspace. Vous devez l'activer pour créer un répertoire WorkSpaces personnel dédié afin de lancer Bring Your Own License (BYOL) Windows 10 ou 11 personal WorkSpaces.

 Note

Si vous ne voyez pas l'Workspaceoption Activer le service dédié sous Configuration, cela signifie que votre compte n'a pas été activé pour BYOL. Pour activer le BYOL pour votre compte, consultez[Apportez vos propres licences de bureau Windows WorkSpaces](#).

12. (Facultatif) Pour les balises, spécifiez la valeur de paire de clés que vous souhaitez utiliser pour les informations personnelles WorkSpaces dans le répertoire.

13. Consultez le résumé du répertoire et choisissez **Create directory**. La connexion de votre annuaire prend plusieurs minutes. Le statut initial de l'annuaire est **Creating**. Lorsque la création de l'annuaire est terminée, le statut est **Active**.

Une application IAM Identity Center est également créée automatiquement en votre nom une fois le répertoire créé. Pour trouver l'ARN de l'application, rendez-vous sur la page de résumé du répertoire.

Vous pouvez désormais utiliser le répertoire pour lancer Windows 10 ou 11 Personal WorkSpaces inscrit à Microsoft Intune et associé à Microsoft Entra ID. Pour de plus amples informations, veuillez consulter [Créez un Workspace in WorkSpaces Personal](#).

Après avoir créé un répertoire WorkSpaces personnel, vous pouvez en créer un Workspace. Pour de plus amples informations, consultez [Créez un Workspace in WorkSpaces Personal](#).

Configuration de l'application IAM Identity Center pour un WorkSpaces annuaire (facultatif)

Une application IAM Identity Center correspondante est automatiquement créée une fois qu'un répertoire est créé. Vous trouverez l'ARN de l'application dans la section Résumé de la page détaillée du répertoire. Par défaut, tous les utilisateurs de l'instance Identity Center peuvent accéder à ce qui leur est attribué WorkSpaces sans configurer l'application Identity Center correspondante. Toutefois, vous pouvez gérer l'accès des utilisateurs à un annuaire WorkSpaces en configurant l'attribution des utilisateurs pour l'application IAM Identity Center.

Pour configurer l'attribution d'utilisateur pour l'application IAM Identity Center

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans l'onglet Applications AWS gérées, choisissez l'application pour le WorkSpaces répertoire. Les noms des applications sont au format suivant :WorkSpaces.wsd-xxxxx, où se wsd-xxxxx trouve l'ID du WorkSpaces répertoire.
3. Choisissez Actions, puis Modifier les détails.
4. Modifiez la méthode d'attribution des utilisateurs et des groupes de Ne pas exiger d'assignments à Exiger des affectations.
5. Sélectionnez Enregistrer les modifications.

Une fois cette modification effectuée, les utilisateurs de l'instance Identity Center perdront l'accès qui leur est attribué, WorkSpaces sauf s'ils sont affectés à l'application. Pour affecter vos utilisateurs à l'application, utilisez la AWS CLI commande `create-application-assignment` pour attribuer

des utilisateurs ou des groupes à une application. Pour plus d'informations, consultez la référence de la commande [AWS CLI](#).

Création d'une intégration entre régions du centre d'identité IAM (facultatif)

Nous recommandons que votre instance IAM Identity Center WorkSpaces et l'instance associée se trouvent dans la même AWS région. Toutefois, si vous avez déjà configuré une instance IAM Identity Center dans une région différente de la vôtre WorkSpaces, vous pouvez créer une intégration entre régions. Lorsque vous créez une intégration entre régions WorkSpaces et IAM Identity Center, vous permettez de passer des appels interrégionaux WorkSpaces pour accéder aux informations de votre instance IAM Identity Center et les stocker, telles que les attributs d'utilisateur et de groupe.

Important

Amazon WorkSpaces prend en charge le centre d'identité IAM interrégional et les WorkSpaces intégrations uniquement pour les instances au niveau de l'organisation. WorkSpaces ne prend pas en charge les intégrations interrégionales de l'IAM Identity Center pour les instances au niveau du compte. Pour plus d'informations sur les types d'instances IAM Identity Center et leurs cas d'utilisation, voir [Comprendre les types d'instances IAM Identity Center](#).

Si vous créez une intégration interrégionale entre un WorkSpaces annuaire et une instance IAM Identity Center, vous risquez de rencontrer une latence plus élevée lors du déploiement WorkSpaces et lors de la connexion en raison des appels interrégionaux. L'augmentation de la latence est proportionnelle à la distance entre votre WorkSpaces région et la région du centre d'identité IAM. Nous vous recommandons d'effectuer des tests de latence pour votre cas d'utilisation spécifique.

Vous pouvez activer les connexions entre régions IAM Identity Center au cours de [l'étape 5 : créer un répertoire Microsoft Entra ID WorkSpaces dédié](#). Pour Source d'identité utilisateur, choisissez l'instance IAM Identity Center que vous avez configurée dans le [the section called “Étape 1 : activer IAM Identity Center et synchroniser avec Microsoft Entra ID”](#) menu déroulant.

Important

Vous ne pouvez pas modifier l'instance IAM Identity Center associée à l'annuaire après l'avoir créé.

Créez un répertoire personnalisé dédié avec WorkSpaces Personal

Avant de créer Windows 10 et 11 BYOL personal WorkSpaces et de les attribuer à vos utilisateurs, gérés par les fournisseurs d'identité AWS IAM Identity Center (IdPs), vous devez créer un répertoire personnalisé WorkSpaces dédié. WorkSpaces Les utilisateurs personnels ne sont associés à aucun Microsoft Active Directory mais peuvent être gérés à l'aide d'une solution de gestion des appareils mobiles (MDM) de votre choix, telle que JumpCloud. Pour plus d'informations JumpCloud, consultez [cet article](#). Pour des didacticiels qui utilisent les autres options, consultez [Création d'un répertoire pour WorkSpaces Personal](#).

Note

- Amazon ne WorkSpaces peut pas créer ni gérer de comptes utilisateur sur Personal WorkSpaces lancé dans un annuaire personnalisé. En tant qu'administrateur, vous devrez les gérer.
- Le WorkSpaces répertoire personnalisé est disponible dans toutes les AWS régions où Amazon WorkSpaces est proposé, à l'exception de l'Afrique (Le Cap), d'Israël (Tel Aviv) et de la Chine (Ningxia).
- Amazon ne WorkSpaces peut pas créer ni gérer de comptes utilisateur à l' WorkSpaces aide d'annuaires personnalisés. Pour vous assurer que le logiciel d'agent MDM que vous utilisez peut créer le profil utilisateur sous Windows WorkSpaces, contactez les fournisseurs de solutions MDM. La création du profil utilisateur permet à vos utilisateurs de se connecter au bureau Windows à partir de l'écran de connexion Windows.

Table des matières

- [Exigences et limitations](#)
- [Étape 1 : Activez IAM Identity Center et connectez-vous à votre fournisseur d'identité](#)
- [Étape 2 : Création d'un WorkSpaces répertoire personnalisé dédié](#)

Exigences et limitations

- Les WorkSpaces répertoires personnalisés ne prennent en charge que Windows 10 ou 11 Bring Your Own License personal WorkSpaces.
- Les WorkSpaces annuaires personnalisés ne prennent en charge que le protocole DCV.

- Assurez-vous d'activer BYOL pour votre AWS compte et de disposer de votre propre AWS KMS serveur auquel votre personnel WorkSpaces peut accéder pour l'activation de Windows 10 et 11. Pour en savoir plus, consultez [Apportez vos propres licences de bureau Windows WorkSpaces](#).
- Assurez-vous de préinstaller le logiciel de l'agent MDM sur l'image BYOL que vous avez importée dans votre compte. AWS

Étape 1 : Activez IAM Identity Center et connectez-vous à votre fournisseur d'identité

Pour les attribuer WorkSpaces à vos utilisateurs gérés par vos fournisseurs d'identité, les informations utilisateur doivent être mises à disposition AWS via AWS IAM Identity Center. Nous vous recommandons d'utiliser IAM Identity Center pour gérer l'accès de vos utilisateurs aux AWS ressources. Pour plus d'informations, consultez [En quoi consiste IAM Identity Center ?](#). Il s'agit d'une configuration unique.

Pour mettre les informations utilisateur à la disposition de AWS

1. Activez IAM Identity Center sur. AWS Vous pouvez activer IAM Identity Center auprès de vos AWS organisations, en particulier si vous utilisez un environnement multi-comptes. Vous pouvez également créer une instance de compte d'IAM Identity Center. Pour plus d'informations, consultez la section [Activation d'AWS IAM Identity Center](#). Chaque WorkSpaces annuaire peut être associé à une organisation ou à une instance de compte IAM Identity Center. Chaque instance d'IAM Identity Center peut être associée à un ou plusieurs annuaires WorkSpaces personnels.

Si vous utilisez une instance d'organisation et que vous essayez de créer un WorkSpaces répertoire dans l'un des comptes membres, assurez-vous de disposer des autorisations IAM Identity Center suivantes.

- "sso:DescribeInstance"
- "sso:CreateApplication"
- "sso:PutApplicationGrant"
- "sso:PutApplicationAuthenticationMethod"
- "sso:DeleteApplication"
- "sso:DescribeApplication"
- "sso:getApplicationGrant"

Pour plus d'informations, consultez la section [Présentation de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center](#). Assurez-vous qu'aucune politique de contrôle des services (SCPs) ne bloque ces autorisations. Pour en savoir plus SCPs, consultez la section [Politiques de contrôle des services \(SCPs\)](#).

2. Configurez IAM Identity Center et votre fournisseur d'identité (IdP) pour synchroniser automatiquement les utilisateurs entre votre IdP et votre instance IAM Identity Center. Pour plus d'informations, consultez la [section Tutoriels de mise en route](#) et choisissez le didacticiel spécifique à l'IdP que vous souhaitez utiliser. Par exemple, [utiliser IAM Identity Center pour vous connecter à votre plate-forme d' JumpCloud annuaire](#).
3. Vérifiez que les utilisateurs que vous avez configurés sur votre IdP sont correctement synchronisés avec l'instance AWS IAM Identity Center. La première synchronisation peut prendre jusqu'à une heure selon la configuration de votre IdP.

Étape 2 : Création d'un WorkSpaces répertoire personnalisé dédié

Créez un répertoire WorkSpaces personnel dédié qui stocke des informations sur vos WorkSpaces et sur vos utilisateurs.

Pour créer un WorkSpaces répertoire personnalisé dédié

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez Créer un annuaire.
4. Sur la page Créer un répertoire, pour le WorkSpace type, choisissez Personnel. Pour la gestion des WorkSpace appareils, choisissez Personnalisé.
5. Pour Source d'identité utilisateur, sélectionnez l'instance IAM Identity Center que vous avez configurée à l'[étape 1](#) dans la liste déroulante. Vous ne pourrez pas modifier l'instance IAM Identity Center associée à l'annuaire une fois celui-ci créé.

Note

Vous devez spécifier une instance IAM Identity Center pour le répertoire, sinon vous ne pourrez pas lancer Personal WorkSpaces avec l'annuaire à l'aide de la WorkSpaces

console. WorkSpaces les annuaires auxquels aucun Identity Center n'est associé ne sont compatibles qu'avec les solutions partenaires de WorkSpaces base.

6. Dans Nom du répertoire, entrez un nom unique pour le répertoire.
7. Pour le VPC, sélectionnez le VPC que vous avez utilisé pour lancer votre WorkSpaces. Pour de plus amples informations, veuillez consulter [Configuration d'un VPC pour le personnel WorkSpaces](#).
8. Pour les sous-réseaux, sélectionnez deux sous-réseaux de votre VPC qui ne proviennent pas de la même zone de disponibilité. Ces sous-réseaux seront utilisés pour lancer votre compte personnel WorkSpaces. Pour de plus amples informations, veuillez consulter [Zones de disponibilité pour le WorkSpaces personnel](#).

 Important

Assurez-vous que ceux qui sont WorkSpaces lancés dans les sous-réseaux disposent d'un accès Internet, ce qui est nécessaire lorsque les utilisateurs se connectent aux ordinateurs de bureau Windows. Pour de plus amples informations, veuillez consulter [Fournir un accès à Internet pour les WorkSpaces particuliers](#).

9. Pour Configuration, sélectionnez Activer le mode dédié Workspace. Vous devez l'activer pour créer un répertoire WorkSpaces personnel dédié afin de lancer Bring Your Own License (BYOL) Windows 10 ou 11 personal WorkSpaces.
10. (Facultatif) Pour les balises, spécifiez la valeur de paire de clés que vous souhaitez utiliser pour les informations personnelles WorkSpaces dans le répertoire.
11. Consultez le résumé du répertoire et choisissez Create directory. La connexion de votre annuaire prend plusieurs minutes. Le statut initial de l'annuaire est Creating. Lorsque la création de l'annuaire est terminée, le statut est Active.

Une application IAM Identity Center est également créée automatiquement en votre nom une fois le répertoire créé. Pour trouver l'ARN de l'application, rendez-vous sur la page de résumé du répertoire.

Vous pouvez désormais utiliser le répertoire pour lancer Windows 10 ou 11 Personal WorkSpaces inscrit à Microsoft Intune et associé à Microsoft Entra ID. Pour de plus amples informations, veuillez consulter [Créez un Workspace in WorkSpaces Personal](#).

Après avoir créé un répertoire WorkSpaces personnel, vous pouvez en créer un Workspace. Pour de plus amples informations, veuillez consulter [Créez un Workspace in WorkSpaces Personal](#).

Mettre à jour les serveurs DNS pour WorkSpaces Personal

Si vous devez mettre à jour les adresses IP du serveur DNS pour votre Active Directory après avoir lancé votre WorkSpaces, vous devez également les mettre à jour WorkSpaces avec les nouveaux paramètres du serveur DNS.

Vous pouvez mettre à jour vos paramètres DNS WorkSpaces avec les nouveaux paramètres DNS de l'une des manières suivantes :

- Mettez à jour les paramètres DNS sur le WorkSpaces avant de mettre à jour les paramètres DNS pour Active Directory.
- Reconstituez le WorkSpaces après avoir mis à jour les paramètres DNS d'Active Directory.

Nous vous recommandons de mettre à jour les paramètres DNS sur le WorkSpaces avant de mettre à jour les paramètres DNS dans Active Directory (comme expliqué à l'[étape 1](#) de la procédure suivante).

Si vous souhaitez WorkSpaces plutôt le reconstruire, mettez à jour l'une des adresses IP du serveur DNS de votre Active Directory ([étape 2](#)), puis suivez la procédure [Reconstruire un WorkSpace in WorkSpaces Personal](#) pour reconstruire votre WorkSpaces. Après avoir reconstruit votre WorkSpaces, suivez la procédure décrite à l'[étape 3](#) pour tester les mises à jour de votre serveur DNS. Une fois cette étape terminée, mettez à jour l'adresse IP de votre deuxième serveur DNS dans Active Directory, puis reconstituez le WorkSpaces vôtre. Assurez-vous de suivre la procédure décrite à l'[Étape 3](#) pour tester la mise à jour du second serveur DNS. Comme indiqué dans la section [Bonnes pratiques](#), nous vous recommandons de mettre à jour les adresses IP des serveurs DNS une par une.

Bonnes pratiques

Lorsque vous mettez à jour les paramètres du serveur DNS, nous vous recommandons de suivre les bonnes pratiques suivantes :

- Pour éviter les déconnexions et l'inaccessibilité des ressources du domaine, nous vous recommandons vivement de mettre à jour le serveur DNS pendant les heures creuses ou pendant une période de maintenance planifiée.
- N'en lancez aucune nouvelle dans WorkSpaces les 15 minutes qui précèdent et dans les 15 minutes qui suivent la modification des paramètres de votre serveur DNS.

- Lorsque vous mettez à jour les paramètres d'un serveur DNS, modifiez les adresses IP une à la fois. Vérifiez que la première mise à jour est correcte avant de mettre à jour la deuxième adresse IP. Nous vous recommandons d'exécuter la procédure suivante ([Étape 1](#), [Étape 2](#) et [Étape 3](#)) deux fois pour mettre à jour les adresses IP une par une.

Étape 1 : mettez à jour les paramètres du serveur DNS sur votre WorkSpaces

Dans la procédure suivante, les valeurs d'adresse IP actuelles et nouvelles du serveur DNS sont désignées comme suit :

- Adresses IP DNS actuelles : *oldIP1*, *oldIP2*
- Nouvelles adresses IP DNS : *NewIP1*, *NewIP2*

Note

Si c'est la deuxième fois que vous effectuez cette procédure, remplacez *oldIP1* par *oldIP2* et *NewIP1* par *NewIP2*.

Mettre à jour les paramètres du serveur DNS pour Windows WorkSpaces

Si vous en avez plusieurs WorkSpaces, vous pouvez déployer la mise à jour de registre suivante sur le WorkSpaces en appliquant un objet de stratégie de groupe (GPO) sur l'unité d'organisation Active Directory pour votre WorkSpaces. Pour plus d'informations sur l'utilisation GPOs, consultez [Gérez votre Windows WorkSpaces dans WorkSpaces Personal](#).

Vous pouvez effectuer ces mises à jour soit à l'aide de l'éditeur du registre, soit à l'aide de Windows PowerShell. Les deux procédures sont décrites dans cette section.

Pour mettre à jour les paramètres de registre DNS à l'aide de l'Éditeur du Registre

1. Sur votre Windows Workspace, ouvrez le champ de recherche Windows, puis entrez **registry editor** pour ouvrir l'éditeur de registre (regedit.exe).
2. À la question « Voulez-vous autoriser cette application à apporter des modifications à votre appareil ? », choisissez Oui.
3. Dans l'Éditeur du Registre, accédez à l'entrée suivante :

HKEY_LOCAL_MACHINE \ LOGICIEL \ Amazon \ SkyLight

4. Ouvrez la clé DomainJoinDns de registre. Mettez à jour *OldIP1* avec *NewIP1*, puis cliquez sur OK.
5. Fermez l'Éditeur du Registre.
6. Redémarrez WorkSpace le ou redémarrez le service SkyLightWorkspaceConfigService.

 Note

Après le redémarrage du service SkyLightWorkspaceConfigService, l'adaptateur réseau peut prendre jusqu'à 1 minute pour refléter la modification.

7. Passez à l'[Étape 2](#) et mettez à jour les paramètres du serveur DNS dans Active Directory afin de remplacer *OldIP1* par *NewIP1*.

Pour mettre à jour les paramètres du registre DNS à l'aide de PowerShell

La procédure suivante utilise des PowerShell commandes pour mettre à jour votre registre et redémarrer le service SkyLightWorkspaceConfigService.

1. Sur votre Windows WorkSpace, ouvrez le champ de recherche Windows et entrez **powershell**. Choisissez Exécuter en tant qu'administrateur.
2. À la question « Voulez-vous autoriser cette application à apporter des modifications à votre appareil ? », choisissez Oui.
3. Dans la PowerShell fenêtre, exécutez la commande suivante pour récupérer les adresses IP actuelles du serveur DNS.

```
Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
```

Le résultat doit être similaire à ce qui suit.

```
DomainJoinDns : OldIP1,OldIP2
PSPath         : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
               \Amazon\SkyLight
PSParentPath   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
               \Amazon
PSChildName    : SkyLight
PSDrive        : HKLM
PSProvider     : Microsoft.PowerShell.Core\Registry
```

4. Dans la PowerShell fenêtre, exécutez la commande suivante pour passer *OldIP1* à *NewIP1*. Assurez-vous de laisser *OldIP2* tel quel pour le moment.

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value  
"NewIP1,OldIP2"
```

5. Exécutez la commande suivante pour redémarrer le service SkyLightWorkspaceConfigService.

```
restart-service -Name SkyLightWorkspaceConfigService
```

 Note

Après le redémarrage du service SkyLightWorkspaceConfigService, l'adaptateur réseau peut prendre jusqu'à 1 minute pour refléter la modification.

6. Passez à l'[Étape 2](#) et mettez à jour les paramètres du serveur DNS dans Active Directory afin de remplacer *OldIP1* par *NewIP1*.

Mettre à jour les paramètres du serveur DNS pour Amazon Linux 2 WorkSpaces

Si vous possédez plusieurs Amazon Linux 2 WorkSpace, nous vous recommandons d'utiliser une solution de gestion de configuration pour distribuer et appliquer les politiques. Par exemple, vous pouvez utiliser [Ansible](#).

Pour mettre à jour les paramètres du serveur DNS sur un Amazon Linux 2 Workspace

1. Sur votre système Linux Workspace, ouvrez une fenêtre de terminal.
2. Utilisez la commande Linux suivante pour modifier le fichier `/etc/dhcp/dhclient.conf`. Vous devez disposer des privilèges utilisateur root pour modifier ce fichier. Vous pouvez devenir utilisateur root soit en utilisant la commande `sudo -i`, soit en exécutant toutes les commandes avec `sudo` comme indiqué.

```
sudo vi /etc/dhcp/dhclient.conf
```

Dans le fichier `/etc/dhcp/dhclient.conf`, vous verrez la commande `prepend` suivante, où *OldIP1* et *OldIP2* sont les adresses IP des serveurs DNS.

```
prepend domain-name-servers OldIP1, OldIP2; # skylight
```

3. Remplacez *OldIP1* par *NewIP1*, et laissez *OldIP2* tel quel pour le moment.
4. Enregistrez vos modifications dans `/etc/dhcp/dhclient.conf`.
5. Redémarrez le WorkSpace.
6. Passez à l'[Étape 2](#) et mettez à jour les paramètres du serveur DNS dans Active Directory afin de remplacer *OldIP1* par *NewIP1*.

Mettre à jour les paramètres du serveur DNS pour Ubuntu WorkSpaces

Si vous possédez plusieurs Ubuntu WorkSpace, nous vous recommandons d'utiliser une solution de gestion de configuration pour distribuer et appliquer les politiques. Par exemple, vous pouvez utiliser [Landscape](#).

Pour mettre à jour les paramètres du serveur DNS sur Ubuntu WorkSpace

1. Sur votre Ubuntu WorkSpace, ouvrez une fenêtre de terminal et exécutez la commande suivante. Vous devez disposer des privilèges utilisateur root pour modifier ce fichier. Vous pouvez devenir utilisateur root soit en utilisant la commande `sudo -i`, soit en exécutant toutes les commandes avec `sudo` comme indiqué.

```
sudo vi /etc/netplan/zz-workspaces-domain.yaml
```

2. Dans le fichier yaml, vous verrez la `nameserver` commande suivante.

```
nameservers:  
  search:[Your domain FQDN]  
  addresses:[OldIP1, OldIP2]
```

Remplacez le *OldIP1* et *OldIP2* par le *NewIP1* and *NewIP2*.

Si vous avez plusieurs adresses IP de serveurs DNS, ajoutez-les sous forme de valeurs séparées par des virgules. Par exemple, [*NewDNSIP1*, *NewDNSIP2*, *NewDNSIP3*].

3. Enregistrez le fichier yaml.
4. Exécutez la commande `sudo netplan apply` pour appliquer les modifications.
5. Exécutez la commande `resolvectl status` pour vérifier que la nouvelle adresse IP DNS est utilisée.
6. Passez à l'[étape 2](#) et mettez à jour les paramètres de votre serveur DNS dans Active Directory.

Mettre à jour les paramètres du serveur DNS pour Red Hat Enterprise Linux WorkSpaces

Si vous possédez plusieurs Red Hat Enterprise Linux WorkSpace, nous vous recommandons d'utiliser une solution de gestion de configuration pour distribuer et appliquer les politiques. Par exemple, vous pouvez utiliser [Ansible](#).

Pour mettre à jour les paramètres du serveur DNS sur Red Hat Enterprise Linux WorkSpace

1. Sur votre Red Hat Enterprise Linux WorkSpace, ouvrez une fenêtre de terminal et exécutez la commande ci-dessous. Vous devez disposer des privilèges utilisateur root pour modifier ce fichier. Vous pouvez devenir utilisateur root soit en utilisant la commande `sudo -i`, soit en exécutant toutes les commandes avec `sudo` comme indiqué.

```
sudo nmcli conn modify CustomerNIC ipv4.dns 'NewIP1 NewIP2'
```

2. Exécutez la commande suivante.

```
sudo systemctl restart NetworkManager
```

3. Pour vérifier la configuration DNS et réseau mise à jour, exécutez la commande suivante.

```
nmcli device show eth1
```

4. Passez à l'[étape 2](#) et mettez à jour les paramètres de votre serveur DNS dans Active Directory.

Étape 2 : Mettre à jour les paramètres de serveur DNS pour Active Directory

Au cours de cette étape, vous mettez à jour les paramètres du serveur DNS pour Active Directory. Comme indiqué dans la section [Bonnes pratiques](#), nous vous recommandons de mettre à jour les adresses IP des serveurs DNS une par une.

Pour mettre à jour les paramètres du DNS pour Active Directory, consultez la documentation suivante dans le Guide d'administration AWS Directory Service :

- AD Connector : [Mise à jour de l'adresse DNS pour votre AD Connector](#)
- AWS Microsoft AD géré : [configuration des redirecteurs conditionnels DNS pour votre domaine local](#)
- Simple AD : [Configurer DNS](#)

Après avoir mis à jour les paramètres du serveur DNS, passez à l'[Étape 3](#).

Étape 3 : Tester les paramètres de serveur DNS mis à jour

Après avoir terminé l'[Étape 1](#) et l'[Étape 2](#), effectuez la procédure suivante pour vérifier que les paramètres mis à jour du serveur DNS fonctionnent comme prévu.

Dans la procédure suivante, les valeurs d'adresse IP actuelles et nouvelles du serveur DNS sont désignées comme suit :

- Adresses IP DNS actuelles : *OldIP1*, *OldIP2*
- Nouvelles adresses IP DNS : *NewIP1*, *NewIP2*

Note

Si c'est la deuxième fois que vous effectuez cette procédure, remplacez *OldIP1* par *OldIP2* et *NewIP1* par *NewIP2*.

Testez les paramètres du serveur DNS mis à jour pour Windows WorkSpaces

1. Arrêtez le serveur DNS *OldIP1*.
2. Connectez-vous à Windows WorkSpace.
3. Dans le menu Démarrer de Windows, choisissez Système Windows, puis Invite de commandes.
4. Exécutez la commande suivante, où *AD_Name* est le nom de votre annuaire Active Directory (par exemple, corp.example.com).

```
nslookup AD_Name
```

La commande nslookup doit renvoyer le résultat suivant. (Si c'est la deuxième fois que vous effectuez cette procédure, vous devez voir *NewIP2* au lieu de *OldIP2*.)

```
Server: Full_AD_Name
Address: NewIP1

Name: AD_Name
Addresses: OldIP2
           NewIP1
```


5. Si le résultat ne correspond pas à ce que vous attendez ou si des erreurs s'affichent, répétez l'[Étape 1](#).
6. Patientez une heure et vérifiez qu'aucun problème n'a été signalé du côté des utilisateurs. Vérifiez que *NewIP1* reçoit des requêtes DNS et renvoie des réponses.
7. Après avoir vérifié que le premier serveur DNS fonctionne correctement, répétez l'[Étape 1](#) pour mettre à jour le second serveur DNS, cette fois en remplaçant *OldIP2* par *NewIP2*. Répétez ensuite les étapes 2 et 3.

Testez les paramètres du serveur DNS mis à jour pour Linux WorkSpaces

1. Arrêtez le serveur DNS *OldIP1*.
2. Connectez-vous à un système Linux WorkSpace.
3. Sur votre système Linux WorkSpace, ouvrez une fenêtre de terminal.
4. Les adresses IP du serveur DNS renvoyées dans la réponse DHCP sont écrites dans le `/etc/resolv.conf` fichier local sur le WorkSpace. Exécutez la commande suivante pour afficher le contenu du fichier `/etc/resolv.conf` .

```
cat /etc/resolv.conf
```

Le résultat suivant doit s'afficher. (Si c'est la deuxième fois que vous effectuez cette procédure, vous devez voir *NewIP2* au lieu de *OldIP2*.)

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your Workspace inaccessible until reboot
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkspaceIP
```

Note

Si vous apportez des modifications manuelles au `/etc/resolv.conf` fichier, ces modifications sont perdues au WorkSpace redémarrage.

5. Si le résultat ne correspond pas à ce que vous attendez ou si des erreurs s'affichent, répétez l'[Étape 1](#).
6. Les adresses IP réelles du serveur DNS sont stockées dans le fichier `/etc/dhcp/dhclient.conf`. Pour afficher le contenu de ce fichier, exécutez la commande suivante.

```
sudo cat /etc/dhcp/dhclient.conf
```

Le résultat suivant doit s'afficher. (Si c'est la deuxième fois que vous effectuez cette procédure, vous devez voir *NewIP2* au lieu de *OldIP2*.)

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your Workspace inaccessible until rebuild
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. Patientez une heure et vérifiez qu'aucun problème n'a été signalé du côté des utilisateurs. Vérifiez que *NewIP1* reçoit des requêtes DNS et renvoie des réponses.
8. Après avoir vérifié que le premier serveur DNS fonctionne correctement, répétez l'[Étape 1](#) pour mettre à jour le second serveur DNS, cette fois en remplaçant *OldIP2* par *NewIP2*. Répétez ensuite les étapes 2 et 3.

Supprimer un répertoire pour WorkSpaces Personal

Note

Simple AD et AD Connector sont mis à votre disposition gratuitement WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire Simple AD ou AD Connector pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé auprès d'Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires.AWS Directory Service](#)

Si vous supprimez votre répertoire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à l'utiliser WorkSpaces .

Que se passe-t-il lorsque vous supprimez un répertoire ? Lorsque vous supprimez un répertoire, les événements suivants se produisent :

- Lorsqu'un Simple AD ou un AWS Directory Service for Microsoft Active Directory annuaire est supprimé, toutes les données de l'annuaire et les instantanés sont supprimés et ne peuvent pas être récupérés. Une fois l'annuaire supprimé, toutes les instances Amazon EC2 qui lui sont associées restent intactes. Toutefois, vous ne pouvez pas utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances. Vous devez vous connecter à ces instances à l'aide d'un Compte AWS identifiant local à l'instance.
- Lorsqu'un annuaire AD Connector est supprimé, votre annuaire sur site reste intact. Toutes les instances associées à l'annuaire restent également intactes, et associée à votre annuaire sur site. Vous pouvez toutefois utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances.

Supprimer un identifiant Entra ou un WorkSpaces répertoire personnalisé

Le WorkSpaces répertoire Entra ID vous permet de créer un WorkSpaces BYOL Windows 10 ou 11 intégré à Entra ID. Pour de plus amples informations, veuillez consulter [Créez un répertoire Microsoft Entra ID dédié avec WorkSpaces Personal](#).

Un WorkSpaces répertoire personnalisé vous permet de créer des répertoires WorkSpaces qui ne sont pas joints à un domaine Active Directory, mais d'utiliser votre propre logiciel de gestion des appareils et IAM Identity Center. Pour de plus amples informations, veuillez consulter [Créez un répertoire personnalisé dédié avec WorkSpaces Personal](#).

Pour supprimer un identifiant Entra ou un WorkSpaces répertoire personnalisé

1. Supprimez tout ce qui WorkSpaces se trouve dans le répertoire. Pour de plus amples informations, veuillez consulter [Supprimer un Workspace dans WorkSpaces Personal](#).
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez l'annuaire.
4. Sélectionnez Actions, Supprimer.
5. Lorsque vous êtes invité à confirmer, saisissez Supprimer.

Supprimer un AWS répertoire du Directory Service

Vous pouvez supprimer le AWS répertoire du Directory Service qui vous concerne WorkSpaces s'il n'est plus utilisé par d'autres applications WorkDocs, telles qu'Amazon WorkMail ou Amazon Chime. WorkSpaces Notez que vous devez annuler l'enregistrement d'un annuaire avant de pouvoir le supprimer.

Pour annuler l'enregistrement d'un annuaire

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez l'annuaire.
4. Choisissez Actions, Deregister (Annuler l'enregistrement).
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Annuler l'enregistrement. Une fois l'enregistrement annulé, la valeur de Membre est No.

Pour supprimer un annuaire

1. Supprimez tout ce WorkSpaces qui se trouve dans le répertoire. Pour de plus amples informations, veuillez consulter [Supprimer un WorkSpace dans WorkSpaces Personal](#).
2. Recherchez et supprimez toutes les applications et tous les services qui sont enregistrés dans l'annuaire. Pour plus d'informations, consultez [Supprimer votre annuaire](#) dans le Guide d'administration AWS Directory Service .
3. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
4. Dans le volet de navigation, choisissez Directories (Annuaire).
5. Sélectionnez l'annuaire et choisissez Actions, Annuler l'enregistrement.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Annuler l'enregistrement.
7. Sélectionnez de nouveau l'annuaire et choisissez Actions, Supprimer.
8. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Note

La suppression des affectations d'applications peut parfois prendre plus de temps que prévu. Si le message d'erreur suivant s'affiche, vérifiez que vous avez supprimé toutes les affectations d'application, puis attendez 30 à 60 minutes avant de réessayer de supprimer le répertoire :

An Error Has Occurred

Cannot delete the directory because it still has authorized applications.
Additional directory details can be viewed at the Directory Service console.

9. (Facultatif) Après avoir supprimé toutes les ressources du Virtual Private Cloud (VPC) de votre répertoire, vous pouvez supprimer le VPC et libérer l'adresse IP Elastic utilisée pour la passerelle NAT. Pour plus d'informations, consultez [Supprimer votre VPC](#) et [Utiliser des adresses IP Elastic](#) dans le Guide de l'utilisateur Amazon VPC.
10. (Facultatif) Pour supprimer tous les bundles et les images personnalisés dont vous n'avez plus besoin, consultez [Supprimer un ensemble ou une image personnalisé dans WorkSpaces Personal](#).

Configuration des outils d'administration Active Directory pour le WorkSpaces personnel

Vous effectuerez la plupart des tâches administratives de votre WorkSpaces annuaire à l'aide d'outils de gestion d'annuaire, tels que les outils d'administration Active Directory. Toutefois, vous allez utiliser la WorkSpaces console pour effectuer certaines tâches liées aux annuaires. Pour de plus amples informations, veuillez consulter [Gérer les annuaires pour WorkSpaces Personal](#).

Si vous créez un annuaire avec AWS Managed Microsoft AD ou Simple AD qui en inclut cinq ou plus WorkSpaces, nous vous recommandons de centraliser l'administration sur une EC2 instance Amazon. Bien que vous puissiez installer les outils de gestion d'annuaire sur un WorkSpace, l'utilisation d'une EC2 instance Amazon est une solution plus robuste.

Pour configurer des outils d'administration Active Directory

1. Lancez une instance Amazon EC2 Windows et associez-la à votre WorkSpaces répertoire en utilisant l'une des options suivantes :
 - Si vous ne possédez pas encore d'instance Amazon EC2 Windows, vous pouvez joindre l'instance à votre domaine d'annuaire lorsque vous lancez l'instance. Pour plus d'informations, voir [Rejoindre facilement une EC2 instance Windows](#) dans le Guide AWS Directory Service d'administration.
 - Si vous possédez déjà une instance Amazon EC2 Windows, vous pouvez la joindre manuellement à votre répertoire. Pour plus d'informations, consultez [Joindre manuellement une instance Windows](#) dans le Guide d'administration AWS Directory Service.
2. Installez les outils d'administration Active Directory sur l'instance Amazon EC2 Windows. Pour plus d'informations, consultez [Installation des outils d'administration Active Directory](#) dans le Guide d'administration AWS Directory Service.

 Note

Lorsque vous installez les outils d'administration Active Directory, assurez-vous de sélectionner également Gestion des stratégies de groupe pour installer l'outil Éditeur de gestion des stratégies de groupe (gpmc.msc).

Lorsque l'installation de la fonctionnalité est terminée, les outils Active Directory sont disponibles dans le menu Démarrer de Windows, sous Outils d'administration Windows.

3. Exécutez les outils en tant qu'administrateur d'annuaire comme suit :
 - a. Dans le menu Démarrer de Windows, ouvrez les Outils d'administration Windows.
 - b. Maintenez la touche Maj enfoncée, cliquez avec le bouton droit sur le raccourci de l'outil à utiliser, puis choisissez Exécuter en tant qu'autre utilisateur.
 - c. Entrez les informations d'identification de l'administrateur. Avec Simple AD, le nom d'utilisateur est **Administrator** et avec AWS Managed Microsoft AD, c'est l'administrateur qui l'est **Admin**.

Vous pouvez désormais exécuter des tâches d'administration d'annuaire avec des outils Active Directory qui vous sont familiers. Par exemple, vous pouvez utiliser l'outil Utilisateurs et ordinateurs Active Directory pour ajouter/supprimer des utilisateurs, promouvoir un utilisateur auprès d'un administrateur d'annuaire ou réinitialiser un mot de passe utilisateur. Notez que vous devez être connecté à votre instance Windows en tant qu'utilisateur autorisé à gérer les utilisateurs de l'annuaire.

Pour promouvoir un utilisateur en tant qu'administrateur d'annuaire

 Note

Cette procédure s'applique uniquement aux annuaires créés avec Simple AD, et non avec AWS Managed AD. Pour les annuaires créés avec AWS Managed AD, voir [Gérer les utilisateurs et les groupes dans AWS Managed Microsoft AD](#) dans le Guide d'AWS Directory Service administration.

1. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory.

2. Accédez au dossier Users sous votre domaine et sélectionnez l'utilisateur à promouvoir.
3. Choisissez Action, Propriétés.
4. Dans la boîte de dialogue **username** Propriétés, choisissez Member Of.
5. Ajoutez l'utilisateur aux groupes suivants et choisissez OK.
 - Administrators
 - Domain Admins
 - Enterprise Admins
 - Group Policy Creator Owners
 - Schema Admins

Pour ajouter ou supprimer des utilisateurs

Vous pouvez créer de nouveaux utilisateurs à partir de la WorkSpaces console Amazon uniquement pendant le processus de lancement d'un WorkSpace, et vous ne pouvez pas supprimer d'utilisateurs via la WorkSpaces console Amazon. La plupart des tâches de gestion des utilisateurs, y compris la gestion des groupes d'utilisateurs, doivent être effectuées via votre annuaire.

 Important

Avant de pouvoir supprimer un utilisateur, vous devez supprimer celui qui lui est WorkSpace attribué. Pour de plus amples informations, veuillez consulter [Supprimer un WorkSpace dans WorkSpaces Personal](#).

Le processus que vous utilisez pour gérer les utilisateurs et les groupes dépend du type de répertoire que vous utilisez.

- Si vous utilisez AWS Managed Microsoft AD, consultez la section [Gérer les utilisateurs et les groupes dans AWS Managed Microsoft AD](#) dans le Guide d'AWS Directory Service administration.
- Si vous utilisez Simple AD, consultez [Gérer des utilisateurs et des groupes dans Simple AD](#) dans le Guide d'administration AWS Directory Service.
- Si vous utilisez Microsoft Active Directory via AD Connector ou une relation d'approbation, vous pouvez gérer des utilisateurs et des groupes à l'aide du [module Active Directory](#).

Pour réinitialiser un mot de passe utilisateur

Lorsque vous réinitialiser le mot de passe pour un utilisateur existant, ne définissez pas le paramètre `ForcePasswordChange`. L'utilisateur doit changer le mot de passe à la prochaine ouverture de session. Dans le cas contraire, les utilisateurs ne peuvent pas se connecter à leur WorkSpaces. Attribuez plutôt un mot de passe temporaire sécurisé à chaque utilisateur, puis demandez-leur de modifier manuellement leur mot de passe lors de leur prochaine connexion. WorkSpace

Note

Si vous utilisez AD Connector ou si vos utilisateurs se trouvent dans la région AWS GovCloud (ouest des États-Unis), ils ne seront pas en mesure de réinitialiser leurs propres mots de passe. (Le mot de passe oublié ? l'option sur l'écran de connexion de l'application WorkSpaces cliente ne sera pas disponible.)

Administrer les utilisateurs dans WorkSpaces Personal

Chacune WorkSpace est attribuée à un seul utilisateur et ne peut pas être partagée par plusieurs utilisateurs. Par défaut, un seul WorkSpace par utilisateur et par répertoire est autorisé.

Table des matières

- [Gérer les utilisateurs dans WorkSpaces Personal](#)
- [Création d'un multiple WorkSpaces pour un utilisateur dans WorkSpaces Personal](#)
- [Personnalisez la façon dont les utilisateurs se connectent à leur compte WorkSpaces dans WorkSpaces Personal](#)
- [Activez les fonctionnalités de WorkSpaces gestion en libre-service pour vos utilisateurs dans Personal WorkSpaces](#)
- [Activez l'optimisation audio Amazon Connect pour vos utilisateurs dans WorkSpaces Personal](#)
- [Activer le téléchargement des journaux de diagnostic dans Personal WorkSpaces](#)

Gérer les utilisateurs dans WorkSpaces Personal

En tant qu'administrateur de WorkSpaces, vous pouvez effectuer les tâches suivantes pour gérer les WorkSpaces utilisateurs.

Modification d'informations utilisateur

Vous pouvez utiliser la WorkSpaces console pour modifier les informations utilisateur d'un WorkSpace.

Note

Cette fonctionnalité n'est disponible que si vous utilisez AWS Managed Microsoft AD ou Simple AD. Si vous utilisez Microsoft Active Directory via AD Connector ou une relation d'approbation, vous pouvez gérer des utilisateurs et des groupes à l'aide du [module Active Directory](#). Si vous utilisez l'identifiant Microsoft Entra ou un WorkSpaces répertoire personnalisé, vous pouvez gérer les utilisateurs et les groupes avec l'identifiant Microsoft Entra ou vos fournisseurs d'identité.

Pour modifier des informations utilisateur

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez un utilisateur, puis choisissez Actions, Modifier les utilisateurs.
4. Mettez à jour le Prénom, le Nom et l'E-mail si nécessaire.
5. Choisissez Mettre à jour.

Ajout ou suppression d'utilisateurs

Vous pouvez créer des utilisateurs à partir de la WorkSpaces console Amazon uniquement pendant le processus de lancement d'un WorkSpace, et vous ne pouvez pas supprimer d'utilisateurs via la WorkSpaces console Amazon. La plupart des tâches de gestion des utilisateurs, y compris la gestion des groupes d'utilisateurs, doivent être effectuées via votre annuaire.

Pour ajouter ou supprimer des utilisateurs et des groupes

Pour ajouter, supprimer ou gérer des utilisateurs et des groupes, vous devez le faire via votre annuaire. Vous effectuerez la plupart des tâches administratives de votre WorkSpaces annuaire à l'aide d'outils de gestion d'annuaire, tels que les outils d'administration Active Directory. Pour de plus amples informations, veuillez consulter [Configuration des outils d'administration Active Directory pour le WorkSpaces personnel](#).

 Important

Avant de pouvoir supprimer un utilisateur, vous devez supprimer celui qui lui est WorkSpace attribué. Pour de plus amples informations, veuillez consulter [Supprimer un WorkSpace dans WorkSpaces Personal](#).

Le processus que vous utilisez pour gérer les utilisateurs et les groupes dépend du type de répertoire que vous utilisez.

- Si vous utilisez AWS Managed Microsoft AD, consultez la section [Gérer les utilisateurs et les groupes dans AWS Managed Microsoft AD](#) dans le Guide d'AWS Directory Service administration.
- Si vous utilisez Simple AD, consultez [Gérer des utilisateurs et des groupes dans Simple AD](#) dans le Guide d'administration AWS Directory Service.
- Si vous utilisez Microsoft Active Directory via AD Connector ou une relation d'approbation, vous pouvez gérer des utilisateurs et des groupes à l'aide du [module Active Directory](#).

Envoi d'un e-mail d'invitation

Vous pouvez envoyer un e-mail d'invitation à un utilisateur manuellement si nécessaire.

 Note

Si vous utilisez AD Connector sur un domaine approuvé, les e-mails d'invitation ne sont pas automatiquement envoyés à vos utilisateurs. Vous devez donc les envoyer manuellement. Les e-mails d'invitation ne sont pas non plus envoyés automatiquement si l'utilisateur existe déjà dans Active Directory.

Pour renvoyer un e-mail d'invitation

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sur la WorkSpaces page, utilisez le champ de recherche pour rechercher l'utilisateur auquel vous souhaitez envoyer une invitation, puis sélectionnez le correspondant dans les résultats WorkSpace de recherche. Vous ne pouvez en sélectionner qu'un WorkSpace à la fois.

4. Choisissez Actions, Inviter un utilisateur.
5. Sur la page Inviter des utilisateurs à accéder à la WorkSpace page, choisissez Envoyer une invitation.

Création d'un multiple WorkSpaces pour un utilisateur dans WorkSpaces Personal

Par défaut, vous ne pouvez en créer qu'un WorkSpace par utilisateur et par répertoire. Toutefois, si nécessaire, vous pouvez en créer plusieurs WorkSpace pour un utilisateur, en fonction de la configuration de votre répertoire.

- Si vous n'avez qu'un seul répertoire pour votre WorkSpaces, créez plusieurs noms d'utilisateur pour cet utilisateur. Par exemple, une utilisatrice nommée Marie Majeur peut avoir mmajeur1, mmajeur2, etc., comme noms d'utilisateur. Chaque nom d'utilisateur est associé à un nom différent WorkSpace dans le même répertoire, mais WorkSpaces ils ont le même code d'enregistrement, à condition qu' WorkSpaces ils soient tous créés dans le même répertoire de la même AWS région.
- Si vous avez plusieurs répertoires pour votre WorkSpaces, créez-les WorkSpaces pour l'utilisateur dans des répertoires distincts. Vous pouvez utiliser le même nom d'utilisateur ou des noms d'utilisateur différents dans les annuaires. Ils WorkSpaces auront des codes d'enregistrement différents.

Tip

Afin de retrouver facilement tout ce WorkSpaces que vous avez créé pour un utilisateur, utilisez le même nom d'utilisateur de base pour chacun d'entre eux WorkSpace.

Par exemple, si vous avez une utilisateur nommée Mary Major avec le nom d'utilisateur Active Directory mmajor, créez WorkSpaces pour elle des noms d'utilisateur tels que mmajor, mmajor1, mmajor2, mmajor3 ou d'autres variantes, telles que mmajor_windows ou mmajor_linux. Tant qu' WorkSpaces ils ont tous le même nom d'utilisateur de base de départ (mmajor), vous pouvez trier le nom d'utilisateur dans votre WorkSpaces console pour tous les regrouper WorkSpaces pour cet utilisateur.

⚠ Important

- Un utilisateur peut avoir à la fois une PCo adresse IP et un DCV à condition WorkSpace que les deux WorkSpaces soient situés dans des répertoires distincts. Le même utilisateur ne peut pas avoir d' PCoadresse IP et de DCV WorkSpace dans le même répertoire.
- Si vous configurez plusieurs répertoires WorkSpaces pour une utilisation avec la redirection entre régions, vous devez les configurer WorkSpaces dans différents répertoires dans différentes AWS régions, et vous devez utiliser les mêmes noms d'utilisateur dans chaque répertoire. Pour plus d'informations sur la redirection entre régions, consultez [Redirection entre régions pour Personal WorkSpaces](#).

Pour passer de l'un à l'autre WorkSpaces, l'utilisateur se connecte à l'aide du nom d'utilisateur et du code d'enregistrement associés à un espace de travail particulier. Si l'utilisateur utilise une version 3.0 ou ultérieure des applications WorkSpaces clientes pour Windows, macOS ou Linux, il peut attribuer différents noms aux applications clientes en WorkSpaces accédant à Paramètres, Gérer les informations de connexion dans l'application cliente.

Personnalisez la façon dont les utilisateurs se connectent à leur compte WorkSpaces dans WorkSpaces Personal

Personnalisez l'accès de vos utilisateurs à WorkSpaces l'aide d'identifiants de ressources uniformes (URIs) afin de fournir une expérience de connexion simplifiée qui s'intègre aux flux de travail existants de votre organisation. Par exemple, vous pouvez générer automatiquement un identifiant URIs qui enregistre vos utilisateurs en utilisant leur code WorkSpaces d'enregistrement. En conséquence :

- Les utilisateurs peuvent contourner le processus d'inscription manuelle.
- Leurs noms d'utilisateur sont automatiquement saisis sur la page de connexion de leur WorkSpaces client.
- Si l'authentification multifactorielle (MFA) est utilisée dans votre organisation, les codes MFA et leur nom d'utilisateur est automatiquement entré sur la page de connexion du client.

L'accès URI fonctionne à la fois avec les codes d'enregistrement basés sur les régions (par exemple, WSpdx+ABC12D) et avec les codes d'enregistrement basés sur les noms de domaine complets (FQDN) (par exemple, desktop.example.com). Pour plus d'informations sur la création et

l'utilisation des codes d'enregistrement FQDN, consultez [Redirection entre régions pour Personal WorkSpaces](#).

Vous pouvez configurer l'accès par URI WorkSpaces pour les applications clientes sur les appareils pris en charge suivants :

- Ordinateurs Windows
- Ordinateurs macOS
- Ordinateurs Ubuntu Linux 18.04, 20.04 et 22.04
- iPads
- Appareils Android

Pour accéder URIs à leur WorkSpaces, les utilisateurs doivent d'abord installer l'application cliente pour leur appareil en ouvrant <https://clients.amazonworkspaces.com/> et en suivant les instructions.

L'accès par URI est pris en charge sur les navigateurs Firefox et Chrome sur les ordinateurs Windows et macOS, sur le navigateur Firefox sur les ordinateurs Ubuntu Linux 18.04, 20.04 et 22.04, et sur les navigateurs Internet Explorer et Microsoft Edge sur les ordinateurs Windows. Pour plus d'informations sur WorkSpaces les clients, consultez la section [WorkSpaces Clients](#) du guide de WorkSpaces l'utilisateur Amazon.

 Note

Sur les appareils Android, l'accès des URI fonctionne uniquement avec le navigateur Firefox, et non avec le navigateur Google Chrome.

Pour configurer l'accès aux URI WorkSpaces, utilisez l'un des formats d'URI décrits dans le tableau suivant.

 Note

Si le composant de données de votre URI inclut l'un des caractères réservés suivants, nous vous recommandons d'utiliser l'encodage en pourcent dans le composant afin d'éviter cette ambiguïté :

@ : / ? & =

Par exemple, si vous avez des noms d'utilisateurs qui incluent l'un de ces caractères, vous devez utiliser l'encodage en pourcentage pour ces noms d'utilisateurs dans votre URI. Pour plus d'informations, consultez [Uniform Resource Identifier \(URI\): Generic Syntax](#).

Syntaxe prise en charge	Description
<code>workspaces://</code>	Ouvre l'application WorkSpaces client. (Remarque : l'utilisation d'espaces de travail : // n'est pas actuellement prise en charge dans l'application client Linux.)
<code>workspaces://@registrationcode</code>	Enregistre un utilisateur à l'aide de son code WorkSpace s d'enregistrement. Affiche également la page de connexion du client.
<code>workspaces://username@registrationcode</code>	Enregistre un utilisateur à l'aide de son code WorkSpace s d'enregistrement. Entre aussi automatiquement le nom d'utilisateur dans le champ username sur la page de connexion du client.
<code>espaces de travail : //username @registrationcode ? MFACode=mfa</code>	Enregistre un utilisateur à l'aide de son code WorkSpace s d'enregistrement. Entre aussi automatiquement le nom d'utilisateur dans le champ username et le code de l'authentification multifactorielle (MFA) dans le champ Code MFA sur la page de connexion du client.
<code>espaces de travail : //@registrationcode ? MFACode=mfa</code>	Enregistre un utilisateur à l'aide de son code WorkSpace s d'enregistrement. Entre aussi automatiquement le code d'authentification MFA dans le champ MFA code (Code MFA) sur la page de connexion du client.

Note

Si les utilisateurs ouvrent un lien URI alors qu'ils sont déjà connectés WorkSpace à un client Windows, une nouvelle WorkSpaces session s'ouvre et leur WorkSpaces session d'origine reste ouverte. Si les utilisateurs ouvrent un lien URI lorsqu'ils sont connectés

Workspace à un client macOS, iPad ou Android, aucune nouvelle session ne s'ouvre ; seule leur WorkSpaces session d'origine reste ouverte.

Activez les fonctionnalités de WorkSpaces gestion en libre-service pour vos utilisateurs dans Personal WorkSpaces

Dans WorkSpaces, vous pouvez activer les fonctionnalités de Workspace gestion en libre-service pour vos utilisateurs afin de leur permettre de mieux contrôler leur expérience. Et vous pouvez également réduire la charge de travail de votre service support informatique pour WorkSpaces. Lorsque vous activez les fonctionnalités de libre-service, les utilisateurs peuvent effectuer une ou plusieurs des tâches suivantes directement depuis leur WorkSpaces client :

- Mettre en cache leurs informations d'identification sur leur client. Cela leur permet de se reconnecter à leur Workspace sans avoir à saisir à nouveau leurs informations d'identification.
- Redémarrez (redémarrez) leur Workspace.
- Augmentez la taille des volumes root et utilisateur sur leur Workspace.
- Modifiez le type de calcul (bundle) de leur Workspace.
- Changez le mode de fonctionnement de leur Workspace.
- Reconstruisez leur Workspace.

Clients pris en charge

- Android, fonctionnant sur Android ou sur des systèmes Chrome OS compatibles avec Android
- Linux
- macOS
- Windows

Pour activer les capacités de gestion en libre-service pour les utilisateurs

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez l'annuaire dans lequel vous souhaitez activer les fonctionnalités de gestion en libre-service.

4. Faites défiler la page jusqu'à Autorisations en libre-service et choisissez Modifier. Activez ou désactivez les options suivantes selon les besoins pour déterminer les tâches WorkSpace de gestion que les utilisateurs peuvent effectuer depuis leur client :
- Se souvenir de moi : les utilisateurs peuvent choisir de mettre en cache leurs informations d'identification sur le client en cochant la case Se souvenir de moi ou Me maintenir connecté dans l'écran de connexion. Les informations d'identification ne sont mises en cache que dans la mémoire RAM. Lorsque les utilisateurs choisissent de mettre en cache leurs informations d'identification, ils peuvent s'y reconnecter WorkSpaces sans avoir à les saisir à nouveau. Pour contrôler la durée pendant laquelle les utilisateurs peuvent mettre en cache leurs informations d'identification, consultez [Définition de la durée de vie maximale d'un ticket Kerberos](#).
 - Redémarrer WorkSpace depuis le client — Les utilisateurs peuvent redémarrer (redémarrer) leur WorkSpace. Le redémarrage déconnecte l'utilisateur de son ordinateur WorkSpace, l'arrête et le redémarre. Les données utilisateur, le système d'exploitation et les paramètres système ne sont pas affectés.
 - Augmenter la taille du volume — Les utilisateurs peuvent étendre les volumes root et utilisateur sur leur WorkSpace ordinateur à une taille spécifiée sans contacter le support informatique. Les utilisateurs peuvent augmenter la taille du volume racine (pour Windows, le lecteur C : ; pour Linux, /) jusqu'à 175 Go, et la taille du volume utilisateur (pour Windows, le lecteur D : ; pour Linux, /home) jusqu'à 100 Go. WorkSpace les volumes root et utilisateur sont regroupés dans des groupes définis qui ne peuvent pas être modifiés. Les groupes disponibles sont \[Racine (Go), Utilisateur (Go)] : [80, 10], [80, 50], [80, 100], [175 jusqu'à 2000, 100 jusqu'à 2000]. Pour de plus amples informations, veuillez consulter [Modifier un WorkSpace dans WorkSpaces Personal](#).

Pour un disque nouvellement créé WorkSpace, les utilisateurs doivent attendre 6 heures avant de pouvoir augmenter la taille de ces disques. Ils ne peuvent par la suite le faire qu'une seule fois par période de 6 heures. Pendant qu'une augmentation de la taille du volume est en cours, les utilisateurs peuvent effectuer la plupart des tâches sur leur WorkSpace. Les tâches qu'ils ne peuvent pas effectuer sont les suivantes : modifier leur type de WorkSpace calcul, changer de mode d' WorkSpace exécution, redémarrer leur WorkSpace ordinateur ou le reconstruire. WorkSpace Lorsque le processus est terminé, WorkSpace il doit être redémarré pour que les modifications prennent effet. Ce processus peut prendre jusqu'à une heure.

 Note

Si les utilisateurs augmentent la taille du volume de leur compte WorkSpace, cela augmente le taux de facturation de leur WorkSpace.

- **Modifier le type de calcul** — Les utilisateurs peuvent passer d'un WorkSpace type de calcul à un autre (ensembles). Pour un nouveau bundle WorkSpace, les utilisateurs doivent attendre 6 heures avant de pouvoir passer à un autre bundle. Ils peuvent ensuite opter pour une solution groupée plus grande une seule fois dans une période de 6 heures, ou pour une solution groupée plus petite, une seule fois dans une période de 30 jours. Lorsqu'un changement de type de WorkSpace calcul est en cours, les utilisateurs sont déconnectés du leur WorkSpace et ils ne peuvent ni utiliser ni modifier le WorkSpace. Le WorkSpace est automatiquement redémarré pendant le processus de changement de type de calcul. Ce processus peut prendre jusqu'à une heure.

 Note

Si les utilisateurs modifient leur type de WorkSpace calcul, cela modifie le taux de facturation de leur WorkSpace.

- **Changer de mode de fonctionnement** — Les utilisateurs peuvent WorkSpace passer du mode de fonctionnement au AlwaysOnmode de AutoStopfonctionnement. Pour de plus amples informations, veuillez consulter [Gérer le mode de course dans WorkSpaces Personal](#).

 Note

Si les utilisateurs changent de mode de fonctionnement WorkSpace, cela modifie le taux de facturation de leur WorkSpace.

- **Reconstruire WorkSpace à partir du client** — Les utilisateurs peuvent rétablir le système d'exploitation WorkSpace d'un dans son état d'origine. Lorsqu'un WorkSpace est reconstruit, le volume utilisateur (lecteur D :) est recréé à partir de la dernière sauvegarde. Les sauvegardes étant effectuées toutes les 12 heures, les données utilisateur ont au maximum 12 heures. Pour une création récente WorkSpace, les utilisateurs doivent attendre 12 heures avant de pouvoir reconstruire leur WorkSpace. Lorsqu'une WorkSpace reconstruction est en cours, les utilisateurs sont déconnectés de leur WorkSpace compte et ils ne peuvent ni utiliser ni modifier leur WorkSpace. Ce processus peut prendre jusqu'à une heure.

- Chargement des journaux de diagnostic : les utilisateurs peuvent télécharger les fichiers journaux WorkSpaces du client directement dans le but de WorkSpaces résoudre les problèmes sans interrompre l'utilisation du client. WorkSpaces Si vous activez le téléchargement des journaux de diagnostic pour vos utilisateurs, ou si vous les autorisez à le faire eux-mêmes, les fichiers journaux sont envoyés WorkSpaces automatiquement à. Vous pouvez activer le téléchargement des journaux de diagnostic avant ou pendant une session de WorkSpaces streaming.

5. Choisissez Enregistrer.

Activez l'optimisation audio Amazon Connect pour vos utilisateurs dans WorkSpaces Personal

Dans la console WorkSpaces de gestion, vous pouvez activer l'optimisation audio du panneau de contrôle des contacts Amazon Connect (CCP) pour vos WorkSpaces flottes afin d'améliorer la sécurité et de permettre un son de qualité native. Après avoir activé l'optimisation audio du CCP, le son du CCP sera traité par les points de terminaison du client, tandis que WorkSpaces les utilisateurs pourront interagir avec le CCP depuis leur propre terminal. WorkSpaces

L'optimisation audio du Panneau de configuration des contacts (CCP) Amazon Connect fonctionne avec :

- Le client WorkSpaces Windows.
- Amazon Linux et Windows WorkSpaces.
- WorkSpaces en utilisant PCo IP ou DCV.

Exigences

- Amazon Connect doit avoir été configuré.
- Vous devez créer un CCP personnalisé avec l'API Amazon Connect Stream en créant un CCP sans média pour la signalisation d'appel. De cette façon, les médias sont traités sur le bureau local à l'aide du CCP standard, et le signalement et les contrôles d'appels sont traités sur la connexion à distance avec le CCP sans média. Pour plus d'informations sur l'API Amazon Connect streams, consultez le GitHub référentiel à l'adresse <https://github.com/aws/amazon-connect-streams>. Le CCP personnalisé que vous créez est le CCP que vos agents Amazon Connect utiliseront dans leur environnement. WorkSpaces

- Un navigateur Web compatible avec Amazon Connect doit être installé sur les terminaux WorkSpaces clients. Pour obtenir la liste des navigateurs pris en charge, consultez [Navigateurs pris en charge par Amazon Connect](#).

 Note

Si les utilisateurs utilisent des navigateurs qui ne sont pas pris en charge, ils seront invités à télécharger un navigateur compatible lorsqu'ils tenteront de se connecter au CCP.

Activation de l'optimisation audio d'Amazon Connect

Pour activer l'optimisation audio d'Amazon Connect pour les utilisateurs :

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez votre annuaire, puis choisissez Actions, Update Details.
4. Développez Optimisation audio d'Amazon Connect.

 Note

Avant de procéder à la configuration avec Amazon Connect, choisissez Mettre à jour pour enregistrer les modifications non enregistrées effectuées précédemment dans la console de gestion.

5. Choisissez Configurer Amazon Connect.
6. Entrez le nom du Panneau de contrôle des contacts (CCP) Amazon Connect.

 Note

Le nom que vous donnez à votre CCP sera utilisé dans le menu de l'extension utilisateur. Choisissez un nom qui aura du sens pour les utilisateurs.

7. Entrez l'URL du Panneau de configuration des contacts Amazon Connect générée par Amazon Connect. Consultez [Fourniture d'un accès au panneau de configuration des contacts](#) pour plus d'informations sur l'obtention de l'URL.
8. Choisissez Créer Amazon Connect.

Mise jour des informations d'optimisation audio Amazon Connect de l'annuaire

Pour mettre à jour les informations d'optimisation audio Amazon Connect de l'annuaire :

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez votre annuaire, puis choisissez Actions, Update Details.
4. Développez Optimisation audio d'Amazon Connect.

Note

Avant de procéder à la configuration avec Amazon Connect, choisissez Mettre à jour pour enregistrer les modifications non enregistrées effectuées précédemment dans la console de gestion.

5. Choisissez Configurer Amazon Connect.
6. Choisissez Modifier.
7. Sélectionnez votre annuaire, puis choisissez Actions, Update Details.
8. Mettez à jour le nom et l'URL du Panneau de configuration des contacts Amazon Connect.
9. Choisissez Enregistrer.

Suppression de l'optimisation audio Amazon Connect de l'annuaire

Pour supprimer les informations d'optimisation audio Amazon Connect de l'annuaire :

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez votre annuaire, puis choisissez Actions, Update Details.
4. Développez Optimisation audio d'Amazon Connect.

Note

Avant de procéder à la configuration avec Amazon Connect, choisissez Mettre à jour pour enregistrer les modifications non enregistrées effectuées précédemment dans la console de gestion.

5. Choisissez Configurer Amazon Connect.
6. Choisissez Supprimer Amazon Connect.

Pour plus d'informations, consultez le [Guide de formation des agents](#).

Activer le téléchargement des journaux de diagnostic dans Personal WorkSpaces

Pour résoudre les problèmes des WorkSpaces clients, activez le téléchargement automatique des journaux de diagnostic. Ceci est actuellement pris en charge pour les clients Windows, macOS, Linux et Web Access.

Note

La fonctionnalité de téléchargement des journaux de diagnostic du WorkSpaces client n'est actuellement pas disponible dans la région AWS GovCloud (ouest des États-Unis).

Chargement des journaux de diagnostic

Grâce aux téléchargements des journaux de diagnostic, vous pouvez télécharger les fichiers journaux WorkSpaces du client directement WorkSpaces vers le site pour résoudre les problèmes sans interrompre l'utilisation du client. WorkSpaces Si vous activez le téléchargement des journaux de diagnostic pour vos utilisateurs, ou si vous les autorisez à le faire eux-mêmes, les fichiers journaux sont envoyés WorkSpaces automatiquement à. Vous pouvez activer le téléchargement des journaux de diagnostic avant ou pendant une session de WorkSpaces streaming.

Pour télécharger automatiquement les journaux de diagnostic à partir des appareils administrés, installez un WorkSpaces client qui prend en charge les téléchargements de diagnostics. Le chargement des journaux est activé par défaut. Vous pouvez modifier les paramètres de l'une des façons suivantes :

Option 1 : utilisation de la AWS console

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez le nom de l'annuaire pour lequel vous voulez activer la journalisation de diagnostic.

4. Faites défiler la page vers le bas jusqu'à Activer les autorisations en libre-service.
5. Choisissez Afficher les détails
6. Choisissez Modifier.
7. Choisissez Chargements du journal de diagnostic.
8. Choisissez Enregistrer.

Option 2 : utilisation d'un appel d'API

Vous pouvez modifier les paramètres du répertoire pour activer ou désactiver le client WorkSpaces Windows, macOS et Linux afin qu'il télécharge automatiquement les journaux de diagnostic à l'aide d'un appel d'API. Si cette option est activée, lorsqu'un problème survient chez le client, les journaux sont envoyés WorkSpaces sans intervention de l'utilisateur. Pour plus d'informations, consultez la [référence de WorkSpaces l'API](#).

Vous pouvez aussi laisser les utilisateurs choisir d'activer le chargement automatique des journaux de diagnostic pendant ou après l'installation du client. Pour plus d'informations, voir [Application cliente WorkSpaces Windows](#), [Application cliente WorkSpaces macOS](#) et [Application cliente WorkSpaces Linux](#).

Note

- Les journaux de diagnostic ne contiennent pas d'informations sensibles. Vous pouvez désactiver le chargement automatique des journaux de diagnostic pour les utilisateurs au niveau de l'annuaire, ou autoriser ces derniers à désactiver cette fonctionnalité eux-mêmes.
- Pour accéder à la fonctionnalité de téléchargement des journaux de diagnostic, vous devez installer les versions suivantes des WorkSpaces clients :
 - 5.4.0 ou version ultérieure du client Windows
 - version 5.8.0 ou ultérieure du client macOS
 - 2023.1 du client Ubuntu 22.04
 - 2023.1 du client Ubuntu 20.04
 - Vous pouvez également accéder à la fonctionnalité de téléchargement du journal de diagnostic avec le client Web Access.

Administrer le WorkSpaces personnel

Vous pouvez administrer votre compte à WorkSpaces l'aide de la WorkSpaces console.

Pour effectuer des tâches d'administration d'annuaires, consultez [the section called “Configuration de l'administration de l'annuaire”](#).

Note

- Assurez-vous de mettre à jour les pilotes de dépendance réseau tels que les pilotes ENA et PV de votre WorkSpaces. NVMe Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez [Installer ou mettre à niveau le pilote Elastic Network Adapter \(ENA\)](#), [Pilotes NVMe AWS pour les instances Windows](#), et [Mettre à niveau les pilotes PV sur les instances Windows](#).
- Assurez-vous de mettre régulièrement à jour les agents EC2 Config, EC2 EC2 Launch et Launch V2 vers les dernières versions. Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez [Update EC2 Config and EC2 Launch](#).

Table des matières

- [Gérez votre Windows WorkSpaces dans WorkSpaces Personal](#)
- [Gérez votre Amazon Linux 2 WorkSpaces en mode WorkSpaces personnel](#)
- [Gérez votre Ubuntu WorkSpaces en mode WorkSpaces personnel](#)
- [Gérez votre Rocky Linux WorkSpaces](#)
- [Gérez votre Red Hat Enterprise Linux WorkSpaces](#)
- [Optimisation WorkSpaces pour une communication en temps réel dans WorkSpaces Personal](#)
- [Gérer le mode de course dans WorkSpaces Personal](#)
- [Gérer les applications dans WorkSpaces Personal](#)
- [Modifier un Workspace dans WorkSpaces Personal](#)
- [Personnaliser l'image de marque dans WorkSpaces Personal](#)
- [Marquer les ressources dans WorkSpaces Personnel](#)
- [Entretien WorkSpaces personnel](#)
- [Chiffré WorkSpaces dans WorkSpaces Personal](#)

- [Redémarrer un WorkSpace dans WorkSpaces Personal](#)
- [Reconstruire un WorkSpace in WorkSpaces Personal](#)
- [Restaurer un compte WorkSpace dans WorkSpaces Personal](#)
- [Microsoft 365 Bring Your Own License \(BYOL\) en WorkSpaces mode personnel](#)
- [Mettre à niveau Windows BYOL WorkSpaces dans Personal WorkSpaces](#)
- [Migrer un WorkSpace dans WorkSpaces Personal](#)
- [Supprimer un WorkSpace dans WorkSpaces Personal](#)

Gérez votre Windows WorkSpaces dans WorkSpaces Personal

Vous pouvez utiliser les objets de stratégie de groupe (GPOs) pour appliquer des paramètres permettant de gérer Windows WorkSpaces ou les utilisateurs qui font partie de votre WorkSpaces répertoire Windows.

Note

- Si vous utilisez l'identifiant Microsoft Entra ou un WorkSpaces répertoire personnalisé, vous pouvez gérer les utilisateurs et les groupes avec l'identifiant Microsoft Entra ou vos fournisseurs d'identité. Pour plus d'informations, voir. [Créez un répertoire Microsoft Entra ID dédié avec WorkSpaces Personal](#)
- Les instances Linux ne respectent pas de stratégie de groupe. Pour plus d'informations sur la gestion d'Amazon Linux WorkSpaces, consultez [Gérez votre Amazon Linux 2 WorkSpaces en mode WorkSpaces personnel](#).

Amazon vous recommande de créer une unité organisationnelle pour vos objets WorkSpaces informatiques et une unité organisationnelle pour vos objets WorkSpaces utilisateur.

Pour utiliser les paramètres de stratégie de groupe spécifiques à Amazon WorkSpaces, vous devez installer le modèle d'administration de stratégie de groupe pour le ou les protocoles que vous utilisez, PCo IP ou DCV.

Warning

Les paramètres de stratégie de groupe peuvent affecter l'expérience de vos WorkSpace utilisateurs comme suit :

- La mise en œuvre d'un message de connexion interactif pour afficher une bannière de connexion empêche les utilisateurs d'accéder à leur WorkSpaces. Le paramètre de stratégie de groupe du message d'ouverture de session interactif n'est actuellement pas pris en charge par PCo IP WorkSpaces. Le message de connexion est pris en charge sur DCV WorkSpaces, et les utilisateurs doivent se reconnecter après avoir accepté la bannière de connexion. Les messages d'ouverture de session ne sont pas pris en charge lorsque l'ouverture de session basée sur des certificats est activée.
- La désactivation du stockage amovible via les paramètres de stratégie de groupe entraîne un échec de connexion qui connecte les utilisateurs à un profil temporaire sans accès au lecteur D.
- La suppression d'utilisateurs du groupe local Remote Desktop Users via les paramètres de stratégie de groupe empêche ces utilisateurs de s'authentifier via les applications WorkSpaces clientes. Pour plus d'informations sur ce paramètre de stratégie de groupe, consultez [Autoriser l'ouverture de session via les services Bureau à distance](#) dans la documentation Microsoft.
- Si vous supprimez le groupe d'utilisateurs intégré de la politique de sécurité Autoriser la connexion en local, WorkSpaces les utilisateurs de votre PCo adresse IP ne pourront pas se connecter à leur compte WorkSpaces via les applications WorkSpaces clientes. Votre PCo adresse IP ne recevra pas non WorkSpaces plus de mises à jour du logiciel de l'agent PCo IP. PCoLes mises à jour de l'agent IP peuvent contenir des correctifs de sécurité et autres, ou elles peuvent activer de nouvelles fonctionnalités pour votre WorkSpaces. Pour plus d'informations sur l'utilisation de cette politique de sécurité, consultez [Autoriser l'ouverture de session locale](#) dans la documentation Microsoft.
- Les paramètres de stratégie de groupe peuvent être utilisés pour restreindre l'accès aux lecteurs. Si vous configurez les paramètres de stratégie de groupe pour restreindre l'accès au lecteur C ou au lecteur D, les utilisateurs ne peuvent pas accéder à leur WorkSpaces. Pour éviter ce problème, assurez-vous que vos utilisateurs peuvent accéder aux lecteurs C et D.
- La fonction d' WorkSpaces entrée audio nécessite un accès de connexion local dans le Workspace. La fonction d'entrée audio est activée par défaut pour Windows WorkSpaces. Toutefois, si vous avez un paramètre de stratégie de groupe qui restreint la connexion locale des utilisateurs dans leur compte WorkSpaces, l'entrée audio ne fonctionnera pas sur votre WorkSpaces. Si vous supprimez ce paramètre de stratégie de groupe, la fonction d'entrée audio est activée après le prochain redémarrage du Workspace. Pour

plus d'informations sur ce paramètre de stratégie de groupe, consultez [Autoriser l'ouverture de session locale](#) dans la documentation Microsoft.

Pour plus d'informations sur l'activation ou la désactivation de la redirection d'entrée audio, consultez [Configurer la redirection d'entrée audio pour IP PCo](#) ou [Configurer la redirection d'entrée audio pour DCV](#).

- L'utilisation de la stratégie de groupe pour régler le mode d'alimentation de Windows sur Équilibré ou Économiseur d'énergie peut vous WorkSpaces empêcher de dormir lorsqu'ils sont laissés inactifs. Nous vous recommandons vivement d'utiliser une stratégie de groupe pour configurer le mode d'alimentation Windows sur Haute performance. Pour de plus amples informations, veuillez consulter [Mon Windows Workspace se met en veille lorsqu'il est laissé inactif](#).
- Certains paramètres de stratégie de groupe peuvent forcer les utilisateurs à se déconnecter lorsque celui-ci est déconnecté d'une session. Toutes les applications ouvertes par les utilisateurs WorkSpaces sont fermées.
- L'option « Définir une limite de temps pour les sessions de Remote Desktop Services actives mais inactives » n'est actuellement pas prise en charge sur le DCV WorkSpaces. Évitez de l'utiliser pendant les sessions DCV car il provoque une déconnexion même en cas d'activité et que la session n'est pas inactive.

Pour plus d'informations sur l'utilisation des outils d'administration Active Directory GPOs, consultez [Configuration des outils d'administration Active Directory pour le WorkSpaces personnel](#).

Table des matières

- [Installation des fichiers modèles d'administration de stratégie de groupe pour DCV](#)
- [Gérer les paramètres de stratégie de groupe pour DCV](#)
- [Installation du modèle administratif de stratégie de groupe pour PCo IP](#)
- [Gérer les paramètres de stratégie de groupe pour PCo IP](#)
- [Définition de la durée de vie maximale d'un ticket Kerberos](#)
- [Configuration des paramètres de serveur proxy de l'appareil pour l'accès à Internet](#)
 - [Utilisation d'un serveur proxy pour le trafic des espaces de travail](#)
 - [Recommandation concernant l'utilisation de serveurs proxy](#)
- [Activer la prise en charge du plugin Amazon WorkSpaces for Zoom Meeting Media](#)
 - [Activer le plug-in Zoom Meeting Media pour DCV](#)

- [Conditions préalables](#)
- [Avant de commencer](#)
- [Installation des composants Zoom](#)
- [Activer le plug-in Zoom Meeting Media pour PCo IP](#)
 - [Conditions préalables](#)
 - [Créez la clé de registre sur un WorkSpaces hôte Windows](#)
 - [Résolution des problèmes](#)

Installation des fichiers modèles d'administration de stratégie de groupe pour DCV

Pour utiliser les paramètres de stratégie de groupe spécifiques à l'utilisation WorkSpaces de DCV, vous devez ajouter le modèle d'administration de stratégie de groupe `wsp.admx` et `wsp.adml` les fichiers pour le DCV dans le magasin central du contrôleur de domaine de votre WorkSpaces répertoire. Pour plus d'informations sur les fichiers `.admx` et `.adml`, consultez [Comment créer et gérer le magasin central des modèles d'administration de stratégie de groupe dans Windows](#).

La procédure suivante décrit comment créer le magasin central et y ajouter les fichiers de modèles d'administration. Effectuez la procédure suivante sur une instance d'administration d'annuaire WorkSpace ou Amazon EC2 jointe à votre WorkSpaces annuaire.

Pour installer les fichiers modèles d'administration de stratégie de groupe pour DCV

1. À partir d'un système Windows en cours d'exécution WorkSpace, faites une copie `wsp.adml` des fichiers `wsp.admx` et du `C:\Program Files\Amazon\WSP` répertoire.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces répertoire, ouvrez l'Explorateur de fichiers Windows et, dans la barre d'adresse, entrez le nom de domaine complet (FQDN) de votre organisation, tel que `\\example.com`
3. Ouvrez le dossier `sysvol`.
4. Ouvrez le dossier nommé *FQDN*.
5. Ouvrez le dossier `Policies`. Vous devez maintenant être ici : `\\FQDN\sysvol\FQDN\Policies`.
6. S'il n'existe pas déjà, créez un dossier nommé `PolicyDefinitions`.
7. Ouvrez le dossier `PolicyDefinitions`.
8. Copiez le fichier `wsp.admx` dans le dossier `\\FQDN\sysvol\FQDN\Policies\PolicyDefinitions`.

9. Créez un dossier nommé en-US dans le dossier PolicyDefinitions.
10. Ouvrez le dossier en-US.
11. Copiez le fichier `wsp.adml` dans le dossier `\\FQDN\\sysvol\\FQDN\\Policies\\PolicyDefinitions\\en-US`.

Pour vérifier que les fichiers du modèle d'administration sont correctement installés

1. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (`gpmc.msc`).
2. Agrandissez la forêt (Forêt : **FQDN**).
3. Développez Domaines.
4. Développez votre FQDN (par exemple, `example.com`).
5. Développez Objets de stratégie de groupe.
6. Sélectionnez Stratégie de domaine par défaut, ouvrez le menu contextuel (via un clic droit) et choisissez Modifier.

Note

Si le domaine sous-jacent WorkSpaces est un AWS Managed Microsoft AD annuaire, vous ne pouvez pas utiliser la politique de domaine par défaut pour créer votre GPO. Au lieu de cela, vous devez créer et lier le GPO sous le conteneur de domaine disposant de privilèges délégués.

Lorsque vous créez un répertoire avec AWS Managed Microsoft AD, Directory Service crée une unité **yourdomainname** organisationnelle (UO) sous la racine du domaine. Le nom de cette unité d'organisation est basé sur le nom NetBIOS que vous avez saisi lors de la création de l'annuaire. Si vous n'avez pas spécifié de nom NetBIOS, il comprend par défaut la première partie du nom DNS de l'annuaire (par exemple, dans le cas de `corp.example.com`, le nom NetBIOS est `corp`).

Pour créer votre objet de stratégie de groupe, au lieu de sélectionner la stratégie de domaine par défaut, sélectionnez l'unité d'organisation (**yourdomainname** ou toute unité d'organisation inférieure à celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un objet de stratégie de groupe dans ce domaine, puis liez-le ici.

Pour plus d'informations sur l'**yourdomainname** UO, voir [What Gets Created](#) dans le Guide d'AWS Directory Service administration.

7. Dans l'éditeur de gestion des politiques de groupe, sélectionnez Configuration de l'ordinateur, Politiques, Modèles d'administration, Amazon et DCV.
8. Vous pouvez désormais utiliser cet objet de stratégie de groupe DCV pour modifier les paramètres de stratégie de groupe spécifiques à WorkSpaces l'utilisation de DCV.

Gérer les paramètres de stratégie de groupe pour DCV

Pour utiliser les paramètres de stratégie de groupe afin de gérer vos systèmes Windows utilisant WorkSpaces le DCV

1. Assurez-vous que le [modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour DCV](#) est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
2. Vérifiez que les fichiers du modèle d'administration sont correctement installés. Pour de plus amples informations, veuillez consulter [Pour vérifier que les fichiers du modèle d'administration sont correctement installés](#).

Configuration de la prise en charge de l'imprimante pour DCV

Par défaut, WorkSpaces active l'impression à distance de base, qui offre des capacités d'impression limitées car elle utilise un pilote d'imprimante générique côté hôte pour garantir une impression compatible.

L'impression à distance avancée pour les clients Windows connectés à Windows vous WorkSpaces permet d'utiliser des fonctionnalités spécifiques de votre imprimante, telles que l'impression recto verso, mais elle nécessite l'installation des pilotes d'imprimante correspondants côté hôte et côté client.

Vous pouvez utiliser les paramètres de stratégie de groupe pour configurer le support de l'imprimante selon vos besoins.

Impression de base ou avancée

Aspect	Impression de base	Impression avancée
Pilote utilisé	pilote XPS générique	pilote spécifique à l'imprimante
Installation du pilote	Automatique	Manuel (hôte et client)

Aspect	Impression de base	Impression avancée
Fonctions	Impression standard uniquement	Fonctionnalités complètes de l'imprimante (recto verso, sélection du bac à papier, finition, etc.)

Quand utiliser l'impression avancée : - Impression recto verso (recto verso) - Sélection spécifique du bac à papier - Options de finition (agrafage, perforation) - Impression d'étiquettes (par exemple, imprimantes Zebra) - Gestion des couleurs et autres fonctionnalités avancées d'une imprimante.

Configuration du support de l'imprimante

Pour configurer la prise en charge de l'imprimante

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configure remote printing.
3. Dans la boîte de dialogue Configure remote printing (Configurer l'impression à distance) effectuez l'une des actions suivantes :
 - Pour l'impression de base : sélectionnez Activé. Pour utiliser automatiquement l'imprimante par défaut actuelle de l'ordinateur client, sélectionnez Associer l'imprimante locale par défaut à l'hôte distant.
 - Pour l'impression avancée : choisissez Activé, puis sélectionnez Activer l'impression avancée. Pour utiliser automatiquement l'imprimante par défaut actuelle de l'ordinateur client, sélectionnez Associer l'imprimante locale par défaut à l'hôte distant. Une fois la politique activée, vous devrez installer les pilotes d'imprimante correspondants côté hôte et côté client.
 - Pour désactiver l'impression, choisissez Désactivé.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :

- Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
- À l'invite de commande administrative, entrez **gpupdate /force**.

Configuration de la redirection avancée de l'imprimante

Conditions préalables

1. WorkSpaces Agent hôte : version 2.2.0.2116 ou ultérieure
2. Client Windows : version 5.31.0 ou ultérieure
3. Pilotes d'imprimante : les pilotes d'imprimante correspondants doivent être installés à la fois sur le périphérique client WorkSpace et sur le périphérique client

Note

L'impression avancée n'est prise en charge que sur les clients Windows connectés à Windows WorkSpaces. Les clients macOS, Linux et Web utiliseront l'impression de base.

Correspondance des versions du pilote

Lorsque l'impression avancée est sélectionnée, trois modes de validation du pilote sont pris en charge :

Modes de validation du pilote

Mode	Comportement	À utiliser quand
Nom uniquement (par défaut)	Correspond uniquement au nom du pilote, ignore la version	Compatibilité maximale requise
Correspondance partielle	Correspond à la version majeure ou mineure (par exemple, 10.6.x.x)	Équilibre entre compatibilité et fonctionnalités

Mode	Comportement	À utiliser quand
Correspondance exacte	Nécessite une correspondance de version exacte	Imprimantes spécialisées (par exemple, imprimantes d'étiquettes Zebra)

Pour configurer le mode de validation, définissez le nom uniquement, la correspondance partielle ou la correspondance exacte dans le menu déroulant de validation du pilote d'imprimante du GPO.

Note

Lorsque la validation du pilote échoue, on revient WorkSpaces automatiquement à l'impression de base.

Vérifier la configuration

1. Connectez-vous au Workspace.
2. Ouvrez Réglages > Appareils > Imprimantes et scanners.
3. Vérifiez que votre imprimante locale apparaît avec le préfixe « Redirigé ».
4. Imprimez un document de test et cliquez sur Propriétés de l'imprimante pour vérifier que les options avancées sont disponibles.

Résolution des problèmes

Fonctionnalités avancées non disponibles : - Vérifiez que « Activer l'impression avancée » est sélectionnée dans le GPO - Vérifiez que les versions des pilotes correspondent à votre mode de validation - Envisagez d'utiliser le mode de validation partiel au lieu du mode exact. Assurez-vous de redémarrer pour que les modifications apportées au GPO soient prises en compte.

L'imprimante ne s'affiche pas : - Vérifiez que la configuration de l'impression à distance est activée - Assurez-vous que l'imprimante est connectée au périphérique client - Redémarrer Workspace la session

Les tâches d'impression échouent : - Vérifiez les versions des pilotes sur les deux clients et Workspace - Consultez les journaux sur : **C:\ProgramData\Amazon\WSP\Logs\agentssession.log** - Recherchez « L'impression avancée est activée » dans les journaux

Activer la journalisation détaillée : dans la stratégie de groupe, définissez Configurer la verbosité du journal pour le déboguer sous Configuration de l'ordinateur > Politiques > Modèles d'administration > Amazon > WSP.

Configurer la redirection du presse-papiers (copier/coller) pour DCV

Par défaut, WorkSpaces prend en charge la redirection bidirectionnelle (copier/coller) du presse-papiers. Pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité ou configurer la direction dans laquelle la redirection du presse-papiers est autorisée.

Pour configurer la redirection du presse-papiers pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer clipboard redirection.
3. Dans la boîte de dialogue Configurer la redirection du presse-papiers, choisissez Activé ou Désactivé.

Lorsque l'option Configurer la redirection du presse-papiers est activée, les options de redirection du presse-papiers suivantes sont disponibles :

- Choisissez Copier et coller pour autoriser la redirection bidirectionnelle copier-coller dans le presse-papiers.
 - Choisissez Copier uniquement pour autoriser uniquement la copie des données du presse-papiers du serveur vers le presse-papiers du client.
 - Choisissez Coller uniquement pour autoriser uniquement le collage des données du presse-papiers du client vers le presse-papiers du serveur.
4. Choisissez OK.
 5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Limitation connue

Lorsque la redirection du presse-papiers est activée sur le WorkSpace, si vous copiez du contenu supérieur à 890 Ko à partir d'une application Microsoft Office, l'application risque de ralentir ou de ne plus répondre pendant 5 secondes au maximum.

Définissez le délai de reprise de session pour DCV

Lorsque vous perdez la connectivité réseau, votre session WorkSpaces client active est déconnectée. WorkSpaces les applications clientes pour Windows et macOS tentent de reconnecter automatiquement la session si la connectivité réseau est rétablie dans un certain laps de temps. Le délai de reprise de session par défaut est de 20 minutes (1 200 secondes), mais vous pouvez modifier cette valeur pour WorkSpaces que cela soit contrôlé par les paramètres de stratégie de groupe de votre domaine.

Pour définir la valeur de délai d'expiration de reprise de session automatique

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer/désactiver la reconnexion automatique.
3. Dans la boîte de dialogue Activer/désactiver la reconnexion automatique, choisissez Activé, puis définissez le délai de reconnexion (en secondes) souhaité.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection d'entrée vidéo pour DCV

Par défaut, WorkSpaces prend en charge la redirection des données depuis une caméra locale. Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour configurer la redirection d'entrée vidéo pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer/désactiver la redirection d'entrée vidéo.
3. Dans la boîte de dialogue Activer/désactiver la redirection d'entrée vidéo, choisissez Activée ou Désactivée.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection d'entrée audio pour DCV

Par défaut, WorkSpaces prend en charge la redirection des données depuis un microphone local. Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour configurer la redirection d'entrée audio pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer/désactiver la redirection d'entrée audio.
3. Dans la boîte de dialogue Activer/désactiver la redirection d'entrée audio, choisissez Activée ou Désactivée.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :

- Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
- À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection de sortie audio pour DCV

Par défaut, WorkSpaces redirige les données vers un haut-parleur local. Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour configurer la redirection de sortie audio pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer/désactiver la redirection de sortie audio.
3. Dans la boîte de dialogue Activer/désactiver la redirection de sortie audio, choisissez Activée ou Désactivée.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace. Dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions > Redémarrer WorkSpaces.
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Désactiver la redirection de fuseau horaire pour DCV

Par défaut, l'heure dans un espace de travail est définie pour refléter le fuseau horaire du client utilisé pour se connecter au WorkSpace. Ce comportement est contrôlé par redirection de fuseau horaire. Vous pouvez désactiver la direction du fuseau horaire pour diverses raisons. Par exemple :

- Votre entreprise souhaite que tous les employés travaillent dans un fuseau horaire spécifique (même si certains employés sont dans d'autres fuseaux horaires).

- Vous avez planifié des tâches dans un WorkSpace qui sont destinées à être exécutées à une certaine heure dans un fuseau horaire spécifique.
- Vos utilisateurs qui voyagent beaucoup veulent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour désactiver la redirection des fuseaux horaires pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer/désactiver la redirection de fuseau horaire.
3. Dans la boîte de dialogue Activer/désactiver la redirection de fuseau horaire, choisissez Désactivée.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.
6. Réglez le fuseau horaire correspondant WorkSpaces au fuseau horaire souhaité.

Le fuseau horaire du WorkSpaces est désormais statique et ne reflète plus le fuseau horaire des machines clientes.

Configuration des paramètres de sécurité DCV

Pour le DCV, les données en transit sont cryptées à l'aide du cryptage TLS 1.2. Par défaut, tous les chiffrements suivants sont autorisés, et le client et le serveur négocient le chiffrement à utiliser :

- ECDHE-RSA- -GCM- AES128 SHA256
- ECDHE-ECDSA- -GCM- AES128 SHA256

- ECDHE-RSA- -GCM- AES256 SHA384
- ECDHE-ECDSA- -GCM- AES256 SHA384
- ECDHE-RSA- - AES128 SHA256
- ECDHE-RSA- - AES256 SHA384

Pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour modifier le mode de sécurité TLS et pour ajouter de nouvelles suites de chiffrement ou bloquer certaines suites de chiffrement. Une explication détaillée de ces paramètres et des suites de chiffrement prises en charge est fournie dans la boîte de dialogue de stratégie de groupe Configurer les paramètres de sécurité.

Pour configurer les paramètres de sécurité DCV

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez Configurer les paramètres de sécurité.
3. Dans la boîte de dialogue Configurer les paramètres de sécurité, choisissez Activé. Ajoutez les suites de chiffrement que vous souhaitez autoriser et supprimez celles que vous souhaitez bloquer. Pour plus d'informations sur ces paramètres, consultez les descriptions fournies dans la boîte de dialogue Configurer les paramètres de sécurité.
4. Choisissez OK.
5. La modification des paramètres de stratégie de groupe prend effet après la prochaine mise à jour de la WorkSpace stratégie de groupe pour et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Pour redémarrer le WorkSpace, dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces.
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configuration des extensions pour DCV

Par défaut, la prise en charge des WorkSpaces extensions est désactivée. Si nécessaire, vous pouvez configurer vos extensions WorkSpace pour utiliser les extensions de la manière suivante :

- Serveur et client : activer les extensions pour le serveur et le client
- Serveur uniquement : activer les extensions pour le serveur uniquement

- Client uniquement : activer les extensions pour le client uniquement

Pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour configurer l'utilisation des extensions.

Pour configurer les extensions pour DCV

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer les extensions.
3. Dans la boîte de dialogue Configurer les extensions, choisissez Activé, puis définissez l'option souhaitée. Choisissez Client uniquement, Serveur et client ou Serveur uniquement.
4. Choisissez OK.
5. La modification des paramètres de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la Workspace session Workspace et après le redémarrage de celle-ci. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le Workspace. Dans la WorkSpaces console Amazon, sélectionnez le Workspace, puis choisissez Actions, Redémarrer WorkSpaces.
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection par carte à puce pour DCV

Par défaut, Amazon WorkSpaces n'est pas autorisé à prendre en charge l'utilisation de cartes à puce pour l'authentification de pré-session ou pour l'authentification en cours de session. L'authentification de pré-session fait référence à l'authentification par carte à puce effectuée pendant que les utilisateurs se connectent à leur WorkSpaces. L'authentification en cours de session fait référence à l'authentification effectuée après la connexion.

Si nécessaire, vous pouvez activer l'authentification avant et pendant la session pour Windows à l'aide des paramètres WorkSpaces de stratégie de groupe. L'authentification de présession doit également être activée via les paramètres de votre annuaire AD Connector à l'aide de l'action ou de la enable-client-authentication AWS CLI commande d'EnableClientAuthenticationAPI. Pour plus d'informations, consultez [Activer l'authentification par carte à puce pour AD Connector](#) dans le Guide d'administration AWS Directory Service .

 Note

Pour activer l'utilisation de cartes à puce sous Windows WorkSpaces, des étapes supplémentaires sont nécessaires. Pour de plus amples informations, veuillez consulter [Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal](#).

Pour configurer la redirection par carte à puce pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer/désactiver la redirection de carte à puce.
3. Dans la boîte de dialogue Activer/désactiver la redirection de carte à puce, choisissez Activée ou Désactivée.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session. Pour appliquer la modification de la politique de groupe, redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).

WebAuthn (FIDO2) Redirection pour DCV

Par défaut, Amazon WorkSpaces active la WebAuthn redirection, ce qui permet aux utilisateurs d'utiliser leurs clés de sécurité et leurs authenticateurs biométriques FIDO2 compatibles avec les applications qui s'exécutent dans leur environnement. WorkSpace Cette fonctionnalité redirige de manière sécurisée les demandes d'authentification des applications WorkSpace vers l'appareil local de l'utilisateur, offrant ainsi un accès fluide aux méthodes d'authentification, notamment Yubikeys et Windows Hello.

Amazon WorkSpaces prend en charge deux versions de WebAuthn redirection :

- Standard WebAuthn : nécessite une extension de navigateur, prise en charge sous Windows et Linux WorkSpaces, pour les applications basées sur un navigateur
- Amélioré WebAuthn - Aucune extension de navigateur requise, avec prise en charge supplémentaire des applications natives, prise en charge sous Windows WorkSpaces uniquement

WebAuthn Redirection standard

WebAuthn La redirection standard nécessite une extension de navigateur pour faciliter la redirection des WebAuthn invites vers le périphérique client.

Exigences relatives à la version

- Windows WorkSpaces : agent hôte DCV version 2.0.0.1425 ou supérieure
- Versions du client :
 - Client Windows : 5.19.0 ou supérieur
 - Client Mac : 5.19.0 ou supérieur
 - Client Linux : 2024.0 ou supérieur

Navigateurs pris en charge sur WorkSpaces

- Google Chrome 116 et versions ultérieures
- Microsoft Edge 116 et versions ultérieures

WebAuthn Redirection améliorée

WebAuthn La redirection améliorée élimine le besoin d'une extension de navigateur et prend en charge WebAuthn l'authentification dans les applications Windows natives qui prennent en charge WebAuthn l'authentification.

Exigences relatives à la version

- Windows WorkSpaces : agent hôte DCV version 2.1.0.2000 ou supérieure
- Versions du client :
 - Client Windows : 5.29.0 ou supérieur
 - Client Mac : 5.29.0 ou supérieur

Principaux avantages

- Aucune extension de navigateur requise
- Amélioration des performances
- Support pour WebAuthn les applications Windows natives

- Expérience d'authentification fluide dans les navigateurs et les applications de bureau

Navigateurs pris en charge sur WorkSpaces

- Google Chrome 116 et versions ultérieures
- Microsoft Edge 116 et versions ultérieures

Configurer WebAuthn la redirection

Pour configurer WebAuthn la redirection pour Windows WorkSpaces

1. Dans l'éditeur de gestion des politiques de groupe, sélectionnez Configuration de l'ordinateur, Politiques, Modèles d'administration, Amazon et DCV.
2. Ouvrez le paramètre Configurer WebAuthn la redirection.
3. Dans la boîte de dialogue Configurer WebAuthn la redirection, choisissez Activé ou Désactivé.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session. Pour appliquer les modifications de la politique de groupe, redémarrez le WorkSpace en accédant à la WorkSpaces console Amazon et en sélectionnant le WorkSpace. Choisissez ensuite Actions, Redémarrer WorkSpaces.

Note

Ce paramètre de stratégie de groupe active WebAuthn la redirection. La version utilisée (standard ou améliorée) dépend de la version de votre agent hôte et du support du système d'exploitation.

Configuration de la compatibilité des WebAuthn processus

Lorsque WebAuthn la redirection est activée, vous pouvez configurer les applications et les processus autorisés à utiliser la WebAuthn redirection via la liste de compatibilité des WebAuthn processus.

Liste de compatibilité des processus par défaut

Par défaut, les processus suivants sont activés pour la WebAuthn redirection :

```
['chrome.exe', 'msedge.exe', 'island.exe', 'firefox.exe', 'dcvwebauthnnativemsgghost.exe', 'msedgewebview2.exe', 'M
```

Processus requis pour Standard WebAuthn

- `dcvwebauthnnativemsgghost.exe`- Ce processus est requis pour les WebAuthn fonctionnalités standard et doit rester dans la liste de compatibilité lors de l'utilisation de Standard WebAuthn.

Pour configurer la liste WebAuthn de compatibilité des processus

1. Dans l'éditeur de gestion des politiques de groupe, sélectionnez Configuration de l'ordinateur, Politiques, Modèles d'administration, Amazon et DCV.
2. Ouvrez le paramètre Configurer WebAuthn la redirection.
3. Choisissez Enabled (Activé).
4. Dans le champ Liste de compatibilité des WebAuthn processus, spécifiez la liste des noms de processus compatibles avec WebAuthn la redirection.
 - Utiliser la liste par défaut comme point de départ
 - Ajoutez des noms de processus supplémentaires selon les besoins de votre environnement
5. Choisissez OK.
6. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session.

Directives relatives aux listes de compatibilité des processus

- Pour le standard WebAuthn : toujours inclure `dcvwebauthnnativemsgghost.exe` dans la liste
- Applications personnalisées : ajoutez tous les noms de `.exe` processus supplémentaires nécessitant une WebAuthn prise en charge dans votre environnement
- Format : utilisez des noms de processus séparés par des virgules entre crochets, chaque nom de processus étant entre guillemets simples

Exemple de liste de processus personnalisée

```
['chrome.exe', 'msedge.exe', 'firefox.exe', 'dcvwebauthnnativemsgghost.exe', 'msedgewebview2.exe', 'M
```

Transition de la version standard à la version améliorée WebAuthn

Lors de la mise à niveau de Standard WebAuthn vers Enhanced WebAuthn, les utilisateurs devront désinstaller ou désactiver l'extension de navigateur Amazon DCV WebAuthn Redirection qu'ils ont précédemment installée pour Standard WebAuthn avant d'utiliser Enhanced WebAuthn.

Pourquoi cette étape est importante

- Enhanced WebAuthn gère la redirection de manière native sans extensions de navigateur
- Si vous laissez l'extension activée, la WebAuthn redirection standard sera activée par défaut

Installation de l'extension de WebAuthn redirection Amazon DCV (standard WebAuthn uniquement)

Note

Cette section s'applique uniquement à Standard WebAuthn. Enhanced WebAuthn ne nécessite aucune extension de navigateur.

Les utilisateurs devront installer l'extension de WebAuthn redirection Amazon DCV pour utiliser le standard une WebAuthn fois la fonctionnalité activée en effectuant l'une des opérations suivantes :

- Les utilisateurs seront invités à activer l'extension de navigateur dans leur navigateur.

Note

Il s'agit d'une invite de navigation unique. Vos utilisateurs recevront une notification lorsque vous mettrez à jour la version de l'agent DCV vers la version 2.0.0.1425 ou supérieure. Si vos utilisateurs finaux n'ont pas besoin de la WebAuthn redirection, ils peuvent simplement supprimer l'extension du navigateur. Vous pouvez également bloquer l'invite d'installation de l'extension de WebAuthn redirection à l'aide de la politique GPO.

- Vous pouvez forcer l'installation de l'extension de redirection pour vos utilisateurs à l'aide de la politique GPO. Si vous activez la politique GPO, l'extension sera automatiquement installée lorsque vos utilisateurs lanceront les navigateurs compatibles avec accès à Internet.
- Les utilisateurs peuvent installer l'extension manuellement à l'aide des [modules complémentaires Microsoft Edge](#) ou du [Chrome Web Store](#).

Comprendre la messagerie native des extensions de WebAuthn redirection

WebAuthn la redirection dans les navigateurs Chrome et Edge utilise une extension de navigateur et un hôte de messagerie natif. L'hôte de messagerie natif est un composant qui permet la communication entre l'extension et l'application hôte. Dans une configuration classique, tous les hôtes de messagerie natifs sont autorisés par défaut par le navigateur. Cependant, vous pouvez choisir d'utiliser une liste de blocage de messagerie native, où la valeur * signifie que tous les hôtes de messagerie natifs sont refusés sauf autorisation explicite. Dans ce cas, vous devez activer l'hôte de messagerie natif Amazon WebAuthn DCV Redirection en spécifiant explicitement la valeur `com.dcv.webauthnredirection.nativemessagehost` dans la liste d'autorisation.

Pour plus d'informations, suivez les instructions de votre navigateur :

- Pour Google Chrome, consultez la section [Hôtes autorisés à utiliser la messagerie native](#).
- Pour Microsoft Edge, voir [Messagerie native](#).

Gérer et installer l'extension de navigateur à l'aide de la stratégie de groupe

Vous pouvez installer l'extension de WebAuthn redirection Amazon DCV à l'aide de la stratégie de groupe, soit de manière centralisée depuis votre domaine pour les hôtes de session joints à un domaine Active Directory (AD), soit en utilisant l'éditeur de stratégie de groupe local pour chaque hôte de session. Ce processus changera en fonction du navigateur que vous utilisez.

Pour Microsoft Edge

1. Téléchargez et installez le [modèle d'administration Microsoft Edge](#).
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc).
3. Agrandissez la forêt (Forêt : **FQDN**).
4. Développez Domaines.
5. Développez votre FQDN (par exemple, `example.com`).
6. Développez Objets de stratégie de groupe.
7. Sélectionnez Stratégie de domaine par défaut, ouvrez le menu contextuel (via un clic droit) et choisissez Modifier.
8. Choisissez la configuration de l'ordinateur, les modèles d'administration, Microsoft Edge et les extensions

9. Ouvrez Configurer les paramètres de gestion des extensions et définissez-les sur Activé.
10. Sous Configurer les paramètres de gestion des extensions, entrez les informations suivantes :

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":  
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/  
extensionwebstorebase/v1/crx"}}
```

11. Choisissez OK.
12. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session. Pour appliquer les modifications de la politique de groupe, redémarrez le WorkSpace en accédant à la WorkSpaces console Amazon et en sélectionnant le WorkSpace. Choisissez ensuite Actions, Reboot WorkSpaces).

Note

Vous pouvez bloquer l'installation de l'extension en appliquant le paramètre de gestion de configuration suivant :

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":  
{"installation_mode":"blocked","update_url":"https://edge.microsoft.com/  
extensionwebstorebase/v1/crx"}}
```

Pour Google Chrome

1. Téléchargez et installez le modèle d'administration de Google Chrome. Pour plus d'informations, voir [Définir les règles du navigateur Chrome en mode géré PCs](#).
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc).
3. Agrandissez la forêt (Forêt : **FQDN**).
4. Développez Domaines.
5. Développez votre FQDN (par exemple, exemple.com).
6. Développez Objets de stratégie de groupe.
7. Sélectionnez Stratégie de domaine par défaut, ouvrez le menu contextuel (via un clic droit) et choisissez Modifier.

8. Choisissez la configuration de l'ordinateur, les modèles d'administration, Google Chrome et les extensions
9. Ouvrez Configurer les paramètres de gestion des extensions et définissez-les sur Activé.
10. Sous Configurer les paramètres de gestion des extensions, entrez les informations suivantes :

```
{"mmioagbgnbojdbcjoddlefhmccocfpmn":  
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/  
service/update2/crx"}}
```

11. Choisissez OK.
12. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session. Pour appliquer les modifications de la politique de groupe, redémarrez le WorkSpace en accédant à la WorkSpaces console Amazon et en sélectionnant le WorkSpace. Choisissez ensuite Actions, Reboot WorkSpaces).

Note

Vous pouvez bloquer l'installation de l'extension en appliquant le paramètre de gestion de configuration suivant :

```
{"mmioagbgnbojdbcjoddlefhmccocfpmn":  
{ "installation_mode":"blocked","update_url":"https://clients2.google.com/  
service/update2/crx"}}
```

Configurer la redirection WebRTC pour DCV

La redirection WebRTC améliore la communication en temps réel en déchargeant le traitement audio et vidéo WorkSpaces de votre client local, ce qui améliore les performances et réduit le temps de latence. Cependant, la redirection WebRTC n'est pas universelle et nécessite que les fournisseurs d'applications tiers développent des intégrations spécifiques avec WorkSpaces. Par défaut, la redirection WebRTC n'est pas activée. Pour utiliser la redirection WebRTC, assurez-vous de ce qui suit :

- Intégration avec des fournisseurs d'applications tiers
- WorkSpaces les extensions sont activées via les paramètres de stratégie de groupe
- La redirection WebRTC est activée

- L'extension de navigateur de redirection WebRTC est installée et activée

Note

Cette redirection est implémentée en tant qu'extension et vous oblige à activer la prise en charge des WorkSpaces extensions à l'aide des paramètres de stratégie de groupe. Si les extensions sont désactivées, la redirection WebRTC ne fonctionnera pas.

Exigences

La redirection WebRTC pour DCV nécessite les éléments suivants :

- Agent hôte DCV version 2.0.0.1622 ou supérieure
- WorkSpaces clients :
 - Windows 5.21.0 ou supérieur
 - Client Web
- Navigateurs Web installés sur votre ordinateur WorkSpaces exécutant l'extension de redirection Amazon DCV WebRTC :
 - Google Chrome 116 et versions ultérieures
 - Microsoft Edge 116 et versions ultérieures

Activation ou désactivation de la redirection WebRTC pour Windows WorkSpaces

Si nécessaire, vous pouvez activer ou désactiver la prise en charge de la redirection WebRTC pour WorkSpaces Windows à l'aide des paramètres de stratégie de groupe. Si vous désactivez ou ne configurez pas ce paramètre, la redirection WebRTC sera désactivée.

Lorsque cette fonctionnalité est activée, les applications Web intégrées à Amazon WorkSpaces pourront rediriger les appels d'API WebRTC vers le client local.

Pour configurer la redirection WebRTC pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer la redirection WebRTC.
3. Dans la boîte de dialogue Configurer la redirection WebRTC, choisissez Activé ou Désactivé.

4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session. Pour appliquer les modifications de la politique de groupe, redémarrez le WorkSpace en accédant à la WorkSpaces console Amazon et en sélectionnant le WorkSpace. Choisissez ensuite Actions, Reboot WorkSpaces).

Installation de l'extension de redirection WebRTC Amazon DCV

Les utilisateurs installent l'extension de redirection WebRTC Amazon DCV pour utiliser la redirection WebRTC une fois la fonctionnalité activée en effectuant l'une des opérations suivantes :

- Les utilisateurs seront invités à activer l'extension de navigateur dans leur navigateur.

Note

En tant qu'invite unique du navigateur, les utilisateurs reçoivent une notification lorsque vous activez la redirection WebRTC.

- Vous pouvez forcer l'installation de l'extension de redirection pour les utilisateurs à l'aide de la politique GPO suivante. Si vous activez la politique GPO, l'extension sera automatiquement installée lorsque les utilisateurs lanceront les navigateurs compatibles avec accès à Internet.
- Les utilisateurs peuvent installer l'extension manuellement à l'aide des [modules complémentaires Microsoft Edge](#) ou du [Chrome Web Store](#).

Gérer et installer l'extension de navigateur à l'aide de la stratégie de groupe

Vous pouvez installer l'extension de redirection WebRTC Amazon DCV à l'aide de la stratégie de groupe, soit de manière centralisée depuis votre domaine, pour les hôtes de session joints à un domaine Active Directory (AD), soit en utilisant l'éditeur de stratégie de groupe local pour chaque hôte de session. Ce processus sera différent selon le navigateur que vous utilisez.

Pour Microsoft Edge

1. Téléchargez et installez le [modèle d'administration Microsoft Edge](#).
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc).
3. Agrandissez la forêt (Forêt : **FQDN**).

4. Développez Domaines.
5. Développez votre FQDN (par exemple, `exemple.com`).
6. Développez Objets de stratégie de groupe.
7. Sélectionnez Stratégie de domaine par défaut, ouvrez le menu contextuel (via un clic droit) et choisissez Modifier.
8. Choisissez la configuration de l'ordinateur, les modèles d'administration, Microsoft Edge et les extensions
9. Ouvrez Configurer les paramètres de gestion des extensions et définissez-les sur Activé.
10. Sous Configurer les paramètres de gestion des extensions, entrez les informations suivantes :

```
{"kjbkkjjiecchbcdoolhghffghfjnbhef":  
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/  
extensionwebstorebase/v1/crx"}}
```

11. Choisissez OK.
12. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session. Pour appliquer les modifications de la politique de groupe, redémarrez le WorkSpace en accédant à la WorkSpaces console Amazon et en sélectionnant le WorkSpace. Choisissez ensuite Actions, Reboot WorkSpaces).

Note

Vous pouvez bloquer l'installation de l'extension en appliquant le paramètre de gestion de configuration suivant :

```
{"kjbkkjjiecchbcdoolhghffghfjnbhef":  
{"installation_mode":"blocked","update_url":"https://edge.microsoft.com/  
extensionwebstorebase/v1/crx"}}
```

Pour Google Chrome

1. Téléchargez et installez le modèle d'administration de Google Chrome. Pour plus d'informations, voir [Définir les règles du navigateur Chrome en mode géré PCs](#).
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (`gpmc.msc`).

3. Agrandissez la forêt (Forêt : **FQDN**).
4. Développez Domaines.
5. Développez votre FQDN (par exemple, `exemple.com`).
6. Développez Objets de stratégie de groupe.
7. Sélectionnez Stratégie de domaine par défaut, ouvrez le menu contextuel (via un clic droit) et choisissez Modifier.
8. Choisissez la configuration de l'ordinateur, les modèles d'administration, Google Chrome et les extensions
9. Ouvrez Configurer les paramètres de gestion des extensions et définissez-les sur Activé.
10. Sous Configurer les paramètres de gestion des extensions, entrez les informations suivantes :

```
{"diilpfplcnhehakckkpmcmibmhbingnd":  
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/  
service/update2/crx"}}
```

11. Choisissez OK.
12. La modification du paramètre de stratégie de groupe prend effet après le redémarrage de la WorkSpace session. Pour appliquer les modifications de la politique de groupe, redémarrez le WorkSpace en accédant à la WorkSpaces console Amazon et en sélectionnant le WorkSpace. Choisissez ensuite Actions, Reboot WorkSpaces).

Note

Vous pouvez bloquer l'installation de l'extension en appliquant le paramètre de gestion de configuration suivant :

```
{"diilpfplcnhehakckkpmcmibmhbingnd":  
{ "installation_mode":"blocked","update_url":"https://clients2.google.com/  
service/update2/crx"}}
```

Configurer la session de déconnexion lors du verrouillage de l'écran pour DCV

Si nécessaire, vous pouvez déconnecter les WorkSpaces sessions des utilisateurs lorsque l'écran de verrouillage Windows est détecté. Pour se reconnecter depuis le WorkSpaces client, les

utilisateurs peuvent utiliser leur mot de passe ou leur carte à puce pour s'authentifier, selon le type d'authentification activé pour eux. WorkSpaces

Par défaut, ce paramètre de stratégie de groupe est désactivé. Si nécessaire, vous pouvez activer la déconnexion de la session lorsque l'écran de verrouillage de Windows est détecté pour Windows à l'aide WorkSpaces des paramètres de stratégie de groupe.

 Note

- Ce paramètre de stratégie de groupe s'applique à la fois aux sessions utilisant l'authentification par mot de passe et à celles utilisant l'authentification par carte à puce.
- Pour activer l'utilisation de cartes à puce sous Windows WorkSpaces, des étapes supplémentaires sont nécessaires. Pour de plus amples informations, veuillez consulter [Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal](#).

Pour configurer la session de déconnexion lors du verrouillage de l'écran pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer/désactiver la déconnexion de session au verrouillage de l'écran.
3. Dans la boîte de dialogue Activer/désactiver la déconnexion de session au verrouillage de l'écran, choisissez Activée ou Désactivée.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la protection de capture d'écran pour DCV

La protection de capture d'écran empêche les captures d'écran, les enregistrements d'écran et le partage d'écran de WorkSpaces sessions à partir d'outils clients locaux. Lorsque cette option est

activée, les tentatives de capture de contenu d'écran depuis le côté client affichent l'arrière-plan ou un rectangle noir, ce qui permet de protéger les informations sensibles contre l'exfiltration.

Exigences

La protection des captures d'écran pour DCV nécessite les éléments suivants :

- Agent hôte DCV version 2.2.0.2116 ou supérieure
- WorkSpaces clients :
 - Windows 5.30.2 ou supérieur
 - macOS 5.30.2 ou supérieur

Note

- Cette fonctionnalité n'est pas prise en charge sur les clients Linux, Web Access ou le protocole PCo IP.
- La protection s'applique aux captures initiées depuis l'appareil client. Les utilisateurs peuvent toujours prendre des captures d'écran à partir de WorkSpace lui-même.
- Cette fonctionnalité n'est pas compatible avec le partage d'écran sur MS Teams.

Limitations connues

- Cette fonctionnalité ne peut pas empêcher les captures d'écran physiques par l'appareil photo.
- Cette fonctionnalité ne protège pas contre les connexions RDP directes au serveur hôte.
- La fonctionnalité ne protège pas contre les tentatives de capture initiées depuis WorkSpace elle-même, notamment les fonctionnalités de partage d'écran des outils de collaboration et de chat.
- Toutes les méthodes de capture sont bloquées lorsqu'elles sont activées (le blocage sélectif n'est pas disponible).
- La fenêtre du client macOS peut être grisée si la fonctionnalité est activée et qu'une capture vidéo est tentée (par exemple en essayant de partager l'écran de la fenêtre du client).

Pour configurer la protection contre les captures d'écran pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.

2. Ouvrez le paramètre Configurer la protection par capture d'écran.
3. Dans la boîte de dialogue Configurer la protection par capture d'écran, choisissez Activé ou Désactivé.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - a. Redémarrez le WorkSpace (dans la WorkSpaces console, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - b. À l'invite de commande administrative, entrez `gpupdate /force`.

Configurer le pilote d'affichage indirect (IDD) pour DCV

Par défaut, WorkSpaces prend en charge l'utilisation du pilote d'affichage indirect (IDD). Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour configurer le pilote d'affichage indirect (IDD) pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Activer le pilote d'affichage AWS indirect.
3. Dans la boîte de dialogue Activer le pilote d'affichage AWS indirect, choisissez Activé ou Désactivé.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - a. Redémarrez le WorkSpace (dans la WorkSpaces console, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - b. À l'invite de commande administrative, entrez `gpupdate /force`.

Configuration des paramètres d'affichage pour DCV

WorkSpaces vous permet de configurer différents paramètres d'affichage, notamment la fréquence d'images maximale, la qualité d'image minimale, la qualité d'image maximale et le codage YUV. Ajustez ces paramètres en fonction de la qualité d'image, de la réactivité et de la précision des couleurs dont vous avez besoin.

Par défaut, la valeur de fréquence d'images maximale est 25. La valeur de fréquence d'images maximale indique le nombre maximal d'images par seconde autorisé. La valeur 0 indique l'absence de limite.

Par défaut, la valeur de qualité d'image minimale est 30. La qualité d'image minimale peut être optimisée pour une meilleure réactivité ou une meilleure qualité d'image. Pour une réactivité optimale, réduisez la qualité minimale. Pour une qualité optimale, augmentez la qualité minimale.

- Les valeurs idéales pour une réactivité optimale se situent entre 30 et 90.
- Les valeurs idéales pour une qualité optimale se situent entre 60 et 90.

Par défaut, la valeur de qualité d'image maximale est 80. La qualité d'image maximale n'affecte pas la réactivité ni la qualité de l'image, mais définit une valeur maximale pour limiter l'utilisation du réseau.

Par défaut, le codage de l'image est défini sur YUV420. La sélection d'Activer le YUV444 YUV444 codage permet de coder pour obtenir une haute précision des couleurs.

Pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour configurer la fréquence d'images maximale, la qualité d'image minimale et les valeurs de qualité d'image maximales.

Pour configurer les paramètres d'affichage pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer les paramètres d'affichage.
3. Dans la boîte de dialogue Configurer les paramètres d'affichage, choisissez Activé, puis définissez les valeurs de fréquence d'images maximale (images par seconde), de qualité d'image minimale et de qualité d'image maximale aux niveaux souhaités.
4. Choisissez OK.

5. La modification des paramètres de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la WorkSpace session WorkSpace et après le redémarrage de celle-ci. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez la WorkSpace WorkSpaces console Amazon, sélectionnez la WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configuration VSync pour le pilote d'affichage AWS virtuel uniquement pour DCV

Par défaut, WorkSpaces prend en charge l'utilisation de la VSync fonctionnalité pour le AWS pilote d'affichage virtuel uniquement. Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour configurer VSync pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez la VSync fonction Activer du paramètre AWS Virtual Display Only Driver.
3. Dans la VSync fonction Activer de la boîte de dialogue AWS Virtual Display Only Driver, choisissez Activé ou Désactivé.
4. Choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications apportées à la politique de groupe, procédez comme suit :
 - a. Redémarrez le WorkSpace en effectuant l'une des opérations suivantes :
 - i. Option 1 — Dans la WorkSpaces console, choisissez celui que WorkSpace vous souhaitez redémarrer. Choisissez ensuite Actions, Redémarrer WorkSpaces.
 - ii. Option 2 — Dans une invite de commande administrative, entrez **gpupdate /force**.
 - b. Reconnectez-vous au WorkSpace afin d'appliquer le réglage.
 - c. Redémarrez l'espace de travail.

Configuration de la verbosité des journaux pour DCV

Par défaut, le niveau de verbosité du journal pour DCV WorkSpaces est défini sur Info. Vous pouvez définir les niveaux de détail des journaux, du moins détaillé au plus détaillé, comme indiqué ici :

- Erreur : le moins détaillé
- Avertissement
- Infos : par défaut
- Déboguer : le plus détaillé

Pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour configurer les niveaux de verbosité des journaux.

Pour configurer les niveaux de verbosité des journaux pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer le niveau de détail des journaux.
3. Dans la boîte de dialogue Configurer le niveau de détail des journaux, choisissez Activé, puis définissez le niveau détail sur Déboguer, Erreur, Infos ou Avertissement.
4. Choisissez OK.
5. La modification des paramètres de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la Workspace session Workspace et après le redémarrage de celle-ci. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le Workspace. Dans la WorkSpaces console Amazon, sélectionnez le Workspace, puis choisissez Actions, Redémarrer WorkSpaces.
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer le délai de déconnexion en cas d'inactivité pour le DCV

WorkSpaces vous permet de configurer la durée pendant laquelle un utilisateur peut rester inactif lorsqu'il est connecté à un Workspace, avant d'être déconnecté. Voici des exemples d'entrées relatives à l'activité des utilisateurs :

- Événements liés au clavier

- Événements liés à la souris (mouvement du curseur, défilement, clic)
- Événements Stylus
- Événements tactiles (toucher des écrans tactiles, des tablettes)
- Événements sur manette de jeu
- Opérations de stockage de fichiers (chargements, téléchargements, création de répertoires, éléments de liste)
- Diffusion par webcam

L'entrée audio, la sortie audio et le changement de pixels ne sont pas considérés comme des activités de l'utilisateur.

Lorsque vous activez le délai de déconnexion en cas d'inactivité, vous pouvez éventuellement informer votre utilisateur que sa session se déconnectera dans le délai configuré, à moins qu'il ne s'engage.

Par défaut, le délai de déconnexion en cas d'inactivité est désactivé, la valeur du délai d'expiration est définie sur 0 minute et la notification est désactivée. Si vous activez ce paramètre de stratégie, la valeur du délai de déconnexion en mode veille est par défaut de 60 minutes et la valeur d'avertissement de déconnexion en mode veille est par défaut de 60 secondes. Pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour configurer cette fonctionnalité.

Pour configurer le délai de déconnexion en cas d'inactivité pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer le délai de déconnexion en mode veille.
3. Dans la boîte de dialogue Configurer le délai de déconnexion en mode veille, choisissez Activé, puis définissez la valeur du délai de déconnexion souhaitée (en minutes), et éventuellement la valeur du délai d'avertissement (en secondes).
4. Choisissez Appliquer, OK.
5. La modification du paramètre de stratégie de groupe prend effet immédiatement après l'application de la modification.

Configurer le transfert de fichiers pour DCV

Par défaut, Amazon WorkSpaces désactive la fonction de transfert de fichiers. Vous pouvez l'activer pour permettre aux utilisateurs de charger et de télécharger des fichiers entre leur ordinateur local et leur WorkSpaces session. Les fichiers seront enregistrés dans un dossier My Storage au WorkSpaces cours de la session.

Pour activer le transfert de fichiers pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer le stockage de session.
3. Dans la boîte de dialogue Configurer le stockage de session, sélectionnez Activé.
4. (Facultatif) Spécifiez un dossier pour le stockage de session (par exemple, `c:/session-storage`). S'il n'est pas spécifié, le dossier par défaut pour le stockage des sessions sera le dossier d'accueil.
5. Vous pouvez configurer votre fichier à l' WorkSpaces aide de l'une des options de transfert de fichiers suivantes :
 - Choisissez **Download and Upload** d'autoriser le transfert de fichiers bidirectionnel.
 - Choisissez **Upload Only** d'autoriser uniquement le téléchargement de fichiers depuis un ordinateur local vers votre WorkSpaces session.
 - Choisissez **Download Only** d'autoriser uniquement le téléchargement de fichiers depuis votre WorkSpaces session vers un ordinateur local.
6. Choisissez OK.
7. La modification des paramètres de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la Workspace session Workspace et après le redémarrage de celle-ci. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le Workspace. Dans la WorkSpaces console Amazon, sélectionnez le Workspace, puis choisissez Actions, Redémarrer WorkSpaces.
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection USB pour DCV

Présentation de

À partir de la version 2.2.0.2047, Amazon WorkSpaces prend en charge la redirection USB générique pour Windows basé sur DCV WorkSpaces, permettant aux utilisateurs d'accéder aux périphériques USB locaux au sein de leurs environnements de bureau virtuels. Cette fonctionnalité complète les solutions de redirection optimisées existantes pour des classes d'appareils spécifiques.

Note

Amazon recommande d'utiliser la redirection générique uniquement pour les appareils sur lesquels aucune solution de redirection optimisée n'est disponible. Lorsqu'elles sont disponibles, les solutions de redirection optimisées offrent de meilleures performances.

Conditions préalables

- Windows WorkSpaces utilisant le protocole DCV 2.2.0.2047 ou version ultérieure
- Dernière version du client WorkSpaces Windows (version 5.30.0 ou ultérieure)
- Accès administratif pour configurer les paramètres de stratégie de groupe

Configuration

La redirection USB est désactivée par défaut. Vous pouvez activer cette fonctionnalité à l'aide des objets de stratégie de groupe (GPO). Une fois la fonctionnalité activée, vous pouvez ajouter des appareils à la liste des appareils autorisés à des fins de redirection. Par défaut, les appareils ne figurant pas dans la liste des appareils autorisés ne sont pas disponibles pour la redirection.

Configuration de la politique de groupe

Pour configurer la redirection USB pour DCV à l'aide de la stratégie de groupe

1. Connect à Windows WorkSpaces.
2. Copiez les fichiers du modèle de politique (`wsp.admxetwsp.adml`) depuis le `C:\Program Files\Amazon\WSP` dossier.
3. Collez `wsp.admx` dans le `C:\Windows\PolicyDefinitions` dossier.
4. Collez `wsp.adml` dans le `C:\Windows\PolicyDefinitions\en-US` dossier.

5. Lancez Local GPO Editor (gpedit.msc).
6. Accédez à Politique informatique locale > Configuration de l'ordinateur > Modèles d'administration > Amazon > WSP.
7. Configurez Activer/désactiver l'USB dans les paramètres WSP.
8. Choisissez Activé pour activer la redirection USB.

Note

Les modifications apportées à ce paramètre sont appliquées lors de la connexion suivante.

Gestion des appareils

Une fois la redirection USB activée, vous pouvez configurer la liste des appareils autorisés dans le GPO pour ajouter les périphériques que vous souhaitez prendre en charge pour la redirection.

Configuration de la liste d'appareils autorisés

La redirection USB suit une position de sécurité par défaut interdisant tout. Les administrateurs doivent autoriser explicitement les appareils en les ajoutant à la liste d'autorisation du GPO en utilisant le format suivant :

```
Name, Base class, Subclass, Protocol, Id Vendor, Id Product, Support Auto-share, Skip  
reset  
// Use * to skip any values
```

Exemples :

Ajouter un appareil avec un ID/Product identifiant fournisseur :

```
Credit Card Reader, *, *, *, 0x0483, 0x2016, 1, 0  
// Allows Credit Card Reader with VID 0x0483 and PID 0x2016 with auto-share support
```

Ajouter un appareil avec une classe/sous-classe :

```
3D Mouse Devices, 03, 01, *, *, *, 1, 0  
// Allows all 3D mice using HID class (03), boot interface subclass (01), with auto-  
share support
```

 Note

Testez la compatibilité et les performances des appareils avant de les ajouter à la liste des appareils autorisés.

Considérations de sécurité

Bonnes pratiques

- Utilisez des méthodes de redirection dédiées lorsqu'elles sont disponibles pour les appareils pris en charge afin d'optimiser les performances et la compatibilité. Par exemple, pour des clés de sécurité telles que YubiKey, utilisez plutôt WebAuthn la redirection.
- Implémentez des listes d'appareils autorisées strictes.
- Surveillez l'accès aux appareils par le biais de journaux d'audit.
- Évaluez les implications en matière de sécurité des données avant d'autoriser de nouveaux appareils.

Configuration de la résolution de la webcam pour DCV

Utilisez ce paramètre pour configurer les paramètres de résolution de la webcam. Si vous activez ce paramètre de stratégie, vous pouvez spécifier :

- Résolution maximale de la webcam : Ceci indique la résolution maximale de la webcam qui peut être sélectionnée parmi les résolutions fournies. Si cette valeur est absente ou (0, 0), la valeur par défaut est utilisée.
- Résolution de webcam préférée : Ceci indique la résolution de webcam préférée parmi les résolutions fournies par le client. Si la résolution spécifiée n'est pas prise en charge, la résolution correspondante la plus proche est sélectionnée. Si cette valeur est absente ou (0, 0), la valeur par défaut est utilisée.

Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les résolutions par défaut sont utilisées.

Pour configurer la résolution de la webcam pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer la résolution de la webcam.
3. Dans la boîte de dialogue Configurer la résolution de la webcam, choisissez Activé, puis définissez la Résolution maximale de la webcam (en pixels) Résolution and/or préférée de la webcam (en pixels).
4. Choisissez OK.
5. La modification des paramètres de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la Workspace session Workspace et après le redémarrage de celle-ci. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le Workspace. Dans la WorkSpaces console Amazon, sélectionnez le Workspace, puis choisissez Actions, Redémarrer WorkSpaces.
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configuration de l'utilisation de la disposition du clavier du serveur pour DCV

Ce paramètre détermine s'il faut utiliser la disposition de clavier côté serveur pour l'interprétation des touches, par opposition à la disposition de clavier côté client par défaut. Les modifications apportées à ce paramètre sont appliquées lors de la connexion suivante. Pour plus d'informations sur la manipulation du clavier, consultez le guide de WorkSpaces l'utilisateur Amazon.

Si vous activez ce paramètre de stratégie, vous pouvez choisir l'une des options suivantes :

- Toujours désactivé : utilisez toujours la mise en page du client
- Always On - Utilisez toujours la disposition du serveur

Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'option Toujours désactivé est utilisée.

 Note

Cette fonctionnalité est prise en charge dans le client Amazon WorkSpaces Windows version 5.29.2 ou ultérieure, et dans le client Amazon WorkSpaces macOS version 5.30.0 ou ultérieure.

Pour configurer l'utilisation de la disposition du clavier du serveur pour Windows WorkSpaces

1. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
2. Ouvrez le paramètre Configurer l'utilisation de la disposition du clavier du serveur.
3. Dans la boîte de dialogue Configurer l'utilisation de la disposition du clavier du serveur, choisissez Activé, puis définissez l'option de disposition du clavier du serveur.
4. Choisissez OK.
5. La modification des paramètres de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la Workspace session Workspace et après le redémarrage de celle-ci. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le Workspace. Dans la WorkSpaces console Amazon, sélectionnez le Workspace, puis choisissez Actions, Redémarrer WorkSpaces.
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Installation du modèle administratif de stratégie de groupe pour PCo IP

Pour utiliser les paramètres de stratégie de groupe spécifiques à Amazon WorkSpaces lors de l'utilisation du protocole PCo IP, vous devez ajouter le modèle d'administration de stratégie de groupe adapté à la version de l'agent PCo IP (32 bits ou 64 bits) utilisée pour votre WorkSpaces.

 Note

Si vous utilisez à la fois WorkSpaces des agents 32 bits et 64 bits, vous pouvez utiliser les modèles administratifs de stratégie de groupe pour les agents 32 bits, et vos paramètres de stratégie de groupe seront appliqués aux agents 32 bits et 64 bits. Lorsque vous WorkSpaces

utilisez tous l'agent 64 bits, vous pouvez passer au modèle d'administration pour les agents 64 bits.

Pour déterminer si vous WorkSpaces disposez de l'agent 32 bits ou de l'agent 64 bits

1. Connectez-vous à un Workspace, puis ouvrez le Gestionnaire des tâches en choisissant Afficher, Envoyer Ctrl + Alt + Supprimer ou en cliquant avec le bouton droit sur la barre des tâches et en choisissant Gestionnaire des tâches.
2. Dans le Gestionnaire des tâches, accédez à l'onglet Détails, cliquez avec le bouton droit sur les en-têtes de colonne, puis choisissez Sélectionner des colonnes.
3. Dans la boîte de dialogue Sélectionner les colonnes, sélectionnez Plateforme, puis cliquez sur OK.
4. Dans l'onglet Détails `pcoip_agent.exe`, recherchez puis vérifiez sa valeur dans la colonne Plateforme pour déterminer si l'agent PCo IP est 32 bits ou 64 bits. (Vous pouvez voir un mélange de WorkSpaces composants 32 bits et 64 bits ; c'est normal.)

Installation du modèle d'administration de stratégie de groupe pour PCo IP (32 bits)

Pour utiliser les paramètres de stratégie de groupe spécifiques à WorkSpaces l'utilisation du protocole PCoIP avec l'agent PCoIP 32 bits, vous devez installer le modèle d'administration de stratégie de groupe pour PCoIP. Effectuez la procédure suivante sur une instance d'administration d'annuaire Workspace ou Amazon EC2 jointe à votre annuaire.

Pour plus d'informations sur l'utilisation des fichiers .adm, consultez [Recommandations pour la gestion des fichiers de modèles d'administration de stratégies de groupe \(.adm\)](#) dans la documentation Microsoft.

Pour installer le modèle d'administration de stratégie de groupe pour PCo IP

1. À partir d'un système Windows en cours d'exécution Workspace, faites une copie du `pcoip.adm` fichier dans le `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` répertoire.
2. Sur une administration d'annuaire Workspace ou sur une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (`gpmc.msc`) et accédez à l'unité organisationnelle de votre domaine qui contient vos comptes de WorkSpaces machines.

3. Ouvrez le menu contextuel (clic droit) de l'unité d'organisation de compte machine et choisissez Create a GPO in this domain, and link it here.
4. Dans la boîte de dialogue Nouveau GPO, entrez un nom descriptif pour le GPO, tel que WorkSpaces Machine Policies, et laissez Source Starter GPO défini sur (none). Choisissez OK.
5. Ouvrez le menu contextuel (clic droit) correspondant au nouvel objet stratégie de groupe et choisissez Modifier.
6. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration, Politiques et Administrative Templates. Choisissez Action, Add/Remove Templates dans le menu principal.
7. Dans la boîte de dialogue Add/Remove Templates, choisissez Add, sélectionnez le fichier pcoip.adm copié précédemment, puis choisissez Open, Close.
8. Fermez l'éditeur de gestion des stratégies de groupe. Vous pouvez désormais utiliser cet objet Stratégie de groupe pour modifier les paramètres de stratégie de groupe qui sont spécifiques à WorkSpaces.

Pour vérifier que le fichier de modèle d'administration est correctement installé

1. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc), naviguez jusqu'au WorkSpaces GPO pour vos WorkSpaces comptes de machine et sélectionnez-le. Choisissez Action, Edit dans le menu principal.
2. Dans l'éditeur de gestion des stratégies de groupe, sélectionnez Configuration de l'ordinateur, Politiques, Modèles d'administration, Modèles d'administration classiques et Variables de session PCo IP.
3. Vous pouvez désormais utiliser cet objet de politique de groupe concernant les variables de session PCo IP pour modifier les paramètres de stratégie de groupe spécifiques à Amazon WorkSpaces lors de l'utilisation de l' PCoadresse IP.

 Note

Pour permettre à l'utilisateur de remplacer vos paramètres, choisissez Paramètres administrateur par défaut remplaçables. Sinon, choisissez Paramètres administrateur par défaut non remplaçables.

Installation du modèle d'administration de stratégie de groupe pour PCo IP (64 bits)

Pour utiliser les paramètres de stratégie de groupe spécifiques à l' WorkSpaces utilisation du protocole PCo IP, vous devez ajouter le modèle d'administration de stratégie de groupe PCoIP .admx et PCoIP .adm1 les fichiers PCo IP dans le magasin central du contrôleur de domaine de votre WorkSpaces répertoire. Pour plus d'informations sur les fichiers .admx et .adm1, consultez [Comment créer et gérer le magasin central des modèles d'administration de stratégie de groupe dans Windows](#).

La procédure suivante décrit comment créer le magasin central et y ajouter les fichiers de modèles d'administration. Effectuez la procédure suivante sur une instance d'administration d'annuaire WorkSpace ou Amazon EC2 jointe à votre WorkSpaces annuaire.

Pour installer les fichiers modèles d'administration de stratégie de groupe pour PCo IP

1. À partir d'un système Windows en cours d'exécution WorkSpace, faites une copie PCoIP .adm1 des fichiers PCoIP .admx et du C:\Program Files\Teradici\PCoIP Agent \configuration\policyDefinitions répertoire. Le fichier PCoIP .adm1 se trouve dans le sous-dossier en-US de ce répertoire.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces répertoire, ouvrez l'Explorateur de fichiers Windows et, dans la barre d'adresse, entrez le nom de domaine complet (FQDN) de votre organisation, tel que. \\example.com
3. Ouvrez le dossier sysvol.
4. Ouvrez le dossier nommé *FQDN*.
5. Ouvrez le dossier Politiques. Vous devez maintenant être ici : *FQDN*\sysvol \ *FQDN*\Politiques.
6. S'il n'existe pas déjà, créez un dossier nommé PolicyDefinitions.
7. Ouvrez le dossier PolicyDefinitions.
8. Copiez le fichier PCoIP .admx dans le dossier *FQDN*\sysvol \ *FQDN*\Politiques \PolicyDefinitions.
9. Créez un dossier nommé en-US dans le dossier PolicyDefinitions.
10. Ouvrez le dossier en-US.
11. Copiez le fichier PCoIP .adm1 dans le dossier *FQDN*\sysvol \ *FQDN*\Politiques \PolicyDefinitions\en-US.

Pour vérifier que les fichiers du modèle d'administration sont correctement installés

1. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc).
2. Agrandissez la forêt (Forêt : **FQDN**).
3. Développez Domaines.
4. Développez votre FQDN (par exemple, `example.com`).
5. Développez Objets de stratégie de groupe.
6. Sélectionnez Stratégie de domaine par défaut, ouvrez le menu contextuel (via un clic droit) et choisissez Modifier.

 Note

Si le domaine sous-jacent WorkSpaces est un AWS Managed Microsoft AD annuaire, vous ne pouvez pas utiliser la politique de domaine par défaut pour créer votre GPO. Au lieu de cela, vous devez créer et lier le GPO sous le conteneur de domaine disposant de privilèges délégués.

Lorsque vous créez un répertoire avec AWS Managed Microsoft AD, Directory Service crée une unité **yourdomainname** organisationnelle (UO) sous la racine du domaine. Le nom de cette unité d'organisation est basé sur le nom NetBIOS que vous avez saisi lors de la création de l'annuaire. Si vous n'avez pas spécifié de nom NetBIOS, il comprend par défaut la première partie du nom DNS de l'annuaire (par exemple, dans le cas de `corp.example.com`, le nom NetBIOS est `corp`).

Pour créer votre objet de stratégie de groupe, au lieu de sélectionner la stratégie de domaine par défaut, sélectionnez l'unité d'organisation (**yourdomainname** ou toute unité d'organisation inférieure à celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un objet de stratégie de groupe dans ce domaine, puis liez-le ici.

Pour plus d'informations sur l'**yourdomainname**UO, voir [What Gets Created](#) dans le Guide d'AWS Directory Service administration.

7. Dans l'éditeur de gestion des stratégies de groupe, sélectionnez Configuration de l'ordinateur, Politiques, Modèles d'administration et Variables de session PCo IP.
8. Vous pouvez désormais utiliser cet objet de stratégie de groupe de variables de session PCo IP pour modifier les paramètres de stratégie de groupe spécifiques à l'utilisation WorkSpaces de l'PCoadresse IP.

 Note

Pour permettre à l'utilisateur de remplacer vos paramètres, choisissez Paramètres administrateur par défaut remplaçables. Sinon, choisissez Paramètres administrateur par défaut non remplaçables.

Gérer les paramètres de stratégie de groupe pour PCo IP

Utilisez les paramètres de stratégie de groupe pour gérer vos systèmes Windows WorkSpaces utilisant l' PCoadresse IP.

Configuration de la prise en charge de l'imprimante pour PCo IP

Par défaut, WorkSpaces active l'impression à distance de base, qui offre des capacités d'impression limitées car elle utilise un pilote d'imprimante générique côté hôte pour garantir une impression compatible.

L'impression à distance avancée pour les clients Windows vous permet d'utiliser des fonctions spécifiques de votre imprimante, telles que l'impression recto-verso, mais elle nécessite l'installation du pilote d'imprimante correspondant côté hôte.

L'impression à distance est implémentée en tant que canal virtuel. Si les canaux virtuels sont désactivés, l'impression à distance ne fonctionne pas.

Pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour configurer le support de l'imprimante selon vos besoins.

Pour configurer la prise en charge de l'imprimante

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\)](#) ou le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc) et accédez à Variables de session PCo IP.
3. Ouvrez le paramètre Configure remote printing.
4. Dans la boîte de dialogue Configure remote printing (Configurer l'impression à distance) effectuez l'une des actions suivantes :

- Pour activer l'impression à distance avancée, choisissez Enabled (Activé), puis sous Options, Configure remote printing (Configurer l'impression à distance), choisissez Basic and Advanced printing for Windows clients (Impression de base et avancée pour les clients Windows). Pour utiliser automatiquement l'imprimante par défaut actuelle de l'ordinateur client, sélectionnez Automatically set default printer (Définir automatiquement l'imprimante par défaut).
 - Pour désactiver l'impression, choisissez Enabled (Activé), puis sous Options, Configure remote printing (Configurer l'impression à distance), choisissez Printing disabled (Impression désactivée).
5. Choisissez OK.
 6. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Par défaut, la redirection d'imprimante locale est désactivée. Vous pouvez utiliser les paramètres de stratégie de groupe pour activer cette fonctionnalité afin que votre imprimante locale soit définie comme imprimante par défaut chaque fois que vous vous connectez à votre WorkSpace.

 Note

La redirection d'imprimante locale n'est pas disponible pour Amazon Linux WorkSpaces.

Pour activer la redirection d'imprimante locale

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc) et accédez à Variables de session PCo IP.

3. Ouvrez le paramètre Configure remote printing.
4. Choisissez Activé, puis sous Options, Configurer l'impression à distance, choisissez l'une des options suivantes :
 - Impression de base et avancée pour les clients Windows
 - Impression de base
5. Sélectionnez Imprimante par défaut définie automatiquement, puis cliquez sur OK.
6. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection du presse-papiers (copier/coller) pour IP PCo

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour activer ou désactiver la redirection du presse-papiers

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc) et accédez à Variables de session PCo IP.
3. Ouvrez le paramètre Configure clipboard redirection.
4. Dans la boîte de dialogue Configure clipboard redirection (Configurer la redirection du presse-papiers), choisissez Enabled (Activé), puis l'un des paramètres suivants afin de déterminer la direction autorisée pour la redirection du presse-papiers. Une fois que vous avez terminé, choisissez OK.
 - Désactivé dans les deux directions

- Agent activé sur le client uniquement (sur WorkSpace l'ordinateur local)
 - Activation du client vers l'agent uniquement (ordinateur local vers WorkSpace)
 - Activé dans les deux directions
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
- Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Limitation connue

Lorsque la redirection du presse-papiers est activée sur le WorkSpace, si vous copiez du contenu supérieur à 890 Ko à partir d'une application Microsoft Office, l'application risque de ralentir ou de ne plus répondre pendant 5 secondes au maximum.

Définissez le délai de reprise de session pour IP PCo

Lorsque vous perdez la connectivité réseau, votre session WorkSpaces client active est déconnectée. WorkSpaces les applications clientes pour Windows et macOS tentent de reconnecter automatiquement la session si la connectivité réseau est rétablie dans un certain laps de temps. Le délai de reprise de session par défaut est de 20 minutes, mais vous pouvez modifier cette valeur pour WorkSpaces que cela soit contrôlé par les paramètres de stratégie de groupe de votre domaine.

Pour définir la valeur de délai d'expiration de reprise de session automatique

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc) et accédez à Variables de session PCo IP.
3. Ouvrez le paramètre Configure Session Automatic Reconnection Policy.

4. Dans la boîte de dialogue Configure Session Automatic Reconnection Policy, choisissez Enabled, définissez l'option Configure Session Automatic Reconnection Policy sur le délai d'expiration souhaité, en minutes, puis choisissez OK.
5. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection d'entrée audio pour IP PCo

Par défaut, Amazon WorkSpaces prend en charge la redirection des données depuis un microphone local. Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Note

Si vous avez un paramètre de stratégie de groupe qui restreint la connexion locale des utilisateurs dans leur compte WorkSpaces, l'entrée audio ne fonctionnera pas sur votre WorkSpaces. Si vous supprimez ce paramètre de stratégie de groupe, la fonction d'entrée audio est activée après le prochain redémarrage du WorkSpace. Pour plus d'informations sur ce paramètre de stratégie de groupe, consultez [Autoriser l'ouverture de session locale](#) dans la documentation Microsoft.

Pour activer ou désactiver la redirection d'entrée audio

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\)](#) ou le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc) et accédez à Variables de session PCo IP.
3. Ouvrez le bouton Activer/désactiver l'audio dans le paramètre de session PCo IP.

4. Dans la boîte de dialogue Activer/désactiver le son dans la session PCo IP, choisissez Activé ou Désactivé.
5. Choisissez OK.
6. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Désactiver la redirection de fuseau horaire pour PCo IP

Par défaut, l'heure dans un espace de travail est définie pour refléter le fuseau horaire du client utilisé pour se connecter au WorkSpace. Ce comportement est contrôlé par redirection de fuseau horaire. Vous pouvez désactiver la direction du fuseau horaire pour diverses raisons :

- Votre entreprise souhaite que tous les employés travaillent dans un fuseau horaire spécifique (même si certains employés sont dans d'autres fuseaux horaires).
- Vous avez planifié des tâches dans un WorkSpace qui sont destinées à être exécutées à une certaine heure dans un fuseau horaire spécifique.
- Vos utilisateurs qui voyagent beaucoup veulent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour désactiver la redirection de fuseau horaire

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.
2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc) et accédez à Variables de session PCo IP.

3. Ouvrez le paramètre Configurer la redirection de fuseau horaire.
4. Dans la boîte de dialogue Configurer la redirection de fuseau horaire, choisissez Désactivé.
5. Choisissez OK.
6. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.
7. Réglez le fuseau horaire correspondant WorkSpaces au fuseau horaire souhaité.

Le fuseau horaire du WorkSpaces est désormais statique et ne reflète plus le fuseau horaire des machines clientes.

Configuration des paramètres de sécurité PCo IP

Pour l' PCoIP, les données en transit sont cryptées à l'aide du cryptage TLS 1.2 et de la signature des demandes SigV4. Le protocole PCo IP utilise le trafic UDP crypté, avec le cryptage AES, pour le streaming de pixels. La connexion de streaming utilisant le port 4172 (TCP et UDP) est cryptée à l'aide des chiffrements AES-128 et AES-256, mais le chiffrement par défaut est de 128 bits. Vous pouvez modifier cette valeur par défaut sur 256 bits à l'aide du paramètre de stratégie de groupe Configurer les paramètres de sécurité PCo IP.

Vous pouvez également utiliser ce paramètre de stratégie de groupe pour modifier le mode de sécurité TLS et pour bloquer certaines suites de chiffrement. Une explication détaillée de ces paramètres et des suites de chiffrement prises en charge est fournie dans la boîte de dialogue Configurer les paramètres de sécurité PCo IP et la politique de groupe.

Pour configurer les paramètres de sécurité PCo IP

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.

2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpms.msc) et accédez à Variables de session PCo IP.
3. Ouvrez le paramètre Configurer les paramètres de sécurité PCo IP.
4. Dans la boîte de dialogue Configurer les paramètres de sécurité PCo IP, choisissez Activé. Pour définir le chiffrement par défaut du trafic de streaming sur 256 bits, accédez à l'option Chiffrements de données PCo IP et sélectionnez AES-256-GCM uniquement.
5. (Facultatif) Réglez le paramètre Mode de sécurité TLS, puis répertoriez les suites de chiffrement que vous souhaitez bloquer. Pour plus d'informations sur ces paramètres, consultez les descriptions fournies dans la boîte de dialogue Configurer les paramètres de sécurité PCo IP.
6. Choisissez OK.
7. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À l'invite de commande administrative, entrez **gpupdate /force**.

Configurer la redirection USB pour PCo IP

Note

Amazon prend WorkSpaces actuellement en charge la redirection USB uniquement pour YubiKey U2F. Il est possible de rediriger d'autres types de périphériques USB, mais ils ne sont pas pris en charge et risquent de ne pas fonctionner correctement.

Pour activer la redirection USB pour PCo IP

1. Assurez-vous d'avoir installé le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(32 bits\)](#) ou le modèle d'[administration de stratégie de WorkSpaces groupe pour PCo IP \(64 bits\)](#) le plus récent.

2. Sur une administration d'annuaire WorkSpace ou une instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmmc.msc) et accédez à Variables de session PCo IP.
3. Ouvrez le paramètre Activer/désactiver l'USB dans la session PCOIP.
4. Choisissez Activé, puis OK.
5. Ouvrez le paramètre Configurer les règles relatives aux périphériques USB autorisés et non autorisés sur PCo IP.
6. Choisissez Activé, puis sous Entrer le tableau d'autorisation USB (10 règles maximum), configurez les règles de la liste d'autorisation du périphérique USB.
 - Règle d'autorisation – 110500407. Cette valeur est une combinaison d'un identifiant de fournisseur (VID) et d'un identifiant de produit (PID). Le format d'une VID/PID combinaison est 1xxxxyyyy, où xxxx est le VID au format hexadécimal et yyyy le PID au format hexadécimal. Dans cet exemple, 1050 est le VID et 0407 le PID. Pour plus de valeurs YubiKey USB, consultez la section [Valeurs des identifiants YubiKey USB](#).
7. Sous Entrer le tableau d'autorisation USB (10 règles maximum), configurez les règles de la liste de blocage du périphérique USB.
 - Pour la règle de non-autorisation, définissez une chaîne vide. Cela signifie que seuls les périphériques USB figurant dans la liste d'autorisation sont autorisés.

 Note

Vous pouvez définir un maximum de 10 règles d'autorisation USB et un maximum de 10 règles de non-autorisation USB. Utilisez le caractère barre verticale (|) pour séparer plusieurs règles. Pour des informations détaillées sur les autorization/unauthorization règles, consultez [Teradici PCo IP Standard Agent pour Windows](#).

8. Choisissez OK.
9. La modification du paramètre de stratégie de groupe prend effet après la prochaine mise à jour de la stratégie de groupe pour la session WorkSpace et après le redémarrage de la WorkSpace session. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).

- À l'invite de commande administrative, entrez **gpupdate /force**.

Une fois le réglage pris en compte, tous les périphériques USB pris en charge peuvent être redirigés vers, WorkSpaces sauf si les restrictions sont configurées via le paramètre des règles du périphérique USB.

Définition de la durée de vie maximale d'un ticket Kerberos

Si vous n'avez pas désactivé la fonctionnalité Se souvenir de moi de votre Windows WorkSpaces, vos WorkSpace utilisateurs peuvent utiliser les cases à cocher Mémoriser moi ou Garder ma session connectée dans leur application WorkSpaces cliente pour enregistrer leurs informations d'identification. Cette fonctionnalité permet aux utilisateurs de se connecter facilement à leur WorkSpaces pendant que l'application cliente est en cours d'exécution. Leurs informations d'identification sont mises en cache de façon sécurisée jusqu'à la fin de la durée de vie maximale de leurs tickets Kerberos.

Si vous utilisez WorkSpace un annuaire AD Connector, vous pouvez modifier la durée de vie maximale des tickets Kerberos pour vos WorkSpaces utilisateurs par le biais de la stratégie de groupe en suivant les étapes décrites dans la section Durée de [vie maximale d'un ticket utilisateur](#) de la documentation Microsoft Windows.

Pour activer ou désactiver la fonctionnalité Se souvenir de moi consultez [Activez les fonctionnalités de WorkSpaces gestion en libre-service pour vos utilisateurs dans Personal WorkSpaces](#).

Configuration des paramètres de serveur proxy de l'appareil pour l'accès à Internet

Par défaut, les applications WorkSpaces clientes utilisent le serveur proxy spécifié dans les paramètres du système d'exploitation de l'appareil pour le trafic HTTPS (port 443). Les applications WorkSpaces clientes Amazon utilisent le port HTTPS pour les mises à jour, l'enregistrement et l'authentification.

Note

Les serveurs proxy qui nécessitent une authentification à l'aide d'informations d'identification à la connexion ne sont pas pris en charge.

Vous pouvez configurer les paramètres du serveur proxy de l'appareil pour votre Windows par le WorkSpaces biais de la stratégie de groupe en suivant les étapes décrites dans la [section Configurer le proxy de l'appareil et les paramètres de connectivité Internet](#) dans la documentation Microsoft.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces Windows, consultez [Proxy Server](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces macOS, consultez [Proxy Server](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces Web Access, consultez la section [Serveur proxy](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Utilisation d'un serveur proxy pour le trafic des espaces de travail

Pour l' PCoIP WorkSpaces, les applications clientes de bureau ne prennent pas en charge l'utilisation d'un serveur proxy ni le déchiffrement TLS ni l'inspection du trafic du port 4172 en UDP (pour le trafic des ordinateurs de bureau). Elles requièrent une connexion directe au port 4172.

Pour le DCV WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et supérieure) et l'application cliente macOS (version 5.4 et supérieure) prennent en charge l'utilisation de serveurs proxy HTTP pour le trafic TCP du port 4195. Le déchiffrement et l'inspection TLS ne sont pas pris en charge.

DCV ne prend pas en charge l'utilisation d'un proxy pour le trafic de bureau via UDP. Seules les applications clientes de bureau WorkSpaces Windows et macOS et l'accès Web prennent en charge l'utilisation d'un proxy pour le trafic TCP.

Note

Si vous choisissez d'utiliser un serveur proxy, les appels d'API que l'application cliente envoie aux WorkSpaces services sont également transmis par proxy. Les appels d'API et le trafic des espaces de travail doivent passer par le même serveur proxy.

Recommandation concernant l'utilisation de serveurs proxy

Nous ne recommandons pas l'utilisation d'un serveur proxy pour le trafic de votre WorkSpaces ordinateur de bureau.

Le trafic des ordinateurs de WorkSpaces bureau Amazon étant déjà chiffré, les proxys n'améliorent pas la sécurité. Un proxy représente un saut supplémentaire sur le chemin du réseau, qui peut avoir un impact sur la qualité du streaming en introduisant de la latence. Un proxy peut également potentiellement réduire le débit s'il n'est pas correctement dimensionné pour gérer le trafic de streaming des espaces de travail. En outre, la plupart des proxys ne sont pas conçus pour prendre en charge les connexions de longue durée WebSocket (TCP) et peuvent affecter la qualité et la stabilité du streaming.

Si vous devez utiliser un proxy, localisez votre serveur proxy le plus près possible du Workspace client, de préférence sur le même réseau, afin d'éviter d'ajouter de la latence au réseau, ce qui pourrait avoir un impact négatif sur la qualité et la réactivité du streaming.

Activer la prise en charge du plugin Amazon WorkSpaces for Zoom Meeting Media

Zoom prend en charge une communication en temps réel optimisée pour les applications DCV et PCo IP basées sur Windows WorkSpaces, grâce au plug-in Zoom VDI. La communication directe avec le client permet aux appels vidéo de contourner le bureau virtuel basé sur le cloud et de fournir une expérience Zoom similaire à celle de votre utilisateur lorsque la réunion se déroule dans le cadre du bureau virtuel de votre utilisateur. Workspace

Activer le plug-in Zoom Meeting Media pour DCV

Avant d'installer les composants Zoom VDI, mettez à jour votre WorkSpaces configuration pour prendre en charge l'optimisation du zoom.

Conditions préalables

Avant d'utiliser le plugin, assurez-vous que les conditions suivantes sont remplies.

- WorkSpaces Client Windows version 5.10.0+ avec plug-in [Zoom VDI](#) version 5.17.10+
- Dans votre WorkSpaces — Client [Zoom VDI Meeting](#) version 5.17.10+

Avant de commencer

1. Activez le paramètre de stratégie de groupe d'extensions. Pour de plus amples informations, veuillez consulter [Configuration des extensions pour DCV](#).
2. Désactivez le paramètre de stratégie de groupe de reconnexion automatique. Pour de plus amples informations, veuillez consulter [Définissez le délai de reprise de session pour DCV](#).

Installation des composants Zoom

Pour activer l'optimisation du zoom, installez deux composants, fournis par Zoom, sur votre Windows WorkSpaces. Pour plus d'informations, consultez la section [Utilisation de Zoom pour Amazon Web Services](#).

1. Installez le client Zoom VDI Meeting version 5.12.6+ dans votre WorkSpace
2. Installez le plug-in Zoom VDI (Windows Universal Installer) version 5.12.6+ sur le client sur lequel le vôtre est installé WorkSpace
3. Vérifiez que le plug-in optimise le trafic Zoom en confirmant que l'état de votre plug-in VDI indique que le statut de votre plug-in VDI est connecté dans le client Zoom VDI. Pour plus d'informations, consultez [Comment confirmer l' WorkSpaces optimisation d'Amazon](#).

Activer le plug-in Zoom Meeting Media pour PCo IP

Les utilisateurs disposant d'une autorisation administrative sur Active Directory peuvent générer une clé de registre à l'aide de leur objet de stratégie de groupe (GPO). Cela permet aux utilisateurs d'envoyer la clé de registre à toutes les fenêtres de votre domaine WorkSpaces à l'aide d'une mise à jour forcée. Les utilisateurs disposant de droits d'administration peuvent également installer les clés de registre individuellement sur leur WorkSpaces hôte.

Conditions préalables

Avant d'utiliser le plugin, assurez-vous que les conditions suivantes sont remplies.

- WorkSpaces Client Windows version 5.4.0+ avec plug-in [Zoom VDI](#) version 5.12.6+.
- Dans votre WorkSpaces — Client [Zoom VDI Meeting](#) version 5.12.6+.

Créez la clé de registre sur un WorkSpaces hôte Windows

Procédez comme suit pour créer une clé de registre sur un WorkSpaces hôte Windows. La clé de registre est requise pour utiliser Zoom sous Windows WorkSpaces.

1. Ouvrez l'Éditeur du Registre Windows en tant qu'administrateur.
2. Accédez à \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon.
3. Si la clé d'extension n'existe pas, cliquez avec le bouton droit de la souris, choisissez Nouveau > Clé et nommez-la Extension.

4. Dans la nouvelle clé Extension, cliquez avec le bouton droit de la souris, choisissez Nouveau > Valeur DWORD et nommez-la enable. Le nom doit être en minuscules.
5. Choisissez le nouveau DWORD et remplacez la valeur par 1.
6. Redémarrez l'ordinateur pour terminer le processus.
7. Sur votre WorkSpaces hôte, téléchargez et installez le dernier client Zoom VDI. Sur votre WorkSpaces client (version 5.4 ou ultérieure), téléchargez et installez le dernier plugin client Zoom VDI pour Amazon WorkSpaces. Pour plus d'informations, consultez [VDI releases and downloads](#) sur le site Web Zoom Assistance.

Lancez Zoom pour démarrer votre appel vidéo.

Résolution des problèmes

Procédez comme suit pour résoudre les problèmes liés à Zoom sous Windows WorkSpaces.

- Vérifiez que la clé de registre est activée et appliquée correctement.
- Accédez à C:\ProgramData\Amazon\Amazon WorkSpaces Extension. Vous devez voir wse_core.dll.
- Assurez-vous que les versions de l'hôte et des clients sont correctes et identiques.

Si vous continuez à rencontrer des difficultés, Support contactez le [Support Centre](#).

Vous pouvez vous inspirer des exemples suivants pour appliquer un GPO en tant qu'administrateur de l'annuaire.

- WSE.adml

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
  schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
  <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
  GPO template files have them set like this. -->
  <displayName>enter display name here</displayName>
  <description>enter description here</description>

  <resources>
  <stringTable>
    <string id="SUPPORTED_ProductOnly">N/A</string>
```

```

    <string id="Amazon">Amazon</string>
    <string id="Amazon_Help">Amazon Group Policies</string>
    <string id="WorkspacesExtension">Workspaces Extension</string>
    <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

    <!-- Extension Itself -->
    <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>

    <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

</stringTable>
</resources>
</policyDefinitionResources>

```

- WSE.admx

```

<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
  <policyNamespaces>
    <target prefix="WorkspacesExtension"
namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
  </policyNamespaces>
  <supersededAdm fileName="wse.adm" />
  <resources minRequiredRevision="1.0" />
  <supportedOn>
    <definitions>
      <definition name="SUPPORTED_ProductOnly"
displayName="$(string.SUPPORTED_ProductOnly)"/>
    </definitions>
  </supportedOn>
  <categories>
    <category name="Amazon" displayName="$(string.Amazon)"
explainText="$(string.Amazon_Help)" />
    <category name="WorkspacesExtension"
displayName="$(string.WorkspacesExtension)"
explainText="$(string.WorkspacesExtension_Help)">
      <parentCategory ref="Amazon" />
    </category>
  </categories>
</policyDefinitions>

```

```
</categories>

<policies>
  <policy name="ToggleExtension" class="Machine"
displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
key="Software\Policies\Amazon\Extension" valueName="enable">
    <parentCategory ref="WorkspacesExtension" />
    <supportedOn ref="SUPPORTED_ProductOnly" />
    <enabledValue>
      <decimal value="1" />
    </enabledValue>
    <disabledValue>
      <decimal value="0" />
    </disabledValue>
  </policy>
</policies>
</policyDefinitions>
```

Gérez votre Amazon Linux 2 WorkSpaces en mode WorkSpaces personnel

Pour les charges de travail qui nécessitent le RPM Package Manager (RPM), nous recommandons d'utiliser [Red Hat Enterprise Linux](#) ou [Rocky Linux](#). Amazon Linux 2 peut ne pas fournir les dernières versions de certaines applications et bibliothèques, telles que Firefox et glibc, dont vous pourriez avoir besoin.

Comme les instances Linux ne respectent pas la stratégie de groupe, nous vous recommandons d'utiliser une solution de gestion de configuration pour distribuer et appliquer la stratégie. Par exemple, vous pouvez utiliser [Ansible](#).

Note

La redirection d'imprimante locale n'est pas disponible pour Amazon Linux WorkSpaces.

Contrôlez le comportement du DCV sur Amazon Linux WorkSpaces

Le comportement du DCV est contrôlé par les paramètres de configuration du `wsp.conf` fichier, qui se trouve dans le `/etc/wsp/` répertoire. Pour déployer et appliquer les modifications apportées à la politique, utilisez une solution de gestion de configuration qui prend en charge Amazon Linux. Toutes les modifications prennent effet lorsque l'agent démarre.

 Note

- Si vous apportez des modifications incorrectes ou non prises en charge au `wsp.conf` fichier, les modifications de politique risquent de ne pas être appliquées aux connexions nouvellement établies sur votre WorkSpace.
- Les bundles Amazon Linux WorkSpaces on DCV présentent actuellement les limites suivantes :
 - Actuellement disponible uniquement dans les régions AWS GovCloud (ouest des États-Unis) et AWS GovCloud (est des États-Unis).
 - L'entrée vidéo n'est pas prise en charge.
 - La déconnexion de session au verrouillage de l'écran n'est pas prise en charge.

Les sections suivantes décrivent comment activer ou désactiver certaines fonctionnalités.

Configurer la redirection du presse-papiers pour DCV Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Utilisez le fichier de configuration DCV pour configurer cette fonctionnalité, si nécessaire. Ce paramètre prend effet lorsque vous déconnectez et reconnectez le WorkSpace.

Pour configurer la redirection du presse-papiers pour DCV Amazon Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `clipboard = X`

Où les valeurs possibles pour `X` sont les suivantes :

`enabled` : la redirection du presse-papiers est activée dans les deux sens (par défaut).

`disabled` : la redirection du presse-papiers est désactivée dans les deux sens.

`paste-only` : la redirection du presse-papiers est activée, mais vous ne pouvez que copier le contenu depuis l'appareil client local et le coller sur le bureau de l'hôte distant.

`copy-only` : la redirection du presse-papiers est activée, mais vous ne pouvez que copier le contenu depuis l'hôte distant et le coller sur l'appareil client local.

Activer ou désactiver la redirection d'entrée audio pour DCV Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée audio. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire. Ce paramètre prend effet lorsque vous vous déconnectez et que vous vous reconnectez au WorkSpace.

Pour activer ou désactiver la redirection d'entrée audio pour DCV Amazon Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du fichier.

```
audio-in = X
```

Où les valeurs possibles pour *X* sont les suivantes :

`enabled` : la redirection d'entrée audio est activée (par défaut).

`disabled` : la redirection d'entrée audio est désactivée.

Activer ou désactiver la redirection de fuseau horaire pour DCV Amazon Linux WorkSpaces

Par défaut, l'heure dans un espace de travail est définie de manière à refléter le fuseau horaire du client utilisé pour se connecter au WorkSpace. Ce comportement est contrôlé par redirection de fuseau horaire. Vous pouvez choisir de désactiver la direction du fuseau horaire pour diverses raisons :

- Votre entreprise souhaite que tous les employés travaillent dans un fuseau horaire spécifique (même si certains employés sont dans d'autres fuseaux horaires).

- Vous avez planifié des tâches dans un WorkSpace qui sont destinées à être exécutées à une certaine heure dans un fuseau horaire spécifique.
- Vos utilisateurs qui voyagent beaucoup veulent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Utilisez le fichier de configuration DCV pour configurer cette fonctionnalité, si nécessaire. Ce paramètre prend effet une fois que vous vous êtes déconnecté et reconnecté au WorkSpace.

Pour activer ou désactiver la redirection de fuseau horaire pour DCV Amazon Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du fichier.

```
timezone_redirect= X
```

Où les valeurs possibles pour **X** sont les suivantes :

enabled : la redirection de fuseau horaire est activée (par défaut).

disabled : la redirection de fuseau horaire est désactivée.

Contrôlez le comportement de l'agent PCo IP sur Amazon Linux WorkSpaces

Le comportement de l'agent PCo IP est contrôlé par les paramètres de configuration du `pcoip-agent.conf` fichier, qui se trouve dans le `/etc/pcoip-agent/` répertoire. Pour déployer et appliquer les modifications apportées à la politique, utilisez une solution de gestion de configuration qui prend en charge Amazon Linux. Toutes les modifications prennent effet lorsque l'agent démarre. Le redémarrage de l'agent met fin aux connexions ouvertes et redémarre le gestionnaire de fenêtres. Pour appliquer les modifications, nous vous recommandons de redémarrer le WorkSpace.

Note

Si vous apportez des modifications incorrectes ou non prises en charge au `pcoip-agent.conf` fichier, vous risquez de ne plus WorkSpace fonctionner. Si votre WorkSpace

appareil cesse de fonctionner, vous devrez peut-être vous [connecter à votre Workspace compte en utilisant SSH](#) pour annuler les modifications, ou vous devrez peut-être [le Workspace reconstruire](#).

Les sections suivantes décrivent comment activer ou désactiver certaines fonctionnalités. Pour obtenir la liste complète des paramètres disponibles, lancez-le man `pcoip-agent.conf` depuis le terminal sur n'importe quel Amazon Linux WorkSpace.

Configurer la redirection du presse-papiers pour PCo IP Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Utilisez la configuration de l'agent PCo IP pour désactiver cette fonctionnalité, si nécessaire. Ce paramètre prend effet lorsque vous redémarrez le Workspace.

Pour configurer la redirection du presse-papiers pour PCo IP Amazon Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `pcoip-agent.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. Ajoutez la ligne suivante à la fin du fichier.

```
pcoip.server_clipboard_state = X
```

Où les valeurs possibles pour **X** sont les suivantes :

0 : la redirection du presse-papiers est désactivée dans les deux sens.

1 : la redirection du presse-papiers est activée dans les deux sens.

2 : la redirection du presse-papiers est activée uniquement du client vers l'agent (copie et collage uniquement du contenu depuis l'appareil client local vers le bureau de l'hôte distant).

3 : la redirection du presse-papiers est activée uniquement de l'agent vers le client (copie et collage uniquement du contenu depuis le bureau de l'hôte distant vers l'appareil client local).

 Note

La redirection du presse-papiers est mise en œuvre en tant que canal virtuel. Si les canaux virtuels sont désactivés, la redirection du presse-papiers ne fonctionne pas. Pour activer les canaux virtuels, consultez la section [Canaux virtuels PCo IP](#) dans la documentation de Teradici.

Activer ou désactiver la redirection d'entrée audio pour PCo IP Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée audio. Utilisez la configuration de l'agent PCo IP pour désactiver cette fonctionnalité, si nécessaire. Ce paramètre prend effet lorsque vous redémarrez le Workspace.

Pour activer ou désactiver la redirection d'entrée audio pour PCo IP Amazon Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `pcoip-agent.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. Ajoutez la ligne suivante à la fin du fichier.

```
pcoip.enable_audio = X
```

Où les valeurs possibles pour *X* sont les suivantes :

0 : la redirection d'entrée audio est désactivée.

1 : la redirection d'entrée audio est activée.

Activer ou désactiver la redirection de fuseau horaire pour PCo IP Amazon Linux WorkSpaces

Par défaut, l'heure dans un espace de travail est définie de manière à refléter le fuseau horaire du client utilisé pour se connecter au Workspace. Ce comportement est contrôlé par redirection

de fuseau horaire. Vous pouvez choisir de désactiver la direction du fuseau horaire pour diverses raisons :

- Votre entreprise souhaite que tous les employés travaillent dans un fuseau horaire spécifique (même si certains employés sont dans d'autres fuseaux horaires).
- Vous avez planifié des tâches dans un WorkSpace qui sont destinées à être exécutées à une certaine heure dans un fuseau horaire spécifique.
- Vos utilisateurs qui voyagent beaucoup veulent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Si nécessaire pour Linux WorkSpaces, vous pouvez utiliser la configuration de l'agent PCo IP pour désactiver cette fonctionnalité. Ce paramètre prend effet lorsque vous redémarrez le WorkSpace.

Pour activer ou désactiver la redirection de fuseau horaire pour PCo IP Amazon Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `pcoip-agent.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. Ajoutez la ligne suivante à la fin du fichier.

```
pcoip.enable_timezone_redirect= X
```

Où les valeurs possibles pour **X** sont les suivantes :

0 : la redirection de fuseau horaire est désactivée.

1 : la redirection de fuseau horaire est activée.

Accorder un accès SSH aux administrateurs Amazon Linux WorkSpaces

Par défaut, seuls les utilisateurs et comptes assignés au sein du groupe des administrateurs de domaine peuvent se connecter à Amazon Linux à l'aide du WorkSpaces protocole SSH.

Nous vous recommandons de créer un groupe d'administrateurs dédié pour vos WorkSpaces administrateurs Amazon Linux dans Active Directory.

Pour activer l'accès sudo pour les membres du groupe Linux_Workspaces_Admins Active Directory

1. Modifiez le fichier sudoers en utilisant visudo, comme illustré dans l'exemple suivant.

```
[example\username@workspace-id ~]$ sudo visudo
```

2. Ajoutez la ligne suivante.

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Une fois que vous avez créé le groupe d'administrateurs dédié, procédez comme suit pour activer la connexion pour les membres du groupe.

Pour activer la connexion pour les membres du groupe Linux_Workspaces_Admins Active Directory

1. Modifiez /etc/security/access.conf avec des droits élevés.

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Ajoutez la ligne suivante.

```
+: (example\Linux_WorkSpaces_Admins):ALL
```

Pour plus d'informations sur vos connexions SSH, consultez [Activez les connexions SSH pour votre Linux WorkSpaces dans Personal WorkSpaces](#).

Remplacer le shell par défaut pour Amazon Linux WorkSpaces

Pour remplacer le shell par défaut pour Linux WorkSpaces, nous vous recommandons de modifier le ~/.bashrc fichier de l'utilisateur. Par exemple, pour utiliser Z shell au lieu du shell Bash, ajoutez les lignes suivantes à /home/*username*/.bashrc.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

Note

Après avoir effectué cette modification, vous devez soit redémarrer le Workspace soit vous déconnecter du Workspace (pas simplement vous déconnecter), puis vous reconnecter pour que la modification prenne effet.

Protection des référentiels personnalisés contre tout accès non autorisé

Pour contrôler l'accès à vos référentiels personnalisés, nous vous recommandons d'utiliser les fonctionnalités de sécurité intégrées à Amazon Virtual Private Cloud (Amazon VPC) plutôt que d'utiliser des mots de passe. Par exemple, utilisez des listes de contrôle d'accès réseau (ACLs) et des groupes de sécurité. Pour plus d'informations sur ces fonctionnalités, consultez [Sécurité](#) dans le Guide de l'utilisateur Amazon VPC.

Si vous devez utiliser des mots de passe pour protéger vos référentiels, veillez à créer vos fichiers de définition de référentiel yum, comme illustré dans [Repository Definition Files \(Fichiers de définition de référentiel\)](#) dans la documentation Fedora.

Utilisation du référentiel de la bibliothèque Amazon Linux Extras

Avec Amazon Linux, vous pouvez utiliser la bibliothèque Extras pour installer les mises à jour d'application et de logiciels sur vos instances. Pour plus d'informations sur l'utilisation de la bibliothèque Extras, consultez [Bibliothèque Extras \(Amazon Linux\)](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

Note

Si vous utilisez le référentiel Amazon Linux, votre Amazon Linux WorkSpaces doit avoir accès à Internet, ou vous devez configurer des points de terminaison de cloud privé virtuel (VPC) sur ce référentiel et sur le référentiel Amazon Linux principal. Pour de plus amples informations, veuillez consulter [Fournir un accès à Internet pour les WorkSpaces particuliers](#).

Utiliser des cartes à puce pour l'authentification sous Linux WorkSpaces

Les packs Linux WorkSpaces on DCV autorisent l'utilisation de cartes à puce [Common Access Card \(CAC\)](#) et de [Personal Identity Verification \(PIV\)](#) pour l'authentification. Pour de plus amples

informations, veuillez consulter [Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal](#).

Configuration des paramètres de serveur proxy de l'appareil pour l'accès à Internet

Par défaut, les applications WorkSpaces clientes utilisent le serveur proxy spécifié dans les paramètres du système d'exploitation de l'appareil pour le trafic HTTPS (port 443). Les applications WorkSpaces clientes Amazon utilisent le port HTTPS pour les mises à jour, l'enregistrement et l'authentification.

Note

Les serveurs proxy qui nécessitent une authentification à l'aide d'informations d'identification à la connexion ne sont pas pris en charge.

Vous pouvez configurer les paramètres du serveur proxy de l'appareil pour votre système Linux WorkSpaces via la stratégie de groupe en suivant les étapes décrites dans la section [Configurer le proxy de l'appareil et les paramètres de connectivité Internet](#) dans la documentation Microsoft.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces Windows, consultez [Proxy Server](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces macOS, consultez [Proxy Server](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces Web Access, consultez la section [Serveur proxy](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Utilisation d'un serveur proxy pour le trafic des espaces de travail

Pour l' PCoIP WorkSpaces, les applications clientes de bureau ne prennent pas en charge l'utilisation d'un serveur proxy, ni le déchiffrement TLS ni l'inspection du trafic du port 4172 en UDP (pour le trafic des ordinateurs de bureau). Elles requièrent une connexion directe au port 4172.

Pour le DCV WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et supérieure) et l'application cliente macOS (version 5.4 et supérieure) prennent en charge l'utilisation de serveurs proxy HTTP pour le trafic TCP du port 4195. Le déchiffrement et l'inspection TLS ne sont pas pris en charge.

DCV ne prend pas en charge l'utilisation d'un proxy pour le trafic de bureau via UDP. Seules les applications clientes de bureau WorkSpaces Windows et macOS et l'accès au Web prennent en charge l'utilisation d'un proxy pour le trafic TCP.

Note

Si vous choisissez d'utiliser un serveur proxy, les appels d'API que l'application cliente envoie aux WorkSpaces services sont également transmis par proxy. Les appels d'API et le trafic des espaces de travail doivent passer par le même serveur proxy.

Recommandation concernant l'utilisation de serveurs proxy

Nous ne recommandons pas l'utilisation d'un serveur proxy pour le trafic de votre WorkSpaces ordinateur de bureau.

Le trafic des ordinateurs de WorkSpaces bureau Amazon étant déjà chiffré, les proxys n'améliorent pas la sécurité. Un proxy représente un saut supplémentaire sur le chemin du réseau, qui peut avoir un impact sur la qualité du streaming en introduisant de la latence. Un proxy peut également potentiellement réduire le débit s'il n'est pas correctement dimensionné pour gérer le trafic de streaming des espaces de travail. En outre, la plupart des proxys ne sont pas conçus pour prendre en charge les connexions de longue durée WebSocket (TCP) et peuvent affecter la qualité et la stabilité du streaming.

Si vous devez utiliser un proxy, localisez votre serveur proxy le plus près possible du Workspace client, de préférence sur le même réseau, afin d'éviter d'ajouter de la latence au réseau, ce qui pourrait avoir un impact négatif sur la qualité et la réactivité du streaming.

Gérez votre Ubuntu WorkSpaces en mode WorkSpaces personnel

Votre WorkSpaces offre Ubuntu inclut un abonnement à Ubuntu Pro de Canonical. Comme Windows et Amazon Linux WorkSpaces, Ubuntu WorkSpaces est joint à un domaine. Vous pouvez donc utiliser les utilisateurs et les groupes Active Directory pour :

- Administrez votre Ubuntu WorkSpaces
- Fournir un accès à ceux-ci WorkSpaces aux utilisateurs

Vous pouvez gérer Ubuntu WorkSpaces avec une politique de groupe en utilisant ADsys. Consultez la [FAQ concernant l'intégration d'Ubuntu et d'Active Directory](#) pour plus d'informations. Vous pouvez également utiliser d'autres solutions de configuration et de gestion, comme [Landscape](#) et [Ansible](#).

Contrôler le comportement du DCV sur Ubuntu WorkSpaces

Le comportement du DCV est contrôlé par les paramètres de configuration du `wsp.conf` fichier, qui se trouve dans le `/etc/wsp/` répertoire. Pour déployer et appliquer les modifications apportées à la stratégie, utilisez une solution de gestion de configuration qui prend en charge Ubuntu. Toutes les modifications prennent effet lorsque l'agent démarre.

Note

Si vous apportez des modifications incorrectes ou non prises en charge aux `wsp.conf` politiques, elles risquent de ne pas être appliquées aux nouvelles connexions établies avec votre Workspace.

Les sections suivantes décrivent comment activer ou désactiver certaines fonctionnalités.

Activer ou désactiver la redirection du presse-papiers pour Ubuntu WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection du presse-papiers pour Ubuntu WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
clipboard = X
```

Où les valeurs possibles pour `X` sont les suivantes :

`enabled` : la redirection du presse-papiers est activée dans les deux sens (par défaut).

disabled : la redirection du presse-papiers est désactivée dans les deux sens.

paste-only : la redirection du presse-papiers est activée et vous permet uniquement de copier le contenu de l'appareil client local et de le coller vers le bureau de l'hôte distant.

copy-only : la redirection du presse-papiers est activée et vous permet uniquement de copier le contenu du bureau de l'hôte distant et de le coller vers l'appareil client local.

Activer ou désactiver la redirection audio pour Ubuntu WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée audio. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection audio d'entrée pour Ubuntu WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
audio-in = X
```

Où les valeurs possibles pour `X` sont les suivantes :

enabled : la redirection d'entrée audio est activée (par défaut).

disabled : la redirection d'entrée audio est désactivée.

Activer ou désactiver la redirection d'entrée vidéo pour Ubuntu WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée vidéo. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection d'entrée vidéo pour Ubuntu WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.


```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe [policies].

```
video-in = X
```

Où les valeurs possibles pour **X** sont les suivantes :

enabled : la redirection d'entrée vidéo est activée (par défaut).

disabled : la redirection d'entrée vidéo est désactivée.

Activer ou désactiver la redirection de fuseau horaire pour Ubuntu WorkSpaces

Par défaut, l'heure dans un espace de travail est définie de manière à refléter le fuseau horaire du client utilisé pour se connecter au WorkSpace. Ce comportement est contrôlé par redirection de fuseau horaire. Vous pouvez choisir de désactiver la direction du fuseau horaire pour diverses raisons :

- Votre entreprise souhaite que tous les employés travaillent dans un fuseau horaire spécifique (même si certains employés sont dans d'autres fuseaux horaires).
- Vous avez planifié des tâches dans un WorkSpace qui sont destinées à être exécutées à une certaine heure dans un fuseau horaire spécifique.
- Vos utilisateurs voyagent beaucoup et souhaitent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Utilisez le fichier de configuration DCV pour configurer cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection de fuseau horaire pour Ubuntu WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe [policies].

```
timezone-redirect = X
```

Où les valeurs possibles pour **X** sont les suivantes :

enabled : la redirection de fuseau horaire est activée (par défaut).

disabled : la redirection de fuseau horaire est désactivée.

Activer ou désactiver la redirection d'imprimante pour Ubuntu WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection de l'imprimante. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection d'imprimantes pour Ubuntu WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
remote-printing = X
```

Où les valeurs possibles pour **X** sont les suivantes :

enabled : la redirection d'imprimante est activée (par défaut).

disabled : la redirection d'imprimante est désactivée.

Activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour DCV

Activez la déconnexion de la session lors du verrouillage de l'écran pour permettre à vos utilisateurs de mettre fin à leur WorkSpaces session lorsque l'écran de verrouillage est détecté. Pour se

reconnecter depuis le WorkSpaces client, les utilisateurs peuvent utiliser leur mot de passe ou leur carte à puce pour s'authentifier, selon le type d'authentification activé pour eux. WorkSpaces

Par défaut, WorkSpaces ne prend pas en charge la déconnexion de la session lors du verrouillage de l'écran. Utilisez le fichier de configuration DCV pour activer cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour Ubuntu WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
disconnect-on-lock = X
```

Où les valeurs possibles pour **X** sont les suivantes :

`enabled` : la déconnexion au verrouillage de l'écran est activée.

`disabled` : la déconnexion au verrouillage de l'écran est désactivée (par défaut).

Accorder l'accès SSH aux administrateurs Ubuntu WorkSpaces

Par défaut, seuls les utilisateurs et comptes assignés dans le groupe des administrateurs de domaine peuvent se connecter à Ubuntu à l'aide du WorkSpaces protocole SSH. Pour permettre à d'autres utilisateurs et comptes de se connecter à Ubuntu WorkSpaces via SSH, nous vous recommandons de créer un groupe d'administrateurs dédié pour vos WorkSpaces administrateurs Ubuntu dans Active Directory.

Pour activer l'accès sudo pour les membres du groupe **Linux_WorkSpaces_Admins** Active Directory

1. Modifiez le fichier `sudoers` en utilisant `visudo`, comme illustré dans l'exemple suivant.

```
[username@workspace-id ~]$ sudo visudo
```

2. Ajoutez la ligne suivante.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Une fois que vous avez créé le groupe d'administrateurs dédié, procédez comme suit pour activer la connexion pour les membres du groupe.

Pour activer la connexion pour les membres du groupe **Linux_WorkSpaces_Admins** Active Directory

1. Modifiez `/etc/security/access.conf` avec des droits élevés.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Ajoutez la ligne suivante.

```
+: (Linux_WorkSpaces_Admins):ALL
```

Avec Ubuntu, il n'est pas nécessaire d'ajouter un nom de domaine lorsque WorkSpaces vous spécifiez le nom d'utilisateur pour la connexion SSH, et par défaut, l'authentification par mot de passe est désactivée. Pour vous connecter via SSH, vous devez soit ajouter votre clé publique SSH `$HOME/.ssh/authorized_keys` sur votre Ubuntu WorkSpace, soit la modifier `/etc/ssh/sshd_config` pour la configurer PasswordAuthentication sur. yes Pour plus d'informations sur l'activation des connexions SSH, consultez [Activer les connexions SSH pour votre système Linux](#). WorkSpaces

Remplacer le shell par défaut pour Ubuntu WorkSpaces

Pour remplacer le shell par défaut pour Ubuntu WorkSpaces, nous vous recommandons de modifier le `~/.bashrc` fichier de l'utilisateur. Par exemple, pour utiliser `Z shell` au lieu du shell Bash, ajoutez les lignes suivantes à `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

Note

Après avoir effectué cette modification, vous devez soit redémarrer le WorkSpace soit vous déconnecter du WorkSpace (pas simplement vous déconnecter), puis vous reconnecter pour que la modification prenne effet.

Utiliser des cartes à puce pour l'authentification sur Ubuntu WorkSpaces

WorkSpaces Les packs Ubuntu permettent l'utilisation de cartes à puce [CAC \(Common Access Card\)](#) et de [vérification d'identité personnelle \(PIV\)](#) pour l'authentification. Pour de plus amples informations, veuillez consulter [Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal](#).

Configuration des paramètres de serveur proxy de l'appareil pour l'accès à Internet

Par défaut, les applications WorkSpaces clientes utilisent le serveur proxy spécifié dans les paramètres du système d'exploitation de l'appareil pour le trafic HTTPS (port 443). Les applications WorkSpaces clientes Amazon utilisent le port HTTPS pour les mises à jour, l'enregistrement et l'authentification.

Note

Les serveurs proxy qui nécessitent une authentification à l'aide d'informations d'identification à la connexion ne sont pas pris en charge.

Vous pouvez configurer les paramètres du serveur proxy de l'appareil pour votre Ubuntu WorkSpaces via la stratégie de groupe en suivant les étapes décrites dans [Configurer les paramètres du proxy de l'appareil et de la connectivité Internet](#) dans la documentation Microsoft.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces Windows, consultez [Proxy Server](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces macOS, consultez [Proxy Server](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Pour plus d'informations sur la configuration des paramètres de proxy dans l'application cliente WorkSpaces Web Access, consultez la section [Serveur proxy](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Utilisation d'un serveur proxy pour le trafic des espaces de travail

Pour l' PCoIP WorkSpaces, les applications clientes de bureau ne prennent pas en charge l'utilisation d'un serveur proxy ni le déchiffrement TLS ni l'inspection du trafic du port 4172 en UDP (pour le trafic des ordinateurs de bureau). Elles requièrent une connexion directe au port 4172.

Pour le DCV WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et supérieure) et l'application cliente macOS (version 5.4 et supérieure) prennent en charge l'utilisation de serveurs proxy HTTP pour le trafic TCP du port 4195. Le déchiffrement et l'inspection TLS ne sont pas pris en charge.

DCV ne prend pas en charge l'utilisation d'un proxy pour le trafic de bureau via UDP. Seules les applications clientes de bureau WorkSpaces Windows et macOS et l'accès Web prennent en charge l'utilisation d'un proxy pour le trafic TCP.

Note

Si vous choisissez d'utiliser un serveur proxy, les appels d'API que l'application cliente envoie aux WorkSpaces services sont également transmis par proxy. Les appels d'API et le trafic des espaces de travail doivent passer par le même serveur proxy.

Recommandation concernant l'utilisation de serveurs proxy

Nous ne recommandons pas l'utilisation d'un serveur proxy pour le trafic de votre WorkSpaces ordinateur de bureau.

Le trafic des ordinateurs de WorkSpaces bureau Amazon étant déjà chiffré, les proxys n'améliorent pas la sécurité. Un proxy représente un saut supplémentaire sur le chemin du réseau, qui peut avoir un impact sur la qualité du streaming en introduisant de la latence. Un proxy peut également potentiellement réduire le débit s'il n'est pas correctement dimensionné pour gérer le trafic de streaming des espaces de travail. En outre, la plupart des proxys ne sont pas conçus pour prendre en

charge les connexions de longue durée WebSocket (TCP) et peuvent affecter la qualité et la stabilité du streaming.

Si vous devez utiliser un proxy, localisez votre serveur proxy le plus près possible du WorkSpace client, de préférence sur le même réseau, afin d'éviter d'ajouter de la latence au réseau, ce qui pourrait avoir un impact négatif sur la qualité et la réactivité du streaming.

Gérez votre Rocky Linux WorkSpaces

Vous pouvez gérer Rocky Linux WorkSpaces avec des solutions de configuration et de gestion, telles qu'[Ansible](#).

Note

Vous ne pouvez pas supprimer, modifier ou masquer les droits d'auteur, les marques commerciales ou autres avis de propriété ou de confidentialité contenus dans ou sur le logiciel Rocky Linux.

Contrôlez le comportement du DCV sur Rocky Linux WorkSpaces

Le comportement du DCV est contrôlé par les paramètres de configuration du `wsp.conf` fichier, qui se trouve dans le `/etc/wsp/` répertoire. Pour déployer et appliquer les modifications apportées à la politique, utilisez une solution de gestion de configuration compatible avec Rocky Linux. Toutes les modifications prennent effet lorsque l'agent démarre.

Note

Si vous apportez des modifications incorrectes ou non prises en charge aux `wsp.conf` politiques, elles risquent de ne pas être appliquées aux nouvelles connexions établies avec votre WorkSpace.

Les sections suivantes décrivent comment activer ou désactiver certaines fonctionnalités.

Activer ou désactiver la redirection du presse-papiers pour Rocky Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection du presse-papiers pour Rocky Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
clipboard = X
```

Où les valeurs possibles pour `X` sont les suivantes :

`enabled` : la redirection du presse-papiers est activée dans les deux sens (par défaut).

`disabled` : la redirection du presse-papiers est désactivée dans les deux sens.

`paste-only` : la redirection du presse-papiers est activée et vous permet uniquement de copier le contenu de l'appareil client local et de le coller vers le bureau de l'hôte distant.

`copy-only` : la redirection du presse-papiers est activée et vous permet uniquement de copier le contenu du bureau de l'hôte distant et de le coller vers l'appareil client local.

Activer ou désactiver la redirection d'entrée audio pour Rocky Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée audio. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection d'entrée audio pour Rocky Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
audio-in = X
```

Où les valeurs possibles pour `X` sont les suivantes :

enabled : la redirection d'entrée audio est activée (par défaut).

disabled : la redirection d'entrée audio est désactivée.

Activer ou désactiver la redirection d'entrée vidéo pour Rocky Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée vidéo. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection d'entrée vidéo pour Rocky Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
video-in = X
```

Où les valeurs possibles pour **X** sont les suivantes :

enabled : la redirection d'entrée vidéo est activée (par défaut).

disabled : la redirection d'entrée vidéo est désactivée.

Activer ou désactiver la redirection de fuseau horaire pour Rocky Linux WorkSpaces

Par défaut, l'heure dans un espace de travail est définie de manière à refléter le fuseau horaire du client utilisé pour se connecter au Workspace. Ce comportement est contrôlé par redirection de fuseau horaire. Vous pouvez choisir de désactiver la direction du fuseau horaire pour diverses raisons :

- Votre entreprise souhaite que tous les employés travaillent dans un fuseau horaire spécifique (même si certains employés sont dans d'autres fuseaux horaires).
- Vous avez planifié des tâches dans un Workspace qui sont destinées à être exécutées à une certaine heure dans un fuseau horaire spécifique.

- Vos utilisateurs voyagent beaucoup et souhaitent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Utilisez le fichier de configuration DCV pour configurer cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection de fuseau horaire pour Rocky Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
timezone-redirection = X
```

Où les valeurs possibles pour **X** sont les suivantes :

`enabled` : la redirection de fuseau horaire est activée (par défaut).

`disabled` : la redirection de fuseau horaire est désactivée.

Activer ou désactiver la redirection d'imprimante pour Rocky Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection de l'imprimante. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection d'imprimante pour Rocky Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
remote-printing = X
```

Où les valeurs possibles pour **X** sont les suivantes :

enabled : la redirection d'imprimante est activée (par défaut).

disabled : la redirection d'imprimante est désactivée.

Activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour DCV

Activez la déconnexion de la session lors du verrouillage de l'écran pour permettre à vos utilisateurs de mettre fin à leur WorkSpaces session lorsque l'écran de verrouillage est détecté. Pour se reconnecter depuis le WorkSpaces client, les utilisateurs peuvent utiliser leur mot de passe ou leur carte à puce pour s'authentifier, selon le type d'authentification activé pour eux. WorkSpaces

Par défaut, WorkSpaces ne prend pas en charge la déconnexion de la session lors du verrouillage de l'écran. Utilisez le fichier de configuration DCV pour activer cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour Rocky Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
disconnect-on-lock = X
```

Où les valeurs possibles pour **X** sont les suivantes :

enabled : la déconnexion au verrouillage de l'écran est activée.

disabled : la déconnexion au verrouillage de l'écran est désactivée (par défaut).

Accorder un accès SSH aux administrateurs de Rocky Linux WorkSpaces

Par défaut, seuls les utilisateurs et comptes assignés dans le groupe des administrateurs de domaine peuvent se connecter à Rocky Linux WorkSpaces en utilisant SSH. Pour permettre à d'autres utilisateurs et comptes de se connecter à Rocky Linux WorkSpaces via SSH, nous vous recommandons de créer un groupe d'administrateurs dédié pour vos WorkSpaces administrateurs Rocky Linux dans Active Directory.

Pour activer l'accès sudo pour les membres du groupe **Linux_WorkSpaces_Admins** Active Directory

1. Modifiez le fichier `sudoers` en utilisant `visudo`, comme illustré dans l'exemple suivant.

```
[username@workspace-id ~]$ sudo visudo
```

2. Ajoutez la ligne suivante.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Une fois que vous avez créé le groupe d'administrateurs dédié, procédez comme suit pour activer la connexion pour les membres du groupe.

Pour activer la connexion pour les membres du groupe **Linux_WorkSpaces_Admins** Active Directory

1. Modifiez `/etc/security/access.conf` avec des droits élevés.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Ajoutez la ligne suivante.

```
+: (Linux_WorkSpaces_Admins):ALL
```

Avec Rocky Linux, WorkSpaces vous n'avez pas besoin d'ajouter de nom de domaine lorsque vous spécifiez le nom d'utilisateur pour la connexion SSH, et par défaut, l'authentification par mot de passe est désactivée. Pour vous connecter via SSH, vous devez soit ajouter votre clé publique SSH `$HOME/.ssh/authorized_keys` sur votre Rocky Linux WorkSpace, soit la modifier `/etc/ssh/sshd_config` pour la configurer PasswordAuthentication sur. yes Pour plus d'informations sur l'activation des connexions SSH, consultez [Activer les connexions SSH pour votre système Linux](#). WorkSpaces

Remplacer le shell par défaut pour Rocky Linux WorkSpaces

Pour remplacer le shell par défaut de Rocky Linux WorkSpaces, nous vous recommandons de modifier le `~/.bashrc` fichier de l'utilisateur. Par exemple, pour utiliser `Z shell` au lieu du shell Bash, ajoutez les lignes suivantes à `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

Note

Après avoir effectué cette modification, vous devez soit redémarrer le, WorkSpace soit vous déconnecter du WorkSpace (pas simplement vous déconnecter), puis vous reconnecter pour que la modification prenne effet.

Utiliser des cartes à puce pour l'authentification sur Rocky Linux WorkSpaces

WorkSpaces Les packs Rocky Linux permettent l'utilisation de cartes à puce [Common Access Card \(CAC\)](#) et de [vérification d'identité personnelle \(PIV\)](#) pour l'authentification. Pour de plus amples informations, veuillez consulter [Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal](#).

Gérez votre Red Hat Enterprise Linux WorkSpaces

Vous pouvez gérer Red Hat Enterprise Linux à l'aide de solutions de configuration et de gestion, telles qu'[Ansible](#).

Contrôlez le comportement du DCV sur Red Hat Enterprise Linux WorkSpaces

Le comportement du DCV est contrôlé par les paramètres de configuration du `wsp.conf` fichier, qui se trouve dans le `/etc/wsp/` répertoire. Pour déployer et appliquer les modifications apportées à la politique, utilisez une solution de gestion de configuration compatible avec Red Hat Enterprise Linux. Toutes les modifications prennent effet lorsque l'agent démarre.

Note

Si vous apportez des modifications incorrectes ou non prises en charge aux `wsp.conf` politiques, elles risquent de ne pas être appliquées aux nouvelles connexions établies avec votre Workspace.

Les sections suivantes décrivent comment activer ou désactiver certaines fonctionnalités.

Activer ou désactiver la redirection du presse-papiers pour Red Hat Enterprise Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection du presse-papiers pour Red Hat Enterprise Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
clipboard = X
```

Où les valeurs possibles pour `X` sont :

enabled : la redirection du presse-papiers est activée dans les deux sens (par défaut).

disabled : la redirection du presse-papiers est désactivée dans les deux sens.

paste-only : la redirection du presse-papiers est activée et vous permet uniquement de copier le contenu de l'appareil client local et de le coller vers le bureau de l'hôte distant.

copy-only : la redirection du presse-papiers est activée et vous permet uniquement de copier le contenu du bureau de l'hôte distant et de le coller vers l'appareil client local.

Activer ou désactiver la redirection d'entrée audio pour Red Hat Enterprise Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée audio. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection d'entrée audio pour Red Hat Enterprise Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
audio-in = X
```

Où les valeurs possibles pour `X` sont :

enabled : la redirection d'entrée audio est activée (par défaut).

disabled : la redirection d'entrée audio est désactivée.

Activer ou désactiver la redirection d'entrée vidéo pour Red Hat Enterprise Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée vidéo. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection vidéo entrante pour Red Hat Enterprise Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
video-in = X
```

Où les valeurs possibles pour `X` sont :

`enabled` : la redirection d'entrée vidéo est activée (par défaut).

`disabled` : la redirection d'entrée vidéo est désactivée.

Activer ou désactiver la redirection de fuseau horaire pour Red Hat Enterprise Linux WorkSpaces

Par défaut, l'heure dans un espace de travail est définie pour refléter le fuseau horaire du client utilisé pour se connecter au Workspace. Ce comportement est contrôlé par redirection de fuseau horaire. Vous pouvez choisir de désactiver la direction du fuseau horaire pour diverses raisons :

- Votre entreprise souhaite que tous les employés travaillent dans un fuseau horaire spécifique (même si certains employés sont dans d'autres fuseaux horaires).
- Vous avez planifié des tâches dans un Workspace qui sont destinées à être exécutées à une certaine heure dans un fuseau horaire spécifique.
- Vos utilisateurs voyagent beaucoup et souhaitent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Utilisez le fichier de configuration DCV pour configurer cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection de fuseau horaire pour Red Hat Enterprise Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.


```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe [policies].

```
timezone-redirection = X
```

Où les valeurs possibles pour **X** sont :

enabled : la redirection de fuseau horaire est activée (par défaut).

disabled : la redirection de fuseau horaire est désactivée.

Activer ou désactiver la redirection d'imprimante pour Red Hat Enterprise Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection de l'imprimante. Utilisez le fichier de configuration DCV pour désactiver cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la redirection d'imprimante pour Red Hat Enterprise Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe [policies].

```
remote-printing = X
```

Où les valeurs possibles pour **X** sont :

enabled : la redirection d'imprimante est activée (par défaut).

disabled : la redirection d'imprimante est désactivée.

Activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour DCV

Activez la déconnexion de la session lors du verrouillage de l'écran pour permettre à vos utilisateurs de mettre fin à leur WorkSpaces session lorsque l'écran de verrouillage est détecté. Pour se reconnecter depuis le WorkSpaces client, les utilisateurs peuvent utiliser leur mot de passe ou leur carte à puce pour s'authentifier, selon le type d'authentification activé pour eux. WorkSpaces

Par défaut, WorkSpaces ne prend pas en charge la déconnexion de la session lors du verrouillage de l'écran. Utilisez le fichier de configuration DCV pour activer cette fonctionnalité, si nécessaire.

Pour activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour Red Hat Enterprise Linux WorkSpaces

1. Dans un éditeur, ouvrez le fichier `wsp.conf` avec des droits élevés à l'aide de la commande suivante.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Ajoutez la ligne suivante à la fin du groupe `[policies]`.

```
disconnect-on-lock = X
```

Où les valeurs possibles pour **X** sont :

`enabled` : la déconnexion au verrouillage de l'écran est activée.

`disabled` : la déconnexion au verrouillage de l'écran est désactivée (par défaut).

Accorder un accès SSH aux administrateurs de Red Hat Enterprise Linux WorkSpaces

Par défaut, seuls les utilisateurs et comptes assignés dans le groupe des administrateurs de domaine peuvent se connecter à Red Hat Enterprise Linux à l'aide du WorkSpaces protocole SSH. Pour permettre à d'autres utilisateurs et comptes de se connecter à Red Hat Enterprise Linux WorkSpaces via SSH, nous vous recommandons de créer un groupe d'administrateurs dédié pour vos WorkSpaces administrateurs Red Hat Enterprise Linux dans Active Directory.

Pour activer l'accès sudo pour les membres du groupe **Linux_WorkSpaces_Admins** Active Directory

1. Modifiez le fichier `sudoers` en utilisant `visudo`, comme illustré dans l'exemple suivant.

```
[username@workspace-id ~]$ sudo visudo
```

2. Ajoutez la ligne suivante.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Une fois que vous avez créé le groupe d'administrateurs dédié, procédez comme suit pour activer la connexion pour les membres du groupe.

Pour activer la connexion pour les membres du groupe **Linux_WorkSpaces_Admins** Active Directory

1. Modifiez `/etc/security/access.conf` avec des droits élevés.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Ajoutez la ligne suivante.

```
+: (Linux_WorkSpaces_Admins):ALL
```

Avec Red Hat Enterprise Linux, il n'est pas nécessaire d'ajouter un nom de domaine lorsque WorkSpaces vous spécifiez le nom d'utilisateur pour la connexion SSH, et par défaut, l'authentification par mot de passe est désactivée. Pour vous connecter via SSH, vous devez soit ajouter votre clé publique SSH `$HOME/.ssh/authorized_keys` sur votre Red Hat Enterprise Linux WorkSpace, soit la modifier `/etc/ssh/sshd_config` pour la configurer `PasswordAuthentication`

sur. [yes](#) Pour plus d'informations sur l'activation des connexions SSH, consultez [Activer les connexions SSH pour votre système Linux](#). WorkSpaces

Remplacer le shell par défaut pour Red Hat Enterprise Linux WorkSpaces

Pour remplacer le shell par défaut pour Red Hat Enterprise Linux WorkSpaces, nous vous recommandons de modifier le `~/ .bashrc` fichier de l'utilisateur. Par exemple, pour utiliser `Z shell` au lieu du shell Bash, ajoutez les lignes suivantes à `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

Note

Après avoir effectué cette modification, vous devez soit redémarrer le Workspace soit vous déconnecter du Workspace (pas simplement vous déconnecter), puis vous reconnecter pour que la modification prenne effet.

Utiliser des cartes à puce pour l'authentification sur Red Hat Enterprise Linux WorkSpaces

WorkSpaces Les offres Red Hat Enterprise Linux permettent l'utilisation de cartes à puce [CAC](#) ([Common Access Card](#)) et de [vérification d'identité personnelle \(PIV\)](#) pour l'authentification. Pour de plus amples informations, veuillez consulter [Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal](#).

Optimisation WorkSpaces pour une communication en temps réel dans WorkSpaces Personal

Amazon WorkSpaces propose un large éventail de techniques pour faciliter le déploiement d'applications de communications unifiées (UC) telles que Microsoft Teams, Zoom, Webex, etc. Dans les environnements applicatifs contemporains, la plupart des applications de communications unifiées comportent diverses fonctionnalités, notamment des salles de discussion individuelles, des canaux de discussion de groupe collaboratifs, un stockage et un échange de fichiers fluides,

des événements en direct, des webinaires, des diffusions, des fonctionnalités de partage et de contrôle d'écran interactifs, de tableau blanc et de messagerie hors ligne audio/video . La plupart de ces fonctionnalités sont facilement disponibles en WorkSpaces tant que fonctionnalités standard, sans qu'il soit nécessaire de les affiner ou de les améliorer. Cependant, il convient de noter que les éléments de communication en temps réel, en particulier les one-on-one appels et les réunions de groupe collectives, constituent une exception à cette règle. L'intégration réussie de telles fonctionnalités exige souvent une attention et une planification spécifiques au cours du processus de WorkSpaces déploiement.

Lorsque vous planifiez la mise en œuvre des fonctionnalités de communication en temps réel des applications UC sur Amazon WorkSpaces, vous avez le choix entre trois modes de configuration de communication en temps réel (RTC) distincts. Leur sélection dépend des applications spécifiques que vous avez l'intention de fournir aux utilisateurs, et des appareils client que vous comptez utiliser.

Ce document se concentre sur l'optimisation de l'expérience utilisateur pour les applications de communications unifiées les plus courantes sur Amazon WorkSpaces. Pour les optimisations spécifiques à WorkSpaces Core, reportez-vous à la documentation spécifique aux partenaires.

Rubriques

- [Présentation des modes d'optimisation des médias](#)
- [Quel mode d'optimisation de la communication en temps réel \(RTC\) utiliser ?](#)
- [Conseils d'optimisation de la communication en temps réel \(RTC\)](#)

Présentation des modes d'optimisation des médias

Les options d'optimisation des médias disponibles sont les suivantes.

Option 1 : Communication en temps réel optimisée pour les médias (RTC optimisée pour les médias)

Dans ce mode, les applications UC et VoIP tierces sont exécutées sur la télécommande WorkSpace, tandis que leur infrastructure multimédia est déchargée sur le client pris en charge pour une communication directe. Les applications UC suivantes utilisent cette approche sur Amazon WorkSpaces :

- [Réunions Zoom](#)
- [Réunions Cisco Webex](#)
- [Microsoft Teams 2.0 \(version préliminaire publique\)](#)

Pour que le mode RTC Media Optimized fonctionne, le fournisseur de l'application UC doit développer l'intégration à WorkSpaces l'aide de l'un des kits de développement logiciel (SDK) disponibles, tel que le SDK d'extension [DCV](#). Ce mode nécessite l'installation des composants d'UC sur l'appareil client.

Pour en savoir plus sur la configuration de ce mode, consultez [Configuration de la RTC optimisée pour les médias](#).

Option 2 : Communication en temps réel optimisée pendant la session (RTC optimisée pendant la session)

Dans ce mode, l'application UC non modifiée s'exécute sur le WorkSpace, canalisant le trafic audio et vidéo via le DCV vers le dispositif client. Le son local provenant du microphone et le flux vidéo provenant d'une webcam sont redirigés vers le WorkSpace, où ils sont consommés par l'application UC. Ce mode assure une compatibilité étendue entre les applications et fournit efficacement l'application UC depuis la télécommande WorkSpace vers diverses plateformes clientes. Il n'est pas nécessaire de déployer les composants de l'application d'UC sur l'appareil client.

Pour en savoir plus sur la configuration de ce mode, consultez [Configuration de la RTC optimisée en cours de session](#).

Option 3 : Communication directe en temps réel (RTC directe)

Dans ce mode, l'application qui fonctionne dans le système WorkSpace prend le contrôle du poste téléphonique physique ou virtuel situé sur le bureau ou le système d'exploitation client de l'utilisateur. Il en résulte que le trafic audio passe directement du téléphone physique au poste de travail de l'utilisateur, ou du téléphone virtuel installé sur l'appareil client à l'application d'appel pair distante. Les exemples notables d'applications fonctionnant dans ce mode incluent :

- [Optimisation d'Amazon Connect pour Amazon WorkSpaces](#)
- [WebRTC Media Helper de Genesys Cloud](#)
- [Passerelle SIP Microsoft Teams](#)
- [Téléphones de bureau et écrans Microsoft Teams](#)
- Participation à une conférence audio via les fonctionnalités d'appel entrant ou « appeler mon téléphone » de l'application d'UC.

Pour en savoir plus sur la configuration de ce mode, consultez [Configuration du mode RTC directe](#).

Quel mode d'optimisation de la communication en temps réel (RTC) utiliser ?

Différents modes d'optimisation de la RTC peuvent être utilisés simultanément, ou configurés pour se compléter en tant que solution de rechange. Par exemple, envisagez d'activer la RTC optimisée pour les médias lors des réunions Cisco Webex. Cette configuration garantit que les utilisateurs bénéficient d'une communication optimisée lorsqu'ils accèdent WorkSpace via un client de bureau. Toutefois, dans les scénarios où l'on accède à Webex depuis une borne Internet partagée sans composants d'optimisation d'UC, Webex passera de façon fluide au mode RTC optimisée en cours de session afin de maintenir le fonctionnement. Lorsque les utilisateurs utilisent plusieurs applications d'UC, les modes de configuration de la RTC peuvent varier en fonction de leurs besoins uniques.

Le tableau suivant présente les fonctionnalités courantes des applications d'UC, et définit le mode de configuration de la RTC qui fournit le meilleur résultat.

Fonctionnalité	RTC directe	RTC optimisée pour les médias	RTC optimisée en cours de session
Chat individuel	Ne nécessite pas de configuration de la RTC		
Salons de chat de groupe	Ne nécessite pas de configuration de la RTC		
Audioconférence de groupe	Meilleur	Meilleur	Bon
Visioconférence de groupe	Bon	Meilleur	Bon
Appels audio individuels	Meilleur	Meilleur	Bon
Appels vidéo individuels	Bon	Meilleur	Bon
Tableaux blancs	Ne nécessite pas de configuration de la RTC		
Audio/video clips/mesaging	Non applicable	Bon	Meilleur

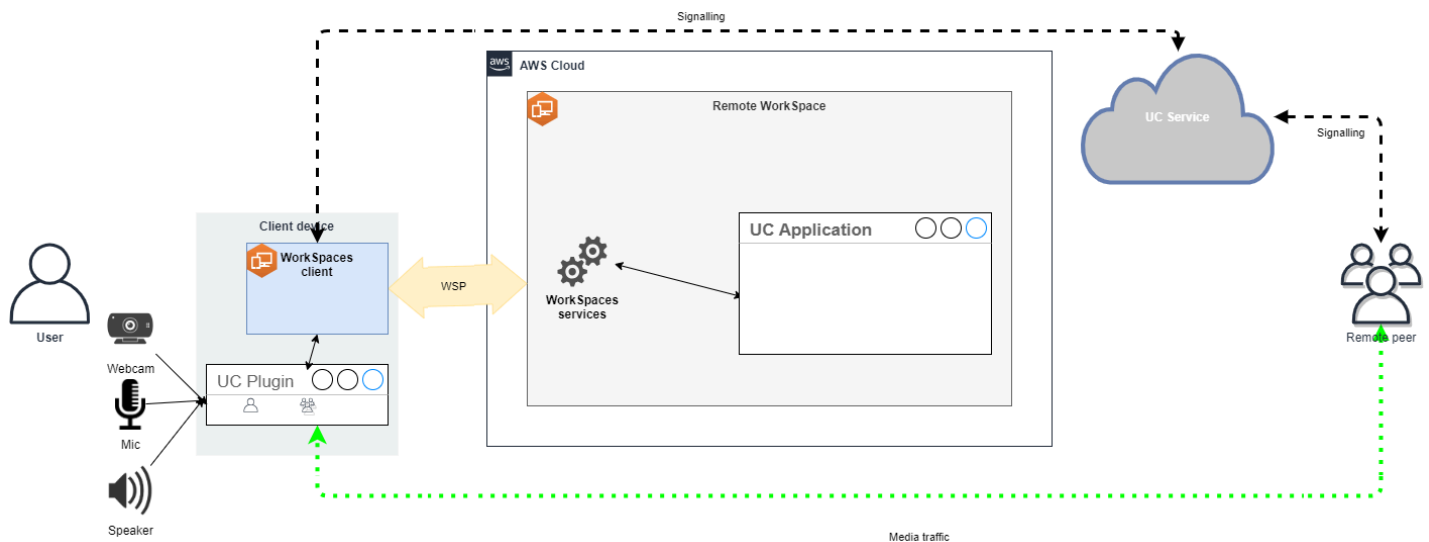
Fonctionnalité	RTC directe	RTC optimisée pour les médias	RTC optimisée en cours de session
Partage de fichiers	Non applicable	Dépend de l'application d'UC	Meilleur
Partage et contrôle d'écran	Non applicable	Dépend de l'application d'UC	Meilleur
Webinaires/événements de diffusion	Non applicable	Bon	Meilleur

Conseils d'optimisation de la communication en temps réel (RTC)

Configuration de la RTC optimisée pour les médias

Le mode RTC Media Optimized est rendu possible par l'utilisation par le fournisseur de l'application UC de celui SDKs fourni par Amazon. L'architecture oblige le fournisseur d'UC à développer un plugin ou une extension spécifique à l'UC, et à les déployer sur le client.

Le SDK, qui inclut des options accessibles au public telles que le SDK d'extension DCV et des versions privées personnalisées, établit un canal de contrôle entre le module d'application UC fonctionnant au sein du module WorkSpace et un plug-in côté client. Généralement, ce canal de contrôle demande à l'extension côté client de lancer ou de rejoindre un appel. Une fois l'appel établi via l'extension côté client, le plug-in d'UC capture le son du microphone et la vidéo de la webcam, qui sont ensuite transmis directement au cloud d'UC ou à une application d'appel pair. Le son entrant est diffusé localement et la vidéo est superposée dans l'interface utilisateur du client distant. Le canal de contrôle est chargé de communiquer le statut de l'appel.



Amazon prend WorkSpaces actuellement en charge les applications suivantes avec le mode RTC optimisé pour les médias :

- [Réunions Zoom](#) (pour PCo IP et DCV) WorkSpaces
- [Réunions Cisco Webex](#) (pour DCV uniquement WorkSpaces)
- [Microsoft Teams 2.0 \(version préliminaire publique\)](#) (pour DCV WorkSpaces uniquement)

Si vous utilisez une application qui ne figure pas dans la liste, il est conseillé de contacter le fournisseur de l'application et de demander de l'aide pour WorkSpaces Media Optimized RTC. Pour accélérer ce processus, encouragez-les à contacter [aws-av-offloading@amazon .com](mailto:aws-av-offloading@amazon.com).

Bien que le mode RTC optimisé pour les médias améliore les performances des appels et minimise l'utilisation des Workspace ressources, il présente certaines limites :

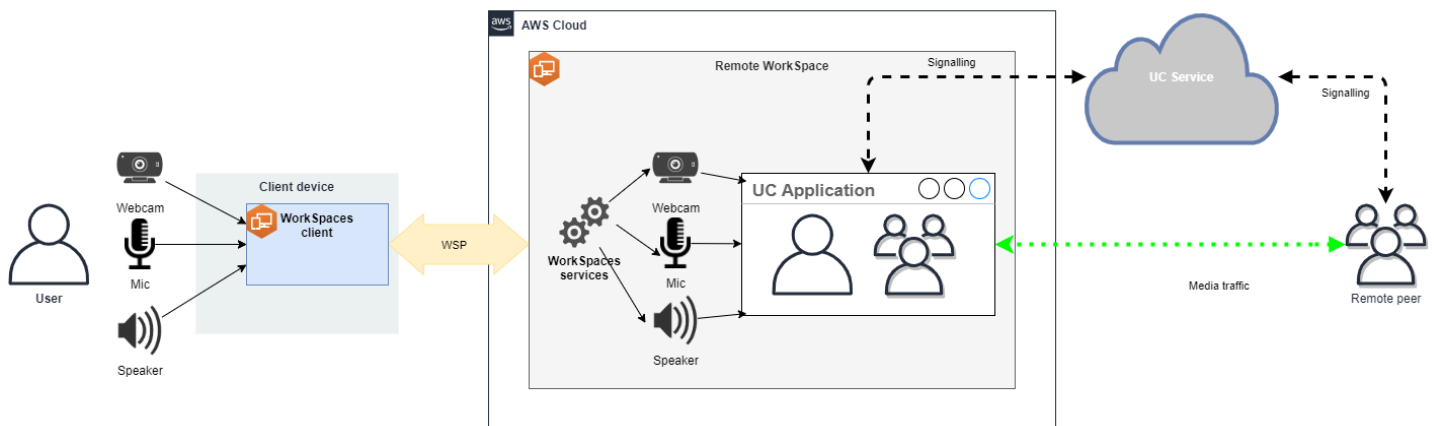
- L'extension client d'UC doit être installée sur l'appareil client.
- L'extension client d'UC nécessite une gestion et des mises à jour indépendantes.
- Les extensions client d'UC peuvent ne pas être disponibles sur certaines plateformes client, comme les plateformes mobiles ou les clients Web.
- Certaines fonctionnalités d'applications d'UC peuvent être limitées dans ce mode. Par exemple, le fonctionnement du partage d'écran peut être différent.
- L'utilisation d'extensions côté client peut ne pas convenir à des scénarios comme Apportez votre propre appareil (BYOD), ou aux bornes partagées.

Si le mode RTC optimisée pour les médias ne convient pas à votre environnement, ou si certains utilisateurs ne peuvent pas installer l'extension client, il est recommandé de configurer le mode RTC optimisée en cours de session comme option de secours.

Configuration de la RTC optimisée en cours de session

En mode RTC optimisé en session, l'application UC fonctionne sur le WorkSpace sans aucune modification, offrant ainsi une expérience locale similaire. Les flux audio et vidéo générés par l'application sont capturés par DCV et transmis au client. Au niveau du client, les signaux du microphone (sur DCV et PCo IP WorkSpaces) et de la webcam (uniquement sur DCV WorkSpaces) sont capturés, redirigés vers l' WorkSpaceapplication UC et transmis de manière fluide à celle-ci.

Cette option garantit notamment une compatibilité exceptionnelle, même avec les applications existantes, et offre une expérience utilisateur cohérente quelle que soit l'origine de l'application. L'optimisation en cours de session fonctionne également avec le client Web.



Le DCV a été méticuleusement optimisé pour améliorer les performances du mode Remote RTC. Les mesures d'optimisation incluent :

- Utilisation d'un transport QUIC adaptatif basé sur UDP, garantissant une transmission de données efficace
- Mise en place d'un chemin audio à faible latence, facilitant une entrée et une sortie audio rapides
- Implémentation de codecs audio optimisés pour la voix afin de conserver la qualité audio tout en réduisant l'utilisation du CPU et du réseau
- Redirection de la webcam permettant l'intégration de ses fonctionnalités
- Configuration de la résolution de la webcam pour optimiser les performances
- Intégration de codecs d'affichage adaptatifs pour équilibrer vitesse et qualité visuelle

- Correction de l'instabilité audio, garantissant une transmission fluide

Ces optimisations contribuent collectivement à une expérience solide et fluide en mode RTC distante.

Recommandations de dimensionnement

Pour prendre en charge efficacement le mode RTC à distance, il est essentiel de garantir le bon dimensionnement d'Amazon WorkSpaces. La télécommande WorkSpace doit satisfaire ou dépasser les exigences système de l'application de communication unifiée (UC) correspondante. Le tableau suivant décrit les WorkSpaces configurations minimales prises en charge et recommandées pour les applications de communications unifiées les plus courantes lorsqu'elles sont utilisées pour des appels vidéo et audio :

Applicati on	Configura tion du CPU requis pour l'applica tion de RTC	Exigences de RAM pour l'applica tion de RTC	Appels vidéo		Appels audio		Référence
			Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	
Microsoft Teams	2 cœurs obligatoi res, 4 recommand és	4 Go de RAM	Power (4 vCPU, 16 Go de mémoire)	• PowerPro (8 vCPU, 32 Go de mémoire) • GeneralF rpose.4xl arge (16 vCPU, 64	Performan ce (2 vCPU, 8 Go de mémoire)	• PowerPro (8 vCPU, 32 Go de mémoire) • GeneralF rpose.4xl arge (16 vCPU, 64	Configura tion matériell e requise pour Microsoft Teams

			Appels vidéo		Appels audio		
Applicati on	Configura tion du CPU requis pour l'applica tion de RTC	Exigences de RAM pour l'applica tion de RTC	Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	Référence
				Go de mémoire)		Go de mémoire)	
				GeneralF rpose8 x large (processu ur 32 V, 128 Go de mémoire)		GeneralF rpose8 x large (processu ur 32 V, 128 Go de mémoire)	

Applicati on	Configura tion du CPU requis pour l'applica tion de RTC	Exigences de RAM pour l'applica tion de RTC	Appels vidéo		Appels audio		Référence
			Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	
Zoom	2 cœurs obligatoi res, 4 recommand és	4 Go de RAM	Power (4 vCPU, 16 Go de mémoire)	- PowerPro (8 vCPU, 32 Go de mémoire) - GeneralF rpose.4xl arge (16 vCPU, 64 Go de mémoire) - GeneralF rpose8 x large (processe ur 32 V, 128 Go de mémoire)	Performan ce (2 vCPU, 8 Go de mémoire)	- PowerPro (8 vCPU, 32 Go de mémoire) - GeneralF rpose.4xl arge (16 vCPU, 64 Go de mémoire) - GeneralF rpose8 x large (processe ur 32 V, 128 Go de mémoire)	Configura tion système requis pour Zoom : Windows, macOS, Linux

Applicati on	Configura tion du CPU requis pour l'applica tion de RTC	Exigences de RAM pour l'applica tion de RTC	Appels vidéo		Appels audio		Référence
			Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	Pris en charge de manière minimale WorkSpace	Recommand é WorkSpace	
Webex	2 cœurs obligatoi res	4 Go de RAM	Power (4 vCPU, 16 Go de mémoire)	- PowerPro (8 vCPU, 32 Go de mémoire) - GeneralF rpose.4xl arge (16 vCPU, 64 Go de mémoire) - GeneralF rpose8 x large (processu ur 32 V, 128 Go de mémoire)	Performan ce (2 vCPU, 8 Go de mémoire)	- PowerPro (8 vCPU, 32 Go de mémoire) - GeneralF rpose.4xl arge (16 vCPU, 64 Go de mémoire) - GeneralF rpose8 x large (processu ur 32 V, 128 Go de mémoire)	Configura tion requis pour les services Webex

Il est important de noter que la visioconférence implique une utilisation importante des ressources pour l'encodage et le décodage vidéo. Dans les scénarios d'ordinateurs physiques, ces tâches sont

déchargées sur le GPU. Dans un environnement autre que WorkSpaces le GPU, ces tâches sont effectuées sur le processeur en parallèle avec le codage du protocole à distance. Par conséquent, pour les utilisateurs régulièrement engagés dans le streaming vidéo ou les appels vidéo, il est fortement recommandé d'opter pour la configuration PowerPro ou une configuration supérieure.

Le partage d'écran consomme également d'importantes ressources, la consommation augmentant avec les résolutions élevées. Par conséquent, sur les appareils autres que le GPU WorkSpaces, le partage d'écran est souvent limité à une fréquence d'images inférieure.

Tirez parti du transport QUIC basé sur UDP avec DCV

Le transport UDP est particulièrement adapté à la transmission d'applications de RTC. Pour optimiser l'efficacité, assurez-vous que votre réseau est configuré pour utiliser le transport QUIC pour le DCV. Notez que le transport basé sur UDP n'est disponible qu'avec les clients natifs.

Configurer l'application UC pour WorkSpaces

Pour améliorer les capacités de traitement vidéo, telles que le flou d'arrière-plan, les arrière-plans virtuels, les réactions ou l'hébergement d'événements en direct, il WorkSpace est essentiel d'opter pour un processeur graphique afin d'obtenir des performances optimales.

La plupart des applications UC fournissent des conseils pour désactiver le traitement vidéo avancé afin de réduire l'utilisation du processeur sur des appareils autres que le GPU WorkSpaces.

Pour plus d'informations, consultez les ressources suivantes.

- Microsoft Teams : [Considérations relatives aux performances de Teams sur VDI](#)
- Réunions Zoom : [Managing the user experience for incompatible VDI plugins](#)
- Webex : [Deployment guide for Webex App for Virtual Desktop Infrastructure \(VDI\) - Manage and troubleshoot Webex App for VDI \[Webex App\]](#)
- Google Meet : [Utiliser une infrastructure VDI](#)

Activation de la redirection bidirectionnelle du son et de la webcam

Amazon prend WorkSpaces en charge par défaut l'entrée audio, la sortie audio et la redirection de caméra via l'entrée vidéo. Toutefois, si ces fonctionnalités ont été désactivées pour des raisons spécifiques, vous pouvez suivre les instructions fournies pour réactiver la redirection. Pour plus d'informations, reportez-vous à la section [Activer ou désactiver la redirection vidéo pour DCV dans le guide](#) d'administration Amazon WorkSpaces. Après leur connexion, les utilisateurs doivent sélectionner la caméra qu'ils souhaitent utiliser en session. Pour plus d'informations, les utilisateurs

sont invités à consulter la section [Webcams et autres appareils vidéo](#) du guide de WorkSpaces l'utilisateur Amazon.

Limitation de la résolution maximale de la webcam

Pour les utilisateurs utilisant Power PowerPro, GeneralPurpose .4xlarge ou GeneralPurpose .8xlarge WorkSpaces pour la visioconférence, il est fortement recommandé de limiter la résolution maximale des webcams redirigées. Dans le cas de PowerPro GeneralPurpose .4xlarge ou de GeneralPurpose .8xlarge, la résolution maximale recommandée est de 640 pixels en largeur par 480 pixels en hauteur. Pour Power, la résolution maximale recommandée est de 320 pixels de large sur 240 pixels de haut.

Procédez comme suit pour configurer la résolution maximale de la webcam.

1. Ouvrez l'Éditeur du Registre Windows.
2. Accédez au chemin de registre suivant :

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. Créez une valeur de chaîne nommée `max-resolution` et définissez-la à la résolution souhaitée dans le format (X,Y), où X représente le nombre de pixels horizontaux (largeur) et Y le nombre de pixels verticaux (hauteur). Par exemple, spécifiez (640,480) pour représenter une résolution de 640 pixels de large et 480 pixels de haut.

Activation de la configuration audio optimisée pour la voix

Par défaut, WorkSpaces ils sont configurés pour fournir un son haute fidélité 7.1 WorkSpaces à destination du client, garantissant ainsi une qualité de lecture musicale supérieure. Toutefois, si la conférence audio ou vidéo constitue votre principal cas d'utilisation, la modification du profil du codec audio vers un paramètre optimisé pour la voix peut permettre d'économiser les ressources du CPU et du réseau.

Procédez comme suit pour définir le profil audio comme optimisé pour la voix.

1. Ouvrez l'Éditeur du Registre Windows.
2. Accédez au chemin de registre suivant :

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

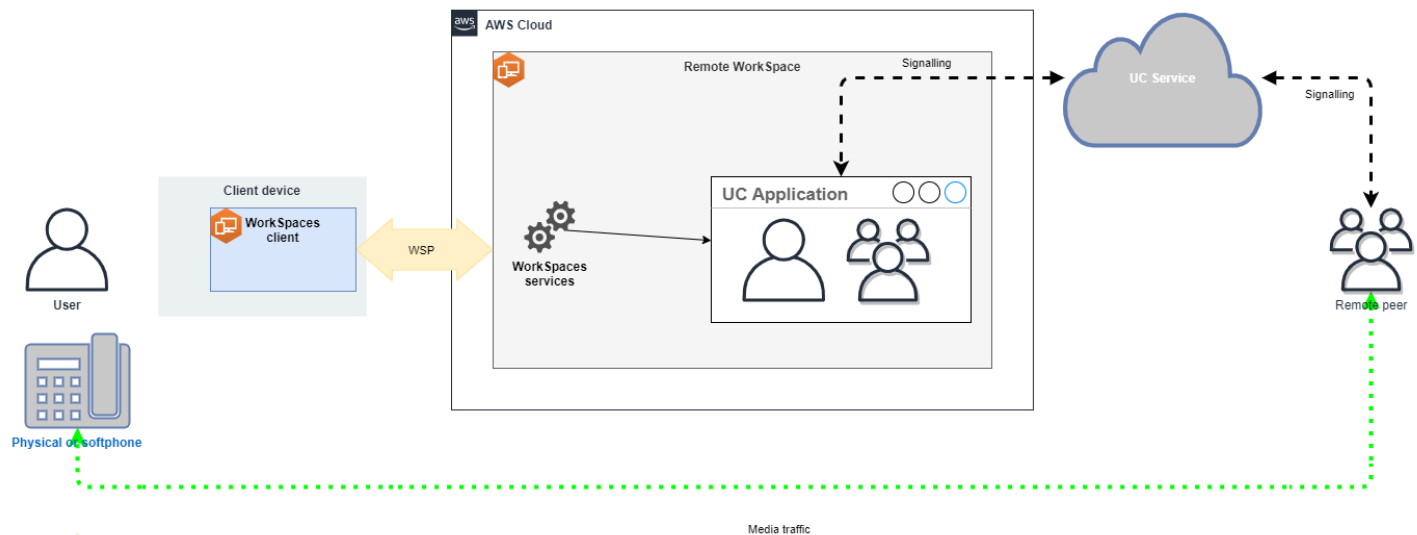
3. Créez un nom de valeur de chaîne `default-profile` et définissez-le à `voice`.

Utilisation de casques de bonne qualité pour les appels audio et vidéo

Pour améliorer l'expérience audio et éviter les échos, il est essentiel d'utiliser des casques haut de gamme. L'utilisation de haut-parleurs de bureau peut entraîner des problèmes d'écho du côté distant de l'appel.

Configuration du mode RTC directe

La configuration du mode Direct RTC dépend de l'application de communication unifiée (UC) spécifique et ne nécessite aucune modification de WorkSpaces configuration. La liste suivante propose une compilation non exhaustive des optimisations pour diverses applications d'UC.



- Microsoft Teams :
 - [Planifier la passerelle SIP](#)
 - [Audioconférence dans Microsoft 365](#)
 - [Planifier votre solution vocale Teams](#)
- Réunions Zoom :
 - [Enabling or disabling toll call dial-in numbers](#)
 - [Using desk phone call control](#)
 - [Desk phone companion mode](#)
- WebEx :
 - [Application Webex | Appeler avec votre téléphone de bureau](#)
 - [Application Webex | Options d'appel prises en charge](#)
- BlueJeans:

- [Dialing into a Meeting from a Desk Telephone](#)
- Genesys :
 - [WebRTC Media Helper de Genesys Cloud](#)
- Amazon Connect :
 - [Optimisation d'Amazon Connect pour Amazon WorkSpaces](#)
- Google Meet :
 - [Utiliser un téléphone pour le son d'une visioconférence](#)

Gérer le mode de course dans WorkSpaces Personal

Le mode de fonctionnement d'un produit WorkSpace détermine sa disponibilité immédiate et le mode de paiement (mensuel ou horaire). Vous pouvez choisir entre les modes de fonctionnement suivants lorsque vous créez le WorkSpace :

- AlwaysOn— À utiliser lorsque vous payez un abonnement mensuel fixe pour une utilisation illimitée de votre WorkSpaces. Ce mode est idéal pour les utilisateurs qui utilisent leur poste de travail principal à WorkSpace plein temps.
- AutoStop— À utiliser lorsque vous payez WorkSpaces à l'heure. Avec ce mode, vous vous WorkSpaces arrêtez après une période de déconnexion spécifiée, et l'état des applications et des données est enregistré.

Pour plus d'informations, consultez [Tarification d'WorkSpaces](#).

AutoStop WorkSpaces

Pour définir l'heure d'arrêt automatique, sélectionnez-la WorkSpace dans la WorkSpaces console Amazon, choisissez Actions, Modifier les propriétés du mode d'exécution, puis définissez l'AutoStop heure (heures). Par défaut, l'AutoStop heure (heures) est définie sur 1 heure, ce qui signifie qu'elle WorkSpace s'arrête automatiquement une heure après la WorkSpace déconnexion.

Une fois WorkSpace qu'un est déconnecté et que le AutoStop délai a expiré, l' WorkSpace arrêt automatique peut prendre plusieurs minutes supplémentaires. Toutefois, la facturation s'arrête dès l'expiration du AutoStop délai, et ce délai supplémentaire ne vous est pas facturé.

Lors de l'hibernation du WorkSpaces support, l'état du bureau est enregistré sur le volume racine du WorkSpace. Le WorkSpace reprend lorsqu'un utilisateur se connecte. Tous les documents ouverts et

les programmes en cours d'exécution retrouvent leur état enregistré, tous les systèmes WorkSpaces d'exploitation prenant en charge l'hibernation.

AutoStop Compatible avec le GPU WorkSpaces et les formats GeneralPurpose .4xlarge ou GeneralPurpose .8xlarge ne prennent pas en charge l'hibernation. L'état de n' applications/data est pas conservé. Nous vous recommandons de sauvegarder votre travail lorsque vous avez fini de l'utiliser à WorkSpaces chaque fois pour éviter toute perte de données.

Dans le cas de la licence Bring Your Own License (BYOL) AutoStop WorkSpaces, un grand nombre de connexions simultanées peut entraîner une augmentation significative du délai WorkSpaces de disponibilité. Si vous vous attendez à ce que de nombreux utilisateurs se connectent AutoStop WorkSpaces à votre BYOL en même temps, veuillez consulter votre responsable de compte pour obtenir des conseils.

 Important

AutoStop WorkSpaces ne s'arrêtent automatiquement que s' WorkSpaces ils sont déconnectés.

A Workspace est déconnecté uniquement dans les cas suivants :

- Si l'utilisateur se déconnecte Workspace ou quitte manuellement l'application WorkSpaces client Amazon.
- Si l'appareil client est arrêté.
- S'il n'y a aucune connexion entre l'appareil client et le Workspace pendant plus de 20 minutes.

Il est recommandé AutoStop Workspace aux utilisateurs de se déconnecter manuellement WorkSpaces lorsqu'ils ont fini de les utiliser chaque jour. Pour vous déconnecter manuellement, choisissez Déconnecter Workspace ou Quitter Amazon dans le WorkSpaces WorkSpaces menu Amazon des applications WorkSpaces clientes pour Linux, macOS ou Windows. Pour Android ou iPad, choisissez Déconnecter dans le menu latéral.

AutoStop WorkSpaces peut ne pas s'arrêter automatiquement dans les situations suivantes :

- Si l'appareil client est uniquement verrouillé, en veille ou inactif (par exemple, si le capot de l'ordinateur portable est fermé) au lieu d'être arrêté, l' WorkSpaces application est peut-être toujours en cours d'exécution en arrière-plan. Tant que l' WorkSpaces application est toujours en

cours d'exécution, il WorkSpace se peut qu'elle ne soit pas déconnectée et WorkSpace qu'elle ne s'arrête donc pas automatiquement.

- WorkSpaces ne peut détecter la déconnexion que lorsque les utilisateurs utilisent des WorkSpaces clients. Si les utilisateurs utilisent des clients tiers, ils ne seront WorkSpaces peut-être pas en mesure de détecter la déconnexion. Par conséquent, il est WorkSpaces possible que la déconnexion ne s'arrête pas automatiquement et que la facturation ne soit pas suspendue.

Modification du mode d'exécution

Vous pouvez passer d'un mode de fonctionnement à un autre à tout moment.

Pour modifier le mode de fonctionnement d'un WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le WorkSpace à modifier, puis choisissez Actions, Modifier le mode d'exécution.
4. Sélectionnez le nouveau mode d'exécution AlwaysOn ou AutoStop, puis cliquez sur Enregistrer.

Pour modifier le mode de fonctionnement d'un à WorkSpace l'aide du AWS CLI

Utilisez la commande [modify-workspace-properties](#).

Arrêtez et démarrez un AutoStop WorkSpace

Lorsque vous AutoStop WorkSpaces êtes déconnecté, ils s'arrêtent automatiquement après une période de déconnexion spécifiée et la facturation horaire est suspendue. Pour optimiser davantage les coûts, vous pouvez suspendre manuellement les frais horaires associés à AutoStop WorkSpaces. Les WorkSpace arrêts et toutes les applications et données sont enregistrés pour la prochaine fois qu'un utilisateur se connecte au WorkSpace.

Lorsqu'un utilisateur se reconnecte à un appareil arrêté WorkSpace, celui-ci reprend là où il s'était arrêté, généralement en moins de 90 secondes.

Vous pouvez redémarrer (redémarrer) AutoStop WorkSpaces s'ils sont disponibles ou s'ils présentent un état d'erreur.

Pour arrêter un AutoStop WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le Workspace pour arrêter, puis choisissez Actions, Arrêter WorkSpaces.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter Workspace.

Pour démarrer un AutoStop Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le WorkSpaces pour commencer, puis choisissez Actions, Démarrer WorkSpaces.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Démarrer Workspace.

Pour supprimer les coûts d'infrastructure fixes qui y sont associés AutoStop WorkSpaces, supprimez les Workspace de votre compte. Pour de plus amples informations, veuillez consulter [Supprimer un Workspace dans WorkSpaces Personal](#).

Pour arrêter et démarrer et AutoStop Workspace utiliser le AWS CLI

Utilisez les [WorkSpaces commandes stop WorkSpaces et start](#).

Gérer les applications dans WorkSpaces Personal

Après avoir lancé un Workspace, vous pouvez voir la liste de tous les ensembles d'applications qui vous sont associés Workspace sur la WorkSpaces console.

Pour voir la liste de tous les ensembles d'applications associés à votre Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation de gauche, choisissez WorkSpaces.
3. Sélectionnez le Workspace et choisissez Afficher les détails.
4. Sous Applications, recherchez la liste des applications qui y sont associées Workspace, ainsi que leur état d'installation.

Vous pouvez mettre à jour les ensembles d'applications sur votre ordinateur de la Workspace manière suivante :

- Installez des ensembles d'applications sur votre Workspace

- Désinstallez les ensembles d'applications de votre WorkSpace
- Installez des ensembles d'applications et désinstallez un autre ensemble d'applications sur votre WorkSpace

Note

- Pour mettre à jour les ensembles d'applications, ils WorkSpace doivent avoir le statut AVAILABLE ou STOPPED.
- La gestion des applications n'est disponible que pour Windows WorkSpaces.
- La gestion des applications n'est disponible que pour les offres d'applications auxquelles vous êtes abonné via AWS.

Offres groupées prises en charge pour la gestion des applications

Gérer les applications vous permet d'installer et de désinstaller les applications suivantes sur votre WorkSpaces. Pour l'offre groupée Microsoft Office 2016 et pour Microsoft Office 2019, vous ne pouvez que désinstaller.

- Microsoft Office LTSC Professionnel Plus 2024
- Microsoft Visio LTSC Professionnel 2024
- Microsoft Project Professional 2024
- Norme Microsoft Office LTSC 2024
- Norme Microsoft Visio LTSC 2024
- Microsoft Project Standard 2024
- Microsoft Office LTSC Professionnel Plus 2021
- Microsoft Visio LTSC Professionnel 2021
- Microsoft Project Professionnel 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021
- Microsoft Visual Studio Professionnel 2022
- Microsoft Visual Studio Entreprise 2022

Le tableau suivant présente la liste des combinaisons d'applications et de systèmes d'exploitation prises en charge et non prises en charge :

	Microsoft Office Professional Plus 2019 (32 bits)	Microsoft Office Professional Plus 2019 (64 bits)	Microsoft Office LTSC Professional Plus 2024 (64 bits)	Microsoft Project Professional Standard 2024 (64 bits)	Microsoft Visio Professional/Standard 2024 (64 bits)	Microsoft Office LTSC Professional Plus/Standard 2019 (64 bits)	Microsoft Project Professional/Standard 2019 (64 bits)	Microsoft Office LTSC Professional/Standard 2019 (64 bits)	Microsoft Visual Studio Professional/Enterprise 2022
Windows Server 2019	Désinstallation	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Windows Server 2022	Non pris en charge	Désinstallation	Non pris en charge	Non pris en charge	Non pris en charge	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation	Non pris en charge
Windows Server 2025	Non pris en charge	Désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation
Windows Server 2025	Non pris en charge	Désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation	Non pris en charge	Non pris en charge	Non pris en charge	Installation/désinstallation

	Microso Office Profess nnel Plus 20 (32 bits)	Microso Office Profess nnel Plus 20 (64 bits)	Microso LTSC Office Profess nal/ Stand ard 2024 (64 bits) 2024 (64 bits)	Microso Project Profess nal/ Stand ard 2024 (64 bits)	Microsoft Visio Professional/ Standard 2024 (64 bits)	Microso LTSC Office Profess nnel Plus/ Stand ard 20 (64 bits)	Microso Project Profess nnel/ Stand ard 20 (64 bits)	Microso LTSC Visio Profess nnel/ Stand ard 20 (64 bits)	Microsoft Visual Studio Professio nnel/ Entr eprise 2022
Window 10	Désinst lation	Désinst lation	Non pris en charge	Non pris en charge	Non pris en charge	Installat ion/ désin stallatio n	Installat ion/ désin stallatio n	Installat ion/ désin stallatio n	Installat ion/ désin stallatio n
Window	Désinst lation	Désinst lation	Installat ion/ désin stallatio n	Installat ion/ désin stallatio n	Installation/ désinstallation	Installat ion/ désin stallatio n	Installat ion/ désin stallatio n	Installat ion/ désin stallatio n	Installat ion/ désin stallatio n

Important

- Microsoft Office/Visio/Project doit suivre les mêmes éditions. Par exemple, vous ne pouvez pas mélanger des applications Standard avec des applications Professionnel.
- Microsoft Office/Visio/Project doit suivre les mêmes versions. Par exemple, vous ne pouvez pas mélanger les applications 2019 avec celles de 2021.
- Microsoft Office/Visio/Project 2021 and 2024 Standard/Professional n'est pas pris en charge pour Value, Graphics et GraphicsPro WorkSpaces les offres groupées.
- Office/Visio/Project Les versions Microsoft 2010 et 2013 (éditions Standard ou Professionnel) ne sont plus prises en charge.

- De plus, les offres groupées avec Office 2016 ou Office 2019 ne seront plus prises en charge après le 14 octobre 2025. Nous vous recommandons de migrer vos WorkSpaces offres groupées avec ces versions d'Office pour utiliser Office 2021 ou Office 2024. Pour plus d'informations, voir [Gérer les applications dans WorkSpaces Personal](#).
- Microsoft Office, Project et Visio nécessitent jusqu'à 25 Go d'espace libre pour les versions 2024 et jusqu'à 20 Go pour les versions 2021.
- Value, Standard, Graphics et GraphicsPro WorkSpaces les offres groupées ne sont pas pris en charge par Microsoft Visual Studio 2022 Enterprise/Professional. Les ensembles de performances peuvent être utilisés pour les charges de travail Visual Studio moins gourmandes en ressources. Toutefois, pour de meilleurs résultats, nous vous recommandons d'utiliser Visual Studio avec des types de bundle à quatre cœurs ou supérieurs. Les types de bundle Power, General Purpose.4XLarge PowerPro, General Purpose.8XLarge, Graphics.G6, Graphics.G4DN et .g4dn répondent à cette exigence. GraphicsPro Pour plus d'informations, consultez la section [Configuration système requise pour la famille de produits Visual Studio 2022](#).
- Lorsque vous désinstallez le bundle d'applications Plus pour Microsoft Office 2016 de votre compte WorkSpaces, vous perdez l'accès à toutes les solutions Trend Micro incluses dans ce WorkSpaces bundle Amazon. Si vous souhaitez continuer à utiliser les solutions Trend Micro avec votre Amazon WorkSpaces, vous pouvez les acheter séparément sur le [AWS marché](#).
- Pour accéder aux applications install/uninstall Microsoft 365, vous devez apporter vos propres outils et installateurs. Gérer le flux de travail des applications ne peut pas être utilisé par les applications install/uninstall Microsoft 365.
- Vous pouvez créer une image personnalisée de WorkSpaces with applications installed/uninstalled via Gérer les applications.
- Pour les régions optionnelles, telles que l'Afrique (Le Cap), la connexion WorkSpaces Internet doit être activée au niveau de l'annuaire.

Mettre à jour les ensembles d'applications sur un WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez WorkSpace et choisissez Actions, Gérer les applications.

4. Sous Applications actuelles, vous verrez une liste des ensembles d'applications déjà installés sur ce site WorkSpace et sous Choisir des applications, vous trouverez une liste des ensembles d'applications disponibles pour installation sur celui-ci. WorkSpace
5. Pour installer des ensembles d'applications sur ce WorkSpace site, procédez comme suit :
 - a. Sélectionnez le bundle d'applications que vous souhaitez y installer WorkSpace, puis choisissez Associer.
 - b. Répétez l'étape précédente pour installer d'autres offres d'applications.
 - c. Pendant l'installation, les offres d'applications sont visibles sous Applications actuelles avec le statut Pending install deployment.
6. Pour désinstaller des ensembles d'applications à partir de ce WorkSpace fichier, procédez comme suit :
 - a. Sous Choisir des applications, sélectionnez l'offre d'applications que vous souhaitez désinstaller, puis choisissez Dissocier.
 - b. Répétez l'étape précédente pour désinstaller d'autres offres d'applications.
 - c. Pendant la désinstallation, les offres d'applications sont visibles sous Applications actuelles avec le statut Pending uninstall deployment.
7. Pour rétablir l'état d'installation ou de désinstallation des offres groupées, effectuez l'une des opérations suivantes.
 - Si vous souhaitez rétablir les offres groupées qui sont à l'état Pending uninstall deployment, sélectionnez l'application à rétablir, puis choisissez Associer.
 - Si vous souhaitez rétablir les offres groupées qui sont à l'état Pending install deployment, sélectionnez l'application à rétablir, puis choisissez Dissocier.
8. Une fois que le statut des offres d'applications que vous avez choisi d'installer ou de désinstaller est En attente, choisissez Déployer les applications.

 Important

Une fois que vous avez sélectionné Déployer les applications, la session de l'utilisateur final se WorkSpaces terminera et ne sera pas accessible pendant l'installation ou la désinstallation des applications.

9. Pour confirmer vos actions, tapez confirmer. Choisissez forcer pour installer ou désinstaller les offres d'applications présentant l'état Erreur.

10. Pour surveiller l'avancement des offres d'applications :

- a. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
- b. Dans le panneau de navigation, sélectionnez WorkSpaces. Sous Statut, vous pouvez voir les statuts suivants :
 - MISE À JOUR : la mise à jour de l'offre d'applications est toujours en cours.
 - DISPONIBLE/ARRÊTÉE - La mise à jour du bundle d'applications est terminée et son état d'origine WorkSpace est revenu à son état d'origine.
- c. Pour surveiller l'état d'installation ou de désinstallation de vos ensembles d'applications, sélectionnez WorkSpace et choisissez Afficher les détails. Sous Applications, Statut, vous pouvez voir les statuts tels que Pending install, Pending uninstall, et Installed.

Note

Si vos utilisateurs constatent que les ensembles d'applications qu'ils ont récemment installés par le biais d'applications gérées ne sont pas activés par licence, vous pouvez effectuer un WorkSpace redémarrage manuel. Les utilisateurs peuvent commencer à utiliser ces applications après un redémarrage. Pour obtenir une assistance supplémentaire, contactez [AWS Support](#).

Mettre à jour les charges de travail Microsoft Visual Studio 2022 sur un WorkSpace

Par défaut, Microsoft Visual Studio 2022 est installé avec les charges de travail suivantes et nécessite 18 Go d'espace disque :

- Éditeur principal de Visual Studio
- Développement Azure
- Stockage et traitement des données
- Développement de bureau .NET
- Développement d'une interface utilisateur d'application multiplateforme NET
- ASP.NET et développement Web
- Développement de Node.js

Les utilisateurs ont la possibilité d'ajouter ou de supprimer des charges de travail et des composants individuels, ce qui leur permet d'adapter l'application à leurs besoins spécifiques. Il est important de noter que l'installation de charges de travail supplémentaires nécessite davantage d'espace disque. Pour en savoir plus sur les configurations de charge de travail, voir [Modifier les charges de travail, les composants et les modules linguistiques de Visual Studio](#).

Gestion des WorkSpaces modifications à l'aide de la fonction Gérer les

Après avoir installé ou désinstallé des ensembles d'applications sur votre ordinateur WorkSpaces, les actions suivantes peuvent avoir un impact sur les configurations existantes.

- **Restaurer un WorkSpace** - La restauration d'un WorkSpace permet de recréer à la fois le volume racine et le volume utilisateur, sur la base des instantanés les plus récents de ces volumes créés alors que le volume WorkSpace était sain. WorkSpace Des instantanés complets sont pris toutes les 12 heures. Pour plus d'informations, consultez [Restaurer un WorkSpace](#). Assurez-vous d'attendre au moins 12 heures avant de restaurer vos WorkSpaces applications modifiées à l'aide de la fonctionnalité Gérer les applications. La restauration de votre instantané complet WorkSpaces avant le suivant, qui a été modifié à l'aide de la fonctionnalité Gérer les applications, aura les résultats suivants :
 - Les ensembles d'applications qui ont été installés sur vous à WorkSpaces l'aide du flux de travail de gestion des applications seront supprimés de votre compte, WorkSpaces mais la licence sera toujours activée et ces applications WorkSpaces vous seront facturées. Pour récupérer ces ensembles d'applications sur votre ordinateur, WorkSpaces vous devez exécuter à nouveau le flux de travail de gestion des applications, désinstaller l'application pour recommencer, puis la réinstaller.
 - Les ensembles d'applications qui vous ont été retirés à WorkSpaces l'aide du flux de travail de gestion des applications seront de nouveau disponibles sur votre WorkSpaces. Toutefois, elles ne fonctionneront pas correctement, car la licence n'est pas activée. Pour vous débarrasser de ces ensembles d'applications, exécutez une désinstallation manuelle de ces ensembles d'applications de votre. WorkSpaces
- **Reconstruire un WorkSpace** - La reconstruction d'un permet de WorkSpace recréer le volume racine. Pour plus d'informations, voir [Reconstruire un WorkSpace](#). La reconstruction de vos WorkSpaces applications modifiées à l'aide de Manage applications se traduira par les résultats suivants :
 - Les ensembles d'applications qui ont été installés sur vous à WorkSpaces l'aide du flux de travail de gestion des applications seront supprimés et désactivés de votre. WorkSpaces Pour remettre

ces applications sur votre ordinateur, WorkSpaces vous devez exécuter à nouveau le flux de travail de gestion des applications.

- Les ensembles d'applications qui ont été supprimés de votre flux de travail WorkSpaces via Manage applications seront installés et activés sur votre WorkSpaces. Pour supprimer ces ensembles d'applications de votre ordinateur WorkSpaces, vous devez exécuter à nouveau le flux de travail de gestion des applications.
- Migrer un Workspace - Le processus de migration recrée le en Workspace utilisant un nouveau volume racine à partir de l'image du bundle cible et le volume utilisateur à partir du dernier instantané disponible de l'original Workspace. Un nouveau Workspace nom avec un nouvel Workspace identifiant est créé. Pour plus d'informations, voir [Migrer une Workspace](#) migration WorkSpaces qui a été modifiée à l'aide de la fonctionnalité Gérer les applications entraînera les résultats suivants :
 - Tous les ensembles d'applications provenant de la source WorkSpaces seront supprimés et désactivés. La nouvelle destination WorkSpaces héritera des applications du WorkSpaces bundle de destination. Les offres groupées WorkSpaces d'applications source seront facturées pour le mois complet, mais les offres groupées d'applications associées à l'offre de destination seront facturées au prorata.

Modifier un Workspace dans WorkSpaces Personal

Après avoir lancé un Workspace, vous pouvez modifier sa configuration de trois manières :

- Vous pouvez modifier la taille de son volume racine (pour Windows, lecteur C ; pour Linux, /) et de son volume utilisateur (pour Windows, lecteur D ; pour Linux /home).
- Vous pouvez modifier son type de calcul pour sélectionner un nouveau bundle.
- Vous pouvez modifier le protocole de streaming à l'aide de la AWS CLI ou de WorkSpaces l'API Amazon si vous avez Workspace été créé avec des bundles PCo IP.

Pour voir l'état de modification actuel d'un Workspace, sélectionnez la flèche pour afficher plus de détails à ce sujet Workspace. Les valeurs possibles pour État sont Modification du calcul, Modification du stockage et Aucun.

Si vous souhaitez modifier un Workspace, il doit avoir le statut AVAILABLE ou STOPPED. Vous ne pouvez pas modifier la taille du volume et le type de calcul en même temps.

La modification de la taille du volume ou du type de calcul d'un WorkSpace modifiera le taux de facturation du WorkSpace.

Pour permettre à vos utilisateurs de modifier eux-mêmes leurs volumes et leurs types de calcul, reportez-vous à la section [Activez les fonctionnalités de WorkSpaces gestion en libre-service pour vos utilisateurs dans Personal WorkSpaces](#).

Modification de la taille des volumes

Vous pouvez augmenter la taille des volumes root et utilisateur jusqu'à 2 000 Go chacun. WorkSpace WorkSpace les volumes root et utilisateur sont regroupés dans des groupes définis qui ne peuvent pas être modifiés. Les groupes disponibles sont :

[Racine (Go), Utilisateur (Go)]

[80, 10]

[80, 50]

[80, 100]

[175 à 2000, 100 à 2000]

Vous pouvez développer les volumes racine et utilisateur, qu'ils soient chiffrés ou non, et vous pouvez développer les deux volumes une fois sur une période de 6 heures. Toutefois, vous ne pouvez pas augmenter la taille des volumes racine et utilisateur en même temps. Pour plus d'informations, consultez [Limitations relatives à l'augmentation des volumes](#).

Note

Lorsque vous étendez un volume pour un WorkSpace, étend WorkSpaces automatiquement la partition du volume sous Windows ou Linux. Lorsque le processus est terminé, vous devez redémarrer le WorkSpace pour que les modifications prennent effet.

Pour garantir la préservation de vos données, vous ne pouvez pas réduire la taille des volumes root ou utilisateur après avoir lancé un WorkSpace. Assurez-vous plutôt de spécifier les tailles minimales pour ces volumes lorsque vous lancez un WorkSpace.

- Vous pouvez lancer un volume Value, Standard, Performance, Power ou PowerPro WorkSpace avec un minimum de 80 Go pour le volume racine et de 10 Go pour le volume utilisateur.
- Vous pouvez lancer un GeneralPurpose fichier .4xlarge ou GeneralPurpose .8xlarge WorkSpace avec un minimum de 175 Go pour le volume racine et de 100 Go pour le volume utilisateur.
- Vous pouvez lancer un Graphics.G6, Graphics.G4DN, GraphicsPro .g4dn, ou GraphicsPro WorkSpace avec un minimum de 100 Go pour le volume racine et de 100 Go pour le volume utilisateur. Les exigences relatives au dimensionnement des volumes varient en fonction des types d'instances graphiques de plus grande taille.

Pendant qu'une augmentation de la taille du WorkSpace disque est en cours, les utilisateurs peuvent effectuer la plupart des tâches sur leur disque WorkSpace. Cependant, ils ne peuvent pas modifier leur type de WorkSpace calcul, changer de mode WorkSpace d'exécution, reconstruire leur WorkSpace ordinateur ou redémarrer (redémarrer) leur ordinateur WorkSpace.

 Note

Si vous souhaitez que vos utilisateurs puissent utiliser leur disque WorkSpaces pendant que l'augmentation de la taille du disque est en cours, assurez-vous qu' WorkSpaces ils ont le statut AVAILABLE au lieu de STOPPED avant de redimensionner les volumes du WorkSpaces. Si tel est le cas STOPPED, WorkSpaces ils ne peuvent pas être démarrés pendant que l'augmentation de la taille du disque est en cours.

Généralement, le processus d'augmentation de la taille des disques peut prendre jusqu'à deux heures. Toutefois, si vous modifiez la taille des volumes pour un grand nombre de WorkSpaces, le processus peut prendre beaucoup plus de temps. Si vous en avez un grand nombre WorkSpaces à modifier, nous vous recommandons de contacter AWS Support pour obtenir de l'aide.

Limites d'augmentation des volumes

- Vous pouvez redimensionner uniquement les volumes SSD.
- Lorsque vous lancez un WorkSpace, vous devez attendre 6 heures avant de pouvoir modifier la taille de ses volumes.
- Vous ne pouvez pas augmenter la taille des volumes racine et utilisateur en même temps. Pour augmenter le volume racine, vous devez d'abord modifier le volume utilisateur en le définissant sur 100 Go. Une fois cette modification effectuée, vous pouvez mettre à jour le volume racine en

utilisant n'importe quelle valeur comprise entre 175 et 2 000 Go. Une fois que le volume racine a été modifié pour une valeur comprise entre 175 et 2 000 Go, vous pouvez mettre à jour le volume utilisateur, en utilisant n'importe quelle valeur comprise entre 100 et 2 000 Go.

 Note

Si vous souhaitez augmenter les deux volumes, vous devez attendre 20 à 30 minutes avant que la première opération se termine pour que vous puissiez commencer la deuxième.

- Non-GPU-enabled WorkSpaces le volume racine ne peut pas être inférieur à 175 Go lorsque le volume utilisateur est de 100 Go. Les exigences de stockage pour l'utilisation du GPU évoluent proportionnellement au WorkSpaces dimensionnement de l'instance. Lorsque vous sélectionnez des WorkSpaces configurations GPU de plus grande taille, vous devez allouer des volumes de stockage proportionnellement plus importants pour maintenir des performances optimales et répondre aux demandes de charge de travail accrues. Pour la plus petite taille d'instance, commencez par l'allocation de stockage suivante : racine : 100 Go, utilisateur : 100 Go. Le GPU prend en WorkSpaces charge un minimum de 100 Go pour le volume racine et de 100 Go pour le volume utilisateur.
- Si le volume utilisateur est de 50 Go, vous ne pouvez pas mettre à jour le volume racine en utilisant une valeur autre que 80 Go. Si le volume racine est de 80 Go, le volume utilisateur ne peut être que de 10, 50 ou 100 Go.

Pour modifier le volume racine d'un Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le Workspace et choisissez Actions, Modifier le volume racine. .
4. Sous Taille du volume racine, choisissez une taille de volume, ou choisissez Personnalisée pour saisir une taille de volume personnalisée.
5. Sélectionnez Enregistrer les modifications.
6. Lorsque l'augmentation de la taille du disque est terminée, vous devez [redémarrer le Workspace](#) pour que les modifications prennent effet. Pour éviter toute perte de données, assurez-vous que l'utilisateur enregistre tous les fichiers ouverts avant de redémarrer le Workspace.

Pour modifier le volume utilisateur d'un WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez WorkSpace et choisissez Actions, Modifier le volume utilisateur. .
4. Sous Taille du volume utilisateur, choisissez une taille de volume, ou choisissez Personnalisée pour saisir une taille de volume personnalisée.
5. Sélectionnez Enregistrer les modifications.
6. Lorsque l'augmentation de la taille du disque est terminée, vous devez [redémarrer le WorkSpace](#) pour que les modifications prennent effet. Pour éviter toute perte de données, assurez-vous que l'utilisateur enregistre tous les fichiers ouverts avant de redémarrer le WorkSpace.

Pour modifier les tailles de volume d'un WorkSpace

Utilisez la [modify-workspace-properties](#) commande avec la UserVolumeSizeGib propriété RootVolumeSizeGib or.

Modification du type de calcul

Vous pouvez alterner WorkSpace entre les types de calcul Standard, Power, Performance, PowerPro GeneralPurpose .4xlarge et GeneralPurpose .8xlarge. Pour plus d'informations sur ces types de calcul, consultez [Amazon WorkSpaces Bundles](#).

Note

- Si votre système d'exploitation source est autre que Windows Server 2022 ou Windows 11, vous ne pouvez pas modifier le type de calcul de PowerPro à GeneralPurpose.
- Si vous modifiez le type de calcul d'un non-GPU-enabled bundle à un format GeneralPurpose .4xlarge ou GeneralPurpose .8xlarge, vous WorkSpaces devez respecter la taille minimale du volume racine de 175 Go et la taille du volume utilisateur de 100 Go. Pour augmenter le volume de votre WorkSpaces, voir [Modification de la taille des volumes](#).
- Le GPU prend en WorkSpaces charge les modifications du type de calcul au sein d'une même famille d'instances, mais ne prend pas en charge les modifications entre familles. Par exemple, vous pouvez modifier le type de calcul entre les instances G4dn ou entre les instances G6, mais vous ne pouvez pas passer d'une instance G4dn à une famille d'instances G6. Pour passer d'un WorkSpace bundle compatible GPU à une autre et

alimentés par différentes familles d'instances, utilisez une fonctionnalité Migrate Workspace. Pour de plus amples informations, consultez [Migrer un Workspace dans WorkSpaces Personal](#).

- GraphicsPro le forfait arrive end-of-life à expiration le 31 octobre 2025. Nous vous recommandons de migrer vers les offres compatibles avant le 31 octobre 2025. GraphicsPro WorkSpaces Pour de plus amples informations, veuillez consulter [Migrer un Workspace dans WorkSpaces Personal](#).
- Vous ne pouvez pas modifier le type de calcul de Graphics et GraphicsPro lui attribuer une autre valeur.

Lorsque vous demandez une modification de calcul, WorkSpaces redémarre le Workspace en utilisant le nouveau type de calcul. WorkSpaces préserve le système d'exploitation, les applications, les données et les paramètres de stockage du Workspace.

Vous pouvez demander un type de calcul de niveau plus élevé une fois par période de 6 heures, ou un type de calcul de niveau moins élevé une fois tous les 30 jours. Pour un nouveau lancement Workspace, vous devez attendre 6 heures avant de demander un type de calcul plus important.

Lorsqu'un changement de type de Workspace calcul est en cours, les utilisateurs sont déconnectés du leur Workspace et ils ne peuvent ni utiliser ni modifier le Workspace. Le Workspace est automatiquement redémarré pendant le processus de changement de type de calcul.

 Important

Pour éviter toute perte de données, assurez-vous que les utilisateurs enregistrent tous les documents ouverts et les autres fichiers d'application avant de modifier le type de Workspace calcul.

Le processus de modification de type de calcul peut prendre jusqu'à une heure.

Pour modifier le type de calcul d'un Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le Workspace et choisissez Actions, Modifier le type de calcul.

4. Sous Type de calcul, choisissez un type de calcul.
5. Sélectionnez Enregistrer les modifications.

Pour modifier le type de calcul d'un WorkSpace

Utilisez la [modify-workspace-properties](#) commande avec la ComputeTypeName propriété.

Modification des protocoles

Si le vôtre WorkSpace est créé avec des bundles PCo IP, vous pouvez modifier leur protocole de streaming à l'aide de la AWS CLI ou de l' WorkSpaces API Amazon. Cela vous permet de migrer le protocole en utilisant votre protocole existant WorkSpace sans utiliser la fonctionnalité de WorkSpace migration. Cela vous permet également d'utiliser DCV et de gérer votre volume racine sans recréer l' PCoadresse IP existante WorkSpaces pendant le processus de migration.

- Vous ne pouvez modifier votre protocole que s'il WorkSpace a été créé avec des ensembles d' PCoaddresse IP et s'il n'est pas compatible avec le GPU. WorkSpace
- Avant de modifier le protocole en DCV, assurez-vous que vous WorkSpace répondez aux exigences suivantes pour un DCV WorkSpace.
 - Votre WorkSpaces client soutient le DCV
 - La région dans laquelle vous êtes déployé WorkSpace prend en charge le DCV
 - Les exigences en matière d'adresse IP et de port pour le DCV sont ouvertes. Pour plus d'informations, consultez la section [Exigences relatives à l'adresse IP et au port pour WorkSpaces](#).
- Assurez-vous que votre offre actuelle est disponible avec DCV.
- Pour une expérience de visioconférence optimale, nous vous recommandons d'utiliser PowerPowerPro, GeneralPurpose .4xlarge ou GeneralPurpose .8xlarge uniquement.

Note

- Nous vous recommandons vivement de tester votre produit hors production WorkSpaces avant de commencer à modifier le protocole.
- Si vous modifiez le protocole d' PCoIP en DCV, puis que vous le remodifiez en PCo IP, vous ne pourrez pas vous y connecter WorkSpaces via Web Access.

Pour modifier le protocole d'un WorkSpace

1. [Facultatif] Redémarrez votre ordinateur WorkSpace et attendez qu'il soit en AVAILABLE bon état avant de modifier le protocole.
2. [Facultatif] Utilisez la `describe-workspaces` commande pour répertorier les WorkSpace propriétés. Assurez-vous qu'elle est à l'état AVAILABLE état et que son `Protocol` actuel est exact.
3. Utilisez la commande `modify-workspace-properties` et remplacez la propriété `Protocols` par PCOIP à DCV, ou inversement.

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

Important

La propriété `Protocols` est sensible à la casse. Assurez-vous d'utiliser PCOIP ou DCV.

4. Après avoir exécuté la commande, le redémarrage et l'exécution des configurations nécessaires peuvent prendre jusqu' WorkSpace à 20 minutes.
5. Utilisez à nouveau la `describe-workspaces` commande pour répertorier les WorkSpace propriétés et vérifier qu'elles sont dans un AVAILABLE état et que la `Protocols` propriété actuelle a été modifiée selon le protocole approprié.

Note

- La modification WorkSpace du protocole n'entraîne pas la mise à jour de la description du bundle dans la console. La description Lancer le bundle ne change pas.
- S'il WorkSpace reste dans un UNHEALTHY état après 20 minutes, redémarrez-le WorkSpace dans la console.

6. Vous pouvez désormais vous connecter à votre WorkSpace.

Personnaliser l'image de marque dans WorkSpaces Personal

Amazon vous WorkSpaces permet de créer une WorkSpaces expérience familière pour vos utilisateurs en personnalisant l' APIs apparence de votre page de connexion avec votre propre logo WorkSpace de marque, des informations d'assistance informatique, un lien vers le mot de passe oublié et un message de connexion. Votre marque sera affichée à vos utilisateurs sur leur page de WorkSpace connexion au lieu de la WorkSpaces marque par défaut.

Les clients suivants sont prises en charge :

- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

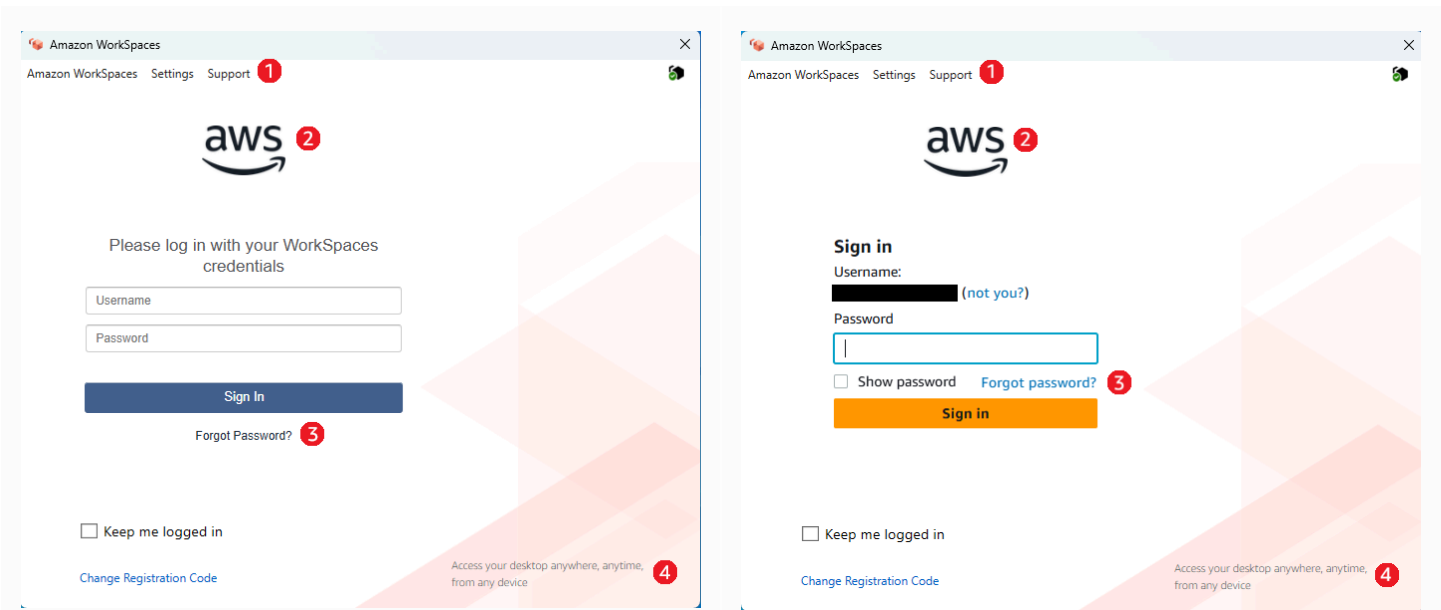
Importation d'une marque personnalisée

Afin d'importer une marque personnalisée pour le client qui vous concerne, utilisez l'action `ImportClientBranding`, qui inclut les éléments suivants. Consultez la [référence de `ImportClientBranding` l'API](#) pour plus d'informations.

Important

Les attributs de marque du client sont destinés à être publics. Assurez-vous de ne pas inclure d'informations sensibles.

Selon que vos annuaires utilisent l'ancien ou le nouveau flux de connexion utilisateur, vos utilisateurs verront les attributs personnalisés de votre marque client, comme indiqué dans les captures d'écran ci-dessous.



- 1. Lien Support
- 2. Logo
- 3. Lien Mot de passe oublié
- 4. Message de connexion

Éléments de marque personnalisés

Élément de personnalisation	Description	Exigences et recommandations
Lien Support	Vous permet de spécifier un lien d'e-mail d'assistance que les utilisateurs peuvent contacter pour obtenir de l'aide concernant leur WorkSpaces. Vous pouvez utiliser l'attribut SupportEmail , ou fournir un lien vers votre page de support à l'aide de l'attribut SupportLink .	• Pour chaque type de plateforme, les paramètres SupportEmail et SupportLink s'excluent mutuellement. Vous pouvez spécifier un seul paramètre pour chaque type de plateforme, pas les deux. • L'e-mail par défaut est workspaces-feedback@amazon.com .

Élément de personnalisation	Description	Exigences et recommandations
		• Contraintes de longueur : longueur minimale de 1. Longueur maximum de 200.
Logo	Permet de personnaliser la page avec le logo de votre organisation à l'aide de l'attribut Logo.	• Le seul format d'image accepté est un objet de données binaires converti à partir d'un fichier .png. • Résolutions recommandées : • Android : 978 x 190 • Bureau : 319 x 55 • iOS @2x : 110 x 200 • iOS @3x : 1 650 x 300
Lien Mot de passe oublié	Vous permet d'ajouter une adresse Web à l'aide de l'ForgotPasswordLink attribut auquel les utilisateurs peuvent accéder s'ils oublient le mot de passe de leur WorkSpace.	Contraintes de longueur : longueur minimale de 1. Longueur maximum de 200.

Élément de personnalisation	Description	Exigences et recommandations
Message de connexion	À l'aide de l'attribut <code>LoginMessage</code> , permet de personnaliser un message affiché sur l'écran de connexion.	• Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2 000 caractères pour l'intégration avec les balises HTML et différentes tailles de police. Pour les casses par défaut sans balises HTML, il est recommandé de limiter le message de connexion à moins de 600 caractères. • Balises HTML prises en charge : <code>a</code>, <code>b</code>, <code>blockquote</code>, <code>br</code>, <code>cite</code>, <code>code</code>, <code>dd</code>, <code>dl</code>, <code>dt</code>, <code>div</code>, <code>em</code>, <code>i</code>, <code>li</code>, <code>ol</code>, <code>p</code>, <code>pre</code>, <code>q</code>, <code>small</code>, <code>span</code>, <code>strike</code>, <code>strong</code>, <code>sub</code>, <code>sup</code>, <code>u</code>, <code>ul</code>

Vous trouverez ci-dessous des exemples d'extraits de code à utiliser. `ImportClientBranding`

AWS Version 2 de la CLI

 Warning

L'importation d'une marque personnalisée remplace, au sein de cette plate-forme, les attributs que vous spécifiez par vos données personnalisées. Elle remplace également les attributs que vous ne spécifiez pas par des valeurs d'attribut de marque personnalisées par défaut. Vous devez inclure les données de tous les attributs que vous ne souhaitez pas remplacer.


```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

Le fichier JSON d'importation doit ressembler à l'exemple de code suivant :

```
{
  "ResourceId": "<directory-id>",
  "DeviceTypeOsx": {
    "Logo":
      "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAAYAAABYtg0kAAAAC01EQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII=",
    "ForgotPasswordLink": "https://amazon.com/",
    "SupportLink": "https://amazon.com/",
    "LoginMessage": {
      "en_US": "Hello!!"
    }
  }
}
```

L'exemple d'extrait de code Java suivant convertit l'image du logo en une chaîne codée en base64 :

```
// Read image as BufferedImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

L'exemple d'extrait de code Python suivant convertit l'image du logo en une chaîne codée en base64 :

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

Warning

L'importation d'une marque personnalisée remplace, au sein de cette plate-forme, les attributs que vous spécifiez par vos données personnalisées. Elle remplace également les attributs que vous ne spécifiez pas par des valeurs d'attribut de marque personnalisées par défaut. Vous devez inclure les données de tous les attributs que vous ne souhaitez pas remplacer.

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferedImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the platform
DefaultImportClientBrandingAttributes attributes =
    DefaultImportClientBrandingAttributes.builder()
        .logo(SdkBytes.fromByteArray(bytes))
        .forgotPasswordLink("https://aws.amazon.com/")
        .supportLink("https://aws.amazon.com/")
        .build();

// Create import request
ImportClientBrandingRequest request =
    ImportClientBrandingRequest.builder()
        .resourceId("<directory-id>")
        .deviceTypeOsx(attributes)
        .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

Warning

L'importation d'une marque personnalisée remplace, au sein de cette plate-forme, les attributs que vous spécifiez par vos données personnalisées. Elle remplace également les attributs que vous ne spécifiez pas par des valeurs d'attribut de marque personnalisées par défaut. Vous devez inclure les données de tous les attributs que vous ne souhaitez pas remplacer.

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"
```

```
# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSCClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

Pour prévisualiser la page de connexion, lancez l' WorkSpaces application ou la page de connexion Web.

Note

Les modifications peuvent prendre jusqu'à 1 minute pour apparaître.

Description de la marque personnalisée

Pour voir les informations concernant la marque personnalisée dont vous disposez actuellement sur le client, utilisez l'action `DescribeCustomBranding`. Voici un exemple de script à utiliser `DescribeClientBranding`. Consultez la [référence de `DescribeClientBranding` l'API](#) pour plus d'informations.

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

Suppression de la marque personnalisée

Pour supprimer du client la marque personnalisée, utilisez l'action `DeleteCustomBranding`. Voici un exemple de script à utiliser `DeleteClientBranding`. Consultez la [référence de `DeleteClientBranding` l'API](#) pour plus d'informations.

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

 Note

Les modifications peuvent prendre jusqu'à 1 minute pour apparaître.

Marquer les ressources dans WorkSpaces Personnel

Vous pouvez organiser et gérer vos ressources WorkSpaces en attribuant vos propres métadonnées à chaque ressource sous forme de balises. Vous spécifiez une clé et une valeur pour chaque balise. Une clé peut être une catégorie générale, telle que « projet », « propriétaire » ou « environnement », avec des valeurs associées spécifiques. L'utilisation de balises est un moyen simple mais puissant de gérer les AWS ressources et d'organiser les données, y compris les données de facturation.

Lorsque vous ajoutez des balises à une ressource existante, elles n'apparaissent dans votre rapport de répartition des coûts que le premier jour du mois suivant. Par exemple, si vous ajoutez des balises à une balise existante WorkSpace le 15 juillet, elles n'apparaîtront dans votre rapport de répartition des coûts que le 1er août. Pour plus d'informations, consultez [Utilisation des balises d'allocation des coûts](#) dans le Guide de l'utilisateur AWS Billing .

 Note

Pour afficher vos balises de WorkSpaces ressources dans le Cost Explorer, vous devez activer les balises que vous avez appliquées à vos WorkSpaces ressources en suivant les instructions de la section [Activation des balises de répartition des coûts définies par l'utilisateur](#) dans le guide de l'AWS Billing utilisateur.

Bien que les balises apparaissent 24 heures après l'activation, les valeurs associées à ces balises peuvent prendre 4 à 5 jours pour apparaître dans l'explorateur de coûts. En outre, pour apparaître et fournir des données de coûts dans Cost Explorer, les WorkSpaces ressources balisées doivent être facturées pendant cette période. L'explorateur de coûts affiche uniquement les données de coûts à partir du moment où les balises ont été activées. Aucune donnée historique n'est disponible pour le moment.

Ressources que vous pouvez baliser

- Vous pouvez ajouter des balises aux ressources suivantes lorsque vous les créez : WorkSpaces images importées et groupes de contrôle d'accès IP.

- Vous pouvez ajouter des balises aux ressources existantes des types suivants : annuaires enregistrés WorkSpaces, ensembles personnalisés, images et groupes de contrôle d'accès IP.

Restrictions liées aux étiquettes

- Nombre maximal de balises par ressource : 50
- Longueur de clé maximale : 127 caractères Unicode
- Longueur de valeur maximale : 255 caractères Unicode
- Les clés et valeurs d'étiquette sont sensibles à la casse. Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : / @. N'utilisez pas d'espaces de début ou de fin.
- N'utilisez pas les `aws:workspaces:` préfixes `aws:` ou dans les noms ou valeurs de vos balises, car ils sont réservés à AWS l'usage. Vous ne pouvez pas modifier ni supprimer les noms ou valeurs de balise ayant ces préfixes.

Pour mettre à jour les balises d'une ressource existante à l'aide de la console (WorkSpaces annuaires ou groupes de contrôle d'accès IP)

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez l'un des types de ressources suivants : Répertoires ou Contrôles d'accès IP. WorkSpaces
3. Sélectionnez la ressource pour ouvrir sa page de détails.
4. Effectuez une ou plusieurs des actions suivantes :
 - Pour mettre à jour une balise, modifiez les valeurs de Clé et Valeur.
 - Pour ajouter une nouvelle balise, choisissez Ajouter une balise , et modifiez les valeurs pour Clé et Valeur.
 - Pour supprimer une balise, choisissez l'icône de suppression (X) à côté de la balise.
5. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer.

Pour mettre à jour les balises d'une ressource existante à l'aide de la console (images ou offres groupées)

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez l'un des types de ressources suivants : Offres ou Images.

3. Choisissez la ressource pour ouvrir sa page de détails.
4. Sous Balises, choisissez Gérer les balises.
5. Effectuez une ou plusieurs des actions suivantes :
 - Pour mettre à jour une balise, modifiez les valeurs de Clé et Valeur.
 - Pour ajouter une nouvelle balise, choisissez Ajouter une nouvelle balise , puis modifiez les valeurs pour Clé et Valeur.
 - Pour supprimer une balise, choisissez Retirer en regard de la balise.
6. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer les modifications.

Pour mettre à jour les balises d'une ressource existante à l'aide du AWS CLI

Utilisez les commandes [create-tags](#) et [delete-tags](#).

Entretien WorkSpaces personnel

Nous vous recommandons de faire régulièrement WorkSpaces l'entretien de votre WorkSpaces planifie les fenêtres de maintenance par défaut pour votre WorkSpaces. Pendant la période de maintenance, WorkSpace installe les mises à jour importantes d'Amazon WorkSpaces et redémarre si nécessaire. Si elles sont disponibles, les mises à jour du système d'exploitation sont également installées à partir du serveur de mise à jour du WorkSpace système d'exploitation configuré pour être utilisé. Pendant la maintenance, il WorkSpaces se peut que vous ne soyez pas disponible.

Par défaut, votre système Windows WorkSpaces est configuré pour recevoir les mises à jour de Windows Update. Pour configurer vos propres mécanismes de mise à jour automatique pour Windows, veuillez consulter la documentation pour [Windows Server Update Services \(WSUS\)](#) et [Configuration Manager](#).

Exigence

Vous WorkSpaces devez avoir accès à Internet pour pouvoir installer les mises à jour du système d'exploitation et déployer des applications. Pour de plus amples informations, veuillez consulter [the section called "Accès Internet"](#).

Fenêtres de maintenance pour AlwaysOn WorkSpaces

En effet AlwaysOn WorkSpaces, la fenêtre de maintenance est déterminée par les paramètres du système d'exploitation. La valeur par défaut est une période de quatre heures comprise entre 00h00 et 04h00, dans le fuseau horaire du WorkSpace, chaque dimanche matin. Par défaut, le fuseau

horaire d'un AlwaysOn WorkSpace est le fuseau horaire de la AWS région pour le WorkSpace. Toutefois, si vous vous connectez depuis une autre région et que la redirection de fuseau horaire est activée, puis que vous vous déconnectez, le fuseau horaire de la région WorkSpace est mis à jour en fonction du fuseau horaire de la région à partir de laquelle vous vous êtes connecté.

Vous pouvez [désactiver la redirection de fuseau horaire pour Windows à WorkSpaces](#) l'aide de la stratégie de groupe. Vous pouvez [désactiver la redirection de fuseau horaire pour Linux](#) à WorkSpaces l'aide de la configuration de l'agent PCo IP.

Pour Windows WorkSpaces, vous pouvez configurer la fenêtre de maintenance à l'aide de la stratégie de groupe ; voir [Configurer les paramètres de stratégie de groupe pour les mises à jour automatiques](#). Vous ne pouvez pas configurer la fenêtre de maintenance pour Linux WorkSpaces.

Fenêtres de maintenance pour AutoStop WorkSpaces

AutoStop WorkSpaces sont lancés automatiquement une fois par mois afin d'installer les mises à jour importantes. À compter du troisième lundi du mois, et pendant deux semaines au maximum, le créneau de maintenance est ouvert chaque jour de 00h00 à 05h00 environ, dans le fuseau horaire de la AWS Région pour le. WorkSpace Il WorkSpace peut être maintenu n'importe quel jour pendant la période de maintenance. Pendant cette période, seules les données WorkSpaces datant de plus de 7 jours sont conservées.

Pendant la période pendant laquelle le WorkSpace est en cours de maintenance, l'état du WorkSpace est réglé sur MAINTENANCE.

Bien que vous ne puissiez pas modifier le fuseau horaire utilisé pour la maintenance AutoStop WorkSpaces, vous pouvez désactiver la fenêtre de maintenance pour vos AutoStop WorkSpaces comme suit. Si vous désactivez le mode maintenance, vous n' WorkSpaces êtes pas redémarré et vous n'entrez pas dans l'MAINTENANCE état.

Pour désactiver le mode maintenance

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez votre annuaire, puis choisissez Actions, Update Details.
4. Développez le Mode maintenance.
5. Pour activer les mises à jour automatiques, choisissez Enabled (Activé). Si vous préférez gérer les mises à jour manuellement, choisissez Disabled (Désactivé).
6. Choisissez Update and Exit (Mettre à jour et quitter).

Maintenance manuelle

Si vous préférez, vous pouvez maintenir votre WorkSpaces propre horaire. Lorsque vous effectuez des tâches de maintenance, nous vous recommandons de passer WorkSpace à l'état Maintenance. Lorsque vous avez terminé, réglez l'état du WorkSpace sur Disponible.

Lorsqu'un WorkSpace est en état de maintenance, les comportements suivants se produisent :

- Le WorkSpace ne répond pas aux demandes de redémarrage, d'arrêt, de démarrage ou de reconstruction.
- Les utilisateurs ne peuvent pas se connecter au WorkSpace.
- An n' AutoStop WorkSpace est pas en hibernation.

Pour modifier l'état d' WorkSpace utilisation de la console

Note

Pour modifier l'état d'un WorkSpace, celui-ci WorkSpace doit être dans l'état Disponible. Le paramètre d'état Modifier n'est pas disponible lorsque a n' WorkSpace est pas dans l'état Disponible.

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez votre état WorkSpace, puis choisissez Actions, Modifier.
4. Sous Modifier l'état, choisissez Disponible ou Maintenance.
5. Choisissez Enregistrer.

Pour modifier l'état de l' WorkSpace utilisation du AWS CLI

Utilisez la commande [modify-workspace-state](#).

Chiffré WorkSpaces dans WorkSpaces Personal

WorkSpaces est intégré au AWS Key Management Service (AWS KMS). Cela vous permet de chiffrer les volumes de stockage à l' WorkSpaces aide de AWS KMS Key. Lorsque vous lancez un WorkSpace, vous pouvez chiffrer le volume racine (pour Microsoft Windows, le lecteur C ; pour

Linux,/) et le volume utilisateur (pour Windows, le lecteur D ; pour Linux, /home). Cela garantit que les données stockées au repos, du disque sur I/O le volume et des instantanés créés à partir des volumes sont tous chiffrés.

Note

- Outre le chiffrement de vos terminaux WorkSpaces, vous pouvez également utiliser le chiffrement FIPS des terminaux dans certaines régions des AWS États-Unis. Pour de plus amples informations, veuillez consulter [Configurer l'autorisation FedRAMP ou la conformité au DoD SRG pour Personal WorkSpaces](#).
- BitLocker Le chiffrement Windows n'est pas pris en charge pour Amazon WorkSpaces. Amazon WorkSpaces tentera de déchiffrer tous les volumes détectés lors du démarrage sur tous les systèmes d'exploitation Windows, le cas échéant. Les volumes peuvent ne plus répondre pendant le processus de démarrage si une combinaison de mots de passe, de codes PIN ou de clés de démarrage est activée pour un volume, Workspace cela peut devenir défectueux et ne pas pouvoir démarrer correctement.

Table des matières

- [Conditions préalables](#)
- [Restrictions](#)
- [Vue d'ensemble du WorkSpaces chiffrement à l'aide de AWS KMS](#)
- [WorkSpaces contexte de chiffrement](#)
- [WorkSpaces Autoriser l'utilisation d'une clé KMS en votre nom](#)
- [Chiffrer un Workspace](#)
- [Afficher crypté WorkSpaces](#)

Conditions préalables

Vous avez besoin d'une AWS KMS clé avant de pouvoir commencer le processus de chiffrement. Cette clé KMS peut être la [clé KMS AWS gérée](#) pour Amazon WorkSpaces (aws/workspaces) ou une clé KMS symétrique gérée par le [client](#).

- AWS clés KMS gérées — La première fois que vous lancez une clé KMS non chiffrée Workspace depuis la WorkSpaces console dans une région, Amazon crée WorkSpaces automatiquement une

clé KMS AWS gérée (aws/workspaces) sur votre compte. Vous pouvez sélectionner cette clé KMS AWS gérée pour chiffrer les volumes utilisateur et racine de votre WorkSpace. Pour en savoir plus, consultez [Vue d'ensemble du WorkSpaces chiffrement à l'aide de AWS KMS](#).

Vous pouvez consulter cette clé KMS AWS gérée, y compris ses politiques et ses autorisations, et suivre son utilisation dans les AWS CloudTrail journaux, mais vous ne pouvez pas utiliser ni gérer cette clé KMS. Amazon WorkSpaces crée et gère cette clé KMS. Seul Amazon WorkSpaces peut utiliser cette clé KMS et ne WorkSpaces peut l'utiliser que pour chiffrer les WorkSpaces ressources de votre compte.

AWS les clés KMS gérées, y compris celle prise WorkSpaces en charge par Amazon, sont renouvelées chaque année. Pour plus de détails, voir [AWS KMS Rotating Key](#) dans le guide du AWS Key Management Service développeur.

- Clé KMS gérée par le client — Vous pouvez également sélectionner une clé KMS symétrique gérée par le client que vous avez créée à l'aide AWS KMS de cette clé. Vous pouvez afficher, utiliser et gérer cette clé KMS, y compris définir ses stratégies. Pour plus d'informations sur la création d'une clé KMS, consultez [Création de clés](#) dans le Guide du développeur AWS Key Management Service . Pour plus d'informations sur la création de clés KMS à l'aide de l' AWS KMS API, consultez la section [Utilisation des clés](#) dans le guide du AWS Key Management Service développeur.

Les clés KMS gérées par le client ne font l'objet d'aucune rotation automatique, sauf si vous décidez d'activer la rotation automatique des clés. Pour plus de détails, voir [AWS KMS Rotating Keys](#) dans le guide du AWS Key Management Service développeur.

Important

Lorsque vous faites pivoter manuellement les clés KMS, vous devez conserver la clé KMS d'origine et la nouvelle clé KMS activées afin de AWS KMS pouvoir déchiffrer celles chiffrées par la clé KMS d'origine. WorkSpaces Si vous ne souhaitez pas que la clé KMS d'origine reste activée, vous devez la recréer WorkSpaces et la chiffrer à l'aide de la nouvelle clé KMS.

Vous devez remplir les conditions suivantes pour utiliser une AWS KMS clé afin de chiffrer votre WorkSpaces :

- La clé doit être symétrique. Amazon WorkSpaces ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations sur la distinction entre clés KMS symétriques et asymétriques, consultez [Identification des clés KMS symétriques et asymétriques](#) dans le Guide du développeur AWS Key Management Service .
- La clé KMS doit être activée. Pour déterminer si une clé KMS est activée, consultez [Affichage de clés KMS dans la console](#) dans le Guide du développeur AWS Key Management Service .
- Vous devez disposer des autorisations appropriées et des stratégies associées à la clé KMS. Pour de plus amples informations, veuillez consulter [Partie 2 : Accorder WorkSpaces aux administrateurs des autorisations supplémentaires à l'aide d'une politique IAM](#).

Restrictions

- Vous ne pouvez pas chiffrer un fichier existant WorkSpace. Vous devez chiffrer un WorkSpace lorsque vous le lancez.
- La création d'une image personnalisée à partir d'une image chiffrée n' WorkSpace est pas prise en charge.
- La désactivation du chiffrement pour un chiffrement n' WorkSpace est actuellement pas prise en charge.
- WorkSpaces lancé avec le chiffrement du volume racine activé, le provisionnement peut prendre jusqu'à une heure.
- Pour redémarrer ou reconstruire une clé chiffrée WorkSpace, assurez-vous d'abord que la AWS KMS clé est activée ; sinon, WorkSpace elle devient inutilisable. Pour déterminer si une clé KMS est activée, consultez [Affichage de clés KMS dans la console](#) dans le Guide du développeur AWS Key Management Service .

Vue d'ensemble du WorkSpaces chiffrement à l'aide de AWS KMS

Lorsque vous créez WorkSpaces avec des volumes chiffrés, WorkSpaces utilise Amazon Elastic Block Store (Amazon EBS) pour créer et gérer ces volumes. Amazon EBS chiffre les volumes avec une clé de données utilisant l'algorithme AES-256 standard. Amazon EBS et Amazon WorkSpaces utilisent tous deux votre clé KMS pour travailler avec les volumes chiffrés. Pour plus d'informations sur le chiffrement des volumes EBS, consultez [Amazon EBS Encryption](#) dans le guide de l'utilisateur Amazon EC2.

Lorsque vous lancez WorkSpaces avec des volumes chiffrés, le end-to-end processus fonctionne comme suit :

1. Vous spécifiez la clé KMS à utiliser pour le chiffrement ainsi que l'utilisateur et le répertoire du WorkSpace. Cette action crée une [autorisation](#) qui permet d'utiliser votre clé KMS uniquement WorkSpaces à cette fin, c'est-à-dire uniquement pour l'utilisateur et le répertoire WorkSpace associés à l'utilisateur et au répertoire spécifiés.
2. WorkSpaces crée un volume EBS chiffré pour le WorkSpace et spécifie la clé KMS à utiliser ainsi que l'utilisateur et le répertoire du volume. Cette action crée une autorisation qui permet à Amazon EBS d'utiliser votre clé KMS uniquement pour ce volume, c'est-à-dire uniquement pour l'utilisateur WorkSpace et le répertoire WorkSpace associés à l'utilisateur et au répertoire spécifiés, et uniquement pour le volume spécifié.
3. Amazon EBS demande une clé de données de volume chiffrée sous votre clé KMS et spécifie l'identifiant de sécurité Active Directory (SID) et l'ID de AWS Directory Service répertoire de l'WorkSpace utilisateur ainsi que l'ID de volume Amazon EBS comme contexte de [chiffrement](#).
4. AWS KMS crée une nouvelle clé de données, la chiffre sous votre clé KMS, puis envoie la clé de données chiffrée à Amazon EBS.
5. WorkSpaces utilise Amazon EBS pour associer le volume chiffré à votre WorkSpace. Amazon EBS envoie la clé de données cryptée AWS KMS avec une [Decrypt](#) demande et spécifie le SID de WorkSpace l'utilisateur, l'ID du répertoire et l'ID du volume, qui sont utilisés comme contexte de chiffrement.
6. AWS KMS utilise votre clé KMS pour déchiffrer la clé de données, puis envoie la clé de données en texte brut à Amazon EBS.
7. Amazon EBS se sert de la clé de données en texte brut pour chiffrer toutes les données en direction et en provenance du volume chiffré. Amazon EBS conserve la clé de données en texte brut en mémoire tant que le volume est attaché au WorkSpace.
8. Amazon EBS stocke la clé de données cryptée (reçue à [Step 4](#)) avec les métadonnées du volume pour une utilisation future au cas où vous redémarreriez ou reconstruisez le WorkSpace.
9. Lorsque vous utilisez le AWS Management Console pour supprimer une WorkSpace (ou que vous utilisez l'[TerminateWorkspaces](#) action dans l' WorkSpaces API) WorkSpaces et qu'Amazon EBS retire les autorisations qui lui permettaient d'utiliser votre clé KMS à cette WorkSpace fin.

WorkSpaces contexte de chiffrement

WorkSpaces n'utilise pas votre clé KMS directement pour des opérations cryptographiques (telles que [Encrypt](#), [Decrypt](#), [GenerateDataKey](#), etc.), ce qui signifie AWS KMS qu' WorkSpaces

il n'envoie pas de demandes incluant un [contexte de chiffrement](#). Toutefois, lorsqu'Amazon EBS demande une clé de données chiffrée pour les volumes chiffrés de votre WorkSpaces ([Step 3](#) dans le [Vue d'ensemble du WorkSpaces chiffrement à l'aide de AWS KMS](#)) et lorsqu'il demande une copie en texte brut de cette clé de données ([Step 5](#)), il inclut le contexte de chiffrement dans la demande.

Le contexte de chiffrement fournit [des données authentifiées supplémentaires](#) (AAD) AWS KMS utilisées pour garantir l'intégrité des données. Le contexte de chiffrement est également écrit dans vos fichiers AWS CloudTrail journaux, ce qui peut vous aider à comprendre pourquoi une clé KMS donnée a été utilisée. Amazon EBS utilise les éléments suivants comme contexte de chiffrement :

- L'identifiant de sécurité (SID) de l'utilisateur Active Directory associé au Workspace
- L'ID du AWS Directory Service répertoire associé au Workspace
- L'ID de volume Amazon EBS du volume chiffré

L'exemple suivant montre une représentation JSON du contexte de chiffrement qu'Amazon EBS utilise :

```
{
  "aws:workspaces:sid-directoryid":
    "[S-1-5-21-277731876-1789304096-451871588-1107]e[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

WorkSpaces Autoriser l'utilisation d'une clé KMS en votre nom

Vous pouvez protéger vos WorkSpace données à l'aide de la clé KMS AWS gérée pour WorkSpaces (aws/espaces de travail) ou d'une clé KMS gérée par le client. Si vous utilisez une clé KMS gérée par le client, vous devez WorkSpaces autoriser l'utilisation de la clé KMS au nom des WorkSpaces administrateurs de votre compte. La clé KMS AWS gérée pour WorkSpaces dispose des autorisations requises par défaut.

Pour préparer votre clé KMS gérée par le client à utiliser avec WorkSpaces, suivez la procédure suivante.

1. [Ajoutez vos WorkSpaces administrateurs à la liste des utilisateurs clés dans la politique clé de KMS](#)
2. [Donnez à vos WorkSpaces administrateurs des autorisations supplémentaires grâce à une politique IAM](#)

Vos WorkSpaces administrateurs ont également besoin d'une autorisation pour l'utiliser WorkSpaces. Pour plus d'informations sur ces autorisations, consultez [Gestion des identités et des accès pour WorkSpaces](#).

Partie 1 : Ajouter des WorkSpaces administrateurs en tant qu'utilisateurs clés

Pour donner WorkSpaces aux administrateurs les autorisations dont ils ont besoin, vous pouvez utiliser l'API AWS Management Console ou l' AWS KMS API.

Pour ajouter des WorkSpaces administrateurs en tant qu'utilisateurs clés pour une clé KMS (console)

1. Connectez-vous à la console AWS Key Management Service (AWS KMS) AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/kms>.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Clés gérées par le client.
4. Choisissez l'ID de clé ou l'alias de votre clé gérée par le client préférée.
5. Choisissez l'onglet Stratégie de clé. Sous Utilisateurs de clé, choisissez Ajouter.
6. Dans la liste des utilisateurs et des rôles IAM, sélectionnez les utilisateurs et les rôles correspondant à vos WorkSpaces administrateurs, puis choisissez Ajouter.

Pour ajouter des WorkSpaces administrateurs en tant qu'utilisateurs clés pour une clé KMS (API)

1. Utilisez cette [GetKeyPolicy](#) opération pour obtenir la politique clé existante, puis enregistrez le document de stratégie dans un fichier.
2. Ouvrez le document de stratégie dans votre éditeur de texte préféré. Ajoutez les utilisateurs et les rôles IAM correspondant à vos WorkSpaces administrateurs aux déclarations de politique qui [accordent des autorisations aux utilisateurs clés](#). Ensuite, enregistrez le fichier.
3. Utilisez l'[PutKeyPolicy](#) opération pour appliquer la politique de clé à la clé KMS.

Partie 2 : Accorder WorkSpaces aux administrateurs des autorisations supplémentaires à l'aide d'une politique IAM

Si vous sélectionnez une clé KMS gérée par le client à utiliser pour le chiffrement, vous devez établir des politiques IAM qui autorisent Amazon WorkSpaces à utiliser la clé KMS au nom d'un utilisateur IAM de votre compte qui lance le chiffrement. WorkSpaces Cet utilisateur doit également être autorisé à utiliser Amazon WorkSpaces. Pour plus d'informations sur la création et la modification de

politiques utilisateur IAM, consultez [Gestion des politiques IAM](#) dans le Guide de l'utilisateur IAM, et [Gestion des identités et des accès pour WorkSpaces](#).

WorkSpaces le chiffrement nécessite un accès limité à la clé KMS. Voici un modèle de stratégie de clé que vous pouvez utiliser. Cette stratégie sépare les mandataires qui peuvent gérer la clé AWS KMS de ceux qui peuvent l'utiliser. Avant d'utiliser cet exemple de stratégie de clé, remplacez l'exemple d'ID de compte et le nom d'utilisateur IAM par des valeurs réelles de votre compte.

La première instruction correspond à la politique AWS KMS clé par défaut. Elle donne à votre compte l'autorisation d'utiliser des politique IAM pour contrôler l'accès à la clé KMS. Les deuxième et troisième instructions définissent les AWS principaux autorisés à gérer et à utiliser la clé, respectivement. La quatrième instruction permet aux AWS services intégrés AWS KMS d'utiliser la clé pour le compte du principal spécifié. Cette instruction permet aux services AWS de créer et gérer les octrois. La déclaration utilise un élément de condition qui limite les autorisations relatives à la clé KMS à celles accordées par les AWS services au nom des utilisateurs de votre compte.

Note

Si vos WorkSpaces administrateurs utilisent le AWS Management Console pour créer WorkSpaces avec des volumes chiffrés, ils doivent être autorisés à répertorier les alias et les clés de liste (les "kms:ListKeys" autorisations "kms:ListAliases" et). Si vos WorkSpaces administrateurs utilisent uniquement l' WorkSpaces API Amazon (et non la console), vous pouvez omettre les "kms:ListKeys" autorisations "kms:ListAliases" et.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```



```

    "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
    "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms>Delete*"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
    "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource": "*",
    "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
}
]
}

```

La politique IAM pour un utilisateur ou un rôle qui chiffre un WorkSpace doit inclure les autorisations d'utilisation sur la clé KMS gérée par le client, ainsi que l'accès à WorkSpaces. Pour accorder des WorkSpaces autorisations à un utilisateur ou à un rôle IAM, vous pouvez associer l'exemple de politique suivant à l'utilisateur ou au rôle IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:*",
        "ds:DescribeDirectories",
        "workspaces:*",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:CreateWorkspaces",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces"
      ],
      "Resource": "*"
    }
  ]
}
```

La politique IAM suivante est requise par l'utilisateur pour l'utilisation de AWS KMS. Elle donne à l'utilisateur un accès en lecture seule à la clé KMS ainsi que la possibilité de créer des octrois.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

        "kms:CreateGrant",
        "kms:Describe*",
        "kms:List*"
    ],
    "Resource": "*"
}
]
}

```

Si vous souhaitez spécifier la clé KMS dans votre politique, utilisez une politique IAM similaire à celle qui suit. Remplacez l'exemple d'ARN de clé KMS par un ARN valide.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}

```

Chiffrer un WorkSpace

Pour chiffrer un WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Choisissez Lancer WorkSpaces et effectuez les trois premières étapes.
3. Pour l'étape WorkSpaces de configuration, procédez comme suit :
 - a. Sélectionnez les volumes à chiffrer : Volume racine, Volume utilisateur ou les deux volumes.
 - b. Pour la clé de chiffrement, sélectionnez une AWS KMS clé, soit la clé KMS AWS gérée créée par Amazon, WorkSpaces soit une clé KMS que vous avez créée. La clé que vous utilisez doit être symétrique. Amazon WorkSpaces ne prend pas en charge les clés KMS asymétriques.
 - c. Choisissez Étape suivante.
4. Choisissez Lancer WorkSpaces.

Afficher crypté WorkSpaces

Pour voir quels volumes WorkSpaces et quels volumes ont été chiffrés depuis la WorkSpaces console, choisissez dans la barre WorkSpaces de navigation de gauche. La colonne Volume Encryption indique si le chiffrement WorkSpace est activé ou désactivé pour chacun d'entre eux. Pour voir quels volumes spécifiques ont été chiffrés, développez l' Workspace entrée pour voir le champ Volumes chiffrés.

Redémarrer un Workspace dans WorkSpaces Personal

De temps en temps, vous devrez peut-être redémarrer (redémarrer) un Workspace manuellement. Le redémarrage d'un Workspace déconnecte l'utilisateur, puis effectue un arrêt et un redémarrage du Workspace. Pour éviter toute perte de données, assurez-vous que l'utilisateur enregistre tous les documents ouverts et les autres fichiers d'application avant de redémarrer le Workspace. Les données utilisateur, le système d'exploitation et les paramètres système ne sont pas affectés.

Warning

Pour redémarrer une clé chiffrée Workspace, assurez-vous d'abord que la AWS KMS clé est activée ; sinon, Workspace elle devient inutilisable. Pour déterminer si une clé KMS est activée, consultez [Affichage de clés KMS dans la console](#) dans le Guide du développeur AWS Key Management Service .

Pour redémarrer un Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le WorkSpaces pour redémarrer, puis choisissez Actions, Redémarrer WorkSpaces.
4. Lorsque vous êtes invité à confirmer, choisissez Redémarrer WorkSpaces.

Pour redémarrer un à WorkSpace l'aide du AWS CLI

Utilisez la commande [reboot-workspaces](#).

Pour redémarrer en bloc WorkSpaces

Utilisez [amazon-workspaces-admin-module](#).

Reconstruire un WorkSpace in WorkSpaces Personal

La reconstruction d'un WorkSpace permet de recréer le volume racine de l'image la plus récente du bundle à partir WorkSpace duquel il a été lancé, son volume utilisateur et son interface Elastic Network principale. La reconstruction d'un volume WorkSpace supprime plus de données que la restauration d'un volume WorkSpace, mais il suffit de disposer d'un instantané du volume utilisateur. Pour restaurer un WorkSpace, voir [Restaurer un compte WorkSpace dans WorkSpaces Personal](#).

La reconstruction d'un WorkSpace entraîne les événements suivants :

- Le volume racine (pour Microsoft Windows, lecteur C ; pour Linux, /) est actualisé avec l'image la plus récente du bundle à partir duquel il WorkSpace a été créé. Toutes les applications installées ou les paramètres système modifiés après WorkSpace leur création sont perdus.
- Le volume utilisateur (pour Microsoft Windows, le lecteur D ; pour Linux, /home) est recréé à partir de l'instantané le plus récent. Le contenu actuel du volume utilisateur est remplacé.

Les instantanés automatiques à utiliser lors de la reconstruction d'un WorkSpace sont planifiés toutes les 12 heures. Ces instantanés du volume utilisateur sont pris indépendamment de l'état de santé du WorkSpace. Lorsque vous sélectionnez Actions, Reconstruire/Restaurer WorkSpace, la date et l'heure du dernier instantané sont affichées.

Lorsque vous reconstruisez un WorkSpace, de nouveaux instantanés sont également pris peu après la fin de la reconstruction (souvent dans les 30 minutes).

- L'interface réseau Elastic principale est recréée. WorkSpace reçoit une nouvelle adresse IP privée.

 Important

Après le 14 janvier 2020, les fichiers WorkSpaces créés à partir d'un bundle Windows 7 public ne peuvent plus être reconstruits. Vous pouvez envisager de migrer votre Windows 7 WorkSpaces vers Windows 10. Pour de plus amples informations, veuillez consulter [Migrer un Workspace dans WorkSpaces Personal](#).

Vous ne pouvez reconstruire un Workspace fichier que si les conditions suivantes sont remplies :

- Ils Workspace doivent avoir un état de AVAILABLEERROR, UNHEALTHY, STOPPED, ou REBOOTING. Pour reconstruire un Workspace dans son REBOOTING état, vous devez utiliser l'opération [RebuildWorkspaces](#) API ou la commande [AWS CLI rebuild-workspaces](#).
- Un instantané du volume utilisateur doit exister.

Pour reconstruire un Workspace

 Warning

Pour reconstruire une clé chiffrée Workspace, assurez-vous d'abord que la AWS KMS clé est activée ; sinon, Workspace elle devient inutilisable. Pour déterminer si une clé KMS est activée, consultez [Affichage de clés KMS dans la console](#) dans le Guide du développeur AWS Key Management Service .

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le Workspace pour reconstruire et choisissez Actions, Reconstruire/Restaurer Workspace.
4. Sous Instantané, sélectionnez l'horodatage de l'instantané.
5. Choisissez Reconstruire.

Pour reconstruire un à Workspace l'aide du AWS CLI

Utilisez la commande [rebuild-workspaces](#).

Résolution des problèmes

Si vous reconstruisez un WorkSpace après avoir modifié l'attribut de dénomination d'utilisateur s AMAccount Name de l'utilisateur dans Active Directory, le message d'erreur suivant peut s'afficher :

```
"ErrorCode": "InvalidUserConfiguration.Workspace"  
"ErrorMessage": "The user was either not found or is misconfigured."
```

Pour contourner ce problème, revenez à l'attribut de dénomination utilisateur d'origine, puis relancez la reconstruction, ou créez-en un nouveau WorkSpace pour cet utilisateur.

Reconstruire l'identifiant Microsoft Entra joint WorkSpaces

Lorsqu'un utilisateur se connecte à son WorkSpace compte pour la première fois après la reconstruction, il doit recommencer l' out-of-boxexpérience (OOBE), comme lorsqu'on lui en a attribué une nouvelle WorkSpace. Par conséquent, un nouveau dossier de profil utilisateur est créé sur le WorkSpace, remplaçant le dossier de profil utilisateur d'origine. Ainsi, lors de la reconstruction d'un Entra joint WorkSpace, le contenu du dossier du profil utilisateur d'origine est enregistré D:\Users \<USERNAME%MMddyyTHHmss%.NotMigrated> lors de la reconstruction WorkSpace. L'utilisateur doit copier le contenu du profil d'origine depuis le dossier D:\Users \<USERNAME%MMddyyTHHmss %.NotMigrated> de profil de l'utilisateur dans D:\Users \ <USERNAME>pour restaurer toutes les données du profil utilisateur, y compris les icônes du bureau, les raccourcis et les fichiers de données.

Note

Pour les applications associées à un identifiant Microsoft Entra WorkSpaces, nous recommandons de toujours utiliser Restore WorkSpaces, dans la mesure du possible, au lieu de Rebuild WorkSpaces.

Restaurer un compte WorkSpace dans WorkSpaces Personal

La restauration d'un volume WorkSpace recrée à la fois le volume racine et le volume utilisateur à l'aide d'un instantané de chaque volume pris alors qu'il WorkSpace était en bon état. La restauration d' WorkSpace un rétablit les données sur le volume racine et sur le volume utilisateur jusqu'au moment où les instantanés ont été créés. La reconstruction d'un fichier annule WorkSpace uniquement les données du volume utilisateur. Cela signifie que la restauration nécessite que vous disposiez d'instantanés du volume racine et du volume utilisateur, tandis que la reconstruction d'un volume WorkSpace ne nécessite qu'un instantané du volume utilisateur. Pour reconstruire un WorkSpace, voir [Reconstruire un WorkSpace in WorkSpaces Personal](#).

La restauration d'un WorkSpace provoque les événements suivants :

- Le volume racine (pour Microsoft Windows, lecteur C ; pour Linux, /) est restauré à la date et à l'heure spécifiées à l'aide d'un instantané. Toutes les applications installées ou les paramètres système modifiés après la création du snapshot sont perdus.
- Le volume utilisateur (pour Microsoft Windows, le lecteur D ; pour Linux, /home) est recréé à la date et à l'heure spécifiées à l'aide d'un instantané. Le contenu actuel du volume utilisateur est remplacé.

Le point de restauration

Lorsque vous sélectionnez Actions et Rebuild/Restore WorkSpace, la date et l'heure des instantanés utilisés pour l'opération sont affichées. Pour vérifier la date et l'heure des instantanés utilisés pour l'opération à l'aide de AWS CLI, utilisez la [describe-workspace-snapshots](#) commande.

Lorsque des instantanés sont pris

Les instantanés des volumes racine et utilisateur sont pris sur la base suivante.

- Après la création d'un WorkSpace : en général, les instantanés initiaux des volumes root et utilisateur sont pris peu de temps après la création de WorkSpace a (souvent dans les 30 minutes). Dans certaines AWS régions, la prise des premiers instantanés peut prendre plusieurs heures après la création d' WorkSpace un.

Si un WorkSpace est défectueux avant que les premiers instantanés ne soient pris, il ne WorkSpace peut pas être restauré. Dans ce cas, vous pouvez essayer de [le reconstruire WorkSpace ou contacter le](#) AWS Support pour obtenir de l'aide.

- Lors d'une utilisation normale : les instantanés automatiques à utiliser lors de la restauration d'un WorkSpace sont programmés toutes les 12 heures. Si le volume WorkSpace est sain, des instantanés du volume racine et du volume utilisateur sont créés à peu près au même moment. En cas WorkSpace de dysfonctionnement, les instantanés sont créés uniquement pour le volume utilisateur.
- Après la restauration WorkSpace d'un fichier : lorsque vous restaurez un WorkSpace, de nouveaux instantanés sont pris peu après la fin de la restauration (souvent dans les 30 minutes). Dans certaines AWS régions, la prise de ces instantanés peut prendre plusieurs heures après la restauration d' WorkSpace un.

Une fois qu'un WorkSpace a été restauré, s'il WorkSpace devient défectueux avant que de nouveaux instantanés puissent être pris, il ne WorkSpace peut pas être restauré à nouveau. Dans ce cas, vous pouvez essayer de [le reconstruire WorkSpace ou contacter le](#) AWS Support pour obtenir de l'aide.

Vous ne pouvez restaurer un WorkSpace fichier que si les conditions suivantes sont remplies :

- Ils WorkSpace doivent avoir un état de AVAILABLEERROR, UNHEALTHY, ou STOPPED.
- Des instantanés des volumes racine et utilisateur doivent exister.

Pour restaurer un WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez le WorkSpace à restaurer, puis choisissez Actions, Reconstruire/Restaurer WorkSpace.
4. Sous Instantané, sélectionnez l'horodatage de l'instantané.
5. Choisissez Restore (Restaurer).

Pour restaurer un à WorkSpace l'aide du AWS CLI

Utilisez la commande [restore-workspace](#).

Microsoft 365 Bring Your Own License (BYOL) en WorkSpaces mode personnel

Amazon vous WorkSpaces permet d'apporter vos propres licences Microsoft 365 si elles répondent aux exigences de licence de Microsoft. Ces licences vous permettent d'installer et d'activer les applications Microsoft 365 pour les logiciels d'entreprise WorkSpaces qui sont alimentés par les systèmes d'exploitation suivants :

- Windows 10 (Apportez votre propres licence)
- Windows 11 (Apportez votre propres licence)
- Windows Server 2016
- Windows Server 2019

- Windows Server 2022
- Windows Server 2025

Pour utiliser Microsoft 365 Apps for Enterprise sur WorkSpaces, vous devez être abonné à Microsoft 365 E3/E5, Microsoft 365 A3/A5, Microsoft 365 G3/G5 ou Microsoft 365 Business Premium.

Sur votre Amazon, WorkSpaces vous pouvez utiliser vos licences Microsoft 365 pour installer et activer les applications Microsoft 365 pour les entreprises, notamment les suivantes :

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

Pour plus d'informations, consultez la liste complète des applications sur la page [Microsoft 365 Apps for enterprise](#).

Vous pouvez également installer des applications Microsoft non incluses dans Microsoft 365, telles que Microsoft Project, Microsoft Visio et Microsoft Power Automate, WorkSpaces mais vous devez apporter vos propres licences supplémentaires.

Vous pouvez installer et utiliser Microsoft 365 et d'autres applications Microsoft sur le système principal WorkSpaces et sur le basculement à WorkSpaces l'aide de la résilience [multirégionale](#).

Table des matières

- [Créez WorkSpaces avec Microsoft 365 Apps pour entreprises](#)
- [Migrez vos applications existantes WorkSpaces pour utiliser les applications Microsoft 365 pour les entreprises](#)
- [Mettez à jour vos applications Microsoft 365 pour entreprises sur WorkSpaces](#)

Créez WorkSpaces avec Microsoft 365 Apps pour entreprises

Pour créer WorkSpaces avec Microsoft 365 Apps for Enterprise, vous devez créer une image personnalisée avec les applications installées et l'utiliser pour créer un bundle personnalisé. Vous pouvez utiliser le bundle pour lancer de nouvelles applications sur WorkSpaces lesquelles les

applications sont installées. WorkSpaces ne fournit pas d'offres groupées publiques avec les applications Microsoft 365 pour entreprises.

Pour créer WorkSpaces avec Microsoft 365 Apps pour entreprises :

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Lancez une image WorkSpace que vous souhaitez utiliser comme image pour une autre application Microsoft WorkSpaces. C'est ici que vous allez installer vos applications Microsoft. Pour plus d'informations sur le lancement d'un WorkSpace, voir [Lancer un bureau virtuel à l'aide de WorkSpaces](#).
3. Lancez l'application client à l'adresse <https://clients.amazonworkspaces.com/>, entrez le code d'enregistrement indiqué dans votre e-mail d'invitation, puis choisissez Enregistrer.
4. Lorsque vous êtes invité à vous connecter, saisissez les informations d'identification de l'utilisateur, puis choisissez Se connecter.
5. Installez et configurez Microsoft 365 Apps for enterprise.
6. Créez une image personnalisée à partir du WorkSpace, et utilisez-la pour créer un bundle personnalisé. Pour plus d'informations sur la création d'images et d'ensembles personnalisés, voir [Création d'une WorkSpaces image et d'un ensemble personnalisés](#).
7. Lancez WorkSpaces à l'aide du bundle personnalisé que vous avez créé. WorkSpaces Les applications Microsoft 365 pour entreprises y sont installées.

Migrez vos applications existantes WorkSpaces pour utiliser les applications Microsoft 365 pour les entreprises

Si vous WorkSpaces ne possédez pas de licence Microsoft Office AWS, vous pouvez installer et configurer Microsoft 365 Apps for Enterprise sur votre WorkSpaces.

Si vous WorkSpaces possédez une licence Microsoft Office AWS, vous devez d'abord annuler l'enregistrement de votre licence Microsoft Office avant d'installer Microsoft 365 Apps for Enterprise.

Important

La désinstallation des applications Microsoft Office de vos licences WorkSpaces n'annule pas l'enregistrement des licences. Pour éviter de devoir payer des licences Microsoft Office, désenregistrez-vous des applications WorkSpaces Microsoft Office AWS en procédant de l'une des manières suivantes :

- Gérer les applications (recommandé) — Vous pouvez désinstaller les licences de version Microsoft Office de votre WorkSpaces. Pour plus d'informations, consultez [Gestion des applications](#). Après la désinstallation, vous pouvez installer Microsoft 365 Apps for Enterprise sur votre WorkSpaces.
- Migrer un WorkSpace — Vous pouvez migrer un WorkSpace bundle vers un autre tout en conservant les données sur le volume utilisateur.
 - Migrez WorkSpaces vers un bundle contenant une image pour laquelle il n'existe pas d'abonnement Microsoft Office. Une fois la migration terminée, vous pouvez installer Microsoft 365 Apps for Enterprise sur votre WorkSpaces.
 - Vous pouvez également créer une WorkSpaces image et un bundle personnalisés sur lesquels Microsoft 365 Apps for Enterprise est déjà installé sur l'image, puis migrer WorkSpaces vers ce nouveau bundle personnalisé. Une fois la migration terminée, vos WorkSpaces utilisateurs peuvent commencer à utiliser Microsoft 365 Apps for Enterprise.
 - Pour plus d'informations sur la façon de migrer WorkSpaces, voir [Migrer un WorkSpace](#).

Mettez à jour vos applications Microsoft 365 pour entreprises sur WorkSpaces

Par défaut, votre ordinateur WorkSpaces fonctionnant sous le système d'exploitation Microsoft Windows est configuré pour recevoir les mises à jour de Windows Update. Toutefois, les mises à jour Microsoft 365 Apps for enterprise ne sont pas disponibles avec Windows Update. Configurez les mises à jour pour qu'elles s'exécutent automatiquement à partir du réseau de diffusion de contenu (CDN) Office, ou utilisez WSUS (Windows Server Update Services) conjointement avec Microsoft Configuration Manager pour mettre à jour Microsoft 365 Apps for enterprise. Pour plus d'informations, consultez [Gérer les mises à jour des Microsoft 365 Apps avec Microsoft Configuration Manager](#). Pour définir la fréquence des mises à jour des applications Microsoft 365, spécifiez un canal de mise à jour et définissez-le sur Current ou Monthly Enterprise afin de respecter la politique de Microsoft 365 en matière de WorkSpaces licences.

Mettre à niveau Windows BYOL WorkSpaces dans Personal WorkSpaces

Sur votre licence Windows Bring Your Own (BYOL) WorkSpaces, vous pouvez effectuer une mise à niveau vers une version plus récente de Windows à l'aide du processus de mise à niveau sur place. Suivez les instructions de cette rubrique pour cela.

Le processus de mise à niveau sur place s'applique uniquement à Windows 10 et 11 WorkSpaces BYOL.

 Important

N'exécutez pas Sysprep sur une version mise à niveau. WorkSpace Sinon, une erreur qui empêche Sysprep de se terminer peut se produire. Si vous envisagez d'exécuter Sysprep, faites-le uniquement sur un ordinateur WorkSpace qui n'a pas été mis à niveau.

 Note

Vous pouvez utiliser ce processus pour mettre à niveau vos systèmes d'exploitation Windows 10 et 11 WorkSpaces vers une version plus récente. Toutefois, ce processus ne peut pas être utilisé pour mettre à niveau votre Windows 10 WorkSpaces vers Windows 11.

Table des matières

- [Conditions préalables](#)
- [Considérations](#)
- [Limitations connues](#)
- [Résumé des paramètres de clé de registre](#)
- [Effectuer une mise à niveau sur place](#)
- [Résolution des problèmes](#)
- [Mettez à jour votre WorkSpace registre à l'aide d'un PowerShell script](#)

Conditions préalables

- Si vous avez reporté ou suspendu les mises à niveau de Windows 10 et 11 à l'aide de Group Policy ou de System Center Configuration Manager (SCCM), activez les mises à niveau du système d'exploitation pour Windows 10 et 11. WorkSpaces
- Si WorkSpace c'est un AutoStop WorkSpace, remplacez-le par un AlwaysOn WorkSpace avant le processus de mise à niveau sur place afin qu'il ne s'arrête pas automatiquement pendant l'application des mises à jour. Pour de plus amples informations, veuillez consulter [Modification du](#)

[mode d'exécution](#). Si vous préférez conserver le WorkSpace réglage AutoStop, passez le AutoStop délai à trois heures ou plus pendant la mise à niveau.

- Le processus de mise à niveau sur place recrée le profil utilisateur en effectuant une copie d'un profil spécial nommé Utilisateur par défaut (C:\Users\Default). N'utilisez pas ce profil utilisateur par défaut pour effectuer des personnalisations. Nous vous recommandons d'apporter des personnalisations au profil utilisateur via Group Policy Objects (GPOs) à la place. Les personnalisations effectuées GPOs peuvent être facilement modifiées ou annulées et sont moins sujettes aux erreurs.
- Le processus de mise à niveau sur place ne peut sauvegarder et recréer qu'un seul profil utilisateur. Si vous disposez de plusieurs profils utilisateur sur le lecteur D, supprimez-les tous, sauf celui dont vous avez besoin.

Considérations

Le processus de mise à niveau sur place utilise deux scripts de registre (enable-inplace-upgrade.ps1 et setup-pvdrivers.ps1) pour apporter les modifications nécessaires au vôtre WorkSpaces afin de permettre au processus Windows Update de s'exécuter. Ces modifications impliquent la création d'un profil utilisateur (temporaire) sur le lecteur C au lieu du lecteur D. Si un profil utilisateur existe déjà sur le lecteur D, les données de ce profil utilisateur d'origine restent sur le lecteur D.

Par défaut, WorkSpaces crée le profil utilisateur dans D:\Users\%USERNAME%. Le script enable-inplace-upgrade.ps1 configure Windows pour créer un nouveau profil utilisateur dans C:\Users\%USERNAME% et redirige les dossiers shell utilisateur vers D:\Users\%USERNAME%. Ce nouveau profil utilisateur est créé lorsqu'un utilisateur ouvre pour la première fois une session.

Après la mise à niveau sur place, vous pouvez laisser vos profils utilisateur sur le lecteur C afin de permettre à vos utilisateurs d'utiliser le processus Windows Update pour mettre à niveau leurs machines ultérieurement. Sachez toutefois que WorkSpaces les profils stockés sur le lecteur C ne peuvent pas être reconstruits ou migrés sans perdre toutes les données du profil de l'utilisateur, sauf si vous les sauvegardez et les restaurez vous-même. Si vous décidez de laisser les profils sur le lecteur C, vous pouvez utiliser la clé de UserShellFoldersRedirectionregistre pour rediriger les dossiers shell de l'utilisateur vers le lecteur D, comme expliqué plus loin dans cette rubrique.

Pour vous assurer de pouvoir reconstruire ou migrer votre dossier WorkSpaces et pour éviter tout problème potentiel lié à la redirection des dossiers de l'interface utilisateur, nous vous recommandons de choisir de restaurer vos profils utilisateur sur le lecteur D après la mise à niveau sur place. Vous

pouvez le faire en utilisant la clé de registre `PostUpgradeRestoreProfileOnD`, comme expliqué plus loin dans cette rubrique.

Limitations connues

- Le changement d'emplacement du profil utilisateur du lecteur D au lecteur C ne se produit pas lors des WorkSpace reconstructions ou des migrations. Si vous effectuez une mise à niveau sur place sur un Windows 10 ou 11 BYOL, WorkSpace puis que vous le reconstruisez ou le migrez, le nouveau profil utilisateur WorkSpace se trouvera sur le lecteur D.

Warning

Si vous laissez le profil utilisateur sur le lecteur C après la mise à niveau sur place, les données du profil utilisateur stockées sur le lecteur C seront perdues pendant les reconstructions ou les migrations, sauf si vous sauvegardez manuellement les données du profil utilisateur avant la reconstruction ou la migration, puis restaurez manuellement les données du profil utilisateur après l'exécution du processus de reconstruction ou de migration.

- Si votre bundle BYOL par défaut contient une image basée sur une version antérieure de Windows 10 et 11, vous devez effectuer à nouveau la mise à niveau sur place après sa reconstruction ou sa migration. WorkSpace

Résumé des paramètres de clé de registre

Pour activer le processus de mise à niveau sur place et spécifier où doit se trouver le profil utilisateur après la mise à niveau, vous devez définir un certain nombre de clés de registre.

Chemin du registre : `HKLM:\Software\Amazon \ WorkSpacesConfig \ .ps1 enable-inplace-upgrade`

Clé de registre	Type	Valeurs
Enabled	DWORD	0 : (valeur par défaut) désactive la mise à niveau sur place 1 : active la mise à niveau sur place

Clé de registre	Type	Valeurs
PostUpgradeRestoreProfileOnD	DWORD	0 : (valeur par défaut) ne tente pas de restaurer le chemin d'accès au profil utilisateur après la mise à niveau sur place 1 — Restaure le chemin du profil utilisateur (ProfileImagePath) après la mise à niveau sur place
UserShellFoldersRedirection	DWORD	0 : n'active pas la redirection des dossiers shell utilisateur 1 : (valeur par défaut) active la redirection des dossiers shell utilisateur vers D:\Users\%USERNAME% après la reconstruction du profil dans C:\Users\%USERNAME%
NoReboot	DWORD	0 : (valeur par défaut) permet de contrôler quand un redémarrage se produit après modification du registre pour le profil utilisateur 1 — N'autorise pas le script à redémarrer WorkSpace après avoir modifié le registre pour le profil utilisateur

Chemin du registre : HKLM:\Software\Amazon \ WorkSpacesConfig \ update-pvdrivers.ps1

Clé de registre	Type	Valeurs
Enabled	DWORD	0 — (par défaut) Désactive la mise à jour des pilotes AWS PV 1 — Active la mise à jour des pilotes AWS PV

Effectuer une mise à niveau sur place

Pour activer les mises à niveau Windows sur place sur votre BYOL WorkSpaces, vous devez définir certaines clés de registre, comme décrit dans la procédure suivante. Vous devez également définir certaines clés de registre pour indiquer le lecteur (C ou D) où doivent se trouver les profils utilisateur une fois les mises à niveau sur place terminées.

Vous pouvez effectuer ces modifications de registre manuellement. Si vous en avez plusieurs WorkSpaces à mettre à jour, vous pouvez utiliser Group Policy ou SCCM pour envoyer un PowerShell script. Pour un exemple de PowerShell script, voir [Mettez à jour votre WorkSpace registre à l'aide d'un PowerShell script](#).

Pour effectuer une mise à niveau sur place de Windows 10 et 11

1. Notez quelle version de Windows est actuellement en cours d'exécution sur les Windows 10 et 11 BYOL WorkSpaces que vous mettez à jour, puis redémarrez-les.
2. Mettez à jour les clés de registre système Windows afin que la valeur de Enabled (Activé) passe de 0 à 1. Ces modifications de registre permettent des mises à niveau sur place pour le Workspace.
 - HKEY_LOCAL_MACHINE \ SOFTWARE \ Amazon \ \ .ps1 WorkSpacesConfig enable-inplace-upgrade
 - HKEY_LOCAL_MACHINE \ SOFTWARE \ Amazon \ \ update-pvdrivers.ps1 WorkSpacesConfig

 Note

Si ces clés n'existent pas, redémarrez le WorkSpace. Les clés doivent être ajoutées au redémarrage du système.

(Facultatif) Si vous utilisez un flux de travail géré, tel que SCCM Task Sequences, pour effectuer la mise à niveau, définissez la valeur de clé suivante sur 1 pour empêcher le redémarrage de l'ordinateur :

HKEY_LOCAL_MACHINE \ SOFTWARE \ Amazon \ \ .ps1 \ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. Choisissez le lecteur sur lequel les profils utilisateur doivent se trouver après le processus de mise à niveau sur place (pour plus amples d'informations, consultez [Considérations](#)), et définissez les clés de registre comme suit :

- Paramètres si vous souhaitez que le profil utilisateur soit sur le lecteur C après la mise à niveau :

HKEY_LOCAL_MACHINE \ SOFTWARE \ Amazon \ \ .ps1 WorkSpacesConfig enable-inplace-upgrade

Nom de la clé : PostUpgradeRestoreProfileOnD

Valeur de la clé : 0

Nom de la clé : UserShellFoldersRedirection

Valeur de la clé : 1

- Paramètres si vous souhaitez que le profil utilisateur soit sur le lecteur D après la mise à niveau :

HKEY_LOCAL_MACHINE \ SOFTWARE \ Amazon \ \ .ps1 WorkSpacesConfig enable-inplace-upgrade

Nom de la clé : PostUpgradeRestoreProfileOnD

Valeur de la clé : 1

Nom de la clé : UserShellFoldersRedirection

Valeur de la clé : 0

4. Après avoir enregistré les modifications dans le registre, redémarrez-le pour que les modifications soient appliquées. WorkSpace

 Note

- Après le redémarrage, la connexion WorkSpace crée un nouveau profil utilisateur. Vous pouvez voir les icônes d'espace réservé dans le menu Démarrer. Ce comportement est automatiquement résolu une fois la mise à niveau sur place terminée.
- Attendez 10 minutes pour vous assurer qu'il WorkSpace est débloqué.

(Facultatif) Vérifiez que la valeur de clé suivante est définie sur 1, ce qui débloque la mise WorkSpace à jour :

HKEY_LOCAL_MACHINE \ SOFTWARE \ Amazon \ \ .ps1 \ Supprimé WorkSpacesConfig
enable-inplace-upgrade profileImagePath

5. Effectuez la mise à niveau sur place. Vous pouvez utiliser la méthode de votre choix, comme SCCM, ISO ou Windows Update (WU). Selon les versions d'origine de Windows 10 et 11 et le nombre d'applications installées, ce processus peut prendre de 40 à 120 minutes.

 Note

Le processus de mise à niveau sur place peut prendre au moins une heure. L'état de l' WorkSpace instance peut apparaître comme UNHEALTHY lors de la mise à niveau.

6. Une fois le processus de mise à jour terminé, vérifiez que la version Windows a été mise à jour.

 Note

Si la mise à niveau sur place échoue, Windows revient automatiquement à la version Windows 10 et 11 qui était en place avant que vous ne commenciez la mise à niveau. Pour plus d'informations sur le dépannage, consultez la [documentation Microsoft](#).

(Facultatif) Pour confirmer que les scripts de mise à jour ont été correctement exécutés, vérifiez que la valeur de clé suivante est définie à 1 :

HKEY_LOCAL_MACHINE \ SOFTWARE \ Amazon \ \ .ps1 \ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. Si vous avez modifié le mode d'exécution du WorkSpace en le réglant sur AlwaysOn ou en modifiant la AutoStop période afin que le processus de mise à niveau sur place puisse s'exécuter sans interruption, redéfinissez le mode d'exécution sur vos paramètres d'origine. Pour de plus amples informations, veuillez consulter [Modification du mode d'exécution](#).

Si vous n'avez pas défini la clé de registre PostUpgradeRestoreProfileOnD sur 1, le profil utilisateur est régénéré par Windows et inséré C:\Users\%USERNAME% après la mise à niveau sur place, de sorte que vous n'avez pas à recommencer les étapes ci-dessus pour les futures mises à niveau sur place de Windows 10 et 11. Par défaut, le script enable-inplace-upgrade.ps1 redirige les dossiers shell suivants vers le lecteur D :

- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent

- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates

Si vous redirigez les dossiers shell vers d'autres emplacements de votre WorkSpaces ordinateur, effectuez les opérations nécessaires WorkSpaces après les mises à niveau sur place.

Résolution des problèmes

Si vous rencontrez des problèmes liés à la mise à jour, vous pouvez vérifier les éléments suivants pour faciliter le dépannage :

- Les journaux Windows, qui se trouvent, par défaut, dans les emplacements suivants :

C:\Program Files\Amazon\WorkSpacesConfig\Logs\

C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED

- Observateur d'événements Windows

Journaux Windows > Application > Source : Amazon WorkSpaces

Tip

Au cours du processus de mise à niveau sur place, si vous constatez que certains raccourcis d'icônes sur le bureau ne fonctionnent plus, c'est parce que WorkSpaces les profils utilisateur situés sur le lecteur D sont déplacés vers le lecteur C pour préparer la mise à niveau. Une fois la mise à niveau terminée, les raccourcis fonctionneront comme prévu.

Mise à niveau de Windows 11 24H2 à l'aide de la résolution d'erreur ISO

Le processus de mise à niveau de Windows 11 24H2 peut rencontrer un échec de démarrage critique lors de la deuxième phase de démarrage, présentant notamment le code d'erreur 0xC1900101 - 0x40017. Cette erreur se produit généralement en raison d'un fichier de pilote système manquant ou endommagé qui empêche l'installation de se terminer correctement pendant la phase de démarrage.

Code d'erreur : 0xC1900101 - 0x40017

Description de l'erreur : échec de l'installation pendant la phase SECOND_BOOT avec erreur d'opération BOOT

1. Assurez-vous de disposer du fichier ISO 24H2 de Windows 11.
2. Ouvrez une invite de commande en tant qu'administrateur.
3. Copiez le fichier système requis à l'aide de cette commande :

```
copy "ISO-Drive:\Sources\WinSetupMon.sys" "C:\Windows\System32\Drivers\"
```

Remplacez ISO-Drive par les informations de votre lecteur ISO.

4. Vérifiez la copie du fichier en utilisant :

```
C:\Windows\System32\Drivers\
```

5. Lancez la mise à niveau de Windows 11 24H2 à l'aide du fichier ISO.

Mettez à jour votre WorkSpace registre à l'aide d'un PowerShell script

Vous pouvez utiliser l'exemple de PowerShell script suivant pour mettre à jour le registre sur votre ordinateur afin WorkSpaces d'activer les mises à niveau sur place. Suivez le [Effectuer une mise à niveau sur place](#), mais utilisez ce script pour mettre à jour le registre sur chacune d'elles WorkSpace.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to run on the next reboot of the
  Workspace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
```

```

{
    if (-not(Test-Path $scriptRegKey))
    {
        Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
with 'Update' enabled."
        New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
        New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
        Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
    }
    else
    {
        Write-Host "Registry key is already present with value '$scriptRegKey'
Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
        if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
        {
            Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
            Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
-Path $scriptRegKey).Enabled)'"
        }
    }
}
catch
{
    write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
    break
}
}

```

Migrer un WorkSpace dans WorkSpaces Personal

Note

Si vous souhaitez vous désabonner des licences de version Microsoft Office ou les désinstaller par le biais AWS de votre compte WorkSpace, nous vous recommandons d'utiliser [Gérer les applications](#).

Vous pouvez migrer un WorkSpace bundle vers un autre, tout en conservant les données sur le volume utilisateur. Voici des exemples de scénarios :

- Vous pouvez passer WorkSpaces de l'expérience de bureau Windows 7 à l'expérience de bureau Windows 10.
- Vous pouvez migrer WorkSpaces du protocole PCo IP vers le protocole DCV.
- Vous pouvez migrer WorkSpaces de l'offre 32 bits alimentée par Microsoft Office sur Windows Server 2016 vers WorkSpaces les offres Microsoft Office sous Windows Server 2019 et Windows Server 64 bits alimentées par Windows Server. WorkSpaces
- Vous pouvez migrer WorkSpaces d'un bundle public ou personnalisé à un autre. Par exemple, vous pouvez effectuer une migration depuis un emplacement compatible GPU (Graphics.G6, Graphics.G4DN). GraphicsPro.g4dn, Graphics, and GraphicsPro) regroupe des non-GPU-enabled ensembles, ainsi que dans l'autre sens.
- Vous pouvez migrer WorkSpaces du BYOL de Windows 10 vers le BYOL de Windows 11, mais la migration de Windows 11 vers Windows 10 n'est pas prise en charge.
- Les bundles Value ne sont pas pris en charge dans Windows 11. Pour migrer votre offre groupée Windows 7 ou 10 WorkSpaces vers Windows 11, vous devez d'abord passer de votre offre Value WorkSpaces à une offre groupée plus importante.
- Avant WorkSpaces de migrer de Windows 7 vers Windows 11, vous devez effectuer la migration vers Windows 10. Connectez-vous à Windows 10 au Workspace moins une fois avant de le migrer vers Windows 11. La migration WorkSpaces directe de Windows 7 vers Windows 11 n'est pas prise en charge.
- Vous pouvez migrer WorkSpaces les systèmes Windows qui utilisent Microsoft Office AWS vers un WorkSpaces ensemble personnalisé contenant des applications Microsoft 365. Après la migration, vous WorkSpaces êtes désinscrit de Microsoft Office.
- Vous pouvez migrer des WorkSpaces systèmes Windows qui utilisent Microsoft Office AWS vers un WorkSpaces bundle sans abonnement Office 2016/2019. Après la migration, vous WorkSpaces êtes désinscrit de Microsoft Office.
- Vous pouvez migrer le BYOL BYOP WorkSpaces de Windows 10 vers Windows 11, et le BYOP avec licence de Windows Server 2019 WorkSpaces vers Windows Server 2022.
- Vous pouvez migrer n'importe quel Workspace bundle alimenté par Windows Server vers Windows Server 2025. Une fois la migration effectuée, vous utiliserez le protocole de streaming DCV pour permettre le streaming à distance de haute performance, même avec des applications gourmandes en ressources graphiques, dans des conditions réseau variables, même avec des appareils clients moins puissants.
- Vous pouvez migrer n'importe quel Workspace bundle BYOP inclus dans une licence Windows Server vers BYOP Windows Server 2025.

Pour plus d'informations sur WorkSpaces les offres Amazon, consultez [Bundles et images pour Personal WorkSpaces](#).

Le processus de migration recrée le en Workspace utilisant un nouveau volume racine à partir de l'image du bundle cible et le volume utilisateur à partir du dernier instantané disponible de l'original Workspace. Un nouveau profil utilisateur est généré lors de la migration pour une compatibilité optimale. L'ancien profil utilisateur est renommé, puis certains fichiers de l'ancien profil utilisateur sont déplacés vers le nouveau profil utilisateur. (Pour plus de détails sur ce qui est déplacé, consultez [Déroulement de la migration](#).)

Le processus de migration prend jusqu'à une heure par migration Workspace. Lorsque vous lancez le processus de migration, un nouveau Workspace est créé. Si une erreur empêche la réussite de la migration, l'original Workspace est restauré et remis dans son état d'origine, et le nouveau Workspace est arrêté.

Table des matières

- [Limites de migration](#)
- [Scénarios de migration](#)
- [Déroulement de la migration](#)
- [Bonnes pratiques](#)
- [Résolution des problèmes](#)
- [Quelles sont les conséquences sur la facturation](#)
- [Migration d'un Workspace](#)

Limites de migration

- Vous ne pouvez pas migrer vers un bundle d'expérience de bureau Windows 7 public ou personnalisé. Vous ne pouvez pas non plus migrer vers les bundles Bring Your Own License (BYOL) Windows 7.
- Vous ne pouvez migrer le BYOL WorkSpaces que vers d'autres bundles BYOL. Pour migrer un BYOL Workspace d' PCoIP vers DCV, vous devez d'abord créer un bundle BYOL avec le protocole DCV. Vous pouvez ensuite migrer votre PCo IP BYOL WorkSpaces vers ce bundle DCV BYOL.
- Vous ne pouvez pas migrer un bundle Workspace créé à partir de bundles publics ou personnalisés vers un bundle BYOL.

- Le protocole DCV prend en charge les bundles Graphics G6, Graphics.G4DN et .g4dn sous Windows. GraphicsPro Sur Ubuntu, seuls Graphics.g4dn et GraphicsPro .g4dn sont disponibles.
- PCoLe protocole IP prend en charge les ensembles Graphics.g4dn et GraphicsPro .g4dn sous Windows uniquement.
- La migration vers Linux n' WorkSpaces est actuellement pas prise en charge.
- Dans AWS les régions qui prennent en charge plusieurs langues, vous pouvez migrer WorkSpaces entre les ensembles linguistiques.
- Les bundles source et cible doivent être différents. (Toutefois, dans les régions qui prennent en charge plusieurs langues, vous pouvez migrer vers le même bundle Windows 10 à condition que les langues diffèrent.) Si vous souhaitez l'actualiser WorkSpace en utilisant le même bundle, [reconstruisez-le à la WorkSpace](#) place.
- Vous ne pouvez pas migrer d'une WorkSpaces région à l'autre.
- Dans certains cas, si la migration ne parvient pas à se terminer correctement, il se peut qu'aucun message d'erreur ne se soit affiché et que le processus de migration n'ait pas démarré. Si le WorkSpace bundle reste le même une heure après la tentative de migration, celle-ci échoue. Contactez le [Centre AWS Support](#) pour obtenir de l'aide.
- Vous ne pouvez pas migrer le BYOP WorkSpaces vers PCo IP ou DCV WorkSpaces.
- Vous ne pouvez pas migrer un domaine joint à Active Directory vers un domaine joint à WorkSpaces Microsoft Entra. WorkSpaces

Scénarios de migration

Le tableau suivant présente les scénarios de migration disponibles :

Système d'exploitation source	Système d'exploitation cible	Disponible ?
Bundle public ou personnalisé Windows 7	Bundle public ou personnalisé Windows 10	Oui
Bundle personnalisé Windows 7	Bundle public Windows 7	Non
Bundle personnalisé Windows 7	Bundle personnalisé Windows 7	Non

Système d'exploitation source	Système d'exploitation cible	Disponible ?
Bundle public Windows 7	Bundle personnalisé Windows 7	Non
Bundle public ou personnalisé Windows 10	Bundle public ou personnalisé Windows 7	Non
Bundle public ou personnalisé Windows 10	Bundle personnalisé Windows 10	Oui
Pack Windows 7 BYOL	Pack Windows 7 BYOL	Non
Pack Windows 7 BYOL	Pack Windows 10 BYOL	Oui
Pack Windows 10 BYOL	Pack Windows 7 BYOL	Non
Pack Windows 10 BYOL	Pack Windows 10 BYOL	Oui
Bundle Windows 10 public sur Windows Server 2016	Bundle Windows 10 public sur Windows Server 2019	Oui
Bundle Windows 10 public sur Windows Server 2019	Bundle Windows 10 public sur Windows Server 2016	Oui
Pack Windows 10 BYOL	Pack Windows 11 BYOL	Oui
Pack Windows 11 BYOL	Pack Windows 10 BYOL	Non
Bundle Windows 10 personnalisé sur Windows Server 2016	Bundle Windows 10 public sur Windows Server 2019	Oui
Bundle Windows 10 personnalisé sur Windows Server 2016	Bundle Windows 10 public sur Windows Server 2022	Oui
Bundle Windows 10 personnalisé sur Windows Server 2019	Bundle Windows 10 public sur Windows Server 2022	Oui
Windows 10 BYOP BYOL	Windows 11 BYOP BYOL	Oui
Windows 11 BYOP BYOL	Windows 10 BYOP BYOL	Non

Système d'exploitation source	Système d'exploitation cible	Disponible ?
BYOP public alimenté par Windows Server 2019	BYOP public alimenté par Windows Server	Oui
BYOP public alimenté par Windows Server	BYOP public alimenté par Windows Server 2019	Non
BYOP public alimenté par Windows Server 2019	BYOP public alimenté par Windows Server 2025	Oui
BYOP public alimenté par Windows Server 2025	BYOP public alimenté par Windows Server 2019	Non
BYOP public alimenté par Windows Server	BYOP public alimenté par Windows Server 2025	Oui
BYOP public alimenté par Windows Server 2025	BYOP public alimenté par Windows Server	Non
Bundle Windows 10 public sur Windows Server 2019	BYOP public alimenté par Windows Server 2025	Oui
Offre groupée Windows 10 personnalisée alimentée par Windows Server 2019	BYOP public alimenté par Windows Server 2025	Oui
Bundle Windows 10 public sur Windows Server 2022	BYOP public alimenté par Windows Server 2025	Oui
Offre groupée Windows 10 personnalisée alimentée par Windows Server	BYOP public alimenté par Windows Server 2025	Oui

 Note

L'accès au Web n'est pas disponible pour la branche PCo IP du bundle Windows 10 public alimentée par Windows Server 2019.

Déroulement de la migration

Pendant la migration, les données qui se trouvent sur le volume utilisateur (lecteur D) sont conservées, mais toutes celles qui se trouvent sur le volume racine (lecteur C) sont perdues. Cela signifie que la totalité des applications installées, des paramètres définis et des modifications apportées au Registre est éliminée. L'ancien dossier de profil utilisateur est renommé avec le suffixe `.NotMigrated` et un nouveau profil utilisateur est créé.

Le processus de migration recrée le lecteur D en fonction du dernier instantané du volume utilisateur d'origine. Lors du premier démarrage du nouveau WorkSpace, le processus de migration déplace le `D:\Users\%USERNAME%` dossier d'origine vers un dossier nommé `D:\Users\%USERNAME%MMddyyTHHmss%.NotMigrated`. Un nouveau dossier `D:\Users\%USERNAME%\` est généré par le nouveau système d'exploitation.

Une fois le nouveau profil utilisateur créé, les fichiers des dossiers shell utilisateur suivants sont déplacés de l'ancien profil `.NotMigrated` vers le nouveau profil :

- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`

Important

Le processus de migration tente de déplacer les fichiers de l'ancien profil utilisateur vers le nouveau. Tous les fichiers qui n'ont pas été déplacés pendant la migration restent dans le dossier `D:\Users\%USERNAME%MMddyyTHHmss%.NotMigrated`. Si la migration réussit, vous pouvez voir quels fichiers ont été déplacés dans `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. Vous pouvez déplacer manuellement tous les fichiers qui ne l'ont pas été automatiquement.

Par défaut, l'indexation des recherches locales est désactivée pour les bundles publics. Si vous devez l'activer, l'opération par défaut est de rechercher `C:\Users` et non `D:\Users`, vous devez donc régler ceci également. Si vous avez défini l'indexation des recherches

locales spécifiquement sur `D:\Users\username` et non sur `D:\Users`, il est possible que celle-ci ne fonctionne pas après la migration pour les fichiers utilisateur présents dans le dossier `D:\Users\%USERNAME%MMddyyTHHmss%.NotMigrated`.

Toutes les balises attribuées à l'original WorkSpace sont reportées lors de la migration, et le mode d'exécution du WorkSpace est préservé. Cependant, le nouveau WorkSpace reçoit un nouvel WorkSpace identifiant, un nouveau nom d'ordinateur et une nouvelle adresse IP.

Bonnes pratiques

Avant de migrer un WorkSpace, procédez comme suit :

- Sauvegardez toutes les données importantes sur le lecteur C vers un autre emplacement. Toutes les données du lecteur C sont effacées pendant la migration.
- Assurez-vous que le volume WorkSpace en cours de migration date d'au moins 12 heures, afin de garantir qu'un instantané du volume utilisateur a été créé. Sur la WorkSpaces page Migrate de la WorkSpaces console Amazon, vous pouvez voir l'heure du dernier instantané. Toutes les données créées après le dernier instantané sont perdues pendant la migration.
- Pour éviter toute perte de données potentielle, assurez-vous que vos utilisateurs se déconnectent WorkSpaces et ne se reconnectent qu'une fois le processus de migration terminé. Notez qu'ils WorkSpaces ne peuvent pas être migrés lorsqu'ils sont en ADMIN_MAINTENANCE mode.
- Assurez-vous que le statut du fichier que WorkSpaces vous souhaitez migrer est AVAILABLESTOPPED, ouERROR.
- Assurez-vous que vous disposez de suffisamment d'adresses IP pour WorkSpaces effectuer la migration. Au cours de la migration, de nouvelles adresses IP seront attribuées au WorkSpaces.
- Si vous utilisez des scripts pour effectuer la migration WorkSpaces, migrez-les par lots de 25 WorkSpaces au maximum à la fois.

Résolution des problèmes

- Si vos utilisateurs signalent des fichiers manquants après la migration, vérifiez si leurs fichiers de profil utilisateur n'ont pas été déplacés pendant le processus de migration. Vous pouvez voir quels fichiers ont été déplacés dans `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. Les fichiers qui n'ont pas été déplacés se trouvent dans le dossier `D:\Users`

\\%USERNAME%MMddyyTHHmss%.NotMigrated. Vous pouvez déplacer manuellement tous les fichiers qui ne l'ont pas été automatiquement.

- Si vous utilisez l'API pour effectuer la migration WorkSpaces et que la migration échoue, l'Workspace ID cible renvoyé par l'API ne sera pas utilisé et Workspace conservera l'Workspace ID d'origine.
- Si une migration ne se termine pas correctement, vérifiez dans Active Directory si elle a été nettoyée en conséquence. Vous devrez peut-être supprimer manuellement WorkSpaces ce dont vous n'avez plus besoin.

Quelles sont les conséquences sur la facturation

Au cours du mois au cours duquel la migration a lieu, des montants vous sont facturés au prorata pour le nouveau et l'original WorkSpaces. Par exemple, si vous migrez de Workspace Workspace A vers B le 10 mai, vous serez facturé pour Workspace A du 1er au 10 mai, et pour Workspace B du 11 au 30 mai.

Note

Si vous migrez Workspace vers un autre type de bundle (par exemple, de Performance à Power ou de Value à Standard), la taille du volume racine (lecteur C) et du volume utilisateur (lecteur D) peuvent augmenter au cours du processus de migration. Si nécessaire, le volume racine augmente pour s'adapter à la taille du volume racine par défaut du nouveau bundle. Toutefois, si vous aviez déjà spécifié pour le volume utilisateur une taille différente (supérieure ou inférieure) de celle par défaut du bundle d'origine, cette même taille de volume utilisateur est conservée pendant le processus de migration. Dans le cas contraire, le processus de migration utilise la plus grande des deux valeurs suivantes : la taille du volume Workspace utilisateur source et la taille du volume utilisateur par défaut pour le nouveau bundle.

Migration d'un Workspace

Vous pouvez effectuer la migration WorkSpaces par le biais de la WorkSpaces console Amazon, AWS CLI ou de l'WorkSpacesAPI Amazon.

Pour migrer un Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez votre Workspace et choisissez Actions, Migrer WorkSpaces.
4. Sous Ensembles, sélectionnez le pack vers lequel vous souhaitez effectuer la migration.
Workspace

 Note

Pour migrer un BYOL Workspace d' PCoIP vers DCV, vous devez d'abord créer un bundle BYOL avec le protocole DCV. Vous pouvez ensuite migrer votre PCo IP BYOL WorkSpaces vers ce bundle DCV BYOL.

5. Choisissez Migrate (Migrer) WorkSpaces.

Un nouveau Workspace dont le statut est égal à PENDING apparaît dans la WorkSpaces console Amazon. Lorsque la migration est terminée, l'original Workspace est résilié et le statut du nouveau Workspace est défini sur AVAILABLE.

6. (Facultatif) Pour supprimer les bundles et les images personnalisés dont vous n'avez plus besoin, consultez [Supprimer un ensemble ou une image personnalisé dans WorkSpaces Personal](#).

Pour effectuer la migration WorkSpaces via le AWS CLI, utilisez la commande [migrate-workspace](#). Pour effectuer la migration WorkSpaces via l' WorkSpaces API Amazon, consultez [MigrateWorkspace](#) le manuel Amazon WorkSpaces API Reference.

Supprimer un Workspace dans WorkSpaces Personal

Lorsque vous avez terminé avec un Workspace, vous pouvez le supprimer. Vous pouvez également supprimer des ressources associées.

 Warning

La suppression d'un Workspace est une action permanente qui ne peut pas être annulée. Les données de l' Workspace utilisateur ne sont pas conservées et sont détruites. Pour plus d'informations sur la sauvegarde des données utilisateur, contactez AWS Support.

 Note

Simple AD et AD Connector sont à votre disposition gratuitement WorkSpaces. [S'il n' WorkSpaces est pas utilisé avec votre annuaire Simple AD ou AD Connector pendant 30 jours consécutifs, cet annuaire sera automatiquement désenregistré pour être utilisé auprès d'Amazon WorkSpaces, et il vous sera facturé conformément aux conditions tarifaires.AWS Directory Service](#)

Pour supprimer des annuaires vides, consultez [Supprimer un répertoire pour WorkSpaces Personal](#). Si vous supprimez votre répertoire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à l'utiliser WorkSpaces .

Pour supprimer un Workspace

Vous pouvez supprimer un Workspace qui est dans n'importe quel état sauf Suspendu.

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez votre Workspace puis cliquez sur Supprimer.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer Workspace. La suppression d'un fichier prend environ 5 minutes Workspace. Lors de la suppression, le statut du Workspace est défini sur Terminant. Lorsque la suppression est terminée, il Workspace disparaît de la console.
5. (Facultatif) Pour supprimer tous les bundles et les images personnalisés dont vous n'avez plus besoin, consultez [Supprimer un ensemble ou une image personnalisé dans WorkSpaces Personal](#).
6. (Facultatif) Une fois que vous avez tout supprimé WorkSpaces dans un répertoire, vous pouvez le supprimer. Pour de plus amples informations, veuillez consulter [Supprimer un répertoire pour WorkSpaces Personal](#).
7. (Facultatif) Après avoir supprimé toutes les ressources du Virtual Private Cloud (VPC) de votre répertoire, vous pouvez supprimer le VPC et libérer l'adresse IP Elastic utilisée pour la passerelle NAT. Pour plus d'informations, consultez [Supprimer votre VPC](#) et [Utiliser des adresses IP Elastic](#) dans le Guide de l'utilisateur Amazon VPC.

Pour supprimer un à Workspace l'aide du AWS CLI

Utilisez la commande [terminate-workspaces](#).

Bundles et images pour Personal WorkSpaces

Un WorkSpace bundle est une combinaison d'un système d'exploitation et de ressources de stockage, de calcul et logicielles. Lorsque vous lancez un WorkSpace, vous sélectionnez le pack qui répond à vos besoins. Les offres groupées par défaut disponibles WorkSpaces sont appelées offres groupées publiques. Pour plus d'informations sur les différents forfaits publics disponibles WorkSpaces, consultez [Amazon WorkSpaces Bundles](#).

Si vous avez lancé un système Windows ou Linux WorkSpace et que vous l'avez personnalisé, vous pouvez créer une image personnalisée à partir de celui-ci WorkSpace.

Une image personnalisée contient uniquement le système d'exploitation, le logiciel et les paramètres du WorkSpace. Un bundle personnalisé est une combinaison de cette image personnalisée et du matériel à partir duquel il WorkSpace peut être lancé.

Après avoir créé une image personnalisée, vous pouvez créer un ensemble personnalisé qui combine l' WorkSpace image personnalisée et la configuration de calcul et de stockage sous-jacente que vous sélectionnez. Vous pouvez ensuite spécifier ce bundle personnalisé lorsque vous lancez un nouveau bundle WorkSpaces pour vous assurer que le nouveau WorkSpaces possède la même configuration cohérente (matérielle et logicielle).

Si vous devez effectuer des mises à jour logicielles ou installer des logiciels supplémentaires sur votre WorkSpaces, vous pouvez mettre à jour votre bundle personnalisé et l'utiliser pour reconstruire votre WorkSpaces.

WorkSpaces prend en charge plusieurs systèmes d'exploitation (OS), protocoles de streaming et offres groupées différents. Le tableau suivant fournit des informations sur les licences, les protocoles de streaming et les offres groupées pris en charge par chaque système d'exploitation.

Système d'exploitation	Licences	Protocoles de streaming	Offres groupées prises en charge	Politique de cycle de vie/ date de retraite
Windows Server 2016	Inclus	DCV, IP PCo	Valeur, standard, performance, puissance,,, PowerPro GraphicsPro, Graphics G4dn	12 janvier 2027
Windows Server 2019	Inclus	DCV, IP PCo	Valeur, standard, performance, puissance,,, PowerPro GraphicsPro, Graphics G4dn	9 janvier 2029
Windows Server 2022	Inclus	DCV, IP PCo	Standard, performance, alimentation,,, PowerPro GeneralPurpose, carte graphique G4dn, carte graphique G6	14 octobre 2031
Windows Server 2025	Inclus	DCV	Standard, performance, alimentation,,, PowerPro GeneralPurpose, carte graphique G4dn, carte graphique G6	14 novembre 2034
Windows 10	Apportez votre propre licence (BYOL)	DCV, IP PCo	Valeur, standard, performance, puissance,,, PowerPro GraphicsPro, Graphics G4dn	À l'appui
Windows 11	Apportez votre propre licence (BYOL)	DCV	Standard, performance, alimentation,,, PowerPro GeneralPurpose, carte graphique G4dn, carte graphique G6	À l'appui
Amazon Linux 2	Inclus	DCV, IP PCo	Valeur, norme, performance, puissance, PowerPro	À l'appui

Système d'exploitation	Licences	Protocoles de streaming	Offres groupées prises en charge	Politique de cycle de vie/ date de retraite
Ubuntu 22.04 LTS	Inclus	DCV	Valeur, standard, performance, puissance PowerPro, carte graphique G4dn	juin 2032
Rocky Linux 8	Inclus	DCV	Valeur, norme, performance, puissance, PowerPro	31 mai 2029
Red Hat Enterprise Linux 8	Inclus	DCV	Valeur, norme, performance, puissance, PowerPro	31 mai 2029

Note

- Les versions du système d'exploitation qui ne sont plus prises en charge par le fournisseur ne sont pas garanties de fonctionner et ne sont pas prises en charge par le AWS support.
- Pour WorkSpaces fonctionner sur le système d'exploitation Windows, les packs graphiques ne prennent en charge que le protocole de streaming PCo IP.

Table des matières

- [Options de bundle pour WorkSpaces Personal](#)
- [Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal](#)
- [Mettre à jour un pack personnalisé pour WorkSpaces Personal](#)
- [Copier une image personnalisée dans WorkSpaces Personal](#)
- [Partager ou annuler le partage d'une image personnalisée dans Personal WorkSpaces](#)
- [Supprimer un ensemble ou une image personnalisé dans WorkSpaces Personal](#)

Options de bundle pour WorkSpaces Personal

Avant de sélectionner un ensemble, assurez-vous que celui-ci est compatible avec votre protocole, votre WorkSpaces système d'exploitation, votre réseau et votre type de calcul. Pour plus d'informations sur les protocoles, consultez [Protocoles pour Amazon WorkSpaces](#). Pour plus d'informations sur les réseaux, consultez les [exigences WorkSpaces du réseau client Amazon](#).

Note

- Nous recommandons de ne pas dépasser une latence réseau maximale de 250 ms pour l' PCoIP WorkSpaces. Pour bénéficier d'une expérience WorkSpaces utilisateur PCoIP optimale, nous recommandons de maintenir la latence du réseau inférieure à 100 ms. Lorsque le temps d'aller-retour (RTT) dépasse 375 ms, la connexion WorkSpaces client s'arrête. Pour une expérience utilisateur optimale du DCV, nous recommandons de maintenir le RTT en dessous de 250 ms. Si le RTT est compris entre 250 ms et 400 ms, l'utilisateur peut y accéder WorkSpace, mais les performances diminueront considérablement.
- Nous recommandons de tester dans un environnement dédié les performances des bundles que vous souhaitez choisir, en exécutant et en utilisant les applications qui reproduisent les tâches quotidiennes des utilisateurs.
- Les packs BYOP (Bring Your Own Protocol) sont destinés WorkSpaces à Core. Aucun protocole de streaming WorkSpaces n'est installé sur les bundles BYOP WorkSpaces fournis par Amazon. Vous ne pourrez pas vous connecter à l'aide de WorkSpaces clients ou de passerelles. Pour comprendre le modèle de responsabilité partagée d'Amazon WorkSpaces Core, consultez le [Guide d'intégration des partenaires technologiques pour Amazon WorkSpaces Core](#). Pour plus d'informations, consultez [Amazon WorkSpaces Core](#).

Important

- GraphicsPro le forfait arrive end-of-life à expiration le 31 octobre 2025. Nous vous recommandons de migrer vers les offres compatibles avant le 31 octobre 2025. GraphicsPro WorkSpaces Pour de plus amples informations, veuillez consulter [Migrer un Workspace dans WorkSpaces Personal](#).

- Le bundle Graphics ne sera plus pris en charge après le 30 novembre 2023. Nous vous recommandons de passer à un bundle compatible avec le GPU pour WorkSpaces utiliser le bundle Graphics.
- Les graphismes et GraphicsPro les offres groupées ne sont actuellement pas disponibles dans la région Asie-Pacifique (Mumbai).
- De plus, les offres groupées avec Office 2016 ou Office 2019 ne seront plus prises en charge après le 14 octobre 2025. Nous vous recommandons de migrer vos WorkSpaces offres groupées avec ces versions d'Office pour utiliser Office 2021 ou Office 2024. Pour plus d'informations, voir [Gérer les applications dans WorkSpaces Personal](#).

Voici les offres groupées WorkSpaces proposées. Pour plus d'informations sur les offres groupées incluses WorkSpaces, consultez [Amazon WorkSpaces Bundles](#).

Offre Value

Ce bundle convient parfaitement aux activités suivantes :

- Édition de texte et saisie de données de base
- Navigation sur le Web avec une utilisation légère
- Messagerie instantanée

Ce bundle n'est pas recommandé pour le traitement de texte, les conférences audio et vidéo, le partage d'écran, les outils de développement logiciel, les applications d'informatique décisionnelle et les applications graphiques.

Offre Standard

Ce bundle convient parfaitement aux activités suivantes :

- Édition de texte et saisie de données de base
- Navigation sur le Web
- Messagerie instantanée
- E-mails

Ce pack n'est pas recommandé pour les conférences audio et vidéo, le partage d'écran, le traitement de texte, les outils de développement de logiciels, les applications de business intelligence et les applications graphiques.

Offre Performance

Ce bundle convient parfaitement aux activités suivantes :

- Navigation sur le Web
- Traitement de texte
- Messagerie instantanée
- E-mails
- Feuilles de calcul
- Traitement audio
- Didacticiels

Ce pack n'est pas recommandé pour les visioconférences, le partage d'écran, les outils de développement de logiciels, les applications de business intelligence et les applications graphiques.

Offre Power

Ce bundle convient parfaitement aux activités suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mail
- Messagerie instantanée
- Feuilles de calcul
- Traitement audio
- Développement logiciel (environnement de développement intégré (IDE))
- Traitement des données de niveau basique à intermédiaire
- Conférences audio et vidéo

Ce bundle n'est pas recommandé pour le partage d'écran, les outils de développement logiciel, les applications d'informatique décisionnelle et les applications graphiques.

PowerPro bundle

Ce bundle convient parfaitement aux activités suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mail
- Messagerie instantanée
- Feuilles de calcul
- Traitement audio
- Développement logiciel (environnement de développement intégré (IDE))
- Entreposage de données
- Applications d'informatique décisionnelle
- Conférences audio et vidéo

Ce pack n'est pas recommandé pour l'apprentissage automatique, la formation de modèles et les applications graphiques.

Packs à usage général

Ces offres groupées, comprenant un format GeneralPurpose .4xlarge et un GeneralPurpose .8xlarge, conviennent parfaitement aux applications suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mail
- Messagerie instantanée
- Feuilles de calcul
- Traitement audio
- Développement logiciel (environnement de développement intégré (IDE))
- Entreposage de données
- Applications d'informatique décisionnelle
- Conférences audio et vidéo

- Traitement par lots
- Formation sur les modèles de ML (machine learning) basée sur le processeur

Ce pack n'est pas recommandé pour le rendu 3D, le design photoréaliste, le streaming de jeux ou l'entraînement de modèles ML pour des modèles complexes.

Offres groupées Graphics G6

WorkSpace Les packs G6 utilisent NVIDIA L4 GPUs avec des processeurs AMD EPYC (Milan) de 3e génération et sont disponibles en trois variantes : G6, Gr6 et G6f. Le G6 présente un WorkSpaces vCPU-to-memory rapport standard de 1:4, fournissant des ressources de calcul et de mémoire équilibrées pour les charges de travail graphiques générales. Le Gr6 WorkSpaces offre un vCPU-to-memory ratio de 1:8, fournissant le double de mémoire par vCPU pour les applications graphiques nécessitant plus de mémoire. Les G6f WorkSpaces fournissent une allocation de GPU fractionnée, ce qui les rend adaptés aux charges de travail qui ne nécessitent pas une capacité de traitement GPU complète pour les opérations de calcul intensives. Reportez-vous à la [page Instances Amazon EC2 G6](#) pour plus d'informations. Les WorkSpace offres G6 prennent en charge tous les cas d'utilisation pris en charge par les offres existantes, tels que les tâches quotidiennes, le traitement et l'analyse des données, les audioconférences et le développement de logiciels. En outre, ils permettent les cas d'utilisation suivants :

- Conception graphique
- CAD/CAM (computer-aided design/computer-fabrication assistée)
- Transcodage vidéo
- Rendu 3D
- Streaming de jeux
- Formation de modèles de machine learning (ML) et inférence de ML

Offre Graphics.g4dn

Cet ensemble offre un haut niveau de performances graphiques, un niveau modéré de performances du processeur et de mémoire pour votre WorkSpaces ordinateur. Il est parfaitement adapté aux applications suivantes :

- Navigation sur le Web
- Traitement de texte

- E-mail
- Feuilles de calcul
- Messagerie instantanée
- Conférence audio
- Développement logiciel (environnement de développement intégré (IDE))
- Traitement des données de niveau basique à intermédiaire
- Entreposage de données
- Applications d'informatique décisionnelle
- Conception graphique
- CAD/CAM (computer-aided design/computer-fabrication assistée)

Ce pack n'est pas recommandé pour les conférences audio et vidéo, le rendu 3D, la conception photoréaliste et la formation de modèles d'apprentissage automatique.

GraphicsProEnsemble .g4dn

Cet ensemble offre un haut niveau de performances graphiques, de performances du processeur et de mémoire pour votre WorkSpaces ordinateur et convient parfaitement aux applications suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mail
- Feuilles de calcul
- Messagerie instantanée
- Conférence audio
- Développement logiciel (environnement de développement intégré (IDE))
- Traitement des données de niveau basique à intermédiaire
- Entreposage de données
- Applications d'informatique décisionnelle
- Conception graphique
- CAD/CAM (computer-aided design/computer-fabrication assistée)
- Transcodage vidéo

- Rendu 3D
- Conception photoréaliste
- Streaming de jeux
- Formation de modèles de machine learning (ML) et inférence de ML

Ce bundle n'est pas recommandé pour les conférences audio et vidéo.

Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal

Si vous avez lancé un système Windows ou Linux WorkSpace et que vous l'avez personnalisé, vous pouvez créer une image personnalisée et des ensembles personnalisés à partir de celui-ci WorkSpace.

Une image personnalisée contient uniquement le système d'exploitation, le logiciel et les paramètres du WorkSpace. Un bundle personnalisé est une combinaison de cette image personnalisée et du matériel à partir duquel il WorkSpace peut être lancé.

Note

Assurez-vous d'attendre au moins 2 heures après avoir supprimé un bundle avant de créer un nouveau bundle portant le même nom.

Après avoir créé une image personnalisée, vous pouvez créer un bundle personnalisé qui combine l'image personnalisée et la configuration de calcul et de stockage sous-jacente que vous sélectionnez. Vous pouvez ensuite spécifier ce bundle personnalisé lorsque vous lancez un nouveau bundle WorkSpaces pour vous assurer que le nouveau WorkSpaces possède la même configuration cohérente (matérielle et logicielle).

Vous pouvez utiliser la même image personnalisée pour créer différents lots personnalisés en sélectionnant différentes options de calcul et de stockage pour chaque lot.

Important

- Si vous envisagez de créer une image à partir d'un système Windows 10 WorkSpace, notez que la création d'image n'est pas prise en charge sur les systèmes Windows 10

qui ont été mis à niveau d'une version de Windows 10 vers une version plus récente de Windows 10 (une feature/version mise à niveau de Windows). Toutefois, les mises à jour cumulatives ou de sécurité de Windows sont prises en charge par le processus de WorkSpaces création d'images.

- Après le 14 janvier 2020, les images ne peuvent pas être créées à partir de packs Windows 7 publics. Vous pouvez envisager de migrer votre Windows 7 WorkSpaces vers Windows 10. Pour de plus amples informations, veuillez consulter [Migrer un Workspace dans WorkSpaces Personal](#).
- Le pack Graphics n'est plus pris en charge depuis le 30 novembre 2023 et le GraphicsPro bundle arrive à end-of-life expiration le 31 octobre 2025. Nous vous recommandons de migrer WorkSpaces vers un bundle GPU compatible. Pour de plus amples informations, veuillez consulter [Migrer un Workspace dans WorkSpaces Personal](#).
- GraphicsPro le forfait arrive end-of-life à expiration le 31 octobre 2025. Nous vous recommandons de migrer votre offre groupée GraphicsPro WorkSpaces de GPU vers un pack compatible avant le 31 octobre 2025. Pour de plus amples informations, veuillez consulter [the section called "Migrer un Workspace"](#).
- Les volumes de stockage groupés personnalisés ne peuvent pas être inférieurs aux volumes de stockage d'images.
- De plus, les offres groupées avec Office 2016 ou Office 2019 ne seront plus prises en charge après le 14 octobre 2025. Nous vous recommandons de migrer vos WorkSpaces offres groupées avec ces versions d'Office pour utiliser Office 2021. Pour plus d'informations, voir [Gérer les applications dans WorkSpaces Personal](#).

Les offres groupées personnalisées coûtent le même prix que les offres groupées publiques à partir desquelles elles sont créées. Pour plus d'informations sur les tarifs, consultez [Amazon WorkSpaces Pricing](#).

Table des matières

- [Conditions requises pour créer des images personnalisées Windows](#)
- [Conditions requises pour créer des images personnalisées Linux](#)
- [Bonnes pratiques](#)
- [\(Facultatif\) Étape 1 : Définir un format de nom d'ordinateur personnalisé pour votre image](#)
- [Étape 2 : Exécuter l'outil de vérification d'image](#)
- [Étape 3 : Créer une image et un bundle personnalisés](#)

- [Ce qui est inclus dans les images WorkSpaces personnalisées Windows](#)
- [Ce qui est inclus dans les images WorkSpace personnalisées Linux](#)

Conditions requises pour créer des images personnalisées Windows

Note

Windows définit actuellement 1 Go comme 1 073 741 824 octets. Les clients devront s'assurer qu'ils disposent de plus de 12 884 901 888 octets (ou 12 Go) libres sur le lecteur C et que le profil utilisateur est inférieur à 10 737 418 240 octets (ou 10 GiB) pour créer une image d'un. Workspace

- Le statut du Workspace doit être Disponible et son état de modification doit être Aucun.
- Toutes les applications et tous les profils utilisateur des WorkSpaces images doivent être compatibles avec Microsoft Sysprep.
- Toutes les applications à inclure dans l'image doivent être installées sur le lecteur C.
- Pour Windows 7 WorkSpaces, sa taille totale (fichiers et données) doit être inférieure à 10 Go.
- Pour Windows 7 WorkSpaces, le C lecteur doit disposer d'au moins 12 Go d'espace disponible.
- Tous les services d'application exécutés sur le Workspace doivent utiliser un compte système local au lieu des informations d'identification de l'utilisateur du domaine. Par exemple, une installation de Microsoft SQL Server Express ne peut pas s'exécuter avec les informations d'identification d'un utilisateur de domaine.
- Ils ne Workspace doivent pas être chiffrés. La création d'images à partir d'une image chiffrée n'Workspace est actuellement pas prise en charge.
- Les composants suivants sont requis dans une image. Sans ces composants, le fichier WorkSpaces que vous lancez à partir de l'image ne fonctionnera pas correctement. Pour de plus amples informations, veuillez consulter [the section called “Configuration requise et composants de service”](#).
 - Windows PowerShell version 3.0 ou ultérieure
 - Services Bureau à distance
 - AWS Pilotes photovoltaïques
 - Gestion à distance Windows (WinRM)
 - Agents et pilotes Teradici PCo IP

- Agents et pilotes STXHD
- AWS et WorkSpaces certificats
- Agent Skylight

Conditions requises pour créer des images personnalisées Linux

- Le statut du Workspace doit être Disponible et son état de modification doit être Aucun.
- Toutes les applications à inclure dans l'image doivent être installées en dehors du volume utilisateur (le répertoire /home).
- Le volume racine (/) doit être plein à moins de 97 %.
- Ils ne Workspace doivent pas être chiffrés. La création d'images à partir d'une image chiffrée n'Workspace est actuellement pas prise en charge.
- Les composants suivants sont requis dans une image. Sans ces composants, le fichier WorkSpaces que vous lancez depuis l'image ne fonctionnera pas correctement :
 - Cloud-init
 - Agents et pilotes Teradici PCo IP ou DCV
 - Agent Skylight

Bonnes pratiques

Avant de créer une image à partir d'un Workspace, procédez comme suit :

- Utilisez un VPC distinct, qui n'est pas connecté à votre environnement de production.
- Déployez le Workspace dans un sous-réseau privé et utilisez une instance NAT pour le trafic sortant.
- Utilisez un petit répertoire Simple AD.
- Utilisez la plus petite taille de volume pour la source Workspace, puis ajustez-la selon vos besoins lors de la création du bundle personnalisé.
- Installez toutes les mises à jour du système d'exploitation (à l'exception des mises à jour des fonctionnalités/versions de Windows) et toutes les mises à jour des applications sur le Workspace. Pour plus d'informations, consultez la [remarque importante](#) au début de cette rubrique.
- Supprimez les données mises en cache Workspace qui ne devraient pas être incluses dans le bundle (par exemple, l'historique du navigateur, les fichiers mis en cache et les cookies du navigateur).

- Supprimez les paramètres de configuration WorkSpace qui ne devraient pas être inclus dans le bundle (par exemple, les profils de messagerie).
- Basculez vers les paramètres d'adresse IP dynamique à l'aide de DHCP.
- Assurez-vous de ne pas avoir dépassé votre quota d' WorkSpace images autorisées dans une région. Par défaut, vous êtes autorisé à 40 WorkSpace images par région. Si vous avez atteint ce quota, les nouvelles tentatives de création d'une image échoueront. Pour demander une augmentation de quota, utilisez le formulaire [Limites WorkSpaces](#) .
- Assurez-vous que vous n'essayez pas de créer une image à partir d'une image chiffrée WorkSpace. La création d'images à partir d'une image chiffrée n' WorkSpace est actuellement pas prise en charge.
- Si vous utilisez un logiciel antivirus sur le WorkSpace, désactivez-le pendant que vous essayez de créer une image.
- Si un pare-feu est activé sur votre WorkSpace ordinateur, assurez-vous qu'il ne bloque aucun port nécessaire. Pour de plus amples informations, veuillez consulter [Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal](#).
- Pour Windows WorkSpaces, ne configurez aucun objet de stratégie de groupe (GPOs) avant la création de l'image.
- Pour Windows WorkSpaces, ne personnalisez pas le profil utilisateur par défaut (C:\Users\Default) avant de créer une image. Nous vous recommandons d'apporter des personnalisations au GPOs profil utilisateur et de les appliquer après la création de l'image. GPOs peuvent être facilement modifiés ou annulés, et sont donc moins sujets aux erreurs que les personnalisations apportées au profil utilisateur par défaut.
- Pour Linux WorkSpaces, consultez également le livre blanc [« Meilleures pratiques pour préparer vos images Amazon WorkSpaces pour Linux »](#).
- Si vous souhaitez utiliser des cartes à puce sous Linux WorkSpaces avec DCV activé, consultez [Utiliser des cartes à puce pour l'authentification dans WorkSpaces Personal](#) les personnalisations que vous devez apporter à votre système Linux WorkSpace avant de créer votre image.
- Assurez-vous de mettre à jour les pilotes de dépendance réseau tels que les pilotes ENA et PV de votre WorkSpaces. NVMe Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, voir [Installer ou mettre à niveau le pilote Elastic Network Adapter \(ENA\)](#), [Pilotes NVMe AWS pour les instances Windows](#), et [Mettre à niveau les pilotes PV sur les instances Windows](#).

- Assurez-vous de mettre régulièrement à jour les agents EC2 Config, EC2 EC2 Launch et Launch V2 vers les dernières versions. Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez [Update EC2 Config and EC2 Launch](#).

(Facultatif) Étape 1 : Définir un format de nom d'ordinateur personnalisé pour votre image

Pour les images WorkSpaces lancées à partir de vos images personnalisées ou des images BYOL (Bring Your Own License), vous pouvez spécifier un préfixe personnalisé pour le format de nom d'ordinateur au lieu d'utiliser le format de [nom d'ordinateur par défaut](#). Pour spécifier un préfixe personnalisé, suivez la procédure adaptée à votre type d'image.

Pour spécifier un format de nom d'ordinateur personnalisé pour les images personnalisées

Note

Par défaut, le format du nom de l'ordinateur pour Windows 10 WorkSpaces est DESKTOP-XXXXX et pour Windows 11 WorkSpaces, WORKSPA-XXXXX.

1. Sur celui WorkSpace que vous utilisez pour créer votre image personnalisée, ouvrez-le dans le Bloc-notes ou C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml dans un autre éditeur de texte. Pour plus d'informations sur l'utilisation du Unattend.xml fichier, consultez [Fichiers de réponses \(unattend.xml\)](#) de la documentation Microsoft.

Note

Pour accéder au lecteur C : depuis l'explorateur de fichiers Windows de votre ordinateur WorkSpace, entrez **C:** dans la barre d'adresse.

2. Dans la section `<settings pass="specialize">`, assurez-vous que `<ComputerName>` est défini avec un astérisque (*). Si `<ComputerName>` est défini à une autre valeur, les paramètres du nom d'ordinateur personnalisé seront ignorés. Pour plus d'informations sur le `<ComputerName>` paramètre, consultez [ComputerName](#) la documentation Microsoft.
3. Dans la section `<settings pass="specialize">`, définissez `<RegisteredOrganization>` et `<RegisteredOwner>` selon vos valeurs préférées.

Pendant la phase Sysprep, les valeurs que vous spécifiez pour `<RegisteredOwner>` et `<RegisteredOrganization>` sont concaténées ensemble, et les 7 premiers caractères de la chaîne combinée sont utilisés pour créer le nom d'ordinateur. Par exemple, si vous spécifiez **Amazon.com** pour `<RegisteredOrganization>` et **EC2** pour `<RegisteredOwner>`. Pour les images basées sur Windows 10, les noms des ordinateurs WorkSpaces utilisant des ensembles personnalisés commenceront par EC2 AMAZ-. **xxxxxxx** Pour les images basées sur Windows 11, les noms des ordinateurs WorkSpaces utilisant des ensembles personnalisés commenceront par WORKSPA-. **xxxxxxx**

 Note

- Les valeurs `<RegisteredOrganization>` et `<RegisteredOwner>` de la section `<settings pass="oobeSystem">` sont ignorées par Sysprep.
- `<RegisteredOrganization>` et `<RegisteredOwner>` sont des valeurs obligatoires.

4. Enregistrez vos modifications dans le fichier `Unattend.xml`.

Pour spécifier un format de nom d'ordinateur personnalisé pour les images BYOL

1. Si vous utilisez Windows 10, ouvrez `C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml` dans le Bloc-notes ou tout autre éditeur de texte. Si vous utilisez Windows 11, ouvrez `C:\ProgramData\Amazon\EC2Launch\sysprep\00BE_unattend.xml`.
2. Dans `<settings pass="specialize">` cette section, si vous utilisez Windows 10, décommentez `<ComputerName>*``</ComputerName>`. Si vous utilisez Windows 11, il n'est pas nécessaire de décommenter cette section. Assurez-vous qu'il `<ComputerName>` est défini sur un astérisque (\*). Si `<ComputerName>` est défini à une autre valeur, les paramètres du nom d'ordinateur personnalisé seront ignorés. Pour plus d'informations sur le `<ComputerName>` paramètre, consultez [ComputerName](#) la documentation Microsoft.
3. Dans la `<settings pass="specialize">` section, le `<RegisteredOrganization>` champ sera présent pour Windows 10 et Windows 11. La `<RegisteredOwner>` balise ne sera présente que dans Windows 10 par défaut. Si vous utilisez Windows 11, vous devez ajouter cette balise. Réglez `<RegisteredOrganization>` et `<RegisteredOwner>` sur vos valeurs préférées.

Pendant la phase Sysprep, les valeurs que vous spécifiez pour <RegisteredOwner> et <RegisteredOrganization> sont concaténées ensemble, et les 7 premiers caractères de la chaîne combinée sont utilisés pour créer le nom d'ordinateur. Par exemple, si vous spécifiez **Amazon.com** pour <RegisteredOrganization> et **EC2** pour <RegisteredOwner>, les noms des ordinateurs WorkSpaces créés à partir de votre bundle personnalisé commenceront par EC2 AMAZ-xxxxxxx.

 Note

- Les valeurs <RegisteredOrganization> et <RegisteredOwner> de la section <settings pass="oobeSystem"> sont ignorées par Sysprep.
- < RegisteredOrganization > et < RegisteredOwner > sont des valeurs obligatoires.

4. Si vous utilisez Windows 10, enregistrez les modifications apportées au fichier Sysprep2008.xml. Si vous utilisez Windows 11, enregistrez vos modifications apportées au fichier 00BE_unattend.xml.

Étape 2 : Exécuter l'outil de vérification d'image

 Note

Le vérificateur d'images n'est disponible que pour Windows WorkSpaces. Si vous créez une image à partir d'un système Linux Workspace, passez directement à [Étape 3 : Créer une image et un bundle personnalisés](#).

Pour vérifier que votre Windows Workspace répond aux exigences relatives à la création d'images, nous vous recommandons d'exécuter le Vérificateur d'images. Le vérificateur d'images effectue une série de tests sur le produit Workspace que vous souhaitez utiliser pour créer votre image et fournit des conseils sur la manière de résoudre les problèmes détectés.

 Important

- Vous Workspace devez réussir tous les tests effectués par le vérificateur d'images avant de pouvoir l'utiliser pour créer une image.

- Avant d'exécuter le vérificateur d'images, vérifiez que les dernières mises à jour de sécurité et cumulatives de Windows sont installées sur votre WorkSpace.

Pour obtenir l'outil de vérification d'image, effectuez l'une des opérations suivantes :

- [Redémarrez votre WorkSpace](#). L'outil de vérification d'image est téléchargé automatiquement pendant le redémarrage et installé à l'emplacement `C:\Program Files\Amazon\ImageChecker.exe`.
- Téléchargez Amazon WorkSpaces Image Checker depuis <https://tools.amazonworkspaces.com/ImageChecker/.zip> et extrayez le fichier. `ImageChecker.exe`. Copiez ce fichier dans `C:\Program Files\Amazon\`.

Pour exécuter le l'outil de vérification d'image

1. Ouvrez le fichier `C:\Program Files\Amazon\ImageChecker.exe`.
2. Dans la boîte de dialogue Amazon WorkSpaces Image Checker, choisissez Run.
3. Lorsqu'un test est terminé, vous pouvez en afficher le statut.

Si un test affiche le statut FAILED (ÉCHEC), choisissez Info (Informations) pour afficher de plus amples informations sur la manière de résoudre le problème qui a provoqué l'échec. Pour de plus amples informations sur la résolution de ces problèmes, veuillez consulter [Conseils pour résoudre les problèmes détectés par l'outil de vérification d'image](#).

Si des tests affichent le statut WARNING (AVERTISSEMENT), choisissez le bouton Fix all Warnings (Corriger tous les avertissements).

L'outil génère un fichier journal de sortie dans le répertoire où se trouve l'outil de vérification d'image. Par défaut, ce fichier est situé à l'emplacement suivant : `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

 Tip

Ne supprimez pas ce fichier journal. Si un problème se produit, ce fichier journal peut être utile pour le résoudre.

4. Le cas échéant, résolvez les problèmes à l'origine d'échecs et d'avertissements, et répétez le processus d'exécution du vérificateur d'images jusqu'à ce qu'il WorkSpace réussisse tous les tests. Tous les échecs et avertissements doivent être résolus pour pouvoir créer une image.
5. Une fois que vous WorkSpace avez réussi tous les tests, le message « Validation réussie » s'affiche. Vous êtes maintenant prêt pour créer un bundle personnalisé.

Conseils pour résoudre les problèmes détectés par l'outil de vérification d'image

En plus de consulter les conseils suivants pour résoudre les problèmes détectés par l'outil de vérification d'image, assurez-vous de consulter le fichier journal de l'outil de vérification d'image à l'adresse `C:\Program Files\Amazon\ImageChecker_YYYYMMDDHHMMSS.log`.

PowerShell la version 3.0 ou ultérieure doit être installée

Installez la dernière version de [Microsoft Windows PowerShell](#).

Important

La politique PowerShell d'exécution d'un WorkSpace doit être définie pour autoriser RemoteSigned les scripts. Pour vérifier la politique d'exécution, exécutez la ExecutionPolicy PowerShell commande Get-. Si la politique d'exécution n'est pas définie sur Unrestricted RemoteSigned, exécutez la ExecutionPolicy RemoteSigned commande Set- ExecutionPolicy — pour modifier la valeur de la politique d'exécution. Ce RemoteSigned paramètre permet l'exécution de scripts sur Amazon WorkSpaces, ce qui est nécessaire pour créer une image.

Seuls les lecteurs C et D peuvent être présents

Seuls les D lecteurs C et peuvent être présents sur un WorkSpace disque utilisé pour l'imagerie. Retirez tous les autres lecteurs, y compris les lecteurs virtuels.

Aucun redémarrage en attente dans le cadre de mises à jour Windows ne peut être détecté

- Le processus de création d'image ne peut pas être exécuté tant que Windows n'a pas été redémarré pour terminer l'installation des mises à jour de sécurité ou cumulatives. Redémarrez Windows pour appliquer ces mises à jour et assurez-vous qu'aucune autre mise à jour cumulative ou de sécurité Windows en attente ne doit être installée.

- La création d'images n'est pas prise en charge sur les systèmes Windows 10 qui ont été mis à niveau d'une version de Windows 10 vers une version plus récente de Windows 10 (feature/version mise à niveau de Windows). Toutefois, les mises à jour cumulatives ou de sécurité de Windows sont prises en charge par le processus de WorkSpaces création d'images.

Le fichier Sysprep doit exister et ne peut pas être vide

En cas de problème avec votre fichier Sysprep, contactez le [AWS Support Centre](#) pour faire réparer votre EC2 Config ou EC2 Launch.

La taille du profil utilisateur doit être inférieure à 10 Go

Pour Windows 7 WorkSpaces, le profil utilisateur (D:\Users*username*) doit être inférieur à 10 Go au total. Pour réduire la taille du profil utilisateur, supprimez des fichiers.

Le lecteur C doit avoir suffisamment d'espace libre

Pour Windows 7 WorkSpaces, vous devez disposer d'au moins 12 Go d'espace libre sur le disque C. Pour libérer de l'espace sur le lecteur C, supprimez des fichiers. Pour Windows 10 WorkSpaces, ignorez si vous recevez un FAILED message et que l'espace disque est supérieur à 2 Go.

Aucun service ne peut être exécuté sous un compte de domaine

Pour exécuter le processus de création d'image, aucun service ne Workspace peut être exécuté sous un compte de domaine. Tous les services doivent être exécutés sous un compte local.

Pour exécuter des services sous un compte local

1. Ouvrez C:\Program Files\Amazon\ImageChecker_*yyyyMMddhhmmss*.log et recherchez la liste des services qui s'exécutent sous un compte de domaine.
2. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
3. Sous Ouvrir une session en tant que, recherchez les services qui s'exécutent sous des comptes de domaine. (Les services s'exécutant en tant que Système local, Service local, ou Service réseau n'interfèrent pas avec la création d'image.)
4. Sélectionnez un service qui s'exécute sous un compte de domaine, puis choisissez Action, Propriétés.
5. Ouvrez l'onglet Ouvrir une session. Sous Ouvrir une session en tant que, choisissez Compte système local.

6. Choisissez OK.

Le WorkSpace doit être configuré pour utiliser le DHCP

Vous devez configurer tous les adaptateurs réseau de manière WorkSpace à utiliser le DHCP au lieu d'adresses IP statiques.

Pour configurer toutes les cartes réseau afin qu'elles utilisent DHCP

1. Dans la zone de recherche Windows, entrez **control panel** pour ouvrir le Panneau de configuration.
2. Choisissez Réseau et Internet.
3. Choisissez Centre Réseau et partage.
4. Choisissez Modifier les paramètres de la carte, puis sélectionnez une carte.
5. Choisissez Modifier les paramètres de cette connexion.
6. Dans l'onglet Réseau, sélectionnez Internet Protocol version 4 (TCP/IPv4), puis choisissez Propriétés.
7. Dans la boîte de dialogue Propriétés du protocole Internet version 4 (TCP/IPv4), sélectionnez Obtenir une adresse IP automatiquement.
8. Choisissez OK.
9. Répétez cette procédure pour tous les adaptateurs réseau du WorkSpace.

Les services Bureau à distance doivent être activés

Le processus de création d'image nécessite l'activation des services Bureau à distance.

Pour activer les services Bureau à distance

1. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
2. Dans la colonne Nom recherchez Services Bureau à distance.
3. Sélectionnez Services Bureau à distance, puis choisissez Action, Propriétés.
4. Sous l'onglet Général pour Type de démarrage, choisissez Manuel ou Automatique.

5. Choisissez OK.

Un profil utilisateur doit exister

Le WorkSpace fichier que vous utilisez pour créer des images doit avoir un profil utilisateur (D : \Users*username*). Si ce test échoue, contactez le [Centre AWS Support](#) pour obtenir de l'aide.

Le chemin d'accès de la variable d'environnement doit être correctement configuré

Le chemin de la variable d'environnement pour la machine locale ne contient pas d'entrées pour System32 et pour Windows PowerShell. Ces entrées sont requises pour l'exécution du processus de création d'image.

Pour configurer le chemin d'accès de votre variable d'environnement

1. Dans la zone de recherche Windows, entrez **environment variables** et choisissez Modifier les variables d'environnement système.
2. Dans la boîte de dialogue Propriétés système ouvrez l'onglet Avancé et choisissez Variables d'environnement.
3. Dans la boîte de dialogue Variables d'environnement sous Variables système, sélectionnez l'entrée Chemin puis choisissez Modifier.
4. Choisissez Nouveau, puis ajoutez le chemin d'accès suivant :

C:\Windows\System32

5. Choisissez de nouveau Nouveau puis ajoutez le chemin suivant :

C:\Windows\System32\WindowsPowerShell\v1.0\

6. Choisissez OK.
7. Redémarrez le WorkSpace.

Tip

L'ordre dans lequel les éléments apparaissent dans le chemin de la variable d'environnement est important. Pour déterminer l'ordre correct, vous pouvez comparer le chemin de votre variable d'environnement WorkSpace avec celui d'une instance Windows nouvellement créée WorkSpace ou nouvelle.

Le programme d'installation pour les modules Windows doit être activé

Le processus de création d'image nécessite l'activation du service Programme d'installation pour les modules Windows.

Pour activer le service Programme d'installation pour les modules Windows

1. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
2. Dans la colonne Nom recherchez le Programme d'installation pour les modules Windows.
3. Sélectionnez le Programme d'installation pour les modules Windows, puis choisissez Action, Propriétés.
4. Sous l'onglet Général pour Type de démarrage, choisissez Manuel ou Automatique.
5. Choisissez OK.

L'agent Amazon SSM doit être désactivé

Le processus de création d'image nécessite la désactivation du service Amazon SSM Agent.

Pour désactiver le service Amazon SSM Agent

1. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
2. Dans la colonne Nom recherchez Amazon SSM Agent.
3. Sélectionnez Agent Amazon SSM, puis choisissez Action, Propriétés.
4. Sous l'onglet Général pour Type de démarrage, choisissez Désactivé.
5. Choisissez OK.

Les versions SSL et TLS 1.2 doivent être activées

Pour configurer SSL/TLS pour Windows, consultez [Comment activer le protocole TLS 1.2](#) dans la documentation Microsoft Windows.

Il ne peut y avoir qu'un seul profil d'utilisateur sur le Workspace

Il ne peut y avoir qu'un seul profil WorkSpaces utilisateur (D:\Users*username*) Workspace que vous utilisez pour créer des images. Supprimez tous les profils utilisateur qui n'appartiennent pas à l'utilisateur prévu du Workspace.

Pour que la création d'images fonctionne, vous ne Workspace pouvez avoir que trois profils utilisateur :

- Le profil utilisateur de l'utilisateur auquel le Workspace (D:\Users*username*) est destiné
- Le profil utilisateur par défaut (également connu sous le nom de Profil par défaut)
- Le profil utilisateur Administrateur

Si d'autres profils utilisateur sont présents, vous pouvez les supprimer via les propriétés système avancées du Panneau de configuration Windows.

Pour supprimer un profil utilisateur

1. Pour accéder aux propriétés système avancées, effectuez l'une des opérations suivantes :
 - Appuyez sur les touches Windows+pause/arrêt, puis choisissez Paramètres système avancés dans le volet gauche de la boîte de dialogue Panneau de configuration > Système et sécurité > Système.
 - Dans la zone de recherche Windows, entrez **control panel**. Dans le Panneau de configuration, choisissez Système et sécurité, puis Système, puis Paramètres système avancés dans le volet gauche de la boîte de dialogue Panneau de configuration > Système et sécurité > Système.
2. Dans la boîte de dialogue Propriétés système sous l'onglet Avancé choisissez Paramètres sous Profils utilisateur.
3. Si un profil autre que le profil administrateur, le profil par défaut et le profil de l'WorkSpacesutilisateur prévu est répertorié, sélectionnez ce profil supplémentaire et choisissez Supprimer.
4. À la question sur la suppression du profil, choisissez Oui.
5. Si nécessaire, répétez les étapes 3 et 4 pour supprimer tout autre profil n'appartenant pas au Workspace.
6. Cliquez deux fois sur OK et fermez le Panneau de configuration.

7. Redémarrez le Workspace.

Aucun package AppX ne peut être dans un état intermédiaire

Un ou plusieurs packages AppX sont dans un état intermédiaire. Cela peut provoquer une erreur Sysprep lors de la création d'image.

Pour supprimer tous les packages AppX intermédiaires

1. Dans la zone de recherche Windows, entrez **powershell**. Choisissez Exécuter en tant qu'administrateur.
2. À la question « Voulez-vous autoriser cette application à apporter des modifications à votre appareil ? », choisissez Oui.
3. Dans la PowerShell fenêtre Windows, entrez les commandes suivantes pour répertorier tous les packages AppX préparés, puis appuyez sur Entrée après chacun d'eux.

```
$workspaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages | Where-Object { `
    (($_ .PackageUserInformation -like "*S-1-5-18*" -
and !($_ .PackageUserInformation -like "$workspaceUserName")) -and `
    ($_ .PackageUserInformation -like "*Staged*" -or
    $_ .PackageUserInformation -like "*Installed*")) -or `
    ((($_ .PackageUserInformation -like "*S-1-5-18*" -
and $_ .PackageUserInformation -like "$workspaceUserName")) -and `
    $_ .PackageUserInformation -like "*Staged*")
}
```

4. Exécutez la commande suivante avec des privilèges SYSTEM élevés pour supprimer toutes les entrées de provisionnement de packages AppX intermédiaires, puis appuyez sur Entrée.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Exécutez de nouveau l'outil de vérification d'image. Si ce test échoue toujours, entrez les commandes suivantes pour supprimer tous les packages AppX et appuyez sur Entrée après chaque package.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -  
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows ne doit pas avoir été mis à niveau à partir d'une version précédente

La création d'images n'est pas prise en charge sur les systèmes Windows qui ont été mis à niveau d'une version de Windows 10 vers une version plus récente de Windows 10 (feature/version mise à niveau de Windows).

Pour créer des images, utilisez une image WorkSpace qui n'a pas subi de feature/version mise à niveau vers Windows.

Le nombre de réinitialisations Windows ne doit pas être nul

La fonction de réinitialisation vous permet de prolonger la période d'activation de la version d'évaluation de Windows. Le processus de création d'image nécessite que la valeur du nombre de réinitialisations soit différente de 0.

Pour vérifier le nombre de réinitialisations Windows

1. Dans le menu Démarrer de Windows, choisissez Système Windows, puis Invite de commandes.
2. À l'invite de commande, saisissez la commande suivante, puis appuyez sur Entrée.

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

Pour réinitialiser le nombre de réinitialisations à une valeur différente de 0, veuillez consulter [Sysprep \(Generalize\) a Windows installation](#) dans la documentation Microsoft Windows.

Autres conseils pour la résolution des problèmes

Si vous WorkSpace réussissez tous les tests effectués par le vérificateur d'images, mais que vous ne parvenez toujours pas à créer une image à partir du WorkSpace, vérifiez les problèmes suivants :

- Assurez-vous que le WorkSpace n'est pas attribué à un utilisateur au sein d'un groupe d'invités du domaine. Pour vérifier s'il existe des comptes de domaine, exécutez la PowerShell commande suivante.

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*$env:USERDOMAIN*" }
```

- Pour Windows 7 WorkSpaces uniquement : si des problèmes surviennent lors de la copie du profil utilisateur lors de la création de l'image, vérifiez les problèmes suivants :
 - Les chemins de profil longs peuvent provoquer des erreurs de création d'image. Assurez-vous que la longueur des chemins de tous les dossiers du profil utilisateur est inférieure à 261 caractères.
 - Assurez-vous d'accorder des autorisations complètes sur le dossier de profil au système et à tous les packages d'application.
 - Si des fichiers du profil utilisateur sont verrouillés par un processus ou sont utilisés lors de la création de l'image, la copie du profil peut échouer.
- Certains objets de stratégie de groupe (GPOs) limitent l'accès à l'empreinte numérique du certificat RDP lorsque celui-ci est demandé par le service EC2 Config ou les scripts de EC2 lancement lors de la configuration de l'instance Windows. Avant d'essayer de créer une image, déplacez-la WorkSpace vers une nouvelle unité organisationnelle (UO) dont l'héritage est bloqué et non GPOs appliqué.
- Assurez-vous que le service Gestion à distance de Windows (WinRM) est configuré de manière à démarrer automatiquement. Procédez comme suit :
 1. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
 2. Dans la colonne Nom recherchez Gestion à distance de Windows (Gestion WSM).
 3. Sélectionnez Gestion à distance de Windows (Gestion WSM), puis choisissez Action, Propriétés.
 4. Sous l'onglet Général pour Type de démarrage, choisissez Automatique.
 5. Choisissez OK.

Étape 3 : Créer une image et un bundle personnalisés

Après avoir validé votre WorkSpace image, vous pouvez procéder à la création de votre image personnalisée et de votre bundle personnalisé.

Pour créer une image et un bundle personnalisés

1. Si vous êtes toujours connecté au WorkSpace, déconnectez-vous en choisissant Amazon WorkSpaces et Disconnect dans l'application WorkSpaces cliente.
2. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
3. Dans le panneau de navigation, sélectionnez WorkSpaces.
4. Sélectionnez le WorkSpace pour ouvrir sa page de détails, puis choisissez Créer une image. Si le statut du WorkSpace est Arrêté, vous devez d'abord le démarrer (choisissez Actions, Démarrer WorkSpaces) avant de choisir Actions, Créer une image.

Note

Pour créer une image par programmation, utilisez l'action CreateWorkspaceImage API. Pour plus d'informations, consultez [CreateWorkspaceImage](#) le Amazon WorkSpaces API Reference.

5. Un message s'affiche, vous invitant à redémarrer (redémarrer) votre ordinateur WorkSpace avant de continuer. Le redémarrage WorkSpace met à jour votre WorkSpaces logiciel Amazon vers la dernière version.

Redémarrez votre ordinateur WorkSpace en fermant le message et en suivant les étapes indiquées [Redémarrer un WorkSpace dans WorkSpaces Personal](#). Lorsque vous avez terminé, répétez l'étape [Step 4](#) de cette procédure, mais cette fois choisissez Suivant lorsque le message de redémarrage apparaît. Pour créer une image, le statut de WorkSpace doit être Disponible et son état de modification doit être Aucun.

6. Saisissez un nom et une description pour l'image qui vous permettront de l'identifier, puis choisissez Create Image (Créer une image). Pendant la création de l'image, le statut du WorkSpace est Suspendu et n' WorkSpace est pas disponible.

Note

Lorsque vous saisissez la description d'une image, assurez-vous de ne pas utiliser le caractère spécial « - », sinon vous obtiendrez un message d'erreur.

7. Dans le volet de navigation, choisissez Images. L'image est complète lorsque le statut WorkSpace passe à Disponible (cela peut prendre jusqu'à 45 minutes).
8. Sélectionnez l'image et choisissez Actions, Créer un bundle.

 Note

Pour créer un bundle par programmation, utilisez l'action d'API `CreateWorkspaceBundle`. Pour plus d'informations, consultez [CreateWorkspaceBundle](#) le Amazon WorkSpaces API Reference.

9. Saisissez un nom et une description pour le bundle, puis effectuez les opérations suivantes :
- Pour le type de matériel du bundle, choisissez le matériel à utiliser lors WorkSpaces du lancement à partir de ce bundle personnalisé.
 - Pour Paramètres de stockage, sélectionnez l'une des combinaisons par défaut pour le volume racine et la taille du volume utilisateur, ou sélectionnez Personnalisé, puis saisissez des valeurs (jusqu'à 2 000 Go) pour Taille du volume racine et Taille du volume utilisateur.

Les tailles par défaut disponibles pour le volume racine (pour Microsoft Windows, le lecteur C, pour Linux, /) et le volume utilisateur (pour Windows, le lecteur D, pour Linux, /home) sont les suivantes :

- Racine : 80 Go, Utilisateur : 10 Go, 50 Go ou 100 Go
- Racine : 175 Go, Utilisateur : 100 Go
- Les exigences de stockage pour l'utilisation du GPU évoluent proportionnellement au WorkSpaces dimensionnement de l'instance. Lorsque vous sélectionnez des WorkSpaces configurations GPU de plus grande taille, vous devez allouer des volumes de stockage proportionnellement plus importants pour maintenir des performances optimales et répondre aux demandes de charge de travail accrues. Pour la plus petite taille d'instance, commencez par l'allocation de stockage suivante : Root : 100 Go, utilisateur : 100 Go

Vous pouvez également étendre les volumes racine et utilisateur jusqu'à 2 000 Go chacun.

 Note

Pour garantir la préservation de vos données, vous ne pouvez pas réduire la taille des volumes root ou utilisateur après avoir lancé un Workspace. Assurez-vous plutôt de spécifier les tailles minimales pour ces volumes lorsque vous lancez un Workspace.

- Vous pouvez lancer un volume Value, Standard, Performance, Power ou PowerPro Workspace avec un minimum de 80 Go pour le volume racine et de 10 Go pour le volume utilisateur.

- Vous pouvez lancer un GeneralPurpose fichier .4xlarge ou GeneralPurpose .8xlarge Workspace avec un minimum de 175 Go pour le volume racine et de 100 Go pour le volume utilisateur.

10. Choisissez Créer un bundle.

11. Pour confirmer que votre bundle est créé, choisissez Bundles, et vérifiez qu'il est répertorié.

Ce qui est inclus dans les images WorkSpaces personnalisées Windows

Lorsque vous créez une image à partir d'un système Windows 7, Windows 10 ou Windows 11 WorkSpace, tout le contenu du C lecteur est inclus.

Pour Windows 10 ou 11 WorkSpaces, le profil utilisateur n'D:\Users*username* est pas inclus dans l'image personnalisée.

Pour Windows 7 WorkSpaces, l'intégralité du contenu du profil utilisateur est incluse, à D:\Users*username* l'exception des éléments suivants :

- Contacts
- Téléchargements
- Musique
- Images
- Jeux enregistrés
- Vidéos
- Podcasts
- Machines virtuelles
- .virtualbox
- Suivi
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\

- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\iconcache\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Ce qui est inclus dans les images WorkSpace personnalisées Linux

Lorsque vous créez une image à partir d'un Amazon Linux WorkSpace, l'intégralité du contenu du volume utilisateur (/home) est supprimée. Le contenu du volume racine (/) est inclus, à l'exception des clés et dossiers suivants qui sont retirés :

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache

- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-données
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/lib/AccountsService/users

Les clés suivantes sont détruites lors de la création de l'image personnalisée :

- /etc/ssh/ssh_hôte_*_clé
- /etc/ssh/ssh_hôte_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.clé
- /var/lib/skylight/public.clé

Mettre à jour un pack personnalisé pour WorkSpaces Personal

Vous pouvez mettre à jour un WorkSpaces ensemble personnalisé existant en modifiant un WorkSpace qui est basé sur le bundle, en créant une image à partir du WorkSpace et en mettant à jour le bundle avec la nouvelle image. Vous pouvez ensuite en lancer un nouveau à WorkSpaces l'aide du bundle mis à jour.

⚠ Important

Les offres existantes WorkSpaces ne sont pas automatiquement mises à jour lorsque vous mettez à jour le pack sur lequel elles sont basées. Pour mettre à jour des fichiers existants WorkSpaces basés sur un bundle que vous avez mis à jour, vous devez soit les reconstruire, WorkSpaces soit les supprimer et les recréer.

Pour mettre à jour un bundle à l'aide de la console

1. Connectez-vous à un WorkSpace groupe basé sur le bundle et apportez les modifications souhaitées. Par exemple, vous pouvez appliquer les derniers correctifs du système d'exploitation et de l'application, et installer d'autres applications.

Vous pouvez également en créer une nouvelle WorkSpace avec le même progiciel de base (Plus ou Standard) que l'image utilisée pour créer le bundle et apporter des modifications.

2. Si vous êtes toujours connecté au WorkSpace, déconnectez-vous en choisissant Amazon WorkSpaces et Disconnect dans l'application WorkSpaces cliente.
3. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
4. Dans le panneau de navigation, sélectionnez WorkSpaces.
5. Sélectionnez WorkSpace et choisissez Actions, Créer une image. Si le statut du WorkSpace est STOPPED, vous devez d'abord le démarrer (choisissez Actions, Démarrer WorkSpaces) avant de choisir Actions, Créer une image.
6. Saisissez le nom et la description de l'image, puis choisissez Create Image (Créer une image). Le WorkSpace n'est pas disponible lors de la création de l'image. Pour plus d'informations sur le processus de création d'images, consultez [Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal](#).
7. Dans le volet de navigation, choisissez Bundles.
8. Choisissez un bundle pour ouvrir sa page de détails, puis sous Image source, choisissez Modifier.
9. Sur la page Mettre à jour l'image source, sélectionnez l'image que vous avez créée, puis choisissez Mettre à jour le bundle.
10. Si nécessaire, mettez à jour tous WorkSpaces les éléments existants basés sur le bundle en les reconstruisant WorkSpaces ou en les supprimant et en les recréant. Pour de plus amples informations, veuillez consulter [Reconstruire un WorkSpace in WorkSpaces Personal](#).

Pour mettre à jour un bundle par programmation

Pour créer un bundle par programmation, utilisez l'action d'API `UpdateWorkspaceBundle`. Pour plus d'informations, consultez [UpdateWorkspaceBundle](#) le Amazon WorkSpaces API Reference.

Copier une image personnalisée dans WorkSpaces Personal

Vous pouvez copier une WorkSpaces image personnalisée au sein d'une région ou d'une AWS région à l'autre. La copie d'une image permet de créer une image identique avec son propre identificateur unique.

Vous pouvez copier une image BYOL (licence à fournir) dans une autre région tant que la région de destination est activée pour l'option BYOL. Assurez-vous que l'option BYOL est activée pour l'ensemble des comptes et des régions concernés.

Note

Pour la région Chine (Ningxia), vous ne pouvez copier des images que dans la même région. Dans les AWS GovCloud (US) Region années s, pour copier des images depuis et vers d'autres AWS régions, contactez le AWS Support.

Dans les régions sélectionnées, pour copier des images dans d'autres régions, contactez le AWS Support. Pour plus d'informations sur les régions d'acceptation, consultez [Régions disponibles](#).

Vous pouvez également copier une image qui a été partagée avec vous par un autre AWS compte. Pour plus d'informations sur les images partagées, consultez [Partager ou annuler le partage d'une image personnalisée dans Personal WorkSpaces](#).

La copie d'une image au sein d'une région ou entre les régions n'entraîne aucuns frais supplémentaires. Cependant, le quota pour le nombre d'images de la région de destination s'applique. Pour plus d'informations sur WorkSpaces les quotas Amazon, consultez [WorkSpaces Quotas Amazon](#).

Autorisations IAM pour copier une image

Si vous passez par un utilisateur IAM pour copier une image, celui-ci doit disposer des autorisations pour `workspaces:DescribeWorkspaceImages` et `workspaces:CopyWorkspaceImage`.

L'exemple de politique suivant permet à l'utilisateur de copier l'image spécifiée vers le compte spécifié dans la région spécifiée.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
        "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-  
a1bcd2efg"
      ]
    }
  ]
}
```

Important

Si vous créez une politique IAM afin de copier des images partagées pour des comptes qui n'en sont pas propriétaires, vous ne pouvez pas spécifier d'ID de compte dans l'ARN (Amazon Resource Name). À la place, vous devez utiliser * pour l'ID de compte, comme illustré dans l'exemple de politique suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
```

```
    "workspaces:CopyWorkspaceImage"
  ],
  "Resource": [
    "arn:aws:workspaces:us-east-1::workspaceimage/wsi-a1bcd2efg"
  ]
}
```

Vous pouvez spécifier un ID de compte dans l'ARN uniquement lorsque ce compte possède les images à copier.

Pour plus d'informations sur l'utilisation d'IAM, consultez [Gestion des identités et des accès pour WorkSpaces](#).

Copie d'images en bloc

Vous pouvez copier les images une par une à l'aide de la console. Pour copier des images en bloc, utilisez l'opération `CopyWorkspaceImage` API ou la `copy-workspace-image` commande contenue dans le AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez [CopyWorkspaceImage](#) le manuel Amazon WorkSpaces API Reference ou [copy-workspace-image](#) le AWS CLI Command Reference.

Important

Avant de copier une image partagée, assurez-vous qu'elle a été partagée depuis le bon AWS compte. Pour déterminer si une image a été partagée et pour voir l'identifiant du AWS compte propriétaire de l'image, utilisez les opérations [DescribeWorkSpaceImages](#) et de l'[DescribeWorkspaceImagePermissions](#) API ou [describe-workspace-image-permissions](#) les commandes [describe-workspace-images](#) et du AWS CLI.

Pour copier une image à l'aide de la console

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Images.

3. Sélectionnez l'image et choisissez Actions, Copier l'image.
4. Pour Sélectionner une destination, sélectionnez la AWS région dans laquelle vous souhaitez copier l'image.
5. Pour Nom de la copie, entrez le nouveau nom de l'image copiée, et dans Description, entrez sa description.
6. (Facultatif) Sous Balises, entrez les balises de l'image copiée. Pour de plus amples informations, veuillez consulter [Marquer les ressources dans WorkSpaces Personnel](#).
7. Choisissez Copier l'image.

Partager ou annuler le partage d'une image personnalisée dans Personal WorkSpaces

Vous pouvez partager WorkSpaces des images personnalisées entre AWS les comptes d'une même AWS région. Une fois qu'une image a été partagée, le compte du destinataire peut copier l'image dans d'autres AWS régions selon les besoins. Pour plus d'informations sur la copie des images, consultez [Copier une image personnalisée dans WorkSpaces Personnel](#).

Note

Pour la région Chine (Ningxia), vous ne pouvez copier des images que dans la même région. Dans les AWS GovCloud (US) Region années s, pour copier des images depuis et vers d'autres AWS régions, contactez le AWS Support.

Le partage d'images n'entraîne pas de frais supplémentaires. Toutefois, le quota du nombre d'images dans la AWS région s'applique. Une image partagée n'est comptabilisée dans le quota du compte destinataire que lorsque le destinataire copie l'image. Pour plus d'informations sur WorkSpaces les quotas Amazon, consultez [WorkSpaces Quotas Amazon](#).

Pour supprimer une image partagée, vous devez annuler le partage avant de pouvoir la supprimer.

Partage d'image Apportez votre propre licence

Vous ne pouvez partager des images Bring Your Own License (BYOL) qu'avec AWS des comptes activés pour le BYOL. Le AWS compte avec lequel vous souhaitez partager des images BYOL doit également faire partie de votre organisation (sous le même compte payeur).

 Note

Le partage d'images BYOL entre AWS comptes n'est pas pris en charge pour le moment dans les régions AWS GovCloud (USA Ouest) et AWS GovCloud (USA Est). Pour partager des images BYOL entre comptes situés dans les régions AWS GovCloud (ouest des États-Unis) et AWS GovCloud (est des États-Unis), contactez le Support. AWS

Images partagées avec vous

Si des images sont partagées avec vous, vous pouvez les copier. Vous pouvez ensuite utiliser vos copies des images partagées pour créer des ensembles destinés au lancement de nouvelles WorkSpaces images.

 Important

Avant de copier une image partagée, assurez-vous qu'elle a été partagée depuis le bon AWS compte. Pour déterminer par programmation si une image a été partagée, utilisez les opérations d'[DescribeWorkspaceImagePermissions](#) API [DescribeWorkSpaceImages](#) et ou les [describe-workspace-image-permissions](#) commandes [describe-workspace-images](#) et de l'interface de ligne de AWS commande (CLI).

La date de création indiquée pour une image partagée avec vous est celle à laquelle l'image a été créée à l'origine, et non la date de partage.

Quand une image a été partagée avec vous, vous ne pouvez plus la partager avec d'autres comptes.

Pour partager une image

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Images.
3. Choisissez une image pour ouvrir la page de ses informations détaillées.
4. Sur la page des détails de l'image, dans la section Comptes partagés, choisissez Ajouter un compte.
5. Sur la page Ajouter un compte, sous Ajouter un compte de partage, entrez l'ID du compte avec lequel vous souhaitez partager l'image.

 Important

Avant de partager une image, vérifiez que le partage a lieu avec l'ID de compte AWS approprié.

6. Choisissez Partager l'image.

 Note

Pour utiliser l'image partagée, le compte du destinataire doit d'abord [copier l'image](#). Le compte du destinataire peut ensuite utiliser sa copie de l'image partagée pour créer des packs en vue d'en lancer de nouveaux WorkSpaces.

Pour annuler le partage d'une image

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Images.
3. Choisissez une image pour ouvrir la page de ses informations détaillées.
4. Sur la page détaillée de l'image, dans la section Comptes partagés, sélectionnez le AWS compte avec lequel vous souhaitez arrêter le partage, puis choisissez Annuler le partage.
5. Lorsque vous êtes invité à confirmer l'annulation du partage de l'image, choisissez Annuler le partage.

 Note

Si vous souhaitez supprimer l'image après avoir annulé son partage, vous devez d'abord annuler son partage de tous les comptes avec lesquels elle a été partagée.

Si vous annulez le partage d'une image, le compte destinataire ne peut plus faire de copies de celle-ci. Cependant, toutes les copies des images partagées qui se trouvent déjà dans le compte du destinataire restent dans ce compte, et de nouvelles images WorkSpaces peuvent être créées à partir de ces copies.

Pour partager des images ou annuler leur partage par programmation

Pour partager ou annuler le partage d'images par programmation, utilisez l'opération [UpdateWorkspaceImagePermission](#) API ou la commande [update-workspace-image-permission](#) AWS Command Line Interface (AWS CLI). Pour déterminer si une image a été partagée, utilisez l'opération [DescribeWorkspaceImagePermissions](#) API ou la commande [describe-workspace-image-permissions](#) CLI.

Supprimer un ensemble ou une image personnalisé dans WorkSpaces Personal

Au besoin, vous pouvez supprimer des images ou des bundles personnalisés non utilisés.

Suppression d'un bundle

Pour supprimer un bundle, vous devez d'abord supprimer tous ceux WorkSpaces qui sont basés sur le bundle.

Pour supprimer un bundle à l'aide de la console

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Bundles.
3. Sélectionnez le bundle à supprimer, puis choisissez Supprimer.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer un bundle par programmation

Pour supprimer un bundle par programmation, utilisez l'action d'API `DeleteWorkspaceBundle`. Pour plus d'informations, consultez [DeleteWorkspaceBundle](#) le Amazon WorkSpaces API Reference.

Note

Assurez-vous d'attendre au moins 2 heures après avoir supprimé un bundle avant de créer un nouveau bundle portant le même nom.

Supprime une image

Lorsque vous supprimez un bundle personnalisé, vous pouvez supprimer l'image utilisée pour créer ou mettre à jour le bundle.

Pour supprimer une image, vous devez d'abord supprimer tous les bundles associés à celle-ci, ou mettre à jour ces bundles pour qu'ils utilisent une autre image source. Si l'image est partagée avec d'autres compte, vous devez également annuler ce partage. L'image ne peut pas non plus être à l'état En attente ni Validation en cours.

Pour supprimer une image à l'aide de la console

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Images.
3. Sélectionnez l'image à supprimer, puis choisissez Supprimer.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer une image par programmation

Pour supprimer une image par programmation, utilisez l'action d'API `DeleteWorkspaceImage`. Pour plus d'informations, consultez [DeleteWorkspaceImage](#) de l'Amazon WorkSpaces API Reference.

Moniteur WorkSpaces personnel

Vous pouvez utiliser les fonctionnalités suivantes pour surveiller votre WorkSpaces.

CloudWatch métriques

Amazon WorkSpaces publie sur Amazon des points de données CloudWatch concernant votre WorkSpaces. CloudWatch vous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Vous pouvez utiliser ces indicateurs pour vérifier que vos performances WorkSpaces sont conformes aux attentes. Pour de plus amples informations, veuillez consulter [Surveillez vos CloudWatch indicateurs WorkSpaces d'utilisation](#).

CloudWatch Événements

Amazon WorkSpaces peut soumettre des événements à Amazon CloudWatch Events lorsque les utilisateurs se connectent à votre compte Workspace. Cela vous permet de répondre lorsque l'événement se produit. Pour de plus amples informations, veuillez consulter [Surveillez votre WorkSpaces utilisation d'Amazon EventBridge](#).

CloudTrail journaux

AWS CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans WorkSpaces. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite WorkSpaces, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires. Pour plus d'informations, consultez la section [Journalisation des appels d' WorkSpacesAPI en utilisant CloudTrail](#). AWS CloudTrail enregistre les événements de connexion réussis et infructueux pour les utilisateurs de cartes à puce. Pour de plus amples informations, veuillez consulter [Comprendre les événements de AWS connexion pour les utilisateurs de cartes à puce](#).

CloudWatch Moniteur Internet

Amazon CloudWatch Internet Monitor fournit une visibilité sur l'impact des problèmes Internet sur les performances et la disponibilité entre vos applications hébergées sur AWS et vos utilisateurs finaux. Vous pouvez également utiliser CloudWatch Internet Monitor pour :

- Créez des moniteurs pour un ou plusieurs Workspace annuaires.
- surveiller les performances Internet ;
- Recevez des alarmes en cas de problème entre le réseau urbain de vos utilisateurs finaux, notamment son emplacement et son ASN, qui est généralement le fournisseur de services Internet (ISP), et leurs régions. Workspace

Internet Monitor utilise les données de connectivité recueillies à partir AWS de son empreinte réseau mondiale pour calculer une base de référence en matière de performances et de disponibilité pour le trafic connecté à Internet. Il est actuellement impossible de fournir des performances Internet à un utilisateur final individuel via Moniteur Internet, mais cela est possible au niveau de la ville et du FSI.

Journaux d'accès Amazon S3

Si vos utilisateurs possèdent des données de paramètres d'application ou de dossiers de base stockées dans des compartiments Amazon S3, pensez à consulter les journaux d'accès au serveur Amazon S3 pour surveiller les accès. Ces journaux contiennent des enregistrements détaillés sur les demandes envoyées à un compartiment. Les journaux d'accès au serveur sont utiles pour de nombreuses applications. Par exemple, les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Pour plus d'informations, consultez [Journalisation des accès au serveur Amazon S3](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

Surveillez votre WorkSpaces santé à l'aide du tableau de bord CloudWatch automatique

Vous pouvez effectuer une surveillance WorkSpaces à l'aide d'un tableau de bord CloudWatch automatique, qui collecte les données brutes et les traite en indicateurs lisibles en temps quasi réel. Les statistiques sont conservées pendant 15 mois afin d'accéder aux informations historiques et de surveiller les performances de votre application ou service Web. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le [guide de CloudWatch l'utilisateur Amazon](#).

Le CloudWatch tableau de bord est automatiquement créé lorsque vous utilisez votre AWS compte pour configurer votre WorkSpaces. Le tableau de bord vous permet de surveiller vos WorkSpaces indicateurs, tels que leur santé et leurs performances, dans toutes les régions. Vous pouvez également utiliser le tableau de bord aux fins suivantes :

- Identifiez les Workspace instances défectueuses.
- Identifiez les modes d'exécution, les protocoles et les systèmes d'exploitation présentant des Workspace instances défectueuses.
- Visualisez l'utilisation des ressources critiques au fil du temps.
- Identifiez les anomalies pour faciliter le dépannage.

WorkSpaces CloudWatch les tableaux de bord automatiques sont disponibles dans toutes les régions AWS commerciales.

Pour utiliser le tableau de bord WorkSpaces CloudWatch automatique

1. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le panneau de navigation, choisissez Dashboards (Tableaux de bord).
3. Choisissez l'onglet Tableaux de bord automatiques.
4. Sélectionnez WorkSpaces.

Comprendre votre tableau WorkSpaces CloudWatch de bord automatique

Le tableau de bord CloudWatch automatique vous permet de mieux comprendre les performances de vos WorkSpaces ressources et d'identifier les problèmes de performance.

Moniteur avec tableau CloudWatch de bord automatique

Le tableau de bord comprend les fonctionnalités suivantes :

1. Affichez les données historiques à l'aide des commandes de plage d'heures et de dates.
2. Ajoutez une vue de tableau de bord CloudWatch personnalisée aux tableaux de bord personnalisés.
3. Surveillez l'état général et l'état d'utilisation de votre WorkSpaces ordinateur en procédant comme suit :
 - a. Affichez le nombre total d'instances provisionnées WorkSpaces, le nombre d'utilisateurs connectés, le nombre d' Workspaceinstances défectueuses et saines.
 - b. Affichez les anomalies WorkSpaces et leurs différentes variables, telles que le protocole et le mode de calcul.
 - c. Passez le curseur sur le graphique linéaire pour afficher le nombre d' Workspace instances saines ou non fonctionnelles pour un protocole et un mode d'exécution spécifiques sur une période donnée.
 - d. Choisissez le menu représentant des points de suspension, puis sélectionnez Afficher dans les mesures pour afficher les mesures sur un graphique à échelle de temps.
4. Consultez vos statistiques de connexion et leurs différentes variables, telles que le nombre de tentatives de connexion, les connexions réussies et les connexions échouées dans votre WorkSpaces environnement à un moment donné.
5. Consultez les InSession latences qui ont un impact sur l'expérience de vos utilisateurs, telles que le temps d'aller-retour (RTT), afin de déterminer l'état de la connexion et les pertes de paquets afin de surveiller l'état du réseau.
6. Consultez les performances de l'hôte et l'utilisation des ressources pour identifier et résoudre les problèmes de performances potentiels.

Surveillez vos CloudWatch indicateurs WorkSpaces d'utilisation

WorkSpaces et Amazon CloudWatch sont intégrés, ce qui vous permet de recueillir et d'analyser les indicateurs de performance. Vous pouvez surveiller ces métriques à l'aide de la CloudWatch console, de l'interface de ligne de CloudWatch commande ou de manière programmatique à l'aide de l' CloudWatch API. CloudWatch vous permet également de définir des alarmes lorsque vous atteignez un seuil spécifié pour une métrique.

Pour plus d'informations sur l'utilisation CloudWatch et les alarmes, consultez le [guide de CloudWatch l'utilisateur Amazon](#).

Prérequis

Pour obtenir CloudWatch des métriques, activez l'accès sur le port 443 du AMAZON sous-ensemble de la us-east-1 région. Pour de plus amples informations, veuillez consulter [Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal](#).

Table des matières

- [WorkSpaces métriques](#)
- [Dimensions pour les WorkSpaces métriques](#)
- [Exemple de surveillance](#)

WorkSpaces métriques

L'espace de noms AWS/WorkSpaces inclut les métriques suivantes.

Métrique	Description	Dimensions	Statistiques	Unités
Available ¹	Le nombre d'entre WorkSpaces eux a renvoyé à un état sain.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre
Unhealthy ¹	Le numéro WorkSpaces renvoyait à un état insalubre.	DirectoryId WorkspaceId RunningMode	Moyenne, Somme, Maximum, Minimum et	Nombre

Métrique	Description	Dimensions	Statistiques	Unités
		Protocol ComputeType BundleId UserName ComputerName	Exemples de données	
ConnectionAttempt ²	Nombre de tentatives de connexion.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

Métrique	Description	Dimensions	Statistiques	Unités
ConnectionSuccess ²	Nombre de connexions ayant réussi.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre
ConnectionFailure ²	Nombre de connexions ayant échoué.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

Métrique	Description	Dimensions	Statistiques	Unités
SessionLaunchTime ^{2, 6}	Le temps nécessaire pour démarrer une WorkSpaces session.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Seconde (temps)
InSessionLatency ^{2, 6}	Le temps de trajet aller-retour entre le WorkSpaces client et le WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Milliseconde (temps)

Métrique	Description	Dimensions	Statistiques	Unités
SessionDisconnect ^{2, 6}	Nombre de connexions qui ont été fermées, y compris les connexions initiées par l'utilisateur et celles ayant échoué.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre
UserConnected ³	Le nombre de WorkSpaces auxquels un utilisateur est connecté.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

Métrique	Description	Dimensions	Statistiques	Unités
Stopped	Le nombre d'WorkSpaces entre eux sont arrêtés.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre
Maintenance ⁴	Le nombre d'entre WorkSpaces eux sont en cours de maintenance.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

Métrique	Description	Dimensions	Statistiques	Unités
TrustedDeviceValidationAttempt ^{5, 6}	Nombre de tentatives de validation des signatures d'authentification de l'appareil.	DirectoryId	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre
TrustedDeviceValidationSuccess ^{5, 6}	Nombre de validations de signature d'authentification de l'appareil réussies.	DirectoryId	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre
TrustedDeviceValidationFailure ^{5, 6}	Nombre de validations de signature d'authentification de l'appareil ayant échoué.	DirectoryId	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre
TrustedDeviceCertificatesBeforeExpiration ⁶	Jours restants avant expiration du certificat racine associé à l'annuaire.	CertificateId	Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

Métrique	Description	Dimensions	Statistiques	Unités
CPUUsage	Pourcentage des ressources du processeur utilisées.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, maximale, minimale	Pourcentage
MemoryUsage	Pourcentage de mémoire de la machine utilisé.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, maximale, minimale	Pourcentage

Métrique	Description	Dimensions	Statistiques	Unités
RootVolumeDiskUsage	Pourcentage du volume du disque racine utilisé.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, maximale, minimale	Pourcentage
UserVolumeDiskUsage	Pourcentage du volume de disque utilisateur utilisé.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, maximale, minimale	Pourcentage

Métrique	Description	Dimensions	Statistiques	Unités
UDPPacketLossRate ⁷	Pourcentage de paquets abandonnés entre le client et la passerelle.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, maximale, minimale, échantillons de données	Pourcentage
UpTime	Le temps écoulé depuis le dernier redémarrage d'un WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Moyenne, maximale, minimale, échantillons de données	Secondes

⁷ envoie WorkSpaces régulièrement des demandes de statut à un WorkSpace. A WorkSpace est marqué Available lorsqu'il répond à ces demandes et Unhealthy lorsqu'il ne répond pas à ces demandes. Ces indicateurs sont disponibles au WorkSpace niveau de granularité par niveau et sont également agrégés pour tous les membres WorkSpaces d'une organisation.

² WorkSpaces enregistre des mesures sur les connexions effectuées avec chacun d'entre eux WorkSpace. Ces métriques sont émises une fois qu'un utilisateur s'est authentifié avec succès via le WorkSpaces client et que le client lance ensuite une session. Les métriques sont disponibles au WorkSpace niveau de granularité par niveau et sont également agrégées pour tous WorkSpaces dans un annuaire.

³ envoie WorkSpaces régulièrement des demandes d'état de connexion à un WorkSpace. Les utilisateurs sont considérés comme connectés lorsqu'ils utilisent activement leurs sessions. Cette métrique est disponible au WorkSpace niveau de granularité par niveau et est également agrégée pour tous les membres WorkSpaces d'une organisation.

⁴ Cette métrique s'applique aux WorkSpaces personnes configurées avec un mode d' AutoStop exécution. Si la maintenance est activée pour votre WorkSpaces, cette métrique indique le nombre de personnes WorkSpaces actuellement en cours de maintenance. Cette métrique est disponible au WorkSpace niveau de granularité, qui décrit à quel moment une maintenance WorkSpace a été effectuée et à quel moment elle a été supprimée.

⁵ Si la fonctionnalité des appareils sécurisés est activée pour le répertoire, Amazon WorkSpaces utilise une authentification basée sur des certificats pour déterminer si un appareil est fiable. Lorsque les utilisateurs tentent d'accéder à leur WorkSpaces, ces mesures sont émises pour indiquer que l'authentification d'un appareil fiable a réussi ou échoué. Ces métriques sont disponibles au niveau de granularité par répertoire, et uniquement pour les applications clientes Amazon WorkSpaces Windows et macOS.

⁶ Non disponible sur WorkSpaces Web Access.

⁷ Cette métrique mesure la perte moyenne de paquets.

- Sur PCo IP : mesure la perte moyenne de paquets UDP entre le client et la passerelle.

 Note

Ceci est mesuré à la passerelle.

- Sur DCV : mesure la perte de paquets UDP entre la passerelle et le client.

 Note

Ceci est mesuré à la passerelle.

Dimensions pour les WorkSpaces métriques

Pour filtrer les données de métriques, utilisez les dimensions suivantes.

Dimension	Description
DirectoryId	Filtre les données métriques WorkSpaces dans le répertoire spécifié. La forme de l'ID d'annuaire est d-XXXXXXXXXX .
WorkspaceId	Filtre les données métriques selon les valeurs spécifiées WorkSpace. La forme de l'WorkSpace identifiant est ws-XXXXXXXXXX .
CertificateId	Filtre les données métriques vers le certificat racine spécifié associé à l'annuaire. La forme de l'ID de certificat est wsc-XXXXXXXXXX .
RunningMode	Filtre les données métriques WorkSpaces selon leur mode de fonctionnement. La forme du mode de fonctionnement est AutoStop ou AlwaysOn.
BundleId	Filtre les données métriques WorkSpaces selon le protocole. La forme du bundle est ws-b-XXXXXXXXXX .
ComputeType	Filtre les données métriques WorkSpaces selon le type de calcul.
Protocol	Filtre les données métriques WorkSpaces selon le type de protocole.
UserName	Filtre les données métriques WorkSpaces selon le nom de l'utilisateur.

Dimension	Description
	 Note Ils <code>UserName</code> ne peuvent pas être composés de caractères non ASCII, tels que les suivants : • Lettres accentuées : é, à, ö, ñ, etc. • Alphabets non latins • Symboles : ©, #, ®, #, €, £, µ, ¥, etc.
ComputerName	Filtre les données métriques selon les valeurs spécifiées WorkSpace. Voir les différents formats pour le nom de WorkSpaces l'ordinateur .

Exemple de surveillance

L'exemple suivant montre comment vous pouvez utiliser le AWS CLI pour répondre à une CloudWatch alarme et déterminer les utilisateurs d'un répertoire qui WorkSpaces ont connu des échecs de connexion.

Pour répondre à une CloudWatch alarme

1. Déterminez l'annuaire auquel l'alarme s'applique avec la commande [describe-alarms](#).

```
aws cloudwatch describe-alarms --state-value "ALARM"
```

```
{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ]
    }
  ],
}
```

```

    ...
  }
]
}

```

2. Obtenez la liste des WorkSpaces dans le répertoire spécifié à l'aide de la commande [describe-workspaces](#).

```

aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}

```

3. Obtenez les CloudWatch métriques pour chacun d'entre eux WorkSpace dans le répertoire à l'aide de la [get-metric-statistics](#) commande.

```

aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{

```

```
"Datapoints" : [  
  {  
    "Timestamp": "2015-04-27T00:18:00Z",  
    "Sum": 1.0,  
    "Unit": "Count"  
  },  
  {  
    "Timestamp": "2014-04-27T01:18:00Z",  
    "Sum": 0.0,  
    "Unit": "Count"  
  }  
],  
"Label" : "ConnectionFailure"  
}
```

Surveillez votre WorkSpaces utilisation d'Amazon EventBridge

Vous pouvez utiliser les événements d'Amazon WorkSpaces pour consulter, rechercher, télécharger, archiver, analyser et répondre aux connexions réussies à votre WorkSpaces. Par exemple, vous pouvez utiliser des événements aux fins suivantes :

- Stockez ou archivez les événements de WorkSpaces connexion sous forme de journaux pour référence future, analysez les journaux pour rechercher des modèles et prenez des mesures en fonction de ces modèles.
- Utilisez l'adresse IP WAN pour déterminer d'où les utilisateurs sont connectés, puis utilisez des politiques pour autoriser les utilisateurs à accéder uniquement aux fichiers ou aux données WorkSpaces qui répondent aux critères d'accès définis dans le type d'événement de WorkSpaces Access.
- Analysez les données de connexion et effectuez des actions automatisées à l'aide de AWS Lambda.
- Utilisez les contrôles de stratégie pour bloquer l'accès aux fichiers et applications à partir d'adresses IP non autorisées.
- Découvrez la version du WorkSpaces client à laquelle vous vous connectez WorkSpaces.

Amazon WorkSpaces diffuse ces événements dans la mesure du possible. Les événements sont diffusés EventBridge en temps quasi réel. Avec EventBridge, vous pouvez créer des règles qui déclenchent des actions programmatiques en réponse à un événement. Par exemple, vous pouvez

configurer une règle qui invoque une rubrique SNS pour envoyer une notification par e-mail ou qui invoque une fonction Lambda pour effectuer une action. Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

WorkSpaces Accédez aux événements

WorkSpaces les applications clientes envoient WorkSpaces Access des événements lorsqu'un utilisateur se connecte avec succès à un WorkSpace. Tous les WorkSpaces clients envoient ces événements.

Les événements émis pour WorkSpaces l'utilisation de DCV nécessitent la version 4.0.1 ou ultérieure de l'application WorkSpaces cliente.

Les événements sont représentés sous la forme d'objets JSON. Voici un exemple de données pour un événement WorkSpaces Access.

```
{
  "version": "0",
  "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
  "detail-type": "WorkSpaces Access",
  "source": "aws.workspaces",
  "account": "123456789012",
  "time": "2023-04-05T16:13:59Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "clientIpAddress": "192.0.2.3",
    "actionType": "successfulLogin",
    "workspacesClientProductName": "WorkSpacesWebClient",
    "loginTime": "2023-04-05T16:13:37.603Z",
    "clientPlatform": "Windows",
    "directoryId": "domain/d-123456789",
    "clientVersion": "5.7.0.3472",
    "workspaceId": "ws-xyskdga"
  }
}
```

Champs spécifiques aux événements

`clientIpAddress`

Adresse IP de réseau étendu (WAN) de l'application client. Pour les clients PCo IP zéro, il s'agit de l'adresse IP du client d'authentification Teradici.

`actionType`

Cette valeur est toujours `successfulLogin`.

`workspacesClientProductName`

Les valeurs suivantes sont sensibles à la casse.

- `WorkSpaces Desktop client` : clients Windows, macOS et Linux
- `Amazon WorkSpaces Mobile client` : client iOS
- `WorkSpaces Mobile Client` : clients Android
- `WorkSpaces Chrome Client` : client Chromebook
- `WorkSpacesWebClient` : client Web Access
- `AmazonWorkSpacesThinClient`— Appareil Amazon WorkSpaces Thin Client
- `Teradici PCoIP Zero Client`, `Teradici PCoIP Desktop Client`, or `Dell Wyse PCoIP Client` : client plume

`loginTime`

Heure à laquelle l'utilisateur s'est connecté au WorkSpace.

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

directoryId

Identifiant du répertoire pour WorkSpace. L'identifiant du répertoire doit être précédé de domain/. Par exemple, "domain/d-123456789".

clientVersion

Version du client à laquelle se connecter WorkSpaces.

workspaceId

L'identifiant de l' WorkSpace.

Création d'une règle pour gérer les WorkSpaces événements

Utilisez la procédure suivante pour créer une règle permettant de gérer les WorkSpaces événements.

Prérequis

Pour recevoir des notifications par e-mail, créez une rubrique Amazon Simple Notification Service.

1. [Ouvrez la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
2. Dans le volet de navigation, choisissez Rubriques.
3. Choisissez Créer une rubrique.
4. Pour Type, choisissez Standard.
5. Pour Nom, saisissez un nom pour votre rubrique.
6. Choisissez Créer une rubrique.
7. Choisissez Créer un abonnement.
8. Pour Protocole, choisissez E-mail.
9. Pour Point de terminaison, saisissez l'adresse e-mail qui reçoit les notifications.
10. Choisissez Créer un abonnement.
11. Vous recevrez un e-mail avec l'objet suivant : AWS Notification - Subscription Confirmation. Suivez les instructions pour confirmer votre abonnement.

Pour créer une règle de gestion des WorkSpaces événements

1. Ouvrez la EventBridge console Amazon à l'adresse <https://console.aws.amazon.com/events/>.
2. Choisissez Créer une règle.

3. Pour Nom, saisissez un nom pour votre règle.
4. Pour Type de règle, choisissez Règle avec un modèle d'événement.
5. Choisissez Suivant.
6. Pour Event pattern (Modèle d'événement), procédez comme suit :
 - a. Pour Event source (Source d'événement), choisissez Services AWS.
 - b. Pour Service AWS, choisissez WorkSpaces.
 - c. Pour Type d'événement, choisissez WorkSpacesAccess.
 - d. Par défaut, nous envoyons des notifications pour chaque événement. Si vous le souhaitez, vous pouvez créer un modèle qui filtre les événements pour des clients ou des espaces de travail spécifiques.
7. Choisissez Suivant.
8. Spécifiez une cible comme suit :
 - a. Pour Target types (Types de cibles), choisissez Service AWS.
 - b. Pour Sélectionner une cible, choisissez Rubrique SNS.
 - c. Pour Rubrique, choisissez la rubriques SNS que vous avez créée pour les notifications.
9. Choisissez Suivant.
10. (Facultatif) Ajoutez des identifications à votre règle.
11. Choisissez Suivant.
12. Choisissez Créer une règle.

Comprendre les événements de AWS connexion pour les utilisateurs de cartes à puce

AWS CloudTrail enregistre les événements de connexion réussis et infructueux pour les utilisateurs de cartes à puce. Cela inclut les événements de connexion qui sont capturés chaque fois qu'un utilisateur est invité à résoudre un problème ou un facteur d'identification spécifique, ainsi que le statut de cette demande de vérification des informations d'identification en particulier. Un utilisateur n'est connecté qu'après avoir répondu à toutes les demandes d'informations d'identification requises, ce qui entraîne l'enregistrement d'un `UserAuthentication` événement.

Le tableau suivant présente les noms de chacun des CloudTrail événements de connexion et leurs objectifs.

Nom de l'événement	But de l'événement
<code>CredentialChallenge</code>	Indique que la AWS connexion a demandé à l'utilisateur de résoudre un problème d'identification spécifique et précise les <code>CredentialType</code> informations requises (par exemple, SMARTCARD).
<code>CredentialVerification</code>	Indique que l'utilisateur a tenté de répondre à une demande <code>CredentialChallenge</code> spécifique, et précise si ces informations d'identification lui ont permis de se connecter ou non.
<code>UserAuthentication</code>	Indique que toutes les exigences d'authentification demandées à l'utilisateur ont été satisfaites, et qu'il a réussi à se connecter. Quand les utilisateurs ne parviennent pas à répondre aux demandes d'informations d'identification, aucun événement <code>UserAuthentication</code> n'est enregistré.

Le tableau suivant présente d'autres champs de données d'événements utiles contenus dans des CloudTrail événements de connexion spécifiques.

Nom de l'événement	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
<code>AuthWorkflowID</code>	Corrèle tous les événements émis sur l'ensemble d'une séquence de connexion. Pour chaque connexion utilisateur, plusieurs événements peuvent être émis lors d'une connexion AWS.	<code>CredentialChallenge</code> , <code>CredentialVerification</code> , <code>UserAuthentication</code>	« AuthWorkflow Identifiant » : « 9de74b32-8362-4a01-a524-de21df59fd83 »
<code>CredentialType</code>	Indique que l'utilisateur a tenté de répondre à une demande <code>CredentialChallenge</code>	<code>CredentialChallenge</code> , <code>CredentialVerification</code>	<code>CredentialType</code> : « SMARTCARD » (valeurs possibles aujourd'hui : SMARTCARD)

Nom de l'événement	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
	1Challenge spécifique, et précise si ces informations d'identification lui ont permis de se connecter ou non.	UserAuthentication	
LoginTo	Indique que toutes les exigences d'authentification demandées à l'utilisateur ont été satisfaites, et qu'il a réussi à se connecter. Quand les utilisateurs ne parviennent pas à répondre aux demandes d'informations d'identification, aucun événement UserAuthentication n'est enregistré.	UserAuthentication	« LoginTo « : " https://skylight.local »

Exemples d'événements pour les AWS scénarios de connexion

Les exemples suivants montrent la séquence d' CloudTrail événements attendue pour différents scénarios de connexion.

Table des matières

- [Connexion réussie lors d'une authentification par carte à puce](#)
- [Échec de connexion lors d'une authentification par carte à puce](#)

Connexion réussie lors d'une authentification par carte à puce

La séquence d'événements suivante présente un exemple de connexion par carte à puce réussie.

CredentialChallenge

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "509318101470",
    "arn": "",
    "accountId": "509318101470",
    "accessKeyId": ""
  },
  "eventTime": "2021-07-30T17:23:29Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
    "CredentialType": "SMARTCARD"
  },
  "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
  "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "509318101470",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}
```

Réussite CredentialVerification

```
{
  "eventVersion": "1.08",
```

```

    "userIdentity": {
      "type": "Unknown",
      "principalId": "509318101470",
      "arn": "",
      "accountId": "509318101470",
      "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
      "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
      "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
      CredentialVerification: "Success"
    }
  }
}

```

Réussite UserAuthentication

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "509318101470",
    "arn": "",
    "accountId": "509318101470",

```

```

    "accessKeyId": "",
  },
  "eventTime": "2021-07-30T17:23:39Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
    "LoginTo": "https://skylight.local",
    "CredentialType": "SMARTCARD"
  },
  "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
  "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "509318101470",
  "serviceEventDetails": {
    UserAuthentication: "Success"
  }
}

```

Échec de connexion lors d'une authentification par carte à puce

La séquence d'événements suivante présente un exemple d'échec de connexion par carte à puce.

CredentialChallenge

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "509318101470",
    "arn": "",
    "accountId": "509318101470",

```

```

    "accessKeyId": "",
  },
  "eventTime": "2021-07-30T17:23:06Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
    "CredentialType": "SMARTCARD"
  },
  "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
  "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "509318101470",
  "serviceEventDetails": {
    CredentialChallenge: "Success"
  }
}

```

Échec CredentialVerification

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "509318101470",
    "arn": "",
    "accountId": "509318101470",
    "accessKeyId": ""
  },
  "eventTime": "2021-07-30T17:23:13Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",

```

```
{
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
    "CredentialType": "SMARTCARD"
  },
  "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
  "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "509318101470",
  "serviceEventDetails": {
    "CredentialVerification": "Failure"
  }
}
```

Créez des CloudWatch tableaux de bord personnalisés à l'aide de modèles CloudFormation

AWS fournit des CloudFormation modèles que vous pouvez utiliser pour créer des CloudWatch tableaux de bord personnalisés. WorkSpaces Choisissez parmi les options de CloudFormation modèle suivantes pour créer des tableaux de bord personnalisés pour vous WorkSpaces dans la CloudFormation console.

Considérations à prendre en compte avant de commencer

Tenez compte des points suivants avant de commencer à utiliser des CloudWatch tableaux de bord personnalisés :

- Créez vos tableaux de bord de la même manière Région AWS que le déploiement que WorkSpaces vous souhaitez surveiller.
- Vous pouvez également créer des tableaux de bord personnalisés à l'aide de la CloudWatch console.

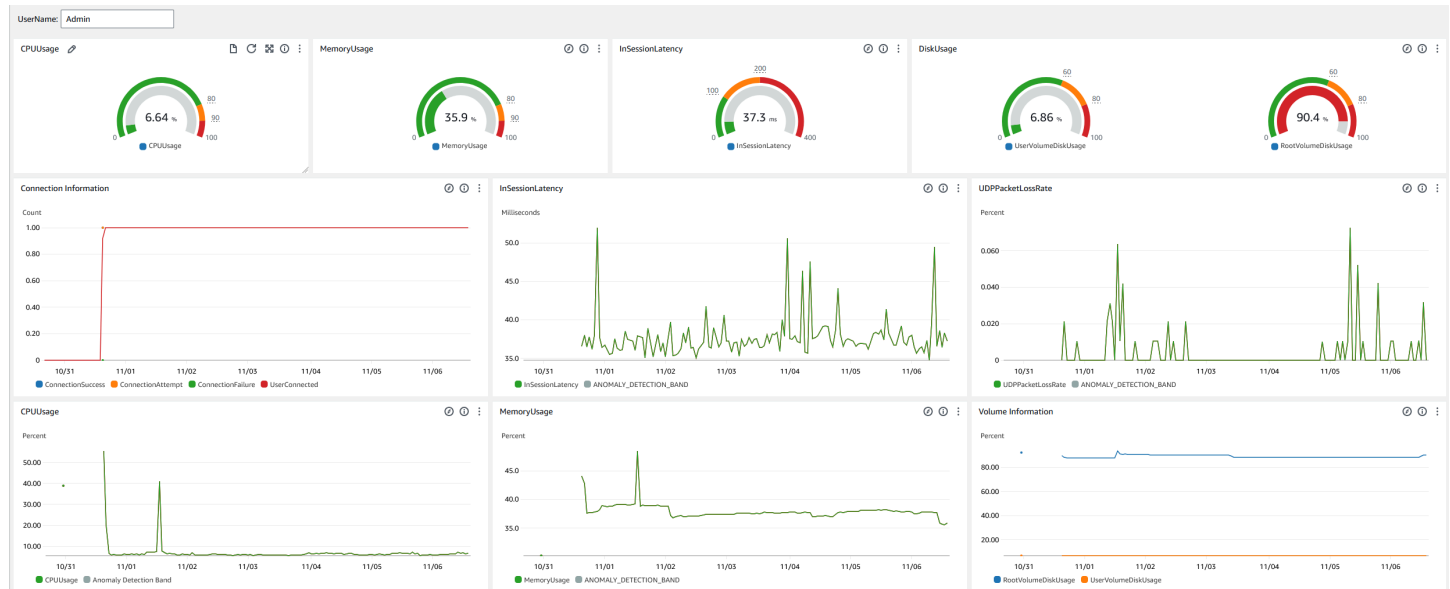
- Un coût peut être associé aux CloudWatch tableaux de bord personnalisés. Pour plus d'informations sur les tarifs, consultez [Amazon CloudWatch Pricing](#)

Tableau de bord du service d'assistance

Le tableau de bord du service d'assistance affiche les statistiques suivantes pour un sujet spécifique WorkSpace :

- Utilisation de l'UC
- Utilisation de la mémoire
- Latence en cours de session
- Volume racine
- Volume d'utilisateurs
- Perte de paquets
- Utilisation du disque

Voici un exemple du tableau de bord du service d'assistance.



Procédez comme suit pour créer un tableau de bord personnalisé lors de CloudWatch l'utilisation CloudFormation.

1. [Ouvrez la page Create Stack dans la CloudFormation console](#). Ce lien ouvre la page contenant l'emplacement du compartiment Amazon S3 du modèle de tableau de CloudWatch bord personnalisé du service d'assistance prérempli.
2. Passez en revue les sélections par défaut sur la page Create Stack. Notez que le champ URL Amazon S3 est prérempli avec l'emplacement du compartiment Amazon S3 du CloudFormation modèle.
3. Choisissez Suivant.
4. Dans la zone de texte Nom de la pile, entrez le nom de la pile.

Ce nom est un identifiant qui vous aidera à retrouver une pile particulière dans une liste de piles. Un nom de pile ne peut contenir que des caractères alphanumériques (sensibles à la casse) et des traits d'union. Il doit commencer par un caractère alphabétique et ne doit pas dépasser 128 caractères.

5. Dans la zone de DashboardNametexte, entrez le nom que vous souhaitez attribuer à votre tableau de bord.

Le nom du tableau de bord ne peut contenir que des caractères alphanumériques, un tiret (-) et un trait de soulignement (_).

6. Choisissez Suivant.
7. Passez en revue les sélections par défaut sur la page Configurer les options de pile, puis choisissez Next.
8. Faites défiler la page vers le bas jusqu'à Transformations susceptibles de nécessiter des fonctionnalités d'accès et cochez les cases de confirmation. Choisissez ensuite Soumettre pour créer la pile et le tableau de CloudWatch bord personnalisé.

 Important

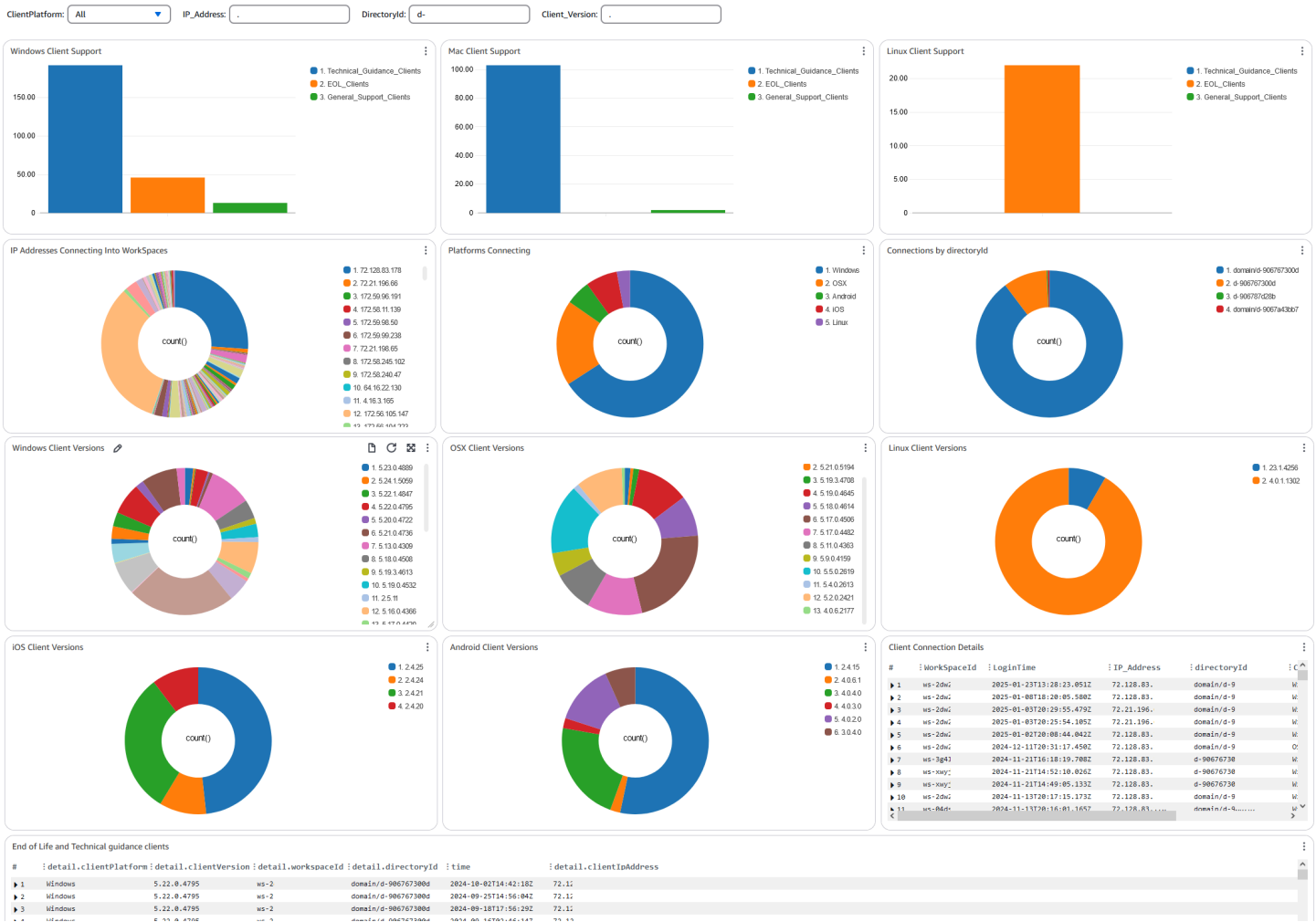
Un coût peut être associé aux CloudWatch tableaux de bord personnalisés. Pour plus d'informations sur les tarifs, consultez [Amazon CloudWatch Pricing](#)

9. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
10. Dans la barre de navigation de gauche, sélectionnez Tableaux de bord.
11. Sous Tableaux de bord personnalisés, choisissez le tableau de bord portant le nom du tableau de bord que vous avez saisi plus tôt dans cette procédure.
12. À l'aide du modèle d'exemple du centre UserName d'assistance, entrez le Workspace pour surveiller ses données.

Tableau de bord Connection Insights

Le tableau de bord Connection Insights affiche les versions des clients, les plateformes et les adresses IP connectées à votre WorkSpaces. Ce tableau de bord vous permet de mieux comprendre comment vos utilisateurs se connectent afin de pouvoir les informer de manière proactive en utilisant un client obsolète. Les variables dynamiques vous permettent de surveiller les détails des adresses IP ou des annuaires spécifiques.

Voici un exemple du tableau de bord Connection Insights.



- Procédez comme suit pour créer un tableau de bord personnalisé lors de CloudWatch l'utilisation CloudFormation.
- [Ouvrez la page Create Stack dans la CloudFormation console.](#) Ce lien ouvre la page contenant l'emplacement du compartiment Amazon S3 du modèle de tableau de bord CloudWatch bord personnalisé Connection Insights prérempli.

2. Passez en revue les sélections par défaut sur la page Create Stack. Notez que le champ URL Amazon S3 est prérempli avec l'emplacement du compartiment Amazon S3 du CloudFormation modèle.
3. Choisissez Suivant.
4. Dans la zone de texte Nom de la pile, entrez le nom de la pile.

Ce nom est un identifiant qui vous aidera à retrouver une pile particulière dans une liste de piles. Un nom de pile ne peut contenir que des caractères alphanumériques (sensibles à la casse) et des traits d'union. Il doit commencer par un caractère alphabétique et ne doit pas dépasser 128 caractères.

5. Dans la zone de DashboardNametexte, entrez le nom que vous souhaitez attribuer à votre tableau de bord. Entrez d'autres informations pertinentes sur la configuration du groupe d'CloudWatch accès.

Le nom du tableau de bord ne peut contenir que des caractères alphanumériques, un tiret (-) et un trait de soulignement (_).

6. Sous LogRetention, entrez le nombre de jours pendant lesquels vous souhaitez conserver votre LogGroup nom.
7. Sous SetupEventBridge, indiquez si vous souhaitez déployer la EventBridge règle pour obtenir les journaux WorkSpaces d'accès.
8. Sous WorkspaceAccessLogsName, entrez le nom du CloudWatch LogGroup titulaire des journaux WorkSpaces d'accès.
9. Choisissez Suivant.
10. Passez en revue les sélections par défaut sur la page Configurer les options de pile, puis choisissez Next.
11. Faites défiler la page vers le bas jusqu'à Transformations susceptibles de nécessiter des fonctionnalités d'accès et cochez les cases de confirmation. Choisissez ensuite Soumettre pour créer la pile et le tableau de CloudWatch bord personnalisé.

 Important

Un coût peut être associé aux CloudWatch tableaux de bord personnalisés. Pour plus d'informations sur les tarifs, consultez [Amazon CloudWatch Pricing](https://aws.amazon.com/fr/cloudwatch/pricing/)

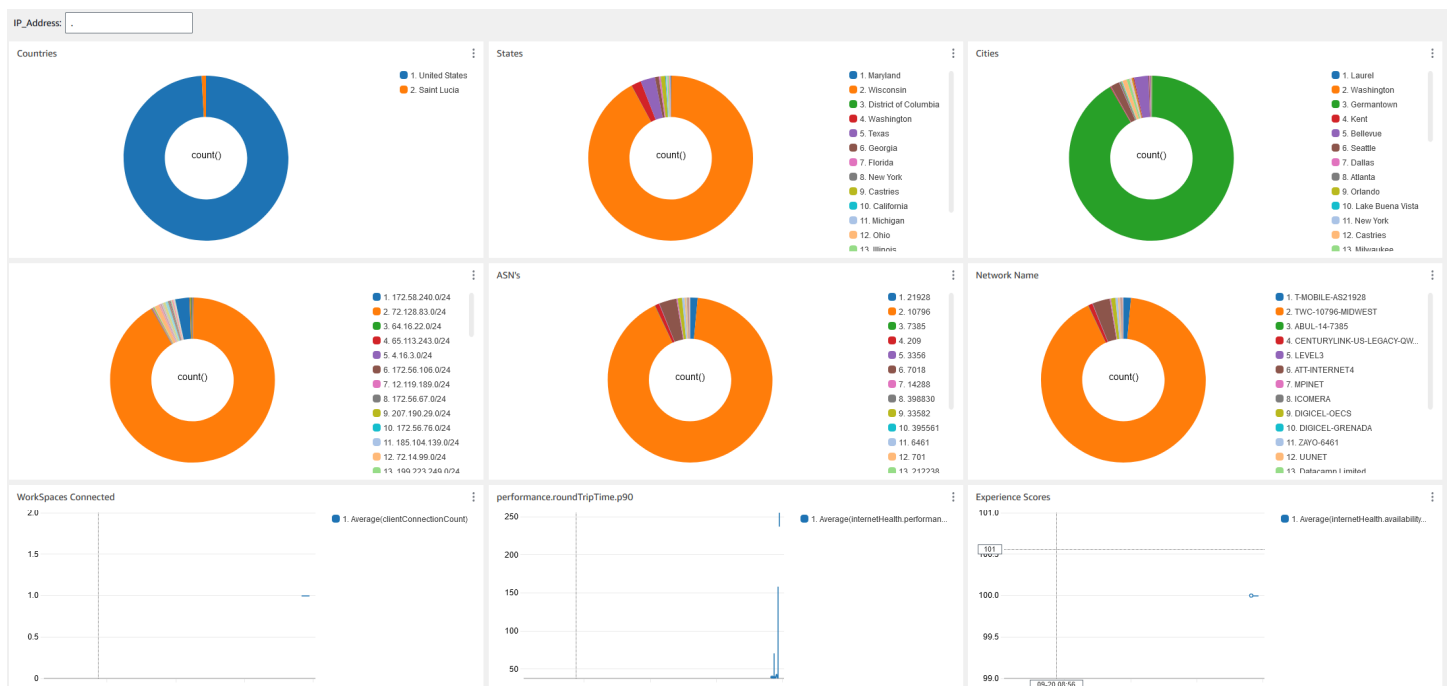
12. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
13. Dans la barre de navigation de gauche, sélectionnez Tableaux de bord.

14. Sous Tableaux de bord personnalisés, choisissez le tableau de bord portant le nom du tableau de bord que vous avez saisi plus tôt dans cette procédure.
15. Vous pouvez désormais surveiller vos données à l'aide WorkSpace du tableau de bord Connection Insights.

Tableau de bord de surveillance Internet

Le tableau de bord de surveillance Internet affiche des informations détaillées sur le fournisseur de services Internet (ISP) que vos utilisateurs utilisent pour rejoindre leurs WorkSpaces instances. Il fournit des détails sur la ville, l'État, l'ASN, le nom du réseau, le nombre de personnes connectées WorkSpaces, les performances et les scores d'expérience. Vous pouvez également utiliser des adresses IP spécifiques pour obtenir les informations de vos utilisateurs qui se connectent à partir d'un emplacement spécifique. Déployez un moniteur CloudWatch Internet pour obtenir des informations sur les données des fournisseurs de services Internet. Pour plus d'informations, consultez la section [Utilisation d'Amazon CloudWatch Internet Monitor](#).

Voici un exemple du tableau de bord de surveillance Internet.



Pour créer un tableau de bord personnalisé en CloudWatch utilisant CloudFormation

Note

Avant de créer un tableau de bord personnalisé, assurez-vous de créer un moniteur Internet avec CloudWatch Internet Monitor. Pour plus d'informations, consultez [Création d'un moniteur dans Amazon CloudWatch Internet Monitor à l'aide de la console](#)

1. [Ouvrez la page Create Stack dans la CloudFormation console](#). Ce lien ouvre la page avec l'emplacement du compartiment Amazon S3 du modèle de tableau de CloudWatch bord personnalisé de surveillance Internet prérempli.
2. Passez en revue les sélections par défaut sur la page Create Stack. Notez que le champ URL Amazon S3 est prérempli avec l'emplacement du compartiment Amazon S3 du CloudFormation modèle.
3. Choisissez Suivant.
4. Dans la zone de texte Nom de la pile, entrez le nom de la pile.

Ce nom est un identifiant qui vous aidera à retrouver une pile particulière dans une liste de piles. Un nom de pile ne peut contenir que des caractères alphanumériques (sensibles à la casse) et des traits d'union. Il doit commencer par un caractère alphabétique et ne doit pas dépasser 128 caractères.

5. Dans la zone de DashboardName texte, entrez le nom que vous souhaitez attribuer à votre tableau de bord. Entrez d'autres informations pertinentes sur la configuration du groupe d'CloudWatch accès.

Le nom du tableau de bord ne peut contenir que des caractères alphanumériques, un tiret (-) et un trait de soulignement (_).

6. Sous ResourcesToMonitor, entrez l'ID du répertoire pour lequel vous avez activé la surveillance Internet.
7. Sous MonitorName, entrez le nom du moniteur Internet que vous souhaitez utiliser.
8. Choisissez Suivant.
9. Passez en revue les sélections par défaut sur la page Configurer les options de pile, puis choisissez Next.

10. Faites défiler la page vers le bas jusqu'à Transformations susceptibles de nécessiter des fonctionnalités d'accès et cochez les cases de confirmation. Choisissez ensuite Soumettre pour créer la pile et le tableau de CloudWatch bord personnalisé.

 Important

Un coût peut être associé aux CloudWatch tableaux de bord personnalisés. Pour plus d'informations sur les tarifs, consultez [Amazon CloudWatch Pricing](https://aws.amazon.com/fr/cloudwatch/pricing/)

11. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
12. Dans la barre de navigation de gauche, sélectionnez Tableaux de bord.
13. Sous Tableaux de bord personnalisés, choisissez le tableau de bord portant le nom du tableau de bord que vous avez saisi plus tôt dans cette procédure.
14. Vous pouvez désormais surveiller vos données à WorkSpace l'aide du tableau de bord de surveillance Internet.

Continuité des activités pour les WorkSpaces particuliers

Amazon WorkSpaces repose sur l'infrastructure AWS mondiale, qui est organisée en AWS régions et en zones de disponibilité. Ces régions et zones de disponibilité assurent la résilience en termes d'isolation physique et de redondance des données. Pour de plus amples informations, veuillez consulter [Résilience chez Amazon WorkSpaces](#).

Amazon propose WorkSpaces également la redirection entre régions, une fonctionnalité qui fonctionne avec les politiques de routage de votre système de noms de domaine (DNS) pour rediriger vos WorkSpaces utilisateurs vers une alternative WorkSpaces lorsque leur principal WorkSpaces n'est pas disponible. Par exemple, en utilisant des politiques de routage de basculement DNS, vous pouvez connecter vos utilisateurs WorkSpaces à la région de basculement que vous avez spécifiée lorsqu'ils ne peuvent pas accéder à leur zone de basculement WorkSpaces dans la région principale.

Vous pouvez utiliser la redirection entre régions pour obtenir une résilience régionale et une haute disponibilité. Vous pouvez également l'utiliser à d'autres fins, telles que la distribution du trafic ou la fourniture d'une alternative WorkSpaces pendant les périodes de maintenance. Si vous utilisez Amazon Route 53 pour votre configuration DNS, vous pouvez tirer parti des contrôles de santé qui surveillent les CloudWatch alarmes Amazon.

Amazon WorkSpaces Multi-Region Resilience fournit une infrastructure de bureau virtuel automatisée et redondante dans une WorkSpace région secondaire et rationalise le processus de redirection des utilisateurs vers la région secondaire lorsque la région principale est inaccessible en raison de pannes.

Vous pouvez utiliser WorkSpaces la résilience multirégionale avec la redirection entre régions pour déployer une infrastructure de bureau virtuel redondante dans une WorkSpace région secondaire et concevoir une stratégie de basculement entre régions en prévision d'événements perturbateurs. Vous pouvez également utiliser cette solution à d'autres fins, telles que la distribution du trafic ou la fourniture d'une alternative WorkSpaces pendant les périodes de maintenance. Si vous utilisez Route 53 pour votre configuration DNS, vous pouvez tirer parti des contrôles de santé qui surveillent les CloudWatch alarmes.

Table des matières

- [Redirection entre régions pour Personal WorkSpaces](#)
- [Résilience multirégionale au service du personnel WorkSpaces](#)

Redirection entre régions pour Personal WorkSpaces

Grâce à la fonctionnalité de redirection entre régions d'Amazon WorkSpaces, vous pouvez utiliser un nom de domaine complet (FQDN) comme code d'enregistrement pour votre. WorkSpaces La redirection entre régions fonctionne avec les politiques de routage de votre système de noms de domaine (DNS) pour rediriger vos WorkSpaces utilisateurs vers une alternative WorkSpaces lorsque leur serveur principal WorkSpaces n'est pas disponible. Par exemple, en utilisant des politiques de routage de basculement DNS, vous pouvez connecter vos utilisateurs WorkSpaces à la AWS région de basculement que vous avez spécifiée lorsqu'ils ne peuvent pas accéder WorkSpaces à leur région principale.

Vous pouvez utiliser la redirection entre régions ainsi que vos stratégies de routage de basculement DNS pour garantir une résilience régionale et une haute disponibilité. Vous pouvez également utiliser cette fonctionnalité à d'autres fins, telles que la distribution du trafic ou la fourniture d'une alternative WorkSpaces pendant les périodes de maintenance. Si vous utilisez Amazon Route 53 pour votre configuration DNS, vous pouvez tirer parti des contrôles de santé qui surveillent les CloudWatch alarmes Amazon.

Pour utiliser cette fonctionnalité, vous devez la configurer WorkSpaces pour vos utilisateurs dans deux AWS régions (ou plus). Vous devez également créer des codes d'enregistrement

spéciaux basés sur un FQDN, appelés alias de connexion. Ces alias de connexion remplacent les codes d'enregistrement spécifiques à la région pour vos utilisateurs. WorkSpaces (Les codes d'enregistrement spécifiques à la région restent valides. Toutefois, pour que la redirection entre régions fonctionne, les utilisateurs doivent plutôt utiliser le FQDN comme code d'enregistrement.)

Pour créer un alias de connexion, vous spécifiez une chaîne de connexion, qui est un FQDN, comme `www.example.com` ou `desktop.example.com`. Afin d'utiliser ce domaine pour la redirection entre régions, vous devez l'enregistrer auprès d'un bureau d'enregistrement de domaines, et configurer le service DNS pour votre domaine.

Après avoir créé vos alias de connexion, vous les associez à vos WorkSpaces annuaires dans différentes régions pour créer des paires d'associations. Chaque paire d'associations comporte une région principale et une ou plusieurs régions de basculement. En cas de panne dans la région principale, vos politiques de routage de basculement DNS redirigent vos WorkSpaces utilisateurs vers celui WorkSpaces que vous avez configuré pour eux dans la région de basculement.

Pour désigner les régions principale et de basculement, vous définissez la priorité de la région (principale ou secondaire) lors de la configuration de vos stratégies de routage de basculement DNS.

Table des matières

- [Conditions préalables](#)
- [Limitations](#)
- [Étape 1 : Créer des alias de connexion](#)
- [\(Facultatif\) Étape 2 : Partager un alias de connexion avec un autre compte](#)
- [Étape 3 : Associer des alias de connexion aux annuaires de chaque région](#)
- [Étape 4 : Configurer le service DNS et définir les stratégies de routage DNS](#)
- [Étape 5 : envoyer la chaîne de connexion à vos WorkSpaces utilisateurs](#)
- [Schéma de l'architecture de redirection entre régions](#)
- [Lancer la redirection entre régions](#)
- [Que se passe-t-il lors de la redirection entre régions](#)
- [Dissociation d'un alias de connexion d'un annuaire](#)
- [Annulation du partage d'un alias de connexion](#)
- [Suppression d'un alias de connexion](#)
- [Autorisations IAM pour associer et dissocier des alias de connexion](#)
- [Considérations de sécurité si vous arrêtez d'utiliser la redirection entre régions](#)

Conditions préalables

- Vous devez posséder et enregistrer le domaine que vous souhaitez utiliser comme FQDN dans les alias de connexion. Si vous n'utilisez pas déjà un autre bureau d'enregistrement de domaines, vous pouvez enregistrer votre domaine avec Amazon Route 53. Pour plus d'informations, consultez [Enregistrement et gestion des domaines à l'aide d'Amazon Route 53](#) dans le Guide du développeur Amazon Route 53.

Important

Vous devez disposer de tous les droits nécessaires pour utiliser tout nom de domaine que vous utilisez conjointement avec Amazon WorkSpaces. Vous admettez que le nom de domaine ne viole ni ne porte atteinte aux droits légaux d'un tiers, ni n'enfreint, de quelque manière que ce soit, la loi applicable.

La longueur totale de votre nom de domaine ne doit pas dépasser 255 caractères. Pour plus d'informations sur les noms de domaine, consultez [Format de nom de domaine DNS](#) dans le Guide du développeur Amazon Route 53.

La redirection entre régions fonctionne à la fois avec les noms de domaine publics et les noms de domaine des zones DNS privées. Si vous utilisez une zone DNS privée, vous devez fournir une connexion de réseau privé virtuel (VPN) au cloud privé virtuel (VPC) qui contient votre WorkSpaces. Si vos WorkSpaces utilisateurs tentent d'utiliser un FQDN privé depuis l'Internet public, les applications WorkSpaces clientes renvoient le message d'erreur suivant :

```
"We're unable to register the WorkSpace because of a DNS server issue.  
Contact your administrator for help."
```

- Vous devez configurer votre service DNS et les stratégies de routage DNS nécessaires. La redirection entre régions fonctionne en conjonction avec vos politiques de routage DNS pour rediriger vos WorkSpaces utilisateurs selon les besoins.
- Dans chaque région principale et de basculement dans laquelle vous souhaitez configurer la redirection entre régions, créez-en WorkSpaces pour vos utilisateurs. Assurez-vous d'utiliser les mêmes noms d'utilisateur dans chaque WorkSpaces répertoire de chaque région. Pour synchroniser les données de vos utilisateurs Active Directory, nous vous recommandons d'utiliser AD Connector pour pointer vers le même Active Directory dans chaque région que vous avez

configurée WorkSpaces pour vos utilisateurs. Pour plus d'informations sur la création WorkSpaces, consultez [Launch WorkSpaces](#).

Important

Si vous configurez votre annuaire Microsoft AD AWS géré pour une réplique multirégionale, seul le répertoire de la région principale peut être enregistré pour être utilisé auprès d'Amazon WorkSpaces. Les tentatives d'enregistrement du répertoire dans une région répliquée pour une utilisation avec Amazon WorkSpaces échoueront. La réplique multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.

Lorsque vous avez terminé de configurer la redirection entre régions, vous devez vous assurer que vos WorkSpaces utilisateurs utilisent le code d'enregistrement basé sur le FQDN au lieu du code d'enregistrement basé sur la région (par exemple, WSpdx+ABC12D) pour leur région principale. Pour ce faire, vous devez leur envoyer un e-mail avec la chaîne de connexion FQDN en suivant la procédure décrite à l'[Étape 5 : envoyer la chaîne de connexion à vos WorkSpaces utilisateurs](#).

Note

Si vous créez vos utilisateurs dans la WorkSpaces console au lieu de les créer dans Active Directory, envoie WorkSpaces automatiquement un e-mail d'invitation à vos utilisateurs avec un code d'enregistrement basé sur la région chaque fois que vous lancez un nouveau. Workspace Cela signifie que lorsque vous configurez la région de basculement WorkSpaces pour vos utilisateurs, ceux-ci recevront également automatiquement des e-mails les concernant. WorkSpaces Vous devrez demander aux utilisateurs d'ignorer les e-mails contenant des codes d'enregistrement basés sur la région.

Limitations

- La redirection entre régions ne vérifie pas automatiquement si les connexions à la région principale ont échoué, puis vous WorkSpaces redirige vers une autre région. En d'autres termes, aucun basculement automatique ne se produit.

Pour implémenter un scénario de basculement automatique, vous devez utiliser un autre mécanisme conjointement avec la redirection entre régions. Par exemple, vous pouvez utiliser

une politique de routage DNS en cas de basculement d'Amazon Route 53 associée à un bilan de santé de Route 53 qui surveille une CloudWatch alarme dans la région principale. Si l' CloudWatch alarme est déclenchée dans la région principale, votre politique de routage de basculement DNS redirige ensuite vos WorkSpaces utilisateurs vers WorkSpaces celle que vous avez configurée pour eux dans la région de basculement.

- La redirection entre régions n'est prise en charge que sur les versions 3.0.9 ou ultérieures des applications WorkSpaces clientes Linux, macOS et Windows. Vous pouvez également utiliser la redirection entre régions avec Web Access.
- La redirection entre régions est disponible dans toutes les [AWS régions où Amazon WorkSpaces est disponible](#), à l'exception de la région AWS GovCloud (US) Region s et de la Chine (Ningxia).

Étape 1 : Créer des alias de connexion

À l'aide du même AWS compte, créez des alias de connexion dans chaque région principale et de reprise où vous souhaitez configurer la redirection entre régions.

Pour créer un alias de connexion

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre WorkSpaces
3. Dans le panneau de navigation, choisissez Paramètres du compte.
4. Sous Redirection entre régions, choisissez Créer un alias de connexion.
5. Pour Chaîne de connexion, entrez un FQDN, tel que `www.example.com` ou `desktop.example.com`. Une chaîne de connexion peut comporter un maximum de 255 caractères. Elle ne peut contenir que des lettres (A-Z et a-z), des chiffres (0-9) et les caractères suivants : .-

Important

Une fois que vous avez créé une chaîne de connexion, celle-ci est toujours associée à votre AWS compte. Vous ne pouvez pas recréer la même chaîne de connexion avec un autre compte, même si vous avez supprimé toutes ses instances du compte d'origine. La chaîne de connexion est globalement réservée à votre compte.

6. (Facultatif) Sous Balises, spécifiez les balises que vous souhaitez associer à votre alias de connexion.
7. Choisissez Créer un alias de connexion.
8. Répétez ces étapes, mais assurez-vous de [Step 2](#) sélectionner la région de basculement correspondant à votre WorkSpaces. Si vous avez plusieurs régions de basculement, répétez ces étapes pour chacune d'entre elles. Veillez à utiliser le même AWS compte pour créer l'alias de connexion dans chaque région de basculement.

(Facultatif) Étape 2 : Partager un alias de connexion avec un autre compte

Vous pouvez partager un alias de connexion avec un autre AWS compte de la même AWS région. Le partage d'un alias de connexion avec un autre compte accorde à ce dernier l'autorisation d'associer ou d'annuler l'association de cet alias à un répertoire appartenant à ce compte dans la même région uniquement. Seul le compte qui possède un alias de connexion peut supprimer cet alias.

Note

Un alias de connexion ne peut être associé qu'à un seul répertoire par AWS région. Si vous partagez un alias de connexion avec un autre AWS compte, un seul compte (votre compte ou le compte partagé) peut associer l'alias à un répertoire dans cette région.

Pour partager un alias de connexion avec un autre AWS compte

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région dans laquelle vous souhaitez partager l'alias de connexion avec un autre AWS compte.
3. Dans le panneau de navigation, choisissez Paramètres du compte.
4. Sous Associations de redirection entre régions, sélectionnez la chaîne de connexion, puis choisissez Actions, Partager/annuler le partage de l'alias de connexion.

Vous pouvez également partager un alias depuis la page des détails de votre alias de connexion. Pour ce faire, sous Compte partagé, choisissez Partager l'alias de connexion.

5. Sur la page Partager ou annuler le partage de l'alias de connexion, sous Partager avec un compte, entrez l'ID du AWS compte avec lequel vous souhaitez partager votre alias de connexion dans cette région. AWS

6. Choisissez Partager.

Étape 3 : Associer des alias de connexion aux annuaires de chaque région

L'association du même alias de connexion à un WorkSpaces répertoire dans deux régions ou plus crée une paire d'associations entre les répertoires. Chaque paire d'associations comporte une région principale et une ou plusieurs régions de basculement.

Par exemple, si votre région principale est la région USA Ouest (Oregon), vous pouvez associer votre WorkSpaces annuaire de la région USA Ouest (Oregon) à un WorkSpaces annuaire de la région USA Est (Virginie du Nord). En cas de panne dans la région principale, la redirection entre régions fonctionne conjointement avec vos politiques de routage en cas de basculement du DNS et avec tous les contrôles de santé que vous avez mis en place dans la région USA Ouest (Oregon) afin de rediriger vos utilisateurs vers la région que WorkSpaces vous avez configurée pour eux dans la région USA Est (Virginie du Nord). Pour plus d'informations sur l'expérience de redirection entre régions, consultez [Que se passe-t-il lors de la redirection entre régions](#).

Note

Si vos WorkSpaces utilisateurs se trouvent à une distance significative de la région de basculement (par exemple, à des milliers de kilomètres), leur WorkSpaces expérience risque d'être moins réactive que d'habitude. Pour vérifier la durée du trajet aller-retour (RTT) vers les différentes AWS régions depuis votre lieu de résidence, utilisez l'Amazon [Connection WorkSpaces Health](#) Check.

Pour associer un alias de connexion à un annuaire

Vous ne pouvez associer un alias de connexion qu'à un seul répertoire par AWS région. Si vous avez partagé un alias de connexion avec un autre AWS compte, un seul compte (votre compte ou le compte partagé) peut associer l'alias à un répertoire dans cette région.

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre WorkSpaces
3. Dans le panneau de navigation, choisissez Paramètres du compte.
4. Sous Associations de redirection entre régions, sélectionnez la chaîne de connexion, puis choisissez Actions, Associer/Dissocier.

Vous pouvez également associer un alias de connexion à un annuaire depuis la page des détails de votre alias de connexion. Pour ce faire, sous Répertoire associé, choisissez Associer le répertoire.

5. Sur la page Associer/dissocier, sous Associer à un répertoire, sélectionnez le répertoire auquel vous souhaitez associer votre alias de connexion dans cette région. AWS

 Note

Si vous configurez votre répertoire Microsoft AD AWS géré pour une réplication multirégionale, seul le répertoire de la région principale peut être utilisé avec Amazon WorkSpaces. Les tentatives d'utilisation de l'annuaire dans une région répliquée avec Amazon WorkSpaces échoueront. La réplication multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.

6. Choisissez Associer.
7. Répétez ces étapes, mais assurez-vous de [Step 2](#) sélectionner la région de basculement correspondant à votre WorkSpaces. Si vous avez plusieurs régions de basculement, répétez ces étapes pour chacune d'entre elles. Assurez-vous d'associer le même alias de connexion à un annuaire dans chaque région de basculement.

Étape 4 : Configurer le service DNS et définir les stratégies de routage DNS

Après avoir créé vos alias de connexion et vos paires d'associations d'alias de connexion, vous pouvez configurer le service DNS pour le domaine que vous avez utilisé dans vos chaînes de connexion. Vous pouvez utiliser n'importe quel fournisseur de services DNS à cette fin. Si vous ne disposez pas déjà d'un fournisseur de services DNS préféré, vous pouvez utiliser Amazon Route 53. Pour plus d'informations, consultez [Configuration d'Amazon Route 53 en tant que service DNS](#) dans le Guide du développeur Amazon Route 53.

Après avoir configuré le service DNS pour votre domaine, vous devez définir les stratégies de routage DNS que vous souhaitez utiliser pour la redirection entre régions. Par exemple, vous pouvez utiliser les bilans de santé d'Amazon Route 53 pour déterminer si vos utilisateurs peuvent se connecter à leur WorkSpaces compte dans une région donnée. Si les utilisateurs ne peuvent pas se connecter, vous pouvez utiliser une stratégie de basculement DNS pour acheminer votre trafic DNS d'une région à l'autre.

Pour plus d'informations sur les stratégies de routage DNS, consultez [Sélection d'une stratégie de routage](#) dans le Guide du développeur Amazon Route 53. Pour plus d'informations sur la surveillance de l'état Amazon Route 53, consultez [Comment Amazon Route 53 vérifie l'état de vos ressources](#) dans le Guide du développeur Amazon Route 53.

Lorsque vous configurez vos politiques de routage DNS, vous aurez besoin de l'identifiant de connexion pour l'association entre l'alias de connexion et le WorkSpaces répertoire dans la région principale. Vous aurez également besoin de l'identifiant de connexion pour l'association entre l'alias de connexion et le WorkSpaces répertoire dans votre ou vos régions de basculement.

 Note

L'identifiant de connexion est différent de l'identifiant d'alias de connexion. L'identifiant d'alias de connexion commence par `wsc-`.

Pour rechercher l'identifiant de connexion d'une association d'alias de connexion

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre WorkSpaces.
3. Dans le panneau de navigation, choisissez Paramètres du compte.
4. Sous Associations de redirection entre régions, sélectionnez le texte de la chaîne de connexion (le FQDN) pour afficher la page des détails de l'alias de connexion.
5. Sur la page des détails de votre alias de connexion, sous Répertoire associé, notez la valeur affichée pour Identifiant de connexion.
6. Répétez ces étapes, mais assurez-vous de [Step 2](#) sélectionner la région de basculement correspondant à votre WorkSpaces. Si vous avez plusieurs régions de basculement, répétez ces étapes afin de rechercher l'identifiant de connexion pour chaque région de basculement.

Exemple : Pour configurer une stratégie de routage de basculement DNS à l'aide de Route 53

L'exemple suivant configure une zone hébergée publique pour votre domaine. Toutefois, vous pouvez configurer une zone hébergée publique ou privée. Pour plus d'informations sur la configuration d'une zone hébergée, consultez [Utilisation des zones hébergées](#) dans le Guide du développeur Amazon Route 53.

Cet exemple utilise également une stratégie de routage de basculement. Vous pouvez utiliser d'autres types de stratégies de routage pour votre stratégie de redirection entre régions. Pour plus d'informations sur les stratégies de routage DNS, consultez [Sélection d'une stratégie de routage](#) dans le Guide du développeur Amazon Route 53.

Lorsque vous configurez une stratégie de routage de basculement dans Route 53, une surveillance de l'état est requise pour la région principale. Pour plus d'informations sur la création d'une surveillance de l'état dans Route 53, consultez [Création de vérifications d'état Amazon Route 53 et configuration du basculement DNS](#) et [Création, mise à jour et suppression de surveillances de l'état](#) dans le Guide du développeur Amazon Route 53.

Si vous souhaitez utiliser une CloudWatch alarme Amazon pour votre bilan de santé de la Route 53, vous devez également configurer une CloudWatch alarme pour surveiller les ressources de votre région principale. Pour plus d'informations CloudWatch, consultez [Qu'est-ce qu'Amazon CloudWatch ?](#) dans le guide de CloudWatch l'utilisateur Amazon. Pour plus d'informations sur la façon dont Route 53 utilise les CloudWatch alarmes dans ses bilans de santé, consultez [Comment Route 53 détermine le statut des bilans de santé qui surveillent les CloudWatch alarmes](#) et [Surveillance CloudWatch d'une alarme](#) dans le manuel du développeur Amazon Route 53.

Pour configurer une stratégie de routage de basculement DNS dans Route 53, vous devez d'abord créer une zone hébergée pour votre domaine.

1. Ouvrez la console Route 53 à l'adresse <https://console.aws.amazon.com/route53/>.
2. Dans le panneau de navigation, choisissez Zones hébergées, puis choisissez Créer une zone hébergée.
3. Sur la page Zone hébergée créée, entrez votre nom de domaine (tel que `example.com`) sous Nom de domaine.
4. Sous Type, sélectionnez Zone hébergée publique.
5. Choisissez Créer une zone hébergée.

Créez ensuite une surveillance de l'état pour votre région principale.

1. Ouvrez la console Route 53 à l'adresse <https://console.aws.amazon.com/route53/>.
2. Dans le volet de navigation, choisissez Vérifications de l'état, puis Créer une vérification de l'état.
3. Sur la page Configurer la vérification de l'état, entrez le nom de la surveillance de l'état.
4. Pour Éléments à surveiller, sélectionnez Endpoint, État des autres bilans de santé (bilan de santé calculé) ou État de l' CloudWatch alarme.

5. En fonction de ce que vous avez sélectionné à l'étape précédente, configurez votre surveillance de l'état, puis choisissez Suivant.
6. Sur la page M'avertir quand une vérification de l'état échoue pour Créer une alarme, choisissez Oui ou Non.
7. Choisissez Créer une vérification de l'état.

Une fois que vous avez créé votre surveillance de l'état, vous pouvez créer les enregistrements de basculement DNS.

1. Ouvrez la console Route 53 à l'adresse <https://console.aws.amazon.com/route53/>.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Sur la page Zones hébergées, sélectionnez votre nom de domaine.
4. Sur la page des détails de votre nom de domaine, choisissez Créer un enregistrement.
5. Sur la page Choisir une stratégie de routage, sélectionnez Basculement, puis Suivant.
6. Sur la page Configurer les enregistrements, sous Configuration de base, entrez le nom de votre sous-domaine dans le champ Nom de l'enregistrement. Par exemple, si votre nom de domaine complet (FQDN) est `desktop.example.com`, entrez **desktop**.

 Note

Si vous souhaitez utiliser le domaine racine, laissez le champ Nom de l'enregistrement vide. Cependant, nous vous recommandons d'utiliser un sous-domaine, tel que `desktop` ou `workspaces`, sauf si vous avez configuré le domaine uniquement pour une utilisation avec votre WorkSpaces.

7. Pour Type d'enregistrement, sélectionnez TXT – Utilisé pour vérifier les expéditeurs d'e-mails et pour les valeurs spécifiques à l'application.
8. Conservez les paramètres de secondes TTL par défaut.
9. Sous Enregistrements de basculement auxquels ajouter **your_domain_name**, choisissez Définir un enregistrement de basculement.

Vous devez maintenant configurer les enregistrements de basculement pour vos régions principale et de basculement.

Exemple : Pour configurer l'enregistrement de basculement pour votre région principale

1. Dans la boîte de dialogue Définir un enregistrement de basculement, pour Évaluer/Acheminer le trafic vers, sélectionnez Adresse IP ou une autre valeur en fonction du type d'enregistrement.
2. Une boîte de dialogue s'ouvre pour vous permettre de saisir vos exemples de texte. Entrez l'identifiant de connexion pour l'association d'alias de connexion de votre région principale.
3. Pour Type d'enregistrement de basculement, sélectionnez Principale.
4. Pour Vérification de l'état, sélectionnez une surveillance de l'état que vous avez créée pour votre région principale.
5. Pour ID d'enregistrement, entrez une description afin d'identifier cet enregistrement.
6. Choisissez Définir un enregistrement de basculement. Votre nouvel enregistrement de basculement apparaît sous Enregistrements de basculement auxquels ajouter.
your_domain_name

Exemple : Pour configurer l'enregistrement de basculement pour votre région de basculement

1. Sous Enregistrements de basculement auxquels ajouter *your_domain_name*, choisissez Définir un enregistrement de basculement.
2. Dans la boîte de dialogue Définir un enregistrement de basculement, pour Évaluer/Acheminer le trafic vers, sélectionnez Adresse IP ou une autre valeur en fonction du type d'enregistrement.
3. Une boîte de dialogue s'ouvre pour vous permettre de saisir vos exemples de texte. Entrez l'identifiant de connexion pour l'association d'alias de connexion de votre région de basculement.
4. Pour Type d'enregistrement de basculement, sélectionnez Secondaire.
5. (Facultatif) Dans Vérification de l'état, entrez une surveillance de l'état que vous avez créée pour votre région de basculement.
6. Pour ID d'enregistrement, entrez une description afin d'identifier cet enregistrement.
7. Choisissez Définir un enregistrement de basculement. Votre nouvel enregistrement de basculement apparaît sous Enregistrements de basculement auxquels ajouter.
your_domain_name

Si le bilan de santé que vous avez configuré pour votre région principale échoue, votre politique de routage de basculement DNS redirige vos WorkSpaces utilisateurs vers votre région de basculement. Route 53 continue de surveiller le bilan de santé de votre région principale, et lorsque le bilan de

santé de votre région principale n'échoue plus, Route 53 redirige automatiquement vos WorkSpaces utilisateurs vers leur WorkSpaces région principale.

Pour plus d'informations sur la création d'enregistrements DNS, consultez [Création d'enregistrements à l'aide de la console Amazon Route 53](#) dans le Guide du développeur Amazon Route 53. Pour plus d'informations sur la configuration des enregistrements TXT DNS, consultez [Type d'enregistrement TXT](#) dans le Guide du développeur Amazon Route 53.

Étape 5 : envoyer la chaîne de connexion à vos WorkSpaces utilisateurs

Pour vous assurer que vos utilisateurs WorkSpaces seront redirigés selon les besoins en cas de panne, vous devez envoyer la chaîne de connexion (FQDN) à vos utilisateurs. Si vous avez déjà délivré des codes d'enregistrement régionaux (par exemple, WSpdx+ABC12D) à vos WorkSpaces utilisateurs, ces codes restent valides. Toutefois, pour que la redirection entre régions fonctionne, vos WorkSpaces utilisateurs doivent utiliser la chaîne de connexion comme code d'enregistrement lorsqu'ils les enregistrent WorkSpaces dans l'application WorkSpaces cliente.

Important

Si vous créez vos utilisateurs dans la WorkSpaces console au lieu de les créer dans Active Directory, envoie WorkSpaces automatiquement un e-mail d'invitation à vos utilisateurs avec un code d'enregistrement basé sur la région (par exemple, WSpdx+ABC12D) chaque fois que vous lancez un nouveau. Workspace Même si vous avez déjà configuré la redirection entre régions, l'e-mail d'invitation envoyé automatiquement WorkSpaces contient ce code d'enregistrement basé sur la région au lieu de votre chaîne de connexion.

Pour vous assurer que vos WorkSpaces utilisateurs utilisent la chaîne de connexion au lieu du code d'enregistrement basé sur la région, vous devez leur envoyer un autre e-mail contenant la chaîne de connexion en suivant la procédure ci-dessous.

Pour envoyer la chaîne de connexion à vos WorkSpaces utilisateurs

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre WorkSpaces
3. Dans le panneau de navigation, sélectionnez WorkSpaces.

4. Sur la WorkSpacespage, utilisez le champ de recherche pour rechercher un utilisateur auquel vous souhaitez envoyer une invitation, puis sélectionnez le correspondant dans les résultats WorkSpace de recherche. Vous ne pouvez en sélectionner qu'un WorkSpace à la fois.
5. Choisissez Actions, Inviter un utilisateur.
6. Sur la WorkSpaces page Inviter des utilisateurs à rejoindre leur site, vous verrez un modèle d'e-mail à envoyer à vos utilisateurs.
7. (Facultatif) Si plusieurs alias de connexion sont associés à votre WorkSpaces répertoire, sélectionnez la chaîne de connexion que vous souhaitez que vos utilisateurs utilisent dans la liste des chaînes d'alias de connexion. Le modèle d'e-mail est mis à jour pour afficher la chaîne que vous avez choisie.
8. Copiez le texte du modèle, puis dans votre propre application de messagerie, collez-le dans un e-mail destiné aux utilisateurs. Dans l'application, vous pouvez modifier le texte selon vos besoins. Lorsque l'e-mail d'invitation est prêt, envoyez-le aux utilisateurs.

Schéma de l'architecture de redirection entre régions

Le schéma suivant décrit le processus de déploiement de la redirection entre régions.

Note

La redirection entre régions facilite uniquement le basculement et le repli entre régions. Cela ne facilite pas la création et la maintenance WorkSpaces dans la région secondaire et n'autorise pas la réplication de données entre régions. WorkSpaces dans les régions primaire et secondaire, elles devraient être gérées séparément.

Lancer la redirection entre régions

En cas de panne, vous pouvez soit mettre à jour les enregistrements DNS manuellement, soit utiliser des politiques de routage automatisées basées sur des contrôles de santé, qui déterminent la région de basculement. Nous vous recommandons de suivre les mécanismes de reprise après sinistre décrits dans [Création de mécanismes de reprise après sinistre à l'aide d'Amazon Route 53](#).

Que se passe-t-il lors de la redirection entre régions

Pendant le basculement d'une région, vos WorkSpaces utilisateurs sont déconnectés de leurs utilisateurs WorkSpaces de la région principale. Lorsqu'ils tentent de se reconnecter, ils reçoivent le message d'erreur suivant :

We can't connect to your Workspace. Check your network connection, and then try again.

Ils sont ensuite invités à se reconnecter. S'ils utilisent le FQDN comme code d'enregistrement, lorsqu'ils se reconnectent, vos politiques de routage de basculement DNS les redirigent vers WorkSpaces celui que vous avez configuré pour eux dans la région de basculement.

Note

Dans certains cas, les utilisateurs peuvent ne pas être en mesure de se reconnecter lorsqu'ils essaient de nouveau. Si ce comportement se produit, ils doivent fermer et redémarrer l'application WorkSpaces cliente, puis essayer de se reconnecter.

Dissociation d'un alias de connexion d'un annuaire

Seul le compte propriétaire d'un annuaire peut dissocier un alias de connexion de celui-ci.

Si vous avez partagé un alias de connexion avec un autre compte et que ce dernier a associé l'alias de connexion à un annuaire lui appartenant, ce compte doit être utilisé pour dissocier l'alias de connexion de l'annuaire.

Pour dissocier un alias de connexion d'un annuaire

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région contenant l'alias de connexion que vous souhaitez dissocier.
3. Dans le panneau de navigation, choisissez Paramètres du compte.
4. Sous Associations de redirection entre régions, sélectionnez la chaîne de connexion, puis choisissez Actions, Associer/Dissocier.

Vous pouvez également dissocier un alias de connexion depuis la page des détails de l'alias de connexion. Pour ce faire, sous Répertoire associé, choisissez Dissocier.

5. Sur la page Associer/dissocier, choisissez Dissocier.
6. Dans la boîte de dialogue demandant de confirmer la dissociation, choisissez Dissocier.

Annulation du partage d'un alias de connexion

Seul le propriétaire d'un alias de connexion peut annuler le partage de l'alias. Si vous annulez le partage d'un alias de connexion avec un compte, ce compte ne peut plus associer l'alias de connexion à un annuaire.

Pour annuler le partage d'un alias de connexion

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région qui contient l'alias de connexion dont vous souhaitez annuler le partage.
3. Dans le panneau de navigation, choisissez Paramètres du compte.
4. Sous Associations de redirection entre régions, sélectionnez la chaîne de connexion, puis choisissez Actions, Partager/annuler le partage de l'alias de connexion.

Vous pouvez également annuler le partage d'un alias de connexion depuis la page des détails de l'alias de connexion. Pour ce faire, sous Compte partagé, choisissez Annuler le partage.

5. Sur la page Partager/annuler le partage de l'alias de connexion, choisissez Annuler le partage.
6. Dans la boîte de dialogue demandant de confirmer l'annulation du partage de l'alias de connexion, choisissez Annuler le partage.

Suppression d'un alias de connexion

Vous pouvez supprimer un alias de connexion uniquement s'il appartient à votre compte et s'il n'est associé à aucun annuaire.

Si vous avez partagé un alias de connexion avec un autre compte et que ce compte l'a associé à un annuaire lui appartenant, ce compte doit d'abord dissocier l'alias de connexion de l'annuaire avant de pouvoir supprimer l'alias de connexion.

Important

Une fois que vous avez créé une chaîne de connexion, celle-ci est toujours associée à votre AWS compte. Vous ne pouvez pas recréer la même chaîne de connexion avec un autre

compte, même si vous avez supprimé toutes ses instances du compte d'origine. La chaîne de connexion est globalement réservée à votre compte.

 Warning

Si vous n'utilisez plus de FQDN comme code d'enregistrement pour vos WorkSpaces utilisateurs, vous devez prendre certaines précautions pour éviter d'éventuels problèmes de sécurité. Pour de plus amples informations, veuillez consulter [Considérations de sécurité si vous arrêtez d'utiliser la redirection entre régions](#).

Pour supprimer un alias de connexion

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région qui contient l'alias de connexion que vous souhaitez supprimer.
3. Dans le panneau de navigation, choisissez Paramètres du compte.
4. Sous Associations de redirection entre régions, sélectionnez la chaîne de connexion, puis choisissez Supprimer.

Vous pouvez également supprimer un alias de connexion depuis la page des détails de l'alias de connexion. Pour ce faire, sélectionnez Supprimer dans l'angle supérieur droit de la page.

 Note

Si le bouton Supprimer est désactivé, assurez-vous d'être le propriétaire de l'alias, et que celui-ci n'est pas associé à un annuaire.

5. Dans la boîte de dialogue demandant de confirmer la suppression, choisissez Supprimer.

Autorisations IAM pour associer et dissocier des alias de connexion

Si vous vous servez d'un utilisateur IAM pour associer ou dissocier des alias de connexion, l'utilisateur doit disposer des autorisations pour `workspaces:AssociateConnectionAlias` et `workspaces:DisassociateConnectionAlias`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
        "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-
a1bcd2efg"
      ]
    }
  ]
}
```

 Important

Si vous créez une politique IAM pour associer ou dissocier des alias de connexion pour des comptes qui ne les possèdent pas, vous ne pouvez pas spécifier d'ID de compte dans l'ARN. À la place, vous devez utiliser * pour l'ID de compte, comme illustré dans l'exemple de politique suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
```

```
    "arn:aws:workspaces:us-east-1::connectionalias/wsca-a1bcd2efg"  
  ]  
}  
]  
}
```

Vous pouvez spécifier un ID de compte dans l'ARN uniquement lorsque ce compte possède l'alias de connexion à associer ou à dissocier.

Pour plus d'informations sur l'utilisation d'IAM, consultez [Gestion des identités et des accès pour WorkSpaces](#).

Considérations de sécurité si vous arrêtez d'utiliser la redirection entre régions

Si vous n'utilisez plus de FQDN comme code d'enregistrement pour vos WorkSpaces utilisateurs, vous devez prendre les précautions suivantes pour éviter d'éventuels problèmes de sécurité :

- Assurez-vous de fournir à vos WorkSpaces utilisateurs le code d'enregistrement spécifique à la région (par exemple, WSpdx+ABC12D) pour leur WorkSpaces répertoire et de leur demander de ne plus utiliser le FQDN comme code d'enregistrement.
- Si vous êtes toujours propriétaire de ce domaine, veillez à mettre à jour votre enregistrement TXT DNS pour supprimer ce domaine afin qu'il ne puisse pas être exploité lors d'une attaque d'hameçonnage. Si vous supprimez ce domaine de votre enregistrement DNS TXT et que vos WorkSpaces utilisateurs tentent d'utiliser le FQDN comme code d'enregistrement, leurs tentatives de connexion échoueront sans problème.
- Si vous ne possédez plus ce domaine, vos WorkSpaces utilisateurs doivent utiliser leur code d'enregistrement spécifique à la région. S'ils continuent d'essayer d'utiliser le FQDN comme code d'enregistrement, ils risquent d'être redirigés vers un site malveillant lors de leurs tentatives de connexion.

Résilience multirégionale au service du personnel WorkSpaces

Amazon WorkSpaces Multi-Region Resilience (MRR) vous permet de rediriger les utilisateurs vers une région secondaire lorsque votre WorkSpaces région principale est inaccessible en raison d'événements perturbateurs, sans que vos utilisateurs n'aient à changer de code d'enregistrement

lorsqu'ils se connectent à leur zone de réserve. WorkSpaces WorkSpaces La mise en veille est une fonctionnalité d'Amazon WorkSpaces Multi-Region Resilience qui rationalise la création et la gestion des déploiements de veille. Après avoir configuré un annuaire d'utilisateurs dans votre région secondaire, sélectionnez le Workspace répertoire de votre région principale Workspace pour lequel vous souhaitez créer un répertoire de secours. Le système reflète automatiquement les images du Workspace bundle principal dans la région secondaire. Il met ensuite automatiquement en service un nouveau mode veille Workspace dans votre région secondaire.

Amazon WorkSpaces Multi-Region Resilience repose sur la redirection entre régions qui tire parti des fonctionnalités de vérification de l'état du DNS et de basculement sur incident. Il vous permet d'utiliser un nom de domaine complet (FQDN) comme code WorkSpaces d'enregistrement. Lorsque vos utilisateurs se connectent à WorkSpaces, vous pouvez les rediriger vers les WorkSpaces régions prises en charge en fonction des politiques de votre système de noms de domaine (DNS) pour le FQDN. Si vous utilisez Amazon Route 53, nous vous recommandons d'utiliser des contrôles de santé qui surveillent les CloudWatch alarmes Amazon lors de l'élaboration d'une stratégie de redirection entre régions pour. WorkSpaces Pour plus d'informations, consultez les [sections Création de contrôles de santé d'Amazon Route 53 et configuration du basculement DNS](#) dans le manuel du développeur Amazon Route 53.

La réplication des données est une fonctionnalité supplémentaire de veille WorkSpaces qui réplique les données dans un sens depuis la région principale vers la région secondaire. Une fois la réplication des données activée, des instantanés EBS du système et des volumes utilisateur sont pris toutes les 12 heures. Multi-Region Resilience vérifie régulièrement la présence de nouveaux instantanés. Lorsque les instantanés sont trouvés, une copie est lancée dans la région secondaire. Lorsque les copies arrivent dans la région secondaire, elles sont utilisées pour mettre à jour la région secondaire Workspace.

Table des matières

- [Conditions préalables](#)
- [Limitations](#)
- [Configurez votre mode de veille multirégional pour la résilience Workspace](#)
- [Création d'un mode veille Workspace](#)
- [Gérer une veille Workspace](#)
- [Supprimer un mode veille Workspace](#)
- [Réplication unidirectionnelle des données pour le mode veille WorkSpaces](#)
- [Prévoyez de réserver la capacité Amazon EC2 pour la restauration](#)

Conditions préalables

- Vous devez créer WorkSpaces pour vos utilisateurs dans la région principale avant de créer le mode veille WorkSpaces. Pour plus d'informations sur la création WorkSpaces, consultez [Création d'un répertoire pour WorkSpaces Personal](#).
- Pour activer la réplication des données en mode veille WorkSpaces, vous devez disposer d'un Active Directory autogéré ou d'un Microsoft AD AWS géré configuré pour effectuer la réplication dans vos régions de secours. Pour plus d'informations, voir [Créer votre répertoire Microsoft AD AWS géré](#) et [Ajouter une région répliquée](#).
- Assurez-vous de mettre à jour les pilotes de dépendance réseau tels que les pilotes ENA et PV sur votre système principal WorkSpaces. NVMe Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, voir [Installer ou mettre à niveau le pilote Elastic Network Adapter \(ENA\)](#), [Pilotes NVMe AWS pour les instances Windows](#), et [Mettre à niveau les pilotes PV sur les instances Windows](#).
- Assurez-vous de mettre régulièrement à jour les agents EC2 Config, EC2 EC2 Launch et Launch V2 vers les dernières versions. Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez [Update EC2 Config and EC2 Launch](#).
- Pour garantir une réplication correcte des données, assurez-vous que les annuaires actifs des régions principale et secondaire sont synchronisés pour le nom de domaine complet, l'unité d'organisation et le SID de l'utilisateur.
- Le quota (limite) par défaut pour le mode veille WorkSpaces est de 0. Vous devez demander une augmentation du quota de service avant de créer un service de secours WorkSpace. Pour de plus amples informations, veuillez consulter [WorkSpaces Quotas Amazon](#).
- Assurez-vous d'utiliser des [clés gérées par le client](#) pour chiffrer à la fois votre clé principale et votre clé de secours WorkSpaces. Vous pouvez utiliser des clés régionales uniques ou des clés [multirégionales pour chiffrer votre clé](#) principale et votre clé de secours. WorkSpaces

Limitations

- Standby copie WorkSpaces uniquement l'image du bundle de votre fichier principal WorkSpaces , mais il ne copie pas le volume système (lecteur C) ou le volume utilisateur (lecteur D) à partir de votre principal WorkSpaces. Pour copier le volume système (lecteur C) ou le volume utilisateur (lecteur D) de votre disque principal WorkSpaces vers le volume de secours WorkSpaces, vous devez activer la réplication des données.

- Vous ne pouvez pas directement modifier, reconstruire, restaurer ou migrer un standby WorkSpace.
- Le basculement pour la redirection entre régions est contrôlé par les paramètres DNS. Pour implémenter un scénario de basculement automatique, vous devez utiliser un autre mécanisme conjointement avec la redirection entre régions. Par exemple, vous pouvez utiliser une politique de routage DNS en cas de basculement d'Amazon Route 53 associée à un bilan de santé de Route 53 qui surveille une CloudWatch alarme dans la région principale. Si l' CloudWatch alarme de la région principale est invoquée, votre politique de routage de basculement DNS redirige ensuite vos WorkSpaces utilisateurs vers WorkSpaces celle que vous avez configurée pour eux dans la région de basculement.
- La réplication des données ne se fait que dans un sens, copiant les données de la région principale vers la région secondaire. Pendant le WorkSpaces basculement en mode veille, vous pouvez accéder aux données et à l'application entre 12 et 24 heures. Après une panne, sauvegardez manuellement toutes les données que vous avez créées sur le périphérique secondaire WorkSpace et déconnectez-vous. Nous vous recommandons d'enregistrer votre travail sur des disques externes, tels que votre lecteur réseau, afin de pouvoir accéder à vos données depuis le disque principal WorkSpace.
- La réplication des données ne prend pas en charge AWS Simple AD.
- Lorsque vous activez la réplication des données en mode veille WorkSpaces, des instantanés EBS du volume principal WorkSpaces (volumes racine et système) sont pris toutes les 12 heures. L'instantané initial d'un volume de données donné est complet et les instantanés suivants sont incrémentiels. Par conséquent, la première réplication pour une donnée WorkSpace prendra plus de temps que les suivantes. Les instantanés sont lancés selon un calendrier interne à WorkSpaces lequel vous ne pouvez pas contrôler le timing.
- Si le serveur principal WorkSpace et le serveur de secours WorkSpace se joignent en utilisant le même domaine, nous vous recommandons de vous connecter uniquement au serveur principal WorkSpace ou WorkSpace au serveur de secours à un moment donné afin d'éviter de perdre la connexion avec le contrôleur de domaine.
- Si vous configurez votre AWS Managed Microsoft AD réplication multirégionale, seul le répertoire de la région principale peut être enregistré pour être utilisé avec WorkSpaces. Si vous essayez d'enregistrer le répertoire dans une région répliquée pour l'utiliser WorkSpaces, il échouera. La réplication multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation WorkSpaces au sein de régions répliquées.
- Si vous avez déjà configuré votre redirection entre régions et que vous l'avez créée WorkSpaces dans vos régions principale et secondaire sans utiliser le mode veille WorkSpaces, vous ne pouvez

pas convertir WorkSpace directement la redirection existant WorkSpace dans la région secondaire en mode veille. Vous devez plutôt arrêter le WorkSpace dans votre région secondaire, sélectionner celui de votre région principale pour lequel vous souhaitez créer un mode veille et utiliser le mode veille WorkSpace WorkSpaces pour créer le mode veille WorkSpace. WorkSpace

- Après une panne, sauvegardez manuellement toutes les données que vous avez créées sur le périphérique secondaire WorkSpace et déconnectez-vous. Nous vous recommandons d'enregistrer votre travail sur des disques externes, tels que votre lecteur réseau, afin de pouvoir accéder à vos données depuis le disque principal WorkSpace.
- WorkSpaces Multi-Region Resilience est actuellement disponible dans les régions suivantes :
 - Région USA Est (Virginie du Nord)
 - Région USA Ouest (Oregon)
 - Région Europe (Francfort)
 - Europe (Irlande) Region
- WorkSpaces La résilience multirégionale n'est prise en charge que sur la version 3.0.9 ou ultérieure des applications WorkSpaces clientes Linux, macOS et Windows. Vous pouvez également utiliser la résilience multirégionale avec Web Access.
- WorkSpaces Multi-Region Resilience prend en charge Windows et Bring Your Own License (BYOL). WorkSpaces Il n'est pas compatible avec Amazon Linux 2, Ubuntu, Red Hat Enterprise Linux, GeneralPurpose .4xlarge, GeneralPurpose .8xlarge ou compatible avec le GPU WorkSpaces (par exemple, Graphics G6, Graphics.G4DN ou .g4dn). GraphicsPro
- Une fois le basculement ou le retour en arrière terminé, attendez 15 à 30 minutes avant de vous connecter à votre. WorkSpace

Configurez votre mode de veille multirégional pour la résilience WorkSpace

Pour configurer votre mode de veille Multi-Region Resilience WorkSpace

1. Configurez des annuaires d'utilisateurs dans vos régions principale et secondaire. Assurez-vous d'utiliser les mêmes noms d'utilisateur dans chaque WorkSpaces répertoire de chaque région.

Pour synchroniser les données de vos utilisateurs Active Directory, nous vous recommandons d'utiliser AD Connector pour pointer vers le même Active Directory dans chaque région que vous avez configurée WorkSpaces pour vos utilisateurs. Pour plus d'informations sur la création d'un répertoire, voir [Enregistrer un répertoire auprès de WorkSpaces](#).

 Important

Si vous configurez votre AWS Managed Microsoft AD répertoire pour la réplication multirégionale, seul le répertoire de la région principale peut être enregistré pour être utilisé avec WorkSpaces. Les tentatives d'enregistrement du répertoire dans une région répliquée pour l'utiliser WorkSpaces échoueront. La réplication multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation WorkSpaces au sein de régions répliquées.

2. Créez WorkSpaces pour vos utilisateurs de la région principale. Pour plus d'informations sur la création WorkSpaces, consultez [Launch WorkSpaces](#).
3. Créez une réserve Workspace dans la région secondaire. Pour plus d'informations sur la création d'un mode veille Workspace, consultez la section [Création d'un mode veille Workspace](#).
4. Créez et associez des chaînes de connexion (FQDN) aux annuaires des utilisateurs dans les régions principales et secondaires.

Vous devez activer la redirection entre régions dans votre compte car le mode veille WorkSpaces repose sur la redirection entre régions. Suivez les étapes 1 à 3 des instructions relatives à la [redirection entre régions pour Amazon WorkSpaces](#).

5. Configurez le service DNS et configurez les politiques de routage DNS.

Vous devez configurer votre [service DNS et configurer les politiques de routage DNS nécessaires](#). La redirection entre régions fonctionne en conjonction avec vos politiques de routage DNS pour rediriger vos WorkSpaces utilisateurs selon les besoins.

6. Une fois que vous avez terminé de configurer la redirection entre régions, vous devez envoyer aux utilisateurs un e-mail contenant une chaîne de connexion FQDN. Pour plus d'informations, voir [Étape 5 : Envoyer la chaîne de connexion à vos WorkSpaces utilisateurs](#). Assurez-vous que vos WorkSpaces utilisateurs utilisent le code d'enregistrement basé sur le FQDN plutôt que le code d'enregistrement basé sur la région (par exemple, WSpdx + ABC12 D) pour leur région principale.

 Important

- Si vous créez vos utilisateurs dans la WorkSpaces console au lieu de les créer dans Active Directory, envoie WorkSpaces automatiquement un e-mail d'invitation à vos utilisateurs avec un code d'enregistrement basé sur la région chaque fois que

vous lancez un nouveau. Workspace Cela signifie que lorsque vous configurez la région secondaire WorkSpaces pour vos utilisateurs, ceux-ci recevront également automatiquement des e-mails pour ces régions secondaires WorkSpaces. Vous devrez demander aux utilisateurs d'ignorer les e-mails contenant des codes d'enregistrement basés sur la région.

- Les codes d'enregistrement spécifiques à la région restent valides ; toutefois, pour que la redirection entre régions fonctionne, vos utilisateurs doivent plutôt utiliser le FQDN comme code d'enregistrement.

Création d'un mode veille Workspace

Avant de créer un service WorkSpaces de secours Workspace, assurez-vous d'avoir rempli les conditions requises, notamment en créant un annuaire des utilisateurs dans les régions principale et secondaire, en fournissant des ressources à vos utilisateurs dans votre région principale, en configurant la redirection entre régions dans votre compte et en demandant une augmentation de la WorkSpaces limite de veille dans le cadre du quota de service.

Pour créer un mode veille Workspace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre WorkSpaces
3. Dans le panneau de navigation, sélectionnez WorkSpaces.
4. Sélectionnez celui pour lequel Workspace vous souhaitez créer une réserve Workspace .
5. Choisissez Actions, puis Create standby Workspace.
6. Sélectionnez la région secondaire dans laquelle vous allez créer votre mode veille Workspace, puis choisissez Next.
7. Sélectionnez l'annuaire d'utilisateurs dans la région secondaire, puis choisissez Suivant.
8. (Facultatif) Ajoutez une clé de chiffrement, activez le chiffrement des données et gérez les balises.
 - Pour ajouter une clé de chiffrement, saisissez-la sous Clé de chiffrement d'entrée.
 - Pour activer la réplication des données, choisissez Activer la réplication des données. Cochez ensuite la case pour confirmer que vous autorisez des frais mensuels supplémentaires.
 - Pour ajouter un nouveau tag, choisissez Ajouter un nouveau tag.

Ensuite, choisissez Suivant.

 Note

- Si l'original WorkSpace est chiffré, ce champ est prérempli. Vous avez toutefois la possibilité de remplacer son contenu par votre propre clé de chiffrement.
- La mise à jour de l'état de réplication des données prend quelques minutes.
- Une fois que le mode veille WorkSpace a été correctement mis à jour avec les instantanés du serveur principal WorkSpace, vous pouvez trouver les horodatages des instantanés sous Recovery Snapshot.

9. Vérifiez les paramètres de votre mode veille, WorkSpaces puis choisissez Create.

 Note

- Pour consulter les informations relatives à votre mode veille WorkSpaces, rendez-vous sur la page WorkSpace détaillée principale.
- Le mode veille copie WorkSpace uniquement l'image du bundle de votre fichier principal WorkSpace, mais il ne copie pas le volume système (lecteur C) ou le volume utilisateur (lecteur D) de votre appareil principal WorkSpaces. Par défaut, la réplication des données est désactivée. Pour copier le volume système (lecteur C) ou le volume utilisateur (lecteur D) de votre disque principal WorkSpaces vers le volume de secours WorkSpaces, vous devez activer la réplication des données.

Gérer une veille WorkSpace

Vous ne pouvez pas directement modifier, reconstruire, restaurer ou migrer un standby WorkSpace.

Pour activer la réplication des données pour votre serveur de secours WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Accédez à votre région principale, sélectionnez l' WorkSpace identifiant principal.
3. Faites défiler la page jusqu'à la WorkSpace section Mise en veille et choisissez Modifier la mise en veille WorkSpace.

4. Choisissez Activer la réplication des données. Cochez ensuite la case pour confirmer que vous autorisez des frais mensuels supplémentaires. Ensuite, choisissez Enregistrer.

Note

- Le mode veille WorkSpaces ne peut pas hiberner. Si vous arrêtez le mode veille WorkSpace, cela ne préserve pas votre travail non enregistré. Nous recommandons aux utilisateurs de toujours enregistrer leur travail avant de quitter leur mode veille WorkSpaces.
- Pour activer la réplication des données en mode veille WorkSpaces, vous devez disposer d'un Active Directory autogéré ou d'un Microsoft AD AWS géré configuré pour effectuer la réplication dans vos régions de secours. Pour configurer vos annuaires, suivez les étapes 1 à 3 de la section Procédure pas à pas de la section [Construire pour la continuité des activités avec Amazon WorkSpaces et AWS Directory Services](#) ou consultez la section [Utilisation d'Active Directory AWS géré par plusieurs régions avec Amazon](#). WorkSpaces La réplication multirégionale n'est prise en charge que pour l'édition Enterprise de AWS Managed Microsoft AD.
- La mise à jour de l'état de réplication des données prend quelques minutes.
- Une fois que le mode veille WorkSpace a été correctement mis à jour avec les instantanés du serveur principal WorkSpace, vous pouvez trouver les horodatages des instantanés sous Recovery Snapshot.

Supprimer un mode veille WorkSpace

Vous pouvez mettre fin à un mode veille WorkSpace de la même manière que vous résiliez un mode normal WorkSpace.

Pour supprimer un mode veille WorkSpace

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre WorkSpaces
3. Dans le panneau de navigation, sélectionnez WorkSpaces.
4. Sélectionnez le mode veille WorkSpace et choisissez Supprimer. La suppression d'un mode veille prend environ 5 minutes WorkSpace. Lors de la suppression, le statut du mode veille

Workspace sera défini sur Terminé. Lorsque la suppression est terminée, le mode veille Workspace disparaît de la console.

 Note

La suppression d'un standby Workspace est une action permanente qui ne peut pas être annulée. Les données de Workspace l'utilisateur en attente ne sont pas conservées et sont détruites. Pour obtenir de l'aide concernant la sauvegarde des données utilisateur, contactez AWS le Support.

Réplication unidirectionnelle des données pour le mode veille WorkSpaces

L'activation de la réplication des données dans Multi-Region Resilience vous permet de répliquer les données d'une région principale vers une région secondaire. En régime permanent, Multi-Region Resilience capture des instantanés du système (lecteur C) et des données (lecteur D) du système principal WorkSpaces toutes les 12 heures. Ces instantanés sont transférés vers la région secondaire et utilisés pour mettre à jour le mode veille WorkSpaces. Par défaut, la réplication des données est désactivée pour le mode veille WorkSpaces.

Une fois la réplication des données activée pour le mode veille WorkSpaces, le cliché initial pour un volume de données donné est terminé, tandis que les instantanés suivants sont incrémentiels. Par conséquent, la première réplication pour une donnée Workspace prendra plus de temps que les suivantes. Les instantanés sont déclenchés à des intervalles prédéterminés WorkSpaces et le timing ne peut pas être contrôlé par les utilisateurs.

Pendant le basculement, lorsque les utilisateurs sont redirigés vers la région secondaire, ils peuvent accéder à leur mode de veille WorkSpaces avec des données et des applications datant de 12 à 24 heures. Lorsque les utilisateurs utilisent le mode veille WorkSpaces, Multi-Region Resilience ne les obligera pas à se déconnecter de leur mode veille WorkSpaces ni à mettre à jour le mode veille WorkSpaces avec les instantanés de la région principale.

Après une panne, les utilisateurs doivent sauvegarder manuellement toutes les données qu'ils ont créées sur leur périphérique secondaire WorkSpaces avant de se déconnecter de leur système de veille WorkSpaces. Lorsqu'ils se reconnecteront, ils seront redirigés vers la région principale et leur région principale WorkSpaces.

Prévoyez de réserver la capacité Amazon EC2 pour la restauration

Amazon Multi-Region Resilience (MRR) s'appuie par défaut sur les pools Amazon EC2 On-Demand. Si un type d'instance Amazon EC2 spécifique n'est pas disponible pour prendre en charge votre restauration, MRR tentera automatiquement de l'agrandir à plusieurs reprises jusqu'à ce qu'un type d'instance disponible soit trouvé, mais dans des circonstances extrêmes, les instances peuvent ne pas toujours être disponibles. Pour améliorer la disponibilité des types d'instances dont vous avez besoin pour les instances les plus critiques WorkSpaces, contactez le AWS Support et nous vous aiderons à planifier les capacités.

Résoudre les problèmes liés à Personal WorkSpaces

Les informations suivantes peuvent vous aider à résoudre les problèmes liés à votre WorkSpaces.

Activation de la journalisation avancée

Pour résoudre les problèmes que vos utilisateurs peuvent rencontrer, vous pouvez activer la connexion avancée sur n'importe quel WorkSpaces client Amazon.

La journalisation avancée génère des fichiers journaux qui contiennent des informations de diagnostic et des détails de niveau débogage, avec notamment des données de performance détaillées. Pour les clients 1.0+ et 2.0+, ces fichiers de journalisation avancés sont automatiquement téléchargés vers une base de données dans AWS.

Note

Pour AWS consulter les fichiers de journalisation avancés et pour bénéficier d'une assistance technique en cas de problème avec vos WorkSpaces clients, contactez AWS Support. Pour plus d'informations, consultez le [Centre AWS Support](#).

Pour activer la journalisation avancée pour Web Access

Pour activer la journalisation avancée pour Web Access

1. Ouvrez votre client Amazon WorkSpaces Web Access.
2. En haut de la page de WorkSpaces connexion, choisissez Enregistrement des diagnostics.
3. Dans la boîte de dialogue contextuelle, assurez-vous que l'option Journalisation du diagnostic est activée.

4. Pour Niveau du journal, sélectionnez Journalisation avancée.

Pour accéder aux fichiers journaux dans Google Chrome, Microsoft Edge et Firefox

1. Ouvrez le menu contextuel (clic droit) dans le navigateur choisi, ou appuyez sur les touches Ctrl+Maj+I (ou pour Mac, commande+option+I) de votre clavier pour ouvrir le panneau des outils pour développeurs.
2. Dans le panneau des outils pour développeurs, cliquez sur l'onglet Console pour rechercher les fichiers journaux.

Pour accéder aux fichiers journaux dans Safari

1. Choisissez Safari, Paramètres.
2. Dans la fenêtre Paramètres, choisissez l'onglet Avancé.
3. Choisissez Afficher le menu Développement dans la barre de menu.
4. Dans l'onglet Développement de la barre de menu, choisissez Développement > Afficher l'inspecteur Web.
5. Dans le panneau Inspecteur Web Safari, cliquez sur l'onglet Console pour rechercher les fichiers journaux.

Pour activer la journalisation avancée pour les clients 4.0+

Les journaux du client Windows sont stockés à l'emplacement suivant :

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Pour activer la journalisation avancée pour les clients Windows

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez l'application Invite de commande.
3. Lancez le WorkSpaces client avec le -l3 drapeau.

```
c:
```

```
cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"
```

```
workspaces.exe -l3
```

 Note

S'il WorkSpaces est installé pour un utilisateur et non pour tous les utilisateurs, utilisez les commandes suivantes :

c :

```
cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

Les journaux du client macOS sont stockés à l'emplacement suivant :

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

Pour activer la journalisation avancée pour les clients macOS

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez Terminal.
3. Exécutez la commande suivante.

```
open -a workspaces --args -l3
```

Pour activer la journalisation avancée pour les clients Android

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez le menu du client Android.
3. Sélectionnez Support.
4. Sélectionnez Paramètres de journalisation.
5. Sélectionnez Activer la journalisation avancée.

Pour récupérer les journaux des clients Android après avoir activé la journalisation avancée :

- Sélectionnez Extraire le journal pour enregistrer localement les journaux compressés.

Les journaux du client Linux sont stockés à l'emplacement suivant :

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Pour activer la journalisation avancée pour les clients Linux

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez Terminal.
3. Exécutez la commande suivante.

```
/opt/workspacesclient/workspacesclient -l3
```

Pour activer la journalisation avancée pour les clients 3.0

Les journaux du client Windows sont stockés à l'emplacement suivant :

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Pour activer la journalisation avancée pour les clients Windows

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez l'application Invite de commande.
3. Lancez le WorkSpaces client avec le -l3 drapeau.

```
c:
```

```
cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"  
  
workspaces.exe -l3
```

Note

S'il WorkSpaces est installé pour un utilisateur et non pour tous les utilisateurs, utilisez les commandes suivantes :

```
c:
```

```
cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon  
WorkSpaces"  
workspaces.exe -l3
```

Les journaux du client macOS sont stockés à l'emplacement suivant :

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

Pour activer la journalisation avancée pour les clients macOS

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez Terminal.
3. Exécutez la commande suivante.

```
open -a workspaces --args -l3
```

Pour activer la journalisation avancée pour les clients Android

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez le menu du client Android.
3. Sélectionnez Support.
4. Sélectionnez Paramètres de journalisation.
5. Sélectionnez Activer la journalisation avancée.

Pour récupérer les journaux des clients Android après avoir activé la journalisation avancée :

- Sélectionnez Extraire le journal pour enregistrer localement les journaux compressés.

Les journaux du client Linux sont stockés à l'emplacement suivant :

```
~/local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Pour activer la journalisation avancée pour les clients Linux

1. Fermez le WorkSpaces client Amazon.
2. Ouvrez Terminal.
3. Exécutez la commande suivante.

```
/opt/workspacesclient/workspacesclient -l3
```


Pour activer la journalisation avancée pour les clients 1.0+ et 2.0+

1. Ouvrez le WorkSpaces client.
2. Choisissez l'icône d'engrenage dans le coin supérieur droit de l'application client.
3. Choisissez Advanced Settings (Paramètres avancés).
4. Cochez la case Enable Advanced Logging (Activer la journalisation avancée).
5. Choisissez Enregistrer.

Les journaux du client Windows sont stockés à l'emplacement suivant :

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

Les journaux du client macOS sont stockés à l'emplacement suivant :

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

Résolution de problèmes spécifiques

Les informations suivantes peuvent vous aider à résoudre des problèmes spécifiques liés à votre WorkSpaces.

Problèmes

- [Je ne parviens pas à créer un Amazon Linux WorkSpace car le nom d'utilisateur contient des caractères non valides](#)
- [J'ai changé le shell de mon Amazon Linux WorkSpace et je ne peux plus configurer de session PCo IP](#)
- [Mon Amazon Linux WorkSpaces ne démarre pas](#)
- [Le lancement WorkSpaces dans mon répertoire connecté échoue souvent](#)
- [Le lancement WorkSpaces échoue avec une erreur interne](#)
- [Lorsque j'essaie d'enregistrer un annuaire, l'enregistrement échoue et laisse l'annuaire avec l'état ERREUR](#)
- [Mes utilisateurs ne peuvent pas se connecter à un système Windows WorkSpace doté d'une bannière de connexion interactive](#)
- [Mes utilisateurs ne peuvent pas se connecter à un système Windows WorkSpace](#)
- [Mes utilisateurs rencontrent des problèmes lorsqu'ils essaient de se connecter WorkSpaces à WorkSpaces Web Access](#)

- [Le WorkSpaces client Amazon affiche un écran gris « Chargement... » pendant un moment avant de revenir à l'écran de connexion. Aucun autre message d'erreur ne s'affiche.](#)
- [Mes utilisateurs reçoivent le message « Workspace Status : Unhealthy ». Nous n'avons pas pu vous connecter à votre Workspace. Veuillez réessayer dans quelques minutes. ».](#)
- [Mes utilisateurs reçoivent le message « Cet appareil n'est pas autorisé à accéder au Workspace. Contactez votre administrateur pour obtenir de l'aide. »](#)
- [Les utilisateurs reçoivent le message « No network. Network connection lost. Check your network connection or contact your administrator for help. » lorsque vous essayez de vous connecter à un DCV Workspace](#)
- [Le WorkSpaces client envoie une erreur réseau à mes utilisateurs, mais ils peuvent utiliser d'autres applications connectées au réseau sur leurs appareils](#)
- [Mes Workspace utilisateurs voient le message d'erreur suivant : « L'appareil ne peut pas se connecter au service d'enregistrement. Veuillez vérifier vos paramètres réseau. »](#)
- [Les utilisateurs du client My PCo IP Zero reçoivent le message d'erreur « Le certificat fourni n'est pas valide en raison de l'horodatage »](#)
- [Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients PCo IP zéro](#)
- [Mes utilisateurs ont ignoré la mise à jour de leurs applications client Windows ou macOS et ne sont pas invités à installer la dernière version](#)
- [Mes utilisateurs ne peuvent pas installer l'application client Android sur leurs Chromebooks](#)
- [Mes utilisateurs ne reçoivent pas d'e-mails d'invitation ou d'e-mails de réinitialisation de mot de passe](#)
- [Mes utilisateurs ne voient pas l'option « Mot de passe oublié ? » sur l'écran de connexion du client](#)
- [Je reçois le message « L'administrateur système a défini des politiques pour empêcher cette installation » lorsque j'essaie d'installer des applications sur un système Windows Workspace](#)
- [Non WorkSpaces , dans mon annuaire, je ne peux pas me connecter à Internet](#)
- [Mon accès à Internet Workspace a été perdu](#)
- [L'erreur « DNS unavailable » s'affiche lorsque j'essaie de me connecter à mon annuaire sur site](#)
- [L'erreur « Connectivity issues detected » s'affiche lorsque je tente de me connecter à mon annuaire sur site](#)
- [L'erreur « SRV record » s'affiche lorsque je tente de me connecter à mon annuaire sur site](#)
- [Mon Windows Workspace se met en veille lorsqu'il est laissé inactif](#)
- [L'un des WorkSpaces miens a un état de UNHEALTHY](#)

- [Mon ordinateur WorkSpace se bloque ou redémarre de façon inattendue](#)
- [Le même nom d'utilisateur en possède plusieurs WorkSpace, mais l'utilisateur ne peut se connecter qu'à l'un des WorkSpaces](#)
- [Je ne parviens pas à utiliser Docker avec Amazon WorkSpaces](#)
- [Je reçois ThrottlingException des erreurs lors de certains de mes appels d'API](#)
- [Je WorkSpace continue de me déconnecter quand je le laisse fonctionner en arrière-plan](#)
- [La fédération SAML 2.0 ne fonctionne pas. Mes utilisateurs ne sont pas autorisés à streamer leur WorkSpaces ordinateur de bureau.](#)
- [Mes utilisateurs sont déconnectés de leur WorkSpaces session toutes les 60 minutes.](#)
- [Mes utilisateurs reçoivent une erreur d'URI de redirection lorsqu'ils se fédèrent à l'aide du flux initié par le fournisseur d'identité \(IdP\) SAML 2.0, ou lorsqu'une instance supplémentaire de l'application WorkSpaces cliente démarre chaque fois que mes utilisateurs tentent de se connecter depuis le client après s'être fédérés avec l'IdP.](#)
- [Mes utilisateurs reçoivent le message « Un problème s'est produit : une erreur s'est produite lors du lancement de votre application WorkSpace » lorsqu'ils tentent de se connecter à l'application WorkSpaces cliente après s'être fédérés avec l'IdP.](#)
- [Mes utilisateurs reçoivent le message « Impossible de valider les balises » lorsqu'ils tentent de se connecter à l'application WorkSpaces cliente après s'être fédérés avec l'IdP.](#)
- [Les utilisateurs reçoivent le message suivant : « The client and the server cannot communicate, because they do not possess a common algorithm ».](#)
- [Mon microphone ou ma webcam ne fonctionnent pas sous Windows WorkSpaces.](#)
- [Mes utilisateurs ne peuvent pas se connecter à l'aide de l'authentification par certificat et sont invités à saisir le mot de passe sur le WorkSpaces client ou sur l'écran de connexion Windows lorsqu'ils se connectent à leur session de bureau.](#)
- [J'essaie de faire quelque chose qui nécessite un support d'installation Windows mais qui WorkSpaces ne le fournit pas.](#)
- [Je souhaite lancer WorkSpaces avec un annuaire AWS géré existant créé dans une WorkSpaces région non prise en charge.](#)
- [Je souhaite mettre à jour Firefox sur Amazon Linux 2.](#)
- [Mon utilisateur peut réinitialiser son mot de passe à l'aide du WorkSpaces client, en ignorant le paramètre Fine Grained Password Policy \(FFGP\) configuré sur AWS Managed Microsoft AD](#)
- [Mes utilisateurs reçoivent le message d'erreur « Ceci n' OS/platform est pas autorisé à accéder à votre WorkSpace » lorsqu'ils tentent d'accéder à l' Windows/Linux WorkSpace aide de Web Access](#)

- [Celui de mon utilisateur WorkSpace s'affiche comme défectueux une fois qu' AutoStop WorkSpace il se connecte à un état arrêté](#)
- [Gnome se bloque sur les bundles WorkSpaces Ubuntu après la connexion](#)

Je ne parviens pas à créer un Amazon Linux WorkSpace car le nom d'utilisateur contient des caractères non valides

Pour Amazon Linux WorkSpaces, noms d'utilisateur :

- Peuvent contenir un maximum de 20 caractères
- Peuvent contenir des lettres, des espaces et des chiffres qui sont représentables en UTF-8
- Peuvent inclure les caractères spéciaux suivants : _ -#
- Impossible de commencer par un tiret (-) comme premier caractère du nom d'utilisateur

 Note

Ces restrictions ne s'appliquent pas à Windows WorkSpaces. Windows WorkSpaces prend en charge les symboles @ et - pour tous les caractères du nom d'utilisateur.

J'ai changé le shell de mon Amazon Linux WorkSpace et je ne peux plus configurer de session PCo IP

Pour remplacer le shell par défaut pour Linux WorkSpaces, consultez [Remplacer le shell par défaut pour Amazon Linux WorkSpaces](#).

Mon Amazon Linux WorkSpaces ne démarre pas

À partir du 20 juillet 2020, Amazon Linux WorkSpaces utilisera de nouveaux certificats de licence. Ces nouveaux certificats sont compatibles uniquement avec les versions 2.14.1.1, 2.14.7, 2.14.9 et 20.10.6 ou ultérieures de l'agent IP. PCo

Si vous utilisez une version non prise en charge de l'agent PCo IP, vous devez la mettre à niveau vers la dernière version (20.10.6), qui contient les derniers correctifs et améliorations de performances compatibles avec les nouveaux certificats. Si vous n'effectuez pas ces mises à niveau avant le 20 juillet, le provisionnement des sessions pour votre système Linux WorkSpaces échouera et vos utilisateurs finaux ne pourront pas se connecter à leur WorkSpaces système.

Pour mettre à niveau votre agent PCo IP vers la dernière version

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le panneau de navigation, sélectionnez WorkSpaces.
3. Sélectionnez votre système Linux WorkSpace, puis redémarrez-le en choisissant Actions, Redémarrer WorkSpaces. Si le WorkSpace statut est STOPPED, vous devez choisir Actions, démarrer d' WorkSpacesabord et attendre que son état soit AVAILABLE rétabli avant de pouvoir le redémarrer.
4. Une fois WorkSpace que vous avez redémarré et que son statut est AVAILABLE rétabli, nous vous recommandons de modifier le statut du WorkSpace to ADMIN_MAINTENANCE pendant que vous effectuez cette mise à niveau. Lorsque vous avez terminé, modifiez le statut du WorkSpace àAVAILABLE. Pour plus d'informations sur le mode ADMIN_MAINTENANCE, consultez [Maintenance manuelle](#).

Pour modifier le statut d'un WorkSpace enADMIN_MAINTENANCE, procédez comme suit :

- a. Sélectionnez WorkSpace et choisissez Actions, Modifier WorkSpace.
 - b. Choisissez Modify State (Modifier l'état).
 - c. Pour État prévu, sélectionnez ADMIN_MAINTENANCE.
 - d. Sélectionnez Modifier.
5. Connectez-vous à votre système Linux WorkSpace via SSH. Pour de plus amples informations, veuillez consulter [Activez les connexions SSH pour votre Linux WorkSpaces dans Personal WorkSpaces](#).
 6. Pour mettre à jour l'agent PCo IP, exécutez la commande suivante :

```
sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
```

7. Pour vérifier la version de l'agent et confirmer la réussite de la mise à jour, exécutez la commande suivante :

```
rpm -q pcoip-agent-standard
```

La commande de vérification doit produire le résultat suivant :

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. Déconnectez-vous du WorkSpace et redémarrez-le à nouveau.

9. Si vous définissez le statut du WorkSpace to ADMIN_MAINTENANCE in [Step 4](#), répétez l'opération [Step 4](#) et définissez l'état prévu sur AVAILABLE.

Si votre système Linux ne démarre WorkSpace toujours pas après la mise à niveau de l'agent PCo IP, contactez le AWS Support.

Le lancement WorkSpaces dans mon répertoire connecté échoue souvent

Vérifiez que les deux serveurs DNS ou les contrôleurs de domaine de votre annuaire sur site sont accessibles à partir de chacun des sous-réseaux que vous avez spécifiés lorsque vous vous êtes connecté à votre annuaire. Vous pouvez vérifier cette connectivité en lançant une instance Amazon EC2 dans chaque sous-réseau, et en associant l'instance à votre annuaire en utilisant les adresses IP des deux serveurs DNS.

Le lancement WorkSpaces échoue avec une erreur interne

Vérifiez si vos sous-réseaux sont configurés pour attribuer automatiquement IPv6 des adresses aux instances lancées dans le sous-réseau. Pour vérifier ce paramètre, ouvrez la console Amazon VPC, sélectionnez votre sous-réseau, puis choisissez Actions de sous-réseau (subnet), puis Modifier les paramètres d'attribution automatique d'adresses IP. Si ce paramètre est activé, vous ne pouvez pas démarrer WorkSpaces à l'aide des packs Performance ou Graphics. Désactivez plutôt ce paramètre et spécifiez IPv6 les adresses manuellement lorsque vous lancez vos instances.

Lorsque j'essaie d'enregistrer un annuaire, l'enregistrement échoue et laisse l'annuaire avec l'état ERREUR

Ce problème peut se produire si vous essayez d'enregistrer un répertoire Microsoft AD AWS géré qui a été configuré pour la réplication multirégionale. Bien que l'annuaire de la région principale puisse être enregistré avec succès pour être utilisé auprès d'Amazon WorkSpaces, la tentative d'enregistrement du répertoire dans une région répliquée échoue. La réplication multirégionale avec AWS Managed Microsoft AD n'est pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.

Mes utilisateurs ne peuvent pas se connecter à un système Windows WorkSpace doté d'une bannière de connexion interactive

Si un message d'ouverture de session interactif a été implémenté pour afficher une bannière de connexion, cela empêche les utilisateurs d'accéder à leur Windows. WorkSpaces Le paramètre de

stratégie de groupe du message d'ouverture de session interactif n'est actuellement pas pris en charge par PCo IP WorkSpaces. Déplacez le WorkSpaces vers une unité organisationnelle (UO) où la politique de Interactive logon: Message text for users attempting to log on groupe n'est pas appliquée. Le message de connexion est pris en charge sur DCV WorkSpaces, et les utilisateurs doivent se reconnecter après avoir accepté la bannière de connexion.

Mes utilisateurs ne peuvent pas se connecter à un système Windows Workspace

Mes utilisateurs reçoivent le message d'erreur suivant lorsqu'ils essaient de se connecter à leur système Windows WorkSpaces :

"An error occurred while launching your Workspace. Please try again."

Cette erreur se produit souvent lorsqu'il est Workspace impossible de charger le bureau Windows à l'aide de l' PCoadresse IP. Vérifiez les éléments suivants :

- Ce message apparaît si le service PCo IP Standard Agent pour Windows n'est pas en cours d'exécution. [Connectez-vous à l'aide de RDP](#) pour vérifier que le service est en cours d'exécution, qu'il est configuré pour démarrer automatiquement et qu'il peut communiquer via l'interface de gestion (eth0).
- Si l'agent PCo IP a été désinstallé, redémarrez-le Workspace via la WorkSpaces console Amazon pour le réinstaller automatiquement.
- Vous pouvez également recevoir cette erreur sur le WorkSpaces client Amazon après un long délai si le [groupe WorkSpaces de sécurité](#) a été modifié pour restreindre le trafic sortant. La restriction du trafic sortant empêche Windows de communiquer avec vos contrôleurs d'annuaire pour la connexion. Vérifiez que vos groupes de sécurité vous permettent WorkSpaces de communiquer avec vos contrôleurs d'annuaire sur tous les [ports requis](#) via l'interface réseau principale.

Une autre cause de cette erreur est liée à la stratégie de groupe d'attribution de droits d'utilisateur. Si la stratégie de groupe suivante n'est pas correctement configurée, elle empêche les utilisateurs d'accéder à leur Windows WorkSpaces :

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment
(Configuration de l'ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales
Attribution des droits utilisateur)

- Stratégie erronées :

Stratégie : Acces this computer from the network (Accéder à cet ordinateur à partir du réseau)

Paramètre : *Domain name* \ Domain Computers

GPO gagnant : Autoriser l'accès au fichier

- Stratégie correcte :

Stratégie : Acces this computer from the network (Accéder à cet ordinateur à partir du réseau)

Paramètre : *Domain name* \ Utilisateurs du domaine

GPO gagnant : Autoriser l'accès au fichier

 Note

Ce paramètre de stratégie doit être appliqué aux Domain Users (Utilisateurs de domaine) au lieu des Domain Computers (Ordinateurs de domaine).

Pour plus d'informations, consultez [Accès à cet ordinateur à partir du réseau - Paramètre de stratégie de sécurité](#) et [Configurer les paramètres de stratégie de sécurité](#) dans la documentation Microsoft Windows.

Mes utilisateurs rencontrent des problèmes lorsqu'ils essaient de se connecter WorkSpaces à WorkSpaces Web Access

Amazon WorkSpaces s'appuie sur une configuration d'écran de connexion spécifique pour permettre aux utilisateurs de se connecter correctement depuis leur client Web Access.

Pour permettre aux utilisateurs de Web Access de se connecter à leur compte WorkSpaces, vous devez configurer un paramètre de stratégie de groupe et trois paramètres de stratégie de sécurité. Si ces paramètres ne sont pas correctement configurés, les utilisateurs peuvent rencontrer de longs délais de connexion ou des écrans noirs lorsqu'ils essaient de se connecter à leur WorkSpaces. Pour configurer ces paramètres, veuillez consulter [Activer et configurer WorkSpaces Web Access for WorkSpaces Personal](#).

 Important

À compter du 1er octobre 2020, les clients ne pourront plus utiliser le client Amazon WorkSpaces Web Access pour se connecter à Windows 7 personnalisé WorkSpaces ou à Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Le WorkSpaces client Amazon affiche un écran gris « Chargement... » pendant un moment avant de revenir à l'écran de connexion. Aucun autre message d'erreur ne s'affiche.

Ce comportement indique généralement que le WorkSpaces client peut s'authentifier via le port 443, mais ne peut pas établir de connexion de streaming via le port 4172 (PCoIP) ou le port 4195 (DCV). Cette situation peut se produire lorsque les [conditions préalables réseau](#) ne sont pas remplies. Les problèmes côté client provoquent souvent l'échec de la surveillance réseau au niveau du client. Pour voir quelles actions de surveillance de l'état échouent, choisissez l'icône de surveillance réseau (généralement un triangle rouge avec un point d'exclamation, situé dans le coin inférieur droit de l'écran de connexion pour les clients version 2.0+, ou l'icône réseau

située dans le coin supérieur droit pour les clients version 3.0+).

 Note

La cause la plus fréquente de ce problème est un pare-feu côté client ou un proxy empêchant l'accès via le port 4172 ou 4195 (TCP et UDP). Si ce contrôle d'intégrité échoue, vérifiez les paramètres de votre pare-feu local.

Si la vérification du réseau réussit, il se peut qu'il y ait un problème de configuration réseau du Workspace. Par exemple, une règle de pare-feu Windows peut bloquer le port UDP 4172 ou 4195 dans l'interface de gestion. [Connectez-vous à l' Workspace aide d'un client RDP \(Remote Desktop Protocol\)](#) pour vérifier qu'il Workspace répond aux [exigences de port](#) nécessaires.

Mes utilisateurs reçoivent le message « WorkSpace Status : Unhealthy ». Nous n'avons pas pu vous connecter à votre WorkSpace. Veuillez réessayer dans quelques minutes. ».

Cette erreur indique généralement que le SkyLightWorkSpacesConfigService service ne répond pas aux tests de santé.

Si vous venez de redémarrer ou de démarrer votre WorkSpace, attendez quelques minutes, puis réessayez.

Si le service est en cours d'exécution WorkSpace depuis un certain temps et que le message d'erreur persiste, [connectez-vous à l'aide du protocole RDP](#) pour vérifier que le SkyLightWorkSpacesConfigService service :

- Est en cours d'exécution.
- Est configuré pour démarrer automatiquement.
- Peut communiquer via l'interface de gestion (eth0).
- N'est pas bloqué par un logiciel antivirus tiers.

Mes utilisateurs reçoivent le message « Cet appareil n'est pas autorisé à accéder au WorkSpace. Contactez votre administrateur pour obtenir de l'aide. »

Cette erreur indique que l'une des situations suivantes peut se produire :

- Les [groupes de contrôle d'accès IP](#) sont configurés WorkSpace dans l'annuaire, mais l'adresse IP du client n'est pas autorisée.

Vérifiez les paramètres de votre répertoire. Vérifiez que l'adresse IP publique à partir de laquelle l'utilisateur se connecte autorise l'accès au WorkSpace.

- Dans le cadre du contrôle d'accès, le système d'exploitation de votre appareil n'est pas autorisé en tant qu'appareil fiable ou les certificats appropriés ne sont pas installés sur votre appareil lorsque vous utilisez l'option Appareils fiables. Ajoutez votre type d'appareil en tant qu'appareil de confiance en procédant comme suit :

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
 2. Dans le volet de navigation, choisissez Directories (Annuaire).
 3. Choisissez le répertoire que vous utilisez.
 4. Faites défiler la page jusqu'à Options de contrôle d'accès, puis sélectionnez Modifier.
 5. Sous Appareils fiables, pour les types d'appareils auxquels vous souhaitez autoriser l'accès, choisissez Tout autoriser dans le menu déroulant. Si vous souhaitez limiter les appareils à ceux sur lesquels des certificats clients sont installés, choisissez Appareils fiables.
 6. Si vous avez choisi Appareils fiables à l'étape précédente, assurez-vous d'avoir importé au moins un certificat racine et que le certificat client émis par l'autorité de certification racine (CA) a été installé sur le client. Pour plus d'informations sur la création, le déploiement et l'importation de certificats racines, consultez [Restreindre l'accès aux appareils fiables pour les WorkSpaces particuliers](#).
 7. Choisissez Enregistrer.
- L'accès à vos types d'appareils n'est pas autorisé WorkSpaces. Accordez l'accès à votre type d'appareil en procédant comme suit :
 1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
 2. Dans le volet de navigation, choisissez Directories (Annuaire).
 3. Choisissez le répertoire que vous utilisez.
 4. Faites défiler la page jusqu'à Autres plateformes, puis sélectionnez Modifier.
 5. Sélectionnez l'un des types d'appareils suivants pour lesquels vous souhaitez accorder WorkSpaces l'accès.
 - ChromeOS
 - iOS
 - Linux
 - Web Access
 - Zéro client
 6. Choisissez Enregistrer.

Les utilisateurs reçoivent le message « No network. Network connection lost. Check your network connection or contact your administrator for help. » lorsque vous essayez de vous connecter à un DCV WorkSpace

Si cette erreur se produit et que les utilisateurs ne rencontrent aucun problème de connectivité, assurez-vous que le port 4195 est ouvert sur les pare-feux de votre réseau. Pour WorkSpaces l'utilisation de DCV, le port utilisé pour diffuser la session client est passé de 4172 à 4195.

Le WorkSpaces client envoie une erreur réseau à mes utilisateurs, mais ils peuvent utiliser d'autres applications connectées au réseau sur leurs appareils

Les applications WorkSpaces clientes dépendent de l'accès aux ressources du AWS cloud et nécessitent une connexion fournissant une bande passante de téléchargement d'au moins 1 Mbits/s. Si un appareil dispose d'une connexion intermittente au réseau, l'application WorkSpaces cliente peut signaler un problème avec le réseau.

WorkSpaces impose l'utilisation de certificats numériques émis par Amazon Trust Services à compter de mai 2018. Amazon Trust Services est déjà une CA racine de confiance sur les systèmes d'exploitation qui sont pris en charge par WorkSpaces. Si la liste des autorités de certification racine du système d'exploitation n'est pas à jour, l'appareil ne peut pas se connecter WorkSpaces et le client génère une erreur réseau.

Pour reconnaître les problèmes de connexion dus à des échecs de certificat

- PCoClients IP zéro : le message d'erreur suivant s'affiche.

```
Failed to connect. The server provided a certificate that is invalid. See below for details:
```

- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store

- Autres clients – Les surveillances de l'état échouent, affichant un triangle d'avertissement rouge pour Internet.

Pour résoudre les échecs de certificat

- [Application client Windows](#)
- [PCoClients sans adresse IP](#)
- [Autres applications client](#)

Application client Windows

Utilisez l'une des solutions suivantes pour les échecs de certificat.

Solution 1 : Mettre à jour l'application client

Téléchargez et installez la dernière application client Windows depuis <https://clients.amazonworkspaces.com/>. Pendant l'installation, l'application client s'assure que votre système d'exploitation approuve les certificats émis par Amazon Trust Services.

Solution 2 : Ajouter Amazon Trust Services à la liste de CA racine locale

1. Ouvrir <https://www.amazontrust.com/repository/>.
2. Téléchargez le certificat Starfield au format DER (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Ouvrez la console de gestion Microsoft. (À partir de l'invite de commande, exécutez mmc.)
4. Choisissez Fichier, Ajouter/Supprimer un composant logiciel enfichable, Certificats, Ajouter.
5. Sur la page Composant logiciel enfichable Certificats, sélectionnez Un compte d'ordinateur et choisissez Suivant. Conservez la valeur par défaut, Ordinateur local. Choisissez Finish (Terminer). Choisissez OK.
6. Développez Certificats (ordinateur local) et sélectionnez Autorités de certification racines de confiance. Choisissez Action, Toutes les tâches, Importer.
7. Suivez l'assistant pour importer le certificat que vous avez téléchargé.
8. Quittez et redémarrez l'application WorkSpaces cliente.

Solution 3 : Déployer Amazon Trust Services en tant que CA (autorité de certification) approuvée à l'aide d'une stratégie de groupe

Ajoutez le certificat Starfield à la racine approuvée du domaine à CAs l'aide de la stratégie de groupe. Pour plus d'informations, consultez [Use Policy to Distribute Certificates](#).

PCoClients sans adresse IP

Pour vous connecter directement à un microprogramme à Workspace l'aide de la version 6.0 ou ultérieure, téléchargez et installez le certificat émis par Amazon Trust Services.

Pour ajouter Amazon Trust Services en tant que CA racine approuvée

1. Ouvrez <https://certs.secureserver.net/repository/>.

2. Téléchargez le certificat sous Starfield Certificate Chain (Chaîne de certificats Starfield) avec l'empreinte numérique 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58.
3. Chargez le certificat sur le client Zero. Pour plus d'informations, consultez [Uploading Certificates](#) dans la documentation Teradici.

Autres applications client

Ajoutez le certificat Starfield

(2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) depuis [Amazon Trust Services](#). Pour plus d'informations sur l'ajout d'une CA racine, consultez la documentation suivante :

- Android : [Add & remove certificates](#)
- Chrome OS : [Manage client certificates on Chrome devices](#)
- macOS et iOS : [Installing a CA's Root Certificate on Your Test Device](#)

Mes WorkSpace utilisateurs voient le message d'erreur suivant : « L'appareil ne peut pas se connecter au service d'enregistrement. Veuillez vérifier vos paramètres réseau. »

En cas de défaillance du service d'enregistrement, vos WorkSpace utilisateurs peuvent voir le message d'erreur suivant s'afficher sur la page Connection Health Check : « Votre appareil ne parvient pas à se connecter au service WorkSpaces d'enregistrement. Vous ne pourrez pas enregistrer votre appareil auprès de WorkSpaces. Veuillez vérifier vos paramètres réseau."

Cette erreur se produit lorsque l'application WorkSpaces cliente ne parvient pas à atteindre le service d'enregistrement. Cela se produit généralement lorsque le WorkSpaces répertoire a été supprimé. Pour résoudre cette erreur, assurez-vous que le code d'enregistrement est valide et correspond à un répertoire actif dans le AWS Cloud.

Les utilisateurs du client My PCo IP Zero reçoivent le message d'erreur « Le certificat fourni n'est pas valide en raison de l'horodatage »

Si le protocole NTP (Network Time Protocol) n'est pas activé dans Teradici, les utilisateurs de votre client PCo IP zéro risquent de recevoir des erreurs de certificat. Pour configurer NTP, consultez [Configurer des clients PCo IP zéro pour WorkSpaces Personal](#).

Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients PCo IP zéro

À partir de la version 20.10.4 de l'agent PCo IP, Amazon WorkSpaces désactive la redirection USB par défaut via le registre Windows. Ce paramètre de registre affecte le comportement des périphériques USB lorsque vos utilisateurs utilisent des appareils clients PCo IP zéro pour se connecter à leur WorkSpaces.

Si vous WorkSpaces utilisez la version 20.10.4 ou ultérieure de l'agent PCo IP, les périphériques USB ne fonctionneront pas avec les périphériques clients PCo IP zéro tant que vous n'aurez pas activé la redirection USB.

Note

Si vous utilisez des pilotes d'imprimante virtuelle 32 bits, vous devez également les mettre à jour vers leur version 64 bits.

Pour activer la redirection USB pour les appareils clients PCo IP zéro

Nous vous recommandons d'appliquer ces modifications de registre à votre compte par le WorkSpaces biais de la politique de groupe. Pour plus d'informations, consultez les rubriques [Configuring the agent](#) et [Configurable settings](#) dans la documentation Teradici.

1. Définissez la valeur de clé de registre suivante sur 1 (activé) :

KeyPath = HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Teradici \ IP \ pcoip_admin PCo

KeyName = pcoip.enable_usb

KeyType = MOT D

KeyValue = 1

2. Définissez la valeur de clé de registre suivante sur 1 (activé) :

KeyPath = HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Teradici \ IP \
pcoip_admin_defaults PCo

KeyName = pcoip.enable_usb

KeyType = MOT D

KeyValue = 1

3. Si ce n'est pas déjà fait, déconnectez-vous du WorkSpace, puis reconnectez-vous. Les périphériques USB devraient maintenant fonctionner.

Mes utilisateurs ont ignoré la mise à jour de leurs applications client Windows ou macOS et ne sont pas invités à installer la dernière version

Lorsque les utilisateurs ignorent les mises à jour de l'application client Amazon WorkSpaces Windows, la clé de SkipThisVersionregistre est définie et ils ne sont plus invités à mettre à jour leurs clients lorsqu'une nouvelle version du client est publiée. Pour effectuer la mise à jour vers la dernière version, vous pouvez modifier le registre comme décrit dans la section [Mettre à jour l'application cliente WorkSpaces Windows vers une version plus récente](#) du guide de WorkSpaces l'utilisateur Amazon. Vous pouvez également exécuter la PowerShell commande suivante :

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces  
\WinSparkle" -Name "SkipThisVersion"
```

Lorsque les utilisateurs ignorent les mises à jour de l'application cliente Amazon WorkSpaces macOS, la SUSkippedVersion préférence est définie et ils ne sont plus invités à mettre à jour leurs clients lorsqu'une nouvelle version du client est publiée. Pour passer à la dernière version, vous pouvez réinitialiser cette préférence comme décrit dans la section [Mettre à jour l'application cliente WorkSpaces macOS vers une version plus récente](#) du guide de WorkSpaces l'utilisateur Amazon.

Mes utilisateurs ne peuvent pas installer l'application client Android sur leurs Chromebooks

La version 2.4.13 est la version finale de l'application client Amazon WorkSpaces Chromebook. Étant donné [que Google supprime progressivement le support pour Chrome Apps](#), aucune autre mise à jour ne sera apportée à l'application cliente WorkSpaces Chromebook, et son utilisation n'est pas prise en charge.

Pour les [Chromebooks qui prennent en charge l'installation d'applications Android](#), nous recommandons d'utiliser plutôt l'[application cliente WorkSpaces Android](#).

Dans certains cas, vous devrez peut-être activer les Chromebooks de vos utilisateurs pour installer des applications Android. Pour de plus amples informations, veuillez consulter [Configurer Android pour Chromebook for Personal WorkSpaces](#).

Mes utilisateurs ne reçoivent pas d'e-mails d'invitation ou d'e-mails de réinitialisation de mot de passe

Les utilisateurs ne reçoivent pas automatiquement d'e-mails de bienvenue ou de réinitialisation de WorkSpaces mot de passe créés à l'aide d'AD Connector ou d'un domaine approuvé. Les e-mails d'invitation ne sont pas non plus envoyés automatiquement si l'utilisateur existe déjà dans Active Directory.

Pour envoyer manuellement des e-mails de bienvenue à ces utilisateurs, consultez [Envoi d'un e-mail d'invitation](#).

Pour réinitialiser les mots de passe utilisateur, veuillez consulter [Configuration des outils d'administration Active Directory pour le WorkSpaces personnel](#).

Mes utilisateurs ne voient pas l'option « Mot de passe oublié ? » sur l'écran de connexion du client

Si vous utilisez AD Connector ou un domaine de confiance, les utilisateurs ne pourront pas réinitialiser leurs propres mots de passe. (Le mot de passe oublié ? l'option sur l'écran de connexion de l'application WorkSpaces cliente ne sera pas disponible.) Pour plus d'informations sur la réinitialisation des mots de passe utilisateur, veuillez consulter [Configuration des outils d'administration Active Directory pour le WorkSpaces personnel](#).

Je reçois le message « L'administrateur système a défini des politiques pour empêcher cette installation » lorsque j'essaie d'installer des applications sur un système Windows WorkSpace

Vous pouvez résoudre ce problème en modifiant le paramètre de stratégie de groupe Windows Installer. Pour déployer cette politique sur plusieurs sites WorkSpaces de votre annuaire, appliquez ce paramètre à un objet de stratégie de groupe lié à l'unité WorkSpaces organisationnelle (UO) à partir d'une instance EC2 jointe à un domaine. Si vous utilisez AD Connector, vous pouvez effectuer ces modifications à partir d'un contrôleur de domaine. Pour plus d'informations sur l'utilisation des outils d'administration Active Directory pour travailler avec des objets de stratégie de groupe, consultez [Installation des outils d'administration Active Directory](#) du Guide d'administration AWS Directory Service .

La procédure suivante indique comment configurer le paramètre Windows Installer pour l'objet de stratégie de WorkSpaces groupe.

1. Assurez-vous que le [modèle d'administration de stratégie de groupe WorkSpaces](#) le plus récent est installé dans votre domaine.
2. Ouvrez l'outil de gestion des stratégies de groupe sur votre WorkSpace client Windows, naviguez jusqu'à l'objet de stratégie de WorkSpaces groupe et sélectionnez-le pour les comptes de votre WorkSpaces machine. Dans le menu principal, choisissez Action, Edition.
3. Dans l'éditeur de gestion des stratégies de groupe, choisissez Computer Configuration (Configuration de l'ordinateur), Politiques (Stratégies), Administrative Templates (Modèles d'administration), Classic Administrative Templates (Modèles d'administration classiques), Windows Components (Composants Windows), Windows Installer.
4. Ouvrez le paramètre Turn Off Windows Installer (Désactiver le programme d'installation Windows).
5. Dans la boîte de dialogue Turn Off Windows Installer (Désactiver le programme d'installation Windows) remplacez Not Configured (Non configuré) par Enabled (Activé), puis définissez Disable Windows Installer (Désactiver le programme d'installation Windows) sur Never (Jamais).
6. Choisissez OK.
7. Pour appliquer les modifications de stratégie de groupe, effectuez l'une des actions suivantes :
 - Redémarrez le WorkSpace (dans la WorkSpaces console, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).
 - À partir d'une invite de commande administrative, entrez `gpupdate /force`.

Non WorkSpaces , dans mon annuaire, je ne peux pas me connecter à Internet

WorkSpaces ne peut pas communiquer avec Internet par défaut. Vous devez fournir explicitement l'accès Internet. Pour de plus amples informations, veuillez consulter [Fournir un accès à Internet pour les WorkSpaces particuliers](#).

Mon accès à Internet WorkSpace a été perdu

Si vous avez WorkSpace perdu l'accès à Internet et que vous ne pouvez pas vous y [connecter à l' WorkSpace aide du protocole RDP](#), ce problème est probablement dû à la perte de l'adresse IP publique du WorkSpace. Si vous avez [activé l'attribution automatique des adresses IP élastiques](#) au niveau du répertoire, une [adresse IP élastique](#) (issue du pool fourni par Amazon) vous est attribuée WorkSpace lors de son lancement. Toutefois, si vous associez une adresse IP élastique que vous possédez à un WorkSpace, puis que vous dissociez ensuite cette adresse IP élastique du WorkSpace, celui-ci WorkSpace perd son adresse IP publique et n'en obtient pas automatiquement une nouvelle depuis le pool fourni par Amazon.

Pour associer une nouvelle adresse IP publique provenant du pool fourni par Amazon au WorkSpace, vous devez [reconstruire](#) le WorkSpace. Si vous ne souhaitez pas reconstruire le WorkSpace, vous devez associer une autre adresse IP élastique que vous possédez au WorkSpace.

Nous vous recommandons de ne pas modifier l'interface Elastic network d'un WorkSpace après son lancement. Une fois qu'une adresse IP élastique a été attribuée à un WorkSpace, celui-ci conserve la même adresse IP publique (sauf si elle est reconstruite, auquel cas il obtient une nouvelle adresse IP publique).

L'erreur « DNS unavailable » s'affiche lorsque j'essaie de me connecter à mon annuaire sur site

Un message d'erreur similaire à ce qui suit s'affiche lors de la connexion à votre annuaire sur site :

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

La passerelle AD Connector doit être capable de communiquer avec vos serveurs DNS sur site via les protocoles TCP et UDP sur le port 53. Vérifiez que vos groupes de sécurité et pare-feu sur site autorisent la communication TCP et UDP sur ce port.

L'erreur « Connectivity issues detected » s'affiche lorsque je tente de me connecter à mon annuaire sur site

Un message d'erreur similaire à ce qui suit s'affiche lors de la connexion à votre annuaire sur site :

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address  
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address  
Please ensure that the listed ports are available and retry the operation.
```

La passerelle AD Connector doit être capable de communiquer avec vos contrôleurs de domaine sur site via les protocoles TCP et UDP sur les ports suivants. Vérifiez que vos groupes de sécurité et pare-feu sur site autorisent la communication TCP et UDP sur ces ports :

- 88 (Kerberos)
- 389 (LDAP)

L'erreur « SRV record » s'affiche lorsque je tente de me connecter à mon annuaire sur site

Un message d'erreur similaire à un ou plusieurs des messages suivants s'affiche lors de la connexion à votre annuaire sur site :

```
SRV record for LDAP does not exist for IP: dns-ip-address
```

```
SRV record for Kerberos does not exist for IP: dns-ip-address
```

La passerelle AD Connector doit obtenir les enregistrements SRV `_ldap._tcp.dns-domain-name` et `_kerberos._tcp.dns-domain-name` lors de la connexion à votre annuaire. Cette erreur s'affiche si le service ne peut pas obtenir ces enregistrements auprès des serveurs DNS que vous avez spécifiés lors de la connexion à votre annuaire. Assurez-vous que vos serveurs DNS contiennent ces enregistrements SRV. Pour plus d'informations, consultez [SRV Resource Records](#) sur Microsoft TechNet.

Mon Windows WorkSpace se met en veille lorsqu'il est laissé inactif

Pour résoudre ce problème, connectez-vous au mode de gestion de l'alimentation WorkSpace et modifiez-le en mode Haute performance en suivant la procédure suivante :

1. Ouvrez le WorkSpace Panneau de configuration, puis sélectionnez Matériel ou Matériel et audio (le nom peut varier en fonction de votre version de Windows).
2. Sous Power Options (Options d'alimentation), choisissez Choose a power plan (Choisir un plan d'alimentation).
3. Dans le panneau Choisir ou personnaliser un mode de gestion de l'alimentation, choisissez le mode d'alimentation Performances élevées, puis choisissez Modifier les paramètres du mode.
 - Si l'option permettant de choisir le mode d'alimentation Performances élevées est désactivée, choisissez Modifier des paramètres actuellement non disponibles, puis choisissez le mode d'alimentation Performances élevées.
 - Si le mode Performances élevées n'est pas visible, cliquez sur la flèche à droite de Afficher les modes supplémentaires pour l'afficher, ou choisissez Créer un mode de gestion de l'alimentation dans le menu de navigation de gauche, choisissez Performances élevées, nommez le mode d'alimentation, puis cliquez sur Suivant.
4. Sur la page Modifier les paramètres du mode : Performances élevées, assurez-vous que les paramètres Éteindre l'écran et (le cas échéant) Mettre l'ordinateur en veille sont définis à Jamais.

5. Si vous avez apporté des modifications au mode Performances élevées, choisissez Enregistrer les modifications (ou choisissez Créer si vous créez un nouveau mode).

Si les étapes précédentes ne permettent pas de résoudre le problème, procédez comme suit :

1. Ouvrez le WorkSpace Panneau de configuration, puis sélectionnez Matériel ou Matériel et audio (le nom peut varier en fonction de votre version de Windows).
2. Sous Power Options (Options d'alimentation), choisissez Choose a power plan (Choisir un plan d'alimentation).
3. Dans le volet Choose or customize a power plan (Choisir ou personnaliser un plan d'alimentation), choisissez le lien Change plan settings (Choisir les paramètres du plan) à droite du plan d'alimentation High performance (Hautes performances), puis choisissez le lien Change advanced power settings (Modifier les paramètres d'alimentation avancés).
4. Dans la boîte de dialogue Power Options (Options d'alimentation), dans la liste des paramètres, choisissez le signe plus à gauche de Hard disk (Disque dur) pour afficher les paramètres appropriés.
5. Vérifiez que valeur Turn off hard disk after (Désactiver le disque dur après) pour Plugged in (Sur secteur) est supérieure à celle de On battery (Sur batterie) (la valeur par défaut est de 20 minutes).
6. Choisissez le signe plus à gauche de PCI Express et faites de même pour Link State Power Management.
7. Vérifiez que les paramètres Link State Power Management sont définis sur Off (Désactivé).
8. Choisissez OK (ou Apply (Appliquer) si vous avez modifié le moindre paramètre) pour fermer la boîte de dialogue.
9. Dans le volet Change settings for the plan (Modifier les paramètres du plan), si vous avez modifié le moindre paramètre, choisissez Enregistrer les modifications.

L'un des WorkSpaces miens a un état de **UNHEALTHY**

Le WorkSpaces service envoie périodiquement des demandes de statut à un WorkSpace. A WorkSpace est marqué UNHEALTHY lorsqu'il ne répond pas à ces demandes. Les causes courantes de ce problème sont les suivantes :

- Une application installée sur le WorkSpace bloque les ports réseau, ce qui l'WorkSpace empêche de répondre à la demande d'état.

- L'utilisation élevée du processeur des WorkSpaces empêche de répondre à la demande d'état en temps opportun.
- Le nom de l'ordinateur WorkSpace a été modifié. Cela empêche l'établissement d'un canal sécurisé entre WorkSpaces et le WorkSpace.

Vous pouvez tenter de remédier à cette situation à l'aide des méthodes suivantes :

- Redémarrez le WorkSpace depuis la WorkSpaces console.
- Connectez-vous au système WorkSpace défaillant à l'aide de la procédure suivante, qui ne doit être utilisée qu'à des fins de dépannage :
 1. Connectez-vous à un opérateur situé WorkSpace dans le même répertoire que celui qui ne fonctionne pas correctement WorkSpace.
 2. À partir du mode opérationnel WorkSpace, utilisez le protocole RDP (Remote Desktop Protocol) pour vous connecter à l'appareil défectueux WorkSpace en utilisant l'adresse IP du périphérique non fonctionnel. WorkSpace En fonction de l'ampleur du problème, il se peut que vous ne puissiez pas vous connecter au système défaillant WorkSpace.
 3. Si le port est WorkSpace défectueux, vérifiez que les [exigences minimales en matière de port](#) sont respectées.
- Assurez-vous que le SkyLightWorkSpacesConfigService service peut répondre aux bilans de santé. Pour résoudre ce problème, consultez [Mes utilisateurs reçoivent le message « WorkSpace Status : Unhealthy ». Nous n'avons pas pu vous connecter à votre WorkSpace. Veuillez réessayer dans quelques minutes. »..](#)
- WorkSpace Reconstructez-le depuis la WorkSpaces console. Étant donné que la reconstruction d'un fichier WorkSpace peut entraîner une perte de données, cette option ne doit être utilisée que si toutes les autres tentatives de résolution du problème ont échoué.

Mon ordinateur WorkSpace se bloque ou redémarre de façon inattendue

Si votre WorkSpace configuration pour PCo IP se bloque ou redémarre à plusieurs reprises et que vos journaux d'erreurs ou vos crash dumps indiquent des problèmes spacedeskHookKmode.sys ou spacedeskHookUmode.dll, ou si vous recevez les messages d'erreur suivants, vous devrez peut-être désactiver l'accès Web au : WorkSpace

```
The kernel power manager has initiated a shutdown transition.  
Shutdown reason: Kernel API
```

The computer has rebooted from a bugcheck.

Note

- Ces étapes de dépannage ne s'appliquent pas aux WorkSpaces personnes configurées pour le DCV. Ils ne s'appliquent WorkSpaces qu'aux personnes configurées pour PCo IP.
- Vous devez désactiver Web Access uniquement si vous n'autorisez pas vos utilisateurs à utiliser Web Access.

Pour désactiver l'accès Web au Workspace, vous devez désactiver l'accès Web dans le WorkSpaces répertoire et redémarrer le Workspace.

Le même nom d'utilisateur en possède plusieurs Workspace, mais l'utilisateur ne peut se connecter qu'à l'un des WorkSpaces

Si vous supprimez un utilisateur dans Active Directory (AD) sans le supprimer au préalable, Workspace puis que vous le réajoutez à nouveau dans Active Directory et que vous en créez un nouveau Workspace pour cet utilisateur, le même nom d'utilisateur en aura désormais deux WorkSpaces dans le même répertoire. Toutefois, si l'utilisateur essaie de se connecter à son original Workspace, il recevra le message d'erreur suivant :

```
"Unrecognized user. No Workspace found under your username. Contact your administrator to request one."
```

De plus, les recherches sur le nom d'utilisateur dans la WorkSpaces console Amazon renvoient uniquement le nouveau Workspace, même si les deux existent WorkSpaces toujours. (Vous pouvez trouver l'original Workspace en recherchant l' Workspace identifiant au lieu du nom d'utilisateur.)

Ce comportement peut également se produire si vous renommez un utilisateur dans Active Directory sans le supprimer au préalable. Workspace Si vous remplacez ensuite leur nom d'utilisateur par le nom d'utilisateur d'origine et que vous en créez un nouveau Workspace pour l'utilisateur, le même nom d'utilisateur en contiendra deux WorkSpaces dans le répertoire.

Ce problème se produit, car Active Directory utilise l'identificateur de sécurité (SID), plutôt que le nom d'utilisateur, pour identifier de manière unique l'utilisateur. Lorsqu'un utilisateur est supprimé et recréé dans Active Directory, un nouveau SID lui est attribué, même si son nom d'utilisateur reste

le même. Lors de la recherche d'un nom d'utilisateur, la WorkSpaces console Amazon utilise le SID pour rechercher des correspondances dans Active Directory. Les WorkSpaces clients Amazon utilisent également le SID pour identifier les utilisateurs lorsqu'ils se connectent à WorkSpaces.

Pour résoudre ce problème, effectuez l'une des opérations suivantes :

- Si ce problème s'est produit, car l'utilisateur a été supprimé et recréé dans Active Directory, vous pouvez restaurer l'objet utilisateur supprimé d'origine si vous avez activé la [fonctionnalité Corbeille dans Active Directory](#). Si vous parvenez à restaurer l'objet utilisateur d'origine, assurez-vous que l'utilisateur peut se connecter à son objet d'origine WorkSpace. S'ils le peuvent, vous pouvez [supprimer le nouveau WorkSpace](#) fichier après avoir sauvegardé et transféré manuellement les données utilisateur du nouveau WorkSpace vers l'original WorkSpace (si nécessaire).
- Si vous ne parvenez pas à restaurer l'objet utilisateur [d'origine, supprimez-le WorkSpace](#). L'utilisateur doit être en mesure de se connecter à son nouveau et de l'utiliser à la WorkSpace place. Veillez à sauvegarder et à transférer manuellement toutes les données utilisateur de l'original WorkSpace vers le nouveau WorkSpace.

Warning

La suppression d'un WorkSpace est une action permanente qui ne peut pas être annulée. Les données de l' WorkSpace utilisateur ne sont pas conservées et sont détruites. Pour plus d'informations sur la sauvegarde des données utilisateur, contactez AWS Support.

Je ne parviens pas à utiliser Docker avec Amazon WorkSpaces

Fenêtres WorkSpaces

La virtualisation imbriquée (y compris l'utilisation de Docker) n'est pas prise en charge sous Windows. WorkSpaces Pour plus d'informations, consultez la [documentation Docker](#).

Linux WorkSpaces

Pour utiliser Docker sous Linux WorkSpaces, assurez-vous que les blocs CIDR utilisés par Docker ne se chevauchent pas avec les blocs CIDR utilisés dans les deux interfaces réseau élastiques (ENIs) associées au. WorkSpace Si vous rencontrez des problèmes lors de l'utilisation de Docker sous Linux WorkSpaces, contactez Docker pour obtenir de l'aide.

Je reçois ThrottlingException des erreurs lors de certains de mes appels d'API

Le taux autorisé par défaut pour les appels d' WorkSpaces API est un taux constant de deux appels d'API par seconde, avec un taux de « rafale » maximal autorisé de cinq appels d'API par seconde. Le tableau suivant montre comment la limite de débit de transmission en rafales fonctionne pour les demandes d'API.

Seconde	Nombre de demandes envoyées	Nombre net de demandes autorisé	Détails
1	0	5	Au cours de la première seconde (seconde 1), cinq demandes sont autorisées, avec un débit en rafale maximal de cinq appels par seconde.
2	2	5	Comme deux appels ou moins ont été émis pendant la seconde 1, la capacité totale de transmission en rafales de cinq appels est toujours disponible.
3	5	5	Étant donné que seulement deux appels ont été émis dans la seconde 2, la capacité totale de transmission en rafales de cinq appels est toujours disponible.
4	2	2	Comme, la capacité totale de transmission en rafales a été utilisée dans la seconde 3, seul le débit constant de deux appels par seconde est disponible.
5	3	2	Comme il ne reste pas de capacité de transmission en rafales, seuls deux appels sont autorisés pour l'instant . Cela signifie que l'un des trois appels d'API est limité. L'appel limité répondra après un court délai.
6	0	1	Comme l'un des appels de la seconde 5 fait l'objet d'une nouvelle tentative pendant la seconde 6, une capacité d'un seul appel supplémentaire est disponible pendant la seconde 6 en raison de la limite de débit constant de deux appels par seconde.

Seconde	Nombre de demandes envoyées	Nombre net de demandes autorisé	Détails
7	0	3	Maintenant que plus aucun appel d'API n'est limité dans la file d'attente, la limite de débit continue d'augmenter jusqu'à la limite de débit de transmission en rafales de cinq appels.
8	0	5	Comme aucun appel n'a été émis au cours de la seconde 7, le nombre maximal de demandes est autorisé.
9	0	5	Même si aucun appel n'a été émis au cours de la seconde 8, la limite de débit n'augmente pas au-delà de cinq.

Je WorkSpace continue de me déconnecter quand je le laisse fonctionner en arrière-plan

Pour les utilisateurs Mac, vérifiez si la fonctionnalité Power Nap est activée. Si elle est activée, cliquez pour la désactiver. Pour désactiver Power Nap, ouvrez votre terminal et exécutez la commande suivante :

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

La fédération SAML 2.0 ne fonctionne pas. Mes utilisateurs ne sont pas autorisés à streamer leur WorkSpaces ordinateur de bureau.

Cela peut se produire car la politique en ligne intégrée pour le rôle IAM de la fédération SAML 2.0 ne comprend pas les autorisations de streaming pour l'annuaire Amazon Resource Name (ARN). Le rôle IAM est assumé par l'utilisateur fédéré qui accède à un WorkSpaces annuaire. Modifiez les autorisations de rôle pour inclure l'ARN du répertoire et assurez-vous que l'utilisateur en possède un WorkSpace dans le répertoire. Pour plus d'informations, consultez [Authentification SAML 2.0](#) et [résolution des problèmes liés à la fédération SAML 2.0](#) avec AWS

Mes utilisateurs sont déconnectés de leur WorkSpaces session toutes les 60 minutes.

Si vous avez configuré l'authentification SAML 2.0 pour WorkSpaces, en fonction de votre fournisseur d'identité (IdP), vous devrez peut-être configurer les informations que l'IdP transmet sous forme d'attributs SAML dans le cadre de la réponse AWS d'authentification. Cela inclut la configuration de l'élément Attribute (Attribut) avec l'attribut SessionDuration défini sur `https://aws.amazon.com/SAML/Attributes/SessionDuration`.

L'attribut SessionDuration spécifie la durée maximale pendant laquelle une session de streaming fédérée peut rester active pour un utilisateur avant qu'une nouvelle authentification soit requise. Bien que l'attribut SessionDuration soit facultatif, nous vous recommandons de l'inclure dans la réponse d'authentification SAML. Si vous ne spécifiez pas cet attribut, la durée de session est définie par défaut à 60 minutes.

Pour résoudre ce problème, configurez votre IdP pour inclure la valeur SessionDuration dans la réponse d'authentification SAML et définissez la valeur comme nécessaire. Pour plus d'informations, consultez l'étape 5, [Create assertions for the SAML authentication response](#).

Mes utilisateurs reçoivent une erreur d'URI de redirection lorsqu'ils se fédèrent à l'aide du flux initié par le fournisseur d'identité (IdP) SAML 2.0, ou lorsqu'une instance supplémentaire de l'application WorkSpaces cliente démarre chaque fois que mes utilisateurs tentent de se connecter depuis le client après s'être fédérés avec l'IdP.

Cette erreur est due à une URL d'état de relais non valide. Assurez-vous que l'état du relais dans la configuration de votre fédération d'IdP est correct et que l'URL d'accès utilisateur et le nom du paramètre d'état du relais sont correctement configurés pour votre fédération d'IdP dans les propriétés du répertoire. WorkSpaces S'ils sont valides et que le problème persiste, contactez le AWS Support. Pour plus d'informations, consultez [Configuration SAML](#).

Mes utilisateurs reçoivent le message « Un problème s'est produit : une erreur s'est produite lors du lancement de votre application WorkSpace » lorsqu'ils tentent de se connecter à l'application WorkSpaces cliente après s'être fédérés avec l'IdP.

Examinez les assertions SAML 2.0 de votre fédération. La valeur SAML Subject NameID doit correspondre WorkSpaces au nom d'utilisateur et est généralement identique à l'attribut AMAccounts Name de l'utilisateur Active Directory. En outre, l'élément Attribute dont l'PrincipalTag:Emailattribut est défini sur `https://aws.amazon.com/SAML/Attributes/`

`PrincipalTag:Email` doit correspondre à l'adresse e-mail de WorkSpaces l'utilisateur telle que définie dans le WorkSpaces répertoire. Pour plus d'informations, consultez [Configuration SAML](#).

Mes utilisateurs reçoivent le message « Impossible de valider les balises » lorsqu'ils tentent de se connecter à l'application WorkSpaces cliente après s'être fédérés avec l'IdP.

Examinez les valeurs de l'attribut `PrincipalTag` dans les assertions SAML 2.0 de votre fédération, comme `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`. Les valeurs des balises peuvent inclure une combinaison des caractères `_ . : / = + - @`, de lettres, de chiffres et d'espaces. Pour plus d'informations, consultez les [sections Règles de balisage dans IAM](#) et. AWS STS

Les utilisateurs reçoivent le message suivant : « The client and the server cannot communicate, because they do not possess a common algorithm ».

Ce problème peut se produire si vous n'activez pas le protocole TLS 1.2.

Mon microphone ou ma webcam ne fonctionnent pas sous Windows WorkSpaces.

Vérifiez vos paramètres de confidentialité en ouvrant le menu Démarrer :

- Démarrer > Paramètres > Confidentialité > Caméra
- Démarrer > Paramètres > Confidentialité > Microphone

S'ils sont désactivés, activez-les.

WorkSpaces Les administrateurs peuvent également créer un objet de stratégie de groupe (GPO) pour activer le microphone et/ou la webcam selon les besoins.

Mes utilisateurs ne peuvent pas se connecter à l'aide de l'authentification par certificat et sont invités à saisir le mot de passe sur le WorkSpaces client ou sur l'écran de connexion Windows lorsqu'ils se connectent à leur session de bureau.

L'authentification par certificat a échoué pour la session. Si le problème persiste, l'échec de l'authentification basée sur les certificats peut être dû à l'un des problèmes suivants :

- Le WorkSpaces ou le client n'est pas pris en charge. L'authentification par certificat est prise en charge avec les packs Windows WorkSpaces on DCV utilisant la dernière WorkSpaces application cliente Windows.
- Il WorkSpaces doit être redémarré après avoir activé l'authentification basée sur les certificats dans le répertoire. WorkSpaces
- WorkSpaces n'a pas pu communiquer avec AWS CA privée le certificat ou AWS CA privée n'a pas émis le certificat. Vérifiez [AWS CloudTrail](#) pour déterminer si un certificat a été émis. Pour de plus amples informations, veuillez consulter [Gestion de l'authentification par certificat](#).
- Le contrôleur de domaine ne possède aucun certificat de contrôleur de domaine pour l'ouverture de session par carte à puce, ou il a expiré. Pour plus d'informations, reportez-vous à l'étape 7, Configurer les contrôleurs de domaine avec un certificat de contrôleur de domaine pour authentifier les utilisateurs de cartes à puce dans [Conditions préalables](#).
- Le certificat n'est pas fiable. Pour plus d'informations, reportez-vous à l'étape 7, « Publier l'autorité de certification dans Active Directory » dans [Conditions préalables](#). Exécutez `certutil -viewstore -enterprise NTAUTH` sur les contrôleurs de domaine pour confirmer que l'autorité de certification est publiée.
- Un certificat est en cache, mais les attributs de l'utilisateur qui l'ont invalidé ont changé. Contactez Support pour vider le cache avant l'expiration du certificat (24 heures). Pour plus d'informations, consultez le [Centre Support](#).
- Le userPrincipalName format de l'attribut UserPrincipalName SAML n'est pas correctement formaté ou ne correspond pas au domaine réel de l'utilisateur. Pour plus d'informations, consultez l'étape 1 dans [Conditions préalables](#).
- L'attribut ObjectSid (facultatif) de votre assertion SAML ne correspond pas à l'identifiant de sécurité Active Directory (SID) de l'utilisateur spécifié dans l'élément NameID SAML_Subject. Vérifiez que le mappage des attributs est correct dans votre fédération SAML et que votre fournisseur d'identité SAML synchronise l'attribut SID pour l'utilisateur Active Directory.
- Certains paramètres de stratégie de groupe modifient les paramètres Active Directory par défaut pour l'ouverture de session par carte à puce, ou prennent des mesures si une carte à puce est retirée d'un lecteur de carte. Ces paramètres peuvent entraîner un comportement inattendu en plus des erreurs répertoriées ci-dessus. L'authentification par certificat présente une carte à puce virtuelle au système d'exploitation de l'instance, et la supprime une fois la connexion effectuée. Vérifiez les [paramètres de stratégie de groupe principaux pour les cartes à puce](#) et les [paramètres supplémentaires de stratégie de groupe pour les cartes à puce et clés de Registre](#), y compris le comportement de retrait des cartes à puce.

- Le point de distribution CRL pour l'autorité de certification privée n'est pas en ligne ni accessible depuis le contrôleur de domaine WorkSpaces ou depuis le contrôleur de domaine. Pour plus d'informations, consultez l'étape 5 de la rubrique [Conditions préalables](#).
- Pour vérifier s'il y a des éléments périmés CAs dans le domaine ou la forêt, lancez-vous PKIVIEW.msc sur l'autorité de certification pour vérifier. S'ils sont périmés CAs, utilisez le PKIVIEW.msc mmc pour les supprimer manuellement.
- Pour vérifier si la réplication Active Directory fonctionne et qu'il n'y a aucun contrôleur de domaine périmé dans le domaine, exécutez `repadmin /replsum`.

Les étapes de résolution des problèmes supplémentaires impliquent l'examen des journaux d'événements Windows de l'instance WorkSpaces. Un événement courant à examiner en cas d'échec de connexion est l'[événement 4625 : un compte n'a pas pu se connecter](#) dans le journal de sécurité Windows.

Si le problème persiste, contactez Support. Pour plus d'informations, consultez le [Centre Support](#).

J'essaie de faire quelque chose qui nécessite un support d'installation Windows mais qui WorkSpaces ne le fournit pas.

Si vous utilisez un bundle public AWS fourni, vous pouvez utiliser le support d'installation du système d'exploitation Windows Server, les instantanés EBS fournis par Amazon EC2 en cas de besoin.

Créez un volume EBS à partir de ces instantanés, joignez-le à Amazon EC2 et transférez les fichiers là où ils se trouvent WorkSpace selon vos besoins. Si vous utilisez Windows 10 sur BYOL activé WorkSpaces et que vous avez besoin d'un support d'installation, vous devrez préparer votre propre support d'installation. Pour plus d'informations, consultez [Ajouter des composants Windows à l'aide de la console](#). Comme vous ne pouvez pas attacher directement un volume EBS à un Workspace, vous devez l'attacher à une instance Amazon EC2 et copier les fichiers.

Je souhaite lancer WorkSpaces avec un annuaire AWS géré existant créé dans une WorkSpaces région non prise en charge.

Pour lancer Amazon à WorkSpaces l'aide d'un annuaire situé dans une région qui n'est pas actuellement prise en charge par WorkSpaces, suivez les étapes ci-dessous.

 Note

Si vous recevez des erreurs lors de l'exécution de AWS Command Line Interface commandes, assurez-vous d'utiliser la AWS CLI version la plus récente. Pour plus d'informations, consultez [Confirm that you're running a recent version of the AWS CLI](#).

Étape 1 : Créer un cloud privé virtuel (VPC) appairé à un autre VPC de votre compte

1. Créez une connexion d'appairage de VPC avec un VPC d'une autre région. Pour plus d'informations, voir [Créer avec le même compte et VPCs dans différentes régions](#).
2. Acceptez la connexion d'appairage de VPC. Pour plus d'informations, consultez [Accepter une connexion d'appairage de VPC](#).
3. Après avoir activé la connexion d'appairage VPC, vous pouvez consulter vos connexions d'appairage VPC à l'aide de la console Amazon VPC, de, ou d'une API. AWS CLI

Étape 2 : Mettre à jour les tables de routage pour l'appairage de VPC dans les deux régions

Mettez à jour vos tables de routage pour activer la communication avec le VPC homologue via IPv4 ou. IPv6 Pour plus d'informations, consultez [Mise à jour de vos tables de routage pour une connexion d'appairage de VPC](#).

Étape 3 : créer un AD Connector et enregistrer Amazon WorkSpaces

1. Pour consulter les conditions préalables requises pour un connecteur AD, consultez [Prérequis AD Connector](#).
2. Connectez votre annuaire existant au connecteur AD. Pour plus d'informations, consultez [Création d'un AD Connector](#).
3. Lorsque l'état du connecteur AD passe à Actif, ouvrez la [console AWS Directory Service](#), puis choisissez le lien hypertexte correspondant à votre ID d'annuaire.
4. Pour les AWS applications et les services, choisissez Amazon WorkSpaces pour activer l'accès WorkSpaces à ce répertoire.
5. Enregistrez le répertoire auprès de WorkSpaces. Pour plus d'informations, voir [Enregistrer un répertoire auprès de WorkSpaces](#).

Je souhaite mettre à jour Firefox sur Amazon Linux 2.

Étape 1 : Vérifier que la mise à jour automatique est activée

Pour vérifier que la mise à jour automatique est activée, exécutez la commande `systemctl status *os-update-mgmt.timer | grep enabled` sur votre WorkSpace. Le résultat doit afficher deux lignes comportant le mot `enabled`.

Étape 2 : Lancer une mise à jour

Firefox se met généralement à jour automatiquement dans Amazon Linux 2, WorkSpaces ainsi que tous les autres progiciels du système, pendant la période de maintenance. Toutefois, cela dépend du type WorkSpaces que vous utilisez.

- En AlwaysOn WorkSpaces effet, la fenêtre de maintenance hebdomadaire est du dimanche de 00h00 à 04h00, dans le fuseau horaire du WorkSpace
- À AutoStop WorkSpaces compter du troisième lundi du mois, et pendant deux semaines au maximum, le créneau de maintenance est ouvert chaque jour de 00h00 à 05h00 environ, dans le fuseau horaire de la AWS Région pour le WorkSpace

Pour plus d'informations sur les fenêtres de maintenance, consultez la section [Workspace maintenance](#).

Vous pouvez également lancer un cycle de mise à jour immédiat en redémarrant votre ordinateur WorkSpace et en vous reconnectant au bout de 15 minutes. Vous pouvez également lancer les mises à jour en saisissant `sudo yum update`. Pour lancer uniquement une mise à jour pour Firefox, saisissez `sudo yum install firefox`.

Si vous ne pouvez pas configurer l'accès aux référentiels Amazon Linux 2 et que vous préférez installer Firefox à l'aide de fichiers binaires créés par Mozilla, consultez [Installation de Firefox avec les binaires de Mozilla](#) du support Mozilla. Nous vous recommandons de désinstaller complètement la version RPM de Firefox afin de ne pas exécuter une version obsolète par erreur. Vous pouvez la désinstaller en exécutant la commande `sudo yum remove firefox`.

Vous pouvez également télécharger les packages RPM nécessaires depuis les référentiels Amazon Linux 2 en exécutant la commande `yumdownloader firefox` sur un autre ordinateur. Ensuite, chargez les référentiels latéralement WorkSpaces, où vous pouvez les installer à l'aide d'une YUM commande standard telle que `sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`

 Note

Le nom exact du fichier changera en fonction de la version du package.

Étape 3 : Vérifier que le référentiel Firefox est utilisé

Amazon Linux Extras fournit automatiquement les mises à jour de Firefox pour Amazon Linux 2 WorkSpaces. Amazon Linux 2 WorkSpaces créé après le 31 juillet 2023 aura déjà activé le référentiel Firefox Extra. Pour vérifier que vous WorkSpace utilisez le dépôt Firefox Extra, exécutez la commande suivante.

```
yum repolist | grep amzn2extra-firefox
```

Le résultat de la commande doit ressembler à `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10` quand le référentiel Firefox Extra est utilisé. Il sera vide si ce n'est pas le cas. Si le référentiel Firefox Extra n'est pas utilisé, vous pouvez essayer de l'activer manuellement avec la commande suivante :

```
sudo amazon-linux-extras install firefox
```

Si l'activation du référentiel Firefox Extra échoue toujours, vérifiez votre accès Internet et assurez-vous que vos points de terminaison VPC ne sont pas configurés. Pour continuer à recevoir les mises à jour de Firefox pour Amazon Linux 2 WorkSpaces via les référentiels YUM, assurez-vous WorkSpaces de pouvoir accéder aux référentiels Amazon Linux 2. Pour plus d'informations sur l'accès aux référentiels Amazon Linux 2 sans accès à Internet, consultez [cet article du Centre de connaissances](#).

Mon utilisateur peut réinitialiser son mot de passe à l'aide du WorkSpaces client, en ignorant le paramètre Fine Grained Password Policy (FFGP) configuré sur AWS Managed Microsoft AD

Si le WorkSpaces client de votre utilisateur est associé à AWS Managed Microsoft AD, il devra réinitialiser son mot de passe en utilisant le paramètre de complexité par défaut.

Le mot de passe de complexité par défaut distingue les majuscules et minuscules et doit comporter entre 8 et 64 caractères inclus. Il doit contenir au moins un caractère de chacune des catégories suivantes :

- Caractères minuscules (a-z)
- Caractères majuscules (A-Z)
- Chiffres (0-9)
- Caractères non alphanumériques (~!@#\$%^&* _-+=`|\\(){}[];:'"<>,.?/)

Assurez-vous que le mot de passe ne contient pas de caractères Unicode non imprimables, tels que des espaces blancs, des onglets en forme de chariot, des sauts de ligne et des caractères nuls.

Si votre organisation vous demande d'appliquer FFGP pour WorkSpaces, contactez votre administrateur Active Directory pour réinitialiser le mot de passe de votre utilisateur directement depuis Active Directory plutôt que depuis le WorkSpaces client.

Mes utilisateurs reçoivent le message d'erreur « Ceci n' OS/platform est pas autorisé à accéder à votre Workspace » lorsqu'ils tentent d'accéder à l' Windows/Linux Workspace aide de Web Access

La version du système d'exploitation que votre utilisateur essaie d'utiliser n'est pas compatible avec WorkSpaces Web Access. Assurez-vous d'activer Web Access dans le paramètre Autre plateforme de l' Workspace annuaire. Pour plus d'informations sur l'activation Workspace de votre accès Web, consultez [Activer et configurer WorkSpaces Web Access for WorkSpaces Personal](#).

Celui de mon utilisateur Workspace s'affiche comme défectueux une fois qu' AutoStop Workspace il se connecte à un état arrêté

Votre utilisateur utilise peut-être un logiciel connu pour provoquer des problèmes au niveau des interfaces réseau lorsqu'il sort de l'hibernation. Par exemple, si l'application NPCAP 1.1 Workspace est installée, passez à la version 1.2 ou supérieure pour résoudre ce problème.

Gnome se bloque sur les bundles WorkSpaces Ubuntu après la connexion

Si un Workspace est lancé en utilisant le ubuntu nom d'utilisateur, il y aura des conflits avec l'ubuntuutilisateur qui existe par défaut. Cela provoquera des pannes dans Gnome et pourrait entraîner d'autres dégradations des performances. Pour éviter ce problème, ne spécifiez pas le ubuntu nom d'utilisateur lors du provisionnement d'Ubuntu WorkSpaces.

Versions de l'agent hôte DCV dans Personal WorkSpaces

L'agent hôte DCV est un agent hôte qui s'exécute dans votre WorkSpace. Il diffuse vos pixels WorkSpace vers une application cliente et inclut des fonctionnalités en cours de session, telles que le son et la vidéo bidirectionnels et l'impression. Pour plus d'informations sur le DCV, consultez [Protocoles pour Amazon WorkSpaces](#).

Nous vous recommandons de mettre à jour le logiciel de l'agent hôte avec la dernière version disponible. Vous pouvez redémarrer manuellement WorkSpaces pour mettre à jour l'agent hôte DCV. L'agent hôte DCV est également mis à jour automatiquement pendant la fenêtre de maintenance WorkSpaces par défaut normale. Pour plus d'informations sur les fenêtres de maintenance, consultez la section [Workspace maintenance](#). Certaines de ces fonctionnalités nécessitent la dernière version WorkSpaces du client. Pour plus d'informations sur les dernières versions du client, consultez la section [WorkSpaces Clients](#).

Le tableau suivant décrit les modifications apportées à chaque version de l'agent hôte DCV pour WorkSpaces Personal.

Version	Date	Modifications
• Windows WorkSpaces - 2.2.0.2116	26 janvier 2026	• Ajout de la prise en charge de l'impression avancée permettant d'accéder aux préférences avancées de l'imprimante, notamment l'impression recto verso, la sélection du bac à papier, etc. lors de l'utilisation de l'impression à distance. • Protection de capture d'écran ajoutée qui aide à empêcher l'exfiltration de données en bloquant le contenu sur l'hôte lorsqu'un utilisateur essaie d'utiliser un outil de capture d'écran côté client. • Nouveaux compteurs de performance du serveur pour le nombre de TCP/QUIC connexions.

Version	Date	Modifications
		• Corrections de bogues et améliorations des performances, y compris le support de Firefox pour Enhanced WebAuthn sur Windows Server 2019.
• Windows WorkSpaces - 2.2.0.2047	1er octobre 2025	• Performances audio améliorées ; ajout d'un nouveau moniteur de périphérique audio qui permet la diffusion audio du microphone uniquement lorsqu'une application distante l'utilise, ce qui permet d'optimiser les performances (voir les notes de version relatives aux clients pour obtenir des clients compatibles). • Expérience clavier internationale améliorée grâce à l'introduction de nouvelles options de disposition du clavier (serveur ou client), qui vous aident à taper avec plus de confiance dans vos cas d'utilisation spécifiques (voir les notes de version relatives aux clients pour obtenir des clients compatibles) • Corrections de bogues, notamment des effets d'écho audio lors du partage du son de l'hôte dans des applications de visioconférence (telles que Zoom et Teams) et améliorations générales des performances
• Windows WorkSpaces - 2.2.0.2021	30 août 2025	• Correctifs de bogues et améliorations de performances

Version	Date	Modifications
Windows WorkSpaces - 2.1.0.2000	7 juillet 2025	- Support WebAuth de redirection amélioré pour les applications natives. - Correctifs de bogues et améliorations de performances
Ubuntu WorkSpaces - 2.1.0.1923	1er mai 2025	Correctifs de bogues et améliorations de performances
- Rocky Linux WorkSpaces - 2.1.0.1843 - Red Hat Enterprise Linux WorkSpaces - 2.1.0.1843	10 avril 2025	Correctifs de bogues et améliorations de performances
Windows WorkSpaces - 2.1.0.1840	19 mars 2025	- Correction d'un problème à cause duquel la liste des imprimantes s'affichait même si le GPO de redirection d'imprimantes était désactivé. - Correctifs de bogues et améliorations de performances
Windows WorkSpaces - 2.1.0.1792	19 novembre 2024	Correctifs de bogues et améliorations de performances

Version	Date	Modifications
Windows WorkSpaces - 2.1.0.1786	31 octobre 2024	- Le protocole de WorkSpaces streaming (WSP) a été renommé Amazon DCV. - Correction d'un problème de distorsion audio sur l'agent DCV pour les clients utilisant l'application Avaya. - Correction des problèmes de SmartCard connexion qui se produisaient lorsque l'utilisateur était inactif sur la page de demande du code PIN. - Correction d'un problème de WebAuthn redirection lors de la première tentative de connexion sur le navigateur Chrome. - Correctifs de bogues et améliorations de performances
Windows WorkSpaces - 2.1.0.1757	19 août 2024	- Ajout du support pour l'intégration avec IAM Identity Center (iDC). - Correctifs de bogues et améliorations de performances
Windows WorkSpaces - 2.1.0.1696	29 juillet 2024	- Ajout du support pour les hôtes Windows Graphics. - Ajout du support de redirection WebRTC pour Amazon Connect. - Correction d'un problème qui empêchait le service de s'exécuter au démarrage du système. - Correctifs de bogues et améliorations de performances

Version	Date	Modifications
Windows WorkSpaces - 2.1.0.1554	15 mai 2024	- Ajout du support pour Idle Disconnect Timeout. - Ajout d'un nouveau paramètre de stratégie de groupe pour configurer le délai d'inactivité de déconnexion. - Correction d'un problème de déconnexion et d'affichage d'un écran blanc lorsque les utilisateurs modifiaient les paramètres d'affichage. WorkSpaces - Correctifs de bogues et améliorations de performances
Ubuntu WorkSpaces - 2.1.0.1342	29 février 2024	- La résolution préférée de la webcam est passée entre 480 x 360 et 640 x 480. - Correctifs de bogues et améliorations de performances

Version	Date	Modifications
Windows WorkSpaces - 2.0.0.1425	22 février 2024	- Ajout de la prise en charge des demandes de WebAuthn redirection en cours de session provenant d'applications Web exécutées dans des navigateurs Google Chrome ou Microsoft Edge distants. Cette fonctionnalité ajoute une invite de navigateur unique demandant à l'utilisateur d'activer l'extension de WebAuthn redirection DCV. Il n'est pris en charge que sur Windows WorkSpaces et les clients WorkSpaces natifs. - Correction d'un problème à cause duquel un écran blanc ou figé apparaissait parfois lors de la connexion. - Correctifs de bogues et améliorations de performances
Windows WorkSpaces - 2.0.0.1304	11 janvier 2024	- Correction d'un bug lié aux blocages potentiels du streaming lors de la connexion. - Correction d'un bug lié à la journalisation.

Version	Date	Modifications
Windows WorkSpaces - 2.0.0.1288	16 novembre 2023	- Ajout de la prise en charge du pilote d'affichage indirect (IDD) sur Windows 10+, qui réduit la consommation du processeur et améliore les performances de streaming. - Ajout d'un nouveau paramètre de stratégie de groupe pour activer ou désactiver le pilote IDD. - Correction de bugs liés à la transparence des images du presse-papiers. - Correction de bogues préservant les facteurs d'échelle de Windows. - Correctifs de bogues et améliorations de performances
Windows WorkSpaces - 2.0.0.1164	13 octobre 2023	- Ajout du support pour VSync le pilote d'affichage virtuel. - Ajout d'un nouveau paramètre de stratégie de groupe pour activer ou désactiver VSync. - Amélioration des problèmes de reconnexion et de fiabilité - Correctifs de bogues et améliorations de performances

Version	Date	Modifications
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces - 2.1.0.1086	18 août 2023	• Ajout d'un nouveau paramètre pour activer ou désactiver la redirection de fuseau horaire • Délai d'ouverture de session prolongé et ajout d'une option de configuration • Passerelle améliorée pour permettre des reconnections plus rapides après une interruption • Correctifs de bogues et améliorations de performances
• Amazon Linux WorkSpaces - 2.0.0.907	30 juin 2023	• Ajout de la prise en charge du kit SDK d'extension DCV afin de permettre les intégrations spécifiques aux fournisseurs indépendants de logiciels (ISV). • Modification du comportement de déconnexion afin que la déconnexion mette fin à la session de l'utilisateur • Ajout de la prise en charge de la redirection de fuseau horaire • Délai d'ouverture de session prolongé et ajout d'une option de configuration • Résolution de problèmes de mise à niveau • Correctifs de bogues et améliorations de performances

Version	Date	Modifications
Windows WorkSpaces - 2.0.0.829	8 juin 2023	- Modification du comportement de déconnexion afin que la déconnexion mette fin à la session de l'utilisateur - Correction de bugs liés à la A/V synchronisation et aux claviers japonais. - Fiabilité améliorée de l'installateur DCV.
Ubuntu WorkSpaces - 2.1.0.829	16 mai 2023	- Modification du comportement de déconnexion afin que la déconnexion mette fin à la session de l'utilisateur - Ajout de la prise en charge du kit SDK d'extension DCV afin de permettre les intégrations spécifiques aux fournisseurs indépendants de logiciels (ISV). - Ajout de la prise en charge de la redirection de fuseau horaire - Résolution de problèmes de mise à niveau

Version	Date	Modifications
Windows WorkSpaces - 2.0.0.799	8 mai 2023	- Amélioration du transport QUIC basé sur UDP avec plusieurs optimisations de la qualité d'image et des performances - Ajout de la prise en charge du kit SDK d'extension DCV afin de permettre les intégrations spécifiques aux fournisseurs indépendants de logiciels (ISV). - Ajout de nouveaux paramètres de stratégie de groupe pour activer ou désactiver le kit SDK d'extension - Amélioration de la disposition des claviers allemand, coréen et japonais. - Correction de bogues liés aux problèmes de blocage de session, à l'accélération matérielle, à la redirection d'imprimantes, à au niveau de détail des journaux et aux paramètres de stratégie de groupe target-fps.

Note

- Pour plus d'informations sur la façon de vérifier la version de votre agent hôte, voir [Quels systèmes d'exploitation client et hôte sont pris en charge par la dernière version de DCV ?](#).
- Pour plus d'informations sur la mise à jour de la version de votre agent hôte, voir [Si j'ai déjà un DCV WorkSpace, comment le mettre à jour ?](#).
- Pour les notes de mise à jour de la version du client DCV macOS, voir les [notes de version](#) dans la section du Guide de l' WorkSpaces utilisateur consacrée aux applications clientes WorkSpaces macOS.

- Pour les notes de mise à jour de la version du client Windows DCV, voir les [notes de version](#) dans la section du Guide de l' WorkSpaces utilisateur consacrée aux applications clientes WorkSpaces Windows.

Utiliser et gérer les WorkSpaces pools

WorkSpaces Pools propose des bureaux virtuels non persistants, conçus pour les utilisateurs qui ont besoin d'accéder à des environnements de bureau hautement sélectionnés hébergés sur une infrastructure éphémère.

Rubriques

- [Régions AWS et zones de disponibilité pour les WorkSpaces piscines](#)
- [Gérer les annuaires pour les WorkSpaces pools](#)
- [Mise en réseau et accès pour les WorkSpaces piscines](#)
- [Création d'un WorkSpaces pool](#)
- [Administrer WorkSpaces les pools](#)
- [Utilisation d'Active Directory avec des WorkSpaces pools](#)
- [Bundles et images pour les piscines WorkSpaces](#)
- [WorkSpaces Pools de surveillance](#)
- [Activer et administrer le stockage persistant pour les WorkSpaces pools](#)
- [Activez la persistance des paramètres de l'application pour les utilisateurs de vos WorkSpaces pools](#)
- [WorkSpaces Codes de notification de dépannage des pools](#)

Régions AWS et zones de disponibilité pour les WorkSpaces piscines

WorkSpaces Les piscines sont disponibles dans les catégories suivantes Régions AWS.

Note

Pour ceux Régions AWS qui s'appliquent à WorkSpaces Personal, consultez la section [WorkSpaces Points de terminaison et quotas Amazon](#) dans le guide de Références générales AWS référence.

Nom de la région	Région	Point de terminaison	Protocole	Zones de disponibilité	
USA Est (Virginie du Nord)	us-east-1	workspaces.us-east-1.amazonaws.com workspaces-fips.us-east-1.amazonaws.com	HTTPS HTTPS	utilisez1-az2, utilisez1-az4, utilisez1-az6	
USA Ouest (Oregon)	us-west-2	workspaces.us-west-2.amazonaws.com workspaces-fips.us-west-2.amazonaws.com	HTTPS HTTPS	usw2-az1, usw2-az2, usw2-az3	
Asie-Pacifique (Mumbai)	ap-south-1	workspaces.ap-south-1.amazonaws.com	HTTPS	aps1-az1, aps1-az3	
Asie-Pacifique (Séoul)	ap-northeast-2	workspaces.ap-northeast-2.amazonaws.com	HTTPS	apné2-az1, apné2-az3	
Asie-Pacifique (Singapour)	ap-southeast-1	workspaces.ap-southeast-1.amazonaws.com	HTTPS	apse1-az1, apse1-az2	
Asie-Pacifique	ap-southeast-2	workspaces.ap-southeast-2.amazonaws.com	HTTPS	apse2-az1,	

Nom de la région	Région	Point de terminaison	Protocole	Zones de disponibilité	
Australie (Sydney)				apse2-az3	
Asie-Pacifique (Tokyo)	ap-northeast-1	workspaces.ap-northeast-1.amazonaws.com	HTTPS	apné1-az1, apné1-az4	
Canada (Centre)	ca-central-1	workspaces.ca-central-1.amazonaws.com	HTTPS	cac1-az1, cac1-az2	
Europe (Francfort)	eu-central-1	workspaces.eu-central-1.amazonaws.com	HTTPS	euc1-az2, euc1-az3	
Europe (Irlande)	eu-west-1	workspaces.eu-west-1.amazonaws.com	HTTPS	euw1-az1, euw1-az2, euw1-az3	
Europe (Londres)	eu-west-2	workspaces.eu-west-2.amazonaws.com	HTTPS	euw2-az2, euw2-az3	

Nom de la région	Région	Point de terminaison	Protocole	Zones de disponibilité	
Europe (Paris)	eu-west-3	workspaces.eu-west-3.amazonaws.com	HTTPS	euw3-az1, euw3-az2, euw3-az3	
Amérique du Sud (São Paulo)	sa-east-1	workspaces.sa-east-1.amazonaws.com	HTTPS	sae1-az1, sae1-az3	
AWS GovCloud (USA Est)	us-gov-east-1	workspaces.us-gov-east-1.amazonaws.com workspaces-fips.us-gov-east-1.amazonaws.com	HTTPS HTTPS	usgw1-az1, usgw1-az2, usgw1-az3	
AWS GovCloud (US-Ouest)	us-gov-west-1	workspaces.us-gov-west-1.amazonaws.com workspaces-fips.us-gov-west-1.amazonaws.com	HTTPS HTTPS	usge1-az1, usge1-az2, usge1-az3	

Gérer les annuaires pour les WorkSpaces pools

WorkSpaces Pools utilise un répertoire pour stocker et gérer des informations pour vos WorkSpaces et pour les utilisateurs. Dans cette section, nous vous montrons comment créer et gérer des annuaires pour les WorkSpaces pools.

Table des matières

- [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#)
- [Mettre à jour les détails du répertoire de vos WorkSpaces pools](#)
- [Supprimer un répertoire WorkSpaces Pools](#)

Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools

Vous pouvez activer l'enregistrement des applications WorkSpaces clientes et la connexion à un WorkSpaces pool WorkSpaces en configurant la fédération d'identités à l'aide de SAML 2.0. Pour ce faire, vous utilisez un rôle Gestion des identités et des accès AWS (IAM) et une URL d'état de relais pour configurer votre fournisseur d'identité (IdP) SAML 2.0 et l'activer pour. AWS Cela permet à vos utilisateurs fédérés d'accéder à un répertoire de Workspace pool. L'état du relais est le point de terminaison du WorkSpaces répertoire vers lequel les utilisateurs sont redirigés après s'être connectés avec succès AWS.

Important

WorkSpaces Les pools ne prennent pas en charge les configurations SAML 2.0 basées sur IP.

Rubriques

- [Étape 1 : Tenez compte des exigences](#)
- [Étape 2 : Exécution des opérations prérequis](#)
- [Étape 3 : créer un fournisseur d'identité SAML dans IAM](#)
- [Étape 4 : créer le répertoire du Workspace pool](#)
- [Étape 5 : Création d'un rôle IAM de fédération SAML 2.0](#)
- [Étape 6 : Configuration de votre fournisseur d'identité SAML 2.0](#)
- [Étape 7 : Création d'assertions pour la réponse d'authentification SAML](#)
- [Étape 8 : Configuration de l'état du relais de votre fédération](#)
- [Étape 9 : Activez l'intégration avec SAML 2.0 dans le répertoire de votre Workspace pool](#)
- [Résolution des problèmes](#)
- [Spécifiez les détails Active Directory pour votre répertoire WorkSpaces Pools](#)

Étape 1 : Tenez compte des exigences

Les exigences suivantes s'appliquent lors de la configuration de SAML pour un répertoire WorkSpaces Pools.

- Le rôle `workspaces_DefaultRole` IAM doit exister dans votre compte. AWS Ce rôle est automatiquement créé lorsque vous utilisez la configuration WorkSpaces rapide ou si vous en avez déjà lancé un WorkSpace à l'aide du AWS Management Console. Il WorkSpaces autorise Amazon à accéder à des AWS ressources spécifiques en votre nom. Si le rôle existe déjà, vous devrez peut-être y associer la politique `AmazonWorkSpacesPoolServiceAccess` gérée, qu'Amazon WorkSpaces utilise pour accéder aux ressources requises dans le AWS compte pour WorkSpaces Pools. Pour plus d'informations, consultez [Création du rôle `workspaces\_DefaultRole`](#) et [AWS politique gérée : `AmazonWorkSpacesPoolServiceAccess`](#).
- Vous pouvez configurer l'authentification SAML 2.0 pour les WorkSpaces pools compatibles avec Régions AWS cette fonctionnalité. Pour de plus amples informations, veuillez consulter [Régions AWS et zones de disponibilité pour les WorkSpaces piscines](#).
- Pour utiliser l'authentification SAML 2.0 avec WorkSpaces, l'IdP doit prendre en charge l'authentification unique non sollicitée initiée par l'IdP avec une ressource cible Deep Link ou une URL de point de terminaison d'état relais. ADFS, Azure AD, Duo Single Sign-On, Okta et. IdPs PingFederate PingOne Pour plus d'informations, consultez la documentation de votre IdP.
- L'authentification SAML 2.0 est prise en charge uniquement sur les WorkSpaces clients suivants. Pour les derniers WorkSpaces clients, consultez la [page de téléchargement WorkSpaces du client Amazon](#).
 - Application cliente Windows version 5.20.0 ou ultérieure
 - Client macOS version 5.20.0 ou ultérieure
 - Web Access

Étape 2 : Exécution des opérations prérequis

Remplissez les conditions préalables suivantes avant de configurer votre connexion IdP SAML 2.0 à un répertoire de pool. WorkSpaces

- Configurez votre fournisseur d'identité pour établir une relation d'approbation avec AWS.
- Voir [Intégration de fournisseurs de solutions SAML tiers avec des fournisseurs de solutions SAML AWS](#) pour plus d'informations sur la configuration de la AWS fédération. Parmi les exemples pertinents, citons l'intégration d'IdP à IAM pour accéder au. AWS Management Console

- Utilisez votre IdP pour générer et télécharger un document de métadonnées de fédération décrivant votre organisation en tant qu'IdP. Ce document XML signé est utilisé pour établir la relation d'approbation des parties utilisatrices. Enregistrez le fichier dans un emplacement auquel vous pouvez accéder ultérieurement depuis la console IAM.
- Créez un répertoire WorkSpaces Pool à l'aide de la WorkSpaces console. Pour de plus amples informations, veuillez consulter [Utilisation d'Active Directory avec des WorkSpaces pools](#).
- Créez un WorkSpaces pool pour les utilisateurs qui peuvent se connecter à l'IdP à l'aide d'un type d'annuaire pris en charge. Pour de plus amples informations, veuillez consulter [Création d'un WorkSpaces pool](#).

Étape 3 : créer un fournisseur d'identité SAML dans IAM

Pour commencer, vous devez créer un IdP SAML dans IAM. Cet IdP définit la relation IdP à AWS confiance de votre organisation à l'aide du document de métadonnées généré par le logiciel IdP de votre organisation. Pour plus d'informations, consultez la section [Création et gestion d'un fournisseur d'identité SAML](#) dans le guide de l'Gestion des identités et des accès AWS utilisateur. Pour plus d'informations sur l'utilisation de SAML IdPs dans AWS GovCloud (US) Regions, consultez [Gestion des identités et des accès AWS](#) le guide de l'AWS GovCloud (US) utilisateur.

Étape 4 : créer le répertoire du Workspace pool

Procédez comme suit pour créer un répertoire de WorkSpaces pool.

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez Créer un annuaire.
4. Pour le Workspace type, choisissez Pool.
5. Dans la section Source d'identité utilisateur de la page :
 - a. Entrez une valeur d'espace réservé dans la zone de texte URL d'accès utilisateur. Par exemple, entrez `placeholder` dans la zone de texte. Vous le modifierez ultérieurement après avoir configuré les droits d'application dans votre IdP.
 - b. Laissez la zone de texte Nom du paramètre d'état du relais vide. Vous le modifierez ultérieurement après avoir configuré les droits d'application dans votre IdP.
6. Dans la section Informations sur le répertoire de la page, entrez le nom et la description du répertoire. Le nom et la description du répertoire doivent comporter moins de 128 caractères,

peuvent contenir des caractères alphanumériques et les caractères spéciaux suivants : _ @ # % * + = : ? . / ! \ - . Le nom et la description du répertoire ne peuvent pas commencer par un caractère spécial.

7. Dans la section Réseau et sécurité de la page :

- a. Choisissez un VPC et deux sous-réseaux qui ont accès aux ressources réseau dont votre application a besoin. Pour une meilleure tolérance aux pannes, vous devez choisir deux sous-réseaux situés dans des zones de disponibilité différentes.
- b. Choisissez un groupe de sécurité qui permet WorkSpaces de créer des liens réseau dans votre VPC. Les groupes de sécurité contrôlent le trafic réseau autorisé à circuler WorkSpaces vers votre VPC. Par exemple, si votre groupe de sécurité restreint toutes les connexions HTTPS entrantes, les utilisateurs accédant à votre portail Web ne pourront pas charger de sites Web HTTPS depuis le WorkSpaces

8. La section Active Directory Config est facultative. Toutefois, vous devez spécifier les détails de votre Active Directory (AD) lors de la création de votre répertoire WorkSpaces Pools si vous prévoyez d'utiliser un AD avec vos WorkSpaces Pools. Vous ne pouvez pas modifier la configuration Active Directory de votre répertoire WorkSpaces Pools après l'avoir créée. Pour plus d'informations sur la spécification des détails de votre AD pour votre répertoire de WorkSpaces pool, consultez [Spécifiez les détails Active Directory pour votre répertoire WorkSpaces Pools](#). Après avoir terminé le processus décrit dans cette rubrique, vous devez revenir à cette rubrique pour terminer la création de votre répertoire WorkSpaces Pools.

Vous pouvez ignorer la section Active Directory Config si vous ne prévoyez pas d'utiliser un AD avec vos WorkSpaces pools.

9. Dans la section Propriétés du streaming de la page :

- Choisissez le comportement des autorisations du presse-papiers, saisissez une copie dans la limite de caractères locale (facultatif) et collez dans la limite de caractères de la session à distance (facultatif).
- Choisissez d'autoriser ou non l'impression sur le périphérique local.
- Choisissez d'autoriser ou de ne pas autoriser la journalisation des diagnostics.
- Choisissez d'autoriser ou non la connexion par carte à puce. Cette fonctionnalité s'applique uniquement si vous avez activé la configuration AD plus tôt dans cette procédure.

10. Dans la section Stockage de la page, vous pouvez choisir d'activer les dossiers de base.

11. Dans la section Rôle IAM de la page, choisissez un rôle IAM qui sera disponible pour toutes les instances de streaming de bureau. Pour en créer un nouveau, choisissez Create new IAM role.

Lorsque vous appliquez un rôle IAM depuis votre compte à un répertoire du WorkSpace pool, vous pouvez effectuer des demandes d' AWS API depuis un WorkSpace répertoire du WorkSpace pool sans gérer manuellement les AWS informations d'identification. Pour plus d'informations, consultez la section [Création d'un rôle pour déléguer des autorisations à un utilisateur IAM](#) dans le Guide de Gestion des identités et des accès AWS l'utilisateur.

12. Choisissez Créer un annuaire.

Étape 5 : Création d'un rôle IAM de fédération SAML 2.0

Procédez comme suit pour créer un rôle IAM de fédération SAML 2.0 dans la console IAM.

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Choisissez Rôles dans le panneau de navigation.
3. Choisissez Créer un rôle.
4. Choisissez la fédération SAML 2.0 pour le type d'entité de confiance.
5. Pour un fournisseur basé sur SAML 2.0, choisissez le fournisseur d'identité que vous avez créé dans IAM. Pour plus d'informations, voir [Création d'un fournisseur d'identité SAML dans IAM](#).
6. Choisissez Autoriser l'accès programmatique uniquement pour que l'accès soit autorisé.
7. Choisissez SAML:SUB_TYPE pour l'attribut.
8. Pour le champ Valeur, saisissez `https://signin.aws.amazon.com/saml`. Cette valeur limite l'accès aux rôles aux demandes de streaming utilisateur SAML qui incluent une assertion de type de sujet SAML avec une valeur de `persistent`. Si le SAML:sub_type est persistant, votre IdP envoie la même valeur unique pour l'NameIDélément dans toutes les demandes SAML d'un utilisateur donné. Pour plus d'informations, voir [Identification unique des utilisateurs dans une fédération basée sur SAML](#) dans le Guide de Gestion des identités et des accès AWS l'utilisateur.
9. Choisissez Next (Suivant) pour continuer.
10. N'apportez aucune modification ou sélection sur la page Ajouter des autorisations. Choisissez Next (Suivant) pour continuer.
11. Entrez un nom et une description pour le rôle.
12. Choisissez Créer un rôle.
13. Sur la page Rôles, choisissez le rôle que vous devez créer.
14. Choisissez l'onglet Relations de confiance.

15. Choisissez Modifier la politique d'approbation.
16. Dans la zone de texte JSON Modifier la politique de confiance, ajoutez l'Action `sts:TagSession` : à la politique de confiance. Pour plus d'informations, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de Gestion des identités et des accès AWS l'utilisateur.

Le résultat doit ressembler à l'exemple suivant :



```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Federated": "arn:aws:iam:::saml-provider/Directory"
8       },
9       "Action": [
10        "sts:AssumeRoleWithSAML",
11        "sts:TagSession"
12      ],
13      "Condition": {
14        "StringEquals": {
15          "SAML:sub_type": "persistent"
16        }
17      }
18    }
19  ]
20 }
```

17. Choisissez Mettre à jour une politique.
18. Sélectionnez l'onglet Autorisations.
19. Dans la section Politiques d'autorisation de la page, choisissez Ajouter des autorisations, puis choisissez Créer une politique intégrée.
20. Dans la section Éditeur de politiques de la page, choisissez JSON.
21. Dans la zone de texte JSON de l'éditeur de stratégie, entrez la politique suivante. Assurez-vous de remplacer :
 - `<region-code>` avec le code de la AWS région dans laquelle vous avez créé votre répertoire WorkSpace Pool.
 - `<account-id>` avec l'identifiant du AWS compte.
 - `<directory-id>` avec l'ID du répertoire que vous avez créé précédemment. Vous pouvez l'obtenir dans la WorkSpaces console.

Pour les ressources en AWS GovCloud (US) Regions, utilisez le format suivant pour l'ARN : `arn:aws-us-gov:workspaces:<region-code>:<account-id>:directory/<directory-id>`.

22. Choisissez Suivant.

23. Entrez un nom pour la stratégie, puis choisissez Create policy (Créer une stratégie).

Étape 6 : Configuration de votre fournisseur d'identité SAML 2.0

En fonction de votre IdP SAML 2.0, vous devrez peut-être mettre à jour manuellement votre IdP pour avoir AWS confiance en tant que fournisseur de services. Pour ce faire, téléchargez le `saml-metadata.xml` fichier qui se trouve dans le fichier <https://signin.aws.amazon.com/static/saml-metadata.xml>, puis chargez-le sur votre IdP. Cela met à jour les métadonnées de votre IdP.

Pour certains IdPs, la mise à jour est peut-être déjà configurée. Vous pouvez ignorer cette étape si elle est déjà configurée. Si la mise à jour n'est pas déjà configurée dans votre IdP, consultez la documentation fournie par votre IdP pour savoir comment mettre à jour les métadonnées. Certains fournisseurs vous offrent la possibilité de saisir l'URL du fichier XML dans leur tableau de bord, et l'IdP obtient et installe le fichier pour vous. D'autres exigent que vous téléchargiez le fichier depuis l'URL, puis que vous le téléchargiez sur leur tableau de bord.

Important

À ce stade, vous pouvez également autoriser les utilisateurs de votre IdP à accéder à l'WorkSpaces application que vous avez configurée dans votre IdP. Les utilisateurs autorisés à accéder à l'WorkSpaces application de votre annuaire n'en ont pas automatiquement WorkSpace créé un. De même, les utilisateurs qui ont WorkSpace créé une application pour eux ne sont pas automatiquement autorisés à accéder à l'WorkSpaces application. Pour se connecter avec succès à une WorkSpace authentification SAML 2.0, un utilisateur doit être autorisé par l'IdP et doit avoir WorkSpace créé un.

Étape 7 : Création d'assertions pour la réponse d'authentification SAML

Configurez les informations que votre IdP envoie AWS sous forme d'attributs SAML dans sa réponse d'authentification. En fonction de votre IdP, il est possible que cela soit déjà configuré. Vous pouvez ignorer cette étape si elle est déjà configurée. S'il n'est pas déjà configuré, fournissez les informations suivantes :

- SAML Subject NameID — Identifiant unique de l'utilisateur qui se connecte. Ne modifiez pas ce champ. format/value Dans le cas contraire, la fonctionnalité du dossier d'accueil ne fonctionnera pas comme prévu car l'utilisateur sera traité comme un autre utilisateur.

Note

Pour les WorkSpaces pools joints à un domaine, la NameID valeur de l'utilisateur doit être fournie dans le `domain\username` format utilisant le `sAMAccountName`, ou dans le `username@domain.com` format utilisant `userPrincipalName`, ou simplement. `userName` Si vous utilisez ce `sAMAccountName` format, vous pouvez spécifier le domaine en utilisant le nom NetBIOS ou le nom de domaine complet (FQDN). Le `sAMAccountName` format est requis pour les scénarios de confiance unidirectionnelle Active Directory. Pour plus d'informations, voir [Utilisation d'Active Directory avec des WorkSpaces pools](#). Si `userName` un seul élément est fourni, l'utilisateur sera connecté au domaine principal

- **Type de sujet SAML** (avec une valeur définie sur **persistant**) : définissez la valeur de manière à **persistant** garantir que votre IdP envoie la même valeur unique pour NameID l'élément dans toutes les demandes SAML d'un utilisateur donné. Assurez-vous que votre politique IAM inclut une condition autorisant uniquement les demandes SAML dont le SAML est `sub_type` défini **surpersistant**, comme décrit dans la section. [Étape 5 : Création d'un rôle IAM de fédération SAML 2.0](#)
- **Attribute** élément dont l'**Name** attribut est défini sur `https://aws.amazon.com/SAML/Attributes/Role` : cet élément contient un ou plusieurs `AttributeValue` éléments répertoriant le rôle IAM et l'IdP SAML auxquels l'utilisateur est mappé par votre IdP. Le rôle et l'IdP sont spécifiés sous la forme d'une paire séparée par des virgules de. ARNs Exemple de la valeur attendue : `arn:aws:iam::<account-id>:role/<role-name>,arn:aws:iam::<account-id>:saml-provider/<provider-name>`.
- **Attribute** élément dont l'**Name** attribut est défini sur `https://aws.amazon.com/SAML/Attributes/RoleSessionName` — Cet élément contient un `AttributeValue` élément qui fournit un identifiant pour les informations d'identification AWS temporaires émises pour l'authentification unique. La valeur de l'`AttributeValue` élément doit comporter entre 2 et 64 caractères, peut contenir des caractères alphanumériques et les caractères spéciaux suivants : `_ . : / = + - @`. Il ne doit pas contenir d'espace. La valeur est généralement une adresse e-mail ou un nom d'utilisateur principal (UPN). La valeur ne peut pas comporter d'espace, comme dans le nom d'affichage d'un utilisateur.
- **Attribute** élément dont l'**Name** attribut est défini sur `https://aws.amazon.com/SAML/Attributes/Email` PrincipalTag — Cet élément contient un élément `AttributeValue` qui fournit l'adresse e-mail de l'utilisateur. La valeur doit correspondre à l'adresse e-mail de WorkSpaces l'utilisateur telle que définie dans le WorkSpaces répertoire. Les valeurs des balises peuvent inclure

des combinaisons de lettres, de chiffres, d'espaces et de _ . : / = + - @ caractères. Pour plus d'informations, voir [Règles de balisage dans IAM et AWS STS dans](#) le Guide de l'Gestion des identités et des accès AWS utilisateur.

- **Attribute**Élément (facultatif) dont l'**Name**attribut est défini sur <https://aws.amazon.com/SAML/Attributes/> PrincipalTag : UserPrincipalName — Cet élément contient un AttributeValue élément qui fournit l'Active Directory userPrincipalName à l'utilisateur qui se connecte. La valeur doit être fournie au username@domain.com format. Ce paramètre est utilisé avec l'authentification par certificat en tant qu'autre nom du sujet dans le certificat utilisateur final. Pour de plus amples informations, veuillez consulter [Authentification basée sur des certificats et authentification personnelle WorkSpaces](#).
- **Attribute**Élément (facultatif) dont l'**Name**attribut est défini sur <https://aws.amazon.com/SAML/Attributes/> PrincipalTag : ObjectSid (facultatif) — Cet élément contient un AttributeValue élément qui fournit l'identifiant de sécurité Active Directory (SID) à l'utilisateur qui se connecte. Ce paramètre est utilisé avec l'authentification par certificat pour permettre un mappage fort vers l'utilisateur Active Directory. Pour de plus amples informations, veuillez consulter [Authentification basée sur des certificats et authentification personnelle WorkSpaces](#).
- **Attribute**Élément (facultatif) dont l'**Name**attribut est défini sur <https://aws.amazon.com/SAML/Attributes/> Domain PrincipalTag — Cet élément contient un élément AttributeValue qui fournit le nom de domaine complet (FQDN) DNS Active Directory aux utilisateurs qui se connectent. Ce paramètre est utilisé avec l'authentification par certificat lorsque l'élément userPrincipalName Active Directory correspondant à l'utilisateur contient un autre suffixe. La valeur doit être fournie au domain.com format et doit inclure tous les sous-domaines.
- **Attribute**Élément (facultatif) dont l'**Name**attribut est défini sur <https://aws.amazon.com/SAML/Attributes/> SessionDuration — Cet élément contient un AttributeValue élément qui indique la durée maximale pendant laquelle une session de streaming fédérée d'un utilisateur peut rester active avant qu'une nouvelle authentification ne soit requise. La valeur par défaut est de 3600 secondes (60 minutes). Pour plus d'informations, consultez le [SAML SessionDurationAttribute](#) dans le guide de l'Gestion des identités et des accès AWS utilisateur.

 Note

Bien que l'attribut SessionDuration soit facultatif, nous vous recommandons de l'inclure dans la réponse SAML. Si vous ne spécifiez pas cet attribut, la durée de la session est définie sur une valeur par défaut de 3600 secondes (60 minutes). WorkSpaces les sessions de bureau sont déconnectées une fois leur durée de session expirée.

Pour plus d'informations sur la configuration de ces éléments, consultez la [section Configuration des assertions SAML pour la réponse d'authentification dans le](#) Guide de l'Gestion des identités et des accès AWS utilisateur. Pour plus d'informations sur les exigences de configuration spécifiques à votre fournisseur d'identité, consultez sa documentation.

Étape 8 : Configuration de l'état du relais de votre fédération

Utilisez votre IdP pour configurer l'état du relais de votre fédération afin qu'il pointe vers l'URL de l'état du relais du répertoire WorkSpaces Pool. Une fois l'authentification réussie par AWS, l'utilisateur est dirigé vers le point de terminaison du répertoire du WorkSpaces pool, défini comme l'état du relais dans la réponse d'authentification SAML.

Le format de URL d'état du relais est le suivant :

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

Le tableau suivant répertorie les points de terminaison de l'état du relais pour les AWS régions où l'authentification WorkSpaces SAML 2.0 est disponible. AWS Les régions dans lesquelles la fonctionnalité WorkSpaces Pools n'est pas disponible ont été supprimées.

Région	Point de terminaison RelayState
Région USA Est (Virginie du Nord)	- workspaces.euc-sso.us-east-1.aws.amazon.com - espaces de travail (FIPS). euc-sso-fips.us-east-1.aws.amazon.com
Région USA Ouest (Oregon)	- workspaces.euc-sso.us-west-2.aws.amazon.com - espaces de travail (FIPS). euc-sso-fips.us-west-2.aws.amazon.com
Région Asie-Pacifique (Mumbai)	workspaces.euc-sso.ap-south-1.aws.amazon.com
Région Asie-Pacifique (Séoul)	workspaces.euc-sso.ap-northeast-2.aws.amazon.com

Région	Point de terminaison RelayState
Région Asie-Pacifique (Singapour)	<code>workspaces.euc-ss0.ap-southeast-1.amazonaws.com</code>
Région Asie-Pacifique (Sydney)	<code>workspaces.euc-ss0.ap-southeast-2.amazonaws.com</code>
Région Asie-Pacifique (Tokyo)	<code>workspaces.euc-ss0.ap-northeast-1.amazonaws.com</code>
Région Canada (Centre)	<code>workspaces.euc-ss0.ca-central-1.amazonaws.com</code>
Région Europe (Francfort)	<code>workspaces.euc-ss0.eu-central-1.amazonaws.com</code>
Région Europe (Irlande)	<code>workspaces.euc-ss0.eu-west-1.amazonaws.com</code>
Région Europe (Londres)	<code>workspaces.euc-ss0.eu-west-2.amazonaws.com</code>
Région Amérique du Sud (São Paulo)	<code>workspaces.euc-ss0.sa-east-1.amazonaws.com</code>

Région	Point de terminaison RelayState
AWS GovCloud (US-Ouest)	- espaces de travail.euc-ss0. us-gov-west-1. amazonaws-us-gov.com - espaces de travail (FIPS). euc-ss0-fips. us-gov-west-1. amazonaws-us-gov.com  Note Pour plus d'informations sur l'utilisation de SAML IdPs dans AWS GovCloud (US) Regions, consultez le guide de l'utilisateur d'Amazon WorkSpaces in the AWS GovCloud (États-Unis).
AWS GovCloud (USA Est)	- espaces de travail.euc-ss0. us-gov-east-1. amazonaws-us-gov.com - espaces de travail (FIPS). euc-ss0-fips. us-gov-east-1. amazonaws-us-gov.com  Note Pour plus d'informations sur l'utilisation de SAML IdPs dans AWS GovCloud (US) Regions, consultez le guide de l'utilisateur d'Amazon WorkSpaces in the AWS GovCloud (États-Unis).

Étape 9 : Activez l'intégration avec SAML 2.0 dans le répertoire de votre WorkSpace pool

Procédez comme suit pour activer l'authentification SAML 2.0 pour le répertoire du WorkSpaces pool.

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez l'onglet Répertoires de pools.
4. Choisissez l'ID du répertoire que vous souhaitez modifier.
5. Choisissez Modifier dans la section Authentification de la page.
6. Choisissez Modifier le fournisseur d'identité SAML 2.0.
7. Pour l'URL d'accès utilisateur, parfois appelée « URL SSO », remplacez la valeur de l'espace réservé par l'URL SSO qui vous a été fournie par votre IdP.
8. Pour le nom du paramètre de lien profond IdP, entrez le paramètre applicable à votre IdP et à l'application que vous avez configurée. La valeur par défaut est RelayState si vous omettez le nom du paramètre.

Le tableau suivant répertorie les noms des paramètres d'accès utilisateur URLs et de lien profond propres aux différents fournisseurs d'identité pour les applications.

Fournisseur d'identité	Paramètre	URL d'accès utilisateur
ADFS	RelayState	https://<host>/ adfs/ls/idpinitia tedsignon.aspx? RelayState=R PID= <relaying- party-uri>
Azure AD	RelayState	https://myapps.mic rosoft.com/signin/ <app-id>?tenantId = <tenant-id>
Duo Single Sign-On	RelayState	https://<sub-doma in> .sso.duos ecurity.com/saml2/ sp/ <app-id>/sso
Okta	RelayState	https://<sub-doma in> .okta.com/

Fournisseur d'identité	Paramètre	URL d'accès utilisateur
		app/<app-name> /<app-id>/sso/saml
OneLogin	RelayState	https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/ <app-id>
JumpCloud	RelayState	https://sso.jumpcloud.com/saml2/ <app-id>
Auth0	RelayState	https://<default-tenant-name>.us.auth0.com/samlp/ <client-id>
PingFederate	TargetResource	https://<host>/idp/startSSO.ping? PartnerSpId= <sp-id>
PingOne pour Enterprise	TargetResource	https://sso.connect.pingidentity.com/sso/sp/initss?saasid= <app-id>&idpid=<idp-id>

9. Choisissez Enregistrer.

Important

La révocation de SAML 2.0 à un utilisateur ne déconnecte pas directement sa session. Ils ne seront supprimés qu'après l'expiration du délai imparti. Ils peuvent également y mettre fin à l'aide de l' [TerminateWorkspacesPoolSessionAPI](#).

Résolution des problèmes

Les informations suivantes peuvent vous aider à résoudre des problèmes spécifiques liés à vos WorkSpaces pools.

Je reçois un message « Impossible de me connecter » dans le client WorkSpaces Pools après avoir terminé l'authentification SAML

Les revendications `nameID` et `PrincipalTag:Email` dans le SAML doivent correspondre au nom d'utilisateur et à l'adresse e-mail configurés dans Active Directory. Certains IdP peuvent nécessiter une mise à jour, une actualisation ou un redéploiement après avoir ajusté certains attributs. Si vous effectuez un ajustement et que celui-ci n'apparaît pas dans votre capture SAML, consultez la documentation ou le programme d'assistance de votre IdP pour connaître les étapes spécifiques requises pour que le changement prenne effet.

Spécifiez les détails Active Directory pour votre répertoire WorkSpaces Pools

Dans cette rubrique, nous vous expliquons comment spécifier les informations relatives à votre Active Directory (AD) sur la page Créer un répertoire de WorkSpaces pool de la WorkSpaces console. Lorsque vous créez votre répertoire de WorkSpaces pool, vous devez spécifier les détails de votre AD si vous prévoyez d'utiliser un AD avec vos WorkSpaces pools. Vous ne pouvez pas modifier la configuration Active Directory de votre répertoire WorkSpaces Pools après l'avoir créée. Voici un exemple de la section Active Directory Config de la page de répertoire Create WorkSpaces Pool.

▼ **Active Directory Config - optional** [Info](#)

Join your WorkSpaces pool directory to domains in Microsoft Active Directory. You can also use your existing Active Directory domains, either cloud-based or on-premises, to launch domain-joined WorkSpace sessions.

Organizational Unit (OU)

Enter the organizational unit (OU) that the directory belongs to.

Directory domain name

A fully qualified domain name for the directory. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

Service account

In order to domain join your directory, we need a service account name and password of an account with domain join permissions. These credentials need to be stored in AWS Secrets Manager. Choose an existing or create a new AWS Secrets Manager secret that contains secret keys of "ServiceAccountName" and "Password". [Learn more](#)

AWS Secrets Manager secret [Info](#)

Select the AWS Secrets Manager secret that contains your service account credentials.

▼ [Create AWS Secret](#)

Note

Le processus complet de création d'un répertoire WorkSpaces Pool est décrit dans cette [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#) rubrique. Les procédures décrites sur cette page ne représentent qu'un sous-ensemble d'étapes du processus complet de création d'un répertoire WorkSpaces Pool.

Rubriques

- [Spécifiez l'unité organisationnelle et le nom de domaine du répertoire pour votre AD](#)
- [Spécifiez le compte de service pour votre AD](#)

Spécifiez l'unité organisationnelle et le nom de domaine du répertoire pour votre AD

Suivez la procédure suivante pour spécifier une unité organisationnelle (UO) et un nom de domaine de répertoire pour votre AD sur la page Créer un répertoire de WorkSpaces pool.

1. Pour Unité d'organisation, entrez l'unité d'organisation à laquelle appartient le pool. WorkSpace les comptes de machine sont placés dans l'unité organisationnelle (UO) que vous spécifiez pour le répertoire du WorkSpaces pool.

 Note

Le nom de l'unité d'organisation ne doit pas contenir d'espace. Si vous spécifiez un nom d'unité d'organisation contenant des espaces, lorsqu'elle tente de rejoindre le domaine Active Directory, elle WorkSpaces ne peut pas effectuer correctement le cycle des objets informatiques et la jonction de domaine ne fonctionne pas.

2. Pour le nom de domaine de l'annuaire, entrez le nom de domaine complet (FQDN) du domaine Active Directory (par exemple, corp.example.com). Chaque AWS région ne peut avoir qu'une seule valeur de configuration de répertoire avec un nom de répertoire spécifique.
 - Vous pouvez joindre les annuaires de votre WorkSpaces pool à des domaines dans Microsoft Active Directory. Vous pouvez également utiliser vos domaines Active Directory existants, qu'ils soient basés sur le cloud ou sur site, pour lancer une connexion à un domaine WorkSpaces.
 - Vous pouvez également utiliser AWS Directory Service for Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD, pour créer un domaine Active Directory. Vous pouvez ensuite utiliser ce domaine pour soutenir vos WorkSpaces ressources.
 - En rejoignant WorkSpaces votre domaine Active Directory, vous pouvez :
 - Permettre à vos utilisateurs et à vos applications d'accéder aux ressources Active Directory, telles que les imprimantes et les partages de fichiers à partir de sessions de streaming.
 - utiliser les paramètres de stratégie de groupe qui sont disponibles dans la console de gestion des stratégies de groupe (GPMC) pour définir l'expérience de l'utilisateur final ;
 - diffuser les applications qui nécessitent l'authentification des utilisateurs à l'aide de leurs informations d'identification de connexion Active Directory ;
 - Appliquer les stratégies de sécurité et de conformité de votre entreprise à vos instances de streaming WorkSpaces .
3. Pour le compte de service, passez à la section [Spécifiez le compte de service pour votre AD](#) suivante de cette page.

Spécifiez le compte de service pour votre AD

Lorsque vous configurez Active Directory (AD) pour vos WorkSpaces pools dans le cadre du processus de création d'annuaire, vous devez spécifier le compte de service AD à utiliser pour gérer l'AD. Cela nécessite que vous fournissiez les informations d'identification du compte de service,

qui doivent être stockées AWS Secrets Manager et cryptées à l'aide d'une clé gérée par le client AWS Key Management Service (AWS KMS). Dans cette section, nous vous expliquons comment créer la clé gérée par le AWS KMS client et le secret Secrets Manager pour stocker les informations d'identification de votre compte de service AD.

Étape 1 : Création d'une clé gérée par AWS KMS le client

Procédez comme suit pour créer une clé gérée par AWS KMS le client

1. Ouvrez la AWS KMS console à l'adresse <https://console.aws.amazon.com/kms>.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Choisissez Créer une clé, puis Next.
4. Choisissez Symetric pour le type de clé, Chiffrer et déchiffrer pour l'utilisation de la clé, puis choisissez Next.
5. Entrez un alias pour la clé, par exemple `WorkSpacesPoolDomainSecretKey`, puis choisissez Next.
6. Ne choisissez pas un administrateur clé. Choisissez Next (Suivant) pour continuer.
7. Ne définissez pas les autorisations d'utilisation des clés. Choisissez Next (Suivant) pour continuer.
8. Dans la section Politique clé de la page, ajoutez ce qui suit :

```
{
  "Sid": "Allow access for Workspaces SP",
  "Effect": "Allow",
  "Principal": {
    "Service": "workspaces.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

Le résultat doit apparaître comme dans l'exemple suivant.

```

4  "Statement": [
5    {
6      "Sid": "Enable IAM User Permissions",
7      "Effect": "Allow",
8      "Principal": {
9        "AWS": "arn:aws:iam::[ID]:root"
10     },
11     "Action": "kms:*",
12     "Resource": "*"
13   },
14   {
15     "Sid": "Allow access for Workspaces SP",
16     "Effect": "Allow",
17     "Principal": {
18       "Service": [
19         "workspaces.amazonaws.com"
20       ]
21     },
22     "Action": "kms:Decrypt",
23     "Resource": "*"
24   }

```

9. Choisissez Finish (Terminer).

Votre clé gérée par le AWS KMS client est maintenant prête à être utilisée avec Secrets Manager. Passez à la [Étape 2 : Créez le secret Secrets Manager pour stocker les informations d'identification de votre compte de service AD](#) section de cette page.

Étape 2 : Créez le secret Secrets Manager pour stocker les informations d'identification de votre compte de service AD

Procédez comme suit pour créer un secret Secrets Manager afin de stocker les informations d'identification de votre compte de service AD.

1. Ouvrez la AWS Secrets Manager console à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Choisissez Create a new secret (Créer un secret).
3. Choisissez Autre type de secret.
4. Pour la première key/value paire, entrez Service Account Name la clé et le nom du compte de service pour la valeur, telle que domain\username.
5. Pour la deuxième key/value paire, entrez a Service Account Password pour la clé et le mot de passe du compte de service pour la valeur.
6. Pour la clé de chiffrement, choisissez la clé gérée par le AWS KMS client que vous avez créée précédemment, puis cliquez sur Suivant.

7. Entrez un nom pour le secret, par exemple `WorkSpacesPoolDomainSecretAD`.
8. Choisissez Modifier les autorisations dans la section Autorisations relatives aux ressources de la page.
9. Entrez la politique d'autorisation suivante :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "workspaces.amazonaws.com"
        ]
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

10. Choisissez Enregistrer pour enregistrer la politique d'autorisation.
11. Choisissez Next (Suivant) pour continuer.
12. Ne configurez pas la rotation automatique. Choisissez Next (Suivant) pour continuer.
13. Choisissez Store pour terminer de stocker votre secret.

Les informations d'identification de votre compte de service AD sont désormais stockées dans Secrets Manager. Passez à la [Étape 3 : Sélectionnez le secret Secrets Manager qui contient les informations d'identification de votre compte de service AD](#) section de cette page.

Étape 3 : Sélectionnez le secret Secrets Manager qui contient les informations d'identification de votre compte de service AD

Procédez comme suit pour sélectionner le secret Secrets Manager que vous avez créé dans la configuration Active Directory de votre répertoire WorkSpaces Pool.

- Pour le compte de service, choisissez le AWS Secrets Manager secret qui contient les informations d'identification de votre compte de service. Procédez comme suit pour créer le secret si ce n'est pas déjà fait. Le secret doit être chiffré à l'aide d'une clé gérée par le AWS Key Management Service client.

Maintenant que vous avez rempli tous les champs de la section Active Directory Config de la page Create WorkSpaces Pool directory directory, vous pouvez continuer à terminer la création de votre répertoire WorkSpaces Pool. Passez à [Étape 4 : créer le répertoire du WorkSpace pool](#) l'étape 9 de la procédure et commencez.

Mettre à jour les détails du répertoire de vos WorkSpaces pools

Vous pouvez effectuer les tâches de gestion d'annuaire suivantes à l'aide de la console WorkSpaces Pools.

Authentification

Vous pouvez configurer des options d'authentification supplémentaires pour vos WorkSpaces pools. Les pools nécessitent une authentification SAML 2.0.

Pour activer et configurer l'authentification du fournisseur d'identité SAML 2.0

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez le répertoire que vous souhaitez configurer.
4. Accédez à l'authentification et choisissez Modifier.
5. Choisissez Modifier le fournisseur d'identité SAML 2.0.
6. Cochez la case Activer l'authentification SAML 2.0.
7. Entrez l'URL d'accès utilisateur pour diriger le client WorkSpaces Pools lors de la connexion fédérée.
8. Entrez le nom du paramètre de lien profond IdP (facultatif).
9. Choisissez Enregistrer.

Pour activer et configurer l'authentification basée sur des certificats

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez le répertoire que vous souhaitez configurer.
4. Accédez à Authentification et choisissez Modifier.
5. Choisissez Modifier l'authentification basée sur les certificats.
6. Cochez la case Activer l'authentification basée sur les certificats.
7. Choisissez dans le menu déroulant l'autorité de certification privée AWS Certificate Manager (ACM) (CA).
8. Choisissez Enregistrer.

Groupe de sécurité

Appliquez un groupe de sécurité à vos WorkSpaces pools dans votre annuaire.

Pour configurer le groupe de sécurité pour vos WorkSpaces pools

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez le répertoire que vous souhaitez configurer.
4. Accédez au groupe de sécurité et choisissez Modifier.
5. Dans le menu déroulant, sélectionnez un groupe de sécurité.

Config Active Directory

Configurez votre annuaire Active Directory Config avec une unité organisationnelle (UO), un nom de domaine de répertoire et un secret du Gestionnaire de AWS Secrets Manager.

Pour configurer votre Active Directory

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez le répertoire que vous souhaitez configurer.
4. Accédez à Active Directory Config et choisissez Modifier.
5. Pour trouver une unité organisationnelle (UO), vous pouvez commencer à taper tout ou partie du nom de l'UO et choisir l'UO que vous souhaitez utiliser.

 Note

(Facultatif) Après avoir choisi l'unité d'organisation, reconstruisez l'unité existante WorkSpaces pour mettre à jour l'unité d'organisation. Pour de plus amples informations, consultez [Reconstruire un Workspace in WorkSpaces Personal](#).

6. Choisissez Enregistrer.

 Note

Le nom de domaine du répertoire et le secret du Gestionnaire de AWS Secrets Manager ne peuvent pas être modifiés une fois que vous avez créé votre pool.

Propriétés du streaming

Configurez la manière dont vos utilisateurs peuvent transférer des données entre leur appareil groupé WorkSpace et leur appareil local.

Pour configurer les propriétés du streaming

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez le répertoire que vous souhaitez configurer.
4. Accédez aux propriétés du streaming et choisissez Modifier.
5. Configurez les propriétés de streaming suivantes :
 - Autorisations du presse-papiers
 - Dans la liste déroulante, sélectionnez l'une des options suivantes :
 - Autoriser le copier-coller : permet de copier sur un appareil local et de coller sur une session à distance.
 - Autoriser le collage dans une session distante : autorise le collage dans une session distante.
 - Autoriser la copie sur un appareil local - Permet de copier sur un appareil local.
 - Désactivé

- Choisissez d'autoriser ou non l'impression sur le périphérique local.
- Choisissez d'autoriser ou non la journalisation des diagnostics.
- Choisissez d'autoriser ou non la connexion par carte à puce.
- Pour activer le stockage des dossiers personnels, choisissez Activer les dossiers personnels.

6. Choisissez Enregistrer.

Rôle IAM

Sélectionnez un rôle IAM pour vos WorkSpaces pools.

Pour sélectionner un rôle IAM

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez le répertoire que vous souhaitez configurer.
4. Accédez au rôle IAM et choisissez Modifier.
5. Choisissez un rôle IAM dans le menu déroulant. Pour créer un nouveau rôle IAM, choisissez Créer un nouveau rôle IAM.
6. Choisissez Enregistrer.

Étiquettes

Ajoutez de nouveaux tags à vos WorkSpaces piscines

Pour ajouter un nouveau tag

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez le répertoire que vous souhaitez configurer.
4. Accédez à Tags, puis sélectionnez Gérer les tags.
5. Choisissez Ajouter de nouvelles balises et entrez la valeur de la paire de clés que vous souhaitez utiliser. Une clé peut être une catégorie générale, telle que « projet », « propriétaire » ou « environnement », avec des valeurs associées spécifiques.
6. Sélectionnez Enregistrer les modifications.

Supprimer un répertoire WorkSpaces Pools

Suivez les procédures ci-dessous pour supprimer un répertoire WorkSpaces Pools.

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Sélectionnez l'annuaire.
4. Sélectionnez Actions, Supprimer.
5. Lorsque vous êtes invité **delete** à confirmer, entrez le texte de confirmation et choisissez Supprimer.

Mise en réseau et accès pour les WorkSpaces piscines

Les rubriques suivantes fournissent des informations sur le fait de permettre aux utilisateurs de se connecter aux WorkSpaces pools et de permettre à vos WorkSpaces pools d'accéder aux ressources du réseau et à Internet.

Table des matières

- [Accès Internet pour WorkSpaces piscines](#)
- [Configuration d'un VPC pour les pools WorkSpaces](#)
- [Configurer l'autorisation FedRAMP ou la conformité DoD SRG pour les pools WorkSpaces](#)
- [Fonctionnalités d'utilisation des points de terminaison VPC Amazon S3 pour les pools WorkSpaces](#)
- [Connexions à votre VPC pour les pools WorkSpaces](#)
- [Connexions utilisateur aux WorkSpaces pools](#)

Accès Internet pour WorkSpaces piscines

Si votre WorkSpaces in WorkSpaces Pools nécessite un accès à Internet, vous pouvez l'activer de plusieurs manières. Lorsque vous choisissez une méthode pour activer l'accès à Internet, tenez compte du nombre d'utilisateurs que votre déploiement doit prendre en charge et de vos objectifs de déploiement. Par exemple :

- Si votre déploiement doit prendre en charge plus de 100 utilisateurs simultanés, [configurez un VPC avec des sous-réseaux privés et une passerelle NAT](#).

- Si votre déploiement prend en charge moins de 100 utilisateurs simultanés, vous pouvez [configurer un VPC nouveau ou existant avec un sous-réseau public](#).
- Si votre déploiement prend en charge moins de 100 utilisateurs simultanés, que vous utilisez WorkSpaces Pools pour la première fois et que vous souhaitez commencer à utiliser le service, vous pouvez [utiliser le VPC, le sous-réseau public et le groupe de sécurité par défaut](#).

Les sections suivantes fournissent davantage d'informations sur chacune de ces options de déploiement.

- [Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT](#) (recommandé) — Avec cette configuration, vous lancez vos générateurs de WorkSpaces pools dans un sous-réseau privé et configurez une passerelle NAT dans un sous-réseau public de votre VPC. Vos instances de streaming se voient attribuer une adresse IP privée qui n'est pas directement accessible depuis Internet.

En outre, contrairement aux configurations qui utilisent l'option d'accès Internet par défaut pour activer l'accès à Internet, la configuration NAT n'est pas limitée à 100 WorkSpaces dans les WorkSpaces pools. Si votre déploiement doit prendre en charge plus de 100 utilisateurs simultanés, utilisez cette configuration.

Vous pouvez créer et configurer un nouveau VPC à utiliser avec une passerelle NAT ou ajouter une passerelle NAT à un VPC existant.

- [Configuration d'un VPC, nouveau ou existant, avec un sous-réseau public](#) — Avec cette configuration, vous lancez vos WorkSpaces pools dans un sous-réseau public. Lorsque vous activez cette option, WorkSpaces Pools utilise la passerelle Internet de votre sous-réseau public Amazon VPC pour fournir la connexion Internet. Vos instances de streaming se voient attribuer une adresse IP publique directement accessible à partir d'Internet. Vous pouvez créer un VPC ou en configurer un existant.

 Note

Lorsque vous configurez un VPC nouveau ou existant avec un sous-réseau public, un maximum de 100 VPC WorkSpaces sont pris en charge dans les pools. WorkSpaces Si votre déploiement doit prendre en charge plus de 100 utilisateurs simultanés, utilisez plutôt la [configuration de la passerelle NAT](#).

- [Utilisation du VPC, du sous-réseau public et du groupe de sécurité par défaut](#)— Si vous utilisez WorkSpaces Pools pour la première fois et que vous souhaitez commencer à utiliser le service, vous pouvez lancer vos WorkSpaces Pools dans un sous-réseau public par défaut. Lorsque vous activez cette option, WorkSpaces Pools utilise la passerelle Internet de votre sous-réseau public Amazon VPC pour fournir la connexion Internet. Vos instances de streaming se voient attribuer une adresse IP publique directement accessible à partir d'Internet.

VPCs Les comptes Amazon Web Services créés après le 04/12/2013 sont disponibles par défaut.

Le VPC par défaut inclut un sous-réseau public par défaut dans chaque zone de disponibilité et une passerelle Internet qui est attachée à votre VPC. Le VPC inclut également un groupe de sécurité par défaut.

 Note

Lorsque vous utilisez le VPC, le sous-réseau public et le groupe de sécurité par défaut, un maximum de 100 WorkSpaces sont pris en charge dans les pools. WorkSpaces Si votre déploiement doit prendre en charge plus de 100 utilisateurs simultanés, utilisez plutôt la [configuration de la passerelle NAT](#).

Configuration d'un VPC pour les pools WorkSpaces

Lorsque vous configurez WorkSpaces des pools, vous devez spécifier le cloud privé virtuel (VPC) et au moins un sous-réseau dans lequel lancer votre. WorkSpaces Un VPC est un réseau virtuel situé dans votre propre zone isolée logiquement au sein du cloud Amazon Web Services. Un sous-réseau est une plage d'adresses IP dans votre VPC.

Lorsque vous configurez votre VPC pour les WorkSpaces pools, vous pouvez spécifier des sous-réseaux publics ou privés, ou une combinaison des deux types de sous-réseaux. Un sous-réseau public accède directement à Internet via une passerelle Internet. Un sous-réseau privé, qui ne comporte pas de route vers une passerelle Internet, nécessite une passerelle NAT (Network Address Translation) ou une instance NAT pour fournir l'accès à Internet.

Table des matières

- [Recommandations de configuration VPC pour les pools WorkSpaces](#)
- [Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT](#)
- [Configuration d'un VPC, nouveau ou existant, avec un sous-réseau public](#)

- [Utilisation du VPC, du sous-réseau public et du groupe de sécurité par défaut](#)

Recommandations de configuration VPC pour les pools WorkSpaces

Lorsque vous créez un WorkSpaces pool, vous spécifiez le VPC et un ou plusieurs sous-réseaux à utiliser. Vous pouvez fournir un contrôle d'accès supplémentaire à votre VPC en spécifiant des groupes de sécurité.

Les recommandations suivantes peuvent vous aider à configurer votre VPC de façon plus efficace et sécurisée. En outre, ils peuvent vous aider à configurer un environnement qui permet une mise à l'échelle efficace WorkSpaces des pools. Grâce à une mise à l'échelle efficace des WorkSpaces pools, vous pouvez répondre à la demande actuelle et prévue des WorkSpaces utilisateurs, tout en évitant l'utilisation inutile des ressources et les coûts associés.

Configuration générale du VPC

- Assurez-vous que votre configuration VPC peut répondre aux besoins de dimensionnement de vos WorkSpaces pools.

Lorsque vous élaborez votre plan de mise à l'échelle des WorkSpaces pools, gardez à l'esprit qu'un utilisateur en a besoin WorkSpaces. Par conséquent, la taille de vos WorkSpaces pools détermine le nombre d'utilisateurs qui peuvent diffuser simultanément. C'est pourquoi, pour chaque [type d'instance](#) que vous prévoyez d'utiliser, assurez-vous que le nombre d'instances WorkSpaces que votre VPC peut prendre en charge est supérieur au nombre d'utilisateurs simultanés prévus pour le même type d'instance.

- Assurez-vous que les quotas de votre compte WorkSpaces Pools (également appelés limites) sont suffisants pour répondre à la demande prévue. Pour demander une augmentation de quota, vous pouvez utiliser la console Service Quotas à l'adresse <https://console.aws.amazon.com/servicequotas/>. Pour plus d'informations sur les quotas de WorkSpaces pool par défaut, consultez [WorkSpaces Quotas Amazon](#).
- Si vous envisagez de fournir WorkSpaces à vos WorkSpaces pools un accès à Internet, nous vous recommandons de configurer un VPC avec deux sous-réseaux privés pour vos instances de streaming et une passerelle NAT dans un sous-réseau public.

La passerelle NAT permet WorkSpaces aux sous-réseaux privés de se connecter à Internet ou à d'autres AWS services. Cependant, cela empêche Internet d'établir une connexion avec ceux-ci WorkSpaces. En outre, contrairement aux configurations qui utilisent l'option d'accès Internet par défaut pour activer l'accès à Internet, la configuration NAT en prend en charge plus de 100

WorkSpaces. Pour de plus amples informations, veuillez consulter [Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT](#).

Interfaces réseau Elastic

- WorkSpaces Les pools créent autant d'[interfaces réseau élastiques](#) (interfaces réseau) que la capacité maximale souhaitée de vos WorkSpaces pools. Par défaut, la limite des interfaces réseau par région est de 5 000.

Lorsque vous planifiez la capacité pour des déploiements de très grande envergure, par exemple des milliers WorkSpaces, tenez compte du nombre d'instances Amazon EC2 également utilisées dans la même région.

Sous-réseaux

- Si vous configurez plusieurs sous-réseaux privés pour votre VPC, configurez chacun d'eux dans une zone de disponibilité différente. En procédant ainsi, vous augmentez la tolérance aux pannes et contribuez à réduire le risque d'erreurs de capacité insuffisante. Si vous utilisez deux sous-réseaux dans la même zone de distribution, vous risquez de manquer d'adresses IP, car les WorkSpaces pools n'utiliseront pas le second sous-réseau.
- Assurez-vous également que les ressources réseau requises pour vos applications sont accessibles via vos deux sous-réseaux privés.
- Configurez chacun de vos sous-réseaux privés avec un masque de sous-réseau qui permet d'avoir un nombre suffisant d'adresses IP client pour prendre en compte le nombre maximal d'utilisateurs simultanés prévu. De plus, prévoyez des adresses IP supplémentaires pour répondre à la demande à venir. Pour plus d'informations, consultez la section [Dimensionnement des VPC et des sous-réseaux](#) pour IPv4.
- Si vous utilisez un VPC avec une passerelle NAT, configurez au moins un sous-réseau public avec une passerelle NAT pour l'accès à Internet, de préférence deux. Configurez les sous-réseaux publics dans les zones de disponibilité où résident vos sous-réseaux privés.

Pour améliorer la tolérance aux pannes et réduire le risque d'erreurs liées à une capacité insuffisante lors de déploiements de WorkSpaces pools de grande taille, envisagez d'étendre votre configuration VPC à une troisième zone de disponibilité. Ajoutez un sous-réseau privé, un sous-réseau public et une passerelle NAT à cette zone de disponibilité supplémentaire.

Groupes de sécurité

- Utilisez des groupes de sécurité pour fournir un contrôle d'accès supplémentaire à votre VPC.

Les groupes de sécurité appartenant à votre VPC vous permettent de contrôler le trafic réseau entre les instances de streaming de WorkSpaces Pools et les ressources réseau requises par les applications. Ces ressources peuvent inclure d'autres AWS services tels qu'Amazon RDS ou Amazon FSx, des serveurs de licences, des serveurs de base de données, des serveurs de fichiers et des serveurs d'applications.

- Assurez-vous que les groupes de sécurité donnent accès aux ressources réseau dont vos applications ont besoin.

Pour obtenir des informations générales sur les groupes de sécurité, consultez la section [Contrôler le trafic vers vos AWS ressources à l'aide de groupes de sécurité](#) dans le guide de l'utilisateur Amazon VPC.

Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT

Si vous envisagez de fournir WorkSpaces à vos WorkSpaces pools un accès à Internet, nous vous recommandons de configurer un VPC avec deux sous-réseaux privés pour vos WorkSpaces et une passerelle NAT dans un sous-réseau public. Vous pouvez créer et configurer un nouveau VPC à utiliser avec une passerelle NAT ou ajouter une passerelle NAT à un VPC existant. Pour d'autres recommandations concernant la configuration d'un VPC, consultez [Recommandations de configuration VPC pour les pools WorkSpaces](#).

La passerelle NAT permet WorkSpaces aux sous-réseaux privés de se connecter à Internet ou à d'autres AWS services, mais empêche Internet d'établir une connexion avec ceux-ci WorkSpaces. En outre, contrairement aux configurations qui utilisent l'option Accès Internet par défaut pour activer l'accès à Internet pour WorkSpaces, cette configuration n'est pas limitée à 100 WorkSpaces.

Pour plus d'informations sur l'utilisation de passerelles NAT et cette configuration, consultez [Passerelles NAT](#) et [VPC avec des sous-réseaux publics et privés \(NAT\)](#) dans le Guide de l'utilisateur Amazon VPC.

Table des matières

- [Création et configuration d'un VPC](#)
- [Ajout d'une passerelle NAT à un VPC existant](#)
- [Activer l'accès à Internet pour les WorkSpaces pools](#)

Création et configuration d'un VPC

Cette rubrique décrit comment utiliser l'Assistant VPC pour créer un VPC avec un sous-réseau public et un sous-réseau privé. Dans le cadre de cette procédure, l'assistant crée une passerelle Internet et une passerelle NAT. Il crée également une table de routage personnalisée associée au sous-réseau public et met à jour la table de routage principale associée au sous-réseau privé. La passerelle NAT est automatiquement créée dans le sous-réseau public de votre VPC.

Après avoir utilisé l'assistant pour créer la configuration initiale du VPC, vous allez ajouter un deuxième sous-réseau privé. Pour plus d'informations sur cette configuration, consultez [VPC avec des sous-réseaux publics et privés \(NAT\)](#) dans le Guide de l'utilisateur Amazon VPC.

Note

Si vous disposez déjà d'un VPC, suivez la procédure de la section [Ajout d'une passerelle NAT à un VPC existant](#).

Table des matières

- [Étape 1 : allouer une adresse IP Elastic](#)
- [Étape 2 : créer un VPC](#)
- [Étape 3 : ajout d'un deuxième sous-réseau privé](#)
- [Étape 4 : vérifier et nommer les tables de routage de votre sous-réseau](#)

Étape 1 : allouer une adresse IP Elastic

Avant de créer votre VPC, vous devez attribuer une adresse IP élastique dans votre WorkSpaces région. Vous devez d'abord allouer une adresse IP Elastic à utiliser dans votre VPC, puis l'associer à votre passerelle NAT. Pour plus d'informations, consultez [Adresses IP Elastic](#) dans le Guide de l'utilisateur Amazon VPC.

Note

Des frais peuvent s'appliquer aux adresses IP Elastic que vous utilisez. Pour plus d'informations, consultez [Adresses IP Elastic](#) sur la page Tarification d'Amazon EC2.

Procédez comme suit si vous ne disposez pas déjà d'une adresse IP Elastic. Si vous voulez utiliser une adresse IP Elastic existante, vérifiez qu'elle n'est pas déjà associée à une autre instance ou interface réseau.

Pour allouer une adresse IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Réseau et sécurité, sélectionnez Elastic IPs.
3. Choisissez Allouer une nouvelle adresse, puis Allouer.
4. Notez l'adresse IP Elastic.
5. Dans le coin supérieur droit du IPs volet Elastic, cliquez sur l'icône X pour fermer le volet.

Étape 2 : créer un VPC

Procédez comme suit pour créer un VPC avec un sous-réseau public et un sous-réseau privé.

Pour créer un VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Tableau de bord du VPC.
3. Choisissez Launch VPC Wizard (Démarrer l'assistant VPC).
4. À l'Étape 1 : sélectionner une configuration VPC, choisissez VPC avec des sous-réseaux publics et privés, puis Sélectionner.
5. À l'Étape 2 : VPC avec des sous-réseaux publics et privés, configurez le VPC comme suit :
 - Pour le bloc IPv4 CIDR, spécifiez un bloc IPv4 CIDR pour le VPC.
 - Pour le bloc IPv6 CIDR, conservez la valeur par défaut, No IPv6 CIDR Block.
 - Pour Nom du VPC, saisissez un nom unique pour le VPC.
6. Configurez le sous-réseau public en procédant comme suit :
 - Pour le IPv4 CIDR du sous-réseau public, spécifiez le bloc CIDR du sous-réseau.
 - Pour Zone de disponibilité, conservez la valeur par défaut, Aucune préférence.
 - Pour Nom du sous-réseau public, nommez le sous-réseau (par exemple, WorkSpaces Public Subnet).
7. Configurez le premier sous-réseau privé en procédant comme suit :

- Pour le IPv4 CIDR du sous-réseau privé, spécifiez le bloc CIDR du sous-réseau. Notez la valeur que vous spécifiez.
 - Pour Zone de disponibilité, sélectionnez une zone spécifique et notez-la.
 - Pour Nom de sous-réseau privé, nommez le sous-réseau (par exemple, WorkSpaces Private Subnet1).
 - Pour les champs restants, si applicable, conservez les valeurs par défaut.
8. Pour ID d'allocation d'adresses IP Elastic, cliquez dans la zone de texte et sélectionnez la valeur correspondant à l'adresse IP Elastic que vous avez créée. Cette adresse est assignée à la passerelle NAT. Si vous n'avez pas d'adresse IP élastique, créez-en une à l'aide de la console Amazon VPC à l'adresse. <https://console.aws.amazon.com/vpc/>
9. Pour Points de terminaison de service, si un point de terminaison Amazon S3 est requis pour votre environnement, spécifiez-en un. Un point de terminaison S3 est requis pour fournir aux utilisateurs un accès aux [dossiers de base](#) ou pour activer la [persistance des paramètres d'application](#) pour vos utilisateurs dans un réseau privé.

Pour spécifier un point de terminaison Amazon S3, procédez comme suit :

- a. Choisissez Ajouter un point de terminaison.
 - b. Pour Service, sélectionnez l'entrée dans la liste qui se termine par « s3 » (l'com.amazonaws.*region*.s3entrée correspondant à la région dans laquelle le VPC est créé).
 - c. Pour Sous-réseau, choisissez Sous-réseau privé.
 - d. Pour Stratégie, conservez la valeur par défaut Accès complet.
10. Pour Activer les noms d'hôte DNS, conservez la valeur par défaut Oui.
11. Pour Location matérielle, conservez la valeur par défaut Par défaut.
12. Sélectionnez Create VPC (Créer un VPC).
13. Notez que la configuration de votre VPC ne prend que quelques minutes. Après avoir créé le VPC, choisissez OK.

Étape 3 : ajout d'un deuxième sous-réseau privé

Au cours de l'étape précédente ([Étape 2 : créer un VPC](#)), vous avez créé un VPC avec un sous-réseau public et un sous-réseau privé. Procédez comme suit pour ajouter un deuxième sous-réseau

privé. Nous vous recommandons d'ajouter un deuxième sous-réseau privé dans une autre zone de disponibilité que celle de votre premier sous-réseau privé.

1. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
2. Sélectionnez le premier sous-réseau privé que vous avez créé à l'étape précédente. Sous l'onglet Description, sous la liste des sous-réseaux, notez la zone de disponibilité de ce sous-réseau.
3. Dans l'angle supérieur gauche du volet des sous-réseaux, choisissez Créer le sous-réseau.
4. Pour Balise Nom, nommez le sous-réseau privé (par exemple, `WorkSpaces Private Subnet2`).
5. Pour VPC, sélectionnez le VPC que vous avez créé à l'étape précédente.
6. Pour Zone de disponibilité, sélectionnez une zone de disponibilité autre que celle que vous utilisez pour votre premier sous-réseau privé. La sélection d'une autre zone de disponibilité augmente la tolérance aux pannes et permet de réduire le risque d'erreurs de capacité insuffisante.
7. Pour le bloc IPv4 CIDR, spécifiez une plage de blocs CIDR unique pour le nouveau sous-réseau. Par exemple, si votre premier sous-réseau privé possède une plage de blocs d'IPv4 adresse CIDR de `10.0.1.0/24`, vous pouvez spécifier une plage de blocs d'adresse CIDR de `10.0.2.0/24` pour le nouveau sous-réseau privé.
8. Choisissez Créer.
9. Une fois le sous-réseau créé, choisissez Fermer.

Étape 4 : vérifier et nommer les tables de routage de votre sous-réseau

Après avoir créé et configuré votre VPC, procédez comme suit pour nommer vos tables de routage et vérifiez que :

- La table de routage associée au sous-réseau dans lequel réside votre passerelle NAT comprend un itinéraire qui pointe le trafic Internet vers une passerelle Internet. Votre passerelle NAT peut ainsi accéder à Internet.
- Les tables de routage associées à vos sous-réseaux privés sont configurées pour pointer le trafic Internet vers la passerelle NAT. Les instances de streaming de vos sous-réseaux privés peuvent ainsi communiquer avec Internet.

1. Dans le volet de navigation, choisissez Sous-réseaux, puis sélectionnez le sous-réseau public que vous avez créé (par exemple, `WorkSpaces Public Subnet`).
 - a. Sous l'onglet Table de routage, choisissez l'ID de la table de routage (par exemple, `rtb-12345678`).
 - b. Sélectionnez la table de routage. Sous Nom, choisissez l'icône de modification (en forme de crayon), saisissez un nom (par exemple, `workspaces-public-routetable`), puis sélectionnez la case à cocher pour enregistrer le nom.
 - c. Avec la table de routage publique toujours sélectionnée, sous l'onglet Routes, vérifiez qu'il existe une route pour le trafic local et une autre qui achemine tout le reste du trafic vers la passerelle Internet du VPC. Le tableau suivant décrit ces deux routes :

Destination	Cible	Description
Bloc IPv4 CIDR du sous-réseau public (par exemple, <code>10.0.0/20</code>)	Local	Tout le trafic provenant des ressources destinées IPv4 aux adresses du bloc IPv4 CIDR du sous-réseau public est acheminé localement au sein du VPC.
Trafic destiné à toutes les autres IPv4 adresses (par exemple, <code>0.0.0.0/0</code>)	Sortant () <code>igw- <i>ID</i></code>	Le trafic destiné à toutes les autres IPv4 adresses est acheminé vers la passerelle Internet (identifiée par <code>igw- <i>ID</i></code>) créée par l'assistant VPC.

2. Dans le volet de navigation, sélectionnez Sous-réseaux, puis sélectionnez le premier sous-réseau privé que vous avez créé (par exemple, `WorkSpaces Private Subnet1`).
 - a. Dans l'onglet Route Table (Table de routage), choisissez l'ID de la table de routage.
 - b. Sélectionnez la table de routage. Sous Nom, choisissez l'icône de modification (en forme de crayon), saisissez un nom (par exemple, `workspaces-private-routetable`), puis sélectionnez la case à cocher pour enregistrer le nom.
 - c. Sous l'onglet Routes, vérifiez que la table de routage comprend les routes suivantes :

Destination	Cible	Description
Bloc IPv4 CIDR du sous-réseau public (par exemple, 10.0.0/20)	Local	Tout le trafic provenant des ressources destinées IPv4 aux adresses du bloc IPv4 CIDR du sous-réseau public est acheminé localement au sein du VPC.
Trafic destiné à toutes les autres IPv4 adresses (par exemple, 0.0.0.0/0)	Sortant () nat - <i>ID</i>	Le trafic destiné à toutes les autres IPv4 adresses est acheminé vers la passerelle NAT (identifiée par nat - <i>ID</i>).
Trafic destiné aux compartiments S3 (applicable si vous avez spécifié un point de terminaison S3) [p1 - <i>ID</i> (com. amazons. <i>region</i> .s3)]	Rangement (vpce - <i>ID</i>)	Le trafic destiné aux compartiments S3 est acheminé vers le point de terminaison S3 (identifié par vpce - <i>ID</i>).

3. Dans le volet de navigation, choisissez Sous-réseaux, puis sélectionnez le deuxième sous-réseau privé que vous avez créé (par exemple, WorkSpaces Private Subnet2).
4. Sous l'onglet Table de routage, vérifiez que la table de routage est bien la table de routage privée (par exemple, workspaces-private-routetable). Si la table de routage est différente, choisissez Edit (Modifier), puis sélectionnez cette table de routage.

Étapes suivantes

Pour permettre à votre WorkSpaces in WorkSpaces Pools d'accéder à Internet, suivez les étapes décrites dans [Activer l'accès à Internet pour les WorkSpaces pools](#).

Ajout d'une passerelle NAT à un VPC existant

Si vous avez déjà configuré un VPC, procédez comme suit pour ajouter une passerelle NAT à votre VPC. Si vous devez créer un VPC, consultez [Création et configuration d'un VPC](#).

Pour ajouter une passerelle NAT à un VPC existant

1. Pour créer votre passerelle NAT, suivez les étapes décrites dans la section [Création d'une passerelle NAT](#) dans le Guide de l'utilisateur Amazon VPC.
2. Vérifiez que votre VPC possède au moins un sous-réseau privé. Nous vous recommandons de spécifier deux sous-réseaux privés dans différentes zones de disponibilité pour une haute disponibilité et une tolérance aux pannes. Pour plus d'informations sur la création d'un deuxième sous-réseau privé, consultez [Étape 3 : ajout d'un deuxième sous-réseau privé](#).
3. Mettez à jour la table de routage associée à un ou plusieurs de vos sous-réseaux privés pour pointer le trafic Internet vers la passerelle NAT. Les instances de streaming de vos sous-réseaux privés peuvent ainsi communiquer avec Internet. Pour ce faire, suivez les étapes décrites dans la section [Mise à jour de votre table de routage](#) dans le Guide de l'utilisateur Amazon VPC.

Étapes suivantes

Pour permettre à votre WorkSpaces in WorkSpaces Pools d'accéder à Internet, suivez les étapes décrites dans [Activer l'accès à Internet pour les WorkSpaces pools](#).

Activer l'accès à Internet pour les WorkSpaces pools

Une fois que votre passerelle NAT est disponible sur un VPC, vous pouvez activer l'accès à Internet pour vos WorkSpaces pools. Vous pouvez activer l'accès à Internet lorsque vous [créez le répertoire WorkSpaces Pool](#). Choisissez le VPC doté d'une passerelle NAT lorsque vous créez le répertoire. Sélectionnez ensuite un sous-réseau privé pour le sous-réseau 1 et, éventuellement, un autre sous-réseau privé pour le sous-réseau 2. Si vous ne possédez pas déjà de sous-réseau privé dans votre VPC, vous devrez peut-être créer un deuxième sous-réseau privé.

Vous pouvez tester votre connectivité Internet en démarrant votre WorkSpaces pool, puis en vous connectant à un pool et Workspace en naviguant sur Internet.

Configuration d'un VPC, nouveau ou existant, avec un sous-réseau public

Si vous avez créé votre compte Amazon Web Services après le 4 décembre 2013, vous disposez d'un [VPC](#) par défaut dans chaque AWS région qui inclut des sous-réseaux publics par défaut. Toutefois, vous souhaitez peut-être créer votre propre VPC autre que celui par défaut ou configurer un VPC existant à utiliser avec votre répertoire de pool. WorkSpaces Cette rubrique décrit comment configurer un VPC et un sous-réseau public autres que ceux par défaut à utiliser avec des pools. WorkSpaces

Après avoir configuré votre VPC et votre sous-réseau public, vous pouvez fournir WorkSpaces à vos WorkSpaces pools un accès à Internet en activant l'option Accès Internet par défaut. Lorsque vous activez cette option, WorkSpaces Pools active la connectivité Internet en associant une [adresse IP élastique](#) à l'interface réseau attachée par l'instance de streaming à votre sous-réseau public. Une adresse IP élastique est une IPv4 adresse publique accessible depuis Internet. Pour cette raison, nous vous recommandons d'utiliser plutôt une passerelle NAT pour fournir un accès Internet à votre WorkSpaces in WorkSpaces Pools. En outre, lorsque l'accès Internet par défaut est activé, un maximum de 100 WorkSpaces sont pris en charge. Si votre déploiement doit prendre en charge plus de 100 utilisateurs simultanés, utilisez plutôt la [configuration de la passerelle NAT](#).

Pour plus d'informations, suivez la procédure de la section [Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT](#). Pour d'autres recommandations concernant la configuration d'un VPC, consultez [Recommandations de configuration VPC pour les pools WorkSpaces](#).

Table des matières

- [Étape 1 : configurer un VPC avec un sous-réseau public](#)
- [Étape 2 : activer l'accès Internet par défaut pour vos WorkSpaces pools](#)

Étape 1 : configurer un VPC avec un sous-réseau public

Vous pouvez configurer votre propre VPC personnalisé avec un sous-réseau public à l'aide de l'une des méthodes suivantes :

- [Créer un VPC avec un seul sous-réseau public](#)
- [Configurer un VPC existant](#)

Créer un VPC avec un seul sous-réseau public

Lorsque vous utilisez l'Assistant VPC pour créer un VPC, l'Assistant crée une passerelle Internet et une table de routage personnalisée associée au sous-réseau public. La table de routage achemine tout le trafic destiné à une adresse extérieure au VPC vers la passerelle Internet. Pour plus d'informations sur cette configuration, consultez [VPC avec un sous-réseau public unique](#) dans le Guide de l'utilisateur Amazon VPC.

1. Suivez la procédure de l'[Étape 1 : créer le VPC](#) du Guide de l'utilisateur Amazon VPC pour créer votre VPC.

2. Pour vous permettre WorkSpaces d'accéder à Internet, suivez les étapes décrites dans [Étape 2 : activer l'accès Internet par défaut pour vos WorkSpaces pools](#).

Configurer un VPC existant

Pour utiliser un VPC existant qui ne dispose pas d'un sous-réseau public, vous pouvez ajouter un nouveau sous-réseau public. Outre un sous-réseau public, vous devez également avoir une passerelle Internet attachée à votre VPC et une table de routage qui achemine tout le trafic destiné à une adresse extérieure au VPC vers la passerelle Internet. Pour configurer ces composants, procédez comme suit.

1. Pour ajouter un sous-réseau public, suivez les étapes de la section [Création d'un sous-réseau dans votre VPC](#). Utilisez le VPC existant que vous prévoyez d'utiliser avec WorkSpaces les pools.

Si votre VPC est configuré pour prendre en charge l'IPv6 adressage, la liste de blocage IPv6 CIDR s'affiche. Sélectionnez Ne pas attribuer de bloc CIDR IPv6.

2. Pour créer et attacher une passerelle Internet à votre VPC, suivez la procédure de la section [Création et attachement d'une passerelle Internet](#).
3. Pour configurer votre sous-réseau afin qu'il achemine le trafic Internet via la passerelle Internet, suivez la procédure de la section [Création d'une table de routage personnalisée](#). À l'étape 5, pour Destination, utilisez IPv4 format (0.0.0.0/0).
4. Pour permettre à vos créateurs d'images WorkSpaces et à vous-même d'accéder à Internet, suivez les étapes décrites dans [Étape 2 : activer l'accès Internet par défaut pour vos WorkSpaces pools](#).

Étape 2 : activer l'accès Internet par défaut pour vos WorkSpaces pools

Vous pouvez activer l'accès à Internet lorsque vous [créez le répertoire WorkSpaces Pool](#). Choisissez le VPC doté d'un sous-réseau public lorsque vous créez le répertoire. Sélectionnez ensuite un sous-réseau public pour le sous-réseau 1 et, éventuellement, un autre sous-réseau public pour le sous-réseau 2.

Vous pouvez tester votre connectivité Internet en démarrant votre WorkSpaces pool, puis en vous connectant à un pool et Workspace en naviguant sur Internet.

Utilisation du VPC, du sous-réseau public et du groupe de sécurité par défaut

Votre compte Amazon Web Services, s'il a été créé après le 04/12/2013, possède un VPC par défaut dans chaque région. AWS Le VPC par défaut inclut un sous-réseau public par défaut dans chaque zone de disponibilité et une passerelle Internet qui est attachée à votre VPC. Le VPC inclut également un groupe de sécurité par défaut. Si vous utilisez WorkSpaces Pools pour la première fois et que vous souhaitez commencer à utiliser le service, vous pouvez conserver le VPC et le groupe de sécurité par défaut sélectionnés lorsque vous créez un WorkSpaces pool. Ensuite, vous pouvez sélectionner au moins un sous-réseau par défaut.

Note

Si votre compte Amazon Web Services a été créé avant le 04/12/2013, vous devez créer un nouveau VPC ou en configurer un existant pour l'utiliser avec les pools. WorkSpaces Nous vous recommandons de configurer manuellement un VPC avec deux sous-réseaux privés pour vos WorkSpaces pools et une passerelle NAT dans un sous-réseau public. Pour de plus amples informations, veuillez consulter [Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT](#). Vous pouvez également configurer un VPC personnalisé avec un sous-réseau public. Pour de plus amples informations, veuillez consulter [Configuration d'un VPC, nouveau ou existant, avec un sous-réseau public](#).

Vous pouvez activer l'accès à Internet lorsque vous [créez le répertoire WorkSpaces Pool](#).

Choisissez le VPC par défaut lorsque vous créez le répertoire. Le nom du VPC par défaut utilise le format suivant : `vpc- vpc-id (No_default_value_Name)`

Sélectionnez ensuite un sous-réseau public par défaut pour le sous-réseau 1 et, éventuellement, un autre sous-réseau public par défaut pour le sous-réseau 2. Les noms de sous-réseaux par défaut utilisent le format suivant : `subnet- subnet-id | ( IPv4 CIDR block ) | Default in availability-zone`.

Vous pouvez tester votre connectivité Internet en démarrant votre WorkSpaces pool, puis en vous connectant à un pool et Workspace en naviguant sur Internet.

Configurer l'autorisation FedRAMP ou la conformité DoD SRG pour les pools WorkSpaces

Pour vous conformer au [Federal Risk and Authorization Management Program \(FedRAMP\)](#) ou au [Guide des exigences de sécurité du cloud computing \(SRG\) du ministère de la Défense \(DoD\)](#), vous devez configurer WorkSpaces Amazon Pools pour utiliser le chiffrement des points de terminaison FIPS (Federal Information Processing Standards) au niveau du répertoire. Vous devez également utiliser une AWS région des États-Unis agréée par FedRAMP ou conforme aux normes SRG du DoD.

Le niveau d'autorisation FedRAMP (modéré ou élevé) ou le niveau d'impact SRG du DoD (2, 4 ou 5) dépend de la AWS région des États-Unis dans laquelle Amazon est utilisé. WorkSpaces Pour connaître les niveaux d'autorisation FedRAMP et de conformité au SRG du DoD qui s'appliquent à chaque région, consultez [Services AWS concernés par le programme de conformité](#).

Prérequis

- Le répertoire WorkSpaces Pools doit être configuré pour utiliser le mode validé FIPS 140-2 pour le chiffrement des terminaux.

Note

Pour utiliser le paramètre Mode validé FIPS 140-2, assurez-vous de ce qui suit :

- Le répertoire WorkSpaces Pools est soit :
 - Nouveau et non associé à un pool
 - Associé à un pool existant à l'état STOPPÉ
 - Le répertoire du pool est [StreamingExperiencePreferredProtocol](#) défini sur TCP.
- Vous devez créer vos WorkSpaces pools dans une [AWS région des États-Unis agréée par FedRAMP ou](#) conforme aux normes SRG du DoD.
 - Les utilisateurs doivent y accéder WorkSpaces depuis l'une des applications WorkSpaces clientes suivantes :
 - macOS : 5.20.0 ou version ultérieure
 - Windows : 5.20.0 ou version ultérieure
 - Web Access

Pour utiliser le chiffrement des points de terminaison FIPS

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez Directories, puis choisissez le répertoire que vous souhaitez utiliser pour l'autorisation FedRAMP et la conformité aux SRG du DoD.
3. Sur la page Détails du répertoire, choisissez le répertoire que vous souhaitez configurer pour le mode de chiffrement FIPS.
4. Dans la section Chiffrement des terminaux, choisissez Modifier, puis sélectionnez le mode validé FIPS 140-2.
5. Choisissez Enregistrer.

Fonctionnalités d'utilisation des points de terminaison VPC Amazon S3 pour les pools WorkSpaces

Lorsque vous activez la persistance des paramètres d'application pour un WorkSpaces pool ou les dossiers de base pour un répertoire de WorkSpaces pool, WorkSpaces utilise le VPC que vous spécifiez pour votre répertoire afin de fournir un accès aux compartiments Amazon Simple Storage Service (Amazon S3). Pour activer l'accès WorkSpaces des pools à votre point de terminaison S3 privé, associez la politique personnalisée suivante à votre point de terminaison VPC pour Amazon S3. Pour plus d'informations sur les points de terminaison Amazon S3 privés, consultez [Points de terminaison d'un VPC](#) et [Points de terminaison pour Amazon S3](#) dans le Guide de l'utilisateur Amazon VPC.

Commercial Régions AWS

Utilisez la politique suivante pour les ressources figurant dans la publicité Régions AWS.

AWS GovCloud (US) Regions

Utilisez la politique suivante pour les ressources figurant dans la publicité AWS GovCloud (US) Regions.

Connexions à votre VPC pour les pools WorkSpaces

Pour activer la connectivité WorkSpaces des Pools aux ressources réseau et à Internet, configurez votre WorkSpaces pool comme suit.

Interfaces réseau

Chacune WorkSpaces des interfaces réseau de WorkSpaces Pools possède les interfaces réseau suivantes :

- L'interface réseau client fournit une connectivité aux ressources de votre VPC, ainsi qu'à Internet, et est utilisée pour les joindre WorkSpaces à votre annuaire.
- L'interface du réseau de gestion est connectée à un réseau de gestion sécurisé des WorkSpaces pools. Il est utilisé pour le streaming interactif du sur WorkSpace l'appareil d'un utilisateur et pour permettre aux WorkSpaces pools de gérer le Workspace.

WorkSpaces Pools sélectionne l'adresse IP de l'interface réseau de gestion dans la plage d'adresses IP privées suivante : 198.19.0.0/16. N'utilisez pas cette plage pour votre VPC CIDR ou n'associez pas votre VPC à un autre VPC de cette plage, car cela pourrait créer un conflit et rendre l'accès inaccessible. WorkSpaces De même, ne modifiez ni ne supprimez aucune des interfaces réseau associées à un Workspace, car cela pourrait également les Workspace rendre inaccessibles.

Ports et plage d'adresses IP d'interface de réseau de gestion

La plage d'adresses IP d'interface de réseau de gestion est 198.19.0.0/16. Les ports suivants doivent tous être ouverts sur l'interface du réseau de gestion WorkSpaces :

- TCP entrant sur le port 8300. Ce port est utilisé pour la création de la connexion de streaming.
- TCP sortant sur le port 3128. Ceci est utilisé pour la gestion de WorkSpaces.
- TCP entrant sur les ports 8000 et 8443. Ils sont utilisés pour la gestion du WorkSpaces.
- UDP entrant sur le port 8300. Ce port est utilisé pour l'établissement de la connexion de streaming via UDP.

Limitez la plage en entrée sur l'interface réseau de gestion à 198.19.0.0/16.

Note

Pour les WorkSpaces pools Windows Amazon DCV BYOL, les plages d'adresses IP 10.0.0.0/8 sont utilisées dans toutes les régions. AWS Ces plages d'adresses IP s'ajoutent au bloc CIDR /16 que vous choisissez pour le trafic de gestion dans vos pools WorkSpaces BYOL.

Dans des circonstances normales, WorkSpaces Pools configure correctement ces ports pour votre WorkSpaces. Si un logiciel de sécurité ou de pare-feu est installé sur un port WorkSpace qui bloque l'un de ces ports, celui-ci WorkSpaces risque de ne pas fonctionner correctement ou d'être inaccessible.

Ne le désactivez pas IPv6. Si vous le désactivez IPv6, WorkSpaces les pools ne fonctionneront pas correctement. Pour plus d'informations sur la configuration IPv6 pour Windows, consultez [les instructions de configuration IPv6 sous Windows pour les utilisateurs expérimentés](#).

Note

WorkSpaces Les pools s'appuient sur les serveurs DNS de votre VPC pour renvoyer une réponse de domaine inexistante (NXDOMAIN) pour les noms de domaine locaux qui n'existent pas. Cela permet à l'interface réseau WorkSpaces gérée par les pools de communiquer avec les serveurs de gestion.

Lorsque vous créez un annuaire avec Simple AD, il AWS Directory Service crée deux contrôleurs de domaine qui fonctionnent également en tant que serveurs DNS en votre nom. Comme les contrôleurs de domaine ne fournissent pas la réponse NXDOMAIN, ils ne peuvent pas être utilisés avec des WorkSpaces pools.

Ports d'interface réseau client

- Pour la connectivité Internet, les ports suivants doivent être ouverts à tous les destinations. Si vous utilisez un groupe de sécurité personnalisé ou modifié, vous devez ajouter les règles requises manuellement. Pour plus d'informations, consultez [Règles des groupes de sécurité](#) dans le Guide de l'utilisateur Amazon VPC.
 - TCP 80 (HTTP)
 - TCP 443 (HTTPS)
 - UDP 4195
- Si vous vous connectez WorkSpaces à un répertoire, les ports suivants doivent être ouverts entre votre VPC WorkSpaces Pools et vos contrôleurs de répertoire.
 - TCP/UDP 53 - DNS
 - TCP/UDP 88 - Authentification Kerberos
 - UDP 123 - NTP
 - TCP 135 - RPC

- UDP 137-138 - Netlogon
- TCP 139 - Netlogon
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP 1024-65535 - Ports dynamiques pour RPC

Pour obtenir la liste complète des ports, consultez les [exigences de port pour Active Directory et les services de domaine Active Directory](#) dans la documentation Microsoft.

- Tous WorkSpaces nécessitent que le port 80 (HTTP) soit ouvert à l'adresse IP 169.254.169.254 pour permettre l'accès au service de métadonnées EC2. La plage d'adresses IP 169.254.0.0/16 est réservée à l'utilisation du service WorkSpaces Pools pour le trafic de gestion. Le fait de ne pas exclure cette plage peut entraîner des problèmes de streaming.

Connexions utilisateur aux WorkSpaces pools

Les utilisateurs peuvent se connecter WorkSpaces à des WorkSpaces pools via le point de terminaison Internet public par défaut.

Par défaut, WorkSpaces Pools est configuré pour acheminer les connexions de streaming via l'Internet public. La connectivité Internet est requise pour authentifier les utilisateurs et fournir les ressources Web dont WorkSpaces Pools a besoin pour fonctionner. Pour autoriser ce trafic, vous devez autoriser les domaines répertoriés dans [Domaines autorisés](#).

Note

Pour l'authentification des utilisateurs, WorkSpaces Pools prend en charge le langage SAML 2.0 (Security Assertion Markup Language 2.0). Pour de plus amples informations, veuillez consulter [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#).

Les rubriques suivantes fournissent des informations sur la manière d'activer les connexions utilisateur aux WorkSpaces pools.

Table des matières

- [Recommandations de bande passante](#)
- [Exigences en matière d'adresse IP et de port pour les appareils utilisateur des WorkSpaces pools](#)

- [Domaines autorisés](#)

Recommandations de bande passante

Pour optimiser les performances des WorkSpaces pools, assurez-vous que la bande passante et la latence de votre réseau répondent aux besoins de vos utilisateurs.

WorkSpaces Pools utilise NICE Desktop Cloud Visualization (DCV) pour permettre à vos utilisateurs d'accéder à vos applications et de les diffuser en toute sécurité sur différentes conditions de réseau. Pour réduire la consommation de bande passante, NICE DCV utilise la compression et le codage vidéo H.264. Pendant les sessions de streaming, la sortie visuelle des applications est compressée, puis diffusée à vos utilisateurs en tant que flux de pixels chiffrés AES-256 via HTTPS. Une fois que le flux est reçu, il est déchiffré puis affiché sur l'écran local de vos utilisateurs. Lorsque les utilisateurs interagissent avec les applications de streaming, le protocole NICE DCV capture leurs entrées et les renvoie aux applications de streaming via HTTPS.

L'état du réseau est constamment mesuré au cours de ce processus et les informations sont WorkSpaces renvoyées aux Pools. WorkSpaces Pools répond de manière dynamique aux conditions changeantes du réseau en modifiant le codage vidéo et audio en temps réel afin de produire un flux de haute qualité pour une grande variété d'applications et de conditions réseau.

La bande passante et la latence recommandées pour les sessions de streaming WorkSpaces Pools dépendent de la charge de travail. Par exemple, si un utilisateur travaille avec des applications graphiques professionnelles afin d'effectuer des tâches de conception assistée par ordinateur, la bande passante requise sera plus élevée et la latence plus faible comparé aux valeurs requises pour un utilisateur qui travaille avec des applications de productivité pour écrire des documents.

Le tableau suivant fournit des conseils sur la bande passante réseau et la latence recommandées pour les sessions de streaming WorkSpaces Pools en fonction des charges de travail courantes.

Pour chaque charge de travail, la bande passante recommandée correspond à ce dont un utilisateur individuel pourrait avoir besoin à un moment précis. Par conséquent, la recommandation ne correspond pas à la bande passante requise pour un débit soutenu. Lorsque seulement quelques pixels changent à l'écran pendant une session de streaming, le débit soutenu est bien moins élevé. Bien que les utilisateurs disposant d'une bande passante moins élevée puissent quand même diffuser leurs applications, la fréquence d'images ou la qualité de ces dernières ne seront pas forcément optimales.

Charge de travail	Description	Bande passante recommandée par utilisateur	Latence aller-retour maximum recommandée
Applications métier	Applications d'écriture de documents, utilitaires d'analyse de bases de données	2 Mbit/s	< 150 ms
Applications graphiques	Applications de conception et de modélisation assistées par ordinateur, montage photo et vidéo	5 Mbit/s	< 100 ms
Haute fidélité	Ensembles de données haute fidélité ou mappages sur plusieurs écrans	10 Mbit/s	< 50 ms

Exigences en matière d'adresse IP et de port pour les appareils utilisateur des WorkSpaces pools

WorkSpaces Les appareils des utilisateurs des pools nécessitent un accès sortant sur les ports 443 (TCP) et 4195 (UDP) lorsqu'ils utilisent des points de terminaison Internet, et si vous utilisez des serveurs DNS pour la résolution des noms de domaine, le port 53 (UDP).

- Le port 443 est utilisé pour la communication HTTPS entre les appareils des utilisateurs de WorkSpaces Pools et WorkSpaces lors de l'utilisation des points de terminaison Internet. En général, lorsque les utilisateurs finaux parcourent le Web au cours de sessions de streaming, le navigateur Web sélectionne de façon aléatoire un port source dans la plage supérieure en vue d'une utilisation pour le trafic de streaming. Vous devez vérifier que le trafic de retour renvoyé vers ce port est autorisé.

- Le port 4195 est utilisé pour la communication HTTPS UDP entre les appareils des utilisateurs de WorkSpaces Pools et WorkSpaces lors de l'utilisation des points de terminaison Internet. Cette option n'est actuellement prise en charge que dans le client natif Windows. UDP n'est pas pris en charge si vous utilisez des points de terminaison de VPC.
- Le port 53 est utilisé pour la communication entre les appareils des utilisateurs de WorkSpaces Pools et vos serveurs DNS. Le port doit être ouvert sur les adresses IP de vos serveurs DNS de manière à permettre la résolution des noms de domaine public. Ce port est facultatif si vous n'utilisez pas de serveurs DNS pour la résolution de noms de domaine.

Domaines autorisés

Pour que les utilisateurs de WorkSpaces Pools WorkSpaces puissent accéder, vous devez autoriser différents domaines du réseau à partir desquels les utilisateurs initient l'accès au WorkSpaces. Pour de plus amples informations, veuillez consulter [Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal](#). Notez que la page indique qu'elle s'applique au WorkSpaces personnel mais qu'elle s'applique également aux WorkSpaces pools.

Note

Si votre compartiment S3 comporte un caractère « . » caractère dans le nom, le domaine utilisé est `https://s3.<aws-region>.amazonaws.com`. Si votre compartiment S3 ne comporte aucun caractère « . » caractère dans le nom, le domaine utilisé est `https://<bucket-name>.s3.<aws-region>.amazonaws.com`.

Création d'un WorkSpaces pool

Configurez et créez un pool à partir duquel les applications utilisateur sont lancées et diffusées en continu.

Note

Vous devez créer un répertoire avant de créer un WorkSpaces pool. Pour de plus amples informations, veuillez consulter [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#).

Pour configurer et créer un pool

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation WorkSpaces, choisissez Pool.
3. Choisissez Create WorkSpaces Pools.
4. Sous Intégration (facultatif), vous pouvez choisir de me recommander des options en fonction de mon cas d'utilisation pour obtenir des recommandations sur le type que WorkSpace vous souhaitez utiliser. Vous pouvez ignorer cette étape si vous savez que vous souhaitez utiliser des WorkSpaces pools.
5. Sous Configurer WorkSpaces, entrez les informations suivantes :
 - Dans Nom, entrez un identifiant de nom unique pour le pool. Les caractères spéciaux ne sont pas autorisés.
 - Dans Description, entrez une description du pool (256 caractères maximum).
 - Pour Bundle, choisissez parmi les options suivantes le type de bundle que vous souhaitez utiliser pour votre WorkSpaces.
 - Utiliser un WorkSpaces pack de base : choisissez l'un des packs dans le menu déroulant. Pour plus d'informations sur le type de bundle que vous avez sélectionné, choisissez Bundle details. Pour comparer les forfaits proposés pour les pools, choisissez Comparer tous les forfaits.
 - Utilisez votre propre bundle personnalisé : choisissez un bundle que vous avez créé précédemment. Pour créer un bundle personnalisé, voir [Créez une WorkSpaces image personnalisée et un bundle pour WorkSpaces Personal](#).
 - Pour le mode Exécution, choisissez l'une des options suivantes pour configurer la disponibilité immédiate du pool et son mode de paiement :
 - AutoStop— Les instances de pool sont facturées des frais d'utilisation horaires, en fonction du forfait choisi, uniquement pour les instances connectées aux utilisateurs. Les instances du pool qui ne sont pas connectées aux utilisateurs sont facturées à un tarif horaire modique pour les instances arrêtées. Lorsque les utilisateurs démarrent leur session, ils commencent le streaming après une attente de 1 à 2 minutes.
 - AlwaysOn— Toutes les instances de pool en cours d'exécution sont facturées aux frais d'utilisation horaires applicables, même lorsque les utilisateurs ne sont pas connectés. Ce mode est idéal pour les utilisateurs qui ne souhaitent pas attendre le début de leur diffusion.
 - Pour Durée maximale de la session en minutes, choisissez la durée maximale pendant laquelle une session de streaming peut rester active. Si les utilisateurs sont toujours connectés

à une instance de streaming cinq minutes avant que cette limite ne soit atteinte, ils sont invités à enregistrer tous les documents ouverts avant d'être déconnectés. Une fois ce délai écoulé, l'instance est résiliée et remplacée par une nouvelle instance. La durée maximale de session que vous pouvez définir dans la console WorkSpaces Pools est de 5760 minutes (96 heures). La durée maximale de session que vous pouvez définir à l'aide de l'API et de la CLI WorkSpaces Pools est de 432 000 secondes (120 heures).

- Pour Disconnect timeout in minutes (Délai avant déconnexion en minutes), choisissez la durée pendant laquelle une session de streaming doit rester active après la déconnexion des utilisateurs. Si les utilisateurs essaient de se reconnecter à la session de streaming après une déconnexion ou une interruption réseau dans cet intervalle de temps, ils sont connectés à leur session précédente. Sinon, ils sont connectés à une nouvelle session avec une nouvelle instance de streaming.
- Si un utilisateur met fin à la session en choisissant Fin de session ou Déconnexion dans la barre d'outils du pool, le délai de déconnexion ne s'applique pas. Au lieu de cela, l'utilisateur est invité à enregistrer les documents ouverts, puis il est immédiatement déconnecté de l'instance de streaming. L'instance que l'utilisateur utilisait est ensuite supprimée.
- Pour Idle disconnect timeout in minutes (Délai d'inactivité avant déconnexion en minutes), choisissez la durée pendant laquelle les utilisateurs peuvent rester inactifs avant d'être déconnectés de leur session de streaming et avant le début de l'intervalle Disconnect timeout in minutes (Délai avant déconnexion en minutes). Les utilisateurs sont avertis avant d'être déconnectés en raison de leur inactivité. S'ils essaient de se reconnecter à la session de streaming avant que l'intervalle de temps spécifié dans Délai avant déconnexion en minutes se soit écoulé, ils sont connectés à leur session précédente. Sinon, ils sont connectés à une nouvelle session avec une nouvelle instance de streaming. Si vous définissez la valeur sur 0, celle-ci est désactivée. Lorsque cette valeur est désactivée, les utilisateurs ne sont pas déconnectés en raison de leur inactivité.

 Note

Les utilisateurs sont considérés comme inactifs lorsqu'ils arrêtent de se servir du clavier ou de la souris lors de leur session de streaming. Pour les pools joints à un domaine, le compte à rebours pour le délai d'inactivité de déconnexion ne commence que lorsque les utilisateurs se connectent à l'aide du mot de passe de leur domaine Active Directory ou à l'aide d'une carte à puce. Les chargements et téléchargements, les entrées audio, les sorties audio, et les modifications de pixels ne sont pas considérés comme une activité de l'utilisateur. Si les utilisateurs

continuent d'être inactifs après que l'intervalle de temps défini par Délai d'inactivité avant déconnexion en minutes se soit écoulé, ils sont déconnectés.

- Pour les politiques de capacité planifiée (facultatif), choisissez Ajouter une nouvelle capacité planifiée. Indiquez les dates et heures de début et de fin auxquelles vous devez fournir le nombre minimum et maximum d'instances pour votre pool en fonction du nombre minimum d'utilisateurs simultanés attendus.
- Pour les politiques de dimensionnement manuel (facultatif), spécifiez les politiques de dimensionnement que les pools doivent utiliser pour augmenter ou diminuer la capacité de votre pool. Développez les politiques de dimensionnement manuel pour ajouter de nouvelles politiques de dimensionnement.

 Note

La taille de votre piscine est limitée par la capacité minimale et maximale que vous avez spécifiée.

- Choisissez Ajouter de nouvelles politiques de scalabilité et entrez les valeurs pour ajouter des instances spécifiées si l'utilisation de la capacité spécifiée est inférieure ou supérieure à la valeur de seuil spécifiée.
 - Choisissez Ajouter une nouvelle échelle dans les politiques et entrez les valeurs pour supprimer les instances spécifiées si l'utilisation de la capacité spécifiée est inférieure ou supérieure à la valeur de seuil spécifiée.
 - Pour les balises, spécifiez la valeur de paire de clés que vous souhaitez utiliser. Une clé peut être une catégorie générale, comme un « projet », un « propriétaire » ou un « environnement » avec des valeurs associées spécifiques.
6. Sur la page Sélectionner un répertoire, choisissez le répertoire que vous avez créé. Pour créer un répertoire, choisissez Create directory. Pour de plus amples informations, veuillez consulter [Gérer les annuaires pour les WorkSpaces pools](#).
 7. Choisissez Create Workspace Pool.

Administrer WorkSpaces les pools

Un WorkSpaces pool consiste à exécuter l'image que vous spécifiez. WorkSpaces

Table des matières

- [Mode de fonctionnement pour les WorkSpaces piscines](#)
- [WorkSpaces Forfaits pour piscines](#)
- [Modifier un pool](#)
- [Suppression d'un groupe](#)
- [Mise à l'échelle automatique pour les WorkSpaces piscines](#)

Mode de fonctionnement pour les WorkSpaces piscines

Le mode de fonctionnement d'un WorkSpaces pool détermine sa disponibilité immédiate et son mode de paiement. Lorsque vous créez un WorkSpaces pool, vous pouvez choisir entre les modes de fonctionnement suivants :

- **AutoStop**— Les instances d'un WorkSpaces pool sont facturées selon des frais d'utilisation horaires basés sur le forfait choisi, uniquement pour les instances connectées aux utilisateurs. Les instances d'un WorkSpaces pool qui ne sont pas connectées à des utilisateurs sont facturées à un tarif horaire modique pour les instances arrêtées. Lorsque les utilisateurs démarrent leur session, ils commencent le streaming au bout de 1 à 2 minutes.
- **AlwaysOn**— Les instances en cours d'exécution d'un WorkSpaces pool sont facturées aux frais d'utilisation horaires applicables, même lorsque les utilisateurs ne sont pas connectés. Ce mode est idéal pour les utilisateurs qui ne souhaitent pas attendre le début de leur diffusion.

Pour plus d'informations, consultez [Tarification d'WorkSpaces](#).

Table des matières

- [Modification du mode d'exécution](#)

Modification du mode d'exécution

Vous pouvez passer d'un mode d'exécution à un autre lorsqu'un WorkSpaces pool est à l'état arrêté.

Pour modifier le mode de fonctionnement d'un WorkSpaces pool

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation, choisissez WorkSpacesPools.

3. Sélectionnez le WorkSpaces pool à modifier et confirmez qu'il est à l'état arrêté. Choisissez ensuite le mode d'exécution Actions et Modifier.
4. Sélectionnez le nouveau mode d'exécution AlwaysOn ou AutoStop, puis cliquez sur Enregistrer.

Pour modifier le mode de fonctionnement d'un WorkSpaces pool à l'aide du AWS CLI

- Utilisez la commande [update-workspaces-pool](#).

WorkSpaces Forfaits pour piscines

Un WorkSpace bundle est une combinaison d'un système d'exploitation et de ressources de stockage, de calcul et logicielles. Lorsque vous lancez un WorkSpace, vous sélectionnez le pack qui répond à vos besoins. Les offres groupées par défaut disponibles WorkSpaces sont appelées offres groupées publiques. Pour plus d'informations sur les différents forfaits publics disponibles WorkSpaces, consultez [Amazon WorkSpaces Bundles](#).

Le tableau suivant fournit des informations sur les licences, les protocoles de streaming et les offres groupées pris en charge par chaque système d'exploitation.

Système d'exploitation	Licences	Protocoles de streaming	Offres groupées prises en charge
Windows Server 2019	Inclus	DCV	Valeur, norme, performance, puissance, PowerPro
Windows Server 2022	Inclus	DCV	Standard, performance, alimentation, carte PowerPro graphique .G4DN, .G4DN GraphicsPro

Note

- Les versions du système d'exploitation qui ne sont plus prises en charge par le fournisseur ne sont pas garanties de fonctionner et ne sont pas prises en charge par le AWS support.

Modifier un pool

Après avoir créé un WorkSpaces pool, vous pouvez modifier les éléments suivants :

- ID du répertoire (si le WorkSpaces pool est arrêté)
- Détails de base
- Bundle et matériel
- Paramètres de déconnexion de session
- Capacité et mise à l'échelle
- Activités de mise à l'échelle
- Balises

Pour modifier un WorkSpaces pool

1. Dans le volet de navigation WorkSpaces, choisissez Pools.
2. Sélectionnez le pool que vous souhaitez modifier.
3. Accédez à la section que vous souhaitez modifier et choisissez Modifier.
4. Apportez les modifications souhaitées, puis cliquez sur Enregistrer.

Suppression d'un groupe

Vous pouvez supprimer des pools pour libérer des ressources et éviter des frais involontaires sur votre compte. Nous vous recommandons d'arrêter tous les pools inutilisés et en cours d'exécution.

Pour supprimer un groupe

1. Dans le volet de navigation WorkSpaces, choisissez Pools.
2. Sélectionnez le pool que vous souhaitez arrêter, puis choisissez Stop. Il faut environ 5 minutes pour arrêter une piscine.
3. Lorsque le statut du pool est arrêté, choisissez Supprimer.

Mise à l'échelle automatique pour les WorkSpaces piscines

Auto Scaling vous permet de modifier automatiquement la taille de vos pools pour adapter l'offre d'instances disponibles à la demande des utilisateurs. La taille de votre pool détermine le nombre

d'utilisateurs qui peuvent diffuser simultanément. Une instance est requise pour chaque session utilisateur. Vous pouvez spécifier la capacité de votre pool en termes d'instances. En fonction de la configuration de votre pool et de vos politiques d'autodimensionnement, le nombre d'instances requis sera mis à disposition. Vous pouvez définir des politiques de dimensionnement qui ajustent automatiquement la taille de votre pool en fonction de diverses mesures d'utilisation, et optimiser le nombre d'instances disponibles pour répondre à la demande des utilisateurs. Vous pouvez également choisir de désactiver le dimensionnement automatique et de faire fonctionner le pool à une taille fixe.

Note

- Lorsque vous élaborez votre plan de dimensionnement WorkSpaces des pools, assurez-vous que la configuration de votre réseau répond à vos exigences.
- Lorsque vous utilisez la mise à l'échelle, vous utilisez l'API Application Auto Scaling. Pour qu'Auto Scaling fonctionne correctement avec les WorkSpaces pools, Application Auto Scaling a besoin d'une autorisation pour décrire et mettre à jour vos pools et décrire vos CloudWatch alarmes Amazon, ainsi que des autorisations pour modifier la capacité de votre pool en votre nom.

Les rubriques suivantes fournissent des informations qui vous aideront à comprendre et à utiliser Auto Scaling for WorkSpaces Pools.

Table des matières

- [Concepts de dimensionnement](#)
- [Gestion du dimensionnement du pool à l'aide de la console](#)
- [Gestion du dimensionnement du pool à l'aide de la AWS CLI](#)
- [Ressources supplémentaires](#)

Concepts de dimensionnement

WorkSpaces Le dimensionnement des pools est assuré par Application Auto Scaling. Pour plus d'informations, consultez la [Référence de l'API Application Auto Scaling](#).

Pour utiliser Auto Scaling with WorkSpaces Pools de manière efficace, vous devez comprendre les termes et concepts suivants.

Nombre minimal de sessions capacity/minimum utilisateur pour le pool

Le nombre minimum d'instances. Le nombre d'instances ne peut pas être inférieur à cette valeur, et les politiques de dimensionnement ne redimensionneront pas votre pool en dessous de cette valeur. Par exemple, si vous définissez la capacité minimale d'un pool sur 2, votre pool ne comportera jamais moins de 2 instances.

Nombre maximal de sessions capacity/maximum utilisateur pour le pool

Le nombre maximum d'instances. Le nombre d'instances ne peut pas être supérieur à cette valeur, et les politiques de dimensionnement ne redimensionneront pas votre pool au-dessus de cette valeur. Par exemple, si vous définissez la capacité maximale d'un pool sur 10, votre pool ne comportera jamais plus de 10 instances.

Capacité de session utilisateur souhaitée

Le nombre total de sessions en cours ou en attente. Cela représente le nombre total de sessions de streaming simultanées que votre pool peut prendre en charge dans un état stable.

Intensification de l'action politique

Action que les politiques de dimensionnement exécutent sur votre pool lorsque la condition de politique de dimensionnement est remplie. Vous pouvez choisir une action basée sur % capacity ou number of instance(s). Par exemple, si la capacité de session utilisateur souhaitée est de 4 et que l'action de politique de dimensionnement est définie sur « Ajouter 25 % de capacité », la capacité de session utilisateur souhaitée est augmentée de 25 % à 5 lorsque la condition de politique de dimensionnement est remplie.

Condition de la politique de dimensionnement

Condition qui déclenche l'action définie dans Action de stratégie de dimensionnement. Cette condition comprend une métrique de la stratégie de dimensionnement, un opérateur de comparaison et un seuil. Par exemple, pour redimensionner un pool si son utilisation est supérieure à 50 %, votre condition de politique de dimensionnement doit être « Si l'utilisation de la capacité est supérieure à 50 % ».

Mesure de la politique de dimensionnement

Votre stratégie de dimensionnement est basée sur cette métrique. Les métriques suivantes sont disponibles pour les stratégies de dimensionnement :

Utilisation de la capacité

Pourcentage d'instances utilisées dans un pool. Vous pouvez utiliser cette métrique pour dimensionner votre pool en fonction de son utilisation. Par exemple, Condition de la stratégie

de dimensionnement : « Si Utilisation de la capacité < 25 % », exécuter Action de stratégie de dimensionnement : « Supprimer 25 % de la capacité ».

Capacité disponible

Le nombre d'instances de votre pool qui sont disponibles pour les utilisateurs. Vous pouvez utiliser cette métrique pour conserver un tampon dans votre capacité disponible afin que les utilisateurs lancent des sessions de streaming. Par exemple, Scaling Policy Condition : « Si Capacité disponible < 5 », exécuter Scaling Policy Action : « Ajouter 5 instance(s) ».

Erreur de capacité insuffisante

Nombre de demandes de session rejetées par manque de capacité. Vous pouvez utiliser cette métrique pour allouer de nouvelles instances aux utilisateurs qui ne sont pas en mesure de démarrer des sessions de streaming en raison d'un manque de capacité. Par exemple, Scaling Policy Condition : « Si Erreur de capacité insuffisante > 0 », exécuter Scaling Policy Action : « Ajouter 1 instance(s) ».

Gestion du dimensionnement du pool à l'aide de la console

Vous pouvez configurer et gérer le dimensionnement à l'aide de la WorkSpaces console de l'une des deux manières suivantes : lors de la création du pool, ou à tout moment, en utilisant l'onglet Pools. Après avoir créé des pools, accédez à l'onglet Scaling Policies pour ajouter de nouvelles politiques de dimensionnement pour votre pool. Pour de plus amples informations, veuillez consulter [Création d'un WorkSpaces pool](#).

Pour les environnements utilisateur dont le nombre d'utilisateurs varie, définissez des stratégies de dimensionnement pour contrôler l'ajustement du dimensionnement en fonction de la demande. Si vous prévoyez un nombre fixe d'utilisateurs ou si vous avez d'autres raisons de désactiver le dimensionnement, vous pouvez configurer votre pool avec un nombre fixe d'instances pour les sessions utilisateur.

Pour ce faire, définissez la capacité minimale sur le nombre d'instances souhaité. Réglez la capacité maximale pour qu'elle soit au moins égale à la valeur de la capacité minimale. Cela permet d'éviter les erreurs de validation, mais la capacité maximale sera finalement ignorée car le pool ne sera pas redimensionné. Supprimez ensuite toutes les politiques de dimensionnement pour ce pool.

Pour définir une politique de dimensionnement du pool à l'aide de la console

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Sélectionnez le pool.
4. Sur la page de ce pool, faites défiler la page vers le bas jusqu'à Capacité et mise à l'échelle.
5. Choisissez Modifier.
6. Modifiez les politiques existantes, définissez les valeurs souhaitées dans leur champ, puis choisissez Enregistrer. Les modifications apportées aux stratégies prennent effet dans un délai de quelques minutes.
7. Vous pouvez également ajouter de nouvelles politiques de capacité et de dimensionnement en choisissant Ajouter une nouvelle capacité de planification, Ajouter une nouvelle politique de scalabilité ou Ajouter une nouvelle politique d'échelonnement.

Voici un exemple de graphique d'utilisation de l'activité de dimensionnement lorsque cinq utilisateurs se connectent au pool puis se déconnectent. Cet exemple provient d'un pool utilisant les valeurs de politique de dimensionnement suivantes :

- Capacité minimale = 10
- Capacité maximale = 50
- Scaler = Si l'utilisation de la capacité de mon pool est supérieure à 75 %, ajoutez 5 instances
- Scale in = Si l'utilisation de la capacité de mon pool est inférieure à 25 %, supprimez 6 instances

 Note

Au cours de la session, 5 nouvelles instances seront lancées lors d'un événement de scale-out. Lors d'un événement d'envergure, 6 instances seront récupérées, s'il y a suffisamment d'instances sans session utilisateur active, et si le nombre total d'instances ne descend pas en dessous de la capacité minimale de 10 instances. Les instances comportant des sessions utilisateur en cours d'exécution ne seront pas récupérées. Seules les instances pour lesquelles aucune session utilisateur n'est en cours d'exécution seront récupérées.

Gestion du dimensionnement du pool à l'aide de la AWS CLI

Vous pouvez configurer et gérer le dimensionnement du pool à l'aide de la AWS Command Line Interface (AWS CLI). Pour des fonctionnalités plus avancées, telles que la définition des temps de

recharge évolutifs et dégressifs, utilisez la CLI. AWS Avant d'exécuter des commandes de politique de dimensionnement, vous devez enregistrer votre pool en tant que cible évolutive. Pour ce faire, utilisez la [register-scalable-target](#) commande suivante :

```
aws application-autoscaling register-scalable-target
  --service-namespace workspaces \
  --resource-id workspacespool/PoolId \
  --scalable-dimension workspaces:workspacespool:DesiredUserSessions \
  --min-capacity 1 --max-capacity 5
```

Exemples

- [Exemple 1 : appliquer une politique de dimensionnement basée sur l'utilisation des capacités](#)
- [Exemple 2 : application d'une politique de dimensionnement basée sur des erreurs de capacité insuffisante](#)
- [Exemple 3 : application d'une politique de dimensionnement basée sur une faible utilisation des capacités](#)
- [Exemple 4 : modifier la capacité du pool en fonction d'un calendrier](#)
- [Exemple 5 : application d'une politique de dimensionnement pour le suivi des cibles](#)

Exemple 1 : appliquer une politique de dimensionnement basée sur l'utilisation des capacités

Cet exemple de AWS CLI définit une politique de dimensionnement qui augmente un pool de 25 % si le taux d'utilisation est supérieur ou égal à 75 %.

La [put-scaling-policy](#) commande suivante définit une politique de dimensionnement basée sur l'utilisation :

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
utilization.json
```

Le contenu du fichier `scale-out-utilization.json` est le suivant :

```
{
  "PolicyName": "policyname",
  "ServiceNamespace": "workspaces",
  "ResourceId": "workspacespool/PoolId",
  "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
```

```

    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
      "AdjustmentType": "PercentChangeInCapacity",
      "StepAdjustments": [
        {
          "MetricIntervalLowerBound": 0,
          "ScalingAdjustment": 25
        }
      ],
      "Cooldown": 120
    }
  }
}

```

Si la commande est réussie, la sortie est similaire à ce qui suit, bien que certains détails soient uniques pour votre compte et votre région. Dans cet exemple, l'identificateur de la stratégie est e3425d21-16f0-d701-89fb-12f98dac64af.

```

{"PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:e3425d21-16f0-d701-89fb-12f98dac64af:resource/workspaces/workspacespool/PoolId:policyName/scale-out-utilization-policy"}

```

Maintenant, configurez une CloudWatch alarme pour cette politique. Utilisez les noms, la région, le numéro de compte et l'identificateur de stratégie qui s'appliquent à votre cas. Vous pouvez utiliser l'ARN de stratégie renvoyé par la commande précédente pour le paramètre `-- alarm-actions`.

```

aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Available User Session Capacity exceeds 75 percent" \
--metric-name AvailableUserSessionCapacity \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 300 \
--threshold 75 \
--comparison-operator GreaterThanOrEqualToThreshold \
--dimensions "Name=WorkSpaces pool ID,Value=PoolId" \
--evaluation-periods 1 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-number-without-hyphens:scalingPolicy:policyid:resource/workspaces/workspacespool/PoolId:policyName/polycyname"

```

Exemple 2 : application d'une politique de dimensionnement basée sur des erreurs de capacité insuffisante

Cet exemple de AWS CLI définit une politique de dimensionnement qui augmente le pool de 1 si le pool renvoie une `InsufficientCapacityError` erreur.

La commande suivante définit une stratégie de dimensionnement basée sur une capacité insuffisante :

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-capacity.json
```

Le contenu du fichier `scale-out-capacity.json` est le suivant :

```
{
  "PolicyName": "polycyname",
  "ServiceNamespace": "workspaces",
  "ResourceId": "workspacespool/PoolId",
  "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
  "PolicyType": "StepScaling",
  "StepScalingPolicyConfiguration": {
    "AdjustmentType": "ChangeInCapacity",
    "StepAdjustments": [
      {
        "MetricIntervalLowerBound": 0,
        "ScalingAdjustment": 1
      }
    ],
    "Cooldown": 120
  }
}
```

Si la commande est réussie, la sortie est similaire à ce qui suit, bien que certains détails soient uniques pour votre compte et votre région. Dans cet exemple, l'identificateur de la stratégie est `f4495f21-0650-470c-88e6-0f393adb64fc`.

```
{"PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:f4495f21-0650-470c-88e6-0f393adb64fc:resource/workspaces/workspacespool/PoolId:policyName/scale-out-insufficient-capacity-policy"}
```

Maintenant, configurez une CloudWatch alarme pour cette politique. Utilisez les noms, la région, le numéro de compte et l'identificateur de stratégie qui s'appliquent à votre cas. Vous pouvez utiliser l'ARN de stratégie renvoyé par la commande précédente pour le paramètre `--alarm-actions`.

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when out of capacity is > 0" \
--metric-name InsufficientCapacityError \
--namespace AWS/WorkSpaces \
--statistic Maximum \
--period 300 \
--threshold 0 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 1 --unit Count \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
```

```
workspacespool/PoolId:policyName/polycyname"
```

Exemple 3 : application d'une politique de dimensionnement basée sur une faible utilisation des capacités

Cet AWS CLI exemple définit une politique de dimensionnement qui évolue dans le pool afin de réduire la capacité réelle en cas `UserSessionsCapacityUtilization` de faible capacité.

La commande suivante définit une stratégie de dimensionnement basée sur une capacité en excès :

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-in-
capacity.json
```

Le contenu du fichier `scale-in-capacity.json` est le suivant :

```
{
  "PolicyName": "polycyname",
  "ServiceNamespace": "workspaces",
  "ResourceId": "workspacespool/PoolId",
  "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
  "PolicyType": "StepScaling",
  "StepScalingPolicyConfiguration": {
    "AdjustmentType": "PercentChangeInCapacity",
    "StepAdjustments": [
      {
```

```

        "MetricIntervalUpperBound": 0,
        "ScalingAdjustment": -25
    }
],
"Cooldown": 360
}
}

```

Si la commande est réussie, la sortie est similaire à ce qui suit, bien que certains détails soient uniques pour votre compte et votre région. Dans cet exemple, l'identificateur de la stratégie est 12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90.

```

{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90:resource/
workspaces/workspacespool/PoolId:policyName/scale-in-utilization-policy"}

```

Maintenant, configurez une CloudWatch alarme pour cette politique. Utilisez les noms, la région, le numéro de compte et l'identificateur de stratégie qui s'appliquent à votre cas. Vous pouvez utiliser l'ARN de stratégie renvoyé par la commande précédente pour le paramètre `--alarm-actions`.

```

aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Capacity Utilization is less than or equal to 25
percent" \
--metric-name UserSessionsCapacityUtilization \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 120 \
--threshold 25 \
--comparison-operator LessThanOrEqualToThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 10 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/polycyname"

```

Exemple 4 : modifier la capacité du pool en fonction d'un calendrier

La modification de la capacité de votre piscine selon un calendrier vous permet d'adapter la capacité de votre piscine en fonction de l'évolution prévisible de la demande. Par exemple, au début d'une journée, vous pouvez prévoir qu'un certain nombre d'utilisateurs vont demander simultanément

des connexions de streaming. Pour modifier la capacité de votre pool en fonction d'un calendrier, vous pouvez utiliser l'action [PutScheduledAction](#) API Application Auto Scaling ou la commande [put-scheduled-action](#) AWS CLI.

Avant de modifier la capacité de votre pool, vous pouvez répertorier la capacité actuelle de votre pool à l'aide de la commande WorkSpaces [describe-workspaces-pools](#) AWS CLI.

```
aws workspaces describe-workspaces-pools --name PoolId
```

La capacité actuelle du pool apparaîtra de la même manière que la sortie suivante (affichée au format JSON) :

```
{
  "CapacityStatus": {
    "AvailableUserSessions": 1,
    "DesiredUserSessions": 1,
    "ActualUserSessions": 1,
    "ActiveUserSessions": 0
  },
}
```

Utilisez ensuite la `put-scheduled-action` commande pour créer une action planifiée afin de modifier la capacité de votre pool. Par exemple, la commande suivante porte la capacité minimale à 3 et la capacité maximale à 5 chaque jour à 9 h 00 UTC.

Note

Pour les expressions cron, spécifiez quand effectuer l'action en heure UTC. Pour plus d'informations consultez [Expressions Cron](#).

```
aws application-autoscaling put-scheduled-action --service-namespace workspaces \
--resource-id workspacespool/PoolId \
--schedule="cron(0 9 * * ? *)" \
--scalable-target-action MinCapacity=3,MaxCapacity=5 \
--scheduled-action-name ExampleScheduledAction \
--scalable-dimension workspaces:workspacespool:DesiredUserSessions
```

Pour vérifier que l'action planifiée visant à modifier la capacité de votre pool a bien été créée, exécutez la [describe-scheduled-actions](#) commande.

```
aws application-autoscaling describe-scheduled-actions --service-namespace workspaces
--resource-id workspacespool/PoolId
```

Si l'action planifiée a été créée avec succès, la sortie apparaît comme suit.

```
{
  "ScheduledActions": [
    {
      "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
      "Schedule": "cron(0 9 * * ? *)",
      "ResourceId": "workspacespool/ExamplePool",
      "CreationTime": 1518651232.886,
      "ScheduledActionARN": "<arn>",
      "ScalableTargetAction": {
        "MinCapacity": 3,
        "MaxCapacity": 5
      },
      "ScheduledActionName": "ExampleScheduledAction",
      "ServiceNamespace": "workspaces"
    }
  ]
}
```

Pour plus d'informations, consultez [Mise à l'échelle planifiée](#) dans le Guide de l'utilisateur Application Auto Scaling..

Exemple 5 : application d'une politique de dimensionnement pour le suivi des cibles

Grâce à la mise à l'échelle du suivi des cibles, vous pouvez spécifier un niveau d'utilisation de la capacité pour votre pool.

Lorsque vous créez une politique de dimensionnement pour le suivi des cibles, Application Auto Scaling crée et gère automatiquement les CloudWatch alarmes qui déclenchent la politique de dimensionnement. La stratégie de dimensionnement ajoute ou supprime de la capacité si nécessaire pour maintenir l'utilisation de la capacité à la valeur cible spécifiée ou proche de celle-ci. Pour garantir la disponibilité des applications, votre pool évolue proportionnellement à la métrique aussi vite que possible, mais de manière plus progressive.

La [put-scaling-policy](#) commande suivante définit une politique de dimensionnement du suivi des cibles qui tente de maintenir 75 % d'utilisation de la capacité d'un WorkSpaces pool.

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://config.json
```

Le contenu du fichier `config.json` est le suivant :

```
{
  "PolicyName": "target-tracking-scaling-policy",
  "ServiceNamespace": "workspaces",
  "ResourceId": "workspacespool/PoolId",
  "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
  "PolicyType": "TargetTrackingScaling",
  "TargetTrackingScalingPolicyConfiguration": {
    "TargetValue": 75.0,
    "PredefinedMetricSpecification": {
      "PredefinedMetricType": "WorkSpacesAverageUserSessionsCapacityUtilization"
    },
    "ScaleOutCooldown": 300,
    "ScaleInCooldown": 300
  }
}
```

Si la commande est réussie, la sortie est similaire à ce qui suit, bien que certains détails soient uniques pour votre compte et votre région. Dans cet exemple, l'identificateur de stratégie est `6d8972f3-efc8-437c-92d1-6270f29a66e7`.

```
{
  "PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:6d8972f3-efc8-437c-92d1-6270f29a66e7:resource/workspaces/workspacespool/PoolId:policyName/target-tracking-scaling-policy",
  "Alarms": [
    {
      "AlarmARN": "arn:aws:cloudwatch:us-west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-b46e-434a-a60f-3b36d653feca",
      "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-b46e-434a-a60f-3b36d653feca"
    },
    {
      "AlarmARN": "arn:aws:cloudwatch:us-west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-d19b-4a63-a812-6c67aaf2910d",
      "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-d19b-4a63-a812-6c67aaf2910d"
    }
  ]
}
```

```
}  
]  
}
```

Pour plus d'informations, consultez [Stratégies de dimensionnement Suivi de cible](#) dans le Guide de l'utilisateur Application Auto Scaling.

Ressources supplémentaires

Pour en savoir plus sur l'utilisation des commandes ou des actions de l'API Application Auto Scaling AWS CLI, consultez les ressources suivantes :

- Section [application-autoscaling](#) du document Référence des commandes AWS CLI
- [Référence de l'API Application Auto Scaling](#)
- [Guide de l'utilisateur Application Auto Scaling](#)

Utilisation d'Active Directory avec des WorkSpaces pools

Vous pouvez associer votre Windows WorkSpaces in WorkSpaces Pools à des domaines de Microsoft Active Directory et utiliser vos domaines Active Directory existants, qu'ils soient basés sur le cloud ou sur site, pour lancer des instances de streaming jointes à des domaines. Vous pouvez également utiliser AWS Directory Service for Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD, pour créer un domaine Active Directory et l'utiliser pour prendre en charge les ressources de vos WorkSpaces pools. Pour plus d'informations sur l'utilisation AWS Managed Microsoft AD, consultez [Microsoft Active Directory](#) dans le Guide AWS Directory Service d'administration.

En associant WorkSpaces des pools à votre domaine Active Directory, vous pouvez :

- permettre à vos utilisateurs et à vos applications d'accéder aux ressources Active Directory, telles que les imprimantes et les partages de fichiers, à partir des sessions de streaming ;
- utiliser les paramètres de stratégie de groupe qui sont disponibles dans la console de gestion des stratégies de groupe (GPMC) pour définir l'expérience de l'utilisateur final ;
- diffuser les applications qui nécessitent l'authentification des utilisateurs à l'aide de leurs informations d'identification de connexion Active Directory ;
- Appliquez les politiques de conformité et de sécurité de votre entreprise à votre WorkSpaces in WorkSpaces Pools.

Table des matières

- [Présentation des domaines Active Directory](#)
- [Avant de commencer à utiliser Active Directory avec des WorkSpaces pools](#)
- [Authentification par certificat](#)
- [WorkSpaces Administration Active Directory des pools](#)
- [Plus d'informations](#)

Présentation des domaines Active Directory

L'utilisation de domaines Active Directory avec des WorkSpaces pools nécessite de comprendre comment ils fonctionnent ensemble et les tâches de configuration que vous devrez effectuer. Vous devrez effectuer les tâches suivantes :

1. Configurer les paramètres de stratégies de groupe comme nécessaire pour définir l'expérience de l'utilisateur final et les exigences de sécurité pour les applications
2. Créez le répertoire joint au domaine dans Pools. WorkSpaces
3. Créez l'application WorkSpaces Pools dans le fournisseur d'identité SAML 2.0 et attribuez-la aux utilisateurs finaux directement ou via des groupes Active Directory.

Flux d'authentification des utilisateurs

1. L'utilisateur accède à `https://applications.exampleco.com`. La page d'authentification demande l'authentification de l'utilisateur.
2. Le service de fédération demande l'authentification à partir de la base d'identités de l'organisation.
3. La base d'identités authentifie l'utilisateur et renvoie la réponse d'authentification au service de fédération.
4. Lorsque l'authentification est réussie, le service de fédération publie l'assertion SAML sur le navigateur de l'utilisateur.
5. Le navigateur de l'utilisateur publie l'assertion SAML sur le point de terminaison SAML de AWS connexion (). `https://signin.aws.amazon.com/saml` AWS Sign-In reçoit la demande SAML, traite la demande, authentifie l'utilisateur et transmet le jeton d'authentification au service Pools. WorkSpaces
6. À l'aide du jeton d'authentification de AWS, WorkSpaces Pools autorise l'utilisateur et présente les applications au navigateur.

7. L'utilisateur choisit une application et, selon la méthode d'authentification de connexion Windows activée dans le répertoire WorkSpaces Pools, il est invité à saisir le mot de passe de son domaine Active Directory ou à choisir une carte à puce. Si les deux méthodes d'authentification sont activées, l'utilisateur peut choisir de saisir le mot de passe de son domaine ou d'utiliser sa carte à puce. L'authentification par certificat peut également être utilisée pour authentifier les utilisateurs en supprimant l'invite.
8. Le contrôleur de domaine est contacté pour l'authentification de l'utilisateur.
9. Une fois que le domaine a authentifié l'utilisateur, la session de l'utilisateur démarre avec la connectivité du domaine.

Ce processus est transparent du point de vue de l'utilisateur. L'utilisateur commence par accéder au portail interne de votre organisation et est redirigé vers un portail WorkSpaces Pools, sans avoir à saisir d'AWS informations d'identification. Seuls un mot de passe de domaine Active Directory ou des informations d'identification par carte à puce sont nécessaires.

Avant qu'un utilisateur puisse lancer ce processus, vous devez configurer Active Directory avec les droits et les paramètres de stratégie de groupe requis et créer un répertoire de pools joints à un domaine. WorkSpaces

Avant de commencer à utiliser Active Directory avec des WorkSpaces pools

Avant d'utiliser des domaines Microsoft Active Directory avec WorkSpaces des pools, tenez compte des exigences et considérations suivantes.

Table des matières

- [Environnement de domaine Active Directory](#)
- [Joint à un domaine dans des pools WorkSpaces WorkSpaces](#)
- [Paramètres de stratégie de groupe](#)
- [Authentification par carte à puce](#)

Environnement de domaine Active Directory

- Vous devez disposer d'un domaine Microsoft Active Directory auquel vous souhaitez joindre votre WorkSpaces. Si vous ne possédez pas de domaine Active Directory ou si vous souhaitez utiliser votre environnement Active Directory sur site, voir [Services de domaine Active Directory sur le AWS cloud : déploiement de référence Quick Start](#).

- Vous devez disposer d'un compte de service de domaine autorisé à créer et à gérer des objets informatiques dans le domaine que vous souhaitez utiliser avec WorkSpaces Pools. Pour plus d'informations, consultez [Comment créer un compte de domaine dans Active Directory](#) dans la documentation Microsoft.

Lorsque vous associez ce domaine Active Directory à des WorkSpaces pools, fournissez le nom du compte de service et le mot de passe. WorkSpaces Pools utilise ce compte pour créer et gérer des objets informatiques dans le répertoire. Pour de plus amples informations, veuillez consulter [Octroi d'autorisations pour la création et la gestion d'objets ordinateur Active Directory](#).

- Lorsque vous enregistrez votre domaine Active Directory auprès de WorkSpaces Pools, vous devez fournir un nom distinctif d'unité organisationnelle (UO). A cet effet, créez une unité d'organisation. Le conteneur Computers par défaut n'est pas une unité d'organisation et ne peut pas être utilisé par les WorkSpaces pools. Pour de plus amples informations, veuillez consulter [Recherche du nom unique d'unité d'organisation](#).
- Les annuaires que vous prévoyez d'utiliser avec les WorkSpaces pools doivent être accessibles via leurs noms de domaine complets (FQDNs) via le cloud privé virtuel (VPC) dans lequel vous WorkSpaces êtes lancé. Pour plus d'informations, consultez [Active Directory and Active Directory Domain Services Port Requirements](#) dans la documentation Microsoft.

Joint à un domaine dans des pools WorkSpaces WorkSpaces

La fédération d'utilisateurs basée sur SAML 2.0 est requise pour le streaming d'applications depuis un domaine joint. WorkSpaces Vous devez également utiliser une image Windows qui permet de joindre un domaine Active Directory. Toutes les images publiques publiées à compter du 24 juillet 2017 inclus prennent en charge la jonction d'un domaine Active Directory.

Paramètres de stratégie de groupe

Vérifiez votre configuration pour les paramètres de stratégie de groupe suivants. Si nécessaire, mettez à jour les paramètres comme décrit dans cette section afin qu'ils n'empêchent pas les WorkSpaces pools de s'authentifier et de se connecter aux utilisateurs de votre domaine. Sinon, lorsque vos utilisateurs essaieront de se connecter, WorkSpaces la connexion risque d'échouer. À la place, un message s'affiche, informant les utilisateurs qu'« une erreur inconnue s'est produite ».

- Configuration de l'ordinateur > Modèles d'administration > Composants Windows > Options d'ouverture de session Windows > Désactiver ou activer la séquence de touches de sécurité : définissez cette option sur Activé pour Services.

- Configuration de l'ordinateur > Modèles d'administration > Système > Connexion > Exclure les informations d'identification des fournisseurs : assurez-vous que le CLSID suivant n'est pas répertorié : e7c1bab5-4b49-4e64-a966-8d99686f8c7c
- Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Connexion interactive > Connexion interactive : Texte du message pour les utilisateurs qui tentent de se connecter : définissez cette option sur Non défini.
- Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Connexion interactive > Connexion interactive : Titre du message pour les utilisateurs qui tentent de se connecter : définissez cette option sur Non défini.

Authentification par carte à puce

WorkSpaces Pools prend en charge l'utilisation de mots de passe de domaine Active Directory ou de cartes à puce telles que [les cartes à puce Common Access Card \(CAC\)](#) et de [vérification d'identité personnelle \(PIV\)](#) pour la connexion Windows WorkSpaces à WorkSpaces des pools. Pour plus d'informations sur la façon de configurer votre environnement Active Directory afin d'activer la connexion par carte à puce à l'aide d'autorités de certification tierces (CAs), consultez les [Directives relatives à l'activation de l'ouverture de session par carte à puce auprès d'autorités de certification tierces](#) dans la documentation Microsoft.

Authentification par certificat

Vous pouvez utiliser l'authentification basée sur des certificats avec les WorkSpaces pools joints à Microsoft Active Directory. Cela supprime l'invite utilisateur à saisir le mot de passe du domaine Active Directory lorsqu'un utilisateur se connecte. En utilisant l'authentification par certificat avec votre domaine Active Directory, vous pouvez :

- vous fier à votre fournisseur d'identité SAML 2.0 pour authentifier l'utilisateur et fournir des assertions SAML correspondant à l'utilisateur dans Active Directory ;
- créer une expérience de connexion et d'authentification unique avec moins d'invites utilisateur ;
- activer les flux d'authentification sans mot de passe à l'aide de votre fournisseur d'identité SAML 2.0.

L'authentification basée sur les certificats utilise AWS Autorité de certification privée (AWS CA privée) les ressources de votre. Compte AWS Avec AWS CA privée, vous pouvez créer des hiérarchies d'autorités de certification (CA) privées, y compris racine et subordonnée CAs. Vous pouvez

également créer votre propre hiérarchie d'autorités de certification et émettre des certificats à partir de celle-ci pour authentifier les utilisateurs internes. Pour plus d'informations, voir [Qu'est-ce que AWS CA privée](#).

Lorsque vous utilisez AWS Private CA pour l'authentification basée sur des certificats, WorkSpaces Pools demande automatiquement des certificats pour vos utilisateurs lors de la réservation de session pour chacun des utilisateurs d'un Workspace WorkSpaces pool. Il authentifie les utilisateurs auprès d'Active Directory à l'aide d'une carte à puce virtuelle dotée des certificats.

L'authentification basée sur des certificats est prise en charge sur les WorkSpaces pools joints à un domaine qui exécutent des instances Windows.

Table des matières

- [Prérequis](#)
- [Activer l'authentification par certificat](#)
- [Gérer l'authentification par certificat](#)
- [Activer le partage PCA entre comptes](#)

Prérequis

Effectuez les étapes suivantes avant d'utiliser l'authentification par certificat.

1. Configurez votre répertoire WorkSpaces Pools avec l'intégration SAML 2.0 pour utiliser l'authentification basée sur des certificats. Pour de plus amples informations, veuillez consulter [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#).

Note

N'activez pas la connexion par carte à puce dans le répertoire de votre pool si vous souhaitez utiliser l'authentification basée sur des certificats.

2. Configurez l'attribut `userPrincipalName` dans votre assertion SAML. Pour de plus amples informations, veuillez consulter [Étape 7 : Création d'assertions pour la réponse d'authentification SAML](#).
3. Configurez l'attribut `ObjectSid` dans votre assertion SAML. Vous pouvez utiliser cet attribut pour effectuer un mappage fort avec l'utilisateur Active Directory. L'authentification par certificat échoue si l'attribut `ObjectSid` ne correspond pas à l'identifiant de sécurité (SID) Active Directory

de l'utilisateur spécifié dans la valeur SAML_Subject NameID. Pour de plus amples informations, veuillez consulter [Étape 7 : Création d'assertions pour la réponse d'authentification SAML](#).

 Note

Selon [Microsoft KB5 014754](#), l'ObjectSidattribut deviendra obligatoire pour l'authentification basée sur des certificats après le 10 septembre 2025.

4. Ajoutez l'autorisation sts:TagSession à la politique de confiance des rôles IAM que vous utilisez avec votre configuration SAML 2.0. Pour plus d'informations, consultez [Transmission des balises de session dans AWS STS](#), dans le Guide de l'utilisateur Gestion des identités et des accès AWS. Cette autorisation est requise pour utiliser l'authentification par certificat. Pour de plus amples informations, veuillez consulter [Étape 5 : Création d'un rôle IAM de fédération SAML 2.0](#).
5. Créez une autorité de certification (CA) AWS privée à l'aide de l'autorité de certification privée, si aucune n'est configurée avec votre Active Directory. AWS Une autorité de certification privée est requise pour utiliser l'authentification basée sur des certificats. Pour plus d'informations, consultez [la section Planification de votre AWS CA privée déploiement](#) dans le guide de AWS Autorité de certification privée l'utilisateur. Les paramètres AWS Private CA suivants sont courants dans de nombreux cas d'utilisation de l'authentification basée sur des certificats :
 - Options de type de CA
 - Mode d'utilisation de l'autorité de certification de courte durée : recommandé si l'autorité de certification émet uniquement des certificats d'utilisateur final pour l'authentification par certificat.
 - Hiérarchie à un seul niveau avec une autorité de certification racine : choisissez une autorité de certification subordonnée pour l'intégrer à une hiérarchie d'autorités de certification existante.
 - Options de l'algorithme de clé : RSA 2048
 - Options de nom unique de l'objet : utilisez les options les plus appropriées pour identifier cette autorité de certification dans votre magasin Active Directory Autorités de certification racine de confiance.
 - Options de révocation des certificats : distribution de CRL

 Note

L'authentification basée sur des certificats nécessite un point de distribution CRL en ligne accessible à la fois depuis les WorkSpaces pools et WorkSpaces le contrôleur

de domaine. Cela nécessite un accès non authentifié au compartiment Amazon S3 configuré pour les entrées AWS privées de la CA CRL, ou une CloudFront distribution avec accès au compartiment Amazon S3 s'il bloque l'accès public. Pour plus d'informations sur ces options, consultez la section [Planification d'une liste de révocation de certificats \(CRL\)](#) dans le guide de l'AWS Autorité de certification privée utilisateur.

6. Marquez votre autorité de certification privée avec une clé habilitée `euc-private-ca` à désigner l'autorité de certification à utiliser avec l'authentification basée sur les certificats de WorkSpaces Pools. Cette clé ne nécessite aucune valeur. Pour plus d'informations, consultez [la section Gestion des balises pour votre autorité de certification privée](#) dans le guide de AWS Autorité de certification privée l'utilisateur.
7. L'authentification par certificat utilise des cartes à puce virtuelles pour la connexion. Pour plus d'informations, consultez [Recommandations pour l'activation de l'ouverture de session par carte à puce auprès d'autorités de certification tierces](#). Procédez comme suit :
 - a. Configurez les contrôleurs de domaine avec un certificat de contrôleur de domaine pour authentifier les utilisateurs de carte à puce. Si une autorité de certification d'entreprise des services de certificats Active Directory est configurée dans votre Active Directory, elle inscrit automatiquement les contrôleurs de domaine avec des certificats qui permettent l'ouverture de session par carte à puce. Si vous ne disposez pas des services de certificats Active Directory, consultez [Configuration requise pour les certificats de contrôleur de domaine provenant d'une autorité de certification tierce](#). Vous pouvez créer un certificat de contrôleur de domaine avec AWS Private CA. Dans ce cas, n'utilisez pas une autorité de certification privée configurée pour les certificats de courte durée.

 Note

Si vous utilisez AWS Managed Microsoft AD, vous pouvez configurer les services de certificats sur une EC2 instance Amazon qui répond aux exigences relatives aux certificats de contrôleur de domaine. Consultez la section [Déployer Active Directory sur un nouvel Amazon Virtual Private Cloud](#) pour des exemples de déploiements de Microsoft AD AWS gérés configurés avec les services de certificats Active Directory. Avec AWS Managed Microsoft AD et Active Directory Certificate Services, vous devez également créer des règles sortantes depuis le groupe de sécurité VPC du contrôleur vers l'instance EC2 Amazon exécutant les services de certificats. Vous devez fournir au groupe de sécurité l'accès au port TCP 135 et aux ports 49152 à 65535 pour permettre l'inscription automatique aux certificats. L'EC2 instance Amazon doit également autoriser l'accès entrant sur ces mêmes ports depuis les instances de domaine, y

compris les contrôleurs de domaine. Pour plus d'informations sur la localisation du groupe de sécurité pour AWS Managed Microsoft AD, voir [Configurer vos sous-réseaux et groupes de sécurité VPC](#).

- b. Sur la console de l'autorité de certification AWS privée, ou à l'aide du SDK ou de la CLI, exportez le certificat de l'autorité de certification privée. Pour plus d'informations, consultez [Exportation d'un certificat privé](#).
- c. Publiez l'autorité de certification privée dans Active Directory. Connectez-vous à un contrôleur de domaine ou à une machine jointe à un domaine. Copiez le certificat de l'autorité de certification privée dans n'importe quel `<path>\<file>` et exécutez les commandes suivantes en tant qu'administrateur de domaine. Vous pouvez également utiliser la stratégie de groupe et le Microsoft PKI Health Tool (PKIView) pour publier l'autorité de certification. Pour plus d'informations, consultez [Instructions de configuration](#).

```
certutil -dspublish -f <path>\<file> RootCA
```

```
certutil -dspublish -f <path>\<file> NTAAuthCA
```

Assurez-vous que les commandes s'exécutent correctement, puis supprimez le fichier du certificat de l'autorité de certification privée. En fonction de vos paramètres de réplication Active Directory, la publication sur vos contrôleurs de domaine et WorkSpaces dans les WorkSpaces pools par l'autorité de certification peut prendre plusieurs minutes.

 Note

Active Directory doit distribuer l'autorité de certification aux autorités de certification racine fiables et aux NTAAuth magasins Enterprise automatiquement pour WorkSpaces les WorkSpaces Pools lorsqu'ils rejoignent le domaine.

 Note

Les contrôleurs de domaine Active Directory doivent être en mode Compatibilité pour que l'application rigoureuse des certificats prenne en charge l'authentification par certificat. Pour plus d'informations, consultez la section [KB5014754—Modifications de l'authentification basée sur les certificats sur les contrôleurs de domaine Windows dans](#)

[la](#) documentation Microsoft Support. Si vous utilisez AWS Managed Microsoft AD, voir [Configurer les paramètres de sécurité des annuaires](#) pour plus d'informations.

Activer l'authentification par certificat

Procédez comme suit pour activer l'authentification par certificat.

Pour activer l'authentification par certificat

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Choisissez Répertoires dans le volet de navigation.
3. Choisissez l'onglet Répertoires de pools.
4. Choisissez le répertoire que vous souhaitez configurer.
5. Choisissez Modifier dans la section Authentification de la page.
6. Choisissez Modifier l'authentification basée sur les certificats dans la section Authentification basée sur les certificats de la page.
7. Choisissez Activer l'authentification par certificat.
8. Choisissez le certificat dans la liste déroulante AWS Certificate Manager (ACM) Private Certificate Authority (CA).

Pour apparaître dans le menu déroulant, vous devez enregistrer l'autorité de certification privée dans le même Compte AWS et Région AWS. Vous devez également identifier l'autorité de certification privée avec une clé nommée `euc-private-ca`.

9. Configurez la solution de secours de connexion au répertoire. La solution de secours permet aux utilisateurs de se connecter à l'aide du mot de passe de leur domaine AD en cas d'échec de l'authentification par certificat. Cette solution n'est recommandée que dans les cas où les utilisateurs connaissent le mot de passe de leur domaine. Lorsque la solution de secours est désactivée, une session peut déconnecter l'utilisateur en cas d'écran de verrouillage ou de déconnexion de Windows. Si la solution de secours est activée, la session invite l'utilisateur à saisir le mot de passe de son domaine AD.
10. Choisissez Enregistrer.

L'authentification par certificat est désormais activée. Lorsque les utilisateurs s'authentifient avec SAML 2.0 dans un répertoire WorkSpaces Pools à l'aide du domaine joint au domaine WorkSpaces,

ils ne sont plus invités à saisir le mot de passe du domaine. Les utilisateurs verront un message de connexion avec une authentification basée sur des certificats lorsqu'ils se connectent à une session activée pour l'authentification basée sur des certificats.

Gérer l'authentification par certificat

Après avoir activé l'authentification par certificat, passez en revue les tâches suivantes.

Certificat d'autorité de certification privée

Dans une configuration classique, le certificat d'autorité de certification privée a une durée de validité de 10 ans. Pour plus d'informations sur le remplacement d'une autorité de certification privée dont le certificat a expiré ou sur la réémission de l'autorité de certification privée avec une nouvelle période de validité, consultez [Gestion du cycle de vie de l'autorité de certification privée](#).

Certificats d'utilisateur final

Les certificats d'utilisateur final émis par l'authentification basée sur WorkSpaces des certificats AWS Autorité de certification privée for Pools ne nécessitent ni renouvellement ni révocation. Ces certificats sont de courte durée. WorkSpaces Pools émet automatiquement un nouveau certificat pour chaque nouvelle session, ou toutes les 24 heures pour les sessions de longue durée. La session WorkSpaces Pools régit l'utilisation de ces certificats d'utilisateur final. Si vous mettez fin à une session, WorkSpaces Pools cesse d'utiliser ce certificat. Ces certificats d'utilisateur final ont une période de validité plus courte qu'une distribution AWS Autorité de certification privée CRL classique. Par conséquent, les certificats d'utilisateur final n'ont pas besoin d'être révoqués et n'apparaîtront pas dans une CRL.

Rapports d'audit

Vous pouvez créer un rapport d'audit pour répertorier tous les certificats émis ou révoqués par votre autorité de certification privée. Pour plus d'informations, consultez [Utilisation de rapports d'audit avec votre autorité de certification privée](#).

Journalisation et surveillance

Vous pouvez l'utiliser CloudTrail pour enregistrer les appels d'API adressés à une autorité de certification privée par WorkSpaces Pools. Pour plus d'informations, voir [Qu'est-ce que c'est AWS CloudTrail ?](#) dans le guide de AWS CloudTrail l'utilisateur et [Utilisation CloudTrail](#) dans le guide de AWS Autorité de certification privée l'utilisateur. Dans l'historique des CloudTrail événements, vous pouvez consulter les noms `GetCertificate` et `IssueCertificate` événements

provenant de la source d'événements acm-pca.amazonaws.com créés par le nom d'utilisateur Pools. WorkSpaces EcmAssumeRoleSession Ces événements seront enregistrés pour chaque demande d'authentification basée sur un certificat WorkSpaces Pools. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#) dans le Guide de AWS CloudTrail l'utilisateur.

Activer le partage PCA entre comptes

Le partage entre comptes d'une autorité de certification privée (PCA) permet d'autoriser d'autres comptes à utiliser une autorité de certification centralisée. L'autorité de certification peut générer et émettre des certificats en utilisant [AWSResource Access Manager](#) (RAM) pour gérer les autorisations. Cela élimine le besoin d'une autorité de certification privée pour chaque compte. Le partage entre comptes CA privés peut être utilisé avec l'authentification basée sur WorkSpaces les certificats (CBA) des applications dans le même cadre. Région AWS

Pour utiliser une ressource privée CA partagée avec WorkSpaces Pools CBA, procédez comme suit :

1. Configurez l'autorité de certification privée pour CBA de manière centraliséeCompte AWS. Pour de plus amples informations, veuillez consulter [the section called “Authentification par certificat”](#).
2. Partagez l'autorité de certification privée avec la ressource Comptes AWS où les ressources de WorkSpaces pool utilisent le CBA. Pour ce faire, suivez les étapes décrites dans [Comment utiliser la AWS RAM pour partager votre compte ACM Private CA entre plusieurs comptes](#). Il n'est pas nécessaire de suivre l'étape 3 pour créer un certificat. Vous pouvez soit partager l'autorité de certification privée avec un individuComptes AWS, soit la partager viaAWS Organizations. Si vous partagez avec des comptes individuels, vous devez accepter l'autorité de certification privée partagée dans votre compte de ressources à l'aide de la AWS Resource Access Manager console ou APIs.

Lors de la configuration du partage, vérifiez que le partage de AWS Resource Access Manager ressources pour l'autorité de certification privée dans le compte de ressources utilise le modèle d'autorisation `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` gérée. Ce modèle s'aligne sur le modèle PCA utilisé par le rôle de service WorkSpaces Pools lors de l'émission de certificats CBA.

3. Une fois le partage réussi, consultez l'autorité de certification privée partagée à l'aide de la console d'autorité de certification privée du compte de ressources.
4. Utilisez l'API ou la CLI pour associer l'ARN CA privé à CBA dans votre répertoire WorkSpaces Pools. À l'heure actuelle, la console WorkSpaces Pools ne prend pas en charge la sélection d'une

autorité de certification privée partagée ARNs. Pour plus d'informations, consultez le [Amazon WorkSpaces Service API Reference](#).

WorkSpaces Administration Active Directory des pools

La configuration et l'utilisation d'Active Directory avec WorkSpaces des pools impliquent les tâches administratives suivantes.

Tâches

- [Octroi d'autorisations pour la création et la gestion d'objets ordinateur Active Directory](#)
- [Recherche du nom unique d'unité d'organisation](#)
- [Octroi de droits d'administrateur local sur des images personnalisées](#)
- [Verrouillage de la session de streaming lorsque l'utilisateur est inactif](#)
- [Configuration de WorkSpaces pools pour utiliser des approbations de domaine](#)

Octroi d'autorisations pour la création et la gestion d'objets ordinateur Active Directory

Pour autoriser les WorkSpaces pools à effectuer des opérations sur les objets informatiques Active Directory, vous devez disposer d'un compte doté d'autorisations suffisantes. La bonne pratique consiste à utiliser un compte disposant uniquement des privilèges minimum nécessaires. Les autorisations minimum de l'unité d'organisation (OU) Active Directory sont les suivantes :

- Créer des objets ordinateur
- Modifier le mot de passe
- Réinitialiser le mot de passe
- Écrire une description

Avant de configurer les autorisations, vous devez effectuer les tâches suivantes :

- Obtenir l'accès à un ordinateur ou à une instance EC2 qui est jointe à votre domaine.
- Installer le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory. Pour plus d'informations, consultez [Installing or Removing Remote Server Administration Tools for Windows 7](#) dans la documentation Microsoft.
- Vous connecter en tant qu'utilisateur du domaine disposant des autorisations appropriées pour modifier les paramètres de sécurité des unités d'organisation.

- Créer ou identifier l'utilisateur, le compte de service ou le groupe auquel déléguer des autorisations.

Pour configurer les autorisations minimum

1. Lancez Utilisateurs et ordinateurs Active Directory dans votre domaine ou sur votre contrôleur de domaine.
2. Dans le volet de navigation de gauche, sélectionnez la première unité d'organisation sur laquelle fournir les privilèges joints au domaine, ouvrez le menu contextuel (clic droit), puis choisissez Déléguer le contrôle.
3. Sur la page Assistant Délégation de contrôle, choisissez Suivant, Ajouter.
4. Pour Sélectionner des utilisateurs, des ordinateurs ou des groupes, sélectionnez l'utilisateur, le compte de service ou le groupe créé au préalable, puis choisissez OK.
5. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
6. Choisissez Seulement des objets suivants dans le dossier, puis Objets ordinateur.
7. Choisissez Créer les objets sélectionnés dans ce dossier, Suivant.
8. Pour Autorisations, choisissez , Lire, Écrire, Modifier le mot de passe, Réinitialiser le mot de passe, Suivant.
9. Sur la page Fin de l'Assistant Délégation de contrôle, vérifiez les informations et choisissez Terminer.
10. Répétez les étapes 2 à 9 pour toutes les autres étapes OUs nécessitant ces autorisations.

Si vous déléguez des autorisations à un groupe, créez un utilisateur ou un compte de service avec un mot de passe fort et ajoutez ce compte au groupe. Ce compte disposera alors de privilèges suffisants pour vous connecter WorkSpaces à l'annuaire. Utilisez ce compte lors de la création de la configuration de votre répertoire WorkSpaces Pools.

Recherche du nom unique d'unité d'organisation

Lorsque vous enregistrez votre domaine Active Directory auprès de WorkSpaces Pools, vous devez fournir un nom distinctif d'unité organisationnelle (UO). A cet effet, créez une unité d'organisation. Le conteneur Computers par défaut n'est pas une unité d'organisation et ne peut pas être utilisé par les WorkSpaces pools. La procédure suivante montre comment obtenir ce nom.

 Note

Le nom unique doit commencer par **OU=** pour pouvoir être utilisé pour des objets ordinateur.

Avant d'effectuer cette procédure, vous devez effectuer les tâches suivantes :

- Obtenir l'accès à un ordinateur ou à une instance EC2 qui est jointe à votre domaine.
- Installer le composant logiciel enfichable MMC Utilisateurs et ordinateurs Active Directory. Pour plus d'informations, consultez [Installing or Removing Remote Server Administration Tools for Windows 7](#) dans la documentation Microsoft.
- Vous connecter en tant qu'utilisateur du domaine disposant des autorisations appropriées pour lire les propriétés de sécurité des unités d'organisation.

Pour trouver le nom unique d'une unité d'organisation

1. Lancez Utilisateurs et ordinateurs Active Directory dans votre domaine ou sur votre contrôleur de domaine.
2. Sous Afficher, assurez-vous que les Fonctions avancées soient activées.
3. Dans le volet de navigation de gauche, sélectionnez la première unité d'organisation à utiliser pour les objets WorkSpaces informatiques, ouvrez le menu contextuel (clic droit), puis choisissez Propriétés.
4. Choisissez Éditeur d'attribut.
5. Sous Attributs , pour distinguishedName, choisissez Afficher .
6. Pour Valeur, sélectionnez le nom unique, ouvrez le menu contextuel et choisissez Copier.

Octroi de droits d'administrateur local sur des images personnalisées

Par défaut, les utilisateurs du domaine Active Directory ne disposent pas de droits d'administrateur local sur les images. Vous pouvez accorder ces droits en utilisant les préférences de stratégie de groupe de votre répertoire, ou manuellement, en utilisant le compte d'administrateur local sur une image. L'octroi de droits d'administrateur local à un utilisateur de domaine permet à cet utilisateur d'installer des applications et de créer des images personnalisées dans des WorkSpaces pools.

Table des matières

- [Utilisation des préférences de stratégie de groupe](#)

- [Utiliser le groupe d'administrateurs local sur le Workspace pour créer des images](#)

Utilisation des préférences de stratégie de groupe

Les préférences de stratégie de groupe peuvent être utilisées pour accorder des droits d'administrateur local aux utilisateurs ou groupes Active Directory, et à tous les objets ordinateur de l'unité d'organisation spécifiée. Les utilisateurs ou groupes Active Directory auxquels vous voulez accorder des autorisations d'administrateur local doivent déjà exister. Pour utiliser les préférences de stratégie de groupe, vous devez tout d'abord effectuer les opérations suivantes :

- Obtenir l'accès à un ordinateur ou à une instance EC2 qui est jointe à votre domaine.
- Installer le composant logiciel enfichable MMC GPMC (Console de gestion des stratégies de groupe). Pour plus d'informations, consultez [Installing or Removing Remote Server Administration Tools for Windows 7](#) dans la documentation Microsoft.
- Connectez-vous en tant qu'utilisateur du domaine autorisé à créer des objets de stratégie de groupe (GPOs). Lien GPOs vers le lien approprié OUs.

Pour utiliser les préférences de stratégie de groupe afin d'accorder les autorisations d'administrateur local

1. Dans votre répertoire ou sur un contrôleur de domaine, ouvrez l'invite de commande en tant qu'administrateur, tapez `gpmc . msc`, puis appuyez sur ENTRÉE.
2. Dans l'arborescence de console de gauche, sélectionnez l'unité d'organisation dans laquelle vous allez créer un nouveau GPO ou utiliser un GPO existant, puis effectuez l'une des actions suivantes :
 - Créez un GPO en ouvrant le menu contextuel (clic droit) et choisissez Create a GPO in this domain, Link it here.. Pour Nom, fournissez un nom descriptif pour ce GPO.
 - Sélectionner un GPO existant.
3. Ouvrez le menu contextuel de l'objet Stratégie de groupe (GPO), puis choisissez Modifier.
4. Dans l'arborescence de la console, choisissez Configuration de l'ordinateur, Préférences, Paramètres Windows, Paramètres du Panneau de configuration et Utilisateurs et groupes locaux.
5. Sélectionnez les Utilisateurs et groupes locaux sélectionnés, ouvrez le menu contextuel, puis choisissez Nouveau, Groupe local.
6. Pour Actions, choisissez Mettre à jour.

7. Pour Nom du groupe, choisissez Administrateurs (intégré).
8. Sous Membres, choisissez Ajouter... et spécifiez les utilisateurs ou les groupes Active Directory auxquels affecter les droits d'administrateur local sur l'instance de streaming. Pour Action, choisissez Ajouter à ce groupe, puis choisissez OK.
9. Pour appliquer cet objet de stratégie de groupe à un autre OUs, sélectionnez l'unité d'organisation supplémentaire, ouvrez le menu contextuel et choisissez Lier un objet de stratégie de groupe existant.
10. À l'aide du nom de GPO nouveau ou existant que vous avez spécifié à l'étape 2, faites défiler l'écran jusqu'au GPO, puis choisissez OK.
11. Répétez les étapes 9 et 10 pour les autres OUs qui devraient bénéficier de cette préférence.
12. Choisissez OK pour fermer la boîte de dialogue Nouvelles propriétés de groupe local.
13. Choisissez OK à nouveau pour fermer la console GPMC.

Pour appliquer la nouvelle préférence au GPO, vous devez arrêter et redémarrer toutes les flottes ou instances Image Builder en cours d'exécution. Les utilisateurs et groupes Active Directory que vous avez spécifiés à l'étape 8 se voient automatiquement accorder les droits d'administrateur local sur les instances Image Builder et flottes de l'unité d'organisation auxquelles le GPO est lié.

Utiliser le groupe d'administrateurs local sur le Workspace pour créer des images

Pour accorder aux utilisateurs ou aux groupes Active Directory des droits d'administrateur local sur une image, vous pouvez ajouter manuellement ces utilisateurs ou groupes au groupe d'administrateurs local sur l'image.

Les utilisateurs ou groupes Active Directory auxquels vous voulez accorder des droits d'administrateur local doivent déjà exister.

1. Connectez-vous à celui Workspace que vous utilisez pour créer des images. Workspace II doit être en cours d'exécution et joint au domaine.
2. Choisissez Démarrer, Outils d'administration, puis double-cliquez sur Gestion d'ordinateur.
3. Dans le volet de navigation de gauche, choisissez Utilisateurs et groupes locaux et ouvrez le dossier Groupes.
4. Ouvrez le groupe Administrateurs et choisissez Ajouter....
5. Sélectionnez tous les utilisateurs ou groupes Active Directory auxquels octroyer les droits d'administrateur local et choisissez OK. Choisissez OK à nouveau pour fermer la fenêtre Propriétés de l'administrateur.

6. Fermez Gestion de l'ordinateur.
7. Pour vous connecter en tant qu'utilisateur Active Directory et vérifier si cet utilisateur possède des droits d'administrateur local sur le WorkSpaces, choisissez Admin Commands, Changer d'utilisateur, puis entrez les informations d'identification de l'utilisateur concerné.

Verrouillage de la session de streaming lorsque l'utilisateur est inactif

WorkSpaces Les pools reposent sur un paramètre que vous configurez dans le GPMC pour verrouiller la session de streaming une fois que votre utilisateur est inactif pendant une durée spécifiée. Pour utiliser la console GPMC, vous devez tout d'abord effectuer les opérations suivantes :

- Obtenir l'accès à un ordinateur ou à une instance EC2 qui est jointe à votre domaine.
- Installer la console GPMC. Pour plus d'informations, consultez [Installing or Removing Remote Server Administration Tools for Windows 7](#) dans la documentation Microsoft.
- Connectez-vous en tant qu'utilisateur du domaine autorisé à créer GPOs. Lien GPOs vers le lien approprié OUs.

Pour verrouiller automatiquement l'instance de streaming lorsque votre utilisateur est inactif

1. Dans votre répertoire ou sur un contrôleur de domaine, ouvrez l'invite de commande en tant qu'administrateur, tapez `gpmc . msc`, puis appuyez sur ENTRÉE.
2. Dans l'arborescence de console de gauche, sélectionnez l'unité d'organisation dans laquelle vous allez créer un nouveau GPO ou utiliser un GPO existant, puis effectuez l'une des actions suivantes :
 - Créez un GPO en ouvrant le menu contextuel (clic droit) et choisissez Create a GPO in this domain, Link it here.. Pour Nom, fournissez un nom descriptif pour ce GPO.
 - Sélectionner un GPO existant.
3. Ouvrez le menu contextuel de l'objet Stratégie de groupe (GPO), puis choisissez Modifier.
4. Sous Configuration utilisateur, développez Stratégies, Modèles d'administration, Panneau de configuration, puis choisissez Personnalisation.
5. Double-cliquez sur Activer l'écran de veille.
6. Dans le paramètre de stratégie Activer l'écran de veille, choisissez Activé.
7. Choisissez Appliquer, puis OK.
8. Double-cliquez sur Forcer un écran de veille spécifique.

9. Dans le paramètre de stratégie Forcer un écran de veille spécifique, choisissez Activé.
10. Sous Nom du fichier exécutable de l'écran de veille, saisissez **scrnsave.scr**. Lorsque ce paramètre est activé, le système affiche un écran de veille noir sur le bureau de l'utilisateur.
11. Choisissez Appliquer, puis OK.
12. Double-cliquez sur Un mot de passe protège l'écran de veille.
13. Dans le paramètre de stratégie Un mot de passe protège l'écran de veille, choisissez Activé.
14. Choisissez Appliquer, puis OK.
15. Double-cliquez sur Dépassement du délai d'expiration de l'écran de veille.
16. Dans le paramètre de stratégie Dépassement du délai d'expiration de l'écran de veille, choisissez Activé.
17. Pour Secondes, spécifiez la durée pendant laquelle les utilisateurs doivent être inactifs avant que l'écran de veille ne s'applique. Pour définir une durée d'inactivité de 10 minutes, spécifiez 600 secondes.
18. Choisissez Appliquer, puis OK.
19. Dans l'arborescence de la console, sous Configuration utilisateur, développez Stratégies, Modèles d'administration, Système, puis choisissez Options Ctrl+Alt+Suppr.
20. Double-cliquez sur Supprimer le verrouillage de l'ordinateur.
21. Dans le paramètre de stratégie Supprimer le verrouillage de l'ordinateur, choisissez Désactivé.
22. Choisissez Appliquer, puis OK.

Configuration de WorkSpaces pools pour utiliser des approbations de domaine

WorkSpaces Les pools prennent en charge les environnements de domaine Active Directory dans lesquels les ressources réseau telles que les serveurs de fichiers, les applications et les objets informatiques résident dans un domaine et les objets utilisateur dans un autre. Le compte de service de domaine utilisé pour les opérations sur les objets informatiques n'a pas besoin de se trouver dans le même domaine que les WorkSpaces objets informatiques du pool.

Lors de la création d'une configuration de répertoire, spécifiez un compte de service qui possède les autorisations appropriées pour gérer les objets ordinateur dans le domaine Active Directory où les serveurs de fichiers, les applications, les objets ordinateur et les autres ressources réseau résident.

Vos comptes Active Directory d'utilisateur final doivent avoir les autorisations « Autorisé à authentifier » pour les éléments suivants :

- WorkSpaces Regroupe des objets informatiques
- Contrôleurs de domaine pour le domaine

Pour de plus amples informations, veuillez consulter [Octroi d'autorisations pour la création et la gestion d'objets ordinateur Active Directory](#).

Plus d'informations

Pour plus d'informations relatives à cette rubrique, consultez les ressources suivantes :

- [Microsoft Active Directory](#) —Informations sur l'utilisation Directory Service de.

Bundles et images pour les piscines WorkSpaces

Un WorkSpace bundle est une combinaison d'un système d'exploitation et de ressources de stockage, de calcul et logicielles. Lorsque vous lancez un WorkSpace, vous sélectionnez le pack qui répond à vos besoins. Les offres groupées par défaut disponibles WorkSpaces sont appelées offres groupées publiques. Pour plus d'informations sur les différents forfaits publics disponibles WorkSpaces, consultez [Amazon WorkSpaces Bundles](#).

Si vous avez lancé un Windows WorkSpace et que vous l'avez personnalisé, vous pouvez créer une image personnalisée à partir de celui-ci WorkSpace à utiliser avec WorkSpaces Pool. Linux n'est pas pris en charge dans WorkSpaces Pool.

Une image personnalisée contient uniquement le système d'exploitation, le logiciel et les paramètres du WorkSpace. Un bundle personnalisé est une combinaison de cette image personnalisée et du matériel à partir duquel il WorkSpace peut être lancé.

Après avoir créé une image personnalisée, vous pouvez créer un ensemble personnalisé qui combine l' WorkSpace image personnalisée et la configuration de calcul et de stockage sous-jacente que vous sélectionnez. Vous pouvez ensuite spécifier ce bundle personnalisé lorsque vous créez de nouveaux WorkSpaces pools afin de vous assurer que WorkSpaces les nouveaux pools ont la même configuration cohérente (matérielle et logicielle).

Si vous devez effectuer des mises à jour logicielles ou installer des logiciels supplémentaires sur votre WorkSpaces, vous pouvez mettre à jour votre bundle personnalisé et l'utiliser pour reconstruire votre WorkSpaces.

WorkSpaces Les pools prennent en charge différents systèmes d'exploitation (OS), protocoles de streaming et offres groupées. Le tableau suivant fournit des informations sur les licences, les protocoles de streaming et les offres groupées pris en charge par chaque système d'exploitation.

Système d'exploitation	Licences	Protocoles de streaming	Offres groupées prises en charge	Politique de cycle de vie/ date de retraite
Windows Server 2019	Inclus	DCV	Valeur, norme, performance, puissance, PowerPro	9 janvier 2029
Windows Server 2022	Inclus	DCV	Standard, performance, alimentation, carte PowerPro graphique .G4DN, .G4DN GraphicsPro	14 octobre 2031

Note

- Les versions du système d'exploitation qui ne sont plus prises en charge par le fournisseur ne sont pas garanties de fonctionner et ne sont pas prises en charge par le AWS support.

Rubriques

- [Options de bundle pour les WorkSpaces piscines](#)
- [Création d'une image personnalisée et d'un bundle pour WorkSpaces Pools](#)
- [Gérez des images et des ensembles personnalisés pour les pools WorkSpaces](#)
- [Utilisez des scripts de session pour gérer l'expérience de streaming de vos utilisateurs](#)

Options de bundle pour les WorkSpaces piscines

Avant de sélectionner un bundle à utiliser avec WorkSpaces Pool, assurez-vous que le bundle que vous souhaitez sélectionner est compatible avec votre protocole WorkSpaces, votre système d'exploitation, votre réseau et votre type de calcul. Nous recommandons de tester dans un environnement dédié les performances des bundles que vous souhaitez choisir, en exécutant

et en utilisant les applications qui reproduisent les tâches quotidiennes des utilisateurs. Pour plus d'informations sur les protocoles, consultez [Protocoles pour le WorkSpaces personnel](#). Pour plus d'informations sur les réseaux, consultez [Configuration requise pour le réseau client pour WorkSpaces Personal](#).

Les bundles publics suivants peuvent être utilisés avec WorkSpaces Pool. Pour plus d'informations sur les offres groupées incluses WorkSpaces, consultez [Amazon WorkSpaces Bundles](#). Valeur, norme, performance, puissance, PowerPro

Offre Value

Ce bundle convient parfaitement aux activités suivantes :

- Édition de texte et saisie de données de base
- Navigation sur le Web avec une utilisation légère
- Messagerie instantanée

Ce bundle n'est pas recommandé pour le traitement de texte, les conférences audio et vidéo, le partage d'écran, les outils de développement logiciel, les applications d'informatique décisionnelle et les applications graphiques.

Offre Standard

Ce bundle convient parfaitement aux activités suivantes :

- Édition de texte et saisie de données de base
- Navigation sur le Web
- Messagerie instantanée
- E-mails

Ce bundle n'est pas recommandé pour les conférences audio et vidéo, le partage d'écran, le traitement de texte, les outils de développement logiciel, les applications d'informatique décisionnelle et les applications graphiques

Offre Performance

Ce bundle convient parfaitement aux activités suivantes :

- Navigation sur le Web

- Traitement de texte
- Messagerie instantanée
- E-mails
- Feuilles de calcul
- Traitement audio
- Didacticiels

Ce bundle n'est pas recommandé pour les visioconférences, le partage d'écran, les outils de développement logiciel, les applications d'informatique décisionnelle et les applications graphiques

Offre Power

Ce bundle convient parfaitement aux activités suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mails
- Messagerie instantanée
- Feuilles de calcul
- Traitement audio
- Développement logiciel (environnement de développement intégré (IDE))
- Traitement des données de niveau basique à intermédiaire
- Conférences audio et vidéo

Ce bundle n'est pas recommandé pour le partage d'écran, les outils de développement logiciel, les applications d'informatique décisionnelle et les applications graphiques.

PowerPro offre groupée

Ce bundle convient parfaitement aux activités suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mails

- Messagerie instantanée
- Feuilles de calcul
- Traitement audio
- Développement logiciel (environnement de développement intégré (IDE))
- Entreposage de données
- Applications d'informatique décisionnelle
- Conférences audio et vidéo

Ce bundle n'est pas recommandé pour le machine learning (ML), la formation de modèles et les applications graphiques.

Offre Graphics.g4dn

Cet ensemble offre un haut niveau de performances graphiques, un niveau modéré de performances du processeur et de mémoire pour votre WorkSpaces ordinateur. Il est parfaitement adapté aux applications suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mails
- Feuilles de calcul
- Messagerie instantanée
- Conférence audio
- Développement logiciel (environnement de développement intégré (IDE))
- Traitement des données de niveau basique à intermédiaire
- Entreposage de données
- Applications d'informatique décisionnelle
- Conception graphique
- CAD/CAM (computer-aided design/computer-fabrication assistée)

Ce bundle n'est pas recommandé pour les conférences audio et vidéo, le rendu 3D, la conception photoréaliste et la formation de modèles de machine learning.

GraphicsProEnsemble .g4dn

Cet ensemble offre un haut niveau de performances graphiques, de performances du processeur et de mémoire pour votre WorkSpaces ordinateur et convient parfaitement aux applications suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mails
- Feuilles de calcul
- Messagerie instantanée
- Conférence audio
- Développement logiciel (environnement de développement intégré (IDE))
- Traitement des données de niveau basique à intermédiaire
- Entreposage de données
- Applications d'informatique décisionnelle
- Conception graphique
- CAD/CAM (computer-aided design/computer-fabrication assistée)
- Transcodage vidéo
- Rendu 3D
- Conception photoréaliste
- Streaming de jeux
- Formation de modèles de machine learning (ML) et inférence de ML

Ce bundle n'est pas recommandé pour les conférences audio et vidéo.

Création d'une image personnalisée et d'un bundle pour WorkSpaces Pools

WorkSpaces Le pool prend uniquement en charge les images et les ensembles Windows. Si vous avez lancé un Windows ou WorkSpace que vous l'avez personnalisé, vous pouvez créer une image personnalisée et des ensembles personnalisés à partir de celui-ci WorkSpace.

Une image personnalisée contient uniquement le système d'exploitation, le logiciel et les paramètres du WorkSpace. Un bundle personnalisé est une combinaison de cette image personnalisée et du matériel à partir duquel il WorkSpace peut être lancé.

Après avoir créé une image personnalisée, vous pouvez créer un bundle personnalisé qui combine l'image personnalisée et la configuration de calcul et de stockage sous-jacente que vous sélectionnez. Vous pouvez ensuite spécifier ce bundle personnalisé lorsque vous lancez un nouveau bundle WorkSpaces pour vous assurer que le nouveau WorkSpaces possède la même configuration cohérente (matérielle et logicielle).

Vous pouvez utiliser la même image personnalisée pour créer différents lots personnalisés en sélectionnant différentes options de calcul et de stockage pour chaque lot.

Important

- Les volumes de stockage groupés personnalisés ne peuvent pas être inférieurs aux volumes de stockage d'images.

Les offres groupées personnalisées coûtent le même prix que les offres groupées publiques à partir desquelles elles sont créées. Pour plus d'informations sur les tarifs, consultez [Amazon WorkSpaces Pricing](#).

Table des matières

- [Conditions requises pour créer des images personnalisées Windows](#)
- [Bonnes pratiques](#)
- [Étape 1 : Exécuter l'outil de vérification d'image](#)
- [Étape 2 : Création d'une image personnalisée et d'un bundle personnalisé](#)
- [Ce qui est inclus dans les images WorkSpaces personnalisées Windows](#)

Conditions requises pour créer des images personnalisées Windows

Note

Windows définit actuellement 1 Go comme 1 073 741 824 octets. Vous devez vous assurer qu'ils disposent de plus de 12 884 901 888 octets (ou 12 Go) libres sur le lecteur C et que le profil utilisateur est inférieur à 10 737 418 240 octets (ou 10 Go) pour créer une image d'un Workspace

- Le statut du Workspace doit être Disponible et son état de modification doit être Aucun.

- Toutes les applications et tous les profils utilisateur sur WorkSpaces les images doivent être compatibles avec Microsoft Sysprep.
- Toutes les applications à inclure dans l'image doivent être installées sur le lecteur C.
- Tous les services d'application exécutés sur le Workspace doivent utiliser un compte système local au lieu des informations d'identification de l'utilisateur du domaine. Par exemple, une installation de Microsoft SQL Server Express ne peut pas s'exécuter avec les informations d'identification d'un utilisateur de domaine.
- Ils ne Workspace doivent pas être chiffrés. La création d'images à partir d'une image chiffrée n'Workspace est actuellement pas prise en charge.
- Les composants suivants sont requis dans une image. Sans ces composants, le fichier WorkSpaces que vous lancez à partir de l'image ne fonctionnera pas correctement. Pour de plus amples informations, veuillez consulter [the section called "Configuration requise et composants de service"](#).
 - Windows PowerShell version 3.0 ou ultérieure
 - Services Bureau à distance
 - AWS Pilotes photovoltaïques
 - Gestion à distance Windows (WinRM)
 - Agents et pilotes Teradici PCo IP
 - Agents et pilotes STXHD
 - AWS et WorkSpaces certificats
 - Agent Skylight
- WorkSpaces Les pools ne prennent en charge qu'une taille maximale de volume bundle/image racine de 200 Go. Lorsque vous créez une image personnalisée Windows, assurez-vous qu'elle est inférieure à la taille du volume racine de 200 Go.

Bonnes pratiques

Avant de créer une image à partir d'un Workspace, procédez comme suit :

- Utilisez un VPC distinct, qui n'est pas connecté à votre environnement de production.
- Déployez le Workspace dans un sous-réseau privé et utilisez une instance NAT pour le trafic sortant.
- Utilisez un petit répertoire Simple AD.

- Utilisez la plus petite taille de volume pour la source WorkSpace, puis ajustez-la selon vos besoins lors de la création du bundle personnalisé.
- Installez toutes les mises à jour du système d'exploitation (à l'exception des mises à jour des fonctionnalités/versions de Windows) et toutes les mises à jour des applications sur le WorkSpace.
- Supprimez les données mises en cache WorkSpace qui ne devraient pas être incluses dans le bundle (par exemple, l'historique du navigateur, les fichiers mis en cache et les cookies du navigateur).
- Supprimez les paramètres de configuration WorkSpace qui ne devraient pas être inclus dans le bundle (par exemple, les profils de messagerie).
- Basculez vers les paramètres d'adresse IP dynamique à l'aide de DHCP.
- Assurez-vous de ne pas avoir dépassé votre quota d' WorkSpace images autorisées dans une région. Par défaut, vous êtes autorisé à 40 WorkSpace images par région. Si vous avez atteint ce quota, les nouvelles tentatives de création d'une image échoueront. Pour demander une augmentation de quota, utilisez le formulaire [Limites WorkSpaces](#).
- Assurez-vous que vous n'essayez pas de créer une image à partir d'une image chiffrée WorkSpace. La création d'images à partir d'une image chiffrée n' WorkSpace est actuellement pas prise en charge.
- Si vous utilisez un logiciel antivirus sur le WorkSpace, désactivez-le pendant que vous essayez de créer une image.
- Si un pare-feu est activé sur votre WorkSpace ordinateur, assurez-vous qu'il ne bloque aucun port nécessaire. Pour de plus amples informations, veuillez consulter [Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal](#).
- Pour Windows WorkSpaces, ne configurez aucun objet de stratégie de groupe (GPOs) avant la création de l'image.
- Pour Windows WorkSpaces, ne personnalisez pas le profil utilisateur par défaut (C:\Users\Default) avant de créer une image. Nous vous recommandons d'apporter des personnalisations au GPOs profil utilisateur et de les appliquer après la création de l'image. GPOs peuvent être facilement modifiés ou annulés, et sont donc moins sujets aux erreurs que les personnalisations apportées au profil utilisateur par défaut.
- Assurez-vous de mettre à jour les pilotes de dépendance réseau tels que les pilotes ENA et PV de votre WorkSpaces. NVMe Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, voir [Installer ou mettre à niveau le pilote Elastic Network Adapter \(ENA\)](#), [Pilotes NVMe AWS pour les instances Windows](#), et [Mettre à niveau les pilotes PV sur les instances Windows](#).

- Assurez-vous de mettre régulièrement à jour les agents EC2 Config, EC2 EC2 Launch et Launch V2 vers les dernières versions. Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez [Update EC2 Config and EC2 Launch](#).

Étape 1 : Exécuter l'outil de vérification d'image

Pour vérifier que votre Windows WorkSpace répond aux exigences relatives à la création d'images, nous vous recommandons d'exécuter l'application Image Checker. Le vérificateur d'images effectue une série de tests sur le produit WorkSpace que vous souhaitez utiliser pour créer votre image et fournit des conseils sur la manière de résoudre les problèmes détectés. Le vérificateur d'images n'est disponible que pour Windows WorkSpaces.

Important

- Vous WorkSpace devez réussir tous les tests effectués par le vérificateur d'images avant de pouvoir l'utiliser pour créer une image.
- Avant d'exécuter le vérificateur d'images, vérifiez que les dernières mises à jour de sécurité et cumulatives de Windows sont installées sur votre WorkSpace.

Pour obtenir l'outil de vérification d'image, effectuez l'une des opérations suivantes :

- [Redémarrez votre WorkSpace](#). L'outil de vérification d'image est téléchargé automatiquement pendant le redémarrage et installé à l'emplacement `C:\Program Files\Amazon\ImageChecker.exe`.
- Téléchargez Amazon WorkSpaces Image Checker depuis <https://tools.amazonworkspaces.com/ImageChecker/.zip> et extrayez le fichier. `ImageChecker.exe`. Copiez ce fichier dans `C:\Program Files\Amazon\`.

Pour exécuter le l'outil de vérification d'image

1. Ouvrez le fichier `C:\Program Files\Amazon\ImageChecker.exe`.
2. Dans la boîte de dialogue Amazon WorkSpaces Image Checker, choisissez Run.
3. Lorsqu'un test est terminé, vous pouvez en afficher le statut.

Si un test affiche le statut FAILED (ÉCHEC), choisissez Info (Informations) pour afficher de plus amples informations sur la manière de résoudre le problème qui a provoqué l'échec. Pour de plus amples informations sur la résolution de ces problèmes, veuillez consulter [Conseils pour résoudre les problèmes détectés par l'outil de vérification d'image](#).

Si des tests affichent le statut WARNING (AVERTISSEMENT), choisissez le bouton Fix all Warnings (Corriger tous les avertissements).

L'outil génère un fichier journal de sortie dans le répertoire où se trouve l'outil de vérification d'image. Par défaut, ce fichier est situé à l'emplacement suivant : C:\Program Files\Amazon\ImageChecker_yyyymmddhhmmss.log. Ne supprimez pas ce fichier journal. Si un problème se produit, ce fichier journal peut être utile pour le résoudre.

4. Le cas échéant, résolvez les problèmes à l'origine d'échecs et d'avertissements, et répétez le processus d'exécution du vérificateur d'images jusqu'à ce qu'il WorkSpace réussisse tous les tests. Tous les échecs et avertissements doivent être résolus pour pouvoir créer une image.
5. Une fois que vous WorkSpace avez réussi tous les tests, le message « Validation réussie » s'affiche. Vous êtes maintenant prêt pour créer un bundle personnalisé.

Conseils pour résoudre les problèmes détectés par l'outil de vérification d'image

En plus de consulter les conseils suivants pour résoudre les problèmes détectés par l'outil de vérification d'image, assurez-vous de consulter le fichier journal de l'outil de vérification d'image à l'adresse C:\Program Files\Amazon\ImageChecker_yyyymmddhhmmss.log.

PowerShell la version 3.0 ou ultérieure doit être installée

Installez la dernière version de [Microsoft Windows PowerShell](#).

Important

La politique PowerShell d'exécution d'un WorkSpace doit être définie pour autoriser RemoteSigned les scripts. Pour vérifier la politique d'exécution, exécutez la ExecutionPolicy PowerShell commande Get-. Si la politique d'exécution n'est pas définie sur Unrestricted RemoteSigned, exécutez la ExecutionPolicy RemoteSigned commande Set- ExecutionPolicy — pour modifier la valeur de la politique d'exécution. Ce RemoteSigned paramètre permet l'exécution de scripts sur Amazon WorkSpaces, ce qui est nécessaire pour créer une image.

Seuls les lecteurs C et D peuvent être présents

Seuls les D lecteurs C et peuvent être présents sur un WorkSpace disque utilisé pour l'imagerie. Retirez tous les autres lecteurs, y compris les lecteurs virtuels.

Aucun redémarrage en attente dans le cadre de mises à jour Windows ne peut être détecté

- Le processus de création d'image ne peut pas être exécuté tant que Windows n'a pas été redémarré pour terminer l'installation des mises à jour de sécurité ou cumulatives. Redémarrez Windows pour appliquer ces mises à jour et assurez-vous qu'aucune autre mise à jour cumulative ou de sécurité Windows en attente ne doit être installée.
- La création d'images n'est pas prise en charge sur les systèmes Windows 10 qui ont été mis à niveau d'une version de Windows 10 vers une version plus récente de Windows 10 (feature/ version mise à niveau de Windows). Toutefois, les mises à jour cumulatives ou de sécurité de Windows sont prises en charge par le processus de WorkSpaces création d'images.

Le fichier Sysprep doit exister et ne peut pas être vide

En cas de problème avec votre fichier Sysprep, contactez le [AWS Support Centre](#) pour faire réparer votre EC2 Config ou EC2 Launch.

La taille du profil utilisateur doit être inférieure à 10 Go

Pour Windows 7 WorkSpaces, le profil utilisateur (D:\Users*username*) doit être inférieur à 10 Go au total. Pour réduire la taille du profil utilisateur, supprimez des fichiers.

Le lecteur C doit avoir suffisamment d'espace libre

Pour Windows 7 WorkSpaces, vous devez disposer d'au moins 12 Go d'espace libre sur le disque C. Pour libérer de l'espace sur le lecteur C, supprimez des fichiers. Pour Windows 10 WorkSpaces, ignorez si vous recevez un FAILED message et que l'espace disque est supérieur à 2 Go.

Aucun service ne peut être exécuté sous un compte de domaine

Pour exécuter le processus de création d'image, aucun service ne WorkSpace peut être exécuté sous un compte de domaine. Tous les services doivent être exécutés sous un compte local.

Pour exécuter des services sous un compte local

1. Ouvrez C:\Program Files\Amazon\ImageChecker_*yyyyMMddhhmmss*.log et recherchez la liste des services qui s'exécutent sous un compte de domaine.

2. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
3. Sous Ouvrir une session en tant que, recherchez les services qui s'exécutent sous des comptes de domaine. (Les services s'exécutant en tant que Système local, Service local, ou Service réseau n'interfèrent pas avec la création d'image.)
4. Sélectionnez un service qui s'exécute sous un compte de domaine, puis choisissez Action, Propriétés.
5. Ouvrez l'onglet Ouvrir une session. Sous Ouvrir une session en tant que, choisissez Compte système local.
6. Choisissez OK.

Le WorkSpace doit être configuré pour utiliser le DHCP

Vous devez configurer tous les adaptateurs réseau de manière WorkSpace à utiliser le DHCP au lieu d'adresses IP statiques.

Pour configurer toutes les cartes réseau afin qu'elles utilisent DHCP

1. Dans la zone de recherche Windows, entrez **control panel** pour ouvrir le Panneau de configuration.
2. Choisissez Réseau et Internet.
3. Choisissez Centre Réseau et partage.
4. Choisissez Modifier les paramètres de la carte, puis sélectionnez une carte.
5. Choisissez Modifier les paramètres de cette connexion.
6. Dans l'onglet Réseau, sélectionnez Internet Protocol version 4 (TCP/IPv4), puis choisissez Propriétés.
7. Dans la boîte de dialogue Propriétés du protocole Internet version 4 (TCP/IPv4), sélectionnez Obtenir une adresse IP automatiquement.
8. Choisissez OK.
9. Répétez cette procédure pour tous les adaptateurs réseau du WorkSpace.

Les services Bureau à distance doivent être activés

Le processus de création d'image nécessite l'activation des services Bureau à distance.

Pour activer les services Bureau à distance

1. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
2. Dans la colonne Nom recherchez Services Bureau à distance.
3. Sélectionnez Services Bureau à distance, puis choisissez Action, Propriétés.
4. Sous l'onglet Général pour Type de démarrage, choisissez Manuel ou Automatique.
5. Choisissez OK.

Un profil utilisateur doit exister

Le Workspace fichier que vous utilisez pour créer des images doit avoir un profil utilisateur (D: \Users*username*). Si ce test échoue, contactez le [Centre AWS Support](#) pour obtenir de l'aide.

Le chemin d'accès de la variable d'environnement doit être correctement configuré

Le chemin de la variable d'environnement pour la machine locale ne contient pas d'entrées pour System32 et pour Windows PowerShell. Ces entrées sont requises pour l'exécution du processus de création d'image.

Pour configurer le chemin d'accès de votre variable d'environnement

1. Dans la zone de recherche Windows, entrez **environment variables** et choisissez Modifier les variables d'environnement système.
2. Dans la boîte de dialogue Propriétés système ouvrez l'onglet Avancé et choisissez Variables d'environnement.
3. Dans la boîte de dialogue Variables d'environnement sous Variables système, sélectionnez l'entrée Chemin puis choisissez Modifier.
4. Choisissez Nouveau, puis ajoutez le chemin d'accès suivant :

C:\Windows\System32

5. Choisissez de nouveau Nouveau puis ajoutez le chemin suivant :

C:\Windows\System32\WindowsPowerShell\v1.0\

6. Choisissez OK.
7. Redémarrez le Workspace.

 Tip

L'ordre dans lequel les éléments apparaissent dans le chemin de la variable d'environnement est important. Pour déterminer l'ordre correct, vous pouvez comparer le chemin de votre variable d'environnement WorkSpace avec celui d'une instance Windows nouvellement créée WorkSpace ou nouvelle.

Le programme d'installation pour les modules Windows doit être activé

Le processus de création d'image nécessite l'activation du service Programme d'installation pour les modules Windows.

Pour activer le service Programme d'installation pour les modules Windows

1. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
2. Dans la colonne Nom recherchez le Programme d'installation pour les modules Windows.
3. Sélectionnez le Programme d'installation pour les modules Windows, puis choisissez Action, Propriétés.
4. Sous l'onglet Général pour Type de démarrage, choisissez Manuel ou Automatique.
5. Choisissez OK.

L'agent Amazon SSM doit être désactivé

Le processus de création d'image nécessite la désactivation du service Amazon SSM Agent.

Pour désactiver le service Amazon SSM Agent

1. Dans la zone de recherche Windows, entrez **services.msc** pour ouvrir le Gestionnaire des services Windows.
2. Dans la colonne Nom recherchez Amazon SSM Agent.
3. Sélectionnez Agent Amazon SSM, puis choisissez Action, Propriétés.
4. Sous l'onglet Général pour Type de démarrage, choisissez Désactivé.
5. Choisissez OK.

SSL3 et la version 1.2 du protocole TLS doit être activée

Pour configurer SSL/TLS pour Windows, consultez la section [Comment activer le protocole TLS 1.2](#) dans la documentation Microsoft Windows.

Il ne peut y avoir qu'un seul profil d'utilisateur sur le WorkSpace

Il ne peut y avoir qu'un seul profil WorkSpaces utilisateur (D:\Users*username*) WorkSpace que vous utilisez pour créer des images. Supprimez tous les profils utilisateur qui n'appartiennent pas à l'utilisateur prévu du WorkSpace.

Pour que la création d'images fonctionne, vous ne WorkSpace pouvez avoir que trois profils utilisateur :

- Le profil utilisateur de l'utilisateur auquel le WorkSpace (D:\Users*username*) est destiné
- Le profil utilisateur par défaut (également connu sous le nom de Profil par défaut)
- Le profil utilisateur Administrateur

Si d'autres profils utilisateur sont présents, vous pouvez les supprimer via les propriétés système avancées du Panneau de configuration Windows.

Pour supprimer un profil utilisateur

1. Pour accéder aux propriétés système avancées, effectuez l'une des opérations suivantes :
 - Appuyez sur les touches Windows+pause/arrêt, puis choisissez Paramètres système avancés dans le volet gauche de la boîte de dialogue Panneau de configuration > Système et sécurité > Système.
 - Dans la zone de recherche Windows, entrez **control panel**. Dans le Panneau de configuration, choisissez Système et sécurité, puis Système, puis Paramètres système avancés dans le volet gauche de la boîte de dialogue Panneau de configuration > Système et sécurité > Système.
2. Dans la boîte de dialogue Propriétés système sous l'onglet Avancé choisissez Paramètres sous Profils utilisateur.
3. Si un profil autre que le profil administrateur, le profil par défaut et le profil de l'WorkSpacesutilisateur prévu est répertorié, sélectionnez ce profil supplémentaire et choisissez Supprimer.
4. À la question sur la suppression du profil, choisissez Oui.

5. Si nécessaire, répétez les étapes 3 et 4 pour supprimer tout autre profil n'appartenant pas au WorkSpace.
6. Cliquez deux fois sur OK et fermez le Panneau de configuration.
7. Redémarrez le WorkSpace.

Aucun package AppX ne peut être dans un état intermédiaire

Un ou plusieurs packages AppX sont dans un état intermédiaire. Cela peut provoquer une erreur Sysprep lors de la création d'image.

Pour supprimer tous les packages AppX intermédiaires

1. Dans la zone de recherche Windows, entrez **powershell**. Choisissez Exécuter en tant qu'administrateur.
2. À la question « Voulez-vous autoriser cette application à apporter des modifications à votre appareil ? », choisissez Oui.
3. Dans la PowerShell fenêtre Windows, entrez les commandes suivantes pour répertorier tous les packages AppX préparés, puis appuyez sur Entrée après chacun d'eux.

```
$workspaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages | Where-Object { `
    (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "$workspaceUserName")) -and `
    ($_.PackageUserInformation -like "*Staged*" -or
    $_.PackageUserInformation -like "*Installed*")) -or `
    (((($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "$workspaceUserName") -and `
    $_.PackageUserInformation -like "*Staged*")
}
```

4. Exécutez la commande suivante avec des privilèges SYSTEM élevés pour supprimer toutes les entrées de provisionnement de packages AppX intermédiaires, puis appuyez sur Entrée.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Exécutez de nouveau l'outil de vérification d'image. Si ce test échoue toujours, entrez les commandes suivantes pour supprimer tous les packages AppX et appuyez sur Entrée après chaque package.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -  
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows ne doit pas avoir été mis à niveau à partir d'une version précédente

La création d'images n'est pas prise en charge sur les systèmes Windows qui ont été mis à niveau d'une version de Windows 10 vers une version plus récente de Windows 10 (feature/version mise à niveau de Windows).

Pour créer des images, utilisez une image WorkSpace qui n'a pas subi de feature/version mise à niveau vers Windows.

Le nombre de réinitialisations Windows ne doit pas être nul

La fonction de réinitialisation vous permet de prolonger la période d'activation de la version d'évaluation de Windows. Le processus de création d'image nécessite que la valeur du nombre de réinitialisations soit différente de 0.

Pour vérifier le nombre de réinitialisations Windows

1. Dans le menu Démarrer de Windows, choisissez Système Windows, puis Invite de commandes.
2. À l'invite de commande, saisissez la commande suivante, puis appuyez sur Entrée.

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

Pour réinitialiser le nombre de réinitialisations à une valeur différente de 0, veuillez consulter [Sysprep \(Generalize\) a Windows installation](#) dans la documentation Microsoft Windows.

Autres conseils pour la résolution des problèmes

Si vous WorkSpace réussissez tous les tests effectués par le vérificateur d'images, mais que vous ne parvenez toujours pas à créer une image à partir du WorkSpace, vérifiez les problèmes suivants :

- Assurez-vous que le WorkSpace n'est pas attribué à un utilisateur au sein d'un groupe d'invités du domaine. Pour vérifier s'il existe des comptes de domaine, exécutez la PowerShell commande suivante.

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*$env:USERDOMAIN*" }
```

- Certains objets de stratégie de groupe (GPOs) limitent l'accès à l'empreinte numérique du certificat RDP lorsque celui-ci est demandé par le service EC2 Config ou les scripts de EC2 lancement lors de la configuration de l'instance Windows. Avant d'essayer de créer une image, déplacez-la WorkSpace vers une nouvelle unité organisationnelle (UO) dont l'héritage est bloqué et non GPOs appliqué.
- Assurez-vous que le service Gestion à distance de Windows (WinRM) est configuré de manière à démarrer automatiquement. Procédez comme suit :
 - Dans la zone de recherche Windows, entrez `services.msc` pour ouvrir le Gestionnaire des services Windows.
 - Dans la colonne Nom recherchez Gestion à distance de Windows (Gestion WSM).
 - Sélectionnez Gestion à distance de Windows (Gestion WSM), puis choisissez Action, Propriétés.
 - Sous l'onglet Général pour Type de démarrage, choisissez Automatique.
 - Choisissez OK.

Étape 2 : Création d'une image personnalisée et d'un bundle personnalisé

Après avoir validé votre WorkSpace image, suivez la procédure suivante pour créer votre image personnalisée et votre bundle personnalisé à l'aide de la WorkSpaces console. Pour créer une image par programmation, utilisez l'action `CreateWorkspacelImage` API. Pour plus d'informations, consultez [CreateWorkspacelImage](#) le Amazon WorkSpaces API Reference. Pour créer un bundle par programmation, utilisez l'action d'API `CreateWorkspaceBundle`. Pour plus d'informations, consultez [CreateWorkspaceBundle](#) le Amazon WorkSpaces API Reference.

Pour créer une image personnalisée et un bundle personnalisé à l'aide de la WorkSpaces console

- Si vous êtes toujours connecté au WorkSpace, déconnectez-vous en choisissant Amazon WorkSpaces et Disconnect dans l'application WorkSpaces cliente.
- Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

3. Dans le panneau de navigation, sélectionnez WorkSpaces.
4. Sélectionnez le Workspace pour ouvrir sa page de détails, puis choisissez Créer une image. Si le statut du Workspace est Arrêté, vous devez d'abord le démarrer (choisissez Actions, Démarrer WorkSpaces) avant de choisir Actions, Créer une image.
5. Un message s'affiche, vous invitant à redémarrer (redémarrer) votre ordinateur Workspace avant de continuer. Le redémarrage Workspace met à jour votre WorkSpaces logiciel Amazon vers la dernière version.

Redémarrez votre ordinateur Workspace en fermant le message et en suivant les étapes indiquées [Redémarrer un Workspace dans WorkSpaces Personal](#). Lorsque vous avez terminé, répétez l'étape [Step 4](#) de cette procédure, mais cette fois choisissez Suivant lorsque le message de redémarrage apparaît. Pour créer une image, le statut de Workspace doit être Disponible et son état de modification doit être Aucun.

6. Saisissez un nom et une description pour l'image qui vous permettront de l'identifier, puis choisissez Create Image (Créer une image). Pendant la création de l'image, le statut du Workspace est Suspendu et n' Workspace est pas disponible.

N'utilisez pas de caractère spécial tiret (-) dans la description. Cela provoquera une erreur.

7. Dans le volet de navigation, choisissez Images. L'image est complète lorsque le statut Workspace passe à Disponible (cela peut prendre jusqu'à 45 minutes).
8. Sélectionnez l'image et choisissez Actions, Créer un bundle.
9. Saisissez un nom et une description pour le bundle, puis effectuez les opérations suivantes :
 - Pour le type de matériel du bundle, choisissez le matériel à utiliser lors WorkSpaces du lancement à partir de ce bundle personnalisé.
 - Les combinaisons de tailles disponibles par défaut pour le volume racine sont de 200 Go par volume Workspace.
10. Pour confirmer que votre bundle est créé, choisissez Bundles, et vérifiez qu'il est répertorié.

Ce qui est inclus dans les images WorkSpaces personnalisées Windows

Lorsque vous créez une image à partir d'un système Windows Workspace, tout le contenu du C lecteur est inclus.

- Contacts
- Téléchargements

- Musique
- Images
- Jeux enregistrés
- Vidéos
- Podcasts
- Machines virtuelles
- .virtualbox
- Suivi
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\iconcache\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\

- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Gérez des images et des ensembles personnalisés pour les pools WorkSpaces

Le processus de gestion des images et des ensembles personnalisés est le même entre WorkSpaces Personal et WorkSpaces Pool. Pour plus d'informations sur la gestion des images et des ensembles, consultez la documentation suivante dans la section WorkSpaces Personnel de ce guide :

Note

La principale différence entre les packs personnalisés que vous pouvez utiliser pour WorkSpaces Personal et ceux que vous pouvez utiliser pour WorkSpaces Pool réside dans le système d'exploitation et le bundle public de base qui peuvent être utilisés. Pour les systèmes d'exploitation et les ensembles pris en charge dans WorkSpaces Pool, consultez

[Un Workspace bundle est une combinaison d'un système d'exploitation et de ressources de stockage, de calcul et logicielles. Lorsque vous lancez un Workspace, vous sélectionnez le pack qui répond à vos besoins. Les offres groupées par défaut disponibles WorkSpaces sont appelées offres groupées publiques. Pour plus d'informations sur les différents forfaits publics disponibles WorkSpaces, consultez \[Amazon WorkSpaces Bundles\]\(#\).](#)

[Le tableau suivant fournit des informations sur les licences, les protocoles de streaming et les offres groupées pris en charge par chaque système d'exploitation.](#)

Windows Server 2019	Inclus	DCV	Valeur, norme, performance, puissance, PowerPro
Windows Server 2022	Inclus	DCV	Standard, performance, alimentation, carte PowerPro graphique .G4DN, .G4DN GraphicsPro
Système d'exploitation	Licences	Protocoles de streaming	Offres groupées prises en charge

 Note

- Les versions du système d'exploitation qui ne sont plus prises en charge par le fournisseur ne sont pas garanties de fonctionner et ne sont pas prises en charge par le AWS support.

- [Mettre à jour un pack personnalisé pour WorkSpaces Personal.](#)
- [Copier une image personnalisée dans WorkSpaces Personal.](#)
- [Partager ou annuler le partage d'une image personnalisée dans Personal WorkSpaces.](#)
- [Supprimer un ensemble ou une image personnalisé dans WorkSpaces Personal.](#)

Utilisez des scripts de session pour gérer l'expérience de streaming de vos utilisateurs

WorkSpaces Pool fournit des scripts de session sur instance. Vous pouvez les utiliser pour exécuter vos propres scripts personnalisés lorsque des événements spécifiques surviennent au cours des sessions de streaming des utilisateurs. Par exemple, vous pouvez utiliser des scripts personnalisés pour préparer votre environnement WorkSpaces Pools avant le début des sessions de streaming de vos utilisateurs. Vous pouvez également utiliser les scripts personnalisés pour nettoyer les instances de streaming après que les utilisateurs ont terminé leur session.

Les scripts de session sont spécifiés dans une Workspace image. Ces scripts sont exécutés au sein du contexte de l'utilisateur ou du contexte du système. Si vos scripts de session utilisent la sortie standard pour écrire des messages d'information, d'erreur ou de débogage, ils peuvent éventuellement être enregistrés dans un compartiment Amazon S3 de votre compte Amazon Web Services.

Table des matières

- [Exécution de scripts avant le début des sessions de streaming](#)
- [Exécution de scripts une fois les sessions de streaming terminées](#)

- [Création et spécification de scripts de session](#)
- [Fichier de configuration des scripts de session](#)
- [Utilisation de PowerShell fichiers Windows](#)
- [Journalisation de la sortie du script de session](#)
- [Utiliser le stockage persistant avec des scripts de session](#)
- [Activation du stockage des journaux de script de session dans un compartiment Amazon S3](#)

Exécution de scripts avant le début des sessions de streaming

Vous pouvez configurer vos scripts pour qu'ils s'exécutent pendant 60 secondes maximum avant que les applications de vos utilisateurs se lancent et que leurs sessions de streaming commencent. Cela vous permet de personnaliser l'environnement WorkSpaces Pools avant que les utilisateurs ne commencent à diffuser leurs applications. Pendant que les scripts de session s'exécutent, une icône de chargement s'affiche sur l'écran de vos utilisateurs. Lorsque l'exécution des scripts est terminée ou que le temps d'attente maximum s'est écoulé, la session de streaming de vos utilisateurs commence. Si vos scripts ne parviennent pas à s'exécuter complètement, un message d'erreur s'affiche sur l'écran de vos utilisateurs. Toutefois, cette erreur ne les empêche pas d'accéder à leur session de streaming.

Lorsque vous spécifiez un nom de fichier sur une instance Windows, vous devez utiliser une double barre oblique inverse. Par exemple :

```
C:\\Scripts\\Myscript.bat
```

Si vous n'utilisez pas de double barre oblique inverse, un message d'erreur s'affiche pour vous informer que le .json fichier est mal formaté.

Note

Si l'exécution de vos scripts réussit complètement, une valeur de 0 devrait vous être renvoyée. Si vos scripts renvoient une valeur autre que 0, WorkSpaces affiche le message d'erreur à l'attention de l'utilisateur.

Lorsque vous exécutez des scripts avant le début des sessions de streaming, le processus suivant se produit :

1. Vos utilisateurs se connectent WorkSpace à un WorkSpaces pool qui n'est pas joint à un domaine. Ils se connectent à l'aide de SAML 2.0.
2. L'un des scénarios suivants survient :
 - Si la persistance des paramètres d'application est activée pour vos utilisateurs, le fichier de paramètres d'application VHD (Virtual Hard Disk), qui stocke les personnalisations et les paramètres Windows de vos utilisateurs, est téléchargé et monté. Dans ce cas, la connexion utilisateur à Windows est requise.

Pour en savoir plus sur la persistance des paramètres d'application, consultez [Activez la persistance des paramètres de l'application pour les utilisateurs de vos WorkSpaces pools](#).
 - Si la persistance des paramètres d'application n'est pas activée, l'utilisateur Windows est déjà connecté.
3. Vos scripts de session démarrent. Si le stockage persistant est activé pour vos utilisateurs, le montage du connecteur de stockage se lance également. Pour en savoir plus sur le stockage persistant, consultez [Activer et administrer le stockage persistant pour les WorkSpaces pools](#).

Note

Le montage du connecteur de stockage n'a pas besoin d'être terminé pour que la session de streaming démarre. Si l'exécution des scripts de session est terminée avant que le connecteur de stockage ne soit monté, la session de streaming commence.

Pour savoir comment surveiller l'état de montage des connecteurs de stockage, consultez [Utiliser le stockage persistant avec des scripts de session](#).

4. L'exécution de vos scripts de session est terminée ou expire.
5. La session de streaming des utilisateurs démarre.

Exécution de scripts une fois les sessions de streaming terminées

Vous pouvez également configurer vos scripts de manière à ce qu'ils s'exécutent après les sessions de streaming. Par exemple, vous pouvez exécuter un script lorsque les utilisateurs sélectionnent Fin de session dans la barre d'outils du WorkSpaces client ou lorsqu'ils atteignent la durée maximale autorisée pour la session. Vous pouvez aussi utiliser ces scripts de session pour nettoyer votre environnement WorkSpaces avant que la session de streaming se termine. Par exemple, vous pouvez utiliser les scripts pour libérer des verrouillages de fichiers ou pour charger des fichiers

journaux. Si vous exécutez des scripts une fois les sessions de streaming terminées, le scénario suivant se produit :

1. La session de WorkSpaces streaming de vos utilisateurs se termine.
2. Vos scripts d'arrêt de session démarrent.
3. L'exécution des scripts d'arrêt de session se termine ou expire.
4. L'utilisateur Windows est déconnecté.
5. Un des scénarios suivants, ou les deux, se produi(sen)t, le cas échéant :
 - Si la persistance des paramètres d'application est activée pour vos utilisateurs, le fichier VHD de paramètres d'application, qui stocke les personnalisations et les paramètres Windows de vos utilisateurs, est démonté et chargé dans un compartiment Amazon S3 de votre compte.
 - Si le stockage persistant est activé pour vos utilisateurs, le connecteur de stockage effectue une synchronisation finale et est démonté.
6. Le Workspace est terminé.

Création et spécification de scripts de session

Suivez la procédure ci-dessous pour créer et spécifier des scripts de session pour votre WorkSpaces compte dans un WorkSpaces pool.

1. Connectez-vous à la fenêtre WorkSpaces à partir de laquelle vous créez une image personnalisée.
2. Créez le répertoire /AWSEUC/SessionScripts s'il n'existe pas déjà.
3. Créez un fichier de configuration /AWSEUC/SessionScripts/config.json s'il n'existe pas déjà, à l'aide du [modèle de configuration de script de session](#).
4. Accédez à C:\AWSEUC\SessionScripts et ouvrez le fichier de configuration config.json.

Pour en savoir plus sur les paramètres des scripts de session, consultez [Fichier de configuration des scripts de session](#).

5. Une fois que vous avez terminé d'effectuer vos modifications, enregistrez puis fermez le fichier config.json.
6. Suivez les étapes pour créer une image à partir du Workspace. Pour de plus amples informations, veuillez consulter [Création d'une image personnalisée et d'un bundle pour WorkSpaces Pools](#).

Fichier de configuration des scripts de session

Pour localiser le fichier de configuration des scripts de session dans une instance Windows, accédez à `C:\AWSEUC\SessionScripts\config.json`. Le format du fichier est le suivant.

Note

Le fichier de configuration est au format JSON. Vérifiez que le texte que vous saisissez dans ce fichier est au format JSON valide.

```
{
  "SessionStart": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  },
  "SessionTermination": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ]
  }
}
```

```
    }  
  ],  
  "waitingTime": 30  
}  
}
```

Vous pouvez utiliser les paramètres suivants dans le fichier de configuration des scripts de session.

SessionStart/SessionTermination

Les scripts de session s'exécutent dans l'événement de session approprié, en fonction du nom de l'objet.

Type : chaîne

Obligatoire : non

Valeurs autorisées : **SessionStart**, **SessionTermination**

WaitingTime

Durée maximale en secondes des scripts de session.

Type : entier

Obligatoire : non

Contraintes : la durée maximale ne peut pas dépasser 60 secondes. Si l'exécution des scripts de session n'est pas terminée au terme de ce délai, elle s'arrête. Si vous avez besoin d'un script pour continuer l'exécution, lancez-le comme un processus distinct.

Executables

Détails sur les scripts de session à exécuter.

Type : chaîne

Obligatoire : oui

Contraintes : le nombre maximum de scripts qui peuvent s'exécuter par événement de session est de 2 (un pour le contexte de l'utilisateur et l'autre pour le contexte du système).

Context

Le contexte dans lequel le script de session doit être exécuté.

Type : chaîne

Obligatoire : oui

Valeurs autorisées : **user**, **system**

Filename

Le chemin d'accès complet au script de session qui doit être exécuter. Si ce paramètre n'est pas spécifié, le script de session n'est pas exécuté.

Type : chaîne

Obligatoire : non

Contraintes : la longueur maximale du nom de fichier et du chemin d'accès complet est de 1 000 caractères.

Valeurs autorisées : **.bat**, **.exe**, **.sh**

Note

Vous pouvez également utiliser des PowerShell fichiers Windows. Pour de plus amples informations, veuillez consulter [Utilisation de PowerShell fichiers Windows](#).

Arguments

Les arguments pour votre script de session ou votre fichier exécutable.

Type : chaîne

Obligatoire : non

Contraintes de longueur : la longueur maximale est de 1 000 caractères.

S3LogEnabled

Lorsque la valeur de ce paramètre est définie sur **True**, un compartiment S3 est créé dans votre compte Amazon Web Services pour stocker les journaux créés par le script de session. Par défaut, cette valeur indique **True**. Pour en savoir plus, consultez la section Journalisation de la sortie du script de session plus loin dans cette rubrique.

Type : valeur booléenne

Obligatoire : non

Valeurs autorisées : **True, False**

Utilisation de PowerShell fichiers Windows

Pour utiliser PowerShell des fichiers Windows, spécifiez le chemin complet du PowerShell fichier dans le `filename` paramètre :

```
"filename":  
"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
```

Ensuite, spécifiez votre script de session dans le paramètre **arguments** :

```
"arguments": "-File \"C:\\path\\to\\session\\script.ps1\"",
```

Enfin, vérifiez que la politique PowerShell d'exécution autorise l'exécution de votre PowerShell fichier.

Journalisation de la sortie du script de session

Lorsque cette option est activée dans le fichier de configuration, WorkSpaces Pool capture automatiquement le résultat du script de session écrit sur la sortie standard. Cette sortie est chargée dans un compartiment Amazon S3 de votre compte. Vous pouvez consulter les fichiers journaux à des fins de dépannage ou de débogage.

Note

Les fichiers journaux sont chargés lorsque le script de session renvoie une valeur, ou lorsque la valeur définit dans **WaitingTime** s'est écoulée, en fonction de l'événement qui se produit en premier.

Utiliser le stockage persistant avec des scripts de session

Lorsque le stockage WorkSpaces persistant est activé, le stockage commence à monter lorsque les scripts de démarrage de session s'exécutent. Si votre script repose sur le montage d'un stockage persistant, vous pouvez attendre que les connecteurs soient disponibles. WorkSpaces conserve l'état de montage des connecteurs de stockage dans le registre Windows sous Windows WorkSpaces, à l'aide de la clé suivante :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\AWSEC\Storage\<provided user  
name>\<Storage connector>
```

Les valeurs de la clé de registre sont les suivantes :

- Nom d'utilisateur fourni : ID utilisateur fourni via le mode d'accès. Les modes d'accès et la valeur pour chaque mode sont les suivants :
 - Groupe d'utilisateurs : adresse e-mail de l'utilisateur
 - URL de streaming : ID utilisateur (UserID)
 - SAML : ID du nom (NameID). Si le nom d'utilisateur inclut une barre oblique (par exemple, le SAMAccount nom d'utilisateur d'un domaine), la barre oblique est remplacée par un caractère « - ».
- Connecteur de stockage : connecteur pour l'option de stockage persistant qui a été activée pour l'utilisateur. Les valeurs du connecteur de stockage sont les suivantes :
 - HomeFolder

Chaque clé de registre du connecteur de stockage contient une valeur MountStatusDWORD. Le tableau suivant répertorie les valeurs possibles pour MountStatus.

 Note

Pour afficher ces clés de registre, vous devez avoir installé Microsoft .NET Framework version 4.7.2 ou ultérieure sur votre image.

Value	Description
0	Connecteur de stockage non activé pour cet utilisateur
1	Montage du connecteur de stockage en cours
2	Montage du connecteur de stockage terminé
3	Échec du montage du connecteur de stockage
4	Le montage du connecteur de stockage est activé, mais pas encore monté

Activation du stockage des journaux de script de session dans un compartiment Amazon S3

Lorsque vous activez la connexion Amazon S3 dans la configuration de votre script de session, WorkSpaces Pool capture le résultat standard de votre script de session. La sortie est régulièrement chargée dans un compartiment S3 au sein de votre compte Amazon Web Services. Pour chaque AWS région, WorkSpaces Pool crée un compartiment dans votre compte qui est unique à votre compte et à la région.

Vous n'avez à effectuer aucune tâche de configuration pour gérer ces compartiments S3. Ils sont entièrement gérés par le WorkSpaces service. Les fichiers journaux qui sont stockés dans chaque compartiment sont chiffrés en transit à l'aide des points de terminaison SSL d'Amazon S3 et au repos à l'aide des clés de chiffrement gérées par Amazon S3. Les compartiments sont nommés dans un format spécifique comme suit :

```
wspool-logs-<region-code>-<account-id-without-hyphens>-random-identifier
```

<region-code>

Il s'agit du code de AWS région dans lequel le WorkSpaces pool est créé avec le stockage par compartiment Amazon S3 activé pour les journaux de script de session.

<account-id-without-hyphens>

Identifiant de votre compte Amazon Web Services. L'identifiant aléatoire permet de garantir qu'aucun conflit ne sera déclenché avec les autres compartiments de la région. La première partie du nom du compartiment, `wspool-logs`, ne change pas quel que soit le compte ou la région.

Par exemple, si vous spécifiez des scripts de session dans une image de la région USA Ouest (Oregon) (`us-west-2`) sur le numéro de compte `123456789012`, WorkSpaces Pool crée un compartiment Amazon S3 au sein de votre compte dans cette région avec le nom affiché. Seul un administrateur disposant d'autorisations suffisantes peut supprimer ce compartiment.

```
wspool-logs-us-west-2-1234567890123-abcdefg
```

La désactivation des scripts de session ne supprime pas les fichiers journaux stockés dans le compartiment S3. Pour supprimer définitivement les fichiers journaux, vous ou un autre administrateur disposant des autorisations appropriées devez le faire à l'aide de la console ou

de l'API Amazon S3. WorkSpaces Pools ajoute une politique de compartiment qui empêche la suppression accidentelle du compartiment.

Lorsque les scripts de session sont activés, un dossier unique est créé pour chaque session de streaming démarrée.

Le chemin d'accès au dossier dans lequel les fichiers journaux sont stockés dans le compartiment S3 de votre compte est structuré comme suit :

```
<bucket-name>/<stack-name>/<fleet-name>/<access-mode>/<user-id-SHA-256-hash>/<session-id>/SessionScriptsLogs/<session-event>
```

<bucket-name>

Le nom du compartiment S3 dans lequel les scripts de session sont stockés. Le format du nom est décrit plus haut dans cette section.

<stack-name>

Le nom de la pile d'où est issue la session.

<fleet-name>

Nom du WorkSpaces pool sur lequel le script de session est exécuté.

<access-mode>

La méthode d'identification de l'utilisateur : custom pour l' WorkSpaces API ou la CLI, federated pour SAML et userpool pour les utilisateurs du groupe d'utilisateurs.

<user-id-SHA-256-hash>

Nom du dossier spécifique à l'utilisateur. Ce nom est créé à l'aide d'une chaîne hexadécimale de hachage SHA-256 en minuscules, générée à partir de l'identifiant utilisateur.

<session-id>

L'identifiant de la session de streaming de l'utilisateur. Chaque session de streaming utilisateur génère un ID unique.

<session-event>

L'événement qui a généré le journal du script de session. Les valeurs des événements sont SessionStart et SessionTermination.

L'exemple de structure de dossier suivant correspond à une session de streaming démarrée à partir de test-stack (pile-test) et test-fleet (flotte-test). La session utilise l'API de l'ID utilisateur `testuser@mydomain.com`, à partir d'un Compte AWS ID de `123456789012`, et le groupe `test-stack` de paramètres de la région USA Ouest (Oregon) (`us-west-2`) :

```
wspool-logs-us-west-2-1234567890123-abcdefg/test-stack/test-fleet/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13/05yd1391-4805-3da6-
f498-76f5x6746016/SessionScriptsLogs/SessionStart/
```

L'exemple de structure de dossier contient un fichier journal pour le script de démarrage de session du contexte utilisateur, et un autre fichier journal pour le script de démarrage de session du contexte système, le cas échéant.

WorkSpaces Pools de surveillance

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de vos WorkSpaces piscines.

Table des matières

- [WorkSpaces Métriques et dimensions des piscines](#)

WorkSpaces Métriques et dimensions des piscines

Amazon WorkSpaces envoie les métriques et informations de dimension des WorkSpaces pools suivantes à Amazon CloudWatch.

WorkSpaces Pools envoie des métriques à CloudWatch une seule fois par minute. L'espace de noms `AWS/Workspaces` inclut les métriques suivantes.

Mesures d'utilisation des pools

Métrique	Description
<code>ActiveUserSessionCapacity</code>	Le nombre de sessions utilisateur actuellement utilisées pour les sessions de streaming. Unités : nombre

Métrique	Description
	Statistiques valides : moyenne, minimum, maximum
ActualUserSessionCapacity	Le nombre total de sessions de pool disponibles en streaming ou en cours de diffusion. $\text{ActualUserSessionCapacity} = \text{AvailableUserSessionCapacity} + \text{ActiveUserSessionCapacity}$ Unités : nombre Statistiques valides : moyenne, minimum, maximum
AvailableUserSessionCapacity	Nombre de sessions de pool inactives actuellement disponibles pour le streaming par les utilisateurs. $\text{AvailableUserSessionCapacity} = \text{ActualUserSessionCapacity} - \text{ActiveUserSessionCapacity}$ Unités : nombre Statistiques valides : moyenne, minimum, maximum
PendingUserSessionCapacity	Le nombre de sessions mises en service pour votre pool. Représente le nombre supplémentaire de sessions de streaming que le pool peut prendre en charge une fois le provisionnement terminé. Unités : nombre Statistiques valides : moyenne, minimum, maximum

Métrique	Description
UserSessionsCapacityUtilization	Pourcentage de sessions utilisées dans un pool, selon la formule suivante. $\text{UserSessionCapacityUtilization} = (\text{ActiveUserSessionCapacity} / \text{ActualUserSessionCapacity}) * 100$ La surveillance de cette métrique aide à prendre des décisions concernant l'augmentation ou la diminution de la valeur de la capacité souhaitée d'un pool. Unités : pourcentage Statistiques valides : moyenne, minimum, maximum
DesiredUserSessionCapacity	Le nombre total de sessions en cours ou en attente. Cela représente le nombre total de sessions de streaming simultanées que votre pool peut prendre en charge dans un état stable. $\text{DesiredUserSessionCapacity} = \text{ActualUserSessionCapacity} + \text{PendingUserSessionCapacity}$ Unités : nombre Statistiques valides : moyenne, minimum, maximum
InsufficientCapacityError	Nombre de demandes de session rejetées par manque de capacité. Vous pouvez configurer des alarmes pour utiliser cette métrique afin d'être averti des utilisateurs qui attendent des sessions de streaming. Unités : nombre Statistiques valides : moyenne, minimum, maximum, somme

Activer et administrer le stockage persistant pour les WorkSpaces pools

WorkSpaces Les pools prennent en charge les dossiers de base pour le stockage persistant. En tant qu'administrateur de WorkSpaces pools, vous devez comprendre comment effectuer les tâches suivantes pour activer et administrer le stockage persistant pour vos utilisateurs.

Table des matières

- [Activez et administrez les dossiers de base pour les utilisateurs de vos WorkSpaces pools](#)

Activez et administrez les dossiers de base pour les utilisateurs de vos WorkSpaces pools

Lorsque vous activez les dossiers de base pour les WorkSpaces pools, les utilisateurs peuvent accéder à un dossier de stockage persistant pendant leurs sessions de streaming. Aucune configuration supplémentaire n'est requise de la part des utilisateurs pour que ceux-ci puissent accéder à leur dossier de base. Les données stockées par les utilisateurs dans leur dossier de base sont automatiquement sauvegardées dans un compartiment Amazon Simple Storage Service de votre compte Amazon Web Services, et les utilisateurs peuvent y accéder dans les sessions ultérieures.

Les fichiers et les dossiers sont chiffrés en transit à l'aide des points de terminaison SSL Amazon S3. Les fichiers et les dossiers sont chiffrés au repos à l'aide des clés de chiffrement gérées par Amazon S3.

Les dossiers de base sont stockés WorkSpaces dans WorkSpaces des pools aux emplacements par défaut suivants :

- Pour une session unique, non-domain-joined Windows WorkSpaces : `C:\Users\PhotonUser\My Files\Home Folder`
- Fenêtres jointes à un domaine : WorkSpaces `C:\Users\%username%\My Files\Home Folder`

En tant qu'administrateur, utilisez le chemin d'accès applicable si vous configurez vos applications pour enregistrer dans le dossier de base. Dans certains cas, il est possible que les utilisateurs ne trouvent pas leur dossier de base, car certaines applications ne reconnaissent pas la redirection qui

affiche le dossier de base en tant que dossier de niveau supérieur dans l'Explorateur de fichiers. Si tel est le cas, vos utilisateurs peuvent accéder à leur dossier de base en accédant au même répertoire dans l'Explorateur de fichiers.

Table des matières

- [Fichiers et répertoires associés aux applications gourmandes en ressources informatiques](#)
- [Activez les dossiers de base pour les utilisateurs de vos WorkSpaces pools](#)
- [Administration de vos dossiers de base](#)

Fichiers et répertoires associés aux applications gourmandes en ressources informatiques

Pendant les sessions de streaming de WorkSpaces Pools, l'enregistrement de fichiers et de répertoires volumineux associés à des applications gourmandes en ressources informatiques sur un stockage persistant peut prendre plus de temps que l'enregistrement des fichiers et des répertoires nécessaires aux applications de productivité de base. Par exemple, les applications peuvent mettre plus de temps à enregistrer une grande quantité de données ou à modifier fréquemment les mêmes fichiers que celles créées par des applications exécutant une seule action d'écriture. L'enregistrement de nombreux petits fichiers peut également prendre plus de temps.

Si vos utilisateurs enregistrent des fichiers et des répertoires associés à des applications gourmandes en ressources informatiques et que les options de stockage persistant des WorkSpaces pools ne fonctionnent pas comme prévu, nous vous recommandons d'utiliser une solution SMB (Server Message Block) telle qu'Amazon FSx pour Windows File Server ou une AWS Storage Gateway passerelle de fichiers. Vous trouverez ci-dessous des exemples de fichiers et de répertoires associés à des applications gourmandes en ressources informatiques qui conviennent mieux à ces solutions SMB :

- Dossiers d'espace de travail pour les environnements de développement intégrés (IDEs)
- Fichiers de base de données locaux
- Dossiers Scratch Space créés par des applications de simulation graphique

Pour plus d'informations, consultez la section [Passerelles de fichiers](#) dans le guide de AWS Storage Gateway l'utilisateur.

Activez les dossiers de base pour les utilisateurs de vos WorkSpaces pools

Avant d'activer les dossiers de base, vous devez effectuer les opérations suivantes :

- Vérifiez que vous disposez des autorisations Gestion des identités et des accès AWS (IAM) correctes pour les actions Amazon S3.
- Utilisez une image créée à partir d'une image de AWS base publiée le 18 mai 2017 ou après cette date.
- Activez la connectivité réseau à Amazon S3 à partir de votre cloud privé virtuel (VPC) en configurant l'accès Internet ou un point de terminaison d'un VPC pour Amazon S3. Pour plus d'informations, consultez [Mise en réseau et accès pour les WorkSpaces piscines](#) et [Fonctionnalités d'utilisation des points de terminaison VPC Amazon S3 pour les pools WorkSpaces](#).

Vous pouvez activer ou désactiver les dossiers de base lors de la création d'un répertoire (voir [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#)), ou après la création du répertoire en utilisant le AWS Management Console for WorkSpaces Pools. Pour chaque région AWS , les dossiers de base sont sauvegardés par un compartiment S3.

La première fois que vous activez les dossiers de base pour un répertoire WorkSpaces Pools dans une AWS région, le service crée un compartiment Amazon S3 dans votre compte dans cette même région. Le même compartiment est utilisé pour stocker le contenu des dossiers de base de tous les utilisateurs et de tous les répertoires de cette région. Pour de plus amples informations, veuillez consulter [Stockage dans un compartiment Amazon S3](#).

Pour activer les dossiers de base lors de la création d'un répertoire

- Suivez les étapes de la section [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#) et vérifiez que la case Activer les dossiers de base est cochée.

Pour activer les dossiers de base pour un répertoire existant

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation de gauche, choisissez Répertoires, puis sélectionnez le répertoire pour lequel vous souhaitez activer les dossiers de base.
3. Sous la liste des répertoires, choisissez Stockage, puis sélectionnez Activer les dossiers personnels.
4. Dans la boîte de dialogue Activer les dossiers de base, choisissez Activer.

Administration de vos dossiers de base

Table des matières

- [Désactivation des dossiers de base](#)
- [Stockage dans un compartiment Amazon S3](#)
- [Synchronisation du contenu du dossier de base](#)
- [Formats du dossier de base](#)
- [Ressources supplémentaires](#)

Désactivation des dossiers de base

Vous pouvez désactiver les dossiers de base d'un répertoire sans perdre le contenu utilisateur déjà stocké dans les dossiers de base. La désactivation des dossiers de base d'un répertoire a les effets suivants :

- Les utilisateurs connectés à des sessions de streaming actives pour l'annuaire reçoivent un message d'erreur. Ils sont notifiés qu'ils ne peuvent plus stocker de contenu dans leur dossier de base.
- Les dossiers de base n'apparaissent pas pour les nouvelles sessions utilisant le répertoire dont les dossiers de base sont désactivés.
- La désactivation des dossiers de base pour un répertoire ne le désactive pas pour les autres répertoires.
- Même si les dossiers de base sont désactivés pour tous les répertoires, WorkSpaces Pools ne supprime pas le contenu utilisateur.

Pour rétablir l'accès aux dossiers de base pour le répertoire, réactivez les dossiers de base en suivant les étapes décrites plus haut dans cette rubrique.

Pour désactiver les dossiers de base lors de la création d'un répertoire

- Suivez les étapes de la section [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#) et vérifiez que l'option Activer les dossiers de base est décochée.

Pour désactiver les dossiers de base d'un répertoire existant

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.

2. Dans le volet de navigation de gauche, choisissez Répertoires, puis sélectionnez le répertoire pour lequel vous souhaitez activer les dossiers de base.
3. Sous la liste des répertoires, choisissez Stockage et décochez la case Activer les dossiers de base.
4. Dans la boîte de dialogue Désactiver les dossiers de base, tapez CONFIRM (sensible à la casse) pour confirmer votre choix, puis choisissez Désactiver.

Stockage dans un compartiment Amazon S3

WorkSpaces Pools gère le contenu utilisateur stocké dans des dossiers personnels à l'aide de compartiments Amazon S3 créés dans votre compte. Pour chaque AWS région, WorkSpaces Pools crée un bucket dans votre compte. Tout le contenu utilisateur généré à partir des sessions de streaming des annuaires de cette région est stocké dans ce compartiment. Les compartiments sont entièrement gérés par le service sans intervention ou configuration d'un administrateur. Les compartiments sont nommés dans un format spécifique comme suit :

```
wspool-home-folder-<region-code>-<account-id-without-hyphens>-<random-identifiant>
```

Où *<region-code>* se trouvent le code de AWS région dans lequel le répertoire a été créé, l'identifiant de votre compte Amazon Web Services, et *>random-identifiant<* un numéro d'identification aléatoire généré par le WorkSpaces service. *<account-id-without-hyphens>* La première partie du nom du compartiment, `wspool-home-folder-`, ne change pas quel que soit le compte ou la région.

Par exemple, si vous activez les dossiers de base pour les annuaires de la région USA Ouest (Oregon) (`us-west-2`) sous le numéro de compte `123456789012`, le service crée un compartiment Amazon S3 dans cette région avec le nom affiché. Seul un administrateur disposant d'autorisations suffisantes peut supprimer ce compartiment.

```
wspool-home-folder-us-west-2-123456789012
```

Comme indiqué précédemment, la désactivation des dossiers personnels pour les annuaires ne supprime aucun contenu utilisateur stocké dans le compartiment Amazon S3. Pour supprimer définitivement le contenu utilisateur, un administrateur disposant d'un accès suffisant doit le faire depuis la console Amazon S3. WorkSpaces Pools ajoute une politique de compartiment qui empêche la suppression accidentelle du compartiment.

Synchronisation du contenu du dossier de base

Lorsque les dossiers de base sont activés, WorkSpaces Pools crée un dossier unique pour chaque utilisateur dans lequel stocker son contenu. Le dossier est créé sous la forme d'un préfixe Amazon S3 unique qui utilise un hachage du nom d'utilisateur dans un compartiment S3 pour votre compte et votre région Amazon Web Services. Une fois que WorkSpaces Pools a créé le dossier de base dans Amazon S3, il copie le contenu consulté dans ce dossier du compartiment S3 vers le Workspace. Cela permet à l'utilisateur d'accéder rapidement au contenu de son dossier de base, depuis le Workspace WorkSpace pool, pendant sa session de streaming. Les modifications que vous apportez au contenu du dossier de base d'un utilisateur dans un compartiment S3 et que l'utilisateur apporte au contenu de son dossier de base Workspace dans un WorkSpace pool sont synchronisées entre Amazon S3 et les WorkSpaces pools comme suit.

1. Au début de la session de streaming WorkSpaces Pools d'un utilisateur, WorkSpaces Pools catalogue les fichiers du dossier de base qui sont stockés pour cet utilisateur dans le compartiment Amazon S3 de votre compte et de votre région Amazon Web Services.
2. Le contenu du dossier personnel d'un utilisateur est également stocké Workspace dans les WorkSpaces pools à partir desquels il diffuse. Lorsqu'un utilisateur accède à son dossier personnel sur le Workspace, la liste des fichiers catalogués s'affiche.
3. WorkSpaces Pools télécharge un fichier depuis le compartiment S3 vers le Workspace uniquement une fois que l'utilisateur a utilisé une application de streaming pour ouvrir le fichier pendant sa session de streaming.
4. Une fois que WorkSpaces Pools a téléchargé le fichier sur le Workspace, la synchronisation a lieu après l'accès au fichier
5. Si l'utilisateur modifie le fichier au cours de sa session de streaming, WorkSpaces Pools télécharge régulièrement la nouvelle version du fichier depuis le Workspace compartiment S3 ou à la fin de la session de streaming. Cependant, le fichier n'est pas téléchargé à nouveau depuis le compartiment S3 pendant la session de streaming.

Les sections suivantes décrivent le comportement de synchronisation lorsque vous ajoutez, remplacez ou supprimez le fichier du dossier de base d'un utilisateur dans Amazon S3.

Table des matières

- [Synchronisation des fichiers ajoutés au dossier de base d'un utilisateur dans Amazon S3](#)
- [Synchronisation des fichiers remplacés du dossier de base d'un utilisateur dans Amazon S3](#)
- [Synchronisation des fichiers remplacés du dossier de base d'un utilisateur dans Amazon S3](#)

Synchronisation des fichiers ajoutés au dossier de base d'un utilisateur dans Amazon S3

Si vous ajoutez un nouveau fichier au dossier personnel d'un utilisateur dans un compartiment S3, WorkSpaces Pools le catalogue et l'affiche dans la liste des fichiers du dossier personnel de l'utilisateur en quelques minutes. Cependant, le fichier n'est pas téléchargé du compartiment S3 vers le WorkSpace tant que l'utilisateur n'ouvre pas le fichier avec une application pendant sa session de streaming.

Synchronisation des fichiers remplacés du dossier de base d'un utilisateur dans Amazon S3

Si un utilisateur ouvre un fichier dans son dossier personnel ou WorkSpace dans le WorkSpace pool pendant sa session de streaming, et que vous remplacez le même fichier dans son dossier de base dans un compartiment S3 par une nouvelle version pendant la session de streaming active de cet utilisateur, la nouvelle version du fichier n'est pas immédiatement téléchargée sur le WorkSpace. La nouvelle version est téléchargée du compartiment S3 vers le WorkSpace uniquement lorsque l'utilisateur démarre une nouvelle session de streaming et ouvre à nouveau le fichier.

Synchronisation des fichiers remplacés du dossier de base d'un utilisateur dans Amazon S3

Si un utilisateur ouvre un fichier dans son dossier personnel ou WorkSpace dans le WorkSpace pool pendant sa session de streaming, et que vous supprimez le fichier de son dossier de base dans un compartiment S3 pendant la session de streaming active de cet utilisateur, le fichier est supprimé WorkSpace après que l'utilisateur a effectué l'une des actions suivantes :

- Ouvre à nouveau le dossier de base
- Actualise le dossier de base

Formats du dossier de base

La hiérarchie d'un dossier utilisateur dépend de la manière dont un utilisateur lance une session de streaming, comme décrit dans la section suivante.

SAML 2.0

Pour les sessions créées à l'aide d'une fédération SAML, la structure du dossier utilisateur se présente comme suit :

```
bucket-name/user/federated/user-id-SHA-256-hash/
```

Dans ce cas, *user-id-SHA-256-hash* est le nom du dossier créé à l'aide d'une chaîne hexadécimale de hachage SHA-256 en minuscules générée à partir de la valeur de l'attribut SAML NameID transmis dans la demande de fédération SAML. Pour différencier les utilisateurs ayant le même nom mais appartenant à deux domaines différents, envoyez la demande SAML avec NameID au format domainname\username. Pour de plus amples informations, veuillez consulter [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#).

L'exemple de structure de dossier suivant concerne l'accès à la session à l'aide de la fédération SAML avec NameID SAMPLEDOMAIN\testuser, ID de compte 123456789012 dans la Région USA Ouest (Oregon) :

```
wspool-home-folder-us-west-2-123456789012/user/  
federated/8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901
```

Lorsqu'une partie ou la totalité de la chaîne NameID est en majuscule (comme le nom de domaine l'*SAMPLEDOMAIN* est dans l'exemple), WorkSpaces Pools génère la valeur de hachage en fonction de la capitalisation utilisée dans la chaîne. Dans cet exemple, la valeur de hachage pour SAMPLEDOMAIN \ testuser est 8 DD9 A642F511609454D344D53 A71190E44 B8 C507012A9901CB861. FED2 AF9 FDE0 Dans le dossier de cet utilisateur, cette valeur est affichée en minuscules, comme suit : 8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901.

Vous pouvez identifier le dossier d'un utilisateur en générant la valeur de hachage SHA-256 du NameID à l'aide des sites web ou des bibliothèques de codage en open source disponibles en ligne.

Ressources supplémentaires

Pour plus d'informations sur la gestion des compartiments Amazon S3 et les meilleures pratiques, veuillez consulter les points suivants dans le Guide de l'utilisateur Amazon Simple Storage Service :

- Grâce aux stratégies Amazon S3, vous pouvez fournir à vos utilisateurs l'accès hors ligne aux données utilisateur. Pour plus d'informations, consultez [Amazon S3: Allows IAM Users Access to Their S3 Home Directory, Programmatically and In the Console](#) dans le Guide de l'utilisateur IAM.
- Vous pouvez activer le contrôle de version des fichiers pour le contenu stocké dans les compartiments Amazon S3 utilisés par WorkSpaces les pools. Pour plus d'informations, consultez [Utilisation de la gestion des versions](#).

Activez la persistance des paramètres de l'application pour les utilisateurs de vos WorkSpaces pools

WorkSpaces Les pools prennent en charge les paramètres d'application persistants pour les annuaires Windows. Cela signifie que les personnalisations de votre application par les utilisateurs et les paramètres de Windows sont automatiquement enregistrés après chaque session de streaming et appliqués lors de la suivante. Parmi les exemples de paramètres d'application persistants que vos utilisateurs peuvent configurer, on peut notamment citer les favoris de navigateur Web, les paramètres, les sessions de page Web, les profils de connexion d'application, les plug-ins et les personnalisations de l'interface utilisateur. Ces paramètres sont enregistrés dans un compartiment Amazon Simple Storage Service (Amazon S3) de votre compte, au sein de AWS la région dans laquelle la persistance des paramètres de l'application est activée. Ils sont disponibles dans chaque session de streaming de WorkSpaces Pools.

Note

Des frais Amazon S3 standard peuvent s'appliquer aux données stockées dans votre compartiment S3. Pour plus d'informations, consultez [Tarification Amazon S3](#).

Table des matières

- [Fonctionnement de la persistance des paramètres de l'application](#)
- [Activer la persistance des paramètres de l'application](#)
- [Gérez les paramètres de l'application VHDs pour vos utilisateurs](#)

Fonctionnement de la persistance des paramètres de l'application

Les paramètres d'application persistants sont enregistrés dans un fichier de disque dur virtuel (VHD). Ce fichier est créé la première fois qu'un utilisateur diffuse une application depuis un répertoire dans lequel la persistance des paramètres de l'application est activée. Si le WorkSpace pool associé au répertoire est basé sur une image contenant les paramètres d'application et Windows par défaut, les paramètres par défaut sont utilisés lors de la première session de streaming de l'utilisateur.

Lorsque la session de streaming prend fin, le VHD est démonté et chargé vers un compartiment Amazon S3 de votre compte. Le bucket est créé lorsque vous activez les paramètres d'application

persistants pour la première fois pour un répertoire dans une AWS région. Le bucket est propre à votre AWS compte et à la région. [Le disque dur virtuel est chiffré en transit à l'aide des points de terminaison SSL Amazon S3, et au repos à l'aide AWS de Managed. CMKs](#)

Le VHD est monté sur les deux WorkSpace entrées C:\Users\%username% et D:\%username%. Si vous WorkSpace n'êtes pas joint à un domaine Active Directory, le nom d'utilisateur Windows est PhotonUser. Si vous WorkSpace êtes joint à un domaine Active Directory, le nom d'utilisateur Windows est celui de l'utilisateur connecté.

La persistance des paramètres d'application ne fonctionne pas entre différentes versions de systèmes d'exploitation. Par exemple, si vous activez la persistance des paramètres d'application pour un WorkSpace pool qui utilise une image Windows Server 2019, si vous mettez à jour le WorkSpace pool pour utiliser une image qui exécute un autre système d'exploitation (tel que Windows Server 2022), les paramètres des sessions de streaming précédentes ne sont pas enregistrés pour les utilisateurs du répertoire. Au lieu de cela, une fois que vous avez mis à jour le WorkSpace pool pour utiliser la nouvelle image, un nouveau profil utilisateur Windows est créé lorsque les utilisateurs lancent une session de streaming à partir d'un WorkSpace. Toutefois, si vous appliquez une mise à jour vers le même système d'exploitation à l'image, les personnalisations et paramètres des utilisateurs provenant de précédentes sessions de streaming sont enregistrés. Lorsque des mises à jour du même système d'exploitation sont appliquées à une image, le même profil utilisateur Windows est utilisé lorsque les utilisateurs lancent une session de streaming à partir du WorkSpace.

Important

WorkSpaces Les pools prennent en charge les applications qui s'appuient sur l'[API Microsoft Data Protection](#) uniquement lorsqu'elles WorkSpace sont jointes à un domaine Microsoft Active Directory. Dans les cas où a n' WorkSpace est pas joint à un domaine Active Directory, l'utilisateur Windows est différent sur chacun d'eux WorkSpace. PhotonUser En raison de la manière dont fonctionne le modèle de sécurité DPAPI, les mots de passe des utilisateurs ne sont pas conservés pour les applications qui utilisent DPAPI dans ce scénario. Dans les cas où vous WorkSpaces êtes joint à un domaine Active Directory et que l'utilisateur est un utilisateur du domaine, le nom d'utilisateur Windows est celui de l'utilisateur connecté, et les mots de passe des utilisateurs sont conservés pour les applications qui utilisent DPAPI.

WorkSpaces Pools enregistre automatiquement tous les fichiers et dossiers situés dans ce chemin, à l'exception des dossiers suivants :

- Contacts
- Desktop
- Documents
- Téléchargements
- Liens
- Images
- Saved Games
- Recherches
- Vidéos

Les fichiers et dossiers créés en dehors de ces dossiers sont enregistrés dans le fichier VHD et synchronisés avec Amazon S3. La taille maximale du VHD par défaut est de 5 Go pour les pools. La taille du VHD enregistré est la taille totale des fichiers et dossiers qu'il contient. WorkSpaces Pools enregistre automatiquement la ruche de HKEY_CURRENT_USER registre pour l'utilisateur. Pour les nouveaux utilisateurs (utilisateurs dont le profil n'existe pas dans Amazon S3), WorkSpaces Pools crée le profil initial en utilisant le profil par défaut. Ce profil est créé à l'emplacement suivant sur le générateur d'images :C:\users\default.

 Note

L'intégralité du VHD doit être téléchargée sur le Workspace avant qu'une session de streaming puisse commencer. De ce fait, un fichier VHD qui contient une grande quantité de données peut retarder le début de la session de streaming. Pour plus d'informations, consultez [Bonnes pratiques pour activer la persistance des paramètres des applications](#).

Lorsque vous activez la persistance des paramètres d'application, vous devez spécifier un groupe de paramètres. Le groupe de paramètres détermine quels paramètres d'application enregistrés sont utilisés pour une session de streaming à partir de ce répertoire. WorkSpaces Pools crée un nouveau fichier VHD pour le groupe de paramètres qui est stocké séparément dans le compartiment S3 de votre AWS compte. Si le groupe de paramètres est partagé entre des annuaires, les mêmes paramètres d'application sont utilisés dans chaque répertoire. Si un répertoire nécessite ses propres paramètres d'application, spécifiez un groupe de paramètres unique pour le répertoire.

Activer la persistance des paramètres de l'application

Table des matières

- [Conditions préalables pour activer la persistance des paramètres de l'application](#)
- [Bonnes pratiques pour activer la persistance des paramètres des applications](#)
- [Comment activer la persistance des paramètres de l'application](#)

Conditions préalables pour activer la persistance des paramètres de l'application

Pour activer la persistance des paramètres d'application, vous devez d'abord effectuer les opérations suivantes :

- Utilisez une image créée à partir d'une image de base publiée AWS le 7 décembre 2017 ou après cette date.
- Activez la connectivité réseau à Amazon S3 à partir de votre cloud privé virtuel (VPC) en configurant l'accès Internet ou un point de terminaison d'un VPC pour Amazon S3. Pour plus d'informations, consultez la section Dossiers de base et points de terminaison d'un VPC dans [Mise en réseau et accès pour les WorkSpaces piscines](#).

Bonnes pratiques pour activer la persistance des paramètres des applications

Pour activer la persistance des paramètres de l'application sans fournir un accès Internet à votre compte WorkSpaces, utilisez un point de terminaison VPC. Ce point de terminaison doit se trouver dans le VPC auquel vos WorkSpaces pools WorkSpaces in sont connectés. Vous devez joindre une politique personnalisée pour permettre aux WorkSpaces Pools d'accéder au point de terminaison. Pour plus d'informations sur la création d'une stratégie personnalisée, consultez la section Dossiers de base et points de terminaison d'un VPC dans [Mise en réseau et accès pour les WorkSpaces piscines](#). Pour plus d'informations sur les points de terminaison Amazon S3 privés, consultez [Points de terminaison d'un VPC](#) et [Points de terminaison pour Amazon S3](#) dans le Guide de l'utilisateur Amazon VPC.

Comment activer la persistance des paramètres de l'application

Vous pouvez activer ou désactiver la persistance des paramètres de l'application lors de la création d'un répertoire ou après la création du répertoire à l'aide de la WorkSpaces console. Pour chaque région AWS , les paramètres d'application persistants sont stockés dans un compartiment S3 de votre compte.

La première fois que vous activez la persistance des paramètres d'application pour un répertoire dans une AWS région, WorkSpaces Pools crée un compartiment S3 dans votre AWS compte dans la même région. Le même compartiment stocke le fichier VHD des paramètres de l'application pour tous les utilisateurs et tous les répertoires de cette AWS région. Pour plus d'informations, consultez [Stockage dans un compartiment Amazon S3 dans Gérez les paramètres de l'application VHDs pour vos utilisateurs](#).

Pour activer la persistance des paramètres de l'application lors de la création d'un répertoire

- Suivez les étapes de la section [Configurer SAML 2.0 et créer un répertoire WorkSpaces Pools](#) et vérifiez que la case Activer la persistance des paramètres d'application est cochée.

Pour activer la persistance des paramètres d'application pour un répertoire existant

1. Ouvrez la WorkSpaces console sur <https://console.aws.amazon.com/workspaces/v2/home>.
2. Dans le volet de navigation de gauche, choisissez Pools, puis sélectionnez le pool pour lequel vous souhaitez activer la persistance des applications.
3. Choisissez Modifier dans la section Paramètres de la page.
4. Dans la section Persistance de l'application de la page, sélectionnez Activer la persistance des paramètres de l'application.
5. Sélectionnez Enregistrer les modifications.

La persistance des paramètres d'application est désormais activée pour les nouvelles sessions de streaming.

Gérez les paramètres de l'application VHDs pour vos utilisateurs

Table des matières

- [Stockage par compartiment Amazon S3](#)
- [Réinitialisation des paramètres de l'application d'un utilisateur](#)
- [Activer la gestion des versions des objets Amazon S3 et rétablir les paramètres de l'application d'un utilisateur](#)
- [Augmenter la taille des paramètres de l'application VHD](#)

Stockage par compartiment Amazon S3

Lorsque vous activez la persistance des paramètres des applications, les personnalisations des applications et les paramètres Windows de vos utilisateurs sont automatiquement enregistrés dans un fichier de disque dur virtuel (VHD) stocké dans un compartiment Amazon S3 créé dans votre AWS compte. Pour chaque AWS région, WorkSpaces Pools crée un compartiment dans votre compte qui est unique à votre compte et à la région. Tous les paramètres d'application configurés par vos utilisateurs sont stockés dans le compartiment de cette région.

Vous n'avez pas besoin d'effectuer de tâches de configuration pour gérer ces compartiments S3 ; ils sont entièrement gérés par le service WorkSpaces Pools. [Le fichier VHD stocké dans chaque compartiment est chiffré en transit à l'aide des points de terminaison SSL d'Amazon S3 et au repos à l'aide AWS de Managed. CMKs](#) Les compartiments sont nommés dans un format spécifique comme suit :

```
wspool-app-settings-<region-code>-<account-id-without-hyphens>-<random-identifiant>
```

region-code

Il s'agit du code de AWS région dans lequel le répertoire est créé avec la persistance des paramètres de l'application.

account-id-without-hyphens

L'identifiant AWS de votre compte. L'identificateur aléatoire garantit l'absence de conflit avec d'autres compartiments de cette région. La première partie du nom du compartiment, wspool-app-settings, ne change pas quel que soit le compte ou la région.

Par exemple, si vous activez la persistance des paramètres d'application pour les annuaires de la région USA Ouest (Oregon) (us-west-2) sous le numéro de compte 123456789012 WorkSpaces , Pools crée un compartiment Amazon S3 au sein de votre compte dans cette région avec le nom indiqué. Seul un administrateur disposant d'autorisations suffisantes peut supprimer ce compartiment.

```
wspool-app-settings-us-west-2-123456789012-abcdefg
```

La désactivation de la persistance des paramètres de l'application ne supprime aucun des paramètres VHDs stockés dans le compartiment S3. Pour supprimer définitivement des paramètres VHDs, vous ou un autre administrateur disposant des autorisations appropriées devez le faire à l'aide

de la console ou de l'API Amazon S3. WorkSpaces Pools ajoute une politique de compartiment qui empêche la suppression accidentelle du compartiment.

Lorsque la persistance des paramètres d'application est activée, un dossier unique est créé pour chaque groupe de paramètres pour stocker le fichier VHD de paramètres. La hiérarchie du dossier dans le compartiment S3 dépend de la manière dont l'utilisateur lance une session de streaming, comme décrit dans la section suivante.

Le chemin d'accès du dossier dans lequel le fichier VHD de paramètres est stocké dans le compartiment S3 de votre compte utilise la structure suivante :

```
bucket-name/Windows/prefix/settings-group/access-mode/user-id-SHA-256-hash
```

bucket-name

Nom du compartiment S3 dans lequel les paramètres d'applications des utilisateurs sont stockés. Le format du nom est décrit plus haut dans cette section.

prefix

Préfixe spécifique à la version de Windows. Par exemple, v4 pour Windows Server 2012 R2.

settings-group

Valeur du groupe de paramètres. Cette valeur est appliquée à un ou plusieurs répertoires qui partagent les mêmes paramètres d'application.

access-mode

La méthode d'identification de l'utilisateur : *custom* pour l'API ou la CLI de WorkSpaces Pools, *federated* pour le SAML et *userpool* pour les utilisateurs du groupe d'utilisateurs.

user-id-SHA-256-hash

Nom du dossier spécifique à l'utilisateur. Ce nom est créé à l'aide d'une chaîne hexadécimale de hachage SHA-256 en minuscules générée à partir de l'ID d'utilisateur.

L'exemple de structure de dossiers suivant s'applique à une session de streaming accessible via l'API ou la CLI avec un ID utilisateur *testuser@mydomain.com*, un Compte AWS ID de *123456789012* et le groupe de paramètres *test-stack* dans la région USA Ouest (Oregon) (*us-west-2*) :

```
wspool-app-settings-us-west-2-123456789012-abcdefg/Windows/v4/test-stack/custom/  
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13
```

Vous pouvez identifier le dossier d'un utilisateur en générant la valeur de hachage SHA-256 de l'ID d'utilisateur en minuscules à l'aide des sites web ou des bibliothèques de codage en open source disponibles en ligne.

Réinitialisation des paramètres de l'application d'un utilisateur

Pour réinitialiser les paramètres de l'application d'un utilisateur, vous devez rechercher et supprimer le disque dur virtuel et le fichier de métadonnées associé dans le compartiment S3 de votre AWS compte. Veillez à ne pas effectuer cette opération pendant une session de streaming active de l'utilisateur. Après avoir supprimé le VHD de l'utilisateur et le fichier de métadonnées, la prochaine fois que l'utilisateur lance une session à partir d'une instance de streaming sur laquelle la persistance des paramètres de l'application est activée, WorkSpaces Pools crée un nouveau VHD de paramètres pour cet utilisateur.

Pour réinitialiser les paramètres d'application d'un utilisateur

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom de compartiment, choisissez le compartiment S3 qui contient le fichier VHD de paramètres d'application que vous souhaitez réinitialiser.
3. Recherchez le dossier qui contient le fichier VHD. Pour plus d'informations sur la navigation dans la structure de dossiers du compartiment S3, consultez la section Stockage dans un compartiment Amazon S3 plus haut dans cette rubrique.
4. Dans la liste Nom, sélectionnez la case à cocher en regard du fichier VHD et du fichier REG, choisissez Plus, puis Supprimer.
5. Dans la boîte de dialogue Supprimer les objets, vérifiez que le fichier VHD et le fichier REG sont répertoriés, puis choisissez Supprimer.

La prochaine fois que l'utilisateur diffuse à partir d'un pool sur lequel la persistance des paramètres d'application est activée avec le groupe de paramètres applicable, un nouveau VHD de paramètres d'application est créé. Ce fichier VHD est enregistré dans le compartiment S3 à la fin de la session.

Activer la gestion des versions des objets Amazon S3 et rétablir les paramètres de l'application d'un utilisateur

Vous pouvez utiliser les stratégies de cycle de vie et la gestion des versions des objets Amazon S3 pour gérer les paramètres d'application de vos utilisateurs lorsque ceux-ci les modifient. Avec la gestion des versions des objets Amazon S3, vous pouvez conserver, récupérer et restaurer chaque

version du fichier VHD de paramètres. Vous pouvez ainsi récupérer tant après des actions utilisateur involontaires que des défaillances de l'application. Lorsque la gestion des versions est activée, après chaque session de streaming, une nouvelle version du fichier VHD des paramètres d'application est synchronisée avec Amazon S3. La nouvelle version ne remplace pas la précédente. Ainsi, en cas de problème avec les paramètres de vos utilisateurs, vous pouvez revenir à une version précédente du fichier VHD.

 Note

Chaque version du fichier VHD des paramètres d'application est enregistrée sur Amazon S3 sous la forme d'un objet distinct et est facturée en conséquence.

La gestion des versions d'objets n'est pas activée par défaut dans votre compartiment S3. Vous devez donc l'activer de manière explicite.

Pour activer la gestion des versions d'objets pour votre fichier VHD de paramètres d'application

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom de compartiment, choisissez le compartiment S3 qui contient le fichier VHD de paramètres d'application sur lequel vous souhaitez activer la gestion des versions d'objets.
3. Choisissez Propriétés.
4. Choisissez Gestion des versions, sélectionnez Activer la gestion des versions, puis choisissez Enregistrer.

Pour faire expirer les anciennes versions des paramètres de votre application VHDs, vous pouvez utiliser les politiques de cycle de vie d'Amazon S3. Pour plus d'informations, consultez [Comment créer une stratégie de cycle de vie pour un compartiment S3 ?](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour restaurer le fichier VHD des paramètres d'application d'un utilisateur

Vous pouvez restaurer une version précédente du fichier VHD de paramètres d'application d'un utilisateur en supprimant les versions plus récentes du fichier VHD applicable du compartiment S3. N'effectuez pas cette opération lorsque l'utilisateur a une session de streaming active.

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.

2. Dans la liste Nom de compartiment, choisissez le compartiment S3 qui contient la version du fichier VHD de paramètres d'application de l'utilisateur que vous souhaitez restaurer.
3. Recherchez et sélectionnez le dossier qui contient le fichier VHD. Pour plus d'informations sur la navigation dans la structure de dossiers du compartiment S3, consultez Stockage dans un compartiment Amazon S3 plus haut dans cette rubrique.

Lorsque vous sélectionnez le dossier, le fichier VHD des paramètres et le fichier de métadonnées associé s'affichent.

4. Pour afficher la liste des versions du fichier VHD et du fichier de métadonnées, choisissez Afficher.
5. Recherchez la version du fichier VHD à restaurer.
6. Dans la liste Nom, cochez les cases en regard des versions les plus récentes du fichier VHD et des fichiers de métadonnées associés, choisissez Plus, puis Supprimer.
7. Assurez-vous que le fichier VHD de paramètres d'application que vous souhaitez restaurer et les fichiers de métadonnées associés sont les versions les plus récentes de ces fichiers.

La prochaine fois que l'utilisateur diffuse à partir d'un pool sur lequel la persistance des paramètres de l'application est activée avec le groupe de paramètres applicable, la version inversée des paramètres de l'utilisateur s'affiche.

Augmenter la taille des paramètres de l'application VHD

La taille maximale du VHD par défaut est de 5 Go pour les pools. Si un utilisateur a besoin de plus d'espace pour les paramètres d'application, vous pouvez télécharger le fichier VHD de paramètres d'application applicable sur un ordinateur Windows pour l'étendre. Ensuite, remplacez le fichier VHD actuel dans le compartiment S3 par le plus grand. N'effectuez pas cette opération lorsque l'utilisateur a une session de streaming active.

Note

Pour réduire la taille physique du disque dur virtuel (VHD), videz la corbeille avant de terminer une session. Cela réduit également les temps de chargement et de téléchargement et améliore l'expérience utilisateur globale.

Pour augmenter la taille du fichier VHD de paramètres d'application

Note

Tout le fichier VHD doit être téléchargé avant qu'un utilisateur puisse diffuser des applications. L'augmentation de la taille d'un fichier VHD de paramètres d'application peut augmenter le temps au lancement des sessions de streaming d'applications par les utilisateurs.

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom de compartiment, choisissez le compartiment S3 qui contient le fichier VHD de paramètres d'application à étendre.
3. Recherchez et sélectionnez le dossier qui contient le fichier VHD. Pour plus d'informations sur la façon de naviguer dans la structure des dossiers de compartiments S3, voir [Stockage par compartiment Amazon S3](#) plus haut dans cette rubrique.

Lorsque vous sélectionnez le dossier, le fichier VHD des paramètres et le fichier de métadonnées associé s'affichent.

4. Téléchargez le `Profile.vhdx` fichier dans un répertoire de votre ordinateur Windows. Ne fermez pas votre navigateur lorsque le téléchargement est terminé, car vous l'utiliserez ensuite pour charger le fichier VHD étendu.
5. Pour utiliser Diskpart afin d'augmenter la taille du disque dur virtuel à 7 Go, ouvrez l'invite de commande en tant qu'administrateur et tapez les commandes suivantes.

```
diskpart
```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
expand vdisk maximum=7000
```

6. Ensuite, tapez les commandes Diskpart suivantes pour trouver et attacher le fichier VHD et afficher la liste des volumes :

```
elect vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
attach vdisk
```

```
list volume
```

Dans la sortie, notez le numéro du volume avec l'étiquette « AwsEucUsers ». À l'étape suivante, vous sélectionnez ce volume afin de pouvoir l'étendre.

7. Tapez la commande suivante dans laquelle *<volume-number>* figure le numéro figurant dans la sortie du volume de la liste.

```
select volume <volume-number>
```

8. Saisissez la commande suivante :

```
extend
```

9. Tapez les commandes suivantes pour confirmer que la taille de la partition du VHD a augmenté comme prévu (7 Go dans cet exemple) :

```
diskpart
```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
list volume
```

10. Tapez la commande suivante pour détacher le fichier VHD pour qu'il puisse être chargé :

```
detach vdisk
```

11. Revenez à votre navigateur à l'aide de la console Amazon S3, choisissez Charger, Ajouter des fichiers, puis sélectionnez le fichier VHD étendu.
12. Choisissez Charger.

Une fois le VHD chargé, la prochaine fois que l'utilisateur diffuse à partir d'un pool sur lequel la persistance des paramètres d'application est activée avec le groupe de paramètres applicable, le VHD avec les paramètres d'application les plus importants est disponible.

WorkSpaces Codes de notification de dépannage des pools

Voici les codes de notification et les étapes de résolution des problèmes de liaison de domaines que vous pourriez rencontrer lors de l'installation et de l'utilisation d'Active Directory avec WorkSpaces.

DOMAIN_JOIN_ERROR_ACCESS_DENIED

Message : Accès refusé.

Résolution : Le compte de service spécifié dans le répertoire n'est pas autorisé à créer l'objet informatique ou à réutiliser un objet existant. Validez les autorisations et démarrez le WorkSpaces pool.

DOMAIN_JOIN_ERROR_LOGON_FAILURE

Message : Le nom d'utilisateur ou le mot de passe est incorrect.

Résolution : Le compte de service indiqué dans le répertoire possède un nom d'utilisateur ou un mot de passe non valide. Mettez à jour les informations d'identification dans le AWS Secrets Manager secret configuré dans le répertoire et redémarrez le WorkSpaces pool.

DOMAIN_JOIN_ERROR_PASSWORD_EXPIRED

Message : le mot de passe de cet utilisateur est expiré.

Résolution : Le mot de passe du compte de service indiqué dans le AWS Secrets Manager secret a expiré. Arrêtez d'abord la WorkSpaces piscine. Modifiez ensuite le mot de passe du secret spécifié dans le WorkSpaces répertoire. Ensuite, lancez le WorkSpaces pool.

DOMAIN_JOIN_ERROR_DS_MACHINE_ACCOUNT_QUOTA_EXCEEDED

Message : Votre ordinateur n'a pas pu joindre le domaine. Vous avez dépassé le nombre maximal de comptes d'ordinateur que vous êtes autorisé à créer dans ce domaine. Contactez votre administrateur système pour que cette limite soit réinitialisée ou augmentée.

Résolution : Le compte de service spécifié dans le répertoire n'est pas autorisé à créer l'objet informatique ou à réutiliser un objet existant. Validez les autorisations et démarrez le WorkSpaces pool.

DOMAIN_JOIN_ERROR_INVALID_PARAMETER

Message : Un paramètre est incorrect. Cette erreur est renvoyée si le paramètre LpName est NULL ou si le paramètre NameType est spécifié en tant que NetSetupUnknown ou type de nom inconnu.

Résolution : l'erreur peut survenir lorsque le nom unique de l'UO (unité d'organisation) est incorrect. Validez l'unité d'organisation et réessayez. Si cette erreur persiste, contactez AWS Support. Pour plus d'informations, consultez le [Centre AWS Support](#).

DOMAIN_JOIN_ERROR_MORE_DATA

Message : D'autres données sont disponibles.

Résolution : l'erreur peut survenir lorsque le nom unique de l'UO (unité d'organisation) est incorrect. Validez l'unité d'organisation et réessayez. Si cette erreur persiste, contactez AWS Support. Pour plus d'informations, consultez le [Centre AWS Support](#).

DOMAIN_JOIN_ERROR_NO_SUCH_DOMAIN

Message : Le domaine spécifié n'existe pas ou n'a pas pu être contacté.

Résolution : L'instance de streaming n'a pas pu contacter votre domaine Active Directory. Pour garantir la connexion réseau, confirmez les paramètres de votre VPC, sous-réseau et groupe de sécurité.

DOMAIN_JOIN_NERR_WORKSTATION_NOT_STARTED

Message : Le service Station de travail n'a pas été mis en route.

Résolution : Une erreur s'est produite lors du démarrage du service de station de travail. Assurez-vous que le service est activé dans votre image. Si cette erreur persiste, contactez AWS Support. Pour plus d'informations, consultez le [Centre AWS Support](#).

DOMAIN_JOIN_ERROR_NOT_SUPPORTED

Message : La requête n'est pas prise en charge. Cette erreur est renvoyée si un ordinateur distant a été spécifié dans le paramètre `IpServer` et que cet appel n'est pas pris en charge sur l'ordinateur distant.

Résolution : contactez AWS Support pour obtenir de l'aide. Pour plus d'informations, consultez le [Centre AWS Support](#).

DOMAIN_JOIN_ERROR_FILE_NOT_FOUND

Message : Le fichier spécifié est introuvable.

Résolution : Cette erreur se produit lorsqu'un nom unique d'unité d'organisation non valide est fourni. Ce nom unique doit commencer par **OU=**. Vérifiez le nom unique de l'UO et réessayez.

DOMAIN_JOIN_INTERNAL_SERVICE_ERROR

Message : Le compte existe déjà.

Résolution : l'erreur peut se produire dans l'un des scénarios suivants :

- Si le problème n'est pas lié aux autorisations, vérifiez la présence d'erreurs dans les journaux Netdom et assurez-vous que vous avez fourni la bonne unité d'organisation.
- Le compte de service spécifié dans le répertoire n'est pas autorisé à créer l'objet informatique ou à réutiliser un objet existant. Si tel est le cas, validez les autorisations et démarrez le WorkSpaces pool.
- Après avoir WorkSpaces créé l'objet informatique, celui-ci est déplacé de l'unité d'organisation dans laquelle il a été créé. Dans ce cas, le premier WorkSpaces pool est créé avec succès, mais tout nouveau WorkSpaces pool utilisant l'objet ordinateur échoue. Lorsqu'Active Directory recherche l'objet ordinateur dans l'unité d'organisation spécifiée et détecte qu'un objet portant le même nom existe ailleurs dans le domaine, la liaison de domaines n'aboutit pas.
- Le nom de l'unité d'organisation spécifiée dans le WorkSpaces répertoire inclut des espaces situés avant ou après les virgules dans le répertoire. Dans ce cas, lorsqu'un WorkSpaces pool tente de rejoindre le domaine Active Directory, il WorkSpaces ne parvient pas à faire tourner correctement les objets de l'ordinateur et le regroupement du domaine échoue. Pour résoudre ce problème pour un WorkSpaces pool, procédez comme suit :
 1. Arrêtez la WorkSpaces piscine.
 2. Modifiez les paramètres de domaine Active Directory du WorkSpaces pool afin de supprimer le répertoire et l'unité d'organisation du répertoire auxquels le WorkSpaces pool est joint.
 3. Mettez à jour le WorkSpaces répertoire pour spécifier une unité d'organisation ne contenant pas d'espaces.
 4. Modifiez les paramètres de domaine Active Directory du WorkSpaces pool afin de spécifier le répertoire avec l'unité d'organisation Directory mise à jour.

Pour résoudre ce problème pour un WorkSpaces pool, procédez comme suit :

1. Supprimez le WorkSpaces pool.
2. Mettez à jour le WorkSpaces répertoire pour spécifier une unité d'organisation ne contenant pas d'espaces.

3. Créez un nouveau WorkSpaces pool et spécifiez le répertoire avec l'unité d'organisation de répertoire mise à jour.

WORKSPACES_POOL_SESSION_RESERVATION_ERROR

Message : Nous ne disposons actuellement pas d'une capacité suffisante pour les sessions demandées dans les zones de disponibilité [us-west-1] pour les sous-réseaux associés à votre pool. WorkSpaces Le système s'occupera d'allouer de la capacité supplémentaire. En attendant, modifiez ou associez un sous-réseau différent en utilisant l'un des éléments suivants AZs [us-west-2, us-west-3].

Solution : attendez que la capacité EC2 soit suffisante ou mettez à jour les sous-réseaux dans d'autres AZs sous-réseaux du répertoire.

INSUFFICIENT_CAPACITY_ERROR_WORKSPACES_POOL_AZ

Message : Nous n'avons actuellement pas de capacité suffisante pour les sessions demandées dans la zone de disponibilité (AZs) [<impacted az>]. Le système s'occupera d'allouer de la capacité supplémentaire. En attendant, veuillez modifier ou associer un autre sous-réseau en utilisant other AZs à votre WorkSpaces pool.

Solution : attendez qu'Amazon EC2 dispose d'une capacité suffisante ou mettez à jour les sous-réseaux dans d'autres sous-réseaux AZs de l'annuaire.

SOUS-NET_CIDR_BLOCK_INVALID_CUSTOMER_SUBNET_

Message : Votre sous-réseau inclut l'utilisation d'une plage d'adresses CIDR non disponible. Veuillez mettre à jour vos sous-réseaux en dehors de la plage /18 actuelle. ».

Solution : attendez que la capacité EC2 soit suffisante ou mettez à jour les sous-réseaux dans d'autres AZs sous-réseaux du répertoire.

Sécurité sur Amazon WorkSpaces

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de [AWS conformité Programmes](#) de de conformité. Pour en savoir plus sur les programmes de conformité applicables à Amazon WorkSpaces, consultez la section [AWS Services concernés par programme de conformitéAWS](#) .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation WorkSpaces. Les rubriques suivantes expliquent comment procéder à la configuration WorkSpaces pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos WorkSpaces ressources.

Rubriques

- [Protection des données sur Amazon WorkSpaces](#)
- [Gestion des identités et des accès pour WorkSpaces](#)
- [Validation de conformité pour Amazon WorkSpaces](#)
- [Résilience chez Amazon WorkSpaces](#)
- [Sécurité de l'infrastructure sur Amazon WorkSpaces](#)
- [Gestion des mises à jour dans WorkSpaces](#)

Protection des données sur Amazon WorkSpaces

Le [modèle de responsabilité AWS partagée](#) de s'applique à la protection des données sur Amazon WorkSpaces. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog [Modèle de responsabilité partagée AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec WorkSpaces ou d'autres Services

AWS utilisateurs de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Pour plus d'informations sur le WorkSpaces chiffrement des terminaux FIPS, consultez [Configurer l'autorisation FedRAMP ou la conformité au DoD SRG pour Personal WorkSpaces](#).

Chiffrement au repos

Vous pouvez chiffrer les volumes de stockage pour votre WorkSpaces utilisation de AWS KMS AWS Key Management Service Key from. Pour de plus amples informations, veuillez consulter [Chiffré WorkSpaces dans WorkSpaces Personal](#).

Lorsque vous créez WorkSpaces avec des volumes chiffrés, WorkSpaces utilise Amazon Elastic Block Store (Amazon EBS) pour créer et gérer ces volumes. EBS chiffre vos volumes avec une clé de données à l'aide de l'algorithme AES-256 standard. Pour plus d'informations, consultez [Amazon EBS Encryption](#) dans le guide de l' EC2 utilisateur Amazon.

Chiffrement en transit

Pour l' PCoIP, les données en transit sont cryptées à l'aide du cryptage TLS 1.2 et de la signature des demandes SigV4. Le protocole PCo IP utilise le trafic UDP crypté, avec cryptage AES, pour le streaming de pixels. La connexion de streaming, utilisant le port 4172 (TCP et UDP), est cryptée à l'aide des chiffrements AES-128 et AES-256, mais le cryptage par défaut est de 128 bits. Vous pouvez modifier cette valeur par défaut sur 256 bits, soit en utilisant le paramètre de stratégie de groupe Configurer les paramètres de sécurité PCo IP pour Windows WorkSpaces, soit en modifiant les paramètres de sécurité PCo IP dans le `pcoip-agent.conf` fichier pour Amazon Linux. WorkSpaces

Pour en savoir plus sur l'administration des politiques de groupe pour Amazon WorkSpaces, consultez [Configuration des paramètres de sécurité PCo IP Gérez votre Windows WorkSpaces dans WorkSpaces Personal](#). Pour en savoir plus sur la modification du `pcoip-agent.conf` fichier, consultez [Contrôlez le comportement de l'agent PCo IP sur Amazon Linux WorkSpaces](#) la section [Paramètres de sécurité PCo IP](#) dans la documentation de Teradici.

Pour le DCV, le streaming et les données de contrôle en transit sont chiffrés à l'aide du cryptage TLS 1.3 pour le trafic UDP et du cryptage TLS 1.2 pour le trafic TCP, avec des chiffrements AES-256.

Gestion des identités et des accès pour WorkSpaces

Par défaut, les utilisateurs IAM ne sont pas autorisés à accéder aux WorkSpaces ressources et aux opérations. Pour permettre aux utilisateurs IAM de gérer les WorkSpaces ressources, vous devez créer une stratégie IAM qui leur accorde explicitement des autorisations, et associer cette politique aux utilisateurs ou aux groupes IAM qui ont besoin de ces autorisations.

Note

Amazon WorkSpaces ne prend pas en charge le provisionnement d'informations d'identification IAM dans un WorkSpace (comme dans le cas d'un profil d'instance).

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Vous trouverez ci-dessous des ressources supplémentaires pour IAM :

- Pour plus d'informations sur les politiques IAM, consultez [Politiques et autorisations](#) dans le Guide de l'utilisateur IAM.
- Pour plus d'informations sur IAM, consultez [Gestion des identités et des accès \(IAM\)](#) et le [Guide de l'utilisateur IAM](#).

- Pour plus d'informations sur les ressources, les actions et les clés contextuelles de condition WorkSpaces spécifiques à utiliser dans les politiques d'autorisation IAM, consultez la section [Actions, ressources et clés de condition pour Amazon WorkSpaces](#) dans le guide de l'utilisateur IAM.
- Pour obtenir un outil qui vous aide à créer des politiques IAM, consultez le billet de blog [AWS Policy Generator](#). Vous pouvez également utiliser le [simulateur de politiques IAM](#) pour tester si une stratégie autorise ou refuse une demande spécifique à AWS.

Table des matières

- [Exemples de politiques](#)
- [Spécifier WorkSpaces les ressources dans une politique IAM](#)
- [Création du rôle workspaces_DefaultRole](#)
- [Création du rôle AmazonWorkSpaces PCAAccess de service](#)
- [AWS politiques gérées pour WorkSpaces](#)
- [Accès aux instances de streaming WorkSpaces et scripts y afférents](#)
- [Référence des autorisations relatives aux opérations sur Amazon WorkSpaces Console](#)

Exemples de politiques

Les exemples suivants présentent des déclarations de politique que vous pouvez utiliser pour contrôler les autorisations accordées aux utilisateurs d'IAM sur Amazon WorkSpaces.

Exemple 1 : accorder l'accès pour effectuer des tâches WorkSpaces personnelles et des tâches de groupe

La déclaration de politique suivante accorde à un utilisateur IAM l'autorisation d'effectuer des tâches WorkSpaces personnelles et des tâches de pool.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
"ds:*",
"workspaces:*",
"application-autoscaling:DeleteScalingPolicy",
"application-autoscaling:DeleteScheduledAction",
"application-autoscaling:DeregisterScalableTarget",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingActivities",
"application-autoscaling:DescribeScalingPolicies",
"application-autoscaling:DescribeScheduledActions",
"application-autoscaling:PutScalingPolicy",
"application-autoscaling:PutScheduledAction",
"application-autoscaling:RegisterScalableTarget",
"cloudwatch:DeleteAlarms",
"cloudwatch:DescribeAlarms",
"cloudwatch:PutMetricAlarm",
"ec2:AssociateRouteTable",
"ec2:AttachInternetGateway",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateInternetGateway",
"ec2:CreateNetworkInterface",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVpc",
"ec2>DeleteNetworkInterface",
"ec2>DeleteSecurityGroup",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeInternetGateways",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"iam:AttachRolePolicy",
"iam:CreatePolicy",
"iam:CreateRole",
"iam:GetRole",
"iam:ListRoles",
"iam:PutRolePolicy",
```



```

        "kms:ListAliases",
        "kms:ListKeys",
        "secretsmanager:ListSecrets",
        "tag:GetResources",
        "sso-directory:SearchUsers",
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationGrant",
        "sso:ListInstances",

        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant"
    ],
    "Resource": "*"
},
{
    "Sid": "iamPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "workspaces.amazonaws.com"
        }
    }
}
]
}

```

Exemple 2 : accorder l'accès pour effectuer des tâches WorkSpaces personnelles

La déclaration de politique suivante accorde à un utilisateur IAM l'autorisation d'effectuer toutes les tâches WorkSpaces personnelles.

Bien qu'Amazon WorkSpaces prenne totalement en charge les Resource éléments Action et lors de l'utilisation de l'API et des outils de ligne de commande, pour utiliser Amazon WorkSpaces depuis le AWS Management Console, un utilisateur IAM doit disposer des autorisations nécessaires pour les actions et ressources suivantes :

- Mesures : "ds:*
- Ressources : "Resource": "*"

L'exemple de politique suivant montre comment autoriser un utilisateur IAM à utiliser Amazon WorkSpaces depuis le AWS Management Console.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
```

```

        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "secretsmanager:ListSecrets",
        "sso-directory:SearchUsers",
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationGrant",
        "sso:ListInstances",

        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant"
    ],
    "Resource": "*"
},
{
    "Sid": "iamPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "workspaces.amazonaws.com"
        }
    }
}
]
}

```

Exemple 3 : accorder l'accès pour effectuer des tâches liées aux WorkSpaces pools

La déclaration de politique suivante accorde à un utilisateur IAM l'autorisation d'effectuer toutes les tâches du WorkSpaces pool.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreateRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PutRolePolicy",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
```

```

        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "workspaces.amazonaws.com"
            }
        },
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/aws-service-
role/workspaces.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_WorkSpacesPool",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "workspaces.application-
autoscaling.amazonaws.com"
                }
            }
        }
    ]
}

```

Exemple 4 : Exécuter toutes les WorkSpaces tâches pour le BYOL WorkSpaces

La déclaration de politique suivante accorde à un utilisateur IAM l'autorisation d'effectuer toutes les WorkSpaces tâches, y compris les tâches Amazon EC2 nécessaires à la création de la licence Bring Your Own License (BYOL). WorkSpaces

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",

```

```

        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyImageAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "iam:CreateRole",
        "iam:GetRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys"
    ],
    "Resource": "*"
},
{
    "Sid": "iamPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "workspaces.amazonaws.com"
        }
    }
}
}

```

```
]
}
```

Spécifier WorkSpaces les ressources dans une politique IAM

Pour spécifier une WorkSpaces ressource dans l'élément de la déclaration de politique, utilisez l'Amazon Resource Name (ARN) de la ressource. Vous contrôlez l'accès à vos WorkSpaces ressources en autorisant ou en refusant les autorisations d'utiliser les actions d'API spécifiées dans l'élément de votre déclaration de politique IAM. WorkSpaces définit ARNs des ensembles WorkSpaces, des groupes d'adresses IP et des annuaires.

Workspace ARN

La syntaxe d'un Workspace ARN est celle illustrée dans l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifieur
```

region

La région dans laquelle Workspace se trouve (par exemple, `us-east-1`).

account_id

L'identifiant du AWS compte, sans tiret (par exemple, `123456789012`).

identificateur_espace de travail

L'ID du Workspace (par exemple, `ws-a1bcd2efg`).

Voici le format de l'élément d'une déclaration de politique qui identifie un élément spécifique Workspace.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifieur"
```

Vous pouvez utiliser le `*` caractère générique pour spécifier tout WorkSpaces ce qui appartient à un compte spécifique dans une région spécifique.

Workspace pool ARN

Un ARN de Workspace pool possède la syntaxe illustrée dans l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifieur
```

region

La région dans laquelle WorkSpace se trouve (par exemple, us-east-1).

account_id

L'identifiant du AWS compte, sans tiret (par exemple, 123456789012).

espace de travail pool_identifieur

L'ID du WorkSpace pool (par exemple, ws-a1bcd2efg).

Voici le format de l'élément d'une déclaration de politique qui identifie un élément spécifique WorkSpace.

```
"Resource":  
  "arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifieur"
```

Vous pouvez utiliser le * caractère générique pour spécifier tout WorkSpaces ce qui appartient à un compte spécifique dans une région spécifique.

ARN du certificat

L'ARN d'un WorkSpace certificat possède la syntaxe illustrée dans l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspacecertificate/  
workspacecertificateidentifieur
```

region

La région dans laquelle WorkSpace se trouve (par exemple, us-east-1).

account_id

L'identifiant du AWS compte, sans tiret (par exemple, 123456789012).

identificateur de certificat d'espace de travail

L'ID du WorkSpace certificat (par exemple, ws-a1bcd2efg).

Le format de l'élément d'une déclaration de politique identifiant un WorkSpace certificat spécifique est le suivant.

```
"Resource":  
  "arn:aws:workspaces:region:account_id:workspacecertificate/  
workspacecertificate_identifieur"
```

Vous pouvez utiliser le * caractère générique pour spécifier tout WorkSpaces ce qui appartient à un compte spécifique dans une région spécifique.

ARN d'image

La syntaxe WorkSpace d'un ARN d'image est celle illustrée dans l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifieur
```

region

La région dans laquelle se trouve l' WorkSpace image (par exemple,us-east-1).

account_id

L'identifiant du AWS compte, sans tiret (par exemple,123456789012).

bundle_identifieur

L'ID de l' WorkSpace image (par exemple,ws-i-a1bcd2efg).

Voici le format de l'élément Resource d'une déclaration de politique qui identifie une image spécifique.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifieur"
```

Vous pouvez utiliser le caractère générique * pour spécifier toutes les images qui appartiennent à un compte spécifique dans une région donnée.

ARN de bundle

La syntaxe d'un ARN d'offre est celle de l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifieur
```

region

La région dans laquelle WorkSpace se trouve (par exemple,us-east-1).

account_id

L'identifiant du AWS compte, sans tiret (par exemple,123456789012).

bundle_identifieur

L'ID du WorkSpace bundle (par exemple,wsb-a1bcd2efg).

Voici le format de l'élément Resource d'une déclaration de stratégie qui identifie un bundle spécifique.

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifieur"
```

Vous pouvez utiliser le caractère générique * pour spécifier tous les bundles qui appartiennent à un compte spécifique dans une région donnée.

ARN de groupe d'IP

La syntaxe d'un ARN de groupe IP est celle de l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifieur
```

region

La région dans laquelle WorkSpace se trouve (par exemple,us-east-1).

account_id

L'identifiant du AWS compte, sans tiret (par exemple,123456789012).

ipgroup_identifieur

ID du groupe d'IP (par exemple, wsipg-a1bcd2efg).

Voici le format de l'élément Resource d'une déclaration de stratégie qui identifie un groupe d'IP spécifique.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifieur"
```

Vous pouvez utiliser le caractère générique * pour spécifier tous les groupes d'IP qui appartiennent à un compte spécifique dans une région donnée.

ARN d'annuaire

La syntaxe d'un ARN d'annuaire est celle de l'exemple suivant.

```
arn:aws:workspaces:region:account_id:directory/directory_identifieur
```

region

La région dans laquelle WorkSpace se trouve (par exemple, us-east-1).

account_id

L'identifiant du AWS compte, sans tiret (par exemple, 123456789012).

directory_identifieur

ID de l'annuaire (par exemple, d-12345a67b8).

Voici le format de l'élément Resource d'une déclaration de stratégie qui identifie un annuaire spécifique.

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifieur"
```

Vous pouvez utiliser le caractère générique * pour spécifier tous les annuaires qui appartiennent à un compte spécifique dans une région donnée.

ARN d'alias de connexion

La syntaxe d'un ARN d'alias de connexion est celle de l'exemple suivant.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifieur
```

region

Région dans laquelle se trouve l'alias de connexion (par exemple, us-east-1).

account_id

L'identifiant du AWS compte, sans tiret (par exemple, 123456789012).

connectionalias_identifieur

ID de l'alias de connexion (par exemple,wsca-12345a67b8).

Voici le format de l'élément Resource d'une déclaration de politique qui identifie un alias de connexion spécifique.

```
"Resource":  
  "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifieur"
```

Vous pouvez utiliser le caractère générique * pour spécifier tous les alias de connexion qui appartiennent à un compte spécifique dans une région donnée.

Actions d'API sans aucune prise en charge des autorisations au niveau des ressources

Vous ne pouvez pas spécifier un ARN de ressource avec les actions d'API suivantes :

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

Pour les actions d'API qui ne prennent pas en charge les autorisations au niveau des ressources, vous devez spécifier l'instruction de ressource indiquée dans l'exemple suivant.

```
"Resource": ""
```

Actions d'API qui ne prennent pas en charge les restrictions au niveau du compte sur les ressources partagées

Pour les actions d'API suivantes, vous ne pouvez pas spécifier d'ID de compte dans l'ARN de ressources qui n'appartiennent pas au compte :

- AssociateConnectionAlias
- CopyWorkspaceImage
- DisassociateConnectionAlias

Pour ces actions d'API, vous pouvez spécifier un ID de compte dans l'ARN uniquement lorsque ce compte possède les ressources sur lesquelles agir. Lorsque le compte ne possède pas les ressources, vous devez spécifier * pour l'ID du compte, comme l'illustre l'exemple suivant.

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

Création du rôle workspaces_ DefaultRole

Avant de pouvoir enregistrer un annuaire à l'aide de l'API, vous devez vérifier qu'il existe un rôle nommé workspaces_DefaultRole. Ce rôle est créé lors de la configuration rapide ou si vous lancez un Workspace en utilisant le AWS Management Console, et il WorkSpaces autorise Amazon à accéder à des AWS ressources spécifiques en votre nom. Si ce rôle n'existe pas, vous pouvez le créer à l'aide de la procédure suivante.

Pour créer le rôle workspaces_ DefaultRole

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le panneau de navigation de gauche, sélectionnez Roles (Rôles).
3. Sélectionnez Create role (Créer un rôle).
4. Sous Sélectionner un type d'entité de confiance, choisissez Autre compte AWS .
5. Pour Account ID (ID de compte), saisissez votre ID de compte sans tirets ni espaces.

6. Pour Options, ne spécifiez pas l'authentification multi-facteurs (MFA).
7. Sélectionnez Next: Permissions (Étape suivante : autorisations).
8. Sur la page Joindre les politiques d'autorisation, sélectionnez les politiques AWS gérées AmazonWorkSpacesServiceAccessAmazonWorkSpacesSelfServiceAccess, et AmazonWorkSpacesPoolServiceAccess. Pour plus d'informations sur ces politiques gérées, consultez [AWS politiques gérées pour WorkSpaces](#).
9. Sous Définir une limite d'autorisations, nous vous recommandons de ne pas utiliser de limite d'autorisations en raison du risque de conflits avec les stratégies attachées à ce rôle. De tels conflits pourraient bloquer certaines autorisations nécessaires pour le rôle.
10. Choisissez Suivant : Balises.
11. Dans la page Add tags (optional) (Ajouter des balises (facultatif)), ajoutez des balises si nécessaire.
12. Choisissez Suivant : Vérification.
13. Sur la page Vérification, pour Nom du rôle, saisissez **workspaces_DefaultRole**.
14. (Facultatif) Pour Role description (Description du rôle), entrez une description.
15. Choisissez Create Role (Créer un rôle).
16. Sur la page Résumé du DefaultRole rôle workspaces_, choisissez l'onglet Relations de confiance.
17. Dans l'onglet Trust relationships (Relations d'approbation), choisissez Edit trust relationship (Modifier la relation d'approbation).
18. Dans la page Edit Trust Relationship (Modifier la relation d'approbation) remplacez la déclaration de stratégie existante par la déclaration suivante.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. Choisissez Mettre à jour la politique d'approbation.

Création du rôle AmazonWorkSpaces PCAAccess de service

Avant que les utilisateurs puissent se connecter via l'authentification basée sur des certificats, vous devez vérifier qu'il existe un rôle nommé `AmazonWorkSpacesPCAAccess`. Ce rôle est créé lorsque vous activez l'authentification basée sur des certificats sur un annuaire à l'aide du AWS Management Console, et il accorde à Amazon WorkSpaces l'autorisation d'accéder aux AWS CA privée ressources en votre nom. Si ce rôle n'existe pas parce que vous n'utilisez pas la console pour gérer l'authentification basée sur des certificats, vous pouvez le créer à l'aide de la procédure suivante.

Pour créer le rôle de AmazonWorkSpaces PCAAccess service à l'aide du AWS CLI

1. Créez un fichier JSON nommé `AmazonWorkSpacesPCAAccess.json` avec le texte suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "prod.euc.ecm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Ajustez le `AmazonWorkSpacesPCAAccess.json` chemin selon vos besoins et exécutez les AWS CLI commandes suivantes pour créer le rôle de service et associer la politique [AmazonWorkspacesPCAAccess](#) gérée.

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file:///AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy --role-name AmazonWorkSpacesPCAAccess --policy-arn
arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

AWS politiques gérées pour WorkSpaces

L'utilisation de politiques AWS gérées permet d'ajouter des autorisations aux utilisateurs, aux groupes et aux rôles plus facilement que de rédiger vous-même des politiques. Il faut du temps et de l'expertise pour créer des [politiques gérées par le client IAM](#) qui ne fournissent aux équipes que les autorisations dont elles ont besoin. Utilisez des politiques AWS gérées pour démarrer rapidement. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les [politiques AWS gérées](#) dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services peuvent parfois ajouter des autorisations supplémentaires à une politique AWS gérée pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont plus susceptibles de mettre à jour une politique AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Quand un service lance une nouvelle fonctionnalité, AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page [politiques gérées par AWS pour les fonctions de tâche](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonWorkSpacesAdmin

Note

Les autorisations répertoriées concernent uniquement le SDK et ne fonctionneront pas pour la console. La console nécessite des autorisations supplémentaires répertoriées dans la [référence des autorisations relatives aux opérations de WorkSpaces la console Amazon](#).

Cette politique donne accès aux actions WorkSpaces administratives d'Amazon. Elle fournit les autorisations suivantes :

- `workspaces`- Permet d'accéder aux ressources WorkSpaces personnelles et aux ressources des WorkSpaces pools pour effectuer des actions administratives.
- `kms` : permet d'accéder à la liste et à la description des clés KMS, ainsi qu'à la liste des alias.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonWorkSpacesAdmin",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces>DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StartWorkspacesPool",

```

```

        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
    ],
    "Resource": "*"
}
]
}

```

AWS politique gérée : AmazonWorkspaces PCAAccess

Cette politique gérée permet d'accéder aux AWS ressources de l'autorité de certification privée (Private CA) de votre AWS compte pour une authentification basée sur des certificats. Il est inclus dans le AmazonWorkSpaces PCAAccess rôle et fournit les autorisations suivantes :

- acm-pca- Permet d'accéder à AWS une autorité de certification privée pour gérer l'authentification basée sur des certificats.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}

```

```
]
}
```

AWS politique gérée : AmazonWorkSpacesSelfServiceAccess

Cette politique donne accès au WorkSpaces service Amazon pour effectuer des actions en WorkSpaces libre-service initiées par un utilisateur. Elle est incluse dans le rôle `workspaces_DefaultRole` et fournit les autorisations suivantes :

- `workspaces-` Permet aux utilisateurs d'accéder aux fonctionnalités WorkSpaces de gestion en libre-service.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

AWS politique gérée : AmazonWorkSpacesServiceAccess

Cette politique permet au compte client d'accéder au WorkSpaces service Amazon pour le lancement d'un Workspace. Elle est incluse dans le rôle `workspaces_DefaultRole` et fournit les autorisations suivantes :

- `ec2-` Permet d'accéder à la gestion des ressources Amazon EC2 associées à un Workspace, telles que les interfaces réseau.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

AWS politique gérée : AmazonWorkSpacesPoolServiceAccess

Cette politique est utilisée dans le `workspaces_DefaultRole`, qui WorkSpaces permet d'accéder aux ressources requises dans le AWS compte client de Pools. WorkSpaces Pour de plus amples informations, veuillez consulter [Création du rôle `workspaces\_DefaultRole`](#). Elle fournit les autorisations suivantes :

- `ec2`- Permet de gérer les ressources Amazon EC2 associées à un WorkSpaces pool, telles que VPCs les sous-réseaux, les zones de disponibilité, les groupes de sécurité et les tables de routage.
- `s3`- Permet d'accéder aux compartiments Amazon S3 pour effectuer des actions requises pour les journaux, les paramètres de l'application et la fonctionnalité Home Folder.

Commercial Régions AWS

La politique JSON suivante s'applique à la publicité Régions AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

{
  "Sid": "ProvisioningWorkSpacesPoolPermissions",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeRouteTables",
    "s3:ListAllMyBuckets"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid": "WorkSpacesPoolS3Permissions",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:ListBucket",
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:GetObjectVersion",
    "s3:DeleteObjectVersion",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutEncryptionConfiguration"
  ],
  "Resource": [
    "arn:aws:s3:::wspool-logs-*",
    "arn:aws:s3:::wspool-app-settings-*",
    "arn:aws:s3:::wspool-home-folder-*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
}
}

```

```
    ]
  }
}
```

AWS GovCloud (US) Regions

La politique JSON suivante s'applique à la publicité AWS GovCloud (US) Regions.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ProvisioningWorkSpacesPoolPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "WorkSpacesPoolS3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",

```

```
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::wspool-logs-*",
        "arn:aws-us-gov:s3:::wspool-app-settings-*",
        "arn:aws-us-gov:s3:::wspool-home-folder-*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
}
}
```

WorkSpaces mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées WorkSpaces depuis que ce service a commencé à suivre ces modifications.

Modifier	Description	Date
the section called “AmazonWorkSpacesPoolServiceAccess” - Ajout d'une nouvelle politique	WorkSpaces a ajouté une nouvelle politique gérée pour autoriser l'accès à Amazon EC2 VPCs et aux ressources associées, ainsi que pour afficher et gérer les compartiments Amazon S3 pour les pools. WorkSpaces	24 juin 2024
the section called “AmazonWorkSpacesAdmin” – Mise à jour de politique	WorkSpaces a ajouté plusieurs actions pour les WorkSpaces pools à la politique WorkSpacesAdmin gérée par Amazon, accordant aux administrateurs l'accès à	24 juin 2024

Modifier	Description	Date
	la gestion des ressources du WorkSpace pool.	
the section called “AmazonWorkSpacesAdmin” – Mise à jour de politique	WorkSpaces a ajouté l'workspace :Restore Workspace action à la politique WorkSpacesAdmin gérée par Amazon, en accordant aux administrateurs l'accès à la restauration. WorkSpaces	25 juin 2023
the section called “AmazonWorkSpacesPCAAccess” - Ajout d'une nouvelle politique	WorkSpaces a ajouté une nouvelle politique gérée pour accorder l'acm-pcaautorisation de gérer une autorité de certification AWS privée afin de gérer l'authentification basée sur des certificats.	18 novembre 2022
WorkSpaces a commencé à suivre les modifications	WorkSpaces a commencé à suivre les modifications apportées WorkSpaces à ses politiques gérées.	1er mars 2021

Accès aux instances de streaming WorkSpaces et scripts y afférents

Les applications et les scripts qui s'exécutent sur des instances de WorkSpaces streaming doivent inclure des AWS informations d'identification dans leurs demandes AWS d'API. Vous pouvez créer un rôle IAM pour gérer ces informations d'identification. Un rôle IAM spécifie un ensemble d'autorisations que vous pouvez utiliser pour accéder aux AWS ressources. Toutefois, ce rôle n'est pas associé de façon unique à une seule personne. Au lieu de cela, il peut être assumé par toute personne en ayant besoin.

Vous pouvez appliquer un rôle IAM à une instance de WorkSpaces streaming. Lorsque l'instance de streaming bascule vers (assume) le rôle, le rôle fournit des informations d'identification de sécurité

temporaires. Votre application ou vos scripts utilisent ces informations d'identification pour effectuer des actions d'API et des tâches de gestion sur l'instance de streaming. WorkSpaces gère pour vous le changement d'identifiant temporaire.

Table des matières

- [Bonnes pratiques d'utilisation des rôles IAM avec des instances de WorkSpaces streaming](#)
- [Configuration d'un rôle IAM existant à utiliser avec des instances de WorkSpaces streaming](#)
- [Comment créer un rôle IAM à utiliser avec les instances de WorkSpaces streaming](#)
- [Comment utiliser le rôle IAM avec les instances de WorkSpaces streaming](#)

Bonnes pratiques d'utilisation des rôles IAM avec des instances de WorkSpaces streaming

Lorsque vous utilisez des rôles IAM avec des instances de WorkSpaces streaming, nous vous recommandons de suivre les pratiques suivantes :

- Limitez les autorisations que vous accordez aux actions et aux ressources de l'AWSAPI.

Respectez le principe du moindre privilège lorsque vous créez et associez des politiques IAM aux rôles IAM associés aux instances de WorkSpaces streaming. Lorsque vous utilisez une application ou un script qui nécessite l'accès aux actions ou aux ressources de l'AWSAPI, déterminez les actions et les ressources spécifiques requises. Ensuite, créez des politiques qui autorisent l'application ou le script à effectuer uniquement ces actions. Pour plus d'informations, consultez [Octroi du moindre privilège](#) dans le Guide de l'utilisateur IAM.

- Créez un rôle IAM pour chaque WorkSpaces ressource.

La création d'un rôle IAM unique pour chaque WorkSpaces ressource est une pratique qui respecte le principe du moindre privilège. Cela vous permet également de modifier les autorisations pour une ressource sans affecter les autres ressources.

- Limitez les endroits où les informations d'identification peuvent être utilisées.

Les politiques IAM vous permettent de définir les conditions dans lesquelles votre rôle IAM peut être utilisé pour accéder à une ressource. Par exemple, vous pouvez inclure des conditions pour spécifier une plage d'adresses IP d'où peuvent parvenir les requêtes. Cela permet d'éviter que les informations d'identification soient utilisées en dehors de votre environnement. Pour plus d'informations, consultez [Utiliser les conditions des stratégies pour une plus grande sécurité](#) dans le Guide de l'utilisateur IAM.

Configuration d'un rôle IAM existant à utiliser avec des instances de WorkSpaces streaming

Cette rubrique décrit comment configurer un rôle IAM existant afin de pouvoir l'utiliser avec WorkSpaces .

Conditions préalables

Le rôle IAM que vous souhaitez utiliser WorkSpaces doit répondre aux conditions préalables suivantes :

- Le rôle IAM doit figurer sur le même compte Amazon Web Services que l'instance de WorkSpaces streaming.
- Le rôle IAM ne peut pas être une fonction du service.
- La politique de relation de confiance attachée au rôle IAM doit inclure le WorkSpaces service en tant que principal. Un mandant est une entité AWS qui peut effectuer des actions et accéder à des ressources. La stratégie doit également inclure l'action `sts:AssumeRole`. Cette configuration de politique est définie WorkSpaces comme une entité de confiance.
- Si vous appliquez le rôle IAM à WorkSpaces, vous WorkSpaces devez exécuter une version de l' WorkSpaces agent publiée le 3 septembre 2019 ou après cette date. Si vous appliquez le rôle IAM à WorkSpaces, vous WorkSpaces devez utiliser une image utilisant une version de l'agent publiée à la même date ou après cette date.

Pour permettre au directeur du WorkSpaces service d'assumer un rôle IAM existant

Pour effectuer les étapes suivantes, vous devez vous connecter au compte en tant qu'utilisateur IAM disposant des autorisations requises pour répertorier et mettre à jour les rôles IAM. Si vous n'avez pas les autorisations requises, demandez à votre administrateur de compte Amazon Web Services d'effectuer ces étapes dans votre compte ou de vous accorder les autorisations requises.

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles.
3. Dans la liste des rôles de votre compte, choisissez le nom du rôle que vous souhaitez modifier.
4. Sélectionnez l'onglet Relations d'approbation, puis Modifier la relation d'approbation.
5. Sous Document de stratégie, vérifiez que la stratégie de relation d'approbation inclut l'action `sts:AssumeRole` pour le principal du service `workspaces.amazonaws.com` :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "workspaces.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Après avoir modifié votre politique d'approbation, choisissez Mettre à jour la politique de confiance pour enregistrer vos modifications.
7. Le rôle IAM que vous avez sélectionné s'affichera dans la WorkSpaces console. Ce rôle accorde des autorisations aux applications et aux scripts pour effectuer des actions d'API et des tâches de gestion sur les instances de streaming.

Comment créer un rôle IAM à utiliser avec les instances de WorkSpaces streaming

Cette rubrique explique comment créer un nouveau rôle IAM afin de pouvoir l'utiliser avec WorkSpaces

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.
3. Pour Select type of trusted entity (Sélectionner le type d'entité de confiance), choisissez Service AWS.
4. Dans la liste des AWS services, sélectionnez WorkSpaces.
5. Sous Sélectionnez votre cas d'utilisation, WorkSpaces l'option « WorkSpaces Autoriser les instances à appeler AWS des services en votre nom » est déjà sélectionnée. Choisissez Suivant : Autorisations.

6. Si possible, sélectionnez la politique à utiliser pour la politique d'autorisations ou choisissez Create policy (Créer une politique) pour ouvrir un nouvel onglet de navigateur et créer une nouvelle politique de bout en bout. Pour plus d'informations, consultez l'étape 4 de la procédure [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Une fois la politique créée, fermez cet onglet et revenez à l'onglet initial. Cochez la case à côté des politiques d'autorisation que vous WorkSpaces souhaitez avoir.
7. (Facultatif) Définissez une limite d'autorisations. Il s'agit d'une fonctionnalité avancée disponible pour les fonctions de service, mais pas pour les rôles liés à un service. Pour plus d'informations, consultez [Limites d'autorisations pour les entités IAM](#) dans le Guide de l'utilisateur IAM.
8. Choisissez Suivant : Balises. Vous pouvez éventuellement joindre des balises en tant que paires clé-valeur. Pour plus d'informations, consultez [Balisage des utilisateurs et des rôles IAM](#) dans le Guide de l'utilisateur IAM.
9. Choisissez Suivant : Vérification.
10. Pour Nom du rôle, saisissez un nom de rôle unique dans votre compte Amazon Web Services. Comme d'autres AWS ressources peuvent faire référence au rôle, vous ne pouvez pas modifier le nom du rôle une fois celui-ci créé.
11. Pour Description du rôle, conservez la description du rôle par défaut ou saisissez une nouvelle description.
12. Passez en revue les informations du rôle, puis choisissez Create role (Créer un rôle).

Comment utiliser le rôle IAM avec les instances de WorkSpaces streaming

Après avoir créé un rôle IAM, vous pouvez l'appliquer WorkSpaces lors du lancement WorkSpaces. Vous pouvez également appliquer un rôle IAM à un rôle existant WorkSpaces.

Lorsque vous appliquez un rôle IAM à WorkSpaces, WorkSpaces récupère les informations d'identification temporaires et crée le profil d'identification `workspaces_machine_role` sur l'instance. Les informations d'identification temporaires sont valides pendant 1 heure et de nouvelles informations d'identification sont récupérées toutes les heures. Les informations d'identification précédentes n'expirent pas. Vous pouvez donc les utiliser aussi longtemps qu'elles sont valides. Vous pouvez utiliser le profil d'identification pour appeler AWS des services par programmation à l'aide de l'interface de ligne de commande (AWSCLI) PowerShell, AWS des outils ou du AWS SDK dans la langue de votre choix.

Lorsque vous effectuez les appels d'API, spécifiez `workspaces_machine_role` comme profil d'identification. Sinon, l'opération échoue en raison d'autorisations insuffisantes.

WorkSpaces assume le rôle spécifié pendant le provisionnement de l'instance de streaming. Dans la WorkSpaces mesure où il utilise l'interface réseau élastique attachée à votre VPC pour les appels d'AWSAPI, votre application ou votre script doit attendre que l'Elastic network interface soit disponible avant de passer des appels d'AWSAPI. Si des appels d'API sont effectués avant que l'interface réseau Elastic soit disponible, les appels échouent.

Les exemples suivants montrent comment utiliser le profil d'identification `workspaces_machine_role` pour décrire les instances de streaming (EC2 instances) et pour créer le client Boto. Boto est le kit SDK Amazon Web Services (AWS) pour Python.

Décrire les instances de streaming (EC2 instances) à l'aide de la AWS CLI

```
aws ec2 describe-instances --region us-east-1 --profile workspaces_machine_role
```

Décrire les instances de streaming (EC2 instances) à l'aide d'AWSoutils pour PowerShell

Vous devez utiliser AWS Tools pour PowerShell la version 3.3.563.1 ou ultérieure, avec le SDK Amazon Web Services pour .NET version 3.3.103.22 ou ultérieure. Vous pouvez télécharger le programme d'installation de AWS Tools for Windows, qui inclut AWS Tools for PowerShell et le SDK Amazon Web Services pour .NET, depuis [AWSle site Web Tools PowerShell](#) for.

```
Get-EC2Instance -Region us-east-1 -ProfileName workspaces_machine_role
```

Création du client Boto à l'aide du AWS SDK pour Python

```
session = boto3.Session(profile_name=workspaces_machine_role')
```

Référence des autorisations relatives aux opérations sur Amazon WorkSpaces Console

Certains Amazon ne WorkSpaces APIs peuvent être appelés que via la console AWS de gestion. Ils ne sont pas publics APIs, dans le sens où ils ne peuvent pas être appelés par programmation, et ils ne sont fournis par aucun SDK. Ces opérations d'API incluent :

- espaces de travail : DirectoryAccessManagement
- espaces de travail : CreateRootClientCertificate
- espaces de travail : UpdateRootClientCertificate

- espaces de travail : DeleteRootClientCertificate
- espaces de travail : DescribeConsent
- espaces de travail : UpdateConsent

WorkSpaces Opérations de console et autorisations requises pour les actions

La console utilise des actions d'API supplémentaires pour ses fonctionnalités, de sorte que les autorisations accordées au WorkSpaces public APIs peuvent ne pas être suffisantes. Par exemple, un utilisateur autorisé à utiliser l'[CreateWorkspaces](#) API CLI/SDK peut rencontrer des erreurs lorsqu'il essaie d'en créer une WorkSpace sur la console, car il ne dispose pas de certaines autorisations pour sélectionner ou créer des utilisateurs. Ce tableau répertorie les fonctionnalités uniquement disponibles sur la WorkSpaces console et les autorisations supplémentaires requises pour permettre aux utilisateurs de travailler avec ces parties spécifiques de la console.

La section [Exemples de politiques](#) fournit la liste des autorisations permettant d'effectuer toutes les WorkSpaces tâches pour Personal, Pools et BYOL WorkSpaces.

Vous pouvez également utiliser des autorisations granulaires pour appliquer des autorisations de moindre privilège afin d'effectuer une tâche.

Ce tableau répertorie les fonctionnalités de la WorkSpaces console qui s'appuient sur APIs celles qui ne sont pas fournies par le SDK et les autorisations requises pour permettre aux utilisateurs de travailler avec ces parties spécifiques de la console. Ces autorisations doivent être ajoutées en plus des autres actions APIs requises par le SDK.

WorkSpaces Opérations sur console	Autorisations requises
WorkSpaces Configuration rapide personnalisée	espaces de travail : DirectoryAccessManagement Annonces : * EC2 : CreateVpc EC2 : CreateSubnet EC2 : CreateNetworkInterface EC2 : CreateInternetGateway

WorkSpaces Opérations sur console	Autorisations requises
	EC2 : CreateRouteTable
	EC2 : CreateRoute
	EC2 : CreateTags
	EC2 : CreateSecurityGroup
	EC2 : DescribeInternetGateways
	EC2 : DescribeSecurityGroups
	EC2 : DescribeRouteTables
	EC2 : DescribeVpcs
	EC2 : DescribeSubnets
	EC2 : DescribeNetworkInterfaces
	EC2 : DescribeAvailabilityZones
	EC2 : AttachInternetGateway
	EC2 : AssociateRouteTable
	EC2 : AuthorizeSecurityGroupIngress
	EC2 : AuthorizeSecurityGroupEgress
	iam : CreateRole
	iam : GetRole
	iam : PutRolePolicy
	espaces de travail : DescribeAccount
	espaces de travail : DescribeWorkspaceDirectories

WorkSpaces Opérations sur console	Autorisations requises
	espaces de travail : CreateWorkspaces espaces de travail : DescribeWorkspaces espaces de travail : RegisterWorkspaceDirectory espaces de travail : DescribeWorkspaceBundles espaces de travail : DescribeWorkspaces
Restreindre l'accès aux appareils sécurisés pour les WorkSpaces particuliers	espaces de travail : CreateRootClientCertificate espaces de travail : UpdateRootClientCertificate espaces de travail : DeleteRootClientCertificate annonces : DescribeDirectories EC2 : DescribeSubnets EC2 : DescribeSecurityGroups espaces de travail : DescribeAccount espaces de travail : DescribeWorkspaceDirectories espaces de travail : DescribeTags espaces de travail : DescribeClientProperties espaces de travail : DescribeConnectClientAddins espaces de travail : DirectoryAccessManagement

WorkSpaces Opérations sur console	Autorisations requises
Création d'un annuaire WorkSpace dans WorkSpaces Personal on the Console — To create/search/describe Directory Service	espaces de travail : DirectoryAccessManagement espaces de travail : DescribeAccount espaces de travail : CreateWorkspaces espaces de travail : DescribeWorkspaces espaces de travail : DescribeWorkspaceDirectories espaces de travail : DescribeWorkspaceBundles espaces de travail : DescribeTags espaces de travail : CreateTags espaces de travail : DescribeClientProperties km : ListKeys km : ListAliases km : DescribeKey annonces : DescribeTrusts annonces : DescribeDirectories EC2 : DescribeSubnets EC2 : DescribeSecurityGroups

WorkSpaces Opérations sur console	Autorisations requises
Gérer les utilisateurs dans WorkSpaces Personal : pour modifier les utilisateurs et leur envoyer un e-mail d'invitation	espaces de travail : DirectoryAccessManagement espaces de travail : DescribeAccount espaces de travail : DescribeWorkspaceDirectories espaces de travail : DescribeWorkspaces espaces de travail : DescribeTags espaces de travail : DescribeWorkspaceBundles espaces de travail : DescribeWorkspacesConnectionStatus espaces de travail : DescribeWorkspaceAssociations espaces de travail : DescribeWorkspaceSnapshots espaces de travail : DescribeWorkspaceImages espaces de travail : DescribeConnectionAliases

WorkSpaces Opérations sur console	Autorisations requises
Mettre à jour le compte AD Connector (AD Connector) pour WorkSpaces Personal	espaces de travail : DirectoryAccessManagement annonces : DescribeDirectories annonces : UpdateDirectory EC2 : DescribeSubnets EC2 : DescribeSecurityGroups espaces de travail : DescribeAccount espaces de travail : DescribeWorkspaceDirectories espaces de travail : DescribeTags espaces de travail : DescribeClientProperties espaces de travail : DescribeConnectClientAddins

WorkSpaces Opérations sur console	Autorisations requises
Sélectionnez une unité organisationnelle pour WorkSpaces Personnel	espaces de travail : DirectoryAccessManagement annonces : DescribeDirectories EC2 : DescribeSubnets EC2 : DescribeSecurityGroups espaces de travail : DescribeAccount espaces de travail : DescribeWorkspaceDirectories espaces de travail : DescribeTags espaces de travail : DescribeClientProperties espaces de travail : DescribeConnectClientAddins espaces de travail : ModifyWorkspaceCreationProperties
Activez votre compte pour BYOL — Pour confirmer que vous comprenez les conditions requises pour utiliser BYOL WorkSpaces	espaces de travail : DescribeConsent espaces de travail : UpdateConsent espaces de travail : DescribeAccount espaces de travail : ListAccountLinks espaces de travail : DescribeWorkspaceBundles espaces de travail : DescribeWorkspaceImages espaces de travail : DescribeWorkspaceDirectories

Validation de conformité pour Amazon WorkSpaces

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon dans WorkSpaces le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir [AWS Services concernés par programme de conformitéAWS](#) . Pour obtenir des renseignements généraux, consultez [Programmes de conformitéAWS](#) .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Pour plus d'informations sur FedRAMP WorkSpaces et FedRAMP, consultez. [Configurer l'autorisation FedRAMP ou la conformité au DoD SRG pour Personal WorkSpaces](#)

Votre responsabilité en matière de conformité lors de l'utilisation WorkSpaces est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Guides démarrage rapide de la sécurité et de la conformité](#). Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- [Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services](#) : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.
- AWS Ressources de <https://aws.amazon.com/compliance/resources/> de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [Évaluation des ressources à l'aide des règles](#) énoncées dans le guide du AWS Config développeur : AWS Config évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub CSPM](#) — Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience chez Amazon WorkSpaces

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section [Infrastructure AWS mondiale](#).

Amazon propose WorkSpaces également la redirection entre régions, une fonctionnalité qui fonctionne avec les politiques de routage par basculement de votre système de noms de domaine (DNS) pour rediriger vos WorkSpaces utilisateurs vers une alternative WorkSpaces dans une autre AWS région lorsque leur principal n'est WorkSpaces pas disponible. Pour de plus amples informations, veuillez consulter [Redirection entre régions pour Personal WorkSpaces](#).

Sécurité de l'infrastructure sur Amazon WorkSpaces

En tant que service géré, Amazon WorkSpaces est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder WorkSpaces via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Rubriques

- [Isolement de réseau](#)

- [Isolation sur les hôtes physiques](#)
- [Credential Guard/Sécurité basée sur la virtualisation \(VBS\)](#)
- [Autorisation des utilisateurs professionnels](#)
- [Création et diffusion à partir de points de terminaison VPC d'interface](#)
- [Effectuer des demandes d' WorkSpaces API Amazon via un point de terminaison d'interface VPC](#)
- [Création d'une politique de point de terminaison VPC pour Amazon WorkSpaces](#)
- [Connexion de votre réseau privé à votre VPC](#)

Isolement de réseau

Un cloud privé virtuel (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée dans le cloud. AWS Vous pouvez le déployer WorkSpaces dans un sous-réseau privé de votre VPC. Pour de plus amples informations, veuillez consulter [Configuration d'un VPC pour le personnel WorkSpaces](#).

Pour autoriser le trafic uniquement à partir de plages d'adresses spécifiques (par exemple, à partir de votre réseau d'entreprise), mettez à jour le groupe de sécurité de votre VPC ou utilisez un [groupe de contrôle d'accès IP](#).

Vous pouvez restreindre WorkSpace l'accès aux appareils fiables dotés de certificats valides. Pour de plus amples informations, veuillez consulter [Restreindre l'accès aux appareils fiables pour les WorkSpaces particuliers](#).

Isolation sur les hôtes physiques

Les différents hôtes WorkSpaces d'un même hôte physique sont isolés les uns des autres par l'intermédiaire de l'hyperviseur. C'est comme si elles se trouvaient sur des hôtes physiques distincts. Lorsque a WorkSpace est supprimé, la mémoire qui lui est allouée est nettoyée (mise à zéro) par l'hyperviseur avant d'être allouée à un nouveau. WorkSpace

Credential Guard/Sécurité basée sur la virtualisation (VBS)

Windows WorkSpaces peut utiliser Credential Guard et la sécurité basée sur la virtualisation (VBS) pour fournir une isolation matérielle et protéger les informations d'identification au sein du système d'exploitation. Vous pouvez désactiver Credential Guard ou VBS via les paramètres de stratégie de groupe.

 Important

La désactivation de VBS réduit le niveau de sécurité de votre Windows. WorkSpace Désactivez VBS uniquement si cela est nécessaire pour des besoins de performance ou de compatibilité spécifiques.

Implications de sécurité liées à la désactivation de VBS

- Protection réduite au niveau du noyau — Le noyau du système d'exploitation devient plus vulnérable aux codes malveillants.
- Risque accru de vol d'informations d'identification : les attaquants peuvent extraire plus facilement les informations d'identification du processus lsass.exe.
- Contrôles d'intégrité du code désactivés — L'intégrité du code appliquée par l'hyperviseur (HVCI) ne fonctionnera pas, ce qui permettra aux pilotes non signés de s'exécuter en mode noyau.
- Vulnérabilité accrue aux exploits — Le système devient plus vulnérable aux attaques susceptibles de compromettre l'intégrité du système.
- Perte de fonctionnalités de sécurité avancées — Les fonctionnalités telles que Windows Defender Credential Guard et System Guard ne peuvent pas fonctionner comme prévu.

Autorisation des utilisateurs professionnels

Avec WorkSpaces, les annuaires sont gérés via le Directory Service. Vous pouvez créer un annuaire autonome géré pour les utilisateurs. Vous pouvez également intégrer directement votre environnement Active Directory de manière à ce que vos utilisateurs puissent utiliser leurs informations d'identification existantes pour accéder en toute transparence aux ressources de l'entreprise. Pour de plus amples informations, veuillez consulter [Gérer les annuaires pour WorkSpaces Personal](#).

Pour mieux contrôler l'accès à votre compte WorkSpaces, utilisez l'authentification multifactorielle. Pour plus d'informations, consultez [Comment activer l'authentification multifactorielle pour les AWS services](#).

Création et diffusion à partir de points de terminaison VPC d'interface

Un cloud privé virtuel (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée du cloud Amazon Web Services. Si vous utilisez Amazon Virtual Private Cloud pour héberger vos AWS

ressources, vous pouvez établir une connexion privée entre votre VPC et WorkSpaces. Vous pouvez utiliser cette connexion pour WorkSpaces communiquer avec vos ressources sur votre VPC sans passer par l'Internet public.

Les points de terminaison de l'interface sont alimentés par AWS PrivateLink, une technologie qui vous permet de continuer à diffuser le trafic au sein d'un VPC que vous spécifiez à l'aide d'adresses IP privées. Lorsque vous utilisez le VPC avec un tunnel Direct AWS Connect ou AWS Virtual Private Network, vous pouvez conserver le trafic de streaming au sein de votre réseau.

Vous pouvez utiliser un point de terminaison VPC dans votre AWS compte pour restreindre tout le trafic de streaming entre votre Amazon VPC et WorkSpaces le réseau. AWS. Après avoir créé le point de terminaison, configurez votre WorkSpaces répertoire pour l'utiliser.

Conditions préalables et limitations

Avant de configurer des points de terminaison VPC pour WorkSpaces, tenez compte des conditions préalables et des limites suivantes.

- La fonctionnalité prend actuellement en charge IPv4 le type d'IP d'enregistrement IPv6 DNS. Le type d'IP d'enregistrement DNS Dualstack n'est pas pris en charge.
- Vous ne pouvez configurer que les points de terminaison VPC qui se trouvent dans le Compte AWS même répertoire. Les points de terminaison VPC situés dans d'autres régions ne Comptes AWS sont pas pris en charge, y compris les points de terminaison partagés. VPCs
- La fonctionnalité ne prend actuellement en charge que le nom DNS privé pour les points de terminaison VPC. Le nom DNS privé d'un point de terminaison VPC ne peut pas être résolu publiquement.
- La fonctionnalité n'est actuellement disponible que pour les utilisateurs WorkSpaces personnels. WorkSpaces Les pools ne prennent pas en charge les points de terminaison VPC pour le streaming.
- La fonctionnalité de point de terminaison VPC est disponible exclusivement pour l'utilisation d' WorkSpaces Amazon DCV. Lorsque vous configurez un point de terminaison VPC pour un annuaire, les utilisateurs ne peuvent pas diffuser depuis Amazon DCV sur Internet. Cependant, vous pouvez activer le streaming Internet pour PCo IP WorkSpaces dans le même répertoire lors de la configuration du point de terminaison VPC.
- Pour maintenir le trafic de streaming au sein de votre VPC, utilisez un point de terminaison VPC de streaming. Vos WorkSpaces clients ont besoin d'une connexion Internet pour s'authentifier. Activez l'accès sortant sur le port 443 (UDP et TCP) pour le trafic d'authentification. En outre,

vous devez ajouter les domaines et adresses IP requis à votre liste d'autorisation en fonction de la méthode d'authentification que vous avez choisie. Pour obtenir la liste complète des domaines pour chaque catégorie, reportez-vous à la section [Domaines et adresses IP à ajouter à votre liste d'autorisations](#).

- CAPTCHA
- Paramètres d'annuaire
- Points de terminaison d'authentification par carte à puce de présession, si vous utilisez une carte à puce
- Pages de connexion utilisateur
- Agent WS
- WorkSpaces Points de terminaison pour l'authentification unique (SSO) SAML
- Le réseau sur lequel les appareils de vos utilisateurs sont connectés doit être en mesure d'acheminer le trafic vers le point de terminaison VPC.
- Vous devez disposer d'une politique d'autorisation IAM pour l'utilisateur IAM ou le rôle IAM de votre AWS compte pour effectuer l'opération `ec2:DescribeVpcEndpoints` d'API.
- WorkSpaces les points de terminaison VPC de streaming ne prennent actuellement pas en charge le chiffrement FIPS. Si vous avez déjà activé le chiffrement FIPS pour un annuaire, vous devez désactiver le chiffrement FIPS avant de configurer un point de terminaison VPC.
- AWSL'intégration de Global Accelerator (AGA) n'est pas disponible lors du streaming via un point de terminaison VPC.
- Lorsqu'un point de terminaison VPC est configuré pour un annuaire, les groupes de contrôle d'accès IP spécifiés pour l'annuaire ne s'appliquent plus.

Configuration du point de terminaison VPC pour le streaming WorkSpaces

Pour configurer un point de terminaison VPC pour le WorkSpaces streaming, procédez comme suit :

Étape 1 : Créer le groupe de sécurité

Au cours de cette étape, vous créez un groupe de sécurité qui permet aux WorkSpaces clients de communiquer avec le point de terminaison VPC que vous allez créer.

1. Dans le volet de navigation de la EC2 console Amazon, accédez à Réseau et sécurité, puis à Groupes de sécurité.
2. Sélectionnez Créer un groupe de sécurité.

3. Dans Détails de base, entrez les informations suivantes :
 - Pour le nom du groupe de sécurité : entrez un nom unique identifiant le groupe de sécurité.
 - Pour la description — Entrez du texte décrivant l'objectif du groupe de sécurité.
 - Pour le VPC : choisissez le VPC dans lequel se trouve le point de terminaison de votre VPC.
4. Accédez à Règles entrantes et sélectionnez Ajouter une règle pour créer des règles entrantes pour le trafic TCP.
5. Saisissez :
 - Pour le type — Choisissez le protocole TCP personnalisé.
 - Pour la plage de ports : entrez les numéros de port suivants : 443, 4195.
 - Pour le type de source, choisissez Personnalisé.
 - Pour la source : entrez la plage d'adresses IP CIDR privées ou l'autre groupe IDs de sécurité à partir duquel vos utilisateurs se connectent au point de terminaison VPC. Assurez-vous d'autoriser le trafic entrant en provenance d'une source d'IPv6 adresse IPv4 ou.
6. Répétez les étapes 4 et 5 pour chaque plage d'adresses CIDR ou groupe de sécurité.
7. Accédez à Règles entrantes, sélectionnez Ajouter une règle pour créer des règles entrantes pour le trafic UDP.
8. Saisissez :
 - Pour le type — Choisissez UDP personnalisé.
 - Pour la plage de ports : entrez les numéros de port suivants : 443, 4195.
 - Pour le type de source, choisissez Personnalisé.
 - Pour la source : entrez la même plage d'adresses IP CIDR privée ou le même groupe de sécurité que celui IDs saisi à l'étape 5. Assurez-vous d'autoriser le trafic entrant en provenance d'une source d'IPv6 adresse IPv4 ou.
9. Répétez les étapes 7 et 8 pour chaque plage d'adresses CIDR ou groupe de sécurité.
10. Sélectionnez Créer un groupe de sécurité.

Étape 2 : Créer le point de terminaison de VPC

Dans Amazon VPC, un point de terminaison VPC vous permet de connecter votre VPC aux services pris en charge. AWS Dans cet exemple, vous configurez Amazon VPC de manière à ce que vos WorkSpaces utilisateurs puissent streamer depuis. WorkSpaces

1. Ouvrez la [console VPC Amazon](#).
2. Dans le volet de navigation, accédez à Endpoints, puis à Create Endpoint.
3. Sélectionnez Create Endpoint (Créer un point de terminaison).
4. Vérifiez les points suivants :
 - Catégorie de service — Assurez-vous que les AWSservices sont sélectionnés.
 - Nom du service — Choisissez com.amazonaws. **Region**.highlander.
 - VPC — Choisissez un VPC dans lequel créer le point de terminaison de l'interface. Vous pouvez choisir un VPC différent du VPC doté de WorkSpaces ressources, à condition que le réseau achemine le trafic vers le point de terminaison du VPC.
 - Activer le nom DNS privé : la case est cochée. Si vos utilisateurs utilisent un proxy réseau pour accéder aux instances de streaming, désactivez toute mise en cache de proxy sur le domaine et les noms de DNS associés au point de terminaison privé. Le nom DNS du point de terminaison VPC doit être autorisé via le proxy. Pour une résolution de nom DNS réussie, il est essentiel d'utiliser les serveurs DNS privés au sein du VPC, car les serveurs DNS publics ne résoudront pas le nom DNS du point de terminaison du VPC.
 - Type IP d'enregistrement DNS — Choisissez IPv4 ou IPv6. Le type d'IP d'enregistrement DNS Dualstack n'est actuellement pas pris en charge. Si vous choisissez Dualstack, vous ne pourrez pas WorkSpaces diffuser depuis le point de terminaison VPC.
 - Sous-réseaux : choisissez les sous-réseaux (zones de disponibilité) pour créer le point de terminaison VPC. Il est recommandé de choisir au moins deux sous-réseaux.
 - Type d'adresse IP — Choisissez IPv4 IPv6 ou Dualstack en fonction de ce que les sous-réseaux que vous avez choisis prennent en charge.
 - Panneau des groupes de sécurité : sélectionnez le groupe de sécurité que vous avez créé précédemment.
5. (Facultatif) Dans le volet Balises, vous pouvez créer une ou plusieurs balises.
6. Sélectionnez Créer un point de terminaison.

Lorsque le point de terminaison est prêt à être utilisé, la valeur de la colonne Status (Statut) devient Available (Disponible).

Étape 3 : configurer le WorkSpaces répertoire pour utiliser le point de terminaison VPC

Vous devez configurer le WorkSpaces répertoire pour utiliser le point de terminaison VPC que vous avez créé pour le streaming.

1. Ouvrez la [WorkSpaces console](#) dans la même AWS région que le point de terminaison VPC.
2. Dans le volet de navigation, sélectionnez Répertoires, puis.
3. Sélectionnez le répertoire que vous souhaitez utiliser.
4. Accédez à la section Points de terminaison VPC, puis sur Modifier.
5. Dans la boîte de dialogue Modifier le point de terminaison VPC, sous Point de terminaison de streaming, sélectionnez le point de terminaison VPC que vous avez créé.
6. Vous pouvez éventuellement activer Autoriser les utilisateurs disposant d'une PCo adresse IP WorkSpaces à diffuser depuis Internet.

 Note

Lorsque cette option est activée, vos utilisateurs peuvent diffuser depuis leur PCo adresse IP WorkSpaces via Internet public. Sinon, l' PCo adresse IP WorkSpaces du répertoire deviendra inaccessible car l'adresse PCo IP WorkSpaces ne prend pas en charge le point de terminaison VPC pour le streaming.

7. Cliquez sur Enregistrer.

Le trafic des nouvelles sessions de streaming sera acheminé via ce point de terminaison VPC. Toutefois, le trafic des sessions de streaming actuelles continue d'être acheminé via le point de terminaison spécifié précédemment.

 Note

Les utilisateurs dotés d'un DCV WorkSpaces ne peuvent pas diffuser via Internet public lorsqu'un point de terminaison VPC est spécifié.

Effectuer des demandes d' WorkSpaces API Amazon via un point de terminaison d'interface VPC

Vous pouvez vous connecter directement aux points de terminaison d' WorkSpaces API Amazon via un point de [terminaison d'interface](#) dans votre cloud privé virtuel (VPC) au lieu de vous connecter via Internet. Lorsque vous utilisez un point de terminaison d'interface VPC, la communication entre votre VPC et le point de terminaison de l' WorkSpaces API Amazon s'effectue de manière entièrement et sécurisée au sein du réseau. AWS

Note

Cette fonctionnalité ne peut être utilisée que pour la connexion aux points de terminaison de WorkSpaces l'API. Pour se connecter à WorkSpaces l'utilisation WorkSpaces des clients, une connexion Internet est requise, comme décrit dans [Exigences relatives à l'adresse IP et au port pour WorkSpaces Personal](#).

Les points de terminaison de WorkSpaces l'API [Amazon prennent en charge les points de terminaison de l'interface Amazon Virtual Private Cloud](#) (Amazon VPC) alimentés par. [AWS PrivateLink](#) Chaque point de terminaison VPC est représenté par une ou plusieurs [interfaces réseau](#) (également appelées interfaces réseau élastiques, ou ENIs) avec des adresses IP privées dans vos sous-réseaux VPC.

Le point de terminaison de l'interface VPC connecte votre VPC directement au point de terminaison de WorkSpaces l'API Amazon sans passerelle Internet, appareil NAT, connexion VPN ou connexion. Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec le point de terminaison de WorkSpaces l'API Amazon.

Vous pouvez créer un point de terminaison d'interface pour vous connecter WorkSpaces à Amazon à l'aide des commandes AWS Management Console or AWS Command Line Interface (AWS CLI). Pour obtenir des instructions, consultez [Création d'un point de terminaison d'interface](#).

Après avoir créé un point de terminaison VPC, vous pouvez utiliser les exemples de commandes CLI suivants qui utilisent le `endpoint-url` paramètre pour spécifier les points de terminaison d'interface pour le point de terminaison de l'API Amazon WorkSpaces :

```
aws workspaces copy-workspace-image --endpoint-  
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  
  
aws workspaces delete-workspace-image --endpoint-  
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com  
  
aws workspaces describe-workspace-bundles --endpoint-  
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com \  
--endpoint-name Endpoint_Name \  
--body "Endpoint_Body" \  
--content-type "Content_Type" \  
Output_File
```

Si vous activez des noms d'hôte DNS privés pour votre point de terminaison de VPC, il n'est pas nécessaire d'indiquer l'URL du point de terminaison. Le nom d'hôte DNS de l' API WorkSpaces Amazon que la CLI et le WorkSpaces SDK Amazon utilisent par défaut (<https://api.workspaces.Region.amazonaws.com>) correspond à votre point de terminaison VPC.

[Le point de terminaison de WorkSpaces l'API Amazon prend en charge les points de terminaison VPC dans toutes les AWS régions où Amazon VPC et Amazon sont disponibles.](#) WorkSpaces Amazon WorkSpaces permet de passer des appels à l'ensemble de son [public au APIs](#) sein de votre VPC.

Pour en savoir plus AWS PrivateLink, consultez la [AWS PrivateLink documentation](#). Pour connaître le prix des points de terminaison VPC, veuillez consulter [Tarification VPC](#). Pour en savoir plus sur les VPC et les points de terminaison, consultez [Amazon VPC](#).

Pour consulter la liste des points de terminaison d' WorkSpaces API Amazon par région, consultez la section Points de [terminaison WorkSpaces d'API](#).

Création d'une politique de point de terminaison VPC pour Amazon WorkSpaces

Vous pouvez créer une politique pour les points de terminaison Amazon VPC pour qu'Amazon spécifie WorkSpaces les éléments suivants :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, veuillez consulter [Contrôle de l'accès aux services avec des points de terminaison d'un VPC](#) dans le Amazon VPC Guide de l'utilisateur.

Note

Les politiques relatives aux points de terminaison VPC ne sont pas prises en charge pour les points de terminaison Amazon Federal Information Processing Standard (FIPS). WorkSpaces

L'exemple de politique de point de terminaison VPC suivant indique que tous les utilisateurs ayant accès au point de terminaison de l'interface VPC sont autorisés à appeler le point de terminaison hébergé par Amazon WorkSpaces nommé. ws-f9abcdefg

```
{
  "Statement": [
    {
      "Action": "workspaces:*",
      "Effect": "Allow",
      "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-f9abcdefg",
      "Principal": "*"
    }
  ]
}
```

Dans cet exemple, les actions suivantes sont refusées :

- Invoquer des points de terminaison WorkSpaces hébergés par Amazon autres que. ws-f9abcdefg
- Exécution d'une action sur une ressource autre que celle spécifiée (WorkSpace ID :ws-f9abcdefg).

Note

Dans cet exemple, les utilisateurs peuvent toujours effectuer d'autres actions d' WorkSpaces API Amazon en dehors du VPC. Pour limiter les appels d'API à ceux provenant du VPC, consultez les informations relatives à l'utilisation de politiques basées sur l'identité [Gestion des identités et des accès pour WorkSpaces](#) pour contrôler l'accès aux points de terminaison des API Amazon. WorkSpaces

Connexion de votre réseau privé à votre VPC

Pour appeler l' WorkSpaces API Amazon via votre VPC, vous devez vous connecter depuis une instance située à l'intérieur du VPC ou connecter votre réseau privé à votre VPC en utilisant () ou. AWS Virtual Private Network Site-to-Site VPN Direct Connect Pour plus d'informations consultez

[Connexions VPN](#) dans le Guide de l'utilisateur Amazon Virtual Private Cloud. Pour plus d'informations AWS Direct Connect, voir [Création d'une connexion](#) dans le guide de Direct Connect l'utilisateur.

Gestion des mises à jour dans WorkSpaces

Nous vous recommandons de corriger, de mettre à jour et de sécuriser régulièrement le système d'exploitation et les applications de votre WorkSpaces. Vous pouvez les configurer WorkSpaces pour qu'ils soient mis à jour WorkSpaces pendant une période de maintenance régulière ou vous pouvez les mettre à jour vous-même. Pour de plus amples informations, veuillez consulter [Entretien WorkSpaces personnel](#).

Pour les applications installées sur votre WorkSpaces ordinateur, vous pouvez utiliser tous les services de mise à jour automatique fournis ou suivre les recommandations d'installation des mises à jour fournies par le fournisseur de l'application.

WorkSpaces Quotas Amazon

Amazon WorkSpaces fournit différentes ressources que vous pouvez utiliser dans votre compte dans une région donnée, notamment des images WorkSpaces, des ensembles, des répertoires, des alias de connexion et des groupes de contrôle IP. Lorsque vous créez votre compte Amazon Web Services, nous définissons des quotas par défaut (également appelés limites) sur le nombre de ressources que vous pouvez créer.

Les quotas par défaut WorkSpaces pour votre AWS compte sont les suivants. Vous pouvez utiliser la [console Service Quotas](#) pour afficher les quotas par défaut et [demander des augmentations](#) pour les quotas ajustables.

Dans certaines régions où les Service Quotas ne sont pas disponibles, vous devez soumettre un cas de support pour demander une augmentation de la limite. Pour plus d'informations, consultez [Affichage des quotas de service](#) et [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur Service Quotas.

Ressource	Par défaut	Description	Ajustable	Usage
WorkSpaces	1	Le nombre maximum de personnes WorkSpaces présentes sur ce compte dans la région actuelle.	Oui	Oui
Graphismes WorkSpaces	0	Le nombre maximum de graphiques WorkSpace s dans ce compte dans la région actuelle. Remarque : le bundle Graphics n'est plus pris	Oui	Non pris en charge

Ressource	Par défaut	Description	Ajustable	Usage
		en charge depuis le 30 novembre 2023 et le GraphicsPro bundle arrive à expiration le 31 end-of-life octobre 2025. Nous vous recommandons de migrer votre offre groupée WorkSpaces vers un bundle compatible avec le GPU. Pour de plus amples informations, veuillez consulter Migrer un Workspace dans WorkSpaces Personal.		
GeneralPurpose4 x large WorkSpaces	1	Le nombre maximum de GeneralPurpose 0,4 x large WorkSpaces sur ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
GeneralPu rpose8 x large WorkSpaces	1	Le nombre maximum de GeneralPu rpose 0,8xlarge WorkSpaces sur ce compte dans la région actuelle.	Oui	Oui
Graphics. g6.xlarge WorkSpaces	0	Le nombre maximum de Graphics. G6.xLarge dans ce compte dans la région actuelle.	Oui	Oui
Carte graphique . G6.2 x Large WorkSpaces	0	Le nombre maximum de Graphics. G6.2xLarge dans ce compte dans la région actuelle.	Oui	Oui
Carte graphique . G 6,4 x large WorkSpaces	0	Le nombre maximum de Graphics. G6.4XLarge dans ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Carte graphique . G 6,8 x large WorkSpaces	0	Le nombre maximum de Graphics. G6.8xLarge dans ce compte dans la région actuelle.	Oui	Oui
Carte graphique G6.16 x Large WorkSpaces	0	Le nombre maximum de Graphics. G6.16XLarge dans ce compte dans la région actuelle.	Oui	Oui
Graphics.gr 6,4 x large WorkSpaces	0	Le nombre maximum de Graphics. gr6.4XLarge dans ce compte dans la région actuelle.	Oui	Oui
Graphics.gr 6,8 x large WorkSpaces	0	Le nombre maximum de Graphics. gr6.8xLarge dans ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Graphisme .G6F.Large WorkSpaces	0	Le nombre maximum de Graphics. G6F.Large dans ce compte dans la région actuelle.	Oui	Oui
Graphics. g6f.xlarge WorkSpaces	0	Le nombre maximum de Graphics. G6F.xlarge dans ce compte dans la région actuelle.	Oui	Oui
Carte graphique . G6F, 2 x Large WorkSpaces	0	Le nombre maximum de Graphics. G6F.2XLarge dans ce compte dans la région actuelle.	Oui	Oui
Carte graphique . G6F, 4 x large WorkSpaces	0	Le nombre maximum de Graphics. G6F.4XLarge dans ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Graphisme .GR6F.4XLarge WorkSpaces	0	Le nombre maximum de Graphics.GR6F.4XLarge dans ce compte dans la région actuelle.	Oui	Oui
Carte graphique .G4DN WorkSpaces	0	Le nombre maximum de Graphics.G4DN WorkSpaces dans ce compte dans la région actuelle.	Oui	Oui
GraphicsPro.g4dn WorkSpaces	0	Le nombre maximum de GraphicsPro.g4dn WorkSpaces dans ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
GraphicsPro WorkSpaces	0	Le nombre maximum de personnes GraphicsPro WorkSpaces présentes sur ce compte dans la région actuelle. (GraphicsPro le forfait arrive end-of-life le 31 octobre 2025. Envisagez d'utiliser d'autres offres compatibles en remplacement.)	Oui	Oui
Veille WorkSpaces	5	Le nombre maximum de personnes WorkSpaces présentes sur ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Bundles	50	Nombre maximal de bundles pour ce compte dans la région actuelle. Ce quota s'applique uniquement aux bundles personnalisés, et non aux bundles publics.	Non	Oui
Alias de connexion	20	Nombre maximal d'alias de connexion pour ce compte dans la région actuelle.	Non	Oui
Annuaire	50	Le nombre maximum d'annuaires qui peuvent être enregistrés pour être utilisés auprès d'Amazon sur WorkSpaces ce compte dans la région actuelle.	Non	Oui
Images	40	Nombre maximal d'images pour ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Groupes de contrôles d'accès IP	140	Nombre maximal de contrôles d'accès IP pour ce compte dans la région actuelle.	Non	Oui
Groupes de contrôle d'accès IP par annuaire	35	Nombre maximal de groupes de contrôle d'accès IP par annuaire pour ce compte dans la région actuelle.	Non	Non pris en charge
Règles par groupe de contrôle d'accès IP	30	Nombre maximal de règles par groupe de contrôle d'accès IP pour ce compte dans la région actuelle.	Non	Non pris en charge
WorkSpaces PISCINES	10	Le nombre maximum de WorkSpace s pools de ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Instances de streaming à valeur ajoutée à usage général pour les WorkSpaces pools	10	Le nombre maximum d'instances de streaming à valeur générale pouvant être utilisées pour les WorkSpace s pools de ce compte dans la région actuelle.	Oui	Oui
Instances de streaming standard à usage général pour les WorkSpaces pools	10	Le nombre maximum d'instances standard à usage général pouvant être utilisées pour les WorkSpace s pools de ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Instances de streaming de performances à usage général pour les WorkSpaces pools	10	Le nombre maximum d'instances de streaming de performances à usage général qui peuvent être utilisées pour les WorkSpaces pools de ce compte dans la région actuelle.	Oui	Oui
Instances Power Streaming à usage général pour les WorkSpaces pools »	10	Le nombre maximum d'instances de streaming Power à usage général qui peuvent être utilisées pour les WorkSpaces pools de ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Instances de PowerPro streaming à usage général pour « WorkSpaces Pools »	10	Le nombre maximum d'instances de PowerPro streaming à usage général pouvant être utilisées pour les WorkSpace s pools de ce compte dans la région actuelle.	Oui	Oui
Instances de streaming Graphics. G4dn xlarge pour Pools WorkSpaces	0	Le nombre maximum d'instances de streaming Graphics.G4dn xlarge qui peuvent être utilisées pour les WorkSpace s pools de ce compte dans la région actuelle.	Oui	Oui

Ressource	Par défaut	Description	Ajustable	Usage
Instances de streaming Graphics. g4dn 4xlarge pour Pools WorkSpaces	0	Le nombre maximum d'instances de streaming Graphics.G4DN 4xlarge qui peuvent être utilisées pour les WorkSpaces pools de ce compte dans la région actuelle.	Oui	Oui
WorkSpaces Instances gérées de base	1 000	Le nombre maximum d'instances WorkSpaces gérées dans ce compte dans la région actuelle.	Oui	Non pris en charge
Instances WorkSpaces gérées simultanées en état d'allocation	700	Le nombre maximum d'instances WorkSpaces gérées simultanées dans l'état d'allocation de ce compte dans la région actuelle.	Oui	Non pris en charge

Limitation d'API

Le débit autorisé est de deux appels par seconde. Pour plus d'informations sur les quotas de limitation, consultez [Erreurs ThrottlingException](#).

Politique de fin de vie pour les applications WorkSpaces clientes

La politique de WorkSpaces fin de vie (EOL) d'Amazon s'applique à des versions majeures spécifiques (et à toutes leurs versions mineures) des WorkSpaces clients pour WorkSpaces Personal et WorkSpaces Pools.

Le cycle de vie d'une version WorkSpaces client comporte trois phases : support général, conseils techniques et fin de vie (EOL). La phase de support général commence à la date de publication publique initiale d'un WorkSpaces client et dure pendant une durée déterminée. Pendant la phase de support général, l'équipe d' WorkSpaces assistance fournit une assistance complète pour les problèmes de configuration. Les résolutions de défauts et les demandes de fonctionnalités sont mises en œuvre pour cette version majeure et les versions secondaires associées du WorkSpaces client.

Des conseils techniques sont fournis de la fin de la phase de prise en charge générale jusqu'à la date de fin de vie. Pendant la phase de conseil technique, vous bénéficiez d'une assistance et de conseils uniquement pour les configurations prises en charge. Les résolutions de défauts et les demandes de fonctionnalités sont mises en œuvre uniquement pour les versions les plus récentes du WorkSpaces client. Elles ne sont pas implémentées pour les anciennes versions. Au cours de la phase d'assistance technique, si un correctif est requis, AWS nous planifierons ce correctif pour la prochaine version accessible au public, et vous aurez la possibilité de passer à la dernière WorkSpaces version pour bénéficier de l'assistance relative au correctif.

La fin de vie d'une version majeure survient lorsque la prise en charge générale et les conseils techniques ont pris fin. Après la date de fin de vie, aucune autre assistance ou maintenance n'est fournie. AWS arrête de tester les problèmes de compatibilité. Pour bénéficier d'un support continu, vous devez passer à la dernière version WorkSpaces du client.

Consultez ce tableau pour plus d'informations sur la prise en charge de versions spécifiques.

Important

Les versions clientes suivantes ont atteint la fin de vie (EOL) le 15 novembre 2025. Assurez-vous de passer à une version client prise en charge avant le 28 février 2026 pour éviter toute interruption de service.

- Linux 2024.6-2024.8 pour Ubuntu 22.04

- Linux 2024.6-2024.8 pour Ubuntu 20.04

Client Windows	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
5,221 et plus	3 septembre 2024			Pris en charge

Client Linux	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
2025.1+ pour Ubuntu 24.04	12 décembre 2025			Pris en charge
2025.0+ pour Ubuntu 22.04	28 mai 2025			Pris en charge
2025.0+ pour Ubuntu 20.04	28 mai 2025			Pris en charge
2024.6-2024.8 pour Ubuntu 22.04	6 septembre 2024	29 août 2025	15 novembre 2025	Assurez-vous de passer à la dernière version du client avant le 28 février 2026.
2024.6-2024.8 pour Ubuntu 20.04	6 septembre 2024	29 août 2025	15 novembre 2025	Assurez-vous de passer à la dernière version du client avant le 28 février 2026.

Client macOS	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
5,221 et plus	3 septembre 2024			Pris en charge

Client iPad	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
2.x	2019			Pris en charge

Client Android	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
5,0,1 et plus	6 novembre 2024			Pris en charge

Web Access	Prise en charge générale
Google Chrome	Version actuelle, plus les deux versions principales les plus récentes
Mozilla Firefox	Version actuelle, plus les deux versions principales les plus récentes
Microsoft Edge	Version actuelle, plus les deux versions principales les plus récentes

Versions du client non prises en charge

Les WorkSpaces clients suivants ne sont pas pris en charge.

Système d'exploitation	Version du client	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
Windows	5,0-5,22,0	2 juin 2022	21 novembre 2021	31 mars 2025	Non pris en charge
Windows	5,11	3 juillet 2023	1er octobre 2023	1er octobre 2025	Non pris en charge
Windows	5,10	19 juin 2023	1er octobre 2023	1er octobre 2025	Non pris en charge
Windows	5,9	9 mai 2023	1er octobre 2023	1er octobre 2025	Non pris en charge
Windows	4. x	30 Juin 2021	21 novembre 2021	31 mars 2025	Non pris en charge
Windows	3.x	25 novembre 2021	21 novembre 2021	31 mars 2025	Non pris en charge
Windows	2.x	2018	31 mars 2023	31 août 2023	Non pris en charge
Ubuntu	2024.6-2024.8 pour Ubuntu 22.04	6 septembre 2024	29 août 2025	15 novembre 2025	Non pris en charge
Ubuntu	2024.6-2024.8 pour Ubuntu 20.04	6 septembre 2024	29 août 2025	15 novembre 2025	Non pris en charge
Ubuntu	2024.0-2024.5 pour Ubuntu 22.04	28 février 2024	21 novembre 2024	31 mars 2025	Non pris en charge

Système d'exploitation	Version du client	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
Ubuntu	2024.0-2024.5 pour Ubuntu 20.04	24 août 2023	21 novembre 2023	31 mars 2025	Non pris en charge
Ubuntu	2023.x pour Ubuntu 22.04	24 août 2023	21 novembre 2023	31 mars 2025	Non pris en charge
Ubuntu	2023.x pour Ubuntu 20.04	24 août 2023	21 novembre 2023	31 mars 2025	Non pris en charge
Ubuntu	4.x pour Ubuntu 20.04	27 octobre 2022	21 novembre 2023	31 mars 2025	Non pris en charge
Ubuntu	4.x pour Ubuntu 18.04	12 août 2021	31 mars 2023	31 août 2023	Non pris en charge
Ubuntu	3.x pour Ubuntu 18.04	25 novembre 2020	31 mars 2023	31 août 2023	Non pris en charge
macOS	5.1-5.22.0	30 juin 2022	21 novembre 2023	31 mars 2025	Non pris en charge
macOS	4. x	5 août 2021	21 novembre 2023	31 mars 2025	Non pris en charge
macOS	3.x	25 novembre 2020	21 novembre 2023	31 mars 2025	Non pris en charge
macOS	2.x	2019	31 mars 2023	31 août 2023	Non pris en charge
macOS	1.x	2018	31 mars 2023	31 août 2023	Non pris en charge

Système d'exploitation	Version du client	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
iPad	1.x	2018	31 mars 2023	31 août 2023	Non pris en charge
Android	5.0.0	26 février 2024	21 novembre 2023	31 mars 2025	Non pris en charge
Android	4. x	12 mai 2022	21 novembre 2023	31 mars 2025	Non pris en charge
Android	3.x	30 Juin 2021	21 novembre 2023	31 mars 2025	Non pris en charge
Android	2.x	2019	31 mars 2023	31 août 2023	Non pris en charge
Android	1.x	2018	31 mars 2023	31 août 2023	Non pris en charge

EOL FAQs

J'utilise une version d'un WorkSpaces client qui a atteint son EOL. Que dois-je faire pour passer à une version prise en charge ?

Accédez à la [page de téléchargement du WorkSpaces client](#) pour télécharger et installer une version entièrement compatible de WorkSpaces.

Puis-je utiliser une version du WorkSpaces client qui a atteint sa fin de vie avec une version compatible ? Workspace

Nous vous recommandons vivement de mettre à niveau vos clients vers la dernière version, car les résolutions et fonctionnalités précédentes ne sont plus appliquées aux versions des clients ayant atteint leur EOL. Si vous utilisez une version client qui a atteint sa fin de vie, contactez l'équipe d'AWS assistance pour plus d'informations.

J'utilise une version d'un WorkSpaces client qui a atteint son EOL. Puis-je tout de même signaler des problèmes à son sujet ?

Vous devez d'abord effectuer une mise à niveau vers une version prise en charge et essayer de reproduire le problème. Si le problème persiste dans la version prise en charge, ouvrez une demande de support technique auprès de l'équipe d'assistance AWS .

J'utilise une version WorkSpaces client prise en charge sur un système d'exploitation qui a atteint sa fin de vie. Puis-je tout de même signaler des problèmes à son sujet ?

L'assistance technique et les mises à jour logicielles ne sont plus disponibles pour les systèmes d'exploitation ayant atteint leur date de fin de vie et AWS ne fournissent pas d'assistance aux WorkSpaces clients utilisant des systèmes d'exploitation ayant atteint leur date de fin de vie. Utilisez un système d'exploitation compatible pour garantir l'assistance de vos WorkSpaces clients.

Extension SDK supportée par DCV

Le DCV permet un accès à distance performant aux WorkSpaces instances pour un large éventail de charges de travail et de cas d'utilisation. Avec le SDK d'extension Amazon DCV, les développeurs peuvent personnaliser l' WorkSpaces expérience DCV pour les utilisateurs finaux, notamment :

- Faciliter la prise en charge de matériel personnalisé
- Améliorer l'utilisabilité des applications tierces lors de sessions distantes. Par exemple, ajouter une terminaison audio locale pour les applications VoIP, ou une lecture vidéo locale pour les applications de conférence.
- Fournir à des logiciels d'accessibilité, comme les lecteurs d'écran, des informations sur la session distante et les applications exécutées à distance
- Permettre au logiciel de sécurité d'analyser le niveau de sécurité du point de terminaison local afin d'autoriser les stratégies d'accès conditionnelles
- Effectuer des transferts de données arbitraires via une session distante établie

Pour commencer à utiliser le SDK d'extension Amazon DCV, consultez la documentation du SDK d'[extension Amazon DCV](#). Vous pouvez trouver le SDK lui-même dans le référentiel [Amazon DCV Extension SDK GitHub](#). En outre, vous pouvez également trouver des exemples d'intégration du SDK dans le référentiel d'exemples du [SDK Amazon DCV Extension](#). GitHub

Les éléments suivants sont pris en charge par WorkSpaces.

- Protocole de diffusion — DCV
- WorkSpaces Client Windows — Windows : 5.9.0.4110 et versions ultérieures.

Note

WorkSpaces Les clients Android, iOS et Web Access ne sont pas compatibles avec le SDK d'extension DCV.

- WorkSpaces pris en charge — serveurs Windows, Linux et Ubuntu

Historique du document pour WorkSpaces

Le tableau suivant décrit les modifications importantes apportées au WorkSpaces service et au guide d' WorkSpaces administration Amazon à compter du 1er janvier 2018. Nous mettons aussi la documentation à jour régulièrement pour prendre en compte les commentaires qui nous sont envoyés.

Pour être informé de ces mises à jour, vous pouvez vous abonner au WorkSpaces flux RSS.

Modification	Description	Date
Redirection USB pour DCV	Vous pouvez configurer la redirection USB pour Windows basé sur DCV afin de permettre WorkSpaces aux utilisateurs d'accéder aux périphériques USB locaux au sein de leur environnement de bureau virtuel.	28 octobre 2025
Support ajouté pour configurer la résolution de la webcam	Vous pouvez configurer la résolution de la webcam sous Windows WorkSpaces lorsque vous utilisez DCV.	21 octobre 2025
Support ajouté pour configurer la disposition du clavier du serveur	Vous pouvez désormais configurer Windows WorkSpaces lorsque vous utilisez DCV pour utiliser une disposition de clavier côté serveur, en plus de la disposition par défaut côté client.	21 octobre 2025
Support ajouté pour les IPv6 réseaux	Amazon WorkSpaces prend en charge IPv4 et met en IPv6 réseau des points de terminais	21 octobre 2025

on VPC pour le streaming.
WorkSpaces

[Modes de course](#)

Le mode de fonctionnement d'un WorkSpaces pool détermine sa disponibilité immédiate et votre mode de paiement. Vous pouvez choisir entre les deux modes de fonctionnement lorsque vous créez un WorkSpaces pool.

15 mai 2025

[Répertoire des identifiants Microsoft Entra](#)

L'intégration entre régions entre IAM Identity Center WorkSpaces est prise en charge.

27 février 2025

[Répertoire des identifiants Microsoft Entra](#)

Vous pouvez créer un répertoire d'identifiants Microsoft Entra dédié.

26 août 2024

[Microsoft Visual Studio](#)

Les bundles Microsoft Visual Studio sont pris en charge pour les applications de gestion.

1er août 2024

[Extension de redirection WebRTC Amazon DCV](#)

Vous pouvez installer l'extension de redirection WebRTC Amazon DCV pour utiliser la redirection WebRTC.

1er août 2024

[WorkSpaces Pools est désormais disponible dans AWS GovCloud \(US\) Region](#)

WorkSpaces Pools propose des bureaux virtuels non persistants conçus pour les utilisateurs qui ont besoin d'un accès à la demande à des environnements de bureau hautement sélectionnés hébergés sur une infrastructure éphémère.

23 juillet 2024

[WorkSpaces Les piscines sont désormais disponibles](#)

WorkSpaces Pools propose des bureaux virtuels non persistants conçus pour les utilisateurs qui ont besoin d'un accès à la demande à des environnements de bureau hautement sélectionnés hébergés sur une infrastructure éphémère.

27 juin 2024

[AmazonWorkSpacesAdmin mise à jour des politiques gérées et nouvelle politique AmazonWorkSpacesPoolServiceAccess gérée](#)

WorkSpaces a mis à jour la stratégie AmazonWorkSpacesAdmin gérée et ajouté la nouvelle stratégie AmazonWorkSpacesPoolServiceAccess gérée.

27 juin 2024

[AmazonWorkSpacesAdmin mise à jour des politiques gérée](#)

WorkSpaces a ajouté les espaces de travail : RestoreWorkspace action à la politique AmazonWorkSpacesAdmin gérée, accordant aux administrateurs l'accès à la restauration. WorkSpaces

17 juillet 2023

Extension SDK supportée par DCV	Avec le SDK d'extension Amazon DCV, les développeurs peuvent personnaliser l'WorkSpaces expérience DCV pour les utilisateurs finaux.	25 mai 2023
Versions de l'agent hôte DCV	Informations de version pour DCV.	8 mai 2023
Amazon WorkSpaces a été lancé en AWS GovCloud (USA Est)	Amazon WorkSpaces est disponible aux États-Unis AWS GovCloud (est des États-Unis).	3 mai 2023
Assistance par WorkSpaces webcam Amazon	Amazon prend WorkSpaces désormais en charge l'audio/vidéo (AV) en temps réel en redirigeant facilement l'entrée vidéo de la webcam locale vers les WorkSpace s ordinateurs de bureau Windows à l'aide du format DCV.	5 avril 2021
Support des cartes à WorkSpaces puce Amazon avec l'application cliente WorkSpaces macOS	Vous pouvez désormais utiliser l'application client Amazon WorkSpaces macOS avec les cartes à puce Common Access Card (CAC) et Personal Identity Verification (PIV). La prise en charge des cartes à puce est disponible lors de WorkSpaces l'utilisation de DCV.	5 avril 2021

[Gestion des WorkSpaces offres Amazon APIs](#)

La gestion WorkSpaces APIs des offres Amazon est désormais disponible. Ces actions d'API prennent en charge les opérations de création, de suppression et d'association d'images pour WorkSpaces les bundles.

15 mars 2021

[Amazon est WorkSpace s lancé en Asie-Pacifique \(Mumbai\)](#)

Amazon WorkSpaces est disponible dans la région Asie-Pacifique (Mumbai).

8 mars 2021

[Cartes à puce](#)

Amazon prend WorkSpaces désormais en charge l'authentification par carte à puce avant session (connexion) et pendant la session sous Windows et Linux WorkSpaces dans la région AWS GovCloud (ouest des États-Unis).

1er décembre 2020

[DCV](#)

Le DCV est désormais disponible à la fois pour la licence incluse (Windows Server 2016) et pour le BYOL basé WorkSpaces sur Windows 10 sur tous les types de bundle, à l'exception de Graphics et. GraphicsPro DCV est également disponible pour Linux WorkSpaces dans la région AWS GovCloud (ouest des États-Unis).

1er décembre 2020

[Partage d'images personnalisées](#)

Vous pouvez désormais partager des WorkSpaces images personnalisées entre différents AWS comptes. Une fois qu'une image a été partagée, le compte destinataire peut copier l'image et l'utiliser pour créer des ensembles en vue du lancement d'une nouvelle WorkSpaces image.

1er octobre 2020

[Redirection entre régions](#)

Vous pouvez désormais utiliser la redirection entre régions, une fonctionnalité qui fonctionne avec les politiques de routage de votre système de noms de domaine (DNS) pour rediriger vos utilisateurs vers une alternative WorkSpaces lorsque leur principal n'est WorkSpaces pas disponible.

10 septembre 2020

[Abonnez-vous à Microsoft Office 2016 ou 2019 pour BYOL WorkSpaces](#)

Vous pouvez désormais vous abonner à Microsoft Office Professional 2016 ou 2019 fourni par la licence AWS On Bring Your Own Windows (BYOL) WorkSpaces.

3 septembre 2020

[Automatisation BYOL dans la région Chine \(Ningxia\)](#)

Vous pouvez utiliser l'automatisation Bring Your Own License (BYOL) pour simplifier le processus d'utilisation de vos licences de bureau Windows 10 pour vos WorkSpaces en Chine (Ningxia).

2 avril 2020

[Vérificateur d'image](#)

L'outil Image Checker vous aide à déterminer si votre Windows Workspace répond aux exigences relatives à la création d'images. Le vérificateur d'images effectue une série de tests sur le produit Workspace que vous souhaitez utiliser pour créer votre image et fournit des conseils sur la manière de résoudre les problèmes détectés.

30 mars 2020

[Migrer WorkSpaces](#)

La fonctionnalité Amazon WorkSpaces Migrate vous permet WorkSpace de migrer un bundle vers un autre, tout en conservant les données relatives au volume d'utilisateurs. Vous pouvez utiliser cette fonctionnalité pour migrer WorkSpaces de l'expérience de bureau Windows 7 vers l'expérience de bureau Windows 10. Vous pouvez également utiliser cette fonctionnalité pour migrer WorkSpaces d'un bundle public ou personnalisé à un autre.

9 janvier 2020

[PrivateLink intégration pour Amazon WorkSpaces APIs](#)

Vous pouvez vous connecter directement aux points de terminaison de WorkSpaces l'API Amazon via un point de terminaison d'interface dans votre Virtual Private Cloud (VPC) au lieu de vous connecter via Internet. Lorsque vous utilisez un point de terminaison d'interface VPC, la communication entre votre VPC et le point de terminaison de l'API Amazon s'effectue de manière entièrement et sécurisée au sein du réseau. AWS

25 novembre 2019

Client Linux pour Amazon WorkSpaces	Les utilisateurs peuvent désormais utiliser le client Linux pour accéder à leur WorkSpaces.	25 novembre 2019
Amazon est WorkSpaces lancé en Chine (Ningxia)	Amazon WorkSpaces est disponible dans la région de Chine (Ningxia).	13 novembre 2019
WorkSpaces Rétablir le dernier état de santé connu	Vous pouvez utiliser la fonction de restauration pour rétablir WorkSpace le dernier état sain connu.	18 septembre 2019
Chiffrement de points de terminaison FIPS	Pour vous conformer au Federal Risk and Authorization Management Program (FedRAMP) ou au Guide des exigences de sécurité du cloud computing (SRG) du ministère de la Défense (DoD), vous pouvez configurer WorkSpaces Amazon pour utiliser le chiffrement des terminaux FIPS (Federal Information Processing Standards) au niveau du répertoire.	12 septembre 2019
Copier WorkSpace des images	Vous pouvez copier vos images dans la même région ou d'une région à une autre.	27 juin 2019

<u>Fonctionnalités de WorkSpace gestion en libre-service pour les utilisateurs</u>	Vous pouvez activer les fonctionnalités de WorkSpace gestion en libre-service pour vos utilisateurs afin de leur permettre de mieux contrôler leur expérience.	19 novembre 2018
<u>Automatisation BYOL</u>	Vous pouvez utiliser l'automatisation BYOL (Bring Your Own License) pour simplifier le processus d'utilisation de vos licences de bureau Windows 7 et Windows 10 pour votre WorkSpaces.	16 novembre 2018
<u>PowerPro et GraphicsPro offres groupées</u>	Les GraphicsPro packs PowerPro et sont désormais disponibles pour WorkSpaces.	18 octobre 2018
<u>Surveiller les WorkSpace connexions réussies</u>	Vous pouvez utiliser les événements d'Amazon CloudWatch Events pour surveiller les WorkSpace connexions réussies et y répondre.	17 septembre 2018
<u>Accès Web pour Windows 10 WorkSpaces</u>	Les utilisateurs peuvent désormais utiliser le client d'accès Web pour accéder à une expérience de bureau WorkSpace fonctionnant sous Windows 10.	24 août 2018

Connexion par URI	Vous pouvez utiliser des identificateurs de ressources uniformes (URIs) pour permettre aux utilisateurs d'accéder à leurs WorkSpaces.	31 juillet 2018
Amazon Linux WorkSpaces	Vous pouvez configurer Amazon Linux WorkSpaces pour vos utilisateurs.	26 juin 2018
Groupes de contrôles d'accès IP	Vous pouvez contrôler les adresses IP à partir desquelles les utilisateurs peuvent accéder à leurs WorkSpaces.	30 avril 2018
Mises à niveau sur place	Vous pouvez mettre à niveau votre Windows 10 BYOL WorkSpaces vers une version plus récente de Windows 10.	9 mars 2018

Mises à jour antérieures

Le tableau suivant décrit les ajouts importants apportés au WorkSpaces service Amazon et à sa documentation établie avant le 1er janvier 2018.

Modifier	Description	Date
Options de calcul flexibles	Vous pouvez alterner WorkSpaces entre les offres Value, Standard, Performance et Power	22 décembre 2017
Stockage configurable	Vous pouvez configurer la taille des volumes root et utilisateur WorkSpaces lorsque vous les lancez et augmenter la taille de ces volumes ultérieurement.	22 décembre 2017

Modifier	Description	Date
Contrôle de l'accès aux appareils	Vous pouvez spécifier les types d'appareils auxquels vous avez accès WorkSpaces. En outre, vous pouvez restreindre l'accès WorkSpaces aux appareils fiables (également appelés appareils administrés).	le 19 juin 2017
Approbations entre forêts	Vous pouvez établir une relation de confiance entre votre AWS Managed Microsoft AD et votre domaine Microsoft Active Directory local, puis le provisionner WorkSpaces pour les utilisateurs dans le domaine local.	9 février 2017
Offres Windows Server 2016	WorkSpaces propose des offres groupées qui incluent une expérience de bureau Windows 10, optimisée par Windows Server 2016.	29 novembre 2016
Web Access	Vous pouvez accéder à Windows à WorkSpaces à partir d'un navigateur Web à l'aide de WorkSpaces Web Access.	le 18 novembre 2016
Par heure WorkSpaces	Vous pouvez configurer votre compte de WorkSpaces manière à ce que les utilisateurs soient facturés à l'heure.	le 18 août 2016
Windows 10 BYOL	Vous pouvez apporter votre licence de bureau Windows 10 à WorkSpaces (BYOL).	21 juillet 2016
Prise en charge du balisage	Vous pouvez utiliser des balises pour gérer et suivre votre WorkSpaces.	17 mai 2016
Enregistrements sauvegardés	Chaque fois que vous entrez un nouveau code d'enregistrement, le WorkSpaces client l'enregistre. Cela permet de passer plus facilement d'un répertoire ou d'une région WorkSpaces à l'autre.	28 janvier 2016

Modifier	Description	Date
Windows 7 BYOL, client Chromebook, chiffrement Workspace	Vous pouvez transférer votre licence de bureau Windows 7 vers WorkSpaces (BYOL), utiliser le client Chromebook et utiliser le chiffrement Workspace.	1er octobre 2015
CloudWatch surveillance	Ajout d'informations sur CloudWatch la surveillance.	28 avril 2015
Reconnexion de session automatique	Ajout d'informations sur la fonctionnalité de reconnexion automatique de session dans les applications clientes WorkSpaces de bureau.	31 mars 2015
Adresses IP publiques	Vous pouvez attribuer automatiquement une adresse IP publique à votre WorkSpaces.	23 janvier 2015
WorkSpaces lancé en Asie-Pacifique (Singapour)	WorkSpaces est disponible dans la région Asie-Pacifique (Singapour).	15 janvier 2015
Ajout de l'offre groupée Value, mise à jour de l'offre groupée Standard, ajout d'Office 2013	L'offre Value est disponible, le matériel de l'offre Standard a été mis à niveau et Microsoft Office 2013 est disponible dans les packages Plus.	6 novembre 2014
Prise en charge des images et des offres	Vous pouvez créer une image à partir d'une image Workspace que vous avez personnalisée et un Workspace ensemble personnalisé à partir de cette image.	28 octobre 2014
PCoSupport client sans adresse IP	Vous pouvez accéder aux appareils clients WorkSpaces PCo IP zéro.	15 octobre 2014
WorkSpaces lancé en Asie-Pacifique (Tokyo)	WorkSpaces est disponible dans la région Asie-Pacifique (Tokyo).	26 août 2014
Prise en charge d'une imprimante locale	Vous pouvez activer le support d'imprimante local pour votre WorkSpaces.	26 août 2014

Modifier	Description	Date
Authentification multifactorielle	Vous pouvez utiliser l'authentification multi-facteurs dans des annuaires connectés.	11 août 2014
Prise en charge d'une UO par défaut et prise en charge d'un domaine cible	Vous pouvez sélectionner une unité organisationnelle (UO) par défaut dans laquelle vos comptes de WorkSpace machine sont placés et un domaine distinct dans lequel vos comptes de WorkSpace machine sont créés.	le 7 juillet 2014
Ajout de groupes de sécurité	Vous pouvez ajouter un groupe de sécurité à votre WorkSpaces.	le 7 juillet 2014
WorkSpaces lancé en Asie-Pacifique (Sydney)	WorkSpaces est disponible dans la région Asie-Pacifique (Sydney).	15 mai 2014
WorkSpaces lancé en Europe (Irlande)	WorkSpaces est disponible dans la région Europe (Irlande).	5 mai 2014
Version bêta publique	WorkSpaces est disponible en version bêta publique.	25 mars 2014

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.