aws

Guide d’administration

Amazon WorkSpaces

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon WorkSpaces: Guide d’administration

Copyright © 2024 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
Fonctionnalités 1
Architecture 2
Accédez à votre WorkSpace 3
Tarification 4
Comment démarrer 4
Mise en route : configuration rapide 6
Avant de commencer 7
En quoi consiste la configuration rapide 7
Étape 1 : Lancer l'instance WorkSpace 8
Étape 2 : Se connecter à l'instance WorkSpace 12
Étape 3 : Nettoyer (Facultatif) 13
Étapes suivantes 13
Mise en route : configuration avancée 15
Avant de commencer 15
Utilisation de la configuration avancée pour lancer une instance WorkSpace 16
Mise en réseau et accès 17
Protocoles pour Amazon WorkSpaces 17
Prérequis 18
Quand utiliser WSP 18
Quand utiliser PCoIP 19
Exigences du VPC 20
Prérequis 20
Configuration d'un VPC avec des sous-réseaux privés et une passerelle NAT 21
Configuration d'un VPC avec des sous-réseaux publics 24
Zones de disponibilité pour WorkSpaces 26
Exigences relatives aux adresses IP et aux ports 28
Ports pour client 28
Ports pour l'accès Web 30
Domaines et adresses IP à ajouter à votre liste d'autorisation 31
..... 46
..... 48
Serveur de surveillance de l'état 49
Serveurs de passerelle PCoIP 52

Serveurs de passerelle WSP 54
Noms de domaine de passerelle WSP 56
Interfaces réseau 57
Exigences relatives aux adresses IP et aux ports par région 62
Exigences réseau 111
Appareils approuvés 114
Étape 1 : Créer des certificats 115
Étape 2 : Déployer les certificats clients vers les appareils approuvés 116
Étape 3 : Configurer la restriction 116
Intégration SAML 2.0 117
Flux de travail d'authentification 117
Configuration de SAML 2.0 121
Authentification par certificat 136
Authentification par carte à puce 141
Prérequis 142
Limites 143
Configuration Active Directory 144
Activer les cartes à puce pour Windows WorkSpaces 144
Activer les cartes à puce pour Linux WorkSpaces 147
Accès Internet 153
Groupes de sécurité 154
Groupes de contrôles d'accès IP 156
Création d'un groupe de contrôles d'accès IP 157
Association d'un groupe de contrôle d'accès IP à un annuaire 158
Copie d'un groupe de contrôles d'accès IP 158
Suppression d'un groupe de contrôles d'accès IP 159
Client plume PCoIP 159
Configuration d'Android pour les Chromebooks 160
Web Access 161
Étape 1 : Activez l'accès Web à votre WorkSpaces 162
Étape 2 : Configurer l'accès entrant et sortant aux ports pour Web Access 162
Étape 3 : Configurer les paramètres de stratégie de groupe et de stratégie de sécurité pour permettre aux utilisateurs de se connecter 163
Chiffrement de points de terminaison FIPS 166
Activation de connexions SSH 168
Conditions préalables pour les connexions SSH à Amazon Linux WorkSpaces 169

Activer les connexions SSH à tous les Amazon Linux WorkSpaces d'un répertoire 171
Authentification par mot de passe dans Amazon Linux 2 WorkSpaces 172
Activer les connexions SSH à un Amazon Linux spécifique WorkSpace 173
Connectez-vous à un Amazon Linux à WorkSpace l'aide de Linux ou PuTTY 173
Configuration requise 175
Configuration de la table de routage 175
Composants pour Windows 176
Composants pour Linux 177
Composants pour Ubuntu 179
Annuaires 181
Enregistrement d'un annuaire 182
Mise à jour des informations de l'annuaire 185
Sélection d'une unité d'organisation 185
Configuration des adresses IP automatiques 186
Contrôle de l'accès aux appareils 187
Gestion des autorisations d'administrateur local 187
Mettre à jour le compte du connecteur AD (AD Connector) 188
Authentification multifactorielle (AD Connector) 188
Mise à jour des serveurs DNS pour WorkSpaces 190
Bonnes pratiques 190
Étape 1 : Mettre à jour les paramètres de serveur DNS de vos instances WorkSpaces 191
Étape 2 : Mettre à jour les paramètres de serveur DNS pour Active Directory 194
Étape 3 : Tester les paramètres de serveur DNS mis à jour 194
Suppression d'un annuaire 197
Activation d'Amazon WorkDocs pour AWS Managed Microsoft AD 199
Configuration de l'administration de l'annuaire 200
Lancer une instance WorkSpace 204
Lancement avec AWS Managed Microsoft AD 206
Avant de commencer 207
Étape 1 : Création d'un annuaire AWS Managed Microsoft AD 207
Étape 2 : Créer une instance WorkSpace 209
Étape 3 : Se connecter à l'instance WorkSpace 210
Étapes suivantes 211
Lancement avec Simple AD 212
Avant de commencer 212
Étape 1 : Créer un annuaire Simple AD 213

Étape 2 : Créer une instance WorkSpace 215
Étape 3 : Se connecter à l'instance WorkSpace 216
Étapes suivantes 217
Lancement avec AD Connector 218
Avant de commencer 218
Étape 1 . Créer un connecteur AD 219
Étape 2 : Créer une instance WorkSpace 220
Étape 3 : Se connecter à l'instance WorkSpace 222
Étapes suivantes 223
Lancement avec un domaine approuvé 223
Avant de commencer 224
Étape 1 : Établir une relation d'approbation 224
Étape 2 : Créer une instance WorkSpace 225
Étape 3 : Se connecter à l'instance WorkSpace 226
Étapes suivantes 227
Administration des utilisateurs d'instances WorkSpaces 229
Gestion des utilisateurs d'instances WorkSpaces 229
Modification d'informations utilisateur 229
Ajout ou suppression d'utilisateurs 230
Envoi d'un e-mail d'invitation 231
Création de plusieurs WorkSpaces pour un utilisateur 231
Personnalisez la façon dont les utilisateurs se connectent à leur WorkSpaces 233
Activation des capacités de gestion d'instances WorkSpaces en libre-service pour les utilisateurs 235
Activation de l'optimisation audio Amazon Connect pour les utilisateurs 238
Prérequis 239
Activation de l'optimisation audio d'Amazon Connect 239
Mise jour des informations d'optimisation audio Amazon Connect de l'annuaire 240
Suppression de l'optimisation audio Amazon Connect de l'annuaire 241
Activation du chargement des journaux de diagnostic 241
Chargement des journaux de diagnostic 241
Administrez votre WorkSpaces 244
Gérer Windows WorkSpaces 245
Installation des fichiers de modèle d'administration de stratégie de groupe pour WSP 247
Gérer les paramètres de stratégie de groupe pour WSP 249
Installation du modèle d'administration de stratégie de groupe 277

Gérer les paramètres de stratégie de groupe pour PCoIP 281
Définition de la durée de vie maximale d'un ticket Kerberos 290
Configuration des paramètres de serveur proxy de l'appareil pour l'accès à Internet 291
Activation de la prise en charge du plug-in multimédia pour les réunions Zoom 292
Gérez votre Amazon Linux WorkSpaces 295
Comportement du protocole WSP (Control WorkSpaces Streaming Protocol) sur Amazon Linux WorkSpaces 296
Configurer la redirection du presse-papiers pour WSP Amazon Linux WorkSpaces 297
Activer ou désactiver la redirection d'entrée audio pour WSP Amazon Linux WorkSpaces ... 297
Activer ou désactiver la redirection de fuseau horaire pour WSP Amazon Linux WorkSpaces 298
Contrôlez le comportement de l'agent PCoIP sur Amazon Linux WorkSpaces 299
Configurer la redirection du presse-papiers pour PCoIP Amazon Linux WorkSpaces 300
Activer ou désactiver la redirection d'entrée audio pour PCoIP Amazon Linux WorkSpaces 301
Activer ou désactiver la redirection de fuseau horaire pour PCoIP Amazon Linux WorkSpaces 301
Accorder un accès SSH aux administrateurs Amazon Linux WorkSpaces 302
Remplacer le shell par défaut pour Amazon Linux WorkSpaces 303
Protection des référentiels personnalisés contre tout accès non autorisé 303
Utilisation du référentiel de la bibliothèque Amazon Linux Extras 304
Utiliser des cartes à puce pour l'authentification sous Linux WorkSpaces 304
Configuration des paramètres de serveur proxy de l'appareil pour l'accès à Internet 304
Gérez votre Ubuntu WorkSpaces 306
Comportement du protocole WSP (Control WorkSpaces Streaming Protocol) sur Ubuntu WorkSpaces 307
Activer ou désactiver la redirection du presse-papiers pour Ubuntu WorkSpaces 307
Activer ou désactiver la redirection audio pour Ubuntu WorkSpaces 308
Activer ou désactiver la redirection d'entrée vidéo pour Ubuntu WorkSpaces 308
Activer ou désactiver la redirection de fuseau horaire pour Ubuntu WorkSpaces 309
Activer ou désactiver la redirection d'imprimante pour Ubuntu WorkSpaces 310
Activation ou désactivation de la déconnexion de session au verrouillage de l'écran pour WSP 310
Accorder l'accès SSH aux administrateurs Ubuntu WorkSpaces 311
Remplacer le shell par défaut pour Ubuntu WorkSpaces 313
Configuration des paramètres de serveur proxy de l'appareil pour l'accès à Internet 313

Optimisation pour la communication en temps réel 315
Présentation des modes d'optimisation des médias 316
Quel mode d'optimisation de la communication en temps réel (RTC) utiliser ? 317
Conseils d'optimisation de la communication en temps réel (RTC) 318
Gestion du mode d'exécution 326
Instances WorkSpaces AutoStop 326
Modification du mode d'exécution 328
Arrêt et démarrage d'une instance WorkSpace AutoStop 328
Gestion des applications 329
Offres groupées prises en charge pour la gestion des applications 330
..... 332
Gestion des WorkSpaces modifications à l'aide de Gérer les applications 334
Modifier un WorkSpace 335
Modification de la taille des volumes 336
Modification du type de calcul 339
Modification des protocoles 340
Personnaliser la WorkSpace marque 342
Importation d'une marque personnalisée 343
Description de la marque personnalisée 350
Suppression de la marque personnalisée 350
Balisage des ressources WorkSpaces 351
Maintenance des instances WorkSpaces 353
Fenêtres de maintenance pour instances WorkSpaces AlwaysOn 354
Fenêtres de maintenance pour les instances WorkSpaces AutoStop 354
Maintenance manuelle 355
Instances WorkSpace chiffrées 356
Prérequis 357
Limites 358
Présentation du chiffrement WorkSpaces avec AWS KMS 359
Contexte de chiffrement WorkSpaces 360
Octroi à WorkSpaces de l'autorisation d'utiliser une clé KMS en votre nom 361
Chiffrement d'une instance WorkSpace 366
Affichage des instances WorkSpaces chiffrées 366
Redémarrer un WorkSpace 366
Reconstruction d'une instance WorkSpace 367
Restauration d'une instance WorkSpace 369

Microsoft 365 BYOL 371
Créez WorkSpaces avec Microsoft 365 Apps pour entreprises 372
Migrez vos applications existantes WorkSpaces pour utiliser les applications Microsoft 365 pour les entreprises 373
Mettez à jour vos applications Microsoft 365 pour entreprises sur WorkSpaces 374
Mettre à niveau Windows BYOL WorkSpaces 374
Prérequis 375
Considérations 375
Limitations connues 376
Résumé des paramètres de clé de registre 377
Effectuer une mise à niveau sur place 378
Résolution des problèmes 382
Mettez à jour votre WorkSpace registre à l'aide d'un PowerShell script 383
Migrer un WorkSpace 384
Limites de migration 386
Scénarios de migration 386
Déroulement de la migration 388
Bonnes pratiques 390
Résolution des problèmes 390
Quelles sont les conséquences sur la facturation 391
Migration d'un WorkSpace 391
Suppression d'une instance WorkSpace 392
Bundles et images 394
Options d'offres groupées 396
Création d'une image et d'un bundle personnalisés 402
Conditions requises pour créer des images personnalisées Windows 403
Conditions requises pour créer des images personnalisées Linux 404
Bonnes pratiques 405
(Facultatif) Étape 1 : Définir un format de nom d'ordinateur personnalisé pour votre image .. 406
Étape 2 : Exécuter l'outil de vérification d'image 408
Étape 3 : Créer une image et un bundle personnalisés 418
Ce qui est inclus dans les images WorkSpaces personnalisées Windows 421
Ce qui est inclus dans les images WorkSpace personnalisées Linux 422
Mise à jour d'un bundle personnalisé 423
Copie d'une image personnalisée 425
Partage ou annulation de partage d'une image personnalisée 428

Suppression d'un bundle ou d'une image personnalisés 431
Suppression d'un bundle 431
Supprime une image 431
Apportez votre propre licence (BYOL) de bureau Windows 432
Prérequis 433
Versions Windows prises en charge pour BYOL 436
Ajout de Microsoft Office à votre image BYOL 437
Étape 1 : Vérifiez l'éligibilité de votre compte au BYOL à l'aide de la console Amazon WorkSpaces 443
Étape 2 : Activez BYOL pour votre compte BYOL à l'aide de la console Amazon WorkSpaces 445
Étape 3 : Exécuter le PowerShell script BYOL Checker sur une machine virtuelle Windows 446
Étape 4 : Exporter la machine virtuelle depuis l'environnement de virtualisation 453
Étape 5 : Importer la machine virtuelle comme image dans Amazon EC2 453
Étape 6 : Création d'une image BYOL à l'aide de la console WorkSpaces 454
Étape 7 : Créer un bundle personnalisé à partir de l'image BYOL 456
Étape 8 : Enregistrez un répertoire dédié pour WorkSpaces 456
Étape 9 : Lancez votre BYOL WorkSpaces 457
Surveillez votre WorkSpaces 458
Moniteur avec tableau CloudWatch de bord automatique 459
Comprendre votre tableau WorkSpaces CloudWatch de bord automatique 460
Surveiller à l'aide CloudWatch de métriques 462
WorkSpaces métriques 463
Dimensions pour les WorkSpaces métriques 470
Exemple de surveillance 471
Surveillez à l'aide d'Amazon EventBridge 473
WorkSpaces Accédez aux événements 474
Création d'une règle pour gérer les WorkSpaces événements 476
Compréhension des événements de connexion AWS pour les utilisateurs de carte à puce 477
Exemples d'événements de scénarios de connexion AWS 479
Continuité des activités 485
Redirection entre régions 486
Prérequis 487
Limites 489
Étape 1 : Créer des alias de connexion 490

(Facultatif) Étape 2 : Partager un alias de connexion avec un autre compte 491
Étape 3 : Associer des alias de connexion aux annuaires de chaque région 492
Étape 4 : Configurer le service DNS et définir les stratégies de routage DNS 493
Étape 5 : envoyer la chaîne de connexion à vos WorkSpaces utilisateurs 498
Schéma de l'architecture de redirection entre régions 499
Lancer la redirection entre régions 499
Que se passe-t-il lors de la redirection entre régions 500
Dissociation d'un alias de connexion d'un annuaire 500
Annulation du partage d'un alias de connexion 501
Suppression d'un alias de connexion 501
Autorisations IAM pour associer et dissocier des alias de connexion 502
Considérations de sécurité si vous arrêtez d'utiliser la redirection entre régions 504
Résilience multirégionale 504
Prérequis 505
Limites 506
Configurez votre mode de veille multirégional pour la résilience WorkSpace 508
Création d'un mode veille WorkSpace 510
Gérer une veille WorkSpace 511
Supprimer un mode veille WorkSpace 512
Réplication unidirectionnelle des données pour le mode veille WorkSpaces 513
Sécurité 514
Protection des données 515
Chiffrement au repos 516
Chiffrement en transit 516
Gestion des identités et des accès 517
Exemples de politiques 518
Spécification de ressources WorkSpaces dans une politique IAM 523
Création du rôle workspaces_DefaultRole 528
Création de la fonction du service AmazonWorkspaceSpacesPCAAccess 530
Politiques gérées par AWS pour WorkSpaces 531
Validation de conformité 535
Résilience 536
Sécurité de l'infrastructure 537
Isolement de réseau 537
Isolation sur les hôtes physiques 538
Autorisation des utilisateurs professionnels 538

Effectuer des demandes d'API Amazon WorkSpaces via un point de terminaison d'interface VPC 538
Création d'une stratégie de point de terminaison d'un VPC pour Amazon WorkSpaces 540
Connexion de votre réseau privé à votre VPC 541
Gestion des mises à jour 542
Résolution des problèmes 543
Activation de la journalisation avancée 543
Résolution de problèmes spécifiques 548
Je ne parviens pas à créer un Amazon Linux WorkSpace car le nom d'utilisateur contient des caractères non valides 550
J'ai changé le shell de mon Amazon Linux WorkSpace et je ne peux plus configurer de session PCoIP 551
Mon Amazon Linux WorkSpaces ne démarre pas 551
Le lancement WorkSpaces dans mon répertoire connecté échoue souvent 552
Le lancement WorkSpaces échoue avec une erreur interne 553
Lorsque j'essaie d'enregistrer un annuaire, l'enregistrement échoue et laisse l'annuaire avec l'état ERREUR 553
Mes utilisateurs ne peuvent pas se connecter à un système Windows WorkSpace doté d'une bannière de connexion interactive 553
Mes utilisateurs ne peuvent pas se connecter à un système Windows WorkSpace 553
Mes utilisateurs rencontrent des problèmes lorsqu'ils essaient de se connecter WorkSpaces à WorkSpaces Web Access 555
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. 556
Mes utilisateurs reçoivent le message « WorkSpace Status : Unhealthy ». Nous n'avons pas pu vous connecter à votre WorkSpace. Veuillez réessayer dans quelques minutes. ». 556
Mes utilisateurs reçoivent le message « Cet appareil n'est pas autorisé à accéder au WorkSpace. Contactez votre administrateur pour obtenir de l'aide. » 557
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 fournisseur de services Internet WorkSpace 557
Le WorkSpaces client envoie une erreur réseau à mes utilisateurs, mais ils peuvent utiliser d'autres applications connectées au réseau sur leurs appareils 558
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. » 560

Mes utilisateurs du client plume PCoIP reçoivent l'erreur « Le certificat fourni n'est pas valide en raison de l'horodatage » 560
Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients plume PCoIP 561
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 562
Mes utilisateurs ne peuvent pas installer l'application client Android sur leurs Chromebooks 562
Mes utilisateurs ne reçoivent pas d'e-mails d'invitation ou d'e-mails de réinitialisation de mot de passe 563
Mes utilisateurs ne voient pas l'option « Mot de passe oublié ? » sur l'écran de connexion du client 563
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 563
Non WorkSpaces , dans mon annuaire, je ne peux pas me connecter à Internet 564
Mon accès à Internet WorkSpace a été perdu 565
L'erreur « DNS unavailable » s'affiche lorsque j'essaie de me connecter à mon annuaire sur site 565
L'erreur « Connectivity issues detected » s'affiche lorsque je tente de me connecter à mon annuaire sur site 565
L'erreur « SRV record » s'affiche lorsque je tente de me connecter à mon annuaire sur site 566
Mon Windows WorkSpace se met en veille lorsqu'il est laissé inactif 566
L'un des WorkSpaces miens a un état de UNHEALTHY 568
Mon ordinateur WorkSpace se bloque ou redémarre de façon inattendue 569
Le même nom d'utilisateur en possède plusieurs WorkSpace, mais l'utilisateur ne peut se connecter qu'à l'un des WorkSpaces 569
Je ne parviens pas à utiliser Docker avec Amazon WorkSpaces 571
Je reçois ThrottlingException des erreurs lors de certains de mes appels d'API 571
Je WorkSpace continue de me déconnecter quand je le laisse fonctionner en arrière-plan .. 573
La fédération SAML 2.0 ne fonctionne pas. Mes utilisateurs ne sont pas autorisés à streamer leur WorkSpaces ordinateur de bureau. 573
Mes utilisateurs sont déconnectés de leur WorkSpaces session toutes les 60 minutes. 573
Mes utilisateurs reçoivent une erreur d'URI de redirection lorsqu'ils se fédérent 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. 574
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. 574
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. 574
Les utilisateurs reçoivent le message suivant : « The client and the server cannot communicate, because they do not possess a common algorithm ». 575
Mon microphone ou ma webcam ne fonctionnent pas sous Windows WorkSpaces. 575
Mes utilisateurs ne peuvent pas se connecter à l'aide de l'authentification basée sur des certificats et sont invités à saisir le mot de passe soit sur le WorkSpaces client, soit sur l'écran de connexion Windows lorsqu'ils se connectent à leur session de bureau. 575
J'essaie de faire quelque chose qui nécessite un support d'installation Windows mais qui WorkSpaces ne le fournit pas. 577
Je souhaite lancer WorkSpaces avec un annuaire AWS géré existant créé dans une WorkSpaces région non prise en charge. 577
Je souhaite mettre à jour Firefox sur Amazon Linux 2. 578
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 580
Fin de vie du client Amazon WorkSpaces 582
Clients non pris en charge 584
Question fréquentes concernant la fin de vie (EOL) 585
J'utilise une version d'un client WorkSpaces qui a atteint sa fin de vie. Que dois-je faire pour passer à une version prise en charge ? 585
Puis-je utiliser une version du client WorkSpaces qui a atteint sa fin de vie avec un client WorkSpace compatible ? 585
J'utilise une version d'un client WorkSpaces qui a atteint sa fin de vie. Puis-je tout de même signaler des problèmes à son sujet ? 585
J'utilise une version de client WorkSpaces compatible sur un système d'exploitation qui a atteint sa fin de vie. Puis-je tout de même signaler des problèmes à son sujet ? 585
Quotas 587
Notes de mise à jour 592
Guide du développeur du kit SDK d'extension 599
Historique de la documentation 600

Mises à jour antérieures 608
..... dcxii

Qu'est-ce qu'Amazon WorkSpaces ?

Amazon vous WorkSpaces permet de fournir des bureaux Microsoft Windows, Amazon Linux ou Ubuntu Linux virtuels basés sur le cloud pour vos utilisateurs, connus sous WorkSpacesle nom de. 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.

Pour plus d'informations, consultez Amazon WorkSpaces.

Fonctionnalités

- Choisissez votre système d'exploitation (Windows, Amazon Linux, Ubuntu Linux), puis faites votre choix parmi les configurations matérielles, logicielles, et les régions AWS. Pour plus d'informations, consultez Amazon WorkSpaces Bundles etthe section called “Création d'une image et d'un bundle personnalisés”.
- Choisissez votre protocole : PCoIP ou WorkSpaces Streaming Protocol (WSP). Pour plus d’informations, consultez Protocoles pour Amazon WorkSpaces.
- Connectez-vous à votre WorkSpace compte et reprenez là où vous vous êtes arrêté. WorkSpacesfournit une expérience de bureau persistante.
- WorkSpaces offre la flexibilité d'une facturation mensuelle ou horaire pour WorkSpaces. Pour plus d'informations, consultez la section WorkSpaces Tarification.
- Pour les bureaux Windows, vous pouvez apporter vos propres licences et applications, ou les acheter sur AWS Marketplace for Desktop Apps.
- Créez un annuaire géré autonome pour vos utilisateurs ou connectez-le WorkSpaces à votre annuaire local afin que vos utilisateurs puissent utiliser leurs informations d'identification existantes pour accéder facilement aux ressources de l'entreprise. Pour plus d’informations, consultez Annuaires.
- 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 de disque et les instantanés de volumes.

- Contrôlez les adresses IP à partir desquelles les utilisateurs sont autorisés à accéder à leur WorkSpaces.

Architecture

Pour Windows et Linux WorkSpaces, 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 plus d'informations, consultez the section called "Exigences du VPC". Les annuaires sont gérés via l'annuaire AWS Directory Service qui offre les options suivantes : Simple AD, AD Connector ou AWS Directory Service pour Microsoft Active Directory, plus connu sous le nom de AWS Managed Microsoft AD. Pour plus d'informations, consultez le Guide d'administration AWS Directory Service.

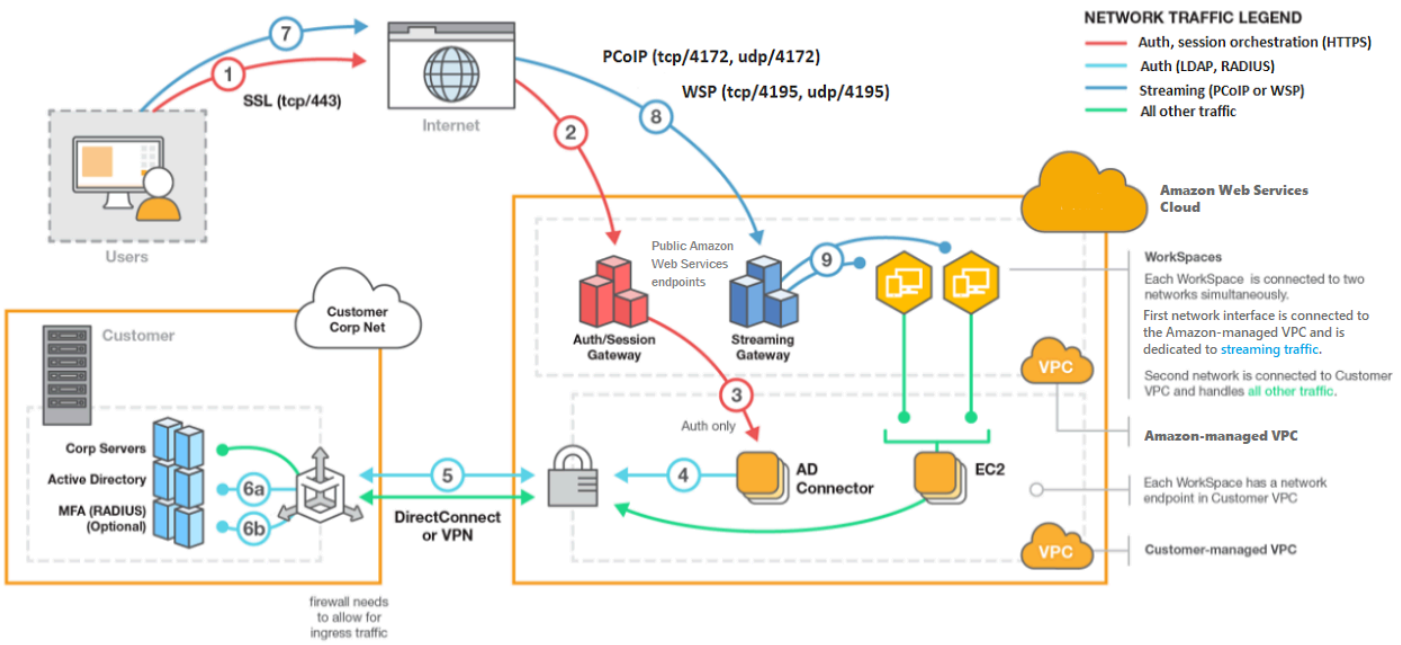
WorkSpaces utilise votre répertoire Simple AD, AD Connector ou AWS Managed Microsoft AD pour authentifier les utilisateurs. Les utilisateurs y WorkSpaces accèdent à l'aide d'une application cliente à partir d'un appareil compatible ou, pour Windows WorkSpaces, d'un navigateur Web, et ils se connectent 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 (WSP) pour le streaming de pixels vers les ports 4172 WorkSpace et 4195 pour les contrôles de santé du réseau. Pour plus d'informations, consultez 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 plus d'informations, consultez Interfaces réseau.

Le schéma suivant montre l'architecture de WorkSpaces.

Amazon WorkSpaces Architectural Diagram



Accédez à votre WorkSpace

Vous pouvez vous connecter à votre en WorkSpaces utilisant l'application client d'un appareil compatible à l'aide d'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
- Les appareils client plume (Les appareils client plume Teradici ne sont pris en charge qu'avec PCoIP.)

Sur les PC Windows, macOS et Linux, 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.

Tarification

Après votre inscriptionAWS, vous pouvez commencer WorkSpaces gratuitement en utilisant l'offre de niveau WorkSpaces gratuit. Pour plus d'informations, consultez la section WorkSpaces Tarification.

Avec WorkSpaces, vous ne payez que pour ce que vous utilisez. Vous êtes débité en fonction du pack et du numéro de celui-ci WorkSpaces que vous lancez. La tarification WorkSpaces inclut l'utilisation de Simple AD et d'AD Connector, mais pas celle de AWS Managed Microsoft AD.

WorkSpaces fournit une facturation mensuelle ou horaire pour WorkSpaces. Avec la facturation mensuelle, vous payez des frais fixes pour une utilisation illimitée, ce qui est préférable pour les utilisateurs qui utilisent leur temps WorkSpaces plein. Avec la facturation horaire, vous payez une petite redevance mensuelle fixe par personne WorkSpace, plus un faible taux horaire pour chaque heure de WorkSpace fonctionnement. Pour plus d'informations, consultez la section WorkSpaces Tarification.

Pour plus d'informations sur les régions prises en charge, consultez la section WorkSpaces Tarification.

Comment démarrer

Pour créer un WorkSpace, essayez l'un des didacticiels suivants :

- Mise en route avec la configuration rapide

- Lancement d'une instance WorkSpace avec AWS Managed Microsoft AD
- Lancement d'une instance WorkSpace avec Simple AD
- Lancement d'une instance WorkSpace avec AD Connector
- Lancement d'une instance WorkSpace avec un domaine approuvé

Vous pouvez également consulter ces ressources pour en savoir plus sur Amazon WorkSpaces :

- Mise en service de bureaux dans le cloud
- Bonnes pratiques pour le déploiement d'Amazon WorkSpaces
- WorkSpaces Ressources Amazon : inclut des livres blancs, des articles de blog, des webinaires et des sessions re:Invent
- WorkSpaces FAQ Amazon

Mise en route avec la configuration rapide

Dans ce didacticiel, vous apprendrez comment allouer un bureau virtuel Microsoft Windows, Amazon Linux ou Ubuntu basé sur le cloud, également appelé instance WorkSpace, avec WorkSpaces et AWS Directory Service.

Ce didacticiel utilise l'option de configuration rapide pour lancer votre instance WorkSpace. Cette option est disponible uniquement si vous n'avez jamais lancé une instance WorkSpace. Sinon, consultez Lancement d'un bureau virtuel avec WorkSpaces.

> **Note**
>
> À l'heure actuelle, la configuration rapide est prise en charge uniquement dans les régions AWS suivantes :
>
> - USA Est (Virginie du Nord)
> - USA Ouest (Oregon)
> - Europe (Irlande)
> - Asie-Pacifique (Singapour)
> - Asie-Pacifique (Sydney)
> - Asie-Pacifique (Tokyo)
>
> Pour modifier votre région, consultez Choisir une région.

Tâches

- Avant de commencer
- En quoi consiste la configuration rapide
- Étape 1 : Lancer l'instance WorkSpace
- Étape 2 : Se connecter à l'instance 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 compte AWS pour créer ou gérer une instance WorkSpace. Les utilisateurs n'ont pas besoin d'un compte AWS pour se connecter à leurs instances WorkSpaces et les utiliser.
- WorkSpaces n'est pas disponible dans toutes les régions. Vérifiez celles prises en charge et sélectionnez une région pour vos instances WorkSpaces. Pour plus d'informations sur les régions prises en charge, consultez la Tarification WorkSpaces par région AWS.

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

- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner un bundle d'instance WorkSpace. Pour plus d'informations, consultez Offres Amazon WorkSpaces et Tarification Amazon WorkSpaces.
- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner le protocole que vous souhaitez utiliser avec votre offre groupée (PCoIP ou WSP [WorkSpaces Streaming Protocol]). Pour plus d'informations, consultez Protocoles pour Amazon WorkSpaces.
- Lorsque vous lancez une instance WorkSpace, vous devez spécifier les informations de profil de l'utilisateur, y compris le nom d'utilisateur et l'adresse e-mail. Les utilisateurs achèvent leurs profils en spécifiant un mot de passe. Les informations sur les instances WorkSpaces et les utilisateurs sont stockées dans un annuaire. Pour plus d'informations, consultez Annuaires.

En quoi consiste la configuration rapide

La configuration rapide exécute les tâches suivantes à votre place :

- Crée un rôle IAM pour permettre au service WorkSpaces de créer des interfaces réseau Elastic et de répertorier vos annuaires WorkSpaces. 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 Configurer un VPC pour WorkSpaces, puis suivez les étapes décrites dans l'un des didacticiels répertoriés dans Lancement d'un bureau virtuel avec WorkSpaces. Choisissez le didacticiel qui correspond au type d'annuaire Active Directory que vous souhaitez utiliser.

- Configure un annuaire Simple AD dans le VPC et l'active pour Amazon WorkDocs. Cet annuaire Simple AD est utilisé pour stocker les informations relatives aux utilisateurs et aux instances WorkSpaces. Le premier Compte AWS créé par la configuration rapide est le Compte AWS de l'administrateur. † 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 spécifiés et les ajoute à l'annuaire.
- Crée les instances WorkSpaces. Chaque instance WorkSpace reçoit une adresse IP publique pour fournir un accès Internet. Le mode d'exécution est AlwaysOn. Pour plus d'informations, consultez Gestion du mode d'exécution d'une instance WorkSpace.
- 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.

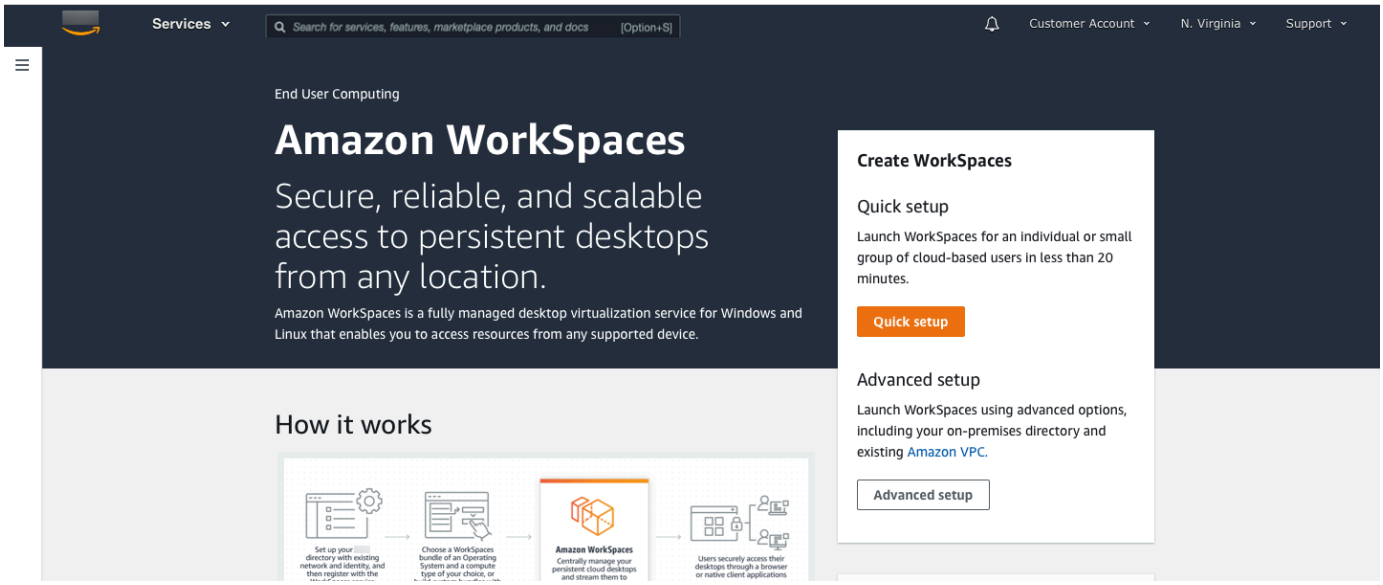
† Le premier Compte AWS créé par la configuration rapide est le Compte AWS de l'administrateur. Vous ne pouvez pas mettre à jour ce Compte AWS à partir de la console WorkSpaces. Ne partagez pas les informations relatives à ce compte avec d'autres personnes. Pour inviter d'autres utilisateurs à utiliser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

Étape 1 : Lancer l'instance WorkSpace

Avec la configuration rapide, vous pouvez lancer votre première instance WorkSpace en quelques minutes.

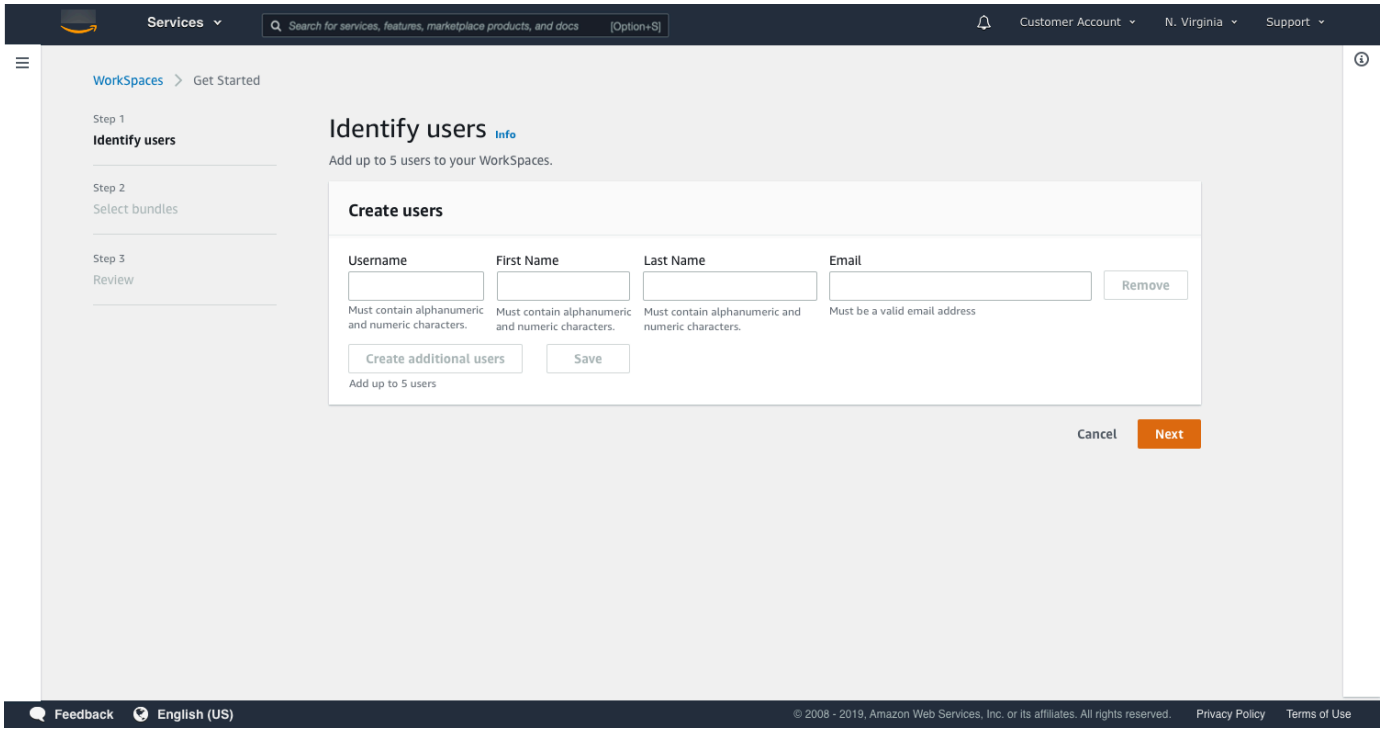
Pour lancer une instance WorkSpace

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Choisissez Configuration rapide. Si vous ne voyez pas ce bouton, soit vous avez déjà lancé une instance WorkSpace dans cette région, soit vous n'utilisez pas l'une des régions où la configuration rapide est prise en charge. Dans ce cas, consultez Lancement d'un bureau virtuel avec WorkSpaces.

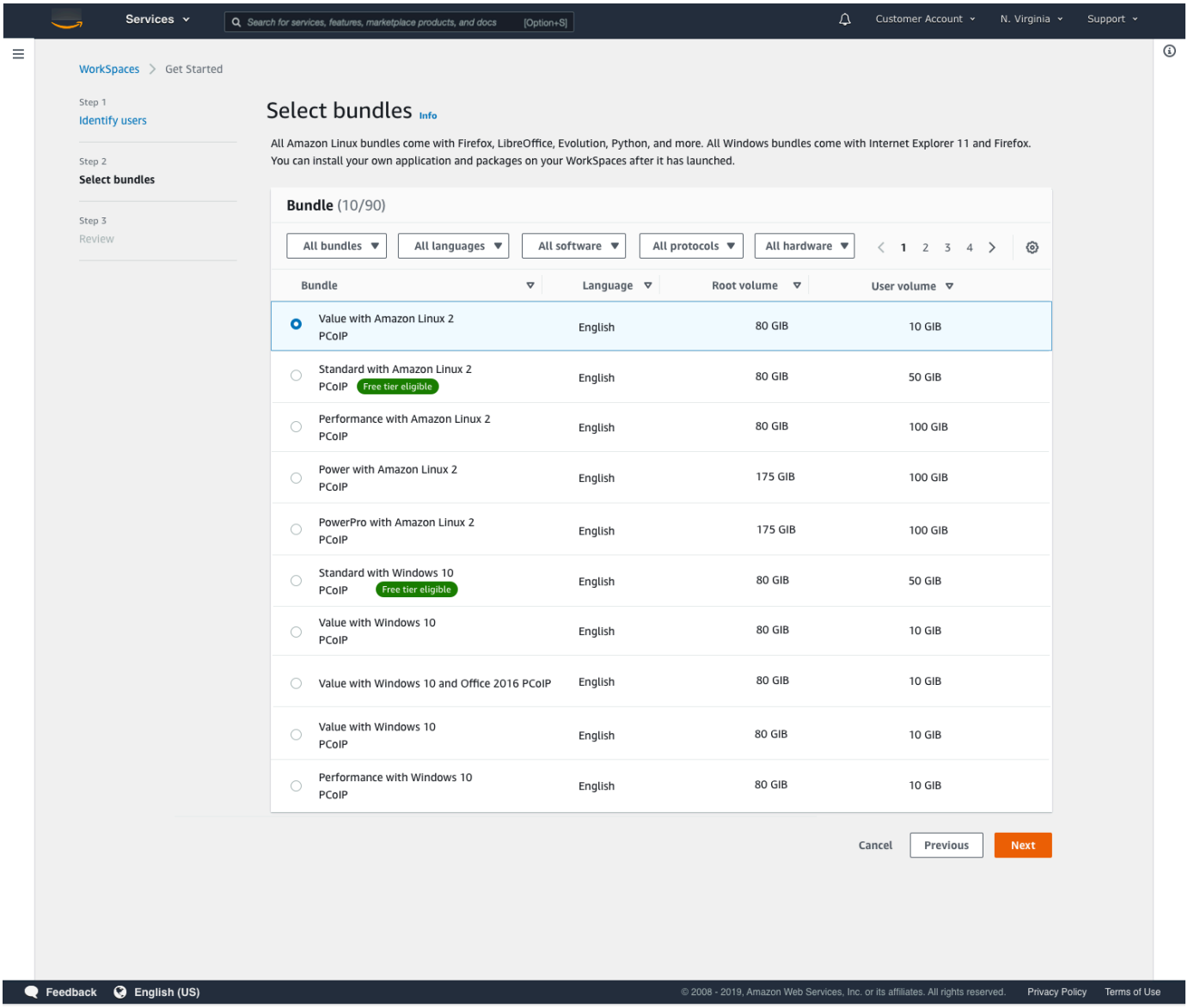


3. Pour Identifier des utilisateurs, entrez le nom d'utilisateur, prénom nom de famille et l'adresse e-mail. Ensuite, sélectionnez Suivant.

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



4. Pour Offres groupées, sélectionnez une offre groupée (matériel et logiciel) pour l'utilisateur, avec le protocole approprié (PCoIP ou WSP). Pour plus d'informations sur les différentes offres groupées publiques disponibles pour les instances WorkSpaces, consultez Offres Amazon WorkSpaces.



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

   Une fois l'annuaire créé et son statut passé à `ACTIVE`, vous pouvez sélectionner Espaces de travail dans le volet de navigation de gauche pour suivre la progression du processus de lancement de l'instance WorkSpace. Le statut initial de l'instance 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 : Se connecter à l'instance WorkSpace

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

Pour se connecter à l'instance 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. Retenez le mot de passe que vous avez spécifié car vous en aurez besoin pour vous connecter à votre instance 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 Clients WorkSpaces dans le Guide de l'utilisateur Amazon WorkSpaces 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 aucune invite ne s'affiche et que vous n'avez pas déjà installé d'application client, ouvrez https://clients.amazonworkspaces.com/ et téléchargez l'une des applications client, ou lancez Web Access.

   > **Note**
   >
   > Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter aux instances WorkSpaces Amazon Linux.

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 client, comme la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez Clients WorkSpaces et Prise en charge des périphériques dans le Guide de l'utilisateur Amazon WorkSpaces.

Étape 3 : Nettoyer (Facultatif)

Lorsque vous avez terminé avec l'instance WorkSpace que vous avez créée pour ce didacticiel, vous pouvez la supprimer. Pour plus d'informations, consultez the section called “Suppression d'une instance WorkSpace”.

> **Note**
>
> Simple AD est mis gratuitement à disposition pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire Simple AD pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.
> Pour supprimer des annuaires vides, consultez Suppression de l'annuaire des instances WorkSpaces. Si vous supprimez l'annuaire Simple AD, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Étapes suivantes

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

- Création d'une WorkSpaces image personnalisée et d'un bundle
- Administrez votre WorkSpaces
- Gestion des annuaires pour les instances WorkSpaces

Pour créer des instances WorkSpaces supplémentaires, effectuez l'une des actions suivantes :

- Si vous souhaitez continuer à utiliser le VPC et l'annuaire Simple AD créés dans le cadre de la configuration rapide, vous pouvez ajouter des instances WorkSpaces pour d'autres utilisateurs en suivant les étapes décrites dans la section Étape 2 : Créer une instance WorkSpace du didacticiel Lancement d'une instance WorkSpace à l'aide de Simple AD.
- Si vous devez utiliser un autre type d'annuaire ou un annuaire Active Directory existant, consultez le didacticiel approprié dans Lancement d'un bureau virtuel avec WorkSpaces.

Pour plus d'informations sur l'utilisation des applications client WorkSpaces, comme la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez Clients WorkSpaces et Prise en charge des périphériques dans le Guide de l'utilisateur Amazon WorkSpaces.

Mise en route avec la configuration avancée d'instances WorkSpaces

Dans ce didacticiel, vous apprendrez comment allouer un bureau virtuel Microsoft Windows ou Amazon Linux basé sur le cloud, également appelé instance WorkSpace, avec WorkSpaces et AWS Directory Service.

Ce didacticiel utilise l'option de configuration avancée pour lancer une instance WorkSpace.

> **Note**
>
> WorkSpaces prend en charge la configuration avancée dans toutes les régions.

Tâches

- Avant de commencer
- Utilisation de la configuration avancée pour lancer une instance WorkSpace

Avant de commencer

Avant de commencer, assurez-vous de disposer d'un compte AWS que vous pouvez utiliser pour créer ou administrer une instance WorkSpace. Les utilisateurs n'ont pas besoin d'un compte AWS pour se connecter à leurs instances WorkSpaces et les utiliser.

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

- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner un bundle d'instance WorkSpace. Pour plus d'informations, consultez Offres Amazon WorkSpaces.
- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner le protocole que vous souhaitez utiliser avec votre offre groupée (PCoIP ou WSP [WorkSpaces Streaming Protocol]). Pour plus d'informations, consultez Protocoles pour Amazon WorkSpaces.
- Lorsque vous lancez une instance WorkSpace, vous devez spécifier les informations de profil de l'utilisateur, y compris le nom d'utilisateur et l'adresse e-mail. Les utilisateurs achèvent leurs profils en spécifiant un mot de passe. Les informations sur les instances WorkSpaces et les utilisateurs sont stockées dans un annuaire. Pour plus d'informations, consultez Annuaires.

Utilisation de la configuration avancée pour lancer une instance WorkSpace

Pour utiliser la configuration avancée afin de lancer une instance WorkSpace :

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Choisissez l'un des types d'annuaire suivants, puis cliquez sur Suivant :

   - AWS Managed Microsoft AD
   - 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.

Mise en réseau et accès concernant les instances WorkSpaces

En tant qu'administrateur d'instance WorkSpace, vous devez comprendre ce qui suit concernant la mise en réseau et l'accès.

Table des matières

- Protocoles pour Amazon WorkSpaces
- Configurer un VPC pour WorkSpaces
- Zones de disponibilité pour Amazon WorkSpaces
- Exigences relatives à l'adresse IP et au port pour WorkSpaces
- Exigences relatives au réseau client Amazon WorkSpaces
- Restreindre WorkSpaces l'accès aux appareils fiables
- Intégration de SAML 2.0 à Amazon WorkSpaces
- Utilisation de cartes à puce pour l'authentification
- Fournissez un accès à Internet depuis votre WorkSpace
- Groupes de sécurité pour votre WorkSpaces
- Groupes de contrôle d'accès IP pour les instances WorkSpaces
- Configuration du client plume PCoIP pour les instances WorkSpaces
- Configuration d'Android pour les Chromebooks
- Activer et configurer Amazon WorkSpaces Web Access
- Configuration d'Amazon WorkSpaces pour l'autorisation FedRAMP ou la conformité SRG pour le Département de la Défense (DoD) des États-Unis
- Activez les connexions SSH pour votre Linux WorkSpaces
- Composants de configuration et de service requis pour WorkSpaces

Protocoles pour Amazon WorkSpaces

Amazon WorkSpaces prend en charge deux protocoles : PCoIP et WorkSpaces Streaming Protocol (WSP). 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.

Prérequis

Les WSP ne WorkSpaces sont pris en charge que si les exigences minimales suivantes sont respectées.

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

Prérequis du client :

- Client natif Windows version 5.1.0.329 ou supérieure
- Client natif macOS version 5.5.0 ou supérieure
- 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 WSP

- Si vous avez besoin d'une tolérance de perte/latence plus élevée pour prendre en charge les conditions de réseau des utilisateurs finaux. 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 WorkSpaces bundle alimenté par Windows Server 2019.
- Si vous devez utiliser Ubuntu WorkSpaces.
- Si vous devez utiliser Windows 11 BYOL WorkSpaces.

- Si vous devez utiliser des bundles basés sur le GPU Ubuntu (Graphics.g4dn et .g4dn). GraphicsPro
- Si vous avez besoin que vos utilisateurs s'authentifient en cours de session avec des WebAuthn authentificateurs tels que YubiKey Windows Hello.

Quand utiliser PCoIP

- Si vous souhaitez utiliser les clients Linux pour iPad ou Android.
- Si vous utilisez des périphériques clients plume Teradici.
- Si vous devez utiliser des ensembles basés sur un processeur graphique (Graphics.G4DN, .g4dn, GraphicsPro Graphics ou). GraphicsPro
- 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 de Chine (Ningxia).

> **Note**
>
> - Un répertoire peut contenir un mélange de PCoIP et de WSP. WorkSpaces
> - Un utilisateur peut avoir à la fois un PCoIP et un WSP WorkSpace tant que les deux WorkSpaces sont situés dans des répertoires distincts. Le même utilisateur ne peut pas avoir de PCoIP et de WSP WorkSpace dans le même répertoire. Pour plus d'informations sur la création de plusieurs WorkSpaces pour un utilisateur, consultezCréation de plusieurs WorkSpaces pour un utilisateur.
> - 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.
> - Si vous avez WorkSpace été créé avec des bundles PCoIP, 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 optimale de visioconférence, nous vous recommandons d'utiliser Power ou des PowerPro offres groupées uniquement.

Configurer un VPC pour 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 pour les VPC et la mise en réseau dans les WorkSpaces déploiements Amazon et les meilleures pratiques pour le déploiement - WorkSpaces Conception de VPC.

Table des matières

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

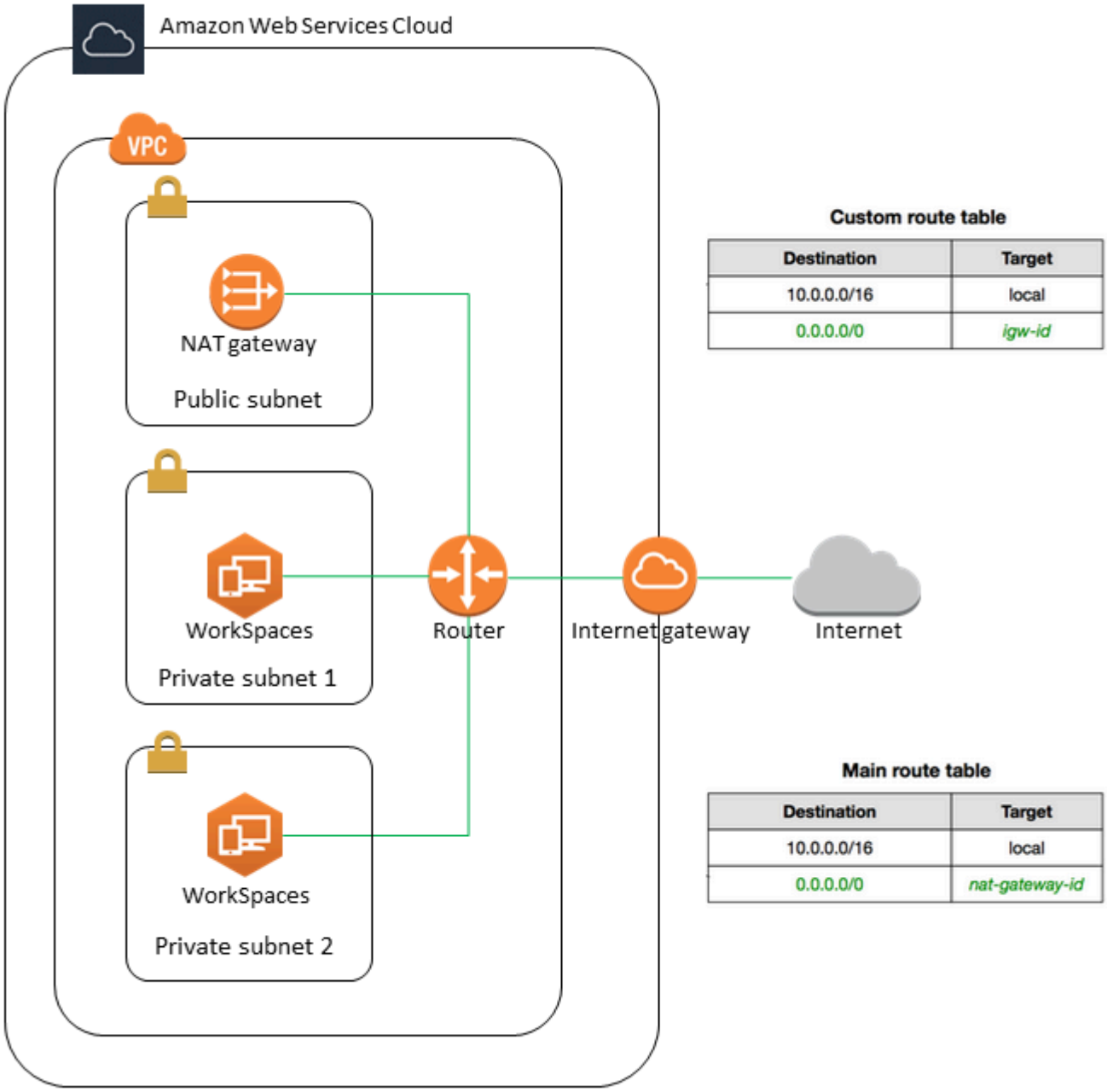
Prérequis

Les sous-réseaux de votre VPC doivent résider dans différentes zones de disponibilité de la région où 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 Amazon WorkSpaces

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

Si vous utilisez AWS Directory Service pour créer un annuaire AWS Managed Microsoft ou Simple AD, nous vous recommandons de configurer le VPC avec un seul 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 les zones de disponibilité, puis sélectionnez celles de votre choix. Sinon, AWS les sélectionne pour vous. Pour effectuer une sélection appropriée, consultez Zones de disponibilité pour Amazon WorkSpaces.

    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).

Blocs d'adresse CIDR IPv6

Vous pouvez associer des blocs d'adresse CIDR IPv6 à votre VPC et à vos sous-réseaux. Toutefois, si vous configurez vos sous-réseaux pour que des adresses IPv6 soient automatiquement affectées aux instances lancées dans le sous-réseau, vous ne pouvez pas utiliser les bundles Graphics. (Vous pouvez toutefois utiliser Graphics.g4dn, GraphicsPro .g4dn et des bundles.) GraphicsPro Cette restriction émane d'une limitation matérielle des types d'instance de la génération précédente qui ne prennent pas en charge IPv6.

Pour contourner ce problème, vous pouvez désactiver temporairement le paramètre d'attribution automatique des adresses IPv6 sur les WorkSpaces sous-réseaux avant de lancer les bundles Graphics, puis réactiver ce paramètre (si nécessaire) après le lancement des bundles Graphics afin que les autres bundles reçoivent les adresses IP souhaitées.

Par défaut, le paramètre auto-assign IPv6 addresses (affecter automatiquement des adresses IPv6) est désactivé. Pour vérifier ce paramètre à partir de la console Amazon VPC, choisissez Sous-réseaux dans le volet de navigation. Sélectionnez le sous-réseau, puis choisissez Actions, Modify auto-assign IP settings (Modifier les paramètres IP d'auto-affectation).

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 les zones de disponibilité, puis sélectionnez celles de votre choix. Sinon, AWS les sélectionne pour vous. Pour effectuer une sélection appropriée, consultez Zones de disponibilité pour Amazon WorkSpaces.
   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).

Blocs d'adresse CIDR IPv6

Vous pouvez associer un bloc d'adresse CIDR IPv6 à votre VPC et à vos sous-réseaux. Toutefois, si vous configurez vos sous-réseaux pour que des adresses IPv6 soient automatiquement affectées aux instances lancées dans le sous-réseau, vous ne pouvez pas utiliser les bundles Graphics. (Vous pouvez toutefois utiliser GraphicsPro des offres groupées.) Cette restriction émane d'une limitation matérielle des types d'instance de la génération précédente qui ne prennent pas en charge IPv6.

Pour contourner ce problème, vous pouvez désactiver temporairement le paramètre d'attribution automatique des adresses IPv6 sur les WorkSpaces sous-réseaux avant de lancer les bundles Graphics, puis réactiver ce paramètre (si nécessaire) après le lancement des bundles Graphics afin que les autres bundles reçoivent les adresses IP souhaitées.

Par défaut, le paramètre auto-assign IPv6 addresses (affecter automatiquement des adresses IPv6) est désactivé. Pour vérifier ce paramètre à partir de la console Amazon VPC, choisissez Sous-réseaux dans le volet de navigation. Sélectionnez le sous-réseau, puis choisissez Actions, Modify auto-assign IP settings (Modifier les paramètres IP d'auto-affectation).

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 un didacticiel vidéo expliquant comment attribuer une adresse IP élastique à un WorkSpace, consultez la vidéo du centre de AWS connaissances Comment associer une adresse IP élastique à un WorkSpace ? .

Pour attribuer une adresse IP publique à WorkSpace un

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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 panneau de navigation, choisissez Adresses IP Elastic. Si vous ne disposez d'aucune adresse IP Elastic disponible, choisissez Allouer une adresse IP Elastic, puis Pool d'adresses IPv4 Amazon ou Pool d'adresses IPv4 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'adresse IPv4 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).

Zones de disponibilité pour Amazon WorkSpaces

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 mappons indépendamment les zones de disponibilité aux noms de chaque compte AWS. Par exemple, la zone de disponibilité `us-east-1a` pour votre compte AWS peut avoir un emplacement autre que `us-east-1a` pour un autre compte AWS.

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` est l'ID de zone de disponibilité de la région `us-east-1` dont l'emplacement est identique dans chaque compte AWS.

Le nom des ID de zone de disponibilité vous 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 les ID de zone de disponibilité que vous pouvez utiliser pour chaque région. Pour voir le mappage des ID de zone de disponibilité aux zones de disponibilité de votre compte, consultez Identifiants de zone de disponibilité pour vos ressources dans le Guide de l'utilisateur AWS RAM.

Nom de la région	Code région	Identifiants de zone de disponibilité pris en charge
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	Identifiants de zone de disponibilité pris en charge
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 régions et les zones de disponibilité, consultez Régions et zones dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

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

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 la région AWS. 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 IP AWS des différentes régions, consultez Plages d'adresses IP AWS dans Référence générale d'Amazon Web Services.

Pour un schéma d'architecture, voir WorkSpaces Architecture. 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 (TCP)

Ce port est utilisé pour les mises à jour d'application client, l'enregistrement et l'authentification. Les client 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 du WorkSpace poste de travail et les contrôles de santé pour PCoIP WorkSpaces. Ce port doit être ouvert à la passerelle PCoIP et aux serveurs de contrôle de santé de la région dans laquelle il se WorkSpace trouve. Pour plus d'informations, consultez Serveur de surveillance de l'état et Serveurs de passerelle PCoIP.

Pour 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 protocole de WorkSpaces streaming (WSP). WorkSpaces Ce port doit être ouvert aux plages d'adresses IP de la passerelle WSP 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 Serveurs de passerelle WSP.

Pour WSP WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et ultérieure) et l'application cliente macOS (version 5.4 et ultérieure) 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.

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 cela, configuré pour le protocole de WorkSpaces streaming (WSP), ce port est utilisé pour diffuser le trafic du WorkSpaces bureau. Ce port doit être ouvert aux plages d'adresses IP de passerelle WSP. Pour plus d'informations, consultez Serveurs de passerelle WSP.

L'accès Web WSP 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 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.

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/
Mise à jour automatique du client	• https://d2td7dqidlhjx7.cloudfront.net/ • Dans la région AWS GovCloud (ouest des États-Unis) : https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/ WorkSpacesAppCastx 64.xml
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaines: • skylight-client-dshttps://.us-east-1.amazonaws.com • skylight-client-dshttps://.us-west-2.amazonaws.com • skylight-client-dshttps://.ap-south-1.amazonaws.com • skylight-client-dshttps://.ap-northeast-2.amazonaws.com • skylight-client-dshttps://.ap-southeast-1.amazonaws.com • skylight-client-dshttps://.ap-southeast-2.amazonaws.com • skylight-client-dshttps://.ap-northeast-1.amazonaws.com • skylight-client-dshttps://ca-central-1.amazonaws.com • skylight-client-dshttps://.eu-central-1.amazonaws.com • skylight-client-dshttps://.eu-west-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	• skylight-client-dshttps://.eu-west-2.amazonaws.com • skylight-client-dshttps://.sa-east-1.amazonaws.com • skylight-client-dshttps://.af-south-1.amazonaws.com • skylight-client-dshttps://.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
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaines: • ws-client-servicehttps://.us-east-1.amazonaws.com • ws-client-servicehttps://.us-west-2.amazonaws.com • ws-client-servicehttps://.ap-south-1.amazonaws.com • ws-client-servicehttps://.ap-northeast-2.amazonaws.com • ws-client-servicehttps://.ap-southeast-1.amazonaws.com • ws-client-servicehttps://.ap-southeast-2.amazonaws.com • ws-client-servicehttps://.ap-northeast-1.amazonaws.com • ws-client-servicehttps://ca-central-1.amazonaws.com • ws-client-servicehttps://.eu-central-1.amazonaws.com • ws-client-servicehttps://.eu-west-1.amazonaws.com • ws-client-servicehttps://.eu-west-2.amazonaws.com • ws-client-servicehttps://.sa-east-1.amazonaws.com • ws-client-servicehttps://.af-south-1.amazonaws.com • ws-client-servicehttps://.il-central-1.amazonaws.com • Dans la région AWS GovCloud (ouest des États-Unis) :

Catégorie	Domaine ou adresse IP
	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

Catégorie	Domaine ou adresse IP
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/*<région>*/*<ID de l'annuaire>* 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://dyoj3cw6iktvg.cloudfront.net • Asie-Pacifique (Singapour) : https://d1525ef92caquk.cloudfront.net/ • Asie-Pacifique (Sydney) : https://dodwxjr2amr8p.cloudfront.net/

Catégorie	Domaine ou adresse IP
	• Asie-Pacifique (Tokyo) : https://d3v7kcib8ir2e1.cloudfront.net/ • Canada (Centre) : https://d1ebdk07rro1qy.cloudfront.net/ • Europe (Francfort) : https://d39q4y7cndearu.cloudfront.net/ • Europe (Irlande) : https://d2127w6wvrc6l3.cloudfront.net/ • Europe (Londres) : https://df4ahgpxbxqy2.cloudfront.net/ • Amérique du Sud (São Paulo) : https://d2nezqurrjvain.cloudfront.net/ • Afrique (Le Cap) : https://dr6ry0pwaoy23.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/ • Asie-Pacifique (Mumbai) : https://d78hovzzqqtsb.cloudfront.net/

Catégorie	Domaine ou adresse IP
	• 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/ • 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 : https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID> • Graphiques de page de connexion pour le comarquage de niveau annuaire de client :

Catégorie	Domaine ou adresse IP
	workspace-client-assets-pdthttps://.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 : Ne s'applique pas Dans la région AWS GovCloud (USA Est) : • Paramètres d'annuaire de client : https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> • Graphiques de page de connexion pour le comarquage de niveau annuaire de client : workspace-client-assets-pdthttps://.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 : Ne s'applique pas
Service de journal Forrester	https://fls-na.amazon.com/

Catégorie	Domaine ou adresse IP
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 • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin. amazonaws-us-gov.com
Pages de connexion utilisateur	https://<id de l'annuaire>.awsapps.com/ (où <id de l'annuaire> représente 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<directory id>.awsapps.com/directory/<directory id>/(où se trouve le domaine du client)

Catégorie	Domaine ou adresse IP
Agent WS	Domaines: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com • ws-broker-servicehttps://.ap-south-1.amazonaws.com • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com • ws-broker-servicehttps://.ap-southeast-1.amazonaws.com • ws-broker-servicehttps://.ap-southeast-2.amazonaws.com • ws-broker-servicehttps://.ap-northeast-1.amazonaws.com • ws-broker-servicehttps://ca-central-1.amazonaws.com • ws-broker-servicehttps://.eu-central-1.amazonaws.com • ws-broker-servicehttps://.eu-west-1.amazonaws.com • ws-broker-servicehttps://.eu-west-2.amazonaws.com • ws-broker-servicehttps://.sa-east-1.amazonaws.com • ws-broker-servicehttps://.af-south-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	• ws-broker-servicehttps://.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

Catégorie	Domaine ou adresse IP
WorkSpaces Points de terminaison de l'API	Domaines: • 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.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

Catégorie	Domaine ou adresse IP
	• 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

Catégorie	Domaine ou adresse IP
WorkSpaces Points de terminaison pour l'authentification unique (SSO) SAML	Domaines: • euc-sso-smhttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-central-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.af-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.il-central-1.amazonaws.com/v1/report-heartbeat • https ://euc-sso-sm. us-gov-west-1.amazonaws.com/v1/report-heartbeat • https ://euc-sso-sm-fips. us-gov-west-1.amazonaws.com/v1/report-heartbeat

Catégorie	Domaine ou adresse IP
	• https ://euc-sso-sm. us-gov-east-1.amazonaws.com/v1/report-heartbeat • https ://euc-sso-sm-fips. us-gov-east-1.amazonaws.com/v1/report-heartbeat

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

Catégorie	Domaine ou adresse IP
PCoIP Session Gateway (PSG)	Serveurs de passerelle PCoIP
Session Broker (PCM)	Domaines: • https://skylight-cm.us-east-1.amazonaws.com • skylight-cm-fipshttps://.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • skylight-cm-fipshttps://.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • 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

Catégorie	Domaine ou adresse IP
	• 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.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
Serveurs TURN de l'accès Web pour PCoIP	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 protocole de WorkSpaces streaming (WSP)

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

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 PCoIP suivants.

Région	Nom d'hôte de vérification de l'état	Adresses IP
USA Est (Virginie du Nord)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
USA Ouest (Oregon)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
Asie-Pacifique (Mumbai)	drp-bom.amazonworkspaces.com	13,127,57,82 13,234,250,73
Asie-Pacifique (Séoul)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105

Région	Nom d'hôte de vérification de l'état	Adresses IP
		52.78.44.253 52.79.54.102
Asie-Pacifique (Singapour)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
Asie-Pacifique (Sydney)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
Asie-Pacifique (Tokyo)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
Canada (Centre)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
Europe (Francfort)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227

Région	Nom d'hôte de vérification de l'état	Adresses IP
Europe (Irlande)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224
Europe (Londres)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
Amérique du Sud (São Paulo)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
Afrique (Le Cap)	drp-cpt.amazonworkspaces.com/	13,244,128,155 13,245,205,255 13,245216,116
Israël (Tel Aviv)	drp-tlv.amazonworkspaces.com/	51,17,52,90 51,17,109,231 51,16,190,43

Région	Nom d'hôte de vérification de l'état	Adresses IP
AWS GovCloud (US-Ouest)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88
AWS GovCloud (USA Est)	drp-osu.amazonworkspaces.com	18,253,251,70 18,254,0,118

Serveurs de passerelle PCoIP

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 plage d'adresses IPv4 publiques Amazon EC2. Cela vous permet de définir des stratégies de pare-feu plus précises pour les appareils qui accèdent à WorkSpaces. Notez que les WorkSpaces clients ne prennent pas en charge les adresses IPv6 comme option de connectivité pour le moment.

Région	Plage d'adresses IP publiques
USA Est (Virginie du Nord)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
USA Ouest (Oregon)	35,80,88,0 - 35,80,95,255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255

Région	Plage d'adresses IP publiques
Asie-Pacifique (Mumbai)	13,126,243,0 - 13,126,243,255
Asie-Pacifique (Séoul)	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
Asie-Pacifique (Singapour)	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255 52.76.127.0 - 52.76.127.255
Asie-Pacifique (Sydney)	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
Asie-Pacifique (Tokyo)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
Canada (Centre)	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
Europe (Francfort)	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
Europe (Irlande)	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255

Région	Plage d'adresses IP publiques
Europe (Londres)	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
Amérique du Sud (São Paulo)	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255
Afrique (Le Cap)	13,246,120,0 - 13,246,123,255
Israël (Tel Aviv)	51,17,28,0-51,17,31,255
AWS GovCloud (US-Ouest)	52.61.193.0 - 52.61.193.255
AWS GovCloud (USA Est)	18,254,140,0 - 18,254,143,255

Serveurs de passerelle WSP

> **Important**
>
> À compter de juin 2020, WorkSpaces diffuse la session de bureau de WSP WorkSpaces aux clients via le port 4195 au lieu du port 4172. Si vous souhaitez utiliser WSP WorkSpaces, assurez-vous que le port 4195 est ouvert au trafic.

WorkSpaces utilise une petite plage d'adresses IPv4 publiques Amazon EC2 pour ses serveurs de passerelle WSP. Cela vous permet de définir des stratégies de pare-feu plus précises pour les appareils qui accèdent à WorkSpaces. Notez que les WorkSpaces clients ne prennent pas en charge les adresses IPv6 comme option de connectivité pour le moment.

Région	Plage d'adresses IP publiques
USA Est (Virginie du Nord)	• 3,227,4,0/22

Région	Plage d'adresses IP publiques
	• 44,209,84,0/22
USA Ouest (Oregon)	34,223,96,0/22
Asie-Pacifique (Mumbai)	65,1156,0/22
Asie-Pacifique (Séoul)	3,35,160,0/22
Asie-Pacifique (Singapour)	13,212,1322,0/22
Asie-Pacifique (Sydney)	3,25,248,0/22
Asie-Pacifique (Tokyo)	3,1114,164,0/22
Canada (Centre)	3,97,20,0/22
Europe (Francfort)	18,2192.216,0/22
Europe (Irlande)	3,248,176,0/22
Europe (Londres)	18,134,68,0/22
Amérique du Sud (São Paulo)	15,228,64,0/22
Afrique (Le Cap)	13,246,108,0/22
Israël (Tel Aviv)	51,17,72,0/22
AWS GovCloud (US-Ouest)	• 3,32,139,0/24 • 3,30,129,0/24 • 3,30,130,0/23
AWS GovCloud (USA Est)	18,254,148,0/22

Noms de domaine de passerelle WSP

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

Région	Domaine
USA Est (Virginie du Nord)	*.prod.us-east-1.highlander.aws.a2z.com
USA Ouest (Oregon)	*.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
Amérique du Sud (São Paulo)	*.prod.sa-east-1.highlander.aws.a2z.com
Afrique (Le Cap)	*.prod.af-south-1.highlander.aws.a2z.com
Israël (Tel Aviv)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (US-Ouest)	*.prod. us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (USA Est)	*.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 WSP BYOL Windows WorkSpaces, les plages d'adresses IP 54.239.224.0/20 et 10.0.0.0/8 s'appliquent dans 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 WSP 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 plages PCoIP/WSP 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
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

Région	Plage d'adresses IP
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
Europe (Londres)	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

Région	Plage d'adresses IP
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. Utilisé pour la création de la connexion de streaming.
- UDP entrant sur le port 4172. Utilisé pour le streaming des entrées utilisateur sur le protocole PCoIP.
- 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. Utilisés pour établir la connexion du streaming des entrées utilisateur sur le protocole WSP.
- UDP entrant sur le port 8220. Utilisé pour établir la connexion du streaming des entrées utilisateur sur le protocole WSP.
- 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 WSP WorkSpaces lorsque l' WorkSpace hôte est configuré pour utiliser un serveur proxy.
- Communications provenant de l'adresse de bouclage 127.0.01.

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 AWS 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 sur TLS/SSL)
- TCP 1024-65535 - Ports dynamiques pour RPC

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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.us-east-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.us-east-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 : • 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/

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.us-east-1.signin.aws
Dépendance d'inscription (pour les clients Web Access et Teradici PCoIP 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	Domaines: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com
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 • skylight-cm-fipshttps://.us-east-1.amazonaws.com
Serveurs TURN de l'accès Web pour PCoIP	Serveur : • turn:*.us-east-1.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-iad.amazonworkspaces.com

Catégorie	Détails
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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	• 3,227,4,0/22 • 44,209,84,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 :

Catégorie	Détails
	skylight-client-dshttps://.us-west-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.us-west-2.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 : • 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://d18af777lco7lp.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.us-west-2.signin.aws
Dépendance d'inscription (pour les clients Web Access et Teradici PCoIP 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	Domaines: • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com
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 • skylight-cm-fipshttps://.us-west-2.amazonaws.com
Serveurs TURN de l'accès Web pour PCoIP	Serveur : • turn:*.us-west-2.rdn.amazonaws.com
Nom d'hôte de vérification de l'état	drp-pdx.amazonworkspaces.com

Catégorie	Détails
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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	34,223,96,0/22
Nom de domaine de la passerelle WSP	*.prod.us-west-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, 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://d2td7dqidlhjx7.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 :

Catégorie	Détails
	skylight-client-dshttps://.ap-south-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.ap-south-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 : • 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 (Mumbai) : https://d78hovzzqqtsb.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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.ap-south-1 .amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : • https://workspaces.ap-south-1.amazon aws.com
Session Broker (PCM)	Domaine : • https://skylight-cm.ap-south-1.amazo naws.com
Serveurs TURN de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	13,126,243,0 - 13,126,243,255
Plage d'adresses IP des serveurs de passerelle WSP	65,1156,0/22
Nom de domaine de la passerelle WSP	*.prod.ap-south-1.highlander.aws.a2z.com

Catégorie	Détails
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://d2td7dqidlhjx7.cloudfront.net/
Vérification de la connectivité	https://connectivity.amazonworkspaces.com/
Device Metrics (pour les applications WorkSpaces clientes 1.0 et 2.0 et supérieures)	device-metrics-ushttps://-2.amazon.com/
Métriques relatives aux clients (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : skylight-client-dshttps://.ap-northeast-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.ap-northeast-2.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • 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 : • https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • 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 (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'inscription (pour les clients Web Access et Teradici PCoIP 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)

Catégorie	Détails
Agent WS	Domaine : • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com
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 de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	3,35,160,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.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 : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 :

Catégorie	Détails
	• 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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.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 de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	13,212,1322,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.ap-southeast-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.ap-southeast-2.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 : • 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://dwcpoxuuza83q.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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.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 de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	3,25,248,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.ap-northeast-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.ap-northeast-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • 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 : • https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • 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 (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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.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 de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	3,1114,164,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 : skylight-client-dshttps://ca-central-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://ca-central-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 :

Catégorie	Détails
	• 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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://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 de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	3,97,20,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.eu-central-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.eu-central-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 : • 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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.eu-central -1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : • https://workspaces.eu-central-1.amaz onaws.com
Session Broker (PCM)	Domaine : • https://skylight-cm.eu-central-1.ama zonaws.com
Serveurs TURN de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	18,2192.216,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.eu-west-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.eu-west-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • 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 : • https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • 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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.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 de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
Plage d'adresses IP des serveurs de passerelle WSP	3,248,176,0/22
Nom de domaine de la passerelle WSP	*.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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.eu-west-2.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.eu-west-2.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • 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 : • https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • 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 (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'inscription (pour les clients Web Access et Teradici PCoIP 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)

Catégorie	Détails
Agent WS	Domaine : • ws-broker-servicehttps://.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 de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 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 WSP	18,134,68,0/22
Nom de domaine de la passerelle WSP	*.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

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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.sa-east-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.sa-east-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 :

Catégorie	Détails
	• 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/
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.sa-east-1.amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : • https://workspaces.sa-east-1.amazonaws.com

Catégorie	Détails
Session Broker (PCM)	Domaine : • https://skylight-cm.sa-east-1.amazonaws.com
Serveurs TURN de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
Plage d'adresses IP des serveurs de passerelle WSP	15,228,64,0/22
Nom de domaine de la passerelle WSP	*.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/

Catégorie	Détails
Mise à jour automatique du client	https://d2td7dqidlhjx7.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 : skylight-client-dshttps://.af-south-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.af-south-1.amazonaws.com

Catégorie	Détails
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> 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 : • 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/

Catégorie	Détails
Serveurs de surveillance de l'état (DRP)	Serveur de surveillance de l'état
Dépendance d'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.af-south-1 .amazonaws.com
WorkSpaces Points de terminaison de l'API	Domaine : • https://workspaces.af-south-1.amazon aws.com
Session Broker (PCM)	Domaine : • https://skylight-cm.af-south-1.amazo naws.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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 13,246,120,0 - 13,246,123,255
Plage d'adresses IP des serveurs de passerelle WSP	15,228,64,0/22
Nom de domaine de la passerelle WSP	*.prod.af-south-1.highlander.aws.a2z.com

Catégorie	Détails
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://d2td7dqidlhjx7.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 : skylight-client-dshttps://.il-central-1.amazonaws.com
Service de messagerie dynamique (pour les applications WorkSpaces clientes de plus de 3 versions)	Domaine : ws-client-servicehttps://.il-central-1.amazonaws.com
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • 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
	• https://d21ui22avrxoh6.cloudfront.net/prod/<région>/<ID annuaire> Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • 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'inscription (pour les clients Web Access et Teradici PCoIP 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 : • ws-broker-servicehttps://.il-central-1.amazonaws.com

Catégorie	Détails
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
Serveurs TURN de l'accès Web pour PCoIP	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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 51,17,28,0-51,17,31,255
Plage d'adresses IP des serveurs de passerelle WSP	51,17,72,0/22
Nom de domaine de la passerelle WSP	*.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/ .xml WorkSpaces AppCast
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-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
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID>

Catégorie	Détails
	Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • https://s3.amazonaws.com/ workspaces-client-assets /prod/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 : • Ne s'applique pas
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.signin. amazonaws-us-gov.com
Dépendance d'inscription (pour les clients Web Access et Teradici PCoIP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(où se trouve le domaine du client)
Agent WS	Domaine : • https ://ws-broker-service. us-gov-west-1. amazonaws.com • https ://ws-broker-service-fips. us-gov-west-1. amazonaws.com

Catégorie	Détails
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
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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 52.61.193.0 - 52.61.193.255
Plage d'adresses IP des serveurs de passerelle WSP	• 3,32,139,0/24 • 3,30,129,0/24 • 3,30,130,0/23
Nom de domaine de la passerelle WSP	*.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/ .xml WorkSpaces AppCast
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-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
Paramètres d'annuaire	Authentification du client auprès du répertoire des clients avant de se connecter au WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<région>/<ID annuaire> Connexions à partir de clients macOS : • https://d32i4gd7pg4909.cloudfront.net/ Paramètres d'annuaire de client : • https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID>

Catégorie	Détails
	Graphiques de page de connexion pour le comarquage de niveau annuaire de client : • 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 : • Ne s'applique pas
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.signin. amazonaws-us-gov.com
Dépendance d'inscription (pour les clients Web Access et Teradici PCoIP Zero)	https://s3.amazonaws.com
Pages de connexion utilisateur	https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(où se trouve le domaine du client)
Agent WS	Domaine : • https ://ws-broker-service. us-gov-east-1. amazonaws.com • https ://ws-broker-service-fips. us-gov-east-1. amazonaws.com

Catégorie	Détails
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
Plages d'adresses IP publiques des serveurs de passerelle PCoIP	• 18,254,140,0 - 18,254,143,255
Plage d'adresses IP des serveurs de passerelle WSP	18,254,148,0/22
Nom de domaine de la passerelle WSP	*.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

Exigences relatives au réseau client Amazon WorkSpaces

Les utilisateurs WorkSpaces peuvent se connecter à leurs instances WorkSpaces via l'application client d'un appareil pris en charge. Ils peuvent également utiliser un navigateur web pour se connecter aux instances WorkSpaces prenant en charge cette forme d'accès. Pour obtenir la liste des instances WorkSpaces qui prennent en charge l'accès via un navigateur Web, consultez

« Quelles solutions groupées Amazon WorkSpaces prennent en charge Web Access ? » dans Accès client, Web Access et expérience utilisateur.

> **Note**
>
> Un navigateur Web ne peut pas être utilisé pour se connecter à WorkSpaces Amazon Linux.

> **Important**
>
> Depuis le 1er octobre 2020, les clients ne peuvent plus utiliser le client Amazon WorkSpaces Web Access pour se connecter aux instances WorkSpaces Windows 7 personnalisées, ni aux instances WorkSpaces Windows 7 Apportez votre propre licence (BYOL).

Pour fournir aux utilisateurs une bonne expérience avec leurs instances WorkSpaces, vérifiez que leurs appareils client 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 plus d'informations, consultez Exigences relatives à l'adresse IP et au port pour WorkSpaces.
- Pour des performances PCoIP optimales, le temps de propagation aller et retour (RTT) entre le réseau du client et la région dans laquelle se trouvent les instances WorkSpaces doit être inférieure à 100 ms. Si le RTT est compris entre 100 et 200 ms, l'utilisateur peut accéder à l'instance 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 du client WorkSpaces est interrompue.

  Pour optimiser les performances du WSP (WorkSpaces Streaming Protocol), le RTT entre le réseau du client et la région dans laquelle se trouvent les instances WorkSpaces doit être inférieur à 250 ms. Si le RTT est compris entre 250 ms et 400 ms, l'utilisateur peut accéder à l'instance WorkSpace, mais les performances se dégradent.

Pour vérifier le RTT dans les différentes régions AWS depuis votre emplacement, utilisez le test Surveillance de l'état de la connexion Amazon WorkSpaces.

- Pour utiliser des webcams avec WSP, nous recommandons une bande passante de chargement minimale de 1,7 mégabits par seconde.
- Si les utilisateurs accèdent à leurs instances 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 accéder à WorkSpaces via un VPN connecté à votre cloud privé virtuel (VPC). Pour accéder à WorkSpaces à 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.

- Les clients ont besoin d'un accès HTTPS aux ressources WorkSpaces hébergées par le service et par Amazon Simple Storage Service (Amazon S3). Les clients ne prennent pas en charge la redirection vers un proxy au niveau de l'application. L'accès HTTPS est requis pour que les utilisateurs puissent terminer l'enregistrement et accéder à leurs instances WorkSpaces.
- Pour autoriser l'accès depuis des appareils client plume PCoIP, vous devez utiliser un bundle de protocoles PCoIP pour WorkSpaces. Vous devez également activer le protocole NTP (Network Time Protocol) dans Teradici. Pour plus d'informations, consultez Configuration du client plume PCoIP pour les instances WorkSpaces.
- Pour les clients 3.0+, si vous utilisez l'authentification unique (SSO) pour Amazon WorkDocs, vous devez suivre les instructions de la page Authentification unique du Guide d'administration AWS Directory Service.

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 le client WorkSpaces. 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 Connections (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 le client WorkSpaces. 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 WorkSpaces l'accès aux appareils fiables

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.

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
> - Clients tiers, y compris, mais sans s'y limiter, PCoIP Teradici, les clients RDP et les applications de bureau à distance

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}BEGIN CERTIFICATE-{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 avec RSA, SHA256 avec ECDSA, SHA384 avec ECDSA ou SHA512 avec ECDSA.
- 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Sélectionnez l'annuaire et choisissez Actions, Mettre à jour les détails.
4. Développez Options de contrôle d'accès.
5. Sélectionnez le type d'appareil sous Pour chaque type d'appareil, spécifiez les appareils autorisés à accéder WorkSpaces.
6. Importez jusqu'à deux certificats racines. Pour chaque certificat racine, procédez comme suit :
   a. Choisissez Import (Importer).
   b. Copiez le corps du certificat dans le formulaire.
   c. Choisissez Import (Importer).
7. (Facultatif) 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 PCoIP 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).

Intégration de SAML 2.0 à Amazon WorkSpaces

L'intégration de SAML 2.0 aux instances WorkSpaces pour l'authentification des sessions de bureau permet aux utilisateurs d'employer les méthodes d'authentification et identifiants actuels de leur fournisseur d'identité (IdP) SAML 2.0 via leur navigateur Web par défaut. En utilisant votre IdP pour authentifier les utilisateurs WorkSpaces, vous pouvez protéger les instances WorkSpaces en utilisant des fonctionnalités IdP comme l'authentification multifactorielle et les stratégies d'accès contextuelles.

Flux de travail d'authentification

Les sections suivantes décrivent le flux de travail d'authentification initié par l'application client WorkSpaces, 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 client WorkSpaces. Par exemple, quand les utilisateurs ouvrent l'application client et se connectent.
- Lorsque le flux est initié par l'accès Web WorkSpaces. 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 annuaire WorkSpaces, et les utilisateurs sont autorisés à se servir de l'application WorkSpaces SAML 2.0. Les utilisateurs créent une instance WorkSpace pour leur nom d'utilisateur `user`, dans un annuaire activé pour l'authentification SAML 2.0. En outre, ils installent l'application client WorkSpaces 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 client WorkSpaces sur leurs appareils sans avoir à saisir de code d'enregistrement WorkSpaces. Ils ne se connectent pas à leurs instances WorkSpaces via le flux initié par l'IdP. L'authentification WorkSpaces doit provenir de l'application client.

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

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

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

Le flux Web Access initié par l'IdP permet aux utilisateurs d'enregistrer automatiquement leurs instances WorkSpaces via un navigateur Web sans avoir à saisir de code d'enregistrement WorkSpaces. Ils ne se connectent pas à leurs instances WorkSpaces via le flux initié par l'IdP. L'authentification WorkSpaces doit provenir de Web Access.

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

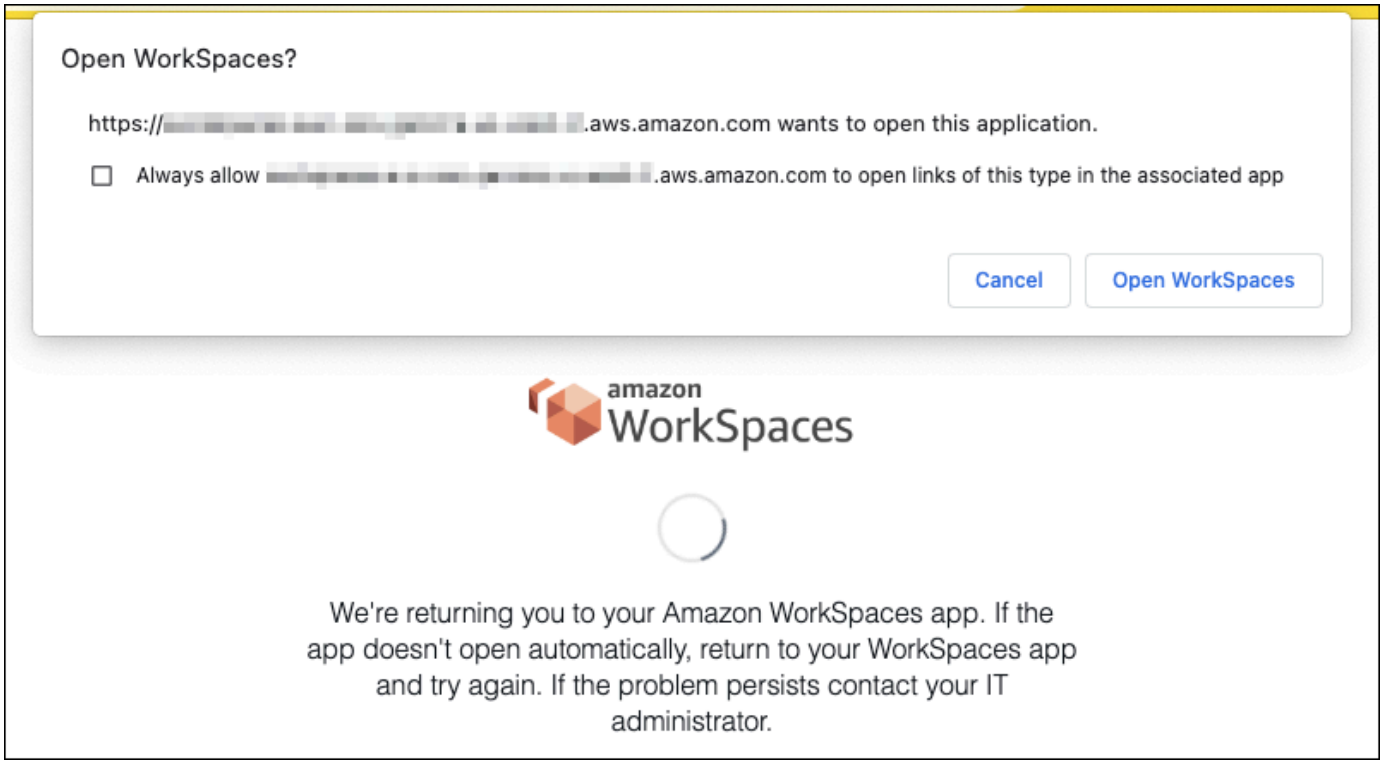
4. L'application client WorkSpaces est désormais enregistrée, et les utilisateurs peuvent continuer à se connecter via WorkSpaces Web Access.

Flux initié par le client WorkSpaces

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

1. Ils lancent l'application client WorkSpaces (si elle n'est pas déjà en cours d'exécution), puis cliquent sur Continuer pour vous 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 client WorkSpaces pour terminer la connexion à leur instance WorkSpace. Les noms d'utilisateur WorkSpaces sont renseignés automatiquement à partir de l'assertion SAML 2.0 de l'IdP. Quand vous utilisez l'authentification par certificat, les utilisateurs sont automatiquement connectés.
5. Les utilisateurs sont connectés à leur instance WorkSpace.

Flux initié par WorkSpaces Web Access

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

1. Ils lancent 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, puis cliquent sur Se connecter à WorkSpaces.
4. Ils sont redirigés vers l'application client WorkSpaces pour terminer la connexion à leur instance WorkSpace. Les noms d'utilisateur WorkSpaces sont renseignés automatiquement à partir de l'assertion SAML 2.0 de l'IdP. Quand vous utilisez l'authentification par certificat, les utilisateurs sont automatiquement connectés.
5. Les utilisateurs sont connectés à leur instance WorkSpace.

Configuration de SAML 2.0

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 succèsAWS.

Table des matières

- Prérequis
- Prérequis
- Étape 1 : Créer un fournisseur d'identité SAML dans AWS IAM
- 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
- Etape 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

Prérequis

- 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 (Francfort)
- 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
  - 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.

Prérequis

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 possédant un WorkSpace, les attributs sAM AccountName et 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.
   - Consultez Intégration de prestataires de solution SAML tiers avec AWS pour plus d'informations sur la configuration d'une fédération AWS. Parmi les exemples pertinents, citons l'intégration d'IdP à AWS IAM pour accéder à la console de gestion AWS.
   - 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 Managed Microsoft AD
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 AWS IAM

Commencez par créer un fournisseur d'identité SAML dans AWS IAM. Cet IdP définit la relation d'approbation de votre organisation entre l'IdP et AWS, à l'aide du document de métadonnées généré par le logiciel d'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 AWSIdentity 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 Identification unique des utilisateurs dans la fédération SAML dans Utilisation de la fédération 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 :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:sub_type": "persistent"
        }
      }
    }
  ]
}
```

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 région AWS, ID de compte et ID d'annuaire. 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS: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 aurez peut-être besoin de le mettre à jour manuellement afin d'approuver AWS en tant que fournisseur de services. Pour ce faire, chargez le fichier `saml-metadata.xml`, disponible à l'adresse https://signin.aws.amazon.com/static/saml-metadata.xml, dans votre IdP. 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' WorkSpacesapplication 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.

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

Ensuite, configurez les informations que l'IdP envoie à AWS comme attributs SAML dans le cadre de la 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. Il s'agit généralement de l'AccountNameattribut SAm 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 le fournisseur d'identité sont spécifiés sous forme d'une paire d'ARN séparés par une virgule. Exemple de la valeur attendue : `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`.
- Élément **`Attribute`** avec l'attribut **`Name`** défini à **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** : cet élément contient un élément `AttributeValue` qui fournit un identifiant pour les informations d'identification temporaires AWS émises pour l'authentification unique (SSO). 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.

- Élément **`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.
- Élément **`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.
- Élément **`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.
- Élément **`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\username``corp.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/:Domain PrincipalTag (facultatif) — 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 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 réussieAWS, 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 Asie-Pacifique (Mumbai)	workspaces.euc-sso.ap-south-1.aws.amazon.com
Région Asia Pacific (Seoul)	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
Région Asie-Pacifique (Singapour)	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
Région Asie-Pacifique (Sydney)	workspaces.euc-sso.ap-southeast-2.aws.amazon.com

Région	Point de terminaison RelayState
Région Asie-Pacifique (Tokyo)	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
Région Canada (Centre)	workspaces.euc-sso.ca-central-1.aws.amazon.com
Région Europe (Francfort)	workspaces.euc-sso.eu-central-1.aws.amazon.com
Région Europe (Irlande)	workspaces.euc-sso.eu-west-1.aws.amazon.com
Région Europe (Londres)	workspaces.euc-sso.eu-west-2.aws.amazon.com
Région Amérique du Sud (São Paulo)	workspaces.euc-sso.sa-east-1.aws.amazon.com
Région Israël (Tel Aviv)	workspaces.euc-sso.il-central-1.aws.amazon.com
AWS GovCloud (US-Ouest)	• espaces de travail.euc-sso. us-gov-west-1. amazonaws-us-gov.com • espaces de travail (FIPS). euc-sso-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).

Région	Point de terminaison RelayState
AWS GovCloud (USA Est)	• espaces de travail.euc-sso. us-gov-east-1. amazonaws-us-gov.com • espaces de travail (FIPS). euc-sso-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).

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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Single Sign-On	`RelayState`	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso`
Okta	`RelayState`	`https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml`
OneLogin	`RelayState`	`https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>`
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>`

Fournisseur d'identité	Paramètre	URL d'accès utilisateur
PingOne pour Enterprise	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?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 la connexion SAML 2.0 sans interrompre votre session actuelle de console de gestion AWS. 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**
>
> PCoIP avec SAML n'est pas pris 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 par certificat

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 ressources AWS Private CA de votre compte AWS. AWS Private CA permet de créer des hiérarchies d'autorités de certification (CA) privées, y compris les CA racine et subordonnées. Avec AWS Private CA, vous pouvez créer votre propre hiérarchie d'autorités de certification et émettre des certificats avec celle-ci pour authentifier les utilisateurs internes. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Private Certificate Authority.

Lorsque vous utilisez AWS Private CA l'authentification basée sur des certificats, WorkSpaces vous demanderez 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 par les packs Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) 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 2.0 et. AppStream WorkSpaces

Prérequis

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 `0bjectSid` dans votre assertion SAML. Cette étape facultative permet de consolider le mappage 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.
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 via AWS Private CA si aucune n'est configurée avec Active Directory. AWS Private CA est obligatoire pour utiliser l'authentification par certificat. Pour plus d'informations, consultez Planification de votre déploiement AWS Private CA et suivez les instructions afin de configurer une autorité de certification pour l'authentification par certificat. Les paramètres AWS Private CA suivants sont les plus courants dans les cas d'utilisation de l'authentification par certificat :
   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 Private CA. Dans ce cas, n'utilisez pas une CA privée configurée pour les certificats de courte durée.

> **Note**
>
> Si vous utilisez AWS Managed Microsoft AD, vous pouvez configurer les services de certificats dans une instance EC2 pour répondre aux exigences des certificats de contrôleur de domaine. Voir par AWS Launch Wizardexemple 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'utilisationAWS Managed Microsoft AD.
> Une tâche de configuration supplémentaire, avec AWS Managed Microsoft AD et les services de certificats Active Directory, consiste à créer des règles sortantes depuis

le groupe de sécurité VPC des contrôleurs vers l'instance EC2 exécutant les services de certificats, en autorisant les ports TCP 135 et 49152-65535 à activer l'inscription automatique des certificats. En outre, l'instance EC2 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 pour AWS Managed Microsoft AD, consultez Configuration de vos groupes de sécurité et sous-réseaux VPC.

- Dans la console AWS Private CA, ou à l'aide du kit SDK ou de l'interface de ligne de commande (CLI), sélectionnez votre CA et sous le certificat de la CA, exportez son certificat privé. 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 la CA. Pour plus d'informations, consultez Instructions de configuration.

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

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 l'autorité de certification aux autorités de certification Trusted Root et les magasins Enterprise NTAuth automatiquement pour les WorkSpaces ordinateurs de bureau lorsqu'ils sont joints au domaine.
> - 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 l'article 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.

Activation de l'authentification par certificat

Procédez comme suit pour activer l'authentification par certificat.

1. Ouvrez la WorkSpaces console à l'adressehttps://console.aws.amazon.com/workspaces.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 ensembles Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) 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 la MFA AWS Directory Service, consultez Authentification multifactorielle (AD Connector) ou Activation de 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 Private CA pour l'authentification WorkSpaces basée sur des certificats ne nécessitent pas de renouvellement ni de révocation. Ces certificats sont de courte durée. WorkSpacesémet automatiquement un nouveau certificat toutes les 24 heures. Ces certificats utilisateur final ont une période de validité plus courte qu'une distribution de CRL AWS Private CA classique. Par conséquent, ils 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 pour votre CA privée.

Journalisation et surveillance

Vous pouvez l'utiliser AWS CloudTrailpour enregistrer les appels d'API vers AWS Private CA by WorkSpaces. Pour plus d'informations, consultez la section Utilisation CloudTrail. Dans l'historique des CloudTrail événements, vous pouvez afficher `GetCertificate` les noms d'`IssueCertificate`événements `acm-pca.amazonaws.com` 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.

Utilisation de cartes à puce pour l'authentification

Les offres Windows et Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) permettent l'utilisation de cartes à puce Common Access Card (CAC) et de Personal Identity Verification (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

- Prérequis
- Limites
- Configuration Active Directory
- Activer les cartes à puce pour Windows WorkSpaces
- Activer les cartes à puce pour Linux WorkSpaces

Prérequis

- 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 ou le client WorkSpaces macOS version 3.1.5 ou ultérieure. 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.

  - 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.

Limites

- Seules l'application cliente WorkSpaces Windows version 3.1.1 ou ultérieure et l'application cliente macOS version 3.1.5 ou ultérieure sont actuellement prises 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.
- Ubuntu WorkSpaces ne prend actuellement pas en charge l'authentification par carte à puce.
- 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 WSP 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 (US-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.
- 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 protocole de streaming WorkSpaces (WSP) 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 nécessite que la partie nom d'utilisateur du compte de service AD Connector corresponde au sAM AccountName du même utilisateur. Un Sam ne AccountName peut pas dépasser 20 caractères.

Configuration d'annuaire sur site

Outre la configuration de l'annuaire AD Connector, vous devez également vous assurer que l'utilisation étendue des clés (EKU) « Authentication KDC » est définie pour les certificats délivrés aux contrôleurs de domaine de votre annuaire sur site. 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.

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 Activation ou désactivation de la déconnexion de session au verrouillage de l'écran pour WSP.

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 Activation ou désactivation de la redirection de carte à puce pour WSP.

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.

Activer les cartes à puce pour Linux WorkSpaces

> **Note**
>
> Linux WorkSpaces sur WSP 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.
> - Vous devez utiliser l'application cliente WorkSpaces Windows pour vous connecter à Linux WorkSpaces sur WSP.

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

Pour obtenir votre certificat de CA racine

Vous pouvez obtenir votre certificat de CA racine de plusieurs façon :

- 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 de CA racine exporté du format DER au format PEM, où *`rootca`* 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 système Linux WorkSpaces

Pour vous aider à activer les cartes à puce, nous avons ajouté le script `enable_smartcard` à nos offres groupées Amazon Linux WSP. 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 d'autorité de certification racine à votre système Linux WorkSpaces et pour activer les cartes à puce pour votre système Linux WorkSpaces.

1. Créez un nouveau Linux WorkSpace avec le protocole WSP activé. Lorsque vous lancez le WorkSpace dans la WorkSpaces console Amazon, sur la page Select Bundles, assurez-vous de sélectionner WSP 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**
   >
   > Linux WorkSpaces suppose que les certificats des 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 sous Linux 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 souhaiterez 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.

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

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.

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 la résolution des problèmes, nous vous recommandons d'ajouter l'utilitaire `pkcs11-tools`. 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_pksc11.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`.

Fournissez un accès à Internet depuis votre WorkSpace

Vous 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 Configurer un VPC pour 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 votre WorkSpaces

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 Groupes de sécurité Amazon EC2 pour les instances Linux ou la page Groupes de sécurité Amazon EC2 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 à l'adresse https://console.aws.amazon.com/workspaces/.
   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 console Amazon EC2 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 autant de fois que nécessaire pour les autres WorkSpaces.

Groupes de contrôle d'accès IP pour les instances WorkSpaces

Amazon WorkSpaces vous permet de contrôler les adresses IP depuis lesquelles les instances WorkSpaces sont accessibles. En utilisant des groupes de contrôle d'accès basés sur les adresses IP, vous pouvez définir et gérer des groupes d'adresses IP fiables, et autoriser les utilisateurs à accéder à leurs instances WorkSpaces uniquement lorsqu'ils sont connectés à un réseau fiable.

Une liste de contrôle d'accès IP agit en tant que pare-feu virtuel qui contrôle les adresses IP à partir desquelles les utilisateurs sont autorisés à accéder à leurs instances 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 associer chaque groupe de contrôle d'accès IP avec un ou plusieurs annuaires. Vous pouvez créer jusqu'à 100 groupes de contrôle d'accès IP par compte AWS. Toutefois, vous pouvez uniquement associer jusqu'à 25 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 inclut une règle par défaut qui permet aux utilisateurs d'accéder à leurs instances 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 accèdent à leurs instances WorkSpaces via une passerelle NAT ou un VPN, vous devez créer des règles qui autorisent le trafic depuis les adresses IP de la passerelle NAT ou du VPN.

Note

- Les groupes de contrôle d'accès IP n'autorisent pas l'utilisation d'adresses IP dynamiques pour les NAT. 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 session WorkSpaces.
- Les groupes de contrôle d'accès IP contrôlent les adresses IP depuis lesquelles les utilisateurs peuvent connecter leurs sessions de streaming aux instances WorkSpaces. À l'aide des API publiques Amazon WorkSpaces, les utilisateurs peuvent toujours exécuter des fonctionnalités, comme le redémarrage, la reconstruction et l'arrêt, depuis n'importe quelle adresse IP.

Vous pouvez utiliser cette fonctionnalité avec l'accès Web, les clients plume PCoIP et les applications client 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 10 règles.

Pour créer un groupe de contrôles d'accès IP

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
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 que l'accès aux instances WorkSpaces a lieu uniquement à partir de réseaux approuvés.

Si vous associez un groupe de contrôle d'accès IP qui ne comporte pas de règles à un annuaire, cela bloque tous les accès à toutes les instances WorkSpaces.

Pour associer un groupe de contrôle d'accès IP à un annuaire

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
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 était utilisée pour autoriser une connexion à une instance WorkSpace, l'utilisateur est déconnecté de cette instance 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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
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.

Configuration du client plume PCoIP pour les instances WorkSpaces

Les clients plume PCoIP ne sont compatibles qu'avec les offres groupées WorkSpaces utilisant le protocole PCoIP.

Si votre appareil client plume exécute la version 6.0.0 ou ultérieure du microprogramme, les utilisateurs peuvent se connecter à leur instance WorkSpaces directement. Lorsque les utilisateurs se connectent directement à leurs instances WorkSpaces à l'aide d'un appareil client plume, nous vous recommandons d'utiliser l'authentification multifactorielle (MFA) avec votre annuaire WorkSpaces. 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)

- 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, le gestionnaire de connexion PCoIP n'est plus pris en charge avec les versions 4.6.0 à 6.0.0 du microprogramme destiné aux appareils client plume. Si la version du microprogramme de votre client plume n'est pas 6.0.0 ou ultérieure, vous pouvez obtenir le dernier microprogramme via un abonnement Desktop Access sur la page https://www.teradici.com/desktop-access.

> **Important**
>
> - Dans l'interface Web d'administration (AWI) PCoIP de Teradici ou la console de gestion (MC) PCoIP 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 NTP n'est pas activé, vos utilisateurs du client plume PCoIP peuvent recevoir des erreurs d'échec de certificat, telles que « Le certificat fourni n'est pas valide en raison de l'horodatage ».
> - Depuis la version 20.10.4 de l'agent PCoIP, Amazon WorkSpaces désactive la redirection USB par défaut via le registre Windows. Ce paramètre de registre affecte le comportement des périphériques USB lorsque les utilisateurs utilisent des appareils client plume PCoIP pour se connecter à leurs instances WorkSpaces. Pour plus d'informations, consultez Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients plume PCoIP.

Pour en savoir plus sur la configuration et la connexion avec un appareil client plume PCoIP, consultez Client plume PCoIP dans le Guide de l'utilisateur Amazon WorkSpaces. Pour obtenir une liste des appareils client plume PCoIP approuvés, consultez PCoIP Zero Clients sur le site Web de Teradici.

Configuration d'Android pour les Chromebooks

La version 2.4.13 est la version finale de l'application client Amazon WorkSpaces Chromebook. Étant donné que Google cesse de prendre en charge les applications Chrome, aucune nouvelle mise à jour

ne sera apportée à l'application client Amazon WorkSpaces Chromebook, et son utilisation n'est pas prise en charge.

Pour les Chromebooks qui prennent en charge l'installation d'applications Android, nous vous recommandons d'utiliser l'application client WorkSpaces Android à la place.

L'installation d'applications Android doit d'abord être activée sur certains Chromebooks lancés avant 2019 pour que les utilisateurs puissent installer l'application client 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 Amazon WorkSpaces Web Access

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**
>
> - L'accès au Web avec WSP pour Windows et Ubuntu WorkSpaces est pris en charge dans toutes les régions où WSP WorkSpaces est disponible. WSP pour Amazon Linux n' WorkSpaces est disponible qu'en AWS GovCloud (ouest des États-Unis).
> - Nous recommandons vivement d'utiliser Web Access avec WSP WorkSpaces pour une qualité de diffusion et une expérience utilisateur optimales. Les limites suivantes s'appliquent à l'utilisation de Web Access avec PCoIP WorkSpaces :
>   - L'accès Web avec PCoIP n'est pas pris en charge en Asie-Pacifique (Mumbai), en Afrique (Le Cap) et en Israël (Tel Aviv) AWS GovCloud (US) Regions
>   - L'accès Web avec PCoIP n'est pris en charge que pour Windows WorkSpaces, pas avec Amazon Linux. WorkSpaces
>   - Web Access n'est pas disponible pour certains systèmes Windows 10 WorkSpaces utilisant le protocole PCoIP. Si vos PCoIP WorkSpaces sont alimentés par Windows Server 2019, Web Access n'est pas disponible.

> **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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 plus d'informations, consultez 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 (GPO) pour appliquer des paramètres afin 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 afin d'utiliser les objets de stratégie de groupe, consultez Installation des outils d'administration Active Directory dans le Guide d'administration AWS Directory Service .

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), Policies (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.

Pour masquer le dernier nom d'utilisateur connecté

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, la liste peut ne pas afficher 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).

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 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 d'Amazon WorkSpaces pour l'autorisation FedRAMP ou la conformité SRG pour le Département de la Défense (DoD) des États-Unis

Pour être en conformité avec le FedRAMP (Federal Risk and Authorization Management Program) ou avec le SRG (Cloud Computing Security Requirements Guide) du Département de la Défense (DoD) des États-Unis, vous devez configurer Amazon WorkSpaces pour utiliser le chiffrement des points de terminaison FIPS (Federal Information Processing Standards) au niveau de l'annuaire. Vous devez également utiliser une région AWS des États-Unis qui dispose de l'autorisation FedRAMP, ou qui est en conformité avec le SRG du Département de la Défense des États-Unis (DoD).

Le niveau d'autorisation FedRAMP (modéré ou élevé) ou le niveau d'impact du SRG du DoD (2, 4 ou 5) dépend de la région AWS des États-Unis dans laquelle Amazon WorkSpaces est utilisé. 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**
>
> Outre l'utilisation du chiffrement des points de terminaisons FIPS, vous pouvez également chiffrer vos instances WorkSpaces. Pour plus d'informations, consultez Instances WorkSpace chiffrées.

Prérequis

- Vous devez créer les instances WorkSpace dans une région AWS des États-Unis qui dispose de l'autorisation FedRAMP ou qui est en conformité avec le SRG du DoD.
- L'annuaire WorkSpaces doit être configuré pour utiliser le Mode validation FIPS 140-2 pour le chiffrement des points de terminaison.

  > **Note**
  >
  > Pour utiliser le paramètre Mode validation FIPS 140-2, l'annuaire WorkSpaces doit être nouveau ou toutes les instances WorkSpaces existantes dans l'annuaire doivent utiliser le Mode validation FIPS 140-2 pour le chiffrement des points de terminaison. Sinon, vous ne pouvez pas utiliser ce paramètre. Les instances WorkSpaces que vous créez ne seront donc pas conformes aux exigences de sécurité du programme FedRAMP ou du DoD.

- Les utilisateurs doivent accéder à leurs instances WorkSpaces à partir de l'une des applications client WorkSpaces suivantes :
  - Windows : 2.4.3 ou version ultérieure
  - macOS : 2.4.3 ou une version ultérieure
  - 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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Vérifiez qu'aucune instance WorkSpace n'est associée à l'annuaire dans lequel vous souhaitez créer des instances WorkSpace autorisées par le programme FedRAMP et conformes au SRG du DoD. Si des instances WorkSpace sont associées à l'annuaire et que l'annuaire n'est pas déjà activé pour utiliser le mode validation FIPS 140-2, arrêtez les instances WorkSpace ou créez un nouvel annuaire.
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 à partir de cet annuaire des instances WorkSpace qui sont autorisées pour FedRAMP et conformes au SRG du DoD. Pour accéder à ces instances WorkSpace, les utilisateurs doivent utiliser l'une des applications client WorkSpaces répertoriées précédemment dans la section Prérequis.

Activez les connexions SSH pour votre Linux WorkSpaces

Si vous ou vos utilisateurs souhaitez vous connecter à votre Amazon 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 Amazon 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.

Table des matières

- Conditions préalables pour les connexions SSH à Amazon Linux WorkSpaces
- Activer les connexions SSH à tous les Amazon Linux WorkSpaces d'un répertoire
- Authentification par mot de passe dans Amazon Linux 2 WorkSpaces
- Activer les connexions SSH à un Amazon Linux spécifique WorkSpace
- Connectez-vous à un Amazon Linux à WorkSpace l'aide de Linux ou PuTTY

Conditions préalables pour les connexions SSH à Amazon Linux WorkSpaces

- Activation du trafic SSH entrant vers un WorkSpace — Pour ajouter une règle autorisant le trafic SSH entrant vers un ou plusieurs Amazon Linux WorkSpaces, assurez-vous de disposer des adresses IP publiques ou privées des appareils nécessitant des connexions SSH à votre. WorkSpaces 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 Amazon 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 de l'Amazon Linux auquel WorkSpace vous souhaitez vous connecter et votre nom d'utilisateur

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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'WorkSpaceadresse IP.
10. Si vous avez WorkSpace une adresse IP publique, elle est affichée dans la colonne IP publique IPv4. Notez cette adresse, le cas échéant.

Pour rechercher le nom NetBIOS du domaine Active Directory auquel vous êtes connecté

1. Ouvrez la AWS 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 Amazon Linux WorkSpaces d'un répertoire

Pour activer les connexions SSH à tous les Amazon Linux WorkSpaces d'un répertoire, procédez comme suit.

Pour créer un groupe de sécurité avec une règle autorisant le trafic SSH entrant vers l'ensemble des Amazon Linux d'un WorkSpaces annuaire

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.

Authentification par mot de passe dans Amazon Linux 2 WorkSpaces

Amazon Linux 2 WorkSpaces lancé avant le 10 novembre 2023 est activé par défaut avec l'authentification par mot de passe SSH. Pour Amazon Linux 2 WorkSpaces lancé après le 10 novembre. 2023, l'authentification par mot de passe SSH est désactivée par défaut.

Pour désactiver l'authentification par mot de passe dans les WorkSpaces instances Amazon Linux 2 existantes

1. Lancez le WorkSpaces client et connectez-vous à votre WorkSpace.
2. Ouvrez la fenêtre Terminal (Application > Outils système > Terminal MATE).
3. Dans la fenêtre Terminal, exécutez la commande suivante.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

Pour activer l'authentification par mot de passe dans les WorkSpaces instances Amazon Linux 2 récemment créées

1. Lancez le WorkSpaces client et connectez-vous à votre WorkSpace.
2. Ouvrez la fenêtre Terminal (Application > Outils système > Terminal MATE).
3. Dans la fenêtre Terminal, exécutez la commande suivante.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

Contrairement à Ubuntu WorkSpaces, Amazon Linux 2 ne conserve pas WorkSpaces par défaut les paramètres d'authentification par mot de passe SSH dans les images personnalisées. Si vous souhaitez activer l'authentification par mot de passe SSH par défaut dans Amazon Linux 2 WorkSpaces provisionné à partir d'une image personnalisée, vous devez également modifier le `/etc/cloud/cloud.cfg` fichier pour supprimer la ligne qui le contient `ssh_pwauth` lors de la création d'une image personnalisée. Pour modifier le fichier `/etc/cloud/cloud.cfg`, exécutez la commande suivante :

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

Activer les connexions SSH à un Amazon Linux spécifique WorkSpace

Pour activer les connexions SSH à un Amazon 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 Amazon 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 adresse IPv4 est `203.0.113.25`, spécifiez `203.0.113.25/32` pour afficher cette seule adresse IPv4 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.

Connectez-vous à un Amazon Linux à WorkSpace l'aide de 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, consultez la section « Conditions requises pour les connexions SSH à Amazon Linux WorkSpaces » plus haut dans cette rubrique.

Pour vous connecter à un Amazon Linux à WorkSpace l'aide de Linux

1. Ouvrez l'invite de commande en tant qu'administrateur, puis entrez la commande suivante : Pour le *nom, le nom d'utilisateur et l'WorkSpace adresse IP NetBIOS*, entrez les valeurs applicables.

   ```
   ssh "NetBIOS_NAME\Username"@WorkSpaceIP
   ```

   Voici un exemple de commande SSH où :

   - Le *NetBIOS_NAME* est anycompany
   - Le *Nom d'utilisateur* est janedoe
   - L'*WorkSpace IP* 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 Amazon 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' WorkSpaceadresse 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

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”

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 la table

de routage doit être modifiée pour votre organisation, contactez AWS Support ou votre équipe de compte AWS avant d'appliquer toute modification.

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`

Agent PCoIP 32 bits

Le 29 mars 2021, nous avons mis à jour l'agent PCoIP de 32 bits à 64 bits. Pour Windows WorkSpaces utilisant le protocole PCoIP, 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 PCoIP 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 effectuez un filtrage sur les chemins d'accès aux composants PCoIP 32 bits, veillez à ajouter les chemins vers les versions 64 bits des composants. Comme vous n' WorkSpaces 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`.

Modification du service d'arbitre PCoIP — Sachez que le service d'arbitre PCoIP (`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.

Clients et périphériques USB PCoIP zéro : à partir de la version 20.10.4 de l'agent PCoIP, WorkSpaces Amazon 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 périphériques PCoIP zéro client pour se connecter à leur. WorkSpaces Pour plus d'informations, consultez Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients plume PCoIP.

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 WorkSpaces.

- `/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
- /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/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

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/X11/xorg.conf
- /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/sssd/sssd.conf
- /etc/wsp
- /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/lib/systemd/system/xdcv-console-update.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/share/X11
- /var/lib/skylight

- `/var/log/skylight`

Gestion des annuaires pour les instances WorkSpaces

WorkSpaces utilise un annuaire pour stocker et gérer les informations des instances WorkSpaces et des 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 leurs instances WorkSpaces à l'aide de leurs informations d'identification sur site, et accéder aux ressources sur site à partir de leurs instances WorkSpaces.
- AWS Managed Microsoft AD : créez un annuaire Microsoft Active Directory hébergé sur AWS.
- Simple AD : créez un annuaire compatible avec Microsoft Active Directory, optimisé par Samba 4 et hébergé sur AWS.
- Approbation croisée : créez une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site.

Pour consulter des didacticiels qui expliquent comment configurer ces annuaires et lancer des instances WorkSpaces, consultez Lancement d'un bureau virtuel avec WorkSpaces.

> **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 Bonnes pratiques de déploiement Amazon WorkSpaces (langue française non garantie).

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 exécuter certaines tâches d'administration d'annuaire avec la console WorkSpaces, et d'autres tâches à l'aide d'une stratégie de groupe. Pour de plus amples informations sur la gestion des utilisateurs et des groupes, veuillez consulter Gestion des utilisateurs d'instances WorkSpaces et Configuration des outils d'administration Active Directory pour WorkSpaces.

> **Note**
>
> - Actuellement, les annuaires partagés ne sont pas pris en charge par Amazon WorkSpaces.
> - Si vous configurez un annuaire AWS Managed Microsoft AD pour une réplication sur plusieurs régions, seul l'annuaire de la région principale peut être enregistré pour être

utilisé avec Amazon WorkSpaces. Toute tentative d'enregistrement de l'annuaire dans une région répliquée pour une utilisation avec Amazon WorkSpaces est vouée à l'échec. La réplication sur plusieurs régions 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 gratuitement à votre disposition pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire Simple AD ou AD connector pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.

  Pour supprimer des annuaires vides, consultez Suppression de l'annuaire des instances WorkSpaces. Si vous supprimez votre annuaire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Table des matières

- Enregistrement d'un annuaire avec WorkSpaces
- Mettez à jour les détails du répertoire pour votre WorkSpaces
- Mise à jour des serveurs DNS pour Amazon WorkSpaces
- Suppression de l'annuaire des instances WorkSpaces
- Activation d'Amazon WorkDocs pour AWS Managed Microsoft AD
- Configuration des outils d'administration Active Directory pour WorkSpaces

Enregistrement d'un annuaire avec WorkSpaces

Pour autoriser les instances WorkSpaces à utiliser un annuaire AWS Directory Service existant, vous devez enregistrer ce dernier auprès de WorkSpaces. Après avoir enregistré un annuaire, vous pouvez y lancer des instances WorkSpaces.

Prérequis

Pour enregistrer un annuaire à utiliser avec les instances WorkSpaces, il doit répondre aux exigences suivantes :

- Si vous utilisez AWS Managed Microsoft AD ou Simple AD, votre annuaire peut se trouver sur un sous-réseau privé dédié, à condition qu'il ait accès au cloud privé virtuel (VPC) où se trouvent les instances 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 gratuitement à votre disposition pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire Simple AD ou AD connector pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.
> Pour supprimer des annuaires vides, consultez Suppression de l'annuaire des instances WorkSpaces. Si vous supprimez votre annuaire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Pour enregistrer un annuaire

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Sélectionnez l'annuaire.
4. Choisissez Actions, Enregistrer.

> **Note**
>
> - Actuellement, les annuaires partagés ne sont pas pris en charge par Amazon WorkSpaces.
> - Si l'annuaire AWS Managed Microsoft AD a été configuré pour une réplication sur plusieurs régions, seul l'annuaire de la région principale peut être enregistré pour être utilisé avec Amazon WorkSpaces. Toute tentative d'enregistrement de l'annuaire dans une région répliquée pour une utilisation avec Amazon WorkSpaces est vouée à l'échec. La réplication sur plusieurs régions avec AWS Managed Microsoft AD n'est

pas prise en charge pour une utilisation avec Amazon WorkSpaces dans les régions répliquées.

5. 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 les instances WorkSpaces. Pour plus d'informations, consultez Zones de disponibilité pour Amazon WorkSpaces.

   > **Note**
   >
   > Si vous ne savez pas quels sous-réseaux choisir, sélectionnez Aucune préférence.

6. Pour Enable Self Service Permissions (Activer les autorisations en libre-service), choisissez Yes (Oui) afin de permettre aux utilisateurs de recréer leurs instances WorkSpaces, ainsi que de modifier la taille du volume, le type de calcul et le mode d'exécution. L'activation de cette fonction peut avoir un impact sur le prix que vous payez pour Amazon WorkSpaces. Sinon, choisissez No (Non).
7. Pour Activer Amazon WorkDocs, choisissez Oui afin d'enregistrer l'annuaire à utiliser avec Amazon WorkDocs, ou choisissez Non dans le cas contraire.

   > **Note**
   >
   > Cette option s'affiche uniquement si Amazon WorkDocs est disponible dans la région, et si vous n'utilisez pas AWS Managed Microsoft AD. Si vous utilisez AWS Managed Microsoft AD, terminez l'enregistrement de votre annuaire, puis consultez Activation d'Amazon WorkDocs pour AWS Managed Microsoft AD.

8. Choisissez Register (S'inscrire). Initialement la valeur de Membre est `REGISTERING`. Une fois l'enregistrement terminé, la valeur est `Yes`.

Lorsque vous n'avez plus besoin d'utiliser l'annuaire avec WorkSpaces, vous pouvez annuler son enregistrement. 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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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`.

Mettez à jour les détails du répertoire pour votre WorkSpaces

Vous pouvez effectuer les tâches de gestion d'annuaire suivantes à l'aide de la WorkSpaces console.

Tâches

- Sélection d'une unité d'organisation
- Configuration des adresses IP automatiques
- Contrôle de l'accès aux appareils
- Gestion des autorisations d'administrateur local
- Mettre à jour le compte du connecteur AD (AD Connector)
- Authentification multifactorielle (AD Connector)

Sélection d'une unité d'organisation

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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 plus d'informations, consultez Reconstruction d'une instance WorkSpace.

Configuration des adresses IP automatiques

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 plus d'informations, consultez Configurer un VPC pour 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 reconstruire 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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.

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).

Pour contrôler l'accès des appareils à WorkSpaces

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 WorkSpaces l'accès aux appareils fiables.
6. Choisissez Enregistrer.

Gestion des autorisations d'administrateur local

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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 du connecteur AD (AD Connector)

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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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)

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 AD Connector et Conditions préalables requises pour AD Connector.

> **Note**
>
> - Le 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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.

Mise à jour des serveurs DNS pour Amazon WorkSpaces

Si vous devez mettre à jour les adresses IP des serveurs DNS de votre annuaire Active Directory après le lancement de vos instances WorkSpaces, vous devez également mettre à jour ces dernières avec les nouveaux paramètres du serveur DNS.

Vous pouvez mettre à jour les instances WorkSpaces avec les nouveaux paramètres DNS de l'une des façons suivantes :

- Mise à jour des paramètres DNS des instances WorkSpaces avant de mettre à jour les paramètres DNS Active Directory.
- Reconstruction des WorkSpaces après avoir mis à jour les paramètres DNS Active Directory.

Nous recommandons de mettre à jour les paramètres DNS dans les instances WorkSpaces avant d'effectuer cette opération dans Active Directory (comme expliqué à l'Étape 1 de la procédure suivante).

Si vous souhaitez plutôt reconstruire les instances WorkSpaces, mettez à jour l'une des adresses IP du serveur DNS dans Active Directory (Étape 2), puis suivez la procédure décrite dans Reconstruction d'une instance WorkSpace. Après avoir reconstruit les instances WorkSpaces, suivez la procédure décrite à l'Étape 3 pour tester les mises à jour du serveur DNS. Une fois cette étape terminée, mettez à jour l'adresse IP de votre deuxième serveur DNS dans Active Directory, puis reconstruisez les instances WorkSpaces de nouveau. 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.
- Ne lancez aucune nouvelle instance WorkSpace dans les 15 minutes qui précèdent et dans les 15 minutes qui suivent la modification des paramètres du 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 : Mettre à jour les paramètres de serveur DNS de vos instances 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 les instances WorkSpaces Windows

Si vous disposez de plusieurs instances WorkSpaces, vous pouvez déployer la mise à jour de registre suivante sur les espaces de travail en appliquant un objet de stratégie de groupe (GPO) sur l'unité d'organisation (UO) Active Directory des instances WorkSpaces. Pour plus d'informations sur l'utilisation des GPO, consultez Gérez votre Windows WorkSpaces.

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. Dans votre instance WorkSpace Windows, ouvrez le champ de recherche Windows, puis entrez **`registry editor`** pour ouvrir l'Éditeur du 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\SOFTWARE\Amazon\SkyLight

4. Ouvrez la clé de registre DomainJoinDNS. Mettez à jour *OldIP1* avec *NewIP1*, puis cliquez sur OK.
5. Fermez l'Éditeur du Registre.
6. Redémarrez l'instance WorkSpace ou le service SkylightWorkspaceConfigService.

> **Note**
>
> Une fois le service SkylightWorkspaceConfigService redémarré, cela peut prendre jusqu'à 1 minute avant que l'adaptateur réseau reflète 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 de registre DNS à l'aide de PowerShell

La procédure suivante utilise les commandes PowerShell pour mettre à jour le registre et redémarrer le service SkylightWorkspaceConfigService.

1. Dans votre instance WorkSpace Windows, ouvrez le champ de recherche Windows, puis 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 fenêtre PowerShell, 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 fenêtre Powershell, exécutez la commande suivante pour remplacer *OldIP1* par *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**
>
> Une fois le service SkylightWorkspaceConfigService redémarré, cela peut prendre jusqu'à 1 minute avant que l'adaptateur réseau reflète 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 les instances WorkSpaces Linux

Si vous avez plusieurs instances WorkSpaces Linux, nous vous recommandons d'utiliser une solution de gestion de configuration pour distribuer et appliquer les stratégies. Par exemple, vous pouvez utiliser AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise ou Ansible.

Pour mettre à jour les paramètres du serveur DNS dans une instance WorkSpace Linux

1. Dans l'instance WorkSpace Linux, ouvrez une fenêtre Terminal (Applications > Outils système > Terminal MATE).
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 l'instance 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`*.

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 Managed Microsoft AD : Configuration des redirecteurs conditionnels DNS pour votre domaine autogéré
- 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'Étapes 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*.

Test des paramètres du serveur DNS mis à jour pour les instances WorkSpaces Windows

1. Arrêtez le serveur DNS *OldIP1*.
2. Connectez-vous à une instance WorkSpace Windows.
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.

Test des paramètres de serveur DNS mis à jour pour les instances WorkSpaces Linux

1. Arrêtez le serveur DNS *OldIP1*.

2. Connectez-vous à une instance WorkSpace Linux.
3. Dans l'instance WorkSpace Linux, ouvrez une fenêtre Terminal (Applications > Outils système > Terminal MATE).
4. Les adresses IP du serveur DNS renvoyées dans la réponse DHCP sont écrites dans le fichier local `/etc/resolv.conf` de l'instance 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 fichier `/etc/resolv.conf`, ces modifications sont perdues au redémarrage de l'instance WorkSpace.

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.

Suppression de l'annuaire des instances WorkSpaces

Vous pouvez supprimer l'annuaire des instances WorkSpaces s'il n'est plus utilisé par d'autres instances WorkSpaces ou d'autres applications comme Amazon WorkDocs, Amazon WorkMail ou Amazon Chime. Notez que vous devez annuler l'enregistrement d'un annuaire avant de pouvoir le supprimer.

> **Note**
>
> Simple AD et AD Connector sont mis gratuitement à votre disposition pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire Simple AD ou AD connector pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.
> Si vous supprimez votre annuaire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Que se passe-t-il lorsque vous supprimez un annuaire ?

Lorsqu'un annuaire Simple AD ou AWS Directory Service for Microsoft Active Directory est supprimé, toutes les données et tous les instantanés de l'annuaire 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 y connecter avec un Compte AWS qui est 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.

Pour supprimer un annuaire

1. Supprimez tous les WorkSpaces du répertoire. Pour plus d'informations, consultez Suppression d'une instance WorkSpace.
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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
4. Dans le volet de navigation, choisissez Directories (Annuaires).
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 WorkSpaces ensemble ou une image personnalisé.

Activation d'Amazon WorkDocs pour AWS Managed Microsoft AD

Si vous utilisez AWS Managed Microsoft AD avec Amazon WorkSpaces, vous pouvez activer Amazon WorkDocs pour votre annuaire via la console Amazon WorkDocs ou la console AWS Directory Service.

> **Note**
>
> Amazon WorkDocs n'est pas disponible dans toutes les régions AWS où Amazon WorkSpaces est disponible. Pour plus d'informations, consultez Tarification d'Amazon WorkDocs.

Pour activer WorkDocs via la console Amazon WorkDocs

1. Ouvrez la console Amazon WorkDocs à l'adresse https://console.aws.amazon.com/zocalo/.
2. Choisissez Create a new WorkDocs site (Créer un nouveau site WorkDocs).
3. Sous Standard Setup (Configuration standard), choisissez Launch (Lancer).
4. Sélectionnez l'annuaire et créez le nom de votre site.
5. Spécifiez l'utilisateur qui administrera le site WorkDocs. Vous pouvez utiliser l'administrateur ou n'importe quel utilisateur créé dans l'annuaire.

Pour plus d'informations, consultez Mise en route avec AWS Managed Microsoft AD dans le Guide d'administration Amazon WorkDocs.

Pour activer WorkDocs via la console AWS Directory Service

1. Ouvrez la console AWS Directory Service à l'adresse https://console.aws.amazon.com/directoryservicev2/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Sur la page Directories (Annuaires), choisissez votre annuaire.
4. Sur la page Directory details (Détails de l'annuaire), choisissez l'onglet Application management (Gestion d'applications).
5. Dans la section Application access URL (URL d'accès à l'application), si aucune URL d'accès n'a été attribuée à l'annuaire, le bouton Créer s'affiche. Entrez un alias d'annuaire, puis

choisissez Créer. Pour plus d'informations, consultez Création d'une URL d'accès dans le Guide d'administration AWS Directory Service.

6. Dans la section Application access URL (URL d'accès à l'application), choisissez Enable (Activer) pour activer l'authentification unique pour Amazon WorkDocs. Pour plus d'informations, consultez Authentification unique dans le Guide d'administration AWS Directory Service.

Configuration des outils d'administration Active Directory pour WorkSpaces

Vous exécuterez les tâches les plus administratives pour votre annuaire d'instances WorkSpaces avec des outils de gestion d'annuaire, comme des outils d'administration Active Directory. Cependant, vous utiliserez la console WorkSpaces pour exécuter certaines tâches liées à l'annuaire. Pour plus d'informations, consultez Gestion des annuaires pour les instances WorkSpaces.

Si vous créez un annuaire avec AWS Managed Microsoft AD ou Simple AD qui inclut au moins cinq instances WorkSpaces, nous vous recommandons de centraliser l'administration dans une instance Amazon EC2. Bien que vous puissiez installer les outils de gestion d'annuaire dans une instance WorkSpace, l'utilisation d'une instance Amazon EC2 est une solution plus solide.

Pour configurer des outils d'administration Active Directory

1. Lancez une instance Amazon EC2 Windows et associez-la à votre annuaire WorkSpaces en utilisant l'une des options suivantes :

   - Si vous ne disposez pas encore d'une instance Amazon EC2 Windows, vous pouvez associer l'instance au domaine de votre annuaire lorsque vous la lancez. Pour plus d'informations, consultez Joindre une instance EC2 Windows de façon transparente dans le Guide d'administration AWS Directory Service.
   - Si vous disposez déjà d'une instance Amazon EC2 Windows, vous pouvez l'associer manuellement à votre annuaire. 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 Microsoft AD, l'administrateur 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 aux annuaires créés avec Simple AD, mais pas avec AWS Managed AD. Pour les annuaires créés avec AWS Managed AD, consultez Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD dans le Guide d'administration AWS Directory Service.

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 Propriétés ***username***, choisissez Membre de.
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 ne pouvez créer de nouveaux utilisateurs à partir de la console Amazon WorkSpaces que pendant le processus de lancement d'une instance WorkSpace, et vous ne pouvez pas supprimer des utilisateurs via la console Amazon WorkSpaces. 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 l'instance WorkSpace qui lui est affectée. Pour plus d'informations, consultez Suppression d'une instance WorkSpace.

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 Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD dans le Guide d'administration AWS Directory Service.
- 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 L'utilisateur doit changer le mot de passe à la prochaine ouverture de session. Sinon, les utilisateurs ne peuvent pas se connecter à leurs instances WorkSpaces. A la place, affectez un mot de passe temporaire sécurisé à chaque utilisateur et demandez-leur de le changer manuellement à partir de l'instance WorkSpace la prochaine fois qu'ils se connectent.

> **Note**
>
> Si vous utilisez AD Connector ou si les utilisateurs résident dans la région AWS GovCloud (US, côte Ouest), ils ne pourront pas réinitialiser leurs propres mots de passe. (L'option Mot de passe oublié ? de l'écran de connexion de l'application client WorkSpaces ne sera pas disponible.)

Lancement d'un bureau virtuel avec WorkSpaces

Avec Amazon WorkSpaces, vous pouvez allouer à des utilisateurs des bureaux virtuels Microsoft Windows, Amazon Linux ou Ubuntu Linux basés sur le cloud, appelés instances WorkSpaces.

> **Note**
>
> La valeur Nom de l'ordinateur affichée pour une instance WorkSpace dans la console Amazon WorkSpaces varie en fonction du type d'instance WorkSpace lancé (Amazon Linux, Ubuntu ou Windows). Le format du nom d'ordinateur d'une instance WorkSpace peut être l'un des suivants :
>
> - Amazon Linux : A-*xxxxxxxxxxxxx*
> - Ubuntu : U-*xxxxxxxxxxxxx*
> - Windows : IP-C*xxxxxx* ou WSAMZN-*xxxxxxx* ou EC2AMAZ-*xxxxxxx*
>
> Pour les instances WorkSpaces Windows, le format du nom d'ordinateur est déterminé par le type d'offre groupée, et dans le cas des instances WorkSpaces créées à partir d'offres groupées publiques ou personnalisées sur la base d'images publiques, par le moment où les images publiques ont été créées.
> Depuis le 22 juin 2020, les noms d'ordinateur des instances WorkSpaces Windows lancées à partir d'offres groupées publiques utilisent le format WSAMZN-*xxxxxxx* au lieu du format IP-C*xxxxxx*.
> Pour les offres groupées personnalisées sur la base d'une image publique, si cette dernière a été créée avant le 22 juin 2020, les noms d'ordinateur sont au format EC2AMAZ-*xxxxxxx*. Si l'image publique a été créée le ou après le 22 juin 2020, les noms d'ordinateur sont au format WSAMZN-*xxxxxxx*.
> Pour les offres groupées Apportez votre propre licence (BYOL), le format DESKTOP-*xxxxxxx* ou EC2AMAZ-*xxxxxxx* est utilisé par défaut pour les noms d'ordinateur.
> 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 Création d'une WorkSpaces image personnalisée et d'un bundle.

Important : si vous modifiez le nom d'ordinateur d'une instance WorkSpace via les paramètres système Windows, vous ne pourrez plus accéder à l'instance WorkSpace.

WorkSpaces utilise un annuaire pour stocker et gérer les informations des instances WorkSpaces et des utilisateurs. Vous pouvez effectuer les actions suivantes :

- Créer un annuaire Simple AD.
- Créez un annuaire AWS Directory Service pour Microsoft Active Directory, également appelé 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.

Note

- Actuellement, les annuaires partagés ne sont pas pris en charge par Amazon WorkSpaces.
- Si vous configurez un annuaire AWS Managed Microsoft AD pour une réplication sur plusieurs régions, seul l'annuaire de la région principale peut être enregistré pour être utilisé avec Amazon WorkSpaces. Toute tentative d'enregistrement de l'annuaire dans une région répliquée pour une utilisation avec Amazon WorkSpaces est vouée à l'échec. La réplication sur plusieurs régions 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 gratuitement à votre disposition pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire Simple AD ou AD connector pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.

  Pour supprimer des annuaires vides, consultez Suppression de l'annuaire des instances WorkSpaces. Si vous supprimez votre annuaire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Les didacticiels suivants vous montrent comment lancer une instance WorkSpace avec les options de service de l'annuaire pris en charge.

Didacticiels

- Lancement d'une instance WorkSpace avec AWS Managed Microsoft AD
- Lancement d'une instance WorkSpace avec Simple AD
- Lancement d'une instance WorkSpace avec AD Connector
- Lancement d'une instance WorkSpace avec un domaine approuvé

Lancement d'une instance WorkSpace avec AWS Managed Microsoft AD

Amazon WorkSpaces vous permet d'allouer à des utilisateurs des bureaux virtuels Windows et Linux basés sur le cloud, appelés instances WorkSpaces.

WorkSpaces utilise des annuaires pour stocker et gérer les informations des instances WorkSpaces et des utilisateurs. Pour votre annuaire, vous pouvez choisir Simple AD, AD Connector ou AWS Directory Service pour Microsoft Active Directory, également appelé AWS Managed Microsoft AD. De plus, vous pouvez établir une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site.

Dans ce didacticiel, nous lançons une instance WorkSpace qui utilise AWS Managed Microsoft AD. Pour des didacticiels qui utilisent les autres options, consultez Lancement d'un bureau virtuel avec WorkSpaces.

Tâches

- Avant de commencer
- Étape 1 : Création d'un annuaire AWS Managed Microsoft AD
- Étape 2 : Créer une instance WorkSpace
- Étape 3 : Se connecter à l'instance WorkSpace
- Étapes suivantes

Avant de commencer

- WorkSpaces n'est pas disponible dans toutes les régions. Vérifiez celles prises en charge et sélectionnez une région pour vos instances WorkSpaces. Pour plus d'informations sur les régions prises en charge, consultez la Tarification WorkSpaces par région AWS.
- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner un bundle d'instance WorkSpace. Un bundle est une combinaison de système d'exploitation et de ressources de stockage, de calcul et de logiciels. Pour plus d'informations, consultez Offres Amazon WorkSpaces.
- Lorsque vous créez un annuaire avec AWS Directory Service ou lancez une instance WorkSpace, vous devez créer ou sélectionner un Virtual Private Cloud configuré avec un sous-réseau public et deux sous-réseaux privés. Pour plus d'informations, consultez Configurer un VPC pour WorkSpaces.

Étape 1 : Création d'un annuaire AWS Managed Microsoft AD

Tout d'abord, créez un annuaire AWS Managed Microsoft AD. AWS Directory Service crée deux serveurs d'annuaire, un dans chaque sous-réseau privé de votre VPC. Notez qu'aucun utilisateur ne se trouve initialement dans l'annuaire. Vous ajoutez un utilisateur dans l'étape suivante lorsque vous lancez l'instance WorkSpace.

> **Note**
>
> - Actuellement, les annuaires partagés ne sont pas pris en charge par Amazon WorkSpaces.
> - Si l'annuaire AWS Managed Microsoft AD a été configuré pour une réplication sur plusieurs régions, seul l'annuaire de la région principale peut être enregistré pour être utilisé avec Amazon WorkSpaces. Toute tentative d'enregistrement de l'annuaire dans une région répliquée pour une utilisation avec Amazon WorkSpaces est vouée à l'échec. La réplication sur plusieurs régions 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 AWS Managed Microsoft AD

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).

3. Choisissez Configurer l'annuaire, Créer un annuaire Microsoft AD.
4. Configurez l'annuaire comme suit :
   a. Pour Organization name (Nom de l'organisation), saisissez 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 le serveur DNS après avoir lancé les instances WorkSpaces, suivez la procédure décrite dans Mise à jour des serveurs DNS pour Amazon WorkSpaces pour garantir que vos instances WorkSpaces sont correctement mises 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 liées aux mot de passe, consultez Création de votre annuaire AWS Managed Microsoft AD dans le Guide d'administration AWS Directory Service.
   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.
5. Choisissez Create Microsoft AD.
6. Sélectionnez Exécuté. Le statut initial de l'annuaire est `Creating`. Lorsque la création de l'annuaire est terminée, le statut est `Active`.

Étape 2 : Créer une instance WorkSpace

Maintenant que vous avez créé un annuaire AWS Managed Microsoft AD, vous êtes prêt à créer une instance WorkSpace.

Pour créer une instance WorkSpace

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Choisissez Lancer des instances WorkSpaces.
4. Sur la page Sélectionner un annuaire, choisissez l'annuaire que vous venez de créer et choisissez Étape suivante. WorkSpaces enregistre l'annuaire.
5. Sur la page Identifier des utilisateurs, ajoutez un nouvel utilisateur à votre annuaire en procédant comme suit :
   a. Remplissez Nom d'utilisateur, Prénom, Nom et E-mail. Utilisez une adresse e-mail à laquelle vous pouvez accéder.
   b. Choisissez Créer des utilisateurs.
   c. Choisissez Étape suivante.
6. Sur la page Sélectionner un bundle, sélectionnez un bundle et choisissez Étape suivante.

   > **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 Offres Amazon WorkSpaces. Pour plus d'informations sur les spécifications des offres groupées, les utilisations recommandées et les tarifs, consultez Tarification Amazon WorkSpaces.

7. Sur la page Configuration des instances WorkSpaces, choisissez un mode d'exécution et choisissez Étape suivante.
8. Sur la page Vérifier et lancer des instances WorkSpaces, choisissez Lancer des instances WorkSpaces. Le statut initial de l'instance WorkSpace est `PENDING`. Lorsque le lancement est terminé, le statut est `AVAILABLE` et une invitation est envoyée à l'adresse e-mail spécifiée pour l'utilisateur.

> **Note**
>
> 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 plus d'informations, consultez Envoi d'un e-mail d'invitation.

9. (Facultatif) Si Amazon WorkDocs est pris en charge dans la région, vous pouvez l'activer pour tous les utilisateurs de l'annuaire. Pour plus d'informations, consultez Activation d'Amazon WorkDocs pour AWS Managed Microsoft AD. Pour plus d'informations sur Amazon WorkDocs, consultez Utilisation d'Amazon WorkDocs Drive dans le Guide d'administration Amazon WorkDocs.

Étape 3 : Se connecter à l'instance WorkSpace

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

Pour se connecter à l'instance WorkSpace

1. Ouvrez le lien dans l'e-mail d'invitation. Lorsque vous y êtes invité, spécifiez un mot de passe et activez l'utilisateur. Retenez ce mot de passe car vous en aurez besoin pour vous connecter à votre instance 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 les caractères ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/.

2. Consultez Clients WorkSpaces dans le Guide de l'utilisateur Amazon WorkSpaces 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 aucune invite ne s'affiche et que vous n'avez pas déjà installé d'application client, ouvrez https://clients.amazonworkspaces.com/ et téléchargez l'une des applications client, ou lancez Web Access.

> **Note**
>
> Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter aux instances WorkSpaces Amazon Linux.

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.

Étapes suivantes

Vous pouvez continuer à personnaliser l'instance WorkSpace que vous venez de créer. Par exemple, vous pouvez installer un logiciel et créer un bundle personnalisé à partir de votre instance WorkSpace. Vous pouvez également effectuer diverses tâches d'administration pour les instances WorkSpaces et l'annuaire WorkSpaces. Lorsque vous n'avez plus besoin de votre instance WorkSpace, vous pouvez la supprimer. Pour plus d'informations, consultez la documentation suivante.

- Création d'une WorkSpaces image personnalisée et d'un bundle
- Administrez votre WorkSpaces
- Gestion des annuaires pour les instances WorkSpaces
- Suppression d'une instance WorkSpace

Pour plus d'informations sur l'utilisation des applications client WorkSpaces, comme la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez Clients WorkSpaces et Prise en charge des périphériques dans le Guide de l'utilisateur Amazon WorkSpaces.

Lancement d'une instance WorkSpace avec Simple AD

Amazon WorkSpaces vous permet d'allouer à des utilisateurs des bureaux virtuels Microsoft Windows ou Linux basés sur le cloud, appelés instances WorkSpaces.

WorkSpaces utilise des annuaires pour stocker et gérer les informations des instances WorkSpaces et des utilisateurs. Pour votre annuaire, vous pouvez choisir Simple AD, AD Connector ou AWS Directory Service pour Microsoft Active Directory, également appelé AWS Managed Microsoft AD. De plus, vous pouvez établir une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site.

Dans ce didacticiel, nous lançons une instance WorkSpace qui utilise Simple AD. Pour des didacticiels qui utilisent les autres options, consultez Lancement d'un bureau virtuel avec WorkSpaces.

Tâches

- Avant de commencer
- Étape 1 : Créer un annuaire Simple AD
- Étape 2 : Créer une instance WorkSpace
- Étape 3 : Se connecter à l'instance WorkSpace
- Étapes suivantes

Avant de commencer

- Simple AD n'est pas disponible dans toutes les régions. Vérifiez celles prises en charge et sélectionnez une région pour l'annuaire Simple AD. Pour plus d'informations sur les régions prenant en charge Simple AD, consultez Disponibilité dans la région pour AWS Directory Service.
- WorkSpaces n'est pas disponible dans toutes les régions. Vérifiez celles prises en charge et sélectionnez une région pour vos instances WorkSpaces. Pour plus d'informations sur les régions prises en charge, consultez la Tarification WorkSpaces par région AWS.
- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner un bundle d'instance WorkSpace. Un bundle est une combinaison de système d'exploitation et de ressources de stockage, de calcul et de logiciels. Pour plus d'informations, consultez Offres Amazon WorkSpaces.
- Lorsque vous créez un annuaire avec AWS Directory Service ou lancez une instance WorkSpace, vous devez créer ou sélectionner un Virtual Private Cloud configuré avec un sous-réseau public

et deux sous-réseaux privés. Pour plus d'informations, consultez Configurer un VPC pour WorkSpaces.

Étape 1 : Créer un annuaire Simple AD

Créez un annuaire Simple AD. AWS Directory Service crée deux serveurs d'annuaire, un dans chaque sous-réseau privé de votre VPC. Notez qu'aucun utilisateur ne se trouve initialement dans l'annuaire. Vous ajouterez un utilisateur dans l'étape suivante lorsque vous créerez l'instance WorkSpace.

> **Note**
>
> Simple AD est mis gratuitement à disposition pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire Simple AD pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.
> Pour supprimer des annuaires vides, consultez Suppression de l'annuaire des instances WorkSpaces. Si vous supprimez l'annuaire Simple AD, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Pour créer un annuaire Simple AD

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Choisissez Configurer un annuaire, Simple AD, puis Suivant.
4. Configurez l'annuaire comme suit :

    a. Pour Organization name (Nom de l'organisation), saisissez 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 le serveur DNS après avoir lancé les instances WorkSpaces, suivez la procédure décrite dans Mise à jour des serveurs DNS pour Amazon WorkSpaces pour garantir que vos instances WorkSpaces sont correctement mises 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.

5. Choisissez Créer un annuaire.
6. 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 à votre place :

- Crée un rôle IAM pour permettre au service WorkSpaces de créer des interfaces réseau Elastic et de répertorier vos annuaires WorkSpaces. Ce rôle est nommé `workspaces_DefaultRole`.
- Configure un annuaire Simple AD dans le VPC utilisé pour stocker les informations relatives à l'utilisateur et à l'instance WorkSpace. 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 d'annuaire et l'autre pour les instances WorkSpaces dans l'annuaire.

Étape 2 : Créer une instance WorkSpace

Vous êtes maintenant prêt à lancer l'instance WorkSpace.

Pour créer une instance WorkSpace pour un utilisateur

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Choisissez Lancer des instances WorkSpaces.
4. Sur la page Sélectionner un annuaire, procédez comme suit :
   a. Pour Directory (Annuaire), choisissez l'annuaire que vous avez créé.
   b. Pour Activer les autorisations en libre-service, choisissez Oui ou Non, puis entrez une description.
   c. Pour Enable Amazon WorkDocs (Activer Amazon WorkDocs), choisissez Yes (Oui).

      > **Note**
      >
      > Cette option est proposée uniquement si Amazon WorkDocs est disponible dans la région sélectionnée.

   d. Choisissez Étape suivante. WorkSpaces enregistre l'annuaire Simple AD.
5. Sur la page Identifier des utilisateurs, ajoutez un nouvel utilisateur à votre annuaire en procédant comme suit :
   a. Remplissez Nom d'utilisateur, Prénom, Nom et E-mail. Utilisez une adresse e-mail à laquelle vous pouvez accéder.
   b. Choisissez Créer des utilisateurs.
   c. Choisissez Étape suivante.
6. Sur la page Sélectionner un bundle, sélectionnez un bundle et choisissez Étape suivante.

   > **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 Offres Amazon

WorkSpaces. Pour plus d'informations sur les spécifications des offres groupées, les utilisations recommandées et les tarifs, consultez Tarification Amazon WorkSpaces.

7. Sur la page Configuration des instances WorkSpaces, choisissez un mode d'exécution et choisissez Étape suivante.
8. Sur la page Vérifier et lancer des instances WorkSpaces, choisissez Lancer des instances WorkSpaces. Le statut initial de l'instance WorkSpace est `PENDING`. Une fois le lancement terminé (cela peut prendre jusqu'à 20 minutes), le statut passe à `AVAILABLE`, et une invitation est envoyée à l'adresse e-mail spécifiée pour l'utilisateur.

> **Note**
>
> 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 plus d'informations, consultez Envoi d'un e-mail d'invitation.

Étape 3 : Se connecter à l'instance WorkSpace

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

Pour se connecter à l'instance WorkSpace

1. Ouvrez le lien dans l'e-mail d'invitation. Lorsque vous y êtes invité, saisissez un mot de passe et activez l'utilisateur. Retenez ce mot de passe car vous en aurez besoin pour vous connecter à votre instance 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 les caractères ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/.

2. Consultez Clients WorkSpaces dans le Guide de l'utilisateur Amazon WorkSpaces 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 aucune invite ne s'affiche et que vous n'avez pas déjà installé d'application client, ouvrez https://clients.amazonworkspaces.com/ et téléchargez l'une des applications client, ou lancez Web Access.

> **Note**
>
> Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter aux instances WorkSpaces Amazon Linux.

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.

Étapes suivantes

Vous pouvez continuer à personnaliser l'instance WorkSpace que vous venez de créer. Par exemple, vous pouvez installer un logiciel et créer un bundle personnalisé à partir de votre instance WorkSpace. Vous pouvez également effectuer diverses tâches d'administration pour les instances WorkSpaces et l'annuaire WorkSpaces. Lorsque vous n'avez plus besoin de votre instance WorkSpace, vous pouvez la supprimer. Pour plus d'informations, consultez la documentation suivante.

- Création d'une WorkSpaces image personnalisée et d'un bundle
- Administrez votre WorkSpaces
- Gestion des annuaires pour les instances WorkSpaces
- Suppression d'une instance WorkSpace

Pour plus d'informations sur l'utilisation des applications client WorkSpaces, comme la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez Clients WorkSpaces et Prise en charge des périphériques dans le Guide de l'utilisateur Amazon WorkSpaces.

Lancement d'une instance WorkSpace avec AD Connector

Amazon WorkSpaces vous permet d'allouer à des utilisateurs des bureaux virtuels Microsoft Windows ou Linux basés sur le cloud, appelés instances WorkSpaces.

WorkSpaces utilise des annuaires pour stocker et gérer les informations des instances WorkSpaces et des utilisateurs. Pour votre annuaire, vous pouvez choisir Simple AD, AD Connector ou AWS Directory Service pour Microsoft Active Directory, également appelé AWS Managed Microsoft AD. De plus, vous pouvez établir une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site.

Dans ce didacticiel, nous lançons une instance WorkSpace qui utilise un connecteur AD. Pour des didacticiels qui utilisent les autres options, consultez Lancement d'un bureau virtuel avec WorkSpaces.

Tâches

- Avant de commencer
- Étape 1 . Créer un connecteur AD
- Étape 2 : Créer une instance WorkSpace
- Étape 3 : Se connecter à l'instance WorkSpace
- Étapes suivantes

Avant de commencer

- WorkSpaces n'est pas disponible dans toutes les régions. Vérifiez celles prises en charge et sélectionnez une région pour vos instances WorkSpaces. Pour plus d'informations sur les régions prises en charge, consultez la Tarification WorkSpaces par région AWS.
- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner un bundle d'instance WorkSpace. Un bundle est une combinaison de système d'exploitation et de ressources de stockage, de calcul et de logiciels. Pour plus d'informations, consultez Offres Amazon WorkSpaces.
- Créez un Virtual Private Cloud avec au moins deux sous-réseaux privés. Pour plus d'informations, consultez Configurer un VPC pour WorkSpaces. Le VPC doit être connecté à votre réseau sur site via une connexion réseau privé virtuel (VPN) ou AWS Direct Connect. Pour plus d'informations, consultez Conditions préalables requises pour AD Connector dans le Guide d'administration AWS Directory Service.

- Fournissez l'accès à Internet à partir de l'instance WorkSpace. Pour plus d'informations, consultez Fournissez un accès à Internet depuis votre WorkSpace.

Étape 1 . Créer un connecteur AD

> **Note**
>
> AD Connector est mis à votre disposition gratuitement pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire AD Connector pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.
> Pour supprimer des annuaires vides, consultez Suppression de l'annuaire des instances WorkSpaces. Si vous supprimez l'annuaire AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Pour créer un connecteur AD

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Choisissez Configurer l'annuaire, Créer un connecteur AD.
4. Pour Organization name (Nom de l'organisation), saisissez 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.
5. Pour Connected directory DNS (DNS de l'annuaire connecté), saisissez le nom complet de votre annuaire sur site (par exemple, exemple.com).
6. Pour Connected directory NetBIOS name (Nom NetBIOS de l'annuaire connecté), saisissez le nom abrégé de votre annuaire sur site (par exemple, exemple).
7. 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.

8. 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.
9. Pour DNS adress (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 du serveur DNS après avoir lancé les instances WorkSpaces, suivez la procédure décrite dans Mise à jour des serveurs DNS pour Amazon WorkSpaces pour garantir que les instances WorkSpaces sont correctement mises à jour.

10. (Facultatif) Dans le champ Description, saisissez une description pour la stratégie.
11. Conservez la Taille sur Petit.
12. Pour VPC, sélectionnez votre VPC.
13. Pour Sous-réseaux (subnets), sélectionnez vos sous-réseaux. Les serveurs DNS spécifiés doivent être accessibles à partir de chaque sous-réseau.
14. Choisissez Étape suivante.
15. Choisissez Créer un connecteur AD. La connexion de votre annuaire prend plusieurs minutes. Le statut initial de l'annuaire est `Requested` et ensuite `Creating`. Lorsque la création de l'annuaire est terminée, le statut est `Active`.

Étape 2 : Créer une instance WorkSpace

Maintenant que vous êtes prêt à lancer des instances WorkSpaces pour un ou plusieurs utilisateurs de votre annuaire sur site.

Pour lancer un espace de travail pour un utilisateur existant

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Choisissez Lancer des instances WorkSpaces.
4. Pour Directory (Annuaire), choisissez l'annuaire que vous avez créé.
5. (Facultatif) Si vous lancez une instance WorkSpace dans cet annuaire pour la première fois et que Amazon WorkDocs est pris en charge dans la région, vous pouvez activer ou désactiver

Amazon WorkDocs pour tous les utilisateurs de l'annuaire. Pour plus d'informations sur Amazon WorkDocs, consultez Utilisation d'Amazon WorkDocs Drive dans le Guide d'administration Amazon WorkDocs.

6. Choisissez Suivant. WorkSpaces enregistre le connecteur AD.
7. Sélectionnez un ou plusieurs utilisateurs existants à partir de votre annuaire sur site. N'ajoutez pas de nouveaux utilisateurs à un annuaire sur site via la console WorkSpaces.

   Pour trouver des utilisateurs à sélectionner, vous pouvez saisir le nom entier de l'utilisateur ou une partie et choisir Search (Rechercher) ou choisir Showw All Users (Afficher tous les utilisateurs). Notez que vous ne pouvez pas sélectionner un utilisateur qui ne dispose pas d'une adresse e-mail.

   Après avoir sélectionné les utilisateurs, choisissez Ajouter la sélection, puis choisissez Étape suivante.
8. Sous Sélectionner un bundle, choisissez le bundle d'instance WorkSpace par défaut à utiliser pour les instances WorkSpaces. Sous Affecter des bundles d'instance WorkSpace, vous pouvez choisir un autre bundle pour chaque instance WorkSpace individuelle si nécessaire. Lorsque vous avez terminé, choisissez Étape suivante.

   > **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 Offres Amazon WorkSpaces. Pour plus d'informations sur les spécifications des offres groupées, les utilisations recommandées et les tarifs, consultez Tarification Amazon WorkSpaces.
9. Choisissez un mode d'exécution pour vos instances WorkSpaces et choisissez Étape suivante. Pour plus d'informations, consultez Gestion du mode d'exécution d'une instance WorkSpace.
10. Choisissez Lancer des instances WorkSpaces. Le statut initial de l'instance WorkSpace est `PENDING`. Lorsque le lancement de l'annuaire est terminé, le statut est `AVAILABLE`.
11. Envoyez des invitations à l'adresse e-mail de chaque utilisateur. (Ces invitations ne sont pas envoyées automatiquement si vous utilisez AD Connector.) Pour plus d'informations, consultez Envoi d'un e-mail d'invitation.

Étape 3 : Se connecter à l'instance WorkSpace

Vous pouvez vous connecter à votre instance WorkSpace avec le client de votre choix. Une fois que vous êtes connecté, le client affiche le bureau de l'instance WorkSpace.

Pour se connecter à l'instance WorkSpace

1. Ouvrez le lien dans l'e-mail d'invitation.
2. Consultez Clients WorkSpaces dans le Guide de l'utilisateur Amazon WorkSpaces 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 aucune invite ne s'affiche et que vous n'avez pas déjà installé d'application client, ouvrez https://clients.amazonworkspaces.com/ et téléchargez l'une des applications client, ou lancez Web Access.

   > **Note**
   >
   > Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter aux instances WorkSpaces Amazon Linux.

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 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. (L'option Mot de passe oublié ? de l'écran de connexion de l'application client WorkSpaces 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 WorkSpaces.

Étapes suivantes

Vous pouvez continuer à personnaliser l'instance WorkSpace que vous venez de créer. Par exemple, vous pouvez installer un logiciel et créer un bundle personnalisé à partir de votre instance WorkSpace. Vous pouvez également effectuer diverses tâches d'administration pour les instances WorkSpaces et l'annuaire WorkSpaces. Lorsque vous n'avez plus besoin de votre instance WorkSpace, vous pouvez la supprimer. Pour plus d'informations, consultez la documentation suivante.

- Création d'une WorkSpaces image personnalisée et d'un bundle
- Administrez votre WorkSpaces
- Gestion des annuaires pour les instances WorkSpaces
- Suppression d'une instance WorkSpace

Pour plus d'informations sur l'utilisation des applications client WorkSpaces, comme la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez Clients WorkSpaces et Prise en charge des périphériques dans le Guide de l'utilisateur Amazon WorkSpaces.

Lancement d'une instance WorkSpace avec un domaine approuvé

Amazon WorkSpaces vous permet d'allouer à des utilisateurs des bureaux virtuels Microsoft Windows, Amazon Linux ou Ubuntu Linux basés sur le cloud, appelés instances WorkSpaces.

WorkSpaces utilise des annuaires pour stocker et gérer les informations des instances WorkSpaces et des utilisateurs. Pour votre annuaire, vous pouvez choisir Simple AD, AD Connector ou AWS Directory Service pour Microsoft Active Directory, également appelé AWS Managed Microsoft AD. De plus, vous pouvez établir une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site.

Dans ce didacticiel, nous lançons une instance WorkSpace qui utilise une relation d'approbation. Pour des didacticiels qui utilisent les autres options, consultez Lancement d'un bureau virtuel avec WorkSpaces.

Tâches

- Avant de commencer
- Étape 1 : Établir une relation d'approbation

- Étape 2 : Créer une instance WorkSpace
- Étape 3 : Se connecter à l'instance WorkSpace
- Étapes suivantes

Avant de commencer

- Le lancement d'instances WorkSpaces avec des Comptes AWS dans un domaine sécurisé distinct fonctionne avec AWS Managed Microsoft AD configuré pour une relation d'approbation avec l'annuaire sur site. Toutefois, les instances WorkSpaces utilisant Simple AD ou AD Connector ne peuvent pas lancer d'instances WorkSpaces pour les utilisateurs d'un domaine approuvé.
- WorkSpaces n'est pas disponible dans toutes les régions. Vérifiez celles prises en charge et sélectionnez une région pour vos instances WorkSpaces. Pour plus d'informations sur les régions prises en charge, consultez la Tarification WorkSpaces par région AWS.
- Lorsque vous lancez une instance WorkSpace, vous devez sélectionner un bundle d'instance WorkSpace. Un bundle est une combinaison de ressources de stockage, de calcul et logicielles. Pour plus d'informations, consultez Offres Amazon WorkSpaces.
- Lorsque vous créez un annuaire avec AWS Directory Service ou lancez une instance WorkSpace, vous devez créer ou sélectionner un Virtual Private Cloud configuré avec un sous-réseau public et deux sous-réseaux privés. Pour plus d'informations, consultez Configurer un VPC pour WorkSpaces.

Étape 1 : Établir une relation d'approbation

Pour configurer la relation d'approbation

1. Configurez AWS Managed Microsoft AD dans votre cloud privé virtuel (VPC). Pour plus d'informations, consultez Création de votre annuaire AWS Managed Microsoft AD dans le Guide d'administration AWS Directory Service.

   > **Note**
   >
   > - Actuellement, les annuaires partagés ne sont pas pris en charge par Amazon WorkSpaces.
   > - Si l'annuaire AWS Managed Microsoft AD a été configuré pour une réplication sur plusieurs régions, seul l'annuaire de la région principale peut être enregistré pour

être utilisé avec Amazon WorkSpaces. Toute tentative d'enregistrement de l'annuaire dans une région répliquée pour une utilisation avec Amazon WorkSpaces est vouée à l'échec. La réplication sur plusieurs régions 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 d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine sur site. Prenez soin de configurer la relation d'approbation en tant que relation d'approbation bidirectionnelle. Pour plus d'informations, consultez Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory sur site dans le Guide d'administration AWS Directory Service.

Il est possible d'utiliser une relation d'approbation unidirectionnelle ou bidirectionnelle afin de gérer et d'authentifier avec WorkSpaces, et d'allouer des instances WorkSpaces pour des utilisateurs et des groupes sur site. Pour plus d'informations, consultez Déploiement d'Amazon WorkSpaces à l'aide d'un domaine de ressource d'approbation unidirectionnelle avec AWS Directory Service (langue française non garantie).

> **Note**
>
> Les instances WorkSpaces Ubuntu utilisent SSSD (System Security Services Daemon) pour l'intégration Active Directory, et SSSD ne prend pas en charge les relations d'approbation dans les forêts. Configurez plutôt une relation d'approbation externe. Une relation d'approbation bidirectionnelle est recommandée pour les instances Amazon Linux et Ubuntu.

Étape 2 : Créer une instance WorkSpace

Une fois que vous avez établi une relation d'approbation entre l'annuaire AWS Managed Microsoft AD et le domaine Microsoft Active Directory sur site, vous pouvez allouer des instances WorkSpaces aux utilisateurs dans le domaine sur site.

Notez que vous devez vous assurer de répliquer les paramètres GPO entre les domaines avant de pouvoir les appliquer aux instances WorkSpaces.

Pour lancer des espaces de travail pour des utilisateurs dans un domaine sur site de confiance

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.

2. Dans le volet de navigation, choisissez WorkSpaces.
3. Choisissez Lancer des instances WorkSpaces.
4. Sur la page Select a Directory, choisissez l'annuaire que vous venez d'enregistrer, puis sélectionnez Next Step.
5. Sur la page Identify Users, procédez comme suit :
   a. Dans Select trust from forest, sélectionnez la relation d'approbation que vous avez créée.
   b. Sélectionnez les utilisateurs dans le domaine sur site, puis choisissez Add Selected.
   c. Choisissez Étape suivante.
6. Sélectionnez l'offre à utiliser pour les espaces de travail, puis choisissez Next Step.

> **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 Offres Amazon WorkSpaces. Pour plus d'informations sur les spécifications des offres groupées, les utilisations recommandées et les tarifs, consultez Tarification Amazon WorkSpaces.

7. Choisissez le mode d'exécution et les paramètres de chiffrement, puis configurez des balises. Lorsque vous avez terminé, choisissez Next Step.
8. Choisissez Lancer des instances WorkSpaces. Notez que vous devrez peut-être attendre jusqu'à 20 minutes pour que les espaces de travail soient disponibles et jusqu'à 40 minutes si le chiffrement est activé. Le statut initial de l'instance WorkSpace est `PENDING`. Lorsque le lancement de l'annuaire est terminé, le statut est `AVAILABLE`.
9. Envoyez des invitations à l'adresse e-mail de chaque utilisateur. (Ces invitations ne sont pas envoyées automatiquement si vous utilisez une relation d'approbation.) Pour plus d'informations, consultez Envoi d'un e-mail d'invitation.

Étape 3 : Se connecter à l'instance WorkSpace

Après avoir reçu l'e-mail d'invitation, vous pouvez vous connecter à votre instance WorkSpace. Les utilisateurs peuvent alors entrer leurs noms d'utilisateur comme suit : nom d'utilisateur, corp\nom d'utilisateur ou corp.exemple.com\nom d'utilisateur).

Pour se connecter à l'instance WorkSpace

1. Ouvrez le lien dans l'e-mail d'invitation. Lorsque vous y êtes invité, saisissez un mot de passe et activez l'utilisateur. Retenez ce mot de passe car vous en aurez besoin pour vous connecter à votre instance 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 les caractères ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Consultez Clients WorkSpaces dans le Guide de l'utilisateur Amazon WorkSpaces 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 aucune invite ne s'affiche et que vous n'avez pas déjà installé d'application client, ouvrez https://clients.amazonworkspaces.com/ et téléchargez l'une des applications client, ou lancez Web Access.

   > **Note**
   >
   > Vous ne pouvez pas utiliser de navigateur Web (Web Access) pour vous connecter aux instances WorkSpaces Amazon Linux.

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.

Étapes suivantes

Vous pouvez continuer à personnaliser l'instance WorkSpace que vous venez de créer. Par exemple, vous pouvez installer un logiciel et créer un bundle personnalisé à partir de votre instance

WorkSpace. Vous pouvez également effectuer diverses tâches d'administration pour les instances WorkSpaces et l'annuaire WorkSpaces. Lorsque vous n'avez plus besoin de votre instance WorkSpace, vous pouvez la supprimer. Pour plus d'informations, consultez la documentation suivante.

- Création d'une WorkSpaces image personnalisée et d'un bundle
- Administrez votre WorkSpaces
- Gestion des annuaires pour les instances WorkSpaces
- Suppression d'une instance WorkSpace

Pour plus d'informations sur l'utilisation des applications client WorkSpaces, comme la configuration de plusieurs moniteurs ou l'utilisation de périphériques, consultez Clients WorkSpaces et Prise en charge des périphériques dans le Guide de l'utilisateur Amazon WorkSpaces.

Administration des utilisateurs d'instances WorkSpaces

Chaque instance WorkSpace est affectée à un seul utilisateur et ne peut pas être partagée par plusieurs utilisateurs. Par défaut, une seule instance WorkSpace par utilisateur et par annuaire est autorisée.

Table des matières

- Gestion des utilisateurs d'instances WorkSpaces
- Création de plusieurs WorkSpaces pour un utilisateur
- Personnalisez la façon dont les utilisateurs se connectent à leur WorkSpaces
- Activation des capacités de gestion d'instances WorkSpaces en libre-service pour les utilisateurs
- Activation de l'optimisation audio Amazon Connect pour les utilisateurs
- Activation du chargement des journaux de diagnostic

Gestion des utilisateurs d'instances WorkSpaces

En tant qu'administrateur d'instances WorkSpaces, vous pouvez exécuter les tâches suivantes et gérer les utilisateurs WorkSpaces.

Modification d'informations utilisateur

Vous pouvez utiliser la console WorkSpaces afin de modifier les informations utilisateur d'une instance WorkSpace.

> **Note**
>
> Cette fonctionnalité est disponible uniquement 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.

Pour modifier des informations utilisateur

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.

2. Dans le volet de navigation, choisissez 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 ne pouvez créer des utilisateurs à partir de la console Amazon WorkSpaces que pendant le processus de lancement d'une instance WorkSpace, et vous ne pouvez pas supprimer d'utilisateurs via la console Amazon WorkSpaces. 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 exécuterez les tâches les plus administratives pour votre annuaire d'instances WorkSpaces avec des outils de gestion d'annuaire, comme des outils d'administration Active Directory. Pour plus d'informations, consultez Configuration des outils d'administration Active Directory pour WorkSpaces.

> **Important**
>
> Avant de pouvoir supprimer un utilisateur, vous devez supprimer l'instance WorkSpace qui lui est affectée. Pour plus d'informations, consultez Suppression d'une instance WorkSpace.

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 Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD dans le Guide d'administration AWS Directory Service.
- 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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Dans la page WorkSpaces, utilisez la zone de recherche pour rechercher l'utilisateur auquel vous souhaitez envoyer une invitation, puis sélectionnez l'instance WorkSpace correspondante dans les résultats de la recherche. Vous ne pouvez sélectionner uniquement une instance WorkSpace à la fois.
4. Choisissez Actions, Inviter un utilisateur.
5. Sur la page Inviter des utilisateurs dans le WorkSpace, choisissez Envoyer l'invitation.

Création de plusieurs WorkSpaces pour un utilisateur

Par défaut, vous ne pouvez créer qu'une instance WorkSpace par utilisateur et par annuaire. Toutefois, si nécessaire, vous pouvez créer plusieurs instances WorkSpaces pour un utilisateur, en fonction de la configuration de votre annuaire.

- Si vous ne disposez que d'un seul annuaire pour les instances WorkSpace, créez plusieurs noms d'utilisateur pour l'utilisateur. Par exemple, une utilisatrice nommée Marie Majeur peut avoir mmajeur1, mmajeur2, etc., comme noms d'utilisateur. Chaque nom d'utilisateur est associé à une instance WorkSpace différente dans le même annuaire, mais les instances WorkSpaces ont le même code d'enregistrement, à condition qu'elles soient toutes créées dans le même annuaire de la même région AWS.
- Si vous disposez de plusieurs annuaires pour vos instances WorkSpace, créez les instances WorkSpaces pour l'utilisateur dans des annuaires distincts. Vous pouvez utiliser le même nom

d'utilisateur ou des noms d'utilisateur différents dans les annuaires. Les instances WorkSpaces auront des codes d'enregistrement différents.

> **Tip**
>
> Afin de localiser facilement toutes les instances WorkSpaces que vous avez créées pour un utilisateur, utilisez la même base de nom d'utilisateur pour chacune d'entre elles.
> Par exemple, si vous avez une utilisatrice nommée Marie Majeur avec le nom d'utilisateur Active Directory mmajeur, créez ses instances WorkSpaces avec des noms d'utilisateur comme mmajeur, mmajeur1, mmajeur2, mmajeur3 ou d'autres variantes comme mmajeur_windows ou mmajeur_linux. Tant que toutes les instances WorkSpaces ont la même base de nom d'utilisateur (mmajeur), vous pouvez effectuer un tri par nom d'utilisateur dans votre console WorkSpaces pour regrouper toutes les instances WorkSpaces de cet utilisateur.

> **Important**
>
> - Un utilisateur peut disposer d'instances WorkSpaces PCoIP et WSP tant que les deux instances WorkSpaces sont situées dans des annuaires distincts. Le même utilisateur ne peut pas disposer d'une instance WorkSpace PCoIP et d'une instance WorkSpace WSP dans le même annuaire.
> - Si vous configurez plusieurs instances WorkSpaces pour une utilisation avec la redirection entre régions, vous devez les configurer dans différents annuaires de différentes régions AWS, et vous devez utiliser les mêmes noms d'utilisateur dans chaque annuaire. Pour plus d'informations sur la redirection entre régions, consultez Redirection entre régions pour Amazon WorkSpaces.

Pour basculer d'une instance WorkSpace à une autre, l'utilisateur se connecte avec le nom d'utilisateur et le code d'enregistrement associés à une instance WorkSpace particulière. Si l'utilisateur utilise une version 3.0+ des applications client WorkSpaces pour Windows, macOS ou Linux, il peut attribuer des noms différents aux instances WorkSpaces en accédant à Paramètres, Gérer les informations de connexion dans l'application client.

Personnalisez la façon dont les utilisateurs se connectent à leur WorkSpaces

Personnalisez l'accès de vos utilisateurs à WorkSpaces l'aide d'identifiants de ressources uniformes (URI) 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 des URI de connexion qui enregistrent vos utilisateurs à l'aide de 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 Amazon 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 utiliser les URI pour accéder à leur WorkSpaces, les utilisateurs doivent d'abord installer l'application cliente pour leur appareil en ouvrant https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

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
workspaces://	Ouvre l'application WorkSpaces cliente. (Remarque : l'utilisation d'espaces de travail : // n'est pas actuellement prise en charge dans l'application client Linux.)
workspaces://@registrationcode	Enregistre un utilisateur à l'aide de son code WorkSpaces d'enregistrement. Affiche également la page de connexion du client.
workspaces://username@registrationcode	Enregistre un utilisateur à l'aide de son code WorkSpaces d'enregistrement. Entre aussi automatiquement le nom d'utilisateur dans le champ username sur la page de connexion du client.

Syntaxe prise en charge	Description
workspaces://username@registrationcode?MFACode=mfa	Enregistre un utilisateur à l'aide de son code WorkSpaces 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.
workspaces://@registrationcode?mfacode=mfa	Enregistre un utilisateur à l'aide de son code WorkSpaces 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.

Activation des capacités de gestion d'instances WorkSpaces en libre-service pour les utilisateurs

Dans WorkSpaces, vous pouvez activer des capacités de gestion d'instances WorkSpaces en libre-service pour les utilisateurs. Ceux-ci bénéficient ainsi d'un plus grand contrôle de leur expérience. Et vous pouvez aussi réduire la charge de travail de votre service support informatique concernant les instances WorkSpaces. L'activation des capacités en libre-service vous permet d'autoriser les utilisateurs à effectuer une ou plusieurs des tâches suivantes directement à partir de leur client Windows ou OS X :

- Mettre en cache leurs informations d'identification sur leur client. Ils peuvent ainsi se reconnecter à leur instance WorkSpace sans saisir à nouveau leurs informations d'identification.
- Redémarrer leur instance WorkSpace
- Augmenter la taille des volumes racine et utilisateur sur leur espace de travail

- Modifier le type de calcul (solution groupée) de leur instance WorkSpace
- Modifier le mode d'exécution de leur instance WorkSpace
- Reconstruire leur instance 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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Sélectionnez votre annuaire, puis choisissez Actions, Update Details.
4. Développez User Self-Service Permissions (Autorisations de libre-service pour l'utilisateur). Le cas échéant, activez ou désactivez les options suivantes afin de déterminer les tâches de gestion de l'instance WorkSpace que les utilisateurs pourront exécuter à partir de 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. Si les utilisateurs choisissent de mettre en cache leurs informations d'identification, ils peuvent se reconnecter à leurs instances WorkSpaces sans avoir besoin de 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 l'instance WorkSpace à partir du client : les utilisateurs peuvent redémarrer leur instance WorkSpace. Le redémarrage les déconnecte de leur instance WorkSpace, ferme celle-ci, puis la redémarre. Les données utilisateur, le système d'exploitation et les paramètres système ne sont pas affectés.
    - Augmenter la taille du volume : les utilisateurs peuvent augmenter les volumes racine et utilisateur de leur instance WorkSpace jusqu'à la taille spécifiée sans avoir à 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. Les volumes racine et utilisateur WorkSpace se trouvent 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 plus d'informations, consultez Modifier un WorkSpace.

Dans le cas d'une instance WorkSpace nouvellement créée, les utilisateurs doivent attendre 6 heures avant d'augmenter la taille de ces lecteurs. Ils ne peuvent par la suite le faire qu'une seule fois par période de 6 heures. Pendant l'augmentation de la taille du volume, les utilisateurs peuvent effectuer la plupart des tâches sur leur instance Workspace. Les tâches qu'ils ne peuvent pas effectuer sont les suivantes : modifier le type de calcul de leur instance WorkSpace, modifier le mode d'exécution de leur instance WorkSpace, redémarrer leur instance WorkSpace ou reconstruire leur instance WorkSpace. Lorsque le processus est terminé, WorkSpace doit être redémarré pour que les modifications prennent effet. Ce processus peut prendre jusqu'à une heure.

> **Note**
>
> Lorsqu'un utilisateur augmente la taille des volumes de son instance WorkSpace, le tarif facturé pour cette instance WorkSpace augmente également.

- Modifier le type de calcul : les utilisateurs peuvent modifier les types de calcul (solutions groupées) sélectionnés pour leur instance WorkSpace. Pour une instance WorkSpace nouvellement créée, les utilisateurs doivent attendre 6 heures avant de pouvoir basculer vers une autre solution groupée. 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. Au cours de la modification du type de calcul d'une instance WorkSpace, les utilisateurs sont déconnectés de leur instance WorkSpace. Ils ne peuvent donc pas l'utiliser ni la modifier. WorkSpace est automatiquement redémarré pendant le processus de modification de type de calcul. Ce processus peut prendre jusqu'à une heure.

  > **Note**
  >
  > Lorsqu'un utilisateur modifie le type de calcul de son instance WorkSpace, le tarif facturé pour celle-ci change également.

- Changer de mode d'exécution : les utilisateurs peuvent faire basculer leur instance WorkSpace entre les modes d'exécution AlwaysOn et AutoStop. Pour plus d'informations, consultez Gestion du mode d'exécution d'une instance WorkSpace.

  > **Note**
  >
  > Lorsqu'un utilisateur modifie le mode d'exécution de son instance WorkSpace, le tarif facturé pour celle-ci change également.

- Reconstruire l'instance WorkSpace à partir du client : les utilisateurs peuvent reconstruire le système d'exploitation d'une instance WorkSpace à son état initial. Lorsqu'une instance WorkSpace est réinitialisée, 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 instance WorkSpace nouvellement créée, les utilisateurs doivent attendre 12 heures avant de pouvoir la reconstruire. Au cours de la reconstruction d'une instance WorkSpace, les utilisateurs sont déconnectés de leur instance WorkSpace. Ils ne peuvent donc pas l'utiliser ni la modifier. Ce processus peut prendre jusqu'à une heure.

5. Choisissez Mettre à jour ou Mettre à jour et quitter.

Activation de l'optimisation audio Amazon Connect pour les utilisateurs

Dans la console de gestion WorkSpaces, vous pouvez activer l'optimisation audio du Panneau de contrôle des contacts Amazon Connect (CCP) pour vos flottes d'instances WorkSpaces afin de renforcer la sécurité et d'offrir un son de qualité native. Une fois l'optimisation audio du CCP activée, le son du CCP sera traité par les points de terminaison du client, tandis que les utilisateurs WorkSpaces pourront interagir avec le CCP depuis leurs instances WorkSpaces.

L'optimisation audio du Panneau de configuration des contacts (CCP) Amazon Connect fonctionne avec :

- le client WorkSpaces Windows ;
- les instances WorkSpaces Windows et Linux ;
- les instances WorkSpaces utilisant PCoIP ou WSP.

Prérequis

- 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 de flux Amazon Connect, consultez le référentiel GitHub à l'adresse https://github.com/aws/amazon-connect-streams. Le CCP personnalisé que vous créez est celui que les agents Amazon Connect utilisent dans leurs instances WorkSpaces.
- Un navigateur Web doit être installé sur les points de terminaison du client WorkSpaces pris en charge par Amazon Connect. 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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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.

Activation du chargement des journaux de diagnostic

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 : à l'aide de la console AWS

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 Modifier.
6. Choisissez Chargements du journal de diagnostic.
7. 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

Administrez votre WorkSpaces

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, NVMe et PV de votre WorkSpaces. 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 AWSpour les instances Windows, et Mettre à niveau les pilotes PV sur les instances Windows.
> - Assurez-vous de mettre régulièrement à jour les agents EC2Config, EC2Launch et EC2Launch V2 vers les dernières versions. Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez Mettre à jour EC2Config et EC2Launch.

Table des matières

- Gérez votre Windows WorkSpaces
- Gérez votre Amazon Linux WorkSpaces
- Gérez votre Ubuntu WorkSpaces
- Optimisez Amazon WorkSpaces pour une communication en temps réel
- Gestion du mode d'exécution d'une instance WorkSpace
- Gestion des applications
- Modifier un WorkSpace
- Personnaliser la WorkSpace marque
- Balisage des ressources WorkSpaces
- Maintenance des instances WorkSpaces
- Instances WorkSpace chiffrées
- Redémarrer un WorkSpace
- Reconstruction d'une instance WorkSpace

- Restauration d'une instance WorkSpace
- Microsoft 365 Apportez votre propre licence (BYOL)
- Mettre à niveau Windows BYOL WorkSpaces
- Migrer un WorkSpace
- Suppression d'une instance WorkSpace

Gérez votre Windows WorkSpaces

Vous pouvez utiliser les objets de stratégie de groupe (GPO) pour appliquer des paramètres afin de gérer Windows WorkSpaces ou les utilisateurs qui font partie de votre WorkSpaces répertoire Windows.

> **Note**
>
> Les instances Linux ne respectent pas de stratégie de groupe. Pour plus d'informations sur la gestion d'Amazon Linux WorkSpaces, consultezGérez votre Amazon Linux WorkSpaces.

Nous vous recommandons 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, qu'il s'agisse du protocole PCoIP ou du protocole de WorkSpaces streaming (WSP).

> **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 WorkSpaces.
> - 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, vos WorkSpaces utilisateurs PCoIP ne pourront pas se connecter à leurs applications WorkSpaces WorkSpaces clientes. Votre PCoIP ne recevra pas non WorkSpaces plus de mises à jour du logiciel de l'agent PCoIP. Les mises à jour de l'agent PCoIP 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 à l'intérieur du. 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 Activation ou désactivation de la redirection d'entrée audio pour PCoIP ou Activation ou désactivation de la redirection d'entrée audio pour WSP.
- 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 plus d'informations, consultez 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 actives mais inactives des services de bureau à distance » n'est actuellement pas prise en charge par WSP WorkSpaces. Évitez de l'utiliser pendant les sessions WSP, car elle provoque une déconnexion même quand il existe une activité et que la session n'est pas inactive.

Pour plus d'informations sur l'utilisation des outils d'administration Active Directory pour travailler avec des objets de stratégie de groupe, consultez Configuration des outils d'administration Active Directory pour WorkSpaces.

Table des matières

- Installation des fichiers modèles d'administration de stratégie de groupe pour le protocole de WorkSpaces streaming (WSP)
- Gérer les paramètres de stratégie de groupe pour le protocole de WorkSpaces streaming (WSP)
- Installation du modèle d'administration de stratégie de groupe
- Gérer les paramètres de stratégie de groupe pour PCoIP
- 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
  - Conditions préalables à l'utilisation de Zoom pour WorkSpaces
  - Créez la clé de registre sur un WorkSpaces hôte Windows
  - Dépannage

Installation des fichiers modèles d'administration de stratégie de groupe pour le protocole de WorkSpaces streaming (WSP)

Pour utiliser les paramètres de stratégie de groupe spécifiques à l'utilisation WorkSpaces du protocole de WorkSpaces streaming (WSP), vous devez ajouter le modèle d'administration de stratégie de groupe `wsp.admx` et `wsp.adml` les fichiers pour WSP 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 le modèle d'administration de stratégie de groupe pour WSP

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. Développez 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, AWS Directory Service crée une unité organisationnelle (UO) *`yourdomainname`* 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 un objet de stratégie de groupe, au lieu de sélectionner la stratégie de domaine par défaut, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici.
> Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

7. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
8. Vous pouvez désormais utiliser cet objet de stratégie de groupe WSP pour modifier les paramètres de stratégie de groupe spécifiques à WorkSpaces l'utilisation de WSP.

Gérer les paramètres de stratégie de groupe pour le protocole de WorkSpaces streaming (WSP)

Utilisez les paramètres de stratégie de groupe pour gérer vos systèmes Windows WorkSpaces qui utilisent WSP.

Configuration de la prise en charge de l'imprimante pour WSP

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 (non disponible pour WSP) vous permet d'utiliser des fonctionnalités spécifiques de votre imprimante, comme l'impression recto-verso, mais 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 que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

> **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. À la place, sélectionnez l'UO *votrenomdedomaine* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici.

Pour plus d'informations sur l'UO *votrenomdedomaine*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Configure remote printing.
10. Dans la boîte de dialogue Configure remote printing (Configurer l'impression à distance) effectuez l'une des actions suivantes :
    - Pour activer la redirection d'imprimante locale, choisissez Activé, puis pour les options d'impression, choisissez Basique. Pour utiliser automatiquement l'imprimante par défaut actuelle de l'ordinateur client, sélectionnez Mapper l'imprimante locale par défaut à l'hôte distant.
    - Pour désactiver l'impression, choisissez Désactivé.
11. Choisissez OK.
12. 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 du presse-papiers pour WSP

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. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.

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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Configure clipboard redirection.
10. 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.
11. Choisissez OK.

12. 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 d'une taille supérieure 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.

Définition du délai d'expiration de reprise de session pour WSP

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. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

> **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. À la place, sélectionnez l'UO *votrenomdedomaine* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *votrenomdedomaine*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver la reconnexion automatique.
10. Dans la boîte de dialogue Activer/désactiver la reconnexion automatique, choisissez Activé, puis définissez le délai de reconnexion (en secondes) souhaité.
11. Choisissez OK.
12. 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`**.

Activation ou désactivation de la redirection d'entrée vidéo pour WSP

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 activer ou désactiver la redirection vidéo entrante pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.

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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver la redirection d'entrée vidéo.
10. Dans la boîte de dialogue Activer/désactiver la redirection d'entrée vidéo, choisissez Activée ou Désactivée.
11. Choisissez OK.
12. 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`**.

Activation ou désactivation de la redirection d'entrée audio pour WSP

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 activer ou désactiver la redirection d'entrée audio pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver la redirection d'entrée audio.
10. Dans la boîte de dialogue Activer/désactiver la redirection d'entrée audio, choisissez Activée ou Désactivée.
11. Choisissez OK.

12. 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`**.

Activation ou désactivation de la redirection de sortie audio pour WSP

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 activer ou désactiver la redirection de sortie audio pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de politique de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

> **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici.

> Pour plus d'informations sur l'UO *votrenomdedomaine*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver la redirection de sortie audio.
10. Dans la boîte de dialogue Activer/désactiver la redirection de sortie audio, choisissez Activée ou Désactivée.
11. Choisissez OK.
12. 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`**.

Désactivation de la redirection de fuseau horaire pour WSP

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. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver la redirection de fuseau horaire.
10. Dans la boîte de dialogue Activer/désactiver la redirection de fuseau horaire, choisissez Désactivée.
11. Choisissez OK.
12. 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`**.

13. 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 WSP

Pour WSP, les données en transit sont chiffrées à l'aide du chiffrement TLS 1.2. Par défaut, tous les chiffrements suivants sont autorisés, et le client et le serveur négocient le chiffrement à utiliser :

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-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 WSP

1. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

> **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. À la place, sélectionnez l'UO *votrenomdedomaine* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *votrenomdedomaine*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez Configurer les paramètres de sécurité.
10. 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.
11. Choisissez OK.
12. 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 WSP

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 WSP

1. Assurez-vous que le modèle d'administration de politique de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Configurer les extensions.
10. Dans la boîte de dialogue Configurer les extensions, choisissez Activé, puis définissez l'option souhaitée. Choisissez Client uniquement, Serveur et client ou Serveur uniquement.
11. Choisissez OK.
12. 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`**.

Activation ou désactivation de la redirection de carte à puce pour WSP

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 de l'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 plus d'informations, consultez Utilisation de cartes à puce pour l'authentification.

Pour activer ou désactiver la redirection par carte à puce pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

> **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. À la place, sélectionnez l'UO *votrenomdedomaine* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *votrenomdedomaine*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver la redirection de carte à puce.
10. Dans la boîte de dialogue Activer/désactiver la redirection de carte à puce, choisissez Activée ou Désactivée.
11. Choisissez OK.
12. 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).

Activer ou désactiver la redirection WebAuthn (FIDO2) pour WSP

Par défaut, Amazon WorkSpaces autorise l'utilisation d' WebAuthn authentificateurs pour l'authentification en cours de session. L'authentification en cours de session fait référence à l' WebAuthn authentification effectuée après la connexion et demandée par les applications Web exécutées au cours de la session.

Prérequis

WebAuthn La redirection (FIDO2) pour WSP nécessite les éléments suivants :

- Agent hôte WSP version 2.0.0.1425 ou supérieure
- WorkSpaces clients :

  - Linux Ubuntu 22.04 2023.3 ou supérieur
  - Windows 5.19.0 ou supérieur
  - Client Mac 5.19.0 ou supérieur
- Navigateurs Web installés sur votre ordinateur WorkSpaces exécutant l'extension de WebAuthn redirection Amazon DCV :
  - Google Chrome 116 et versions ultérieures
  - Microsoft Edge 116 et versions ultérieures

Activation ou désactivation de la WebAuthn redirection (FIDO2) pour Windows WorkSpaces

Si nécessaire, vous pouvez activer ou désactiver la prise en charge de l'authentification en cours de session avec WebAuthn les authentificateurs pour Windows à l'aide des paramètres de WorkSpaces stratégie de groupe. Si vous activez ou ne configurez pas ce paramètre, la WebAuthn redirection sera activée et les utilisateurs pourront utiliser des authentificateurs locaux au sein de la télécommande. WorkSpace

Lorsque la fonctionnalité est activée, toutes les WebAuthn demandes du navigateur pendant la session sont redirigées vers le client local. Les utilisateurs peuvent utiliser Windows Hello ou des dispositifs de sécurité connectés localement tels que YubiKey d'autres authentificateurs conformes à la norme FIDO2 pour terminer le processus d'authentification.

Pour activer ou désactiver la redirection WebAuthn (FIDO2) pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

> **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. À la place, sélectionnez l'UO *votrenomdedomaine* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *votrenomdedomaine*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver WebAuthn la redirection.
10. Dans la boîte de dialogue Activer/désactiver WebAuthn la redirection, choisissez Activé ou Désactivé.
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).

Installation de l'extension de WebAuthn redirection Amazon DCV

Les utilisateurs devront installer l'extension de WebAuthn redirection Amazon DCV à utiliser une WebAuthn fois la fonctionnalité activée en effectuant l'une des opérations suivantes :

- Vos 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 WSP 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 en utilisant la politique GPO ci-dessous.

- Vous pouvez forcer l'installation de l'extension de redirection pour vos utilisateurs en utilisant la politique GPO ci-dessous. Si vous activez la politique GPO, l'extension sera automatiquement installée lorsque vos utilisateurs lanceront les navigateurs compatibles avec accès à Internet.
- Vos utilisateurs peuvent installer l'extension manuellement à l'aide des modules complémentaires Microsoft Edge ou du Chrome Web Store.

Gérez et installez 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. Développez 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, consultez la section Définir les règles du navigateur Chrome sur les PC administrés.
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. Développez 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, 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 :

    ```
    {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
    { "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 :
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Activation ou désactivation de la déconnexion de session au verrouillage de l'écran pour WSP

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 plus d'informations, consultez Utilisation de cartes à puce pour l'authentification.

Pour activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer/désactiver la déconnexion de session au verrouillage de l'écran.
10. Dans la boîte de dialogue Activer/désactiver la déconnexion de session au verrouillage de l'écran, choisissez Activée ou Désactivée.
11. Choisissez OK.
12. 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`**.

Activer ou désactiver le pilote d'affichage indirect (IDD) pour WSP

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 activer ou désactiver le pilote d'affichage indirect (IDD) pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
2. Sur une instance d'administration d'annuaire WorkSpace ou sur une instance Amazon Elastic Compute Cloud associée à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc).
3. Développez la forêt (forest: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 contexte en cliquant avec le bouton droit sur le menu, puis choisissez Modifier.

> **Note**
>
> Si le domaine sous-jacent WorkSpaces est un annuaire Microsoft AD AWS géré, vous ne pouvez pas utiliser la politique de domaine par défaut pour créer votre GPO. Sélectionnez plutôt l'unité `yourdomainname` organisationnelle (UO) ou toute unité d'organisation sous ce nom de domaine, ouvrez le contexte en cliquant avec le bouton droit sur le menu, puis choisissez Créer un objet de stratégie de groupe dans ce domaine, puis liez-le ici. Pour plus d'informations sur l'unité d'`yourdomainname`organisation, reportez-vous à la section What Gets Created du Guide d'administration du AWS Directory Service.

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Activer le pilote d'affichage AWS indirect.
10. Dans la boîte de dialogue Activer le pilote d'affichage AWS indirect, choisissez Activé ou Désactivé.
11. Choisissez OK.
12. 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 WSP

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 à YUV420. Sélectionnez Activer le codage YUV444 pour bénéficier d'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. Assurez-vous que le modèle d'administration de politique de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Configurer les paramètres d'affichage.
10. 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.

11. Choisissez OK.
12. 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`**.

Activer ou désactiver VSync pour le pilote d'affichage AWS virtuel uniquement pour WSP

Par défaut, WorkSpaces prend en charge l'utilisation de la fonction VSync pour le pilote d'affichage AWS virtuel uniquement. Si cela est nécessaire pour Windows WorkSpaces, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver cette fonctionnalité.

Pour activer ou désactiver VSync pour Windows WorkSpaces

1. Assurez-vous que le modèle d'administration de politique de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
2. Sur une instance d'administration d'annuaire WorkSpace ou sur une instance Amazon Elastic Compute Cloud associée à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe (gpmc.msc).
3. Développez la forêt (forest: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 contexte en cliquant avec le bouton droit sur le menu, puis choisissez Modifier.

> **Note**
>
> Si le domaine sous-jacent WorkSpaces est un annuaire Microsoft AD AWS géré, vous ne pouvez pas utiliser la politique de domaine par défaut pour créer votre GPO. Choisissez plutôt l'unité `yourdomainname` organisationnelle (UO) ou toute unité d'organisation sous

ce nom de domaine, ouvrez le contexte en cliquant avec le bouton droit sur le menu, puis choisissez Créer un objet de stratégie de groupe dans ce domaine, puis liez-le ici. Pour plus d'informations sur l'unité d'`yourdomainname`organisation, consultez la section What gets created dans le Guide d'administration du AWS Directory Service.

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez la fonction Enable VSync du paramètre AWS Virtual Display Only Driver.
10. Dans la fonction Enable VSync de la boîte de dialogue AWS Virtual Display Only Driver, choisissez Activé ou Désactivé.
11. Choisissez OK.
12. 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 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 à nouveau l'espace de travail.

Configuration du niveau de détail des journaux pour WSP

Par défaut, le niveau de verbosité du journal pour WSP 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. Assurez-vous que le modèle d'administration de politique de WorkSpaces groupe le plus récent pour WSP est installé dans le magasin central du contrôleur de domaine de votre WorkSpaces annuaire.
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. Développez 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.

   > **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. À la place, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici. Pour plus d'informations sur l'UO *`votrenomdedomaine`*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, Amazon et WSP.
9. Ouvrez le paramètre Configurer le niveau de détail des journaux.
10. 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.
11. Choisissez OK.
12. 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 d'administration de stratégie de groupe

Pour utiliser les paramètres de stratégie de groupe spécifiques à Amazon WorkSpaces lors de l'utilisation du protocole PCoIP, vous devez ajouter le modèle d'administration de stratégie de groupe adapté à la version de l'agent PCoIP (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 et vérifiez sa valeur dans la colonne Plateforme pour déterminer si l'agent PCoIP 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 PCoIP (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 PCoIP

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, Policies 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 ce GPO pour modifier les paramètres de stratégie de groupe 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, choisissez Computer Configuration, Policies, Administrative Templates, Classic Administrative Templates, puis PCoIP Session Variables.

3. Vous pouvez désormais utiliser cet objet de politique de groupe de variables de session PCoIP pour modifier les paramètres de stratégie de groupe spécifiques à Amazon WorkSpaces lors de l'utilisation de PCoIP.

> **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 PCoIP (64 bits)

Pour utiliser les paramètres de stratégie de groupe spécifiques au WorkSpaces protocole PCoIP, vous devez ajouter le modèle d'administration de stratégie de groupe `PCoIP.admx` et `PCoIP.adml` les fichiers pour PCoIP dans le magasin central du contrôleur de domaine de votre répertoire. WorkSpaces 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 de modèle d'administration de stratégie de groupe pour PCoIP

1. À partir d'un système Windows en cours d'exécution WorkSpace, faites une copie `PCoIP.adml` des fichiers `PCoIP.admx` et du `C:\Program Files\Teradici\PCoIP Agent \configuration\policyDefinitions` répertoire. Le fichier `PCoIP.adml` 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 `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 `PCoIP.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 `PCoIP.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. Développez 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, AWS Directory Service crée une unité organisationnelle (UO) *`yourdomainname`* 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 un objet de stratégie de groupe, au lieu de sélectionner la stratégie de domaine par défaut, sélectionnez l'UO *`votrenomdedomaine`* (ou toute UO sous celle-ci), ouvrez le menu contextuel (clic droit), puis choisissez Créer un GPO dans ce domaine et le lier ici.

Pour plus d'informations sur l'UO *votrenomdedomaine*, consultez Ce qui est créé dans le Guide d'administration AWS Directory Service .

7. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration informatique, Politiques, Modèles d'administration, puis Variables de session PCoIP.
8. Vous pouvez désormais utiliser cet objet de stratégie de groupe de variables de session PCoIP pour modifier les paramètres de stratégie de groupe spécifiques à l'utilisation de WorkSpaces PCoIP.

> **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 PCoIP

Utilisez les paramètres de stratégie de groupe pour gérer vos systèmes Windows WorkSpaces utilisant PCoIP.

Configuration de la prise en charge de l'imprimante pour PCoIP

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 le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
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 le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
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`**.

Activation ou désactivation de la redirection du presse-papiers pour PCoIP

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 le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
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 d'une taille supérieure 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.

Définition du délai d'expiration de reprise de session pour PCoIP

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 le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
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`**.

Activation ou désactivation de la redirection d'entrée audio pour PCoIP

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 le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
3. Ouvrez le paramètre Activer/désactiver l'audio dans la session PCoIP.
4. Dans la boîte de dialogue Activer/désactiver l'audio dans la session PCoIP, 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`**.

Désactivation de la redirection de fuseau horaire pour PCoIP

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 le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
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

Pour PCoIP, les données en transit sont chiffrées à l'aide du chiffrement TLS 1.2 et de la signature de requêtes SigV4. Le protocole PCoIP utilise le trafic UDP chiffré, avec chiffrement 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 définir cette valeur par défaut à 256 bits à l'aide du paramètre de stratégie de groupe Configurer les paramètres de sécurité PCoIP.

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 concernant ces paramètres et les suites de chiffrement prises en charge est fournie dans la boîte de dialogue de stratégie de groupe Configurer les paramètres de sécurité PCoIP.

Pour configurer les paramètres de sécurité PCoIP

1. Assurez-vous d'avoir installé le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
3. Ouvrez le paramètre Configurer les paramètres de sécurité PCoIP.
4. Dans la boîte de dialogue Configurer les paramètres de sécurité PCoIP, choisissez Activé. Pour définir le chiffrement par défaut du trafic de streaming à 256 bits, accédez à l'option Chiffrements des données PCoIP, puis 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 PCoIP.
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`**.

Activer la redirection USB pour YubiKey U2F

> **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 YubiKey U2F

1. Assurez-vous d'avoir installé le modèle d'administration de stratégie de WorkSpaces groupe le plus récent pour PCoIP (32 bits) ou le modèle d'administration de stratégie de WorkSpaces groupe pour PCoIP (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 aux variables de session PCoIP.
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 par PCoIP.
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 combinaison VID/PID est 1xxxxyyyy, où xxxx représente le VID et yyyy le PID, au format hexadécimal. Dans cet exemple, 1050 est le VID et 0407 le PID. Pour plus de valeurs YubiKey USB, voir Valeurs d'identifiant 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 règles d'autorisation/de non-autorisation, consultez Teradici PCoIP Standard Agent for 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 toujours 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 Activation des capacités de gestion d'instances WorkSpaces en libre-service pour les utilisateurs.

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 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 WSP WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et ultérieure) et l'application cliente macOS (version 5.4 et ultérieure) 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.

Le protocole de streaming WorkSpaces (WSP) ne prend pas en charge l'utilisation d'un proxy pour le trafic des espaces de travail via UDP. Seules les applications clientes de bureau WorkSpaces Windows et macOS et l'accès Web WSP 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

Tout utilisateur disposant de l'autorisation administrateur pour Active Directory peut générer une clé de registre à l'aide de son objet de stratégie de groupe (GPO). Cela permet à l'utilisateur d'envoyer la clé de registre à toutes les fenêtres de votre domaine WorkSpaces à l'aide d'une mise à jour forcée. Les clients disposant de droits d'administrateur peuvent également installer les clés de registre individuellement sur leur WorkSpaces hôte.

Conditions préalables à l'utilisation de Zoom pour WorkSpaces

Version WorkSpaces client prise en charge : Windows : 5.4.0.xxxx ou supérieur.

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. Cliquez sur la nouvelle valeur 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.

Dépannage

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, AWS Support contactez le AWS 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>

    <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 WorkSpaces

Comme pour Windows WorkSpaces, Amazon Linux WorkSpaces est joint à un domaine. Vous pouvez donc utiliser les utilisateurs et les groupes Active Directory pour :

- Administrez votre Amazon Linux WorkSpaces
- Fournir un accès à ceux-ci WorkSpaces aux utilisateurs

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 AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise ou Ansible.

> **Note**
>
> La redirection d'imprimante locale n'est pas disponible pour Amazon Linux WorkSpaces.

Comportement du protocole WSP (Control WorkSpaces Streaming Protocol) sur Amazon Linux WorkSpaces

Le comportement du WSP est contrôlé par les paramètres de configuration du fichier `wsp.conf`, stocké dans le répertoire `/etc/wsp/`. 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 offres groupées Amazon Linux WorkSpaces sur WSP 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 WSP Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Si nécessaire, utilisez le fichier de configuration WSP pour configurer cette fonctionnalité. Ce paramètre prend effet lorsque vous déconnectez et reconnectez le WorkSpace.

Pour configurer la redirection du presse-papiers pour WSP 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 WSP Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée audio. Si nécessaire, utilisez le fichier de configuration WSP pour désactiver cette fonctionnalité. 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 WSP 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 WSP Amazon 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 qui voyagent beaucoup veulent rester WorkSpaces dans le même fuseau horaire pour des raisons de cohérence et de préférence personnelle.

Si nécessaire, utilisez le fichier de configuration WSP pour configurer cette fonctionnalité. 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 WSP 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 PCoIP sur Amazon Linux WorkSpaces

Le comportement de l'agent PCoIP est contrôlé par les paramètres de configuration du fichier `pcoip-agent.conf`, stocké dans le répertoire `/etc/pcoip-agent/`. 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 PCoIP Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection du presse-papiers. Si nécessaire, utilisez le fichier de configuration de l'agent PCoIP pour désactiver cette fonctionnalité. Ce paramètre prend effet lorsque vous redémarrez le WorkSpace.

Pour configurer la redirection du presse-papiers pour PCoIP 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 PCoIP Virtual Channels dans la documentation Teradici.

Activer ou désactiver la redirection d'entrée audio pour PCoIP Amazon Linux WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection d'entrée audio. Si nécessaire, utilisez le fichier de configuration de l'agent PCoIP pour désactiver cette fonctionnalité. Ce paramètre prend effet lorsque vous redémarrez le WorkSpace.

Pour activer ou désactiver la redirection d'entrée audio pour PCoIP 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 PCoIP Amazon 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 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 PCoIP pour désactiver cette fonctionnalité. Ce paramètre prend effet lorsque vous redémarrez le WorkSpace.

Pour activer ou désactiver la redirection de fuseau horaire pour PCoIP (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.

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 (ACL) réseau 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 plus d'informations, consultez Fournissez un accès à Internet depuis votre WorkSpace.

Utiliser des cartes à puce pour l'authentification sous Linux WorkSpaces

Les packs Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) permettent d'utiliser des cartes à puce CAC (Common Access Card) et PIV (Personal Identity Verification) pour l'authentification. Pour plus d'informations, consultez Utilisation de cartes à puce pour l'authentification.

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 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 WSP WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et ultérieure) et l'application cliente macOS (version 5.4 et ultérieure) 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.

Le protocole de streaming WorkSpaces (WSP) ne prend pas en charge l'utilisation d'un proxy pour le trafic des espaces de travail via UDP. Seules les applications clientes de bureau WorkSpaces Windows et macOS et l'accès Web WSP 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

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 à l'aide d'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.

Comportement du protocole WSP (Control WorkSpaces Streaming Protocol) sur Ubuntu WorkSpaces

Le comportement du WSP est contrôlé par les paramètres de configuration du fichier `wsp.conf`, stocké dans le répertoire `/etc/wsp/`. 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. Si nécessaire, utilisez le fichier de configuration WSP pour désactiver cette fonctionnalité.

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. Si nécessaire, utilisez le fichier de configuration WSP pour désactiver cette fonctionnalité.

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. Si nécessaire, utilisez le fichier de configuration WSP pour désactiver cette fonctionnalité.

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 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.

Si nécessaire, utilisez le fichier de configuration WSP pour configurer cette fonctionnalité.

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-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 Ubuntu WorkSpaces

Par défaut, WorkSpaces prend en charge la redirection de l'imprimante. Si nécessaire, utilisez le fichier de configuration WSP pour désactiver cette fonctionnalité.

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.

Activation ou désactivation de la déconnexion de session au verrouillage de l'écran pour WSP

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 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, WorkSpaces ne prend pas en charge la déconnexion de la session lors du verrouillage de l'écran. Si nécessaire, utilisez le fichier de configuration WSP pour activer cette fonctionnalité.

Pour activer ou désactiver la session de déconnexion lors du verrouillage de l'écran pour Windows 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.

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 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 WSP WorkSpaces, l'application cliente WorkSpaces Windows (version 5.1 et ultérieure) et l'application cliente macOS (version 5.4 et ultérieure) 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.

Le protocole de streaming WorkSpaces (WSP) ne prend pas en charge l'utilisation d'un proxy pour le trafic des espaces de travail via UDP. Seules les applications clientes de bureau WorkSpaces Windows et macOS et l'accès Web WSP 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.

Optimisez Amazon WorkSpaces pour une communication en temps réel

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 salons de chat individuel, des canaux de chat de groupe collaboratives, le stockage et l'échange fluides de fichiers, des événements en direct, des webinaires, des diffusions, le partage et le contrôle interactifs d'écran, des tableaux blancs et des capacités de messagerie audio/vidéo hors ligne. 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

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 protocole de WorkSpaces streaming vers le périphérique 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		

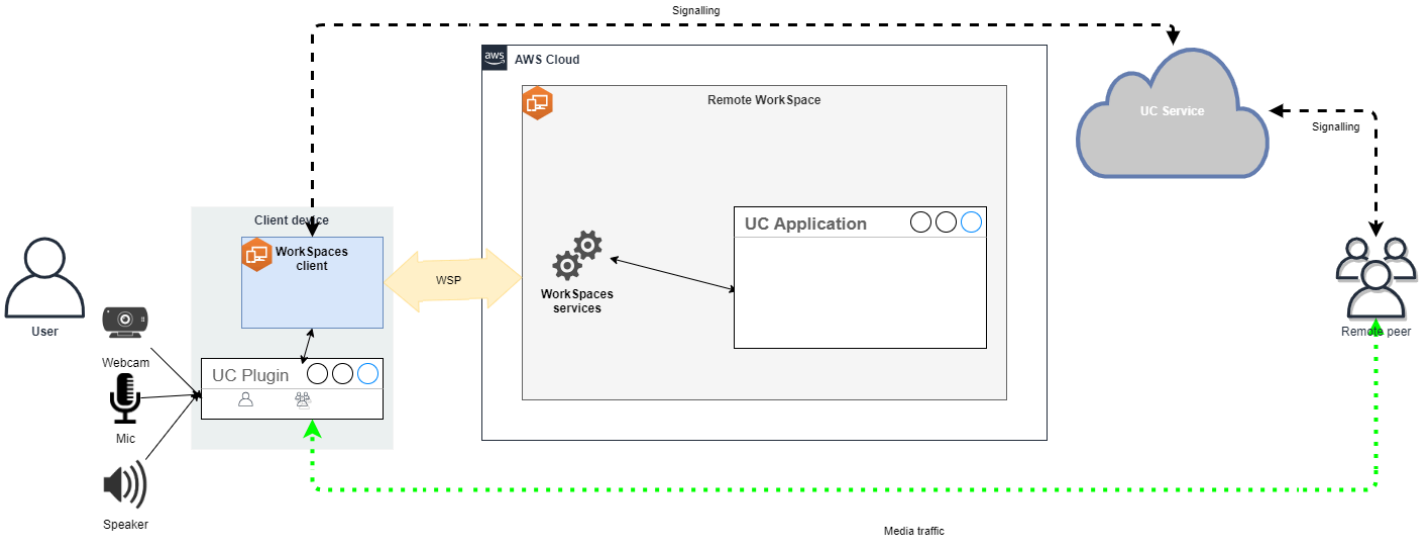
Fonctionnalité	RTC directe	RTC optimisée pour les médias	RTC optimisée en cours de session
Salons de chat de groupe	Ne nécessite pas de configuration de la RTC		
Audioconférence de groupe	Meilleur	Meilleur	Bon
Visioconférence de groupe	Bon	Meilleur	Bon
Appels audio individuels	Meilleur	Meilleur	Bon
Appels vidéo individuels	Bon	Meilleur	Bon
Tableaux blancs	Ne nécessite pas de configuration de la RTC		
Clips audio/vidéo/ messagerie	Ne s'applique pas	Bon	Meilleur
Partage de fichiers	Ne s'applique pas	Dépend de l'application d'UC	Meilleur
Partage et contrôle d'écran	Ne s'applique pas	Dépend de l'application d'UC	Meilleur
Webinaires/événements de diffusion	Ne s'applique pas	Bon	Meilleur

Conseils d'optimisation de la communication en temps réel (RTC)

Configuration de la RTC optimisée pour les médias

Le mode RTC optimisée pour les médias est possible quand le fournisseur d'applications d'UC utilise les kits SDK fournis 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 PCoIP et WSP) WorkSpaces
- Réunions Cisco Webex (pour WSP uniquement) WorkSpaces

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.

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.

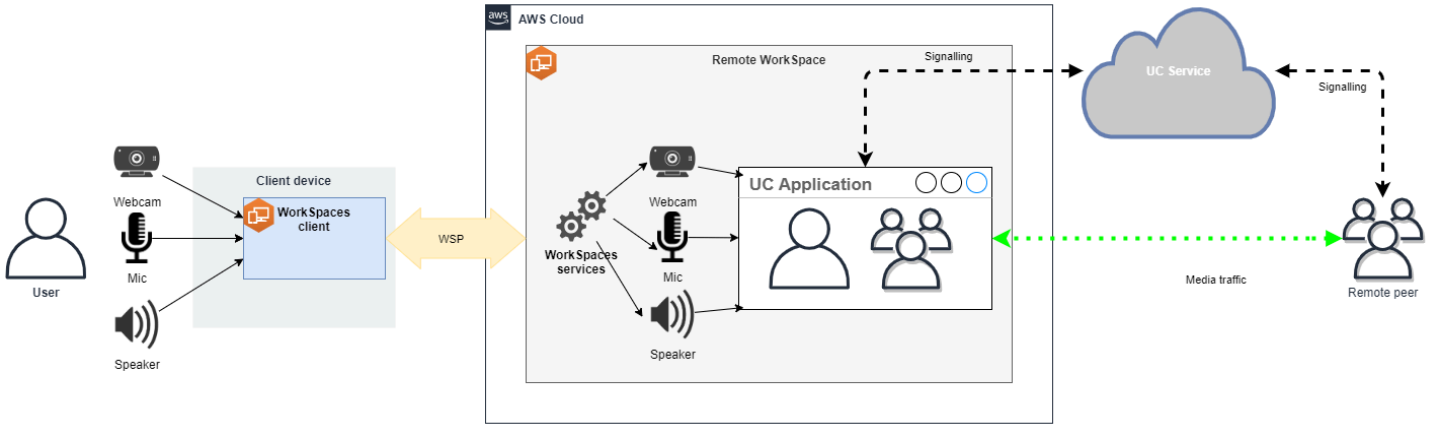
- Les extensions client d'UC peuvent ne pas être disponibles sur certaines plateformes client, comme les plateformes mobiles ou les clients Web.
- Certaines fonctionnalités d'applications d'UC peuvent être limitées dans ce mode. Par exemple, le fonctionnement du partage d'écran peut être différent.
- 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 le protocole de WorkSpaces streaming (WSP) et transmis au client. Au niveau du client, les signaux du microphone (sur WSP et PCoIP WorkSpaces) et de la webcam (uniquement sur WSP 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.



WorkSpaces Le protocole de streaming (WSP) a été méticuleusement optimisé pour améliorer les performances du mode RTC à distance. 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 :

			Appels vidéo		Appels audio		
Application	Configuration du CPU requise pour l'application de RTC	Exigences de RAM pour l'application de RTC	Pris en charge de manière minimale WorkSpace	Recommandé WorkSpace	Pris en charge de manière minimale WorkSpace	Recommandé WorkSpace	Référence
Microsoft Teams	2 cœurs obligatoires, 4	4 Go de RAM	Power (4 vCPU, 16 Go de mémoire)	PowerPro (8 vCPU, 32 Go de mémoire)	Performance (2 vCPU,	Power (4 vCPU, 16 Go de mémoire)	Configuration matérielle requise

			Appels vidéo		Appels audio		
Application	Configuration du CPU requise pour l'application de RTC	Exigences de RAM pour l'application de RTC	Pris en charge de manière minimale WorkSpace	Recommandé WorkSpace	Pris en charge de manière minimale WorkSpace	Recommandé WorkSpace	Référence
	recommandés				8 Go de mémoire)		pour Microsoft Teams
Zoom	2 cœurs obligatoires, 4 recommandés	4 Go de RAM	Power (4 vCPU, 16 Go de mémoire)	PowerPro (8 vCPU, 32 Go de mémoire)	Performance (2 vCPU, 8 Go de mémoire)	Power (4 vCPU, 16 Go de mémoire)	Configuration système requise pour Zoom : Windows, macOS, Linux
Webex	2 cœurs obligatoires	4 Go de RAM	Power (4 vCPU, 16 Go de mémoire)	PowerPro (8 vCPU, 32 Go de mémoire)	Performance (2 vCPU, 8 Go de mémoire)	Power (4 vCPU, 16 Go de mémoire)	Configuration requise 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 PowerPro configuration.

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 le protocole de WorkSpaces streaming (WSP)

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 WSP. 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 WSP 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 ou PowerPro WorkSpaces pour la visioconférence, il est fortement recommandé de limiter la résolution maximale des webcams redirigées. Dans le cas de PowerPro, la résolution maximale recommandée est de 640 pixels de largeur sur 480 pixels de 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
   ```

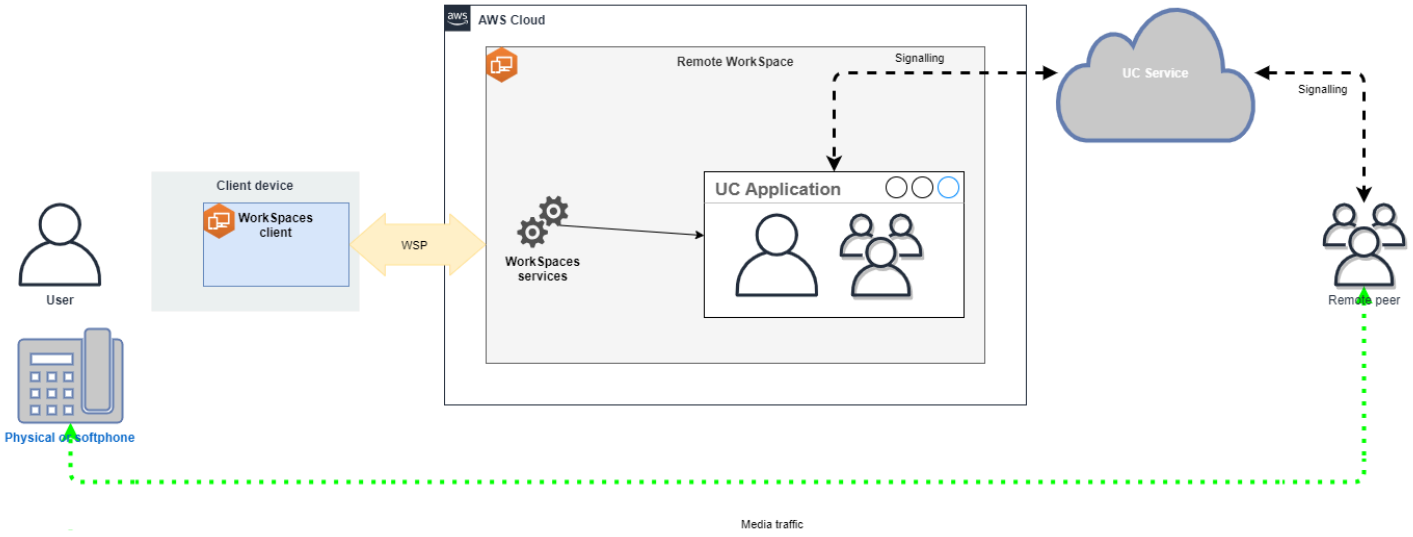
3. Créez un nom de valeur de chaîne `default-profile` et définissez-le à `voice`.

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

Gestion du mode d'exécution d'une instance WorkSpace

Le mode d'exécution d'une instance WorkSpace détermine sa disponibilité immédiate et son mode de tarification (mensuel ou horaire). Vous pouvez choisir entre les modes d'exécution suivants lorsque vous créez l'instance WorkSpace :

- AlwaysOn : à utiliser lorsque vous payez des frais mensuels fixes pour une utilisation illimitée des instances WorkSpaces. Ce mode convient mieux aux utilisateurs qui se servent de leur instance WorkSpace à plein temps comme bureau principal.
- AutoStop : à utiliser lorsque vous payez les instances WorkSpaces à l'heure. Avec ce mode, les instances WorkSpace s'arrêtent après une période d'inactivité spécifiée, et l'état des applications et des données est enregistré.

Pour plus d'informations, consultez Tarification Amazon WorkSpaces.

Instances WorkSpaces AutoStop

Pour définir l'heure d'arrêt automatique, sélectionnez l'instance WorkSpace dans la console Amazon WorkSpaces, choisissez Actions, Modification des propriétés du mode d'exécution, puis définissez l'option Temps AutoStop (heures). Par défaut, l'option Temps AutoStop (heures) est définie à 1 heure, ce qui signifie que l'instance WorkSpace s'arrête automatiquement une heure après sa déconnexion.

Une fois qu'une instance WorkSpace est déconnectée et que le délai défini pour Temps AutoStop a expiré, l'arrêt automatique de l'instance WorkSpace peut prendre plusieurs minutes supplémentaires. Toutefois, la facturation s'arrête dès que le délai défini pour Temps AutoStop expire, et ces minutes supplémentaires ne vous sont pas facturées.

Lorsque c'est possible, l'état du bureau est enregistré dans le volume racine de l'espace de travail. L'instance WorkSpace reprend lorsqu'un utilisateur se connecte, et lorsque tous les documents ouverts et les programmes en cours d'exécution reviennent à leur état enregistré.

Les instances WorkSpaces AutoStop Graphics.g4dn, GraphicsPro.g4dn, Graphics et GraphicsPro ne préservent pas l'état des données et des programmes lorsqu'elles s'arrêtent. Pour ces instances WorkSpaces Autostop, nous vous recommandons d'enregistrer votre travail à chaque fois que vous avez fini de les utiliser.

Pour les instances WorkSpaces AutoStop Apportez votre propre licence (BYOL), un grand nombre de connexions simultanées peut entraîner une augmentation significative de leur temps de disponibilité. Si vous pensez qu'un grand nombre d'utilisateurs se connecteront aux instances WorkSpaces AutoStop BYOL en même temps, veuillez contacter votre responsable de compte pour obtenir des conseils.

> **Important**
>
> Les instances WorkSpaces AutoStop ne s'arrêtent automatiquement que si elles sont déconnectées.

Une instance WorkSpace est déconnectée uniquement dans les cas suivants :

- Si l'utilisateur se déconnecte manuellement de l'instance WorkSpaces ou quitte l'application client Amazon WorkSpaces.
- Si l'appareil client est arrêté.
- S'il n'y a aucune connexion entre l'appareil client et l'instance WorkSpace pendant plus de 20 minutes.

Il est recommandé aux utilisateurs de se déconnecter chaque jour manuellement de leurs instances WorkSpaces AutoStop lorsqu'ils ont fini de les utiliser. Pour vous déconnecter manuellement, choisissez Déconnecter une instance WorkSpace ou Quitter Amazon WorkSpaces dans le menu Amazon WorkSpaces des applications client WorkSpaces pour Linux, macOS ou Windows. Pour Android ou iPad, choisissez Déconnecter dans le menu latéral.

Les instances WorkSpaces AutoStop peuvent ne pas s'arrêter automatiquement dans les cas suivants :

- Si l'appareil client est seulement verrouillé, en veille ou inactif (par exemple, quand le capot d'un ordinateur portable est fermé) au lieu d'être arrêté, l'application WorkSpaces est peut toujours être en cours d'exécution à l'arrière-plan. Tant que l'application WorkSpaces est toujours en cours d'exécution, il est possible que l'instance WorkSpace ne soit pas déconnectée et qu'elle ne s'arrête donc pas automatiquement.
- WorkSpaces ne peut détecter la déconnexion que lorsque les utilisateurs utilisent des clients WorkSpaces. Si les utilisateurs utilisent des clients tiers, WorkSpaces peut ne pas détecter la déconnection. Dans ce cas, l'instance WorkSpace peut ne pas s'arrêter automatiquement et la facturation risque de ne pas être interrompue.

Modification du mode d'exécution

Vous pouvez changer de mode d'exécution à tout moment.

Pour modifier le mode d'exécution d'une instance WorkSpace

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Sélectionnez les instances WorkSpaces à modifier, puis choisissez Actions, Modifier le mode d'exécution.
4. Sélectionnez le nouveau mode d'exécution, AlwaysOn ou AutoStop, puis choisissez Enregistrer.

Pour modifier le mode d'exécution d'une instance WorkSpace à l'aide de AWS CLI

Utilisez la commande modify-workspace-state.

Arrêt et démarrage d'une instance WorkSpace AutoStop

Lorsque vos instances WorkSpaces AutoStop sont pas déconnectées, elles sont automatiquement arrêtées après une période d'inactivité spécifiée, et le relevé horaire est interrompu. Afin d'optimiser davantage les coûts, vous pouvez interrompre les frais horaires associés aux instances WorkSpaces AutoStop. L'instance WorkSpace s'arrête, et toutes les applications et données sont enregistrées pour la prochaine fois qu'un utilisateur s'y connecte.

Lorsqu'un utilisateur se reconnecte à une instance WorkSpace arrêtée, il reprend là où il s'était arrêté, généralement en moins de 90 secondes.

Vous pouvez redémarrer des instances WorkSpace AutoStop qui sont disponibles ou à l'état d'erreur.

Pour arrêter un espace de travail AutoStop

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Sélectionnez l'instance WorkSpace à arrêter, puis choisissez Actions, Arrêter des WorkSpaces.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter.

Pour démarrer une instance WorkSpace AutoStop

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Sélectionnez les instances WorkSpaces à démarrer, puis choisissez Actions, Démarrer des WorkSpaces.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Démarrer des WorkSpaces.

Pour supprimer les coûts d'infrastructure fixes associés aux instances WorkSpace AutoStop, supprimez l'instance WorkSpace de votre compte. Pour plus d'informations, consultez Suppression d'une instance WorkSpace.

Pour arrêter et démarrer une instance WorkSpace AutoStop avec AWS CLI

Utilisez les commandes stop-WorkSpaces et start-WorkSpaces.

Gestion des applications

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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation de gauche, choisissez WorkSpaces.

3. Sélectionnez 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 WorkSpace ordinateur de différentes manières :

- 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 2021
- Microsoft Visio LTSC Professionnel 2021
- Microsoft Project Professionnel 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021

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 Professionnel Plus 2016 (32 bits)	Microsoft Office Professionnel Plus 2019 (64 bits)	Microsoft LTSC Office Professionnel Plus/Standard 2021 (64 bits)	Microsoft Project Professionnel/Standard 2021 (64 bits)	Microsoft LTSC Visio Professionnel/Standard 2021 (64 bits)
Windows Server 2016	Désinstallation	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Windows Server 2019	Non pris en charge	Désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation
Windows Server 2022	Non pris en charge	Désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation
Windows 10	Désinstallation	Désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation
Windows 11	Désinstallation	Désinstallation	Installation/désinstallation	Installation/désinstallation	Installation/désinstallation

Important

- Ces applications doivent correspondre aux mêmes éditions. Par exemple, vous ne pouvez pas mélanger des applications Standard avec des applications Professionnel.
- Ces applications doivent correspondre aux mêmes versions. Par exemple, vous ne pouvez pas mélanger les applications 2019 avec celles de 2021.

- Microsoft Office/Visio/Project 2021 Standard/Professional ne sont pas pris en charge pour Value, Graphics et les offres groupées. GraphicsPro WorkSpaces
- 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 AWSmarché.
- Pour installer/désinstaller des applications Microsoft 365, vous devez utiliser vos propres outils et programmes d'installation. Le flux de travail Gestion des applications ne peut pas installer/désinstaller les applications Microsoft 365.
- Vous ne pouvez pas créer une image personnalisée WorkSpaces d'applications installées via Gérer les applications, mais vous pouvez créer une image personnalisée à WorkSpaces partir de laquelle vous désinstallez des ensembles d'applications à l'aide de Gérer les applications.
- La résolution DNS doit être activée pour utiliser le flux de travail Gestion des applications.
- Pour les régions optionnelles, telles que l'Afrique (Le Cap), la connexion WorkSpaces Internet doit être activée au niveau de l'annuaire.

Pour mettre à jour les ensembles d'applications sur un WorkSpace

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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 y installer des ensembles d'applications : WorkSpace
   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 celui-ci WorkSpace :

   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 à l'adresse https://console.aws.amazon.com/workspaces/.

    b. Dans le volet de navigation, choisissez 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.

Gestion des WorkSpaces modifications à l'aide de Gérer les applications

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 lorsque 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 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

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 l' WorkSpacesAPI Amazon si vous avez WorkSpace été créé avec des bundles PCoIP.

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 Activation des capacités de gestion d'instances WorkSpaces en libre-service pour les utilisateurs.

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 Graphics.g4dn, GraphicsPro .g4dn, Graphics, ou GraphicsPro WorkSpace avec un minimum de 100 Go pour le volume racine et de 100 Go pour le volume utilisateur.

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.

- À moins qu'il ne WorkSpace s'agisse d'un Graphics.g4dn, GraphicsPro .g4dn, Graphics ou GraphicsPro WorkSpace, le volume racine ne peut pas être inférieur à 175 Go lorsque le volume utilisateur est de 100 Go. Graphics.g4dn, GraphicsPro .g4dn, Graphics, et les volumes root et utilisateur GraphicsPro WorkSpaces peuvent être tous deux définis sur 100 Go minimum.
- 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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-propertiescommande avec la `UserVolumeSizeGib` propriété `RootVolumeSizeGib` or.

Modification du type de calcul

Vous pouvez basculer WorkSpace entre les types Standard, Power, Performance et PowerPro Compute. Pour plus d'informations sur ces types de calcul, consultez Amazon WorkSpaces Bundles.

> **Note**
>
> - Vous pouvez modifier le type de calcul de Graphics.G4DN à .g4dn, ou de GraphicsPro .g4dn à Graphics.G4DN. GraphicsPro Vous ne pouvez pas remplacer le type de calcul de Graphics.g4dn et GraphicsPro .g4dn par une autre valeur.
> - Le bundle Graphics ne sera plus pris en charge après le 30 novembre 2023. Nous vous recommandons de migrer votre offre groupée WorkSpaces vers Graphics.G4DN. Pour plus d'informations, consultez Migrer un WorkSpace.
> - 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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-propertiescommande avec la `ComputeTypeName` propriété.

Modification des protocoles

Si le vôtre WorkSpace est créé avec des bundles PCoIP, vous pouvez modifier leur protocole de streaming à l'aide de la AWS CLI ou de l'API Amazon. WorkSpaces 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 le protocole de WorkSpaces streaming (WSP) et

de gérer votre volume racine sans recréer le PCoIP existant WorkSpaces pendant le processus de migration.

- Vous ne pouvez modifier votre protocole que s'il WorkSpace a été créé avec des bundles PCoIP.
- Avant de modifier le protocole en WSP, assurez-vous que vous WorkSpace répondez aux exigences suivantes pour un WorkSpace WSP.
  - Votre WorkSpaces client soutient WSP
  - La région dans laquelle vous êtes déployé WorkSpace prend en charge WSP
  - Les exigences relatives à l'adresse IP et au port pour WSP sont satisfaites. Pour plus d'informations, consultez la section Exigences relatives à l'adresse IP et au port pour WorkSpaces.
  - Assurez-vous que votre bundle actuel est disponible avec WSP.
  - Pour une expérience optimale de visioconférence, nous vous recommandons d'utiliser Power ou des PowerPro offres groupées 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 de PCoIP à WSP, puis que vous le modifiez à nouveau en PCoIP, vous ne pourrez pas vous y connecter via Web Access. WorkSpaces

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 `WSP`, 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 `WSP`.

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 la WorkSpace marque

Amazon vous WorkSpaces permet de créer une WorkSpaces expérience familière pour vos utilisateurs en utilisant des API pour personnaliser l'apparence de votre page WorkSpace de connexion avec votre propre logo 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

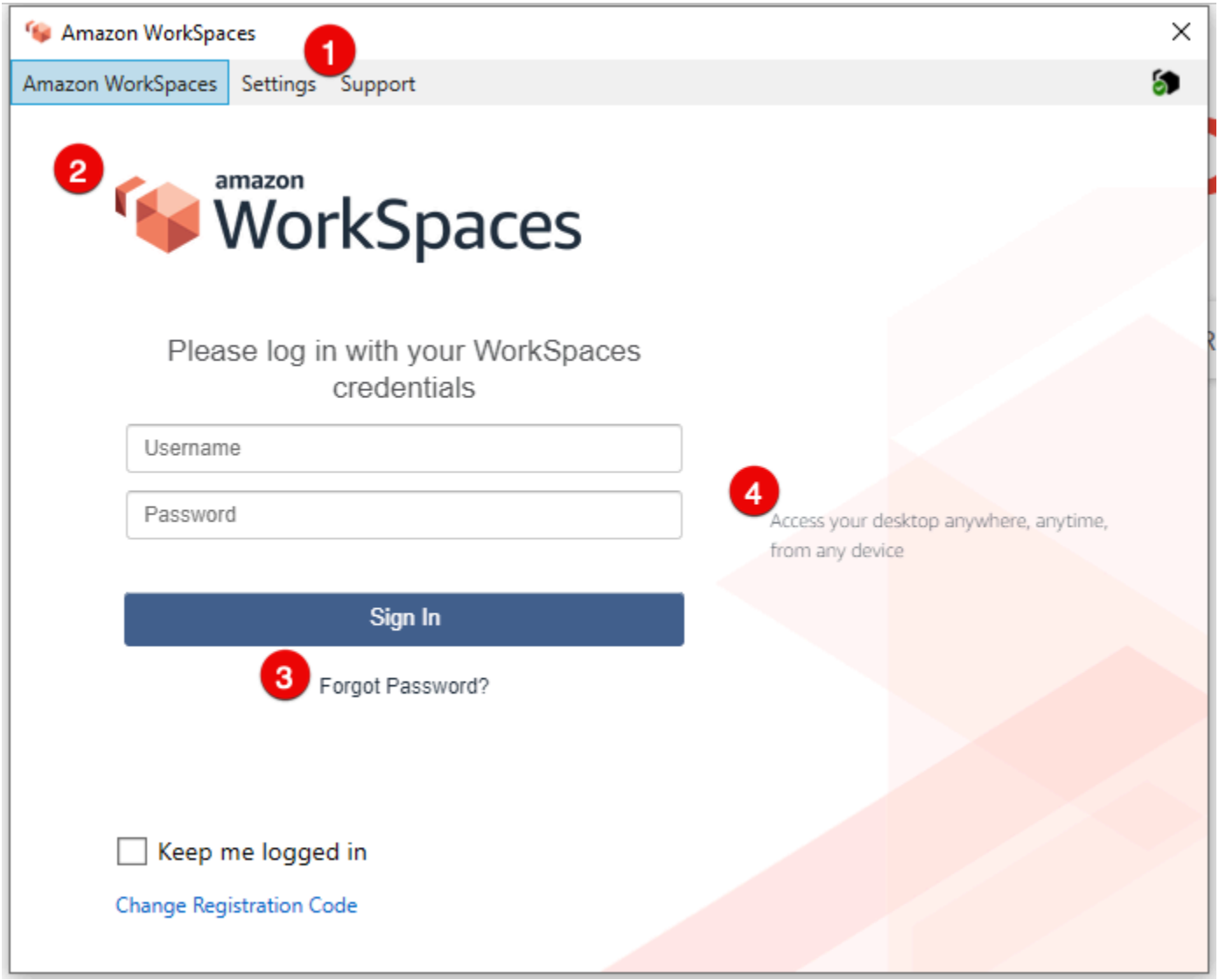
- Web Access

> **Note**
>
> Pour modifier les éléments de marque à l'aide des ClientBranding API duAWS GovCloud (US) Region, utilisez une version WorkSpaces client 5.10.0.

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.



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	• Pour chaque type de plateforme, les paramètre

Élément de personnalisation	Description	Exigences et recommandations
	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` .	s `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` . • 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 `LoginMessage` , 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 : `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

Vous trouverez ci-dessous des exemples d'extraits de code à utiliser. ImportClientBranding

Version 2 de la CLI AWS

> **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":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "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 BufferImage
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 BufferImage
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 plateform
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-WKSClientBranding -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.

Balisage des ressources WorkSpaces

Vous pouvez organiser et gérer les ressources pour vos instances WorkSpaces en affectant vos propres métadonnées à chaque ressource sous la forme de balises. Vous spécifiez une clé et une valeur pour chaque balise. Une clé peut être une catégorie générale, comme un « projet », un « propriétaire » ou un « environnement » avec des valeurs associées spécifiques. Les balises constituent une méthode simple et puissante de gestion des ressources AWS et d'organisation des 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 un espace de travail existant le 15 juillet, les balises 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 les balises de ressources WorkSpaces dans l'explorateur de coûts, vous devez activer les balises que vous avez appliquées aux ressources de vos instances WorkSpaces en suivant les instructions de la section Activation des balises de répartition des coûts définies par l'utilisateur dans le Guide de l'utilisateur AWS Billing.
> 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. De plus, pour apparaître et fournir des données de coûts dans l'explorateur de coûts, les ressources WorkSpaces qui ont été 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 lors de leur création : instances WorkSpaces, images importées et groupes de contrôle d'accès IP.
- Vous pouvez ajouter des balises aux ressources existantes des types suivants : instances WorkSpaces, annuaires enregistrés, offres groupées 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 préfixes `aws:` ni `aws:workspaces:` dans les noms ou les valeurs de balises, car celui-ci est réservé pour AWS. 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 (annuaires, instances WorkSpaces ou groupes de contrôle d'accès IP)

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez l'un des types de ressource suivants : Annuaires, WorkSpaces ou Contrôles d'accès IP.
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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
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 de l'AWS CLI

Utilisez les commandes create-tags et delete-tags.

Maintenance des instances WorkSpaces

Nous vous recommandons d'effectuer une maintenance régulière des instances WorkSpaces. WorkSpaces planifie des fenêtres de maintenance par défaut pour les instances WorkSpaces. Pendant la fenêtre de maintenance, l'instance WorkSpace installe des mises à jour Amazon WorkSpaces importantes, 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 système d'exploitation que WorkSpace est configuré pour utiliser. Pendant la maintenance, vos instances WorkSpaces risquent ne pas être disponibles.

Par défaut, vos espaces de travail Windows sont configurés pour recevoir des 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

Vos instances WorkSpaces doivent avoir accès à Internet pour vous permettre d'installer les mises à jour sur le système d'exploitation et déployer des applications. Pour plus d'informations, consultez the section called “Accès Internet”.

Fenêtres de maintenance pour instances WorkSpaces AlwaysOn

Pour les instances WorkSpace AlwaysOn, la fenêtre de maintenance est déterminée par les paramètres du système d'exploitation. La période par défaut est de 4 heures, de minuit à 04h00, dans le fuseau horaire de l'instance WorkSpace, chaque dimanche matin. Par défaut, le fuseau horaire d'une instance WorkSpace AlwaysOn est celui de la région AWS de l'instance WorkSpace. Toutefois, si vous vous connectez à partir d'une autre région et que la redirection de fuseau horaire est activée, puis que vous vous déconnectez, le fuseau horaire de l'instance WorkSpace est mis à jour avec le fuseau horaire de la région à partir de laquelle vous vous êtes connecté.

Vous pouvez désactiver la redirection de fuseau horaire pour les instances WorkSpaces Windows à l'aide d'une stratégie de groupe. Vous pouvez désactiver la redirection de fuseau horaire pour les instances WorkSpaces Linux via la configuration de l'agent PCoIP.

Pour les instances WorkSpace Windows, vous pouvez configurer la fenêtre de maintenance à l'aide d'une stratégie de groupe. Consultez Configure Group Policy Settings for Automatic Updates. Vous ne pouvez pas configurer la fenêtre de maintenance pour les instances WorkSpace Linux.

Fenêtres de maintenance pour les instances WorkSpaces AutoStop

Les instances WorkSpace AutoStop sont démarrées automatiquement une fois par mois pour installer les mises à jour importantes. À partir du troisième lundi du mois et pour une durée maximale de deux semaines, la fenêtre de maintenance est ouverte chaque jour entre 0 h et 5 h dans le fuseau horaire de la région AWS de l'instance WorkSpace. L'instance WorkSpace peut faire l'objet d'une maintenance chaque jour lors de la fenêtre de maintenance. Pendant cette période, seules les instances WorkSpaces datant de plus de 7 jours font l'objet d'une maintenance.

Durant la période pendant laquelle l'instance WorkSpaces est en maintenance, l'état de l'instance est défini sur `MAINTENANCE`.

Bien que vous ne puissiez pas modifier le fuseau horaire utilisé pour gérer les instances WorkSpace AutoStop, vous pouvez désactiver la fenêtre de maintenance de vos instances WorkSpace AutoStop comme suit. Si vous désactivez le mode maintenance, vos instances WorkSpace ne sont pas redémarrées et ne passent pas à l'état `MAINTENANCE`.

Pour désactiver le mode maintenance

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
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 gérer vos instances WorkSpace sur votre propre calendrier. Lorsque vous effectuez des tâches de maintenance, nous vous recommandons faire passer l'état de l'instance WorkSpace à Maintenance. Lorsque vous avez terminé, définissez l'état de l'instance WorkSpace à Disponible.

Lorsqu'une instance WorkSpace est à l'état Maintenance, les comportements suivants se produisent :

- L'instance WorkSpace ne répond pas aux demandes de redémarrage, d'arrêt, de démarrage ou de reconstruction.
- Les utilisateurs ne peuvent pas se connecter à l'instance WorkSpace.
- Une instance WorkSpace AutoStop n'est pas mise en veille.

Pour modifier l'état de l'instance WorkSpace à l'aide de la console

> **Note**
>
> Pour modifier l'état d'une instance WorkSpace, celle-ci doit être à l'état Disponible. Le paramètre Modifier l'état est indisponible lorsque l'état d'une instance WorkSpace n'est pas Disponible.

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.

3. Sélectionnez l'instance WorkSpace, puis choisissez Actions, Modifier un WorkSpace.
4. Sous Modifier l'état, choisissez Disponible ou Maintenance.
5. Choisissez Enregistrer.

Pour modifier l'état de l'instance WorkSpace à l'aide de l'AWS CLI

Utilisez la commande modify-workspace-state.

Instances WorkSpace chiffrées

WorkSpaces est intégré à AWS Key Management Service (AWS KMS). Cela vous permet de chiffrer les volumes de stockage des instances WorkSpaces à l'aide de clés AWS KMS. Lorsque vous lancez une instance 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). Vous garantissez ainsi que les données stockées au repos, les E/S de disque vers le volume et les instantanés créés à partir des volumes sont tous chiffrés.

> **Note**
>
> Outre le chiffrement de vos instances WorkSpaces, vous pouvez également utiliser le chiffrement des points de terminaison FIPS dans certaines régions AWS des États-Unis. Pour plus d'informations, consultez Configuration d'Amazon WorkSpaces pour l'autorisation FedRAMP ou la conformité SRG pour le Département de la Défense (DoD) des États-Unis.

Table des matières

- Prérequis
- Limites
- Présentation du chiffrement WorkSpaces avec AWS KMS
- Contexte de chiffrement WorkSpaces
- Octroi à WorkSpaces de l'autorisation d'utiliser une clé KMS en votre nom
- Chiffrement d'une instance WorkSpace
- Affichage des instances WorkSpaces chiffrées

Prérequis

Vous avez besoin d'une clé AWS KMS avant de commencer le processus de chiffrement. Cette clé KMS peut être soit une clé KMS gérée par AWS pour Amazon WorkSpaces (aws/workspaces), soit une clé KMS symétrique gérée par le client.

- Clés KMS gérées par AWS : la première fois que vous lancez une instance WorkSpace non chiffrée à partir de la console WorkSpaces dans une région, Amazon WorkSpaces crée automatiquement une clé KMS gérée par AWS (aws/workspaces) dans votre compte. Vous pouvez sélectionner la clé KMS gérée par AWS pour chiffrer les volumes racine et utilisateur de votre instance WorkSpace. Pour plus de détails, veuillez consulter Présentation du chiffrement WorkSpaces avec AWS KMS.

  Vous pouvez voir la clé KMS gérée par AWS, y compris ses stratégies et attributions, et suivre son utilisation dans les journaux AWS CloudTrail, mais vous ne pouvez pas l'utiliser ni la gérer. Amazon WorkSpaces crée et gère cette clé KMS. Seul Amazon WorkSpaces peut utiliser cette clé KMS, et uniquement pour chiffrer les ressources WorkSpaces dans votre compte.

  Les clés gérées par AWS, y compris celle prise en charge par Amazon WorkSpaces, font l'objet d'une rotation tous les trois ans. Pour plus d'informations, consultez Rotation des clés AWS KMS dans le Guide du développeur AWS Key Management Service.
- Clé KMS gérée par le client : vous pouvez aussi sélectionner une clé KMS symétrique gérée par le client, que vous créez à l'aide de AWS KMS. 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 d'une clé KMS à l'aide de l'API AWS KMS, consultez Utilisation de clés dans le Guide du développeur AWS Key Management Service.

  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 d'informations, consultez Rotation des clés AWS KMS dans le Guide du développeur AWS Key Management Service.

> **Important**
>
> Lorsque vous effectuez manuellement une rotation des clés KMS, vous devez conserver la clé d'origine et la nouvelle clé KMS activées afin que AWS KMS puisse déchiffrer les instances WorkSpaces chiffrées avec la clé KMS d'origine. Si vous ne souhaitez pas que la

clé KMS d'origine reste activée, vous devez recréer les instances WorkSpaces et les chiffrer à l'aide de la nouvelle clé KMS.

Vous devez respecter les exigences suivantes pour utiliser une clé AWS KMS afin de chiffrer vos instances 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 plus d'informations, consultez 2e partie : Octroyer aux administrateurs d'instances WorkSpaces des autorisations supplémentaires à l'aide d'une politique IAM.

Limites

- Vous ne pouvez pas chiffrer une instance WorkSpace existante. Vous devez chiffrer une instance WorkSpace lorsque vous la lancez.
- La création d'une image personnalisée à partir d'un espace de travail chiffré n'est pas prise en charge.
- La désactivation du chiffrement pour un espace de travail chiffré n'est pas actuellement prise en charge.
- Les espaces de travail lancés avec le chiffrement de volume racine activé peuvent prendre jusqu'à une heure pour être provisionnés.
- Pour redémarrer ou reconstruire une instance WorkSpace chiffrée, vérifiez d'abord que la clé AWS KMS est activée, sinon l'instance WorkSpace 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.

Présentation du chiffrement WorkSpaces avec AWS KMS

Lorsque vous créez des instances 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 la clé KMS pour travailler avec les volumes chiffrés. Pour plus d'informations sur le chiffrement ESB des volumes, consultez Chiffrement Amazon EBS dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Lorsque vous lancez WorkSpaces avec des volumes chiffrés, le processus de bout en bout fonctionne comme suit :

1. Vous spécifiez la clé KMS à utiliser pour le chiffrement, ainsi que l'utilisateur et l'annuaire de l'instance WorkSpace. Cette action crée un octroi qui autorise WorkSpaces à utiliser la clé KMS uniquement pour cette instance WorkSpace, c'est-à-dire uniquement pour l'instance WorkSpace associée à l'utilisateur et à l'annuaire spécifiés.
2. WorkSpaces crée un volume EBS chiffré pour l'instance WorkSpace, et spécifie la clé KMS à utiliser ainsi que l'utilisateur et l'annuaire du volume. Cette action crée un octroi qui autorise Amazon EBS à utiliser la clé KMS uniquement pour cette instance WorkSpace et ce volume, c'est-à-dire uniquement pour l'instance WorkSpace associée à l'utilisateur et à l'annuaire spécifiés, et uniquement pour le volume spécifié.
3. Amazon EBS demande une clé de données de volume qui est chiffrée sous la clé KMS, et spécifie l'identifiant de sécurité (SID) Active Directory de l'utilisateur de l'instance WorkSpace et l'ID d'annuaire AWS Directory Service, ainsi que l'ID de volume Amazon EBS comme contexte de chiffrement.
4. AWS KMS crée une nouvelle clé de données, la chiffre sous la clé KMS, puis envoie la clé de données chiffrée à Amazon EBS.
5. WorkSpaces utilise Amazon EBS pour attacher le volume chiffré à votre instance WorkSpace. Amazon EBS envoie la clé de données chiffrée à AWS KMS avec une demande `Decrypt`, et spécifie le SID de l'utilisateur de l'instance WorkSpace, l'ID d'annuaire, ainsi que l'ID de volume, qui sont utilisés comme contexte de chiffrement.
6. AWS KMS utilise la 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 associé à l'instance WorkSpace.

8. Amazon EBS stocke la clé de données chiffrée (reçue à l'Step 4) avec les métadonnées du volume pour pouvoir les utiliser ultérieurement si vous redémarrez ou reconstruisez l'instance WorkSpace.
9. Lorsque vous utilisez AWS Management Console pour supprimer une instance WorkSpace (ou l'action `TerminateWorkspaces` dans l'API WorkSpaces), WorkSpaces et Amazon EBS abandonnent les octrois qui leur ont permis d'utiliser la clé KMS pour cette instance WorkSpace.

Contexte de chiffrement WorkSpaces

WorkSpaces n'utilise pas directement la clé KMS pour les opérations cryptographiques (comme `Encrypt`, `Decrypt`, `GenerateDataKey`, etc.), ce qui signifie que WorkSpaces n'envoie pas de demandes à AWS KMS incluant un contexte de chiffrement. Toutefois, quand Amazon EBS demande une clé de données chiffrée pour les volumes chiffrés de vos instances WorkSpaces (Step 3 de la section Présentation du chiffrement WorkSpaces avec AWS KMS) et 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) qu'AWS KMS utilise pour garantir l'intégrité des données. Le contexte de chiffrement est également écrit dans les fichiers journaux AWS CloudTrail, 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 :

- Identifiant de sécurité (SID) de l'utilisateur Active Directory associé à l'instance WorkSpace
- L'ID de l'annuaire AWS Directory Service associé à l'instance 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]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

Octroi à WorkSpaces de l'autorisation d'utiliser une clé KMS en votre nom

Vous pouvez protéger les données de votre instance WorkSpace sous la clé KMS gérée par AWS pour WorkSpaces (aws/workspaces) ou sous une clé KMS gérée par le client. Si vous utilisez une clé KMS gérée par le client, vous devez octroyer à WorkSpaces l'autorisation d'utiliser la clé KMS au nom des administrateurs WorkSpaces de votre compte. Par défaut, la clé KMS gérée par AWS pour WorkSpaces dispose des autorisations requises.

Pour préparer la clé KMS gérée par le client pour une utilisation avec WorkSpaces, utilisez la procédure suivante.

1. Ajouter des administrateurs d'instances WorkSpaces à la liste des utilisateurs de clé figurant dans la stratégie de clé de la clé KMS
2. Octroyer à des administrateurs d'instances WorkSpaces des autorisations supplémentaires à l'aide d'une politique IAM

Les administrateurs d'instances WorkSpaces ont également besoin de l'autorisation d'utiliser WorkSpaces. Pour plus d'informations sur ces autorisations, consultez Gestion des identités et des accès pour WorkSpaces.

1re partie : Ajouter des administrateurs WorkSpaces en tant qu'utilisateurs de clé

Pour fournir aux administrateurs WorkSpaces les autorisations dont ils ont besoin, vous pouvez utiliser AWS Management Console ou l'API AWS KMS.

Pour ajouter les administrateurs WorkSpaces en tant qu'utilisateurs de clé pour une clé KMS (console)

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Key Management Service (AWS KMS) à l'adresse https://console.aws.amazon.com/kms.
2. Pour changer le paramètre Région AWS, utilisez le sélecteur de région dans l'angle supérieur droit de la page.
3. Dans le volet 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 qui correspondent aux administrateurs de vos instances WorkSpace, puis choisissez Attacher.

Pour ajouter des administrateurs WorkSpace comme utilisateurs de clé pour une clé KMS (API)

1. Utilisez l'opération GetKeyPolicy pour récupérer la stratégie de 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 qui correspondent aux administrateurs de vos instances WorkSpaces dans les instructions de stratégie qui accordent une autorisation à des utilisateurs de clé. Ensuite, enregistrez le fichier.
3. Utilisez l'opération PutKeyPolicy pour appliquer la stratégie de clé à la clé KMS.

2e partie : Octroyer aux administrateurs d'instances WorkSpaces des autorisations supplémentaires à l'aide d'une politique IAM

Si pour le chiffrement, vous sélectionnez une clé KMS gérée par le client, vous devez établir des politiques IAM permettant à Amazon WorkSpaces d'utiliser la clé KMS au nom d'un utilisateur IAM de votre compte qui lance des instances WorkSpaces chiffrées. Cet utilisateur a également besoin d'une autorisation pour 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.

Le chiffrement WorkSpaces 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 stratégie de clé AWS KMS 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 mandataires AWS qui peuvent gérer et utiliser la clé, respectivement. La quatrième instruction permet aux services AWS intégrés à AWS KMS d'utiliser la clé au nom du mandataire spécifié. Cette instruction permet aux services AWS de créer et gérer les octrois. L'instruction utilise un élément de condition qui limite les octrois sur la clé KMS à ceux accordés par les services AWS au nom des utilisateurs de votre compte.

> **Note**
>
> En outre, si les administrateurs WorkSpaces utilisent AWS Management Console pour créer des instances WorkSpaces avec des volumes chiffrés, ils ont besoin d'autorisations

pour répertorier les alias et les clés (les autorisations `"kms:ListAliases"` et `"kms:ListKeys"`). Si les administrateurs WorkSpaces utilisent uniquement l'API Amazon WorkSpaces (pas la console), vous pouvez ignorer les autorisations `"kms:ListAliases"` et `"kms:ListKeys"`.

```
{
  "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:ReEncrypt",
        "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 une instance WorkSpace doit inclure des autorisations d'utilisation sur la clé KMS gérée par le client, ainsi que l'accès à WorkSpaces. Pour accorder à un utilisateur IAM ou à un rôle des autorisations WorkSpaces, vous pouvez associer l'exemple de politique suivant à l'utilisateur ou au rôle.

```
{
    "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.

```
{
    "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.

```
{
  "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": "*"
    }
  ]
}
```

Chiffrement d'une instance WorkSpace

Pour chiffrer une instance WorkSpace

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Choisissez Lancer des instances WorkSpaces et exécutez les trois premières étapes.
3. Pour l'étape Configuration des instances WorkSpaces, procédez comme suit :
   a. Sélectionnez les volumes à chiffrer : Volume racine, Volume utilisateur ou les deux volumes.
   b. Pour Clé de chiffrement, sélectionnez une clé AWS KMS, soit la clé KMS gérée par AWS 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 des instances WorkSpaces.

Affichage des instances WorkSpaces chiffrées

Pour voir quels espaces de travail et volumes ont été chiffrés à partir de la console WorkSpaces, sélectionnez WorkSpaces dans la barre de navigation de gauche. La colonne Chiffrement de volume montre si le chiffrement est activé ou désactivé pour chaque espace de travail. Pour voir quels volumes spécifiques ont été chiffrés, développez l'entrée WorkSpace pour afficher le champ Volumes chiffrés.

Redémarrer un WorkSpace

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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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 le amazon-workspaces-admin-module.

Reconstruction d'une instance WorkSpace

La reconstruction d'une instance WorkSpace permet de recréer le volume racine, le volume utilisateur et l'interface réseau Elastic principale de l'image la plus récente de l'offre groupée à partir de laquelle l'instance WorkSpace a été lancée. La reconstruction d'une instance WorkSpace supprime davantage de données que sa restauration, mais seul un instantané du volume utilisateur est nécessaire. Pour restaurer une instance WorkSpace, consultez Restauration d'une instance WorkSpace.

La reconstruction d'une instance WorkSpace entraîne les événements suivants :

- Le volume racine (pour Microsoft Windows, le lecteur C ; pour Linux, /) est actualisé avec l'image la plus récente de l'offre groupée à partir de laquelle l'instance WorkSpace a été créée. Les applications qui ont été installées ou les paramètres système qui ont été modifiés après la création de l'instance WorkSpace 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 recréation d'une instance WorkSpace sont planifiés toutes les 12 heures. Ces instantanés du volume utilisateur sont pris quelle que soit l'état de l'instance WorkSpace. Lorsque vous sélectionnez Actions, Régénérer/restaurer WorkSpace, la date et l'heure du dernier instantané sont visibles.

- L'interface réseau Elastic principale est recréée. L'instance WorkSpace reçoit une nouvelle adresse IP privée.

> **Important**
>
> Après le 14 janvier 2020, les instances WorkSpaces créées à partir d'un pack Windows 7 public ne peuvent plus être reconstruites. Vous pouvez envisager de migrer vos instances WorkSpaces Windows 7 vers Windows 10. Pour plus d'informations, consultez Migrer un WorkSpace.

Vous ne pouvez reconstruire une instance WorkSpace que si les conditions suivantes sont réunies :

- L'état de l'instance WorkSpace doit être `AVAILABLE`, `ERROR`, `UNHEALTHY`, `STOPPED` ou `REBOOTING`. Pour reconstruire une instance WorkSpace à l'état `REBOOTING`, vous devez utiliser l'opération d'API RebuildWorkspaces ou la commande AWS CLI rebuild-workspaces.
- Un instantané du volume utilisateur doit exister.

Pour reconstruire une instance WorkSpace

> **Warning**
>
> Pour reconstruire une instance WorkSpace chiffrée, vérifiez d'abord que la clé AWS KMS est activée, sinon l'espace de travail 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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.

3. Sélectionnez l'instance WorkSpace à reconstruire et choisissez Actions, Régénérer/restaurer WorkSpace.
4. Sous Instantané, sélectionnez l'horodatage de l'instantané.
5. Choisissez Reconstruire.

Pour reconstruire une instance WorkSpace via AWS CLI

Utilisez la commande rebuild-workspaces.

Résolution des problèmes

Si vous reconstruisez un espace de travail après avoir modifié l'attribut d'attribution de noms d'utilisateur sAMAccountName 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 d'attribution de noms d'utilisateur d'origine, puis relancez la reconstruction, ou créez une nouvelle instance WorkSpace pour cet utilisateur.

Restauration d'une instance WorkSpace

La restauration d'une instance WorkSpace recrée les volumes racine et utilisateur en se basant sur les instantanés les plus récents de ces volumes, créés quand l'instance WorkSpace était saine. La restauration d'une instance WorkSpace supprime moins de données que sa reconstruction. Toutefois, vous devez disposer d'instantanés des volumes racine et utilisateur, tandis que la reconstruction d'une instance WorkSpace ne nécessite qu'un instantané du volume utilisateur. Pour reconstruire une instance WorkSpace, consultez Reconstruction d'une instance WorkSpace.

La restauration d'une instance WorkSpace entraîne les événements suivants :

- Le volume racine (pour Microsoft Windows, lecteur C ; pour Linux,/) est restauré d'après l'instantané le plus récent. Les applications qui ont été installées ou les paramètres système qui ont été modifiés après la création de l'instantané le plus récent 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.

Lorsque des instantanés sont pris

Les instantanés des volumes racine et utilisateur sont pris sur la base suivante. Lorsque vous sélectionnez Actions, Régénérer/restaurer WorkSpace, la date et l'heure des instantanés les plus récents sont visibles.

- Après la création d'une instance WorkSpace : en général, les premiers instantanés des volumes racine et utilisateur sont pris peu après la création d'une instance WorkSpace (souvent dans les 30 minutes qui suivent). Dans certaines régions AWS, la prise des premiers instantanés peut prendre plusieurs heures après la création d'une instance WorkSpace.

  Si une instance WorkSpace devient défectueuse avant que les premiers instantanés ne soient pris, il n'est pas possible de la restaurer. Dans ce cas, vous pouvez essayer de reconstruire l'instance WorkSpace ou de contacter AWS Support pour obtenir de l'aide.
- Au cours d'une utilisation habituelle : les instantanés automatiques à utiliser lors de la restauration d'une instance WorkSpace sont planifiés toutes les 12 heures. Si l'instance WorkSpace est saine, les instantanés du volume racine et du volume utilisateur sont créés à peu près en même temps. Si l'instance WorkSpace est défectueuse, les instantanés ne sont créés que pour le volume utilisateur.
- Après la restauration d'une instance WorkSpace : lorsque vous restaurez une instance WorkSpace, de nouveaux instantanés sont pris peu après la fin de la restauration (souvent dans les 30 minutes qui suivent). Dans certaines régions AWS, la prise de ces instantanés peut prendre plusieurs heures après la restauration d'une instance WorkSpace.

  Après restauration d'une instance WorkSpace, si elle devient défectueuse avant que de nouveaux instantanés puissent être pris, elle ne peut pas être restaurée une nouvelle fois. Dans ce cas, vous pouvez essayer de reconstruire l'instance WorkSpace ou de contacter AWS Support pour obtenir de l'aide.

Vous ne pouvez restaurer une instance WorkSpace que si les conditions suivantes sont réunies :

- L'état de l'instance WorkSpace doit être `AVAILABLE`, `ERROR`, `UNHEALTHY` ou `STOPPED`.
- Des instantanés des volumes racine et utilisateur doivent exister.

Pour restaurer une instance WorkSpace

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.

2. Dans le volet de navigation, choisissez WorkSpaces.
3. Sélectionnez l'instance WorkSpace à restaurer, puis choisissez Actions, Régénérer/restaurer WorkSpace.
4. Sous Instantané, sélectionnez l'horodatage de l'instantané.
5. Choisissez Restore (Restaurer).

Pour restaurer une instance WorkSpace via AWS CLI

Utilisez la commande restore-workspace.

Microsoft 365 Apportez votre propre licence (BYOL)

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

Pour utiliser Microsoft 365 Apps for Enterprise sur WorkSpaces, vous devez être abonné à Microsoft 365 E3/E5, Microsoft 365 A3/A5 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 à l'adresse https://console.aws.amazon.com/workspaces/.
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/, saisissez 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 OfficeAWS, vous pouvez installer et configurer Microsoft 365 Apps for Enterprise sur votre WorkSpaces.

Si vous WorkSpaces possédez une licence Microsoft OfficeAWS, 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 Microsoft Office 2016 et 2019 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

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 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

- Prérequis
- 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

Prérequis

- 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 plus d'informations, consultez 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 plutôt d'effectuer des personnalisations au profil utilisateur via des objets de stratégie de groupe (GPO). Les personnalisations effectuées via des objets de stratégie de groupe 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.ps1etupdate-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 : HKL M:\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
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

Clé de registre	Type	Valeurs
		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 : HKL M:\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, voirMettez 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 plus d'informations, consultez 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.

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 leEffectuer 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

> **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 PCoIP vers le protocole de WorkSpaces streaming (WSP).
- 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.G4DN). GraphicsPro.g4dn, Graphics, and GraphicsPro) regroupe des bundles non compatibles avec le GPU, ainsi que dans le sens inverse.
- 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.

Pour plus d'informations sur WorkSpaces les offres Amazon, consultezWorkSpace bundles et images.

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 de PCoIP vers WSP, vous devez d'abord créer un bundle BYOL avec le protocole WSP. Vous pouvez ensuite migrer votre BYOL PCoIP WorkSpaces vers ce bundle WSP BYOL.
- Vous ne pouvez pas migrer un bundle WorkSpace créé à partir de bundles publics ou personnalisés vers un bundle BYOL.
- Graphics.g4dn, GraphicsPro .g4dn, Graphics et GraphicsPro les bundles ne sont actuellement disponibles que pour le protocole PCoIP. Graphics.G4dn, .g4dn, Graphics et Graphics ne peuvent donc pas encore être migrés vers WSP. GraphicsPro GraphicsPro WorkSpaces
- 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.

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
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

Système d'exploitation source	Système d'exploitation cible	Disponible ?
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

Note

L'accès Web n'est pas disponible pour la branche PCoIP du bundle Windows 10 public sur Windows Server 2019.

Important

Le bundle Windows 10 Plus public sur Windows Server 2016 inclut Microsoft Office 2016 et les services de sécurité professionnels Trend Micro Worry-Free. Le bundle Windows 10 Plus public sur Windows Server 2019 inclut uniquement Microsoft Office 2019, pas les services de sécurité professionnels Trend Micro Worry-Free.

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 éliminé. 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 nomméD:\Users\%USERNAME %MMddyyTHHmmss%.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%MMddyyTHHmmss%.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%MMddyyTHHmmss%.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 `AVAILABLE` `STOPPED`, ou `ERROR`.
- 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%MMddyyTHHmmss%.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. Il se peut que vous deviez 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 faire migrer un WorkSpace

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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 de PCoIP vers WSP, vous devez d'abord créer un bundle BYOL avec le protocole WSP. Vous pouvez ensuite migrer votre BYOL PCoIP WorkSpaces vers ce bundle WSP BYOL.

5. Choisissez 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 WorkSpaces ensemble ou une image personnalisé.

Pour effectuer la migration WorkSpaces via leAWS CLI, utilisez la commande migrate-workspace. Pour effectuer la migration WorkSpaces via l' WorkSpaces API Amazon, consultez MigrateWorkSpacele manuel Amazon WorkSpaces API Reference.

Suppression d'une instance WorkSpace

Lorsque vous avez terminé avec une instance WorkSpace, vous pouvez la supprimer. Vous pouvez également supprimer des ressources associées.

> **Warning**
>
> La suppression d'un espace de travail est une action permanente et ne peut pas être annulée. Les données utilisateur de l'instance WorkSpace 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 mis gratuitement à disposition pour une utilisation avec WorkSpaces. Si aucune instance WorkSpace n'est utilisée avec l'annuaire Simple AD ou AD connector pendant 30 jours consécutifs, l'enregistrement de celui-ci pour une utilisation

avec Amazon WorkSpaces est automatiquement annulé, et il vous est facturé conformément aux conditions de tarification AWS Directory Service.
Pour supprimer des annuaires vides, consultez Suppression de l'annuaire des instances WorkSpaces. Si vous supprimez votre annuaire Simple AD ou AD Connector, vous pouvez toujours en créer un nouveau lorsque vous souhaitez recommencer à utiliser WorkSpaces.

Pour supprimer une instance WorkSpace

Vous pouvez supprimer une instance WorkSpace dans n'importe quel état, sauf l'état Suspendu.

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez WorkSpaces.
3. Sélectionnez votre instance WorkSpace, puis choisissez Supprimer.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer l'instance WorkSpace.
   La suppression d'une instance WorkSpace prend environ 5 minutes. Pendant la suppression, le statut de l'instance WorkSpace passe à Résiliation. Une fois la suppression terminée, l'instance 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 WorkSpaces ensemble ou une image personnalisé.
6. (Facultatif) Après avoir supprimé toutes les instances WorkSpaces d'un annuaire, vous pouvez supprimer l'annuaire. Pour plus d'informations, consultez Suppression de l'annuaire des instances WorkSpaces.
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 une instance WorkSpace à l'aide de la AWS CLI

Utilisez la commande terminate-workspaces.

WorkSpace bundles et images

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	WSP, PCoIP	Valeur, norme, performance, puissance, graphismes (obsolète	12 janvier 2027

Système d'exploitation	Licences	Protocoles de streaming	Offres groupées prises en charge	Politique de cycle de vie/ date de retraite
			) PowerPro, Graphics.g4dn GraphicsPro, .g4dn GraphicsPro	
Windows Server 2019	Inclus	WSP, PCoIP	Valeur, norme, performance, puissance, graphismes (obsolète) PowerPro, Graphics.g4dn GraphicsPro, .g4dn GraphicsPro	9 janvier 2029
Windows Server 2022	Inclus	WSP, PCoIP	Standard, Performance, Power, Graphics (obsolète) PowerPro, Graphics.G4DN GraphicsPro, .g4dn GraphicsPro	14 octobre 2031
Windows 10	Bring Your Own License (Licence à fournir)	WSP, PCoIP	Valeur, norme, performance, puissance, graphismes (obsolète) PowerPro, Graphics.g4dn GraphicsPro, .g4dn GraphicsPro	À l'appui
Windows 11	Bring Your Own License (Licence à fournir)	WSP	Standard, performance, puissance, PowerPro	À l'appui
Amazon Linux 2	Inclus	WSP, PCoIP	Valeur, norme, performance, puissance, PowerPro	30 juin 2025

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	WSP	Valeur, norme, performance, puissance, carte PowerPro graphique.G4DN, .g4dn GraphicsPro	juin 2032

> **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 PCoIP.

Table des matières

- Options d'offres groupées
- Création d'une WorkSpaces image personnalisée et d'un bundle
- Mise à jour d'un bundle d'instances WorkSpaces personnalisé
- Copie d'une image WorkSpaces personnalisée
- Partage ou annulation de partage d'une image WorkSpaces personnalisée
- Supprimer un WorkSpaces ensemble ou une image personnalisé
- Apportez votre propre licence (BYOL) de bureau Windows

Options d'offres groupées

Avant de sélectionner une offre groupée (ou bundle), assurez-vous que celle-ci est compatible avec le protocole, le système d'exploitation, le réseau et le type de calcul des instances WorkSpaces. Pour

plus d'informations sur les protocoles, consultez Protocoles pour Amazon WorkSpaces. Pour plus d'informations sur les réseaux, consultez Exigences relatives au réseau client Amazon WorkSpaces.

> **Note**
>
> - Nous recommandons de ne pas dépasser une latence réseau maximale de 250 ms pour les instances WorkSpaces PCoIP. Pour bénéficier d'une expérience utilisateur optimale sur les instances WorkSpaces PCoIP, nous recommandons de garder la latence réseau inférieure à 100 ms. Lorsque le temps de propagation aller et retour (RTT) dépasse 375 ms, la connexion du client WorkSpaces est interrompue. Pour une expérience utilisateur optimale avec le protocole WSP (WorkSpaces Streaming Protocol), nous recommandons de garder le RTT inférieur à 250 ms. Quand le RTT est compris entre 250 ms et 400 ms, l'utilisateur peut accéder à l'instance WorkSpace, mais les performances diminuent 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.

> **Important**
>
> - Le bundle Graphics ne sera plus pris en charge après le 30 novembre 2023. Nous vous recommandons de passer au bundle Graphics.g4dn pour WorkSpaces à l'aide du bundle Graphics.
> - Les bundles Graphics et GraphicsPro ne sont actuellement pas disponibles dans la région Asie-Pacifique (Mumbai).

Vous trouverez ci-dessous la liste de offres groupées proposées par WorkSpaces. Pour plus d'informations sur les offres groupées dans WorkSpaces, consultez Offres Amazon WorkSpaces.

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.

Offre PowerPro

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 GraphicsPro

Cet bundle offre un niveau de performances graphiques de référence, ainsi qu'un niveau élevé de mémoire et de performances du CPU pour les instances WorkSpaces. Il convient parfaitement aux activités suivantes :

- Navigation sur le Web
- Traitement de texte
- E-mails
- Messagerie instantanée
- Feuilles de calcul
- Conférence audio
- Développement logiciel (environnement de développement intégré (IDE))
- Entreposage de données
- Applications d'informatique décisionnelle
- Conception graphique
- Traitement graphique

Ce bundle n'est pas recommandé pour les conférences audio et vidéo, le rendu 3D et la conception photoréaliste

Offre Graphics.g4dn

Cet bundle offre un haut niveau de performances graphiques, ainsi qu'un niveau modéré de mémoire et de performances du CPU pour les instances WorkSpaces. Il convient parfaitement aux activités 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
- CAO/FAO (conception assistée par ordinateur/fabrication assistée par ordinateur)

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.

GraphicsPro.g4dn

Offre GraphicsPro.g4dn

Ce bundle offre un haut niveau de mémoire, de performances graphiques et de performances du CPU pour les instances WorkSpaces, et convient parfaitement aux activités 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
- CAO/FAO (conception assistée par ordinateur/fabrication assistée par ordinateur)
- 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 WorkSpaces image personnalisée et d'un bundle

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 (mise à niveau des fonctionnalités/versions 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 plus d'informations, consultez Migrer un WorkSpace.
- Le bundle Graphics ne sera plus pris en charge après le 30 novembre 2023. Nous vous recommandons de migrer votre offre groupée WorkSpaces vers Graphics.G4DN. Pour plus d'informations, consultez Migrer un WorkSpace.
- Les graphismes et GraphicsPro les offres groupées ne sont actuellement pas disponibles dans la région Asie-Pacifique (Mumbai).
- Les volumes de stockage groupés personnalisés ne peuvent pas être inférieurs aux volumes de stockage d'images.

Les lots personnalisés coûtent autant que les lots publics à partir desquels ils sont créés. 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 plus d'informations, consultez the section called “Configuration requise”.
  - Windows PowerShell version 3.0 ou ultérieure
  - Services Bureau à distance
  - AWS Pilotes photovoltaïques
  - Gestion à distance Windows (WinRM)
  - Agents et pilotes PCoIP Teradici
  - 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
  - Pilotes et agents WSP ou PCoIP Teradici
  - 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 WorkSpaces Limites.
- 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 plus d'informations, consultez Exigences relatives à l'adresse IP et au port pour WorkSpaces.
- Pour Windows WorkSpaces, ne configurez aucun objet de stratégie de groupe (GPO) 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 de personnaliser le profil utilisateur via des objets de stratégie de groupe (GPO) et d'appliquer les personnalisations après la création de l'image. Les objets de stratégie de groupe peuvent être facilement modifiés ou annulés et sont donc moins sujets aux erreurs que les personnalisations effectuées sur le 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 le protocole de WorkSpaces streaming (WSP) activé, vérifiez Utilisation de cartes à puce pour l'authentification 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, NVMe et PV de votre WorkSpaces. 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 EC2Config, EC2Launch et EC2Launch V2 vers les dernières versions. Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez Mettre à jour EC2Config et EC2Launch.

(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

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 ComputerNamela 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>`, les noms des ordinateurs WorkSpaces créés à partir de votre bundle personnalisé commenceront par EC2AMAZ- xxxxxxx.*

   > **Note**
   >
   > Les valeurs `<RegisteredOrganization>` et `<RegisteredOwner>` de la section `<settings pass="oobeSystem">` sont ignorées par Sysprep.

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\OOBE_unattend.xml`.

2. Dans la section `<settings pass="specialize">`, supprimez la mise en commentaire de `<ComputerName>*</ComputerName>`, et 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 ComputerNamela 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>, les noms des ordinateurs WorkSpaces créés à partir de votre bundle personnalisé commenceront par EC2AMAZ- xxxxxxx.*

   > **Note**
   >
   > Les valeurs `<RegisteredOrganization>` et `<RegisteredOwner>` de la section `<settings pass="oobeSystem">` sont ignorées par Sysprep.

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 `OOBE_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 àÉtape 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 RemoteSignedles 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 RemoteSignedparamètre 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'image n'est pas prise en charge sur les systèmes Windows 10 mis à niveau depuis une version de Windows 10 vers une version plus récente de Windows 10 (mise à niveau d'une fonction/version 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

Si vous rencontrez des problèmes avec votre fichier Sysprep, contactez le Centre AWS Support pour faire réparer EC2Config ou EC2Launch.

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. Sous l'onglet Mise en réseau sélectionnez Protocole Internet 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 TLS version 1.2 doivent être activés

Pour configurer SSL/TLS pour Windows, veuillez consulter Comment activer TLS 1.2 dans la documentation Microsoft Windows.

Un seul profil d'utilisateur peut exister 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. Entrez la commande suivante pour supprimer tous les 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'image n'est pas prise en charge sur les systèmes Windows mis à niveau depuis une version de Windows 10 vers une version plus récente de Windows 10 (mise à niveau d'une fonction/version Windows).

Pour créer des images, utilisez une image WorkSpace qui n'a pas fait l'objet d'une mise à niveau des fonctionnalités/versions de 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 (GPO) restreignent l'accès à l'empreinte numérique du certificat RDP lorsqu'elle est demandée par le service EC2Config ou les scripts EC2Launch 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 où aucun GPO n'est 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 à l'adresse https://console.aws.amazon.com/workspaces/.
3. Dans le volet de navigation, choisissez 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 CreateWorkspaceImagele 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 indiquéesRedémarrer un WorkSpace. 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.
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 CreateWorkspaceBundlele 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
     - Pour Graphics.G4DN, GraphicsPro .g4dn, Graphics, et GraphicsPro WorkSpaces uniquement : 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 Graphics.g4dn, GraphicsPro .g4dn, Graphics ou GraphicsPro WorkSpace avec un minimum de 100 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\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\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-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/ .yaml zz-workspaces-domain
- /etc/netplan/ .yaml yy-workspaces-base
- /var/lib/ /utilisateurs AccountsService

Les clés suivantes sont détruites lors de la création de l'image personnalisée :

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

Mise à jour d'un bundle d'instances WorkSpaces personnalisé

Vous pouvez mettre à jour un bundle d'instances WorkSpaces personnalisé existant en modifiant une instance WorkSpace basée sur le bundle, en créant une image à partir de l'instance WorkSpace et en mettant à jour le bundle avec la nouvelle image. Vous pouvez ensuite lancer de nouvelles instances WorkSpaces avec le bundle mis à jour.

> **Important**
>
> Les WorkSpaces existants ne sont pas automatiquement mis à jour lorsque vous mettez à jour le bundle sur lequel ils sont basés. Pour mettre à jour des WorkSpaces existants basés sur un ensemble que vous avez mis à jour, vous devez reconstruire les WorkSpaces ou les supprimer et les recréer.

Pour mettre à jour un bundle à l'aide de la console

1. Connectez-vous à une instance WorkSpace basée 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 créer une nouvelle instance WorkSpace avec le même package de logiciels de base (Plus ou Standard) que l'image utilisée pour créer le bundle et effectuer les modifications.
2. Si vous êtes toujours connecté à l'instance WorkSpace, déconnectez-vous en choisissant Amazon WorkSpaces, puis Se déconnecter dans l'application client WorkSpaces.
3. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
4. Dans le volet de navigation, choisissez WorkSpaces.
5. Sélectionnez l'instance WorkSpace et choisissez Actions, Créer l'image. Si le statut de l'instance WorkSpace est `STOPPED`, vous devez d'abord la démarrer (choisissez Actions, Démarrer des 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). L'instance WorkSpace n'est pas disponible lorsque l'image est en cours de création. Pour plus d'informations sur le processus de création d'images, consultez Création d'une WorkSpaces image personnalisée et d'un bundle.
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 les WorkSpaces existants basés sur l'ensemble en reconstruisant les WorkSpaces ou en les supprimant et en les recréant. Pour plus d'informations, consultez Reconstruction d'une instance WorkSpace.

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 dans Référence des API Amazon WorkSpaces.

Copie d'une image WorkSpaces personnalisée

Vous pouvez copier une image WorkSpaces personnalisée au sein d'une région AWS ou entre différentes régions. 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) Regions, pour copier des images depuis et vers d'autres régions AWS, contactez AWS Support.
> Dans les régions d'acceptation, pour copier des images vers d'autres régions, contactez AWS Support. Pour plus d'informations sur les régions d'acceptation, consultez Régions disponibles.

Vous pouvez également copier une image partagée avec vous par un autre compte AWS. Pour plus d'informations sur les images partagées, consultez Partage ou annulation de partage d'une image WorkSpaces personnalisée.

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 les quotas Amazon WorkSpaces, 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.

```
{
```

```
  "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.

```
{
  "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 d'API CopyWorkspaceImage ou la commande copy-workspace-image dans AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez CopyWorkspaceImage dans Référence des API Amazon WorkSpaces ou copy-workspace-image dans Référence des commandes AWS CLI.

> **Important**
>
> Avant de copier une image partagée, assurez-vous qu'elle a été partagée depuis le compte AWS approprié. Afin de déterminer si une image a été partagée et pour connaître l'ID du compte AWS propriétaire d'une image, utilisez les opérations d'API DescribeWorkSpaceImages et DescribeWorkspaceImagePermissions, ou les commandes describe-workspace-images et describe-workspace-image-permissions dans AWS CLI.

Pour copier une image à l'aide de la console

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
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 vers 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 plus d'informations, consultez Balisage des ressources WorkSpaces.
7. Choisissez Copier l'image.

Partage ou annulation de partage d'une image WorkSpaces personnalisée

Vous pouvez partager des images WorkSpaces personnalisées entre des comptes AWS au sein de la même région AWS. Une fois qu'une image a été partagée, le compte destinataire peut copier l'image vers d'autres régions AWS si nécessaire. Pour plus d'informations sur la copie des images, consultez Copie d'une image WorkSpaces personnalisée.

> **Note**
>
> Pour la région Chine (Ningxia), vous ne pouvez copier des images que dans la même région. Dans les AWS GovCloud (US) Regions, pour copier des images depuis et vers d'autres régions AWS, contactez AWS Support.

Le partage d'images n'entraîne pas de frais supplémentaires. Cependant, le quota du nombre d'images de la région AWS 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 les quotas Amazon WorkSpaces, 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 pouvez partager des images Apportez votre propre licence (BYOL) uniquement avec des comptes AWS activés pour BYOL. Le compte AWS avec lequel vous souhaitez partager des images BYOL doit également faire partie de votre organisation (sous le même compte payeur).

> **Note**
>
> Le partage des images BYOL entre comptes AWS n'est actuellement pas pris en charge dans les régions AWS GovCloud (US, côte ouest) et AWS GovCloud (US, côte est). Pour partager des images BYOL entre comptes dans les régions AWS GovCloud (US, côte ouest) et AWS GovCloud (US, côte est), contactez AWS Support.

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 offres groupées afin de lancer de nouvelles instances WorkSpaces.

> **Important**
>
> Avant de copier une image partagée, assurez-vous qu'elle a été partagée depuis le compte AWS approprié. Afin de déterminer par programmation si une image a été partagée, utilisez les opérations d'API DescribeWorkSpaceImages et DescribeWorkspaceImagePermissions, ou les commandes describe-workspace-images et describe-workspace-image-permissions dans l'interface de ligne de commande (CLI) AWS.

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 console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
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 destinataire peut ensuite utiliser sa copie pour créer des offres groupées afin de lancer de nouvelles instances WorkSpaces.

Pour annuler le partage d'une image

1. Ouvrez la console WorkSpaces à l'adresse https://console.aws.amazon.com/workspaces/.
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, sélectionnez le compte AWS avec lequel vous souhaitez annuler 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. Toutefois, toutes les copies d'images partagées qui se trouvent déjà dans le compte destinataire restent dans ce compte, et de nouveaux espaces de travail peuvent être lancés à partir de ces copies.

Pour partager des images ou annuler leur partage par programmation

Pour partager des images ou annuler leur partage par programmation, utilisez l'opération d'API UpdateWorkspaceImagePermission ou la commande AWS Command Line Interface (AWS CLI) update-workspace-image-permission. Pour déterminer si une image a été partagée, utilisez l'opération d'API DescribeWorkspaceImagePermissions ou la commande CLI describe-workspace-image-permissions.

Supprimer un WorkSpaces ensemble ou une image personnalisé

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 à l'adresse https://console.aws.amazon.com/workspaces/.
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 DeleteWorkspaceBundlele 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 à l'adresse https://console.aws.amazon.com/workspaces/.
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 DeleteWorkspaceImagele Amazon WorkSpaces API Reference.

Apportez votre propre licence (BYOL) de bureau Windows

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 la section WorkSpaces Tarification.

> **Important**
>
> La création d'images n'est pas prise en charge sur les systèmes Windows 10 ou 11 qui ont été mis à niveau d'une version de Windows 10 ou 11 vers une version plus récente de Windows 10 ou 11 (mise à niveau de fonctionnalité/version Windows). Toutefois, les mises à jour cumulatives ou de sécurité de Windows sont prises en charge par le processus de WorkSpaces création d'images.

Table des matières

- Prérequis

- Versions Windows prises en charge pour BYOL
- Ajout de Microsoft Office à votre image BYOL
- Étape 1 : Vérifiez l'éligibilité de votre compte au BYOL à l'aide de la console Amazon WorkSpaces
- Étape 2 : Activez BYOL pour votre compte BYOL à l'aide de la console Amazon WorkSpaces
- Étape 3 : Exécuter le PowerShell script BYOL Checker sur une machine virtuelle Windows
- Étape 4 : Exporter la machine virtuelle depuis l'environnement de virtualisation
- Étape 5 : Importer la machine virtuelle comme image dans Amazon EC2
- Étape 6 : Création d'une image BYOL à l'aide de la console WorkSpaces
- Étape 7 : Créer un bundle personnalisé à partir de l'image BYOL
- Étape 8 : Enregistrez un répertoire dédié pour WorkSpaces
- Étape 9 : Lancez votre BYOL WorkSpaces

Prérequis

Avant de commencer, vérifiez les éléments suivants :

- Votre contrat de licence Microsoft autorise l'exécution de Windows dans un environnement hébergé virtuel.
- Si vous comptez utiliser des ensembles non compatibles avec le GPU (autres que Graphics.G4DN, GraphicsPro .g4dn, Graphics et GraphicsPro), vérifiez que vous en utiliserez au moins 100 par région. WorkSpaces Ces 100 WorkSpaces peuvent être n'importe quel mélange de AlwaysOn et AutoStop WorkSpaces. Il est nécessaire d'en utiliser un minimum de 100 WorkSpaces par région pour fonctionner WorkSpaces sur du matériel dédié. Il est nécessaire de l'exécuter WorkSpaces sur du matériel dédié pour respecter les exigences de licence Microsoft. Le matériel dédié est fourni sur le AWS côté, de sorte que votre VPC peut conserver sa location par défaut.

  Si vous prévoyez d'utiliser des packs compatibles GPU (Graphics.G4DN, GraphicsPro .g4dn, Graphics, and GraphicsPro), vérifiez que vous exécuterez au moins 4 AlwaysOn ou 20 AutoStop packs compatibles GPU dans une région par mois sur du matériel dédié. WorkSpaces

  > **Note**
  >
  > - Graphics.g4dn, GraphicsPro .g4dn, Graphics et GraphicsPro les bundles ne peuvent être créés que pour le protocole PCoIP pour le moment.

- Le bundle Graphics ne sera plus pris en charge après le 30 novembre 2023. Nous vous recommandons de migrer votre offre groupée WorkSpaces vers Graphics.G4DN. Pour plus d'informations, consultez Migrer un WorkSpace.
- Les graphismes et GraphicsPro les offres groupées ne sont actuellement pas disponibles dans la région Asie-Pacifique (Mumbai).
- Graphics.g4dn, GraphicsPro .g4dn, Graphics et GraphicsPro les bundles ne sont actuellement pas disponibles dans la région Afrique (Le Cap).
- 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 bundles Windows 11 peuvent uniquement être créés pour le protocole WSP.
- Les ensembles Graphics.g4dn et GraphicsPro .g4dn ne sont actuellement pas disponibles pour Windows 11.
- Les cartes graphiques et GraphicsPro les offres groupées ne sont pas prises en charge sous Windows 11.
- Les bundles Value ne sont pas disponibles pour Windows 11. Pour plus d'informations sur la migration de votre offre groupée de valeur existante, WorkSpaces consultezMigrer un WorkSpace.
- Pour une expérience de visioconférence optimale, nous vous recommandons d'utiliser Power ou PowerPro des offres groupées.

- 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 plus d'informations, consultez Interfaces réseau. Vous devez réserver un masque de réseau /16 à partir d'au moins une des plages d'adresses IP suivantes à cette fin :
  - 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**
>
> - Lorsque 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

- Assurez-vous d'avoir ouvert les ports d'interface de gestion nécessaires pour Microsoft Windows et d'activer Microsoft Office KMS pour BYOL WorkSpaces. Pour plus d'informations, consultez Ports de l'interface de gestion.
- Vous disposez d'une machine virtuelle (VM) qui exécute une version 64 bits de Windows prise en charge. Pour obtenir la liste des versions prises en charge, consultez suivante de cette rubrique Versions Windows prises en charge pour BYOL. La machine virtuelle doit également répondre à ces exigences :
  - Votre système d'exploitation Windows doit être activé sur vos serveurs de gestion des clés.
  - La langue principale de votre système d'exploitation Windows est French (France).
  - Aucun logiciel outre ceux inclus avec Windows ne peut être installé sur la machine virtuelle. Vous pouvez ajouter d'autres logiciels, comme une solution anti-virus, lorsque vous créez ultérieurement une image personnalisée.
  - Ne personnalisez pas le profil utilisateur par défaut (`C:\Users\Default`) et n'effectuez pas d'autres personnalisations avant de créer une image. Toutes les personnalisations doivent être effectuées après la création de l'image. Nous vous recommandons de personnaliser le profil utilisateur via des objets de stratégie de groupe (GPO) et d'appliquer les personnalisations après la création de l'image. En effet, les personnalisations effectuées via des objets de stratégie de groupe peuvent être facilement modifiées ou annulées et sont moins sujettes aux erreurs que les personnalisations effectuées sur le profil utilisateur par défaut.
  - Vous devez créer un compte WorkSpaces_BYOL avec accès administrateur local avant de partager l'image. Le mot de passe du compte peut être requis ultérieurement. Notez-le.
  - La machine virtuelle doit se trouver sur un seul volume avec une taille maximale de 70 Go et au moins 10 Go d'espace libre. Si vous envisagez également de vous abonner à Microsoft Office pour votre image BYOL, la machine virtuelle doit se trouver sur un seul volume d'une taille

maximale de 70 Go et disposant d'au moins 20 Go d'espace libre. Le DISQUE sur lequel se trouve le volume racine ne peut pas dépasser 70 Go.

- Votre machine virtuelle doit exécuter Windows PowerShell version 4 ou ultérieure.

- Assurez-vous d'avoir installé les derniers correctifs Microsoft Windows avant d'exécuter le script BYOL Checker à l'Étape 3 : Exécuter le PowerShell script BYOL Checker sur une machine virtuelle Windows.

> **Note**
>
> - Pour le BYOL AutoStop WorkSpaces, un grand nombre de connexions simultanées pourrait 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.
> - Les AMI chiffrées ne sont pas prises en charge dans le processus d'importation. Assurez-vous de désactiver l'instance utilisée pour créer l'AMI EC2 disposant d'un chiffrement EBS. Le chiffrement peut être activé après le provisionnement de WorkSpaces la version finale.

Versions Windows prises en charge pour BYOL

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

- Windows 10 version 21H2 (mise à jour de décembre 2021)
- Windows 10 version 22H2 (mise à jour de novembre 2022)
- Windows 10 Entreprise LTSC 2019 (1809)
- Windows 10 Entreprise LTSC 2021 (21H2)
- Windows 11 version 23H2 (version d'octobre 2023)
- Windows 11 version 22H2 (version d'octobre 2022)

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.

Ajout de Microsoft Office à votre image BYOL

Si vous choisissez de vous abonner à Office par le biais de ce service AWS, des frais supplémentaires s'appliqueront. Pour plus d'informations, consultez la section WorkSpaces Tarification.

> **Important**
>
> - Si Microsoft Office est déjà installé sur la machine virtuelle que vous utilisez pour créer votre image BYOL, vous devez la désinstaller de la machine virtuelle si vous souhaitez vous abonner à Office via AWS.
> - Si vous envisagez de vous abonner à Office via AWS, assurez-vous que votre machine virtuelle dispose d'au moins 20 Go d'espace disque disponible.
> - Lors de l'importation d'images, vous pouvez vous abonner à Office 2016 ou 2019, mais pas à Office 2021. Pour Office 2021 et d'autres applications comme Microsoft Visio 2021 et Microsoft Project 2021, consultez Gestion des applications.
> - Pour apporter vos propres licences Microsoft 365 pour les applications basées sur le navigateur et de bureau sur Amazon WorkSpaces, installez les applications Microsoft 365 sur votre image BYOL une fois le processus d'ingestion d'image BYOL terminé.

> **Note**
>
> Les images Graphics.g4dn et GraphicsPro .g4dn BYOL ne sont compatibles qu'avec Office 2019 et non avec Office 2016.

Si vous choisissez de vous abonner à Office, le processus d'ingestion d'images BYOL prend au moins 3 heures.

Pour plus d'informations sur l'abonnement à Office pendant le processus d'ingestion BYOL, consultez l'Étape 6 : Création d'une image BYOL à l'aide de la console WorkSpaces .

Paramètres de langue Office

Nous choisissons la langue utilisée pour votre abonnement Office en fonction de la AWS région dans laquelle vous effectuez votre ingestion d'images BYOL. Par exemple, quand vous effectuez une ingestion d'image BYOL dans la région Asie-Pacifique (Tokyo), la langue de votre abonnement Office est le japonais.

Par défaut, nous installons un certain nombre de modules linguistiques Office fréquemment utilisés sur votre ordinateur WorkSpaces. Si celui que vous souhaitez n'est pas installé, vous pouvez télécharger des modules linguistiques supplémentaires auprès de Microsoft. Pour plus d'informations, consultez Module linguistique complémentaire de la documentation Microsoft.

Pour modifier la langue utilisée dans Office, plusieurs options s'offrent à vous :

Option 1 : Autoriser les utilisateurs individuels à personnaliser leurs paramètres de langue Office

Les utilisateurs individuels peuvent ajuster les paramètres de langue d'Office sur leur WorkSpaces. Pour plus d'informations, consultez Ajouter une langue d'édition ou de création, ou définir des préférences linguistiques dans Office de la documentation Microsoft.

Option 2 : utiliser les modèles d'administration GPO (.admx/.adml) pour appliquer les paramètres linguistiques par défaut d'Office à tous vos utilisateurs WorkSpaces

Vous pouvez utiliser les paramètres GPO (Group Policy Object) pour appliquer les paramètres de langue Office par défaut à vos WorkSpaces utilisateurs.

> **Note**
>
> Vos WorkSpaces utilisateurs ne pourront pas annuler les paramètres linguistiques imposés par le biais de GPO.

Pour plus d'informations sur l'utilisation d'un GPO pour définir les paramètres de langue Office, consultez Personnalisation de la configuration et des paramètres des langues pour Office de la documentation Microsoft. Office 2016 et Office 2019 utilisent les mêmes paramètres GPO (étiquetés avec Office 2016).

Pour utiliser les GPO, vous devez installer les outils d'administration Active Directory. Pour plus d'informations sur l'utilisation des outils d'administration Active Directory pour travailler avec des objets de stratégie de groupe, consultez Configuration des outils d'administration Active Directory pour WorkSpaces.

Avant de configurer les paramètres de stratégie Office 2016 ou Office 2019, vous devez télécharger les fichiers de modèles d'administration (.admx/.adml) pour Office depuis le Centre de téléchargement Microsoft. Après avoir téléchargé les fichiers modèles d'administration, vous devez ajouter les `office16.adml` fichiers `office16.admx` et dans le magasin central du contrôleur de domaine de votre WorkSpaces répertoire. (Les fichiers `office16.admx` et `office16.adml` s'appliquent à Office 2016 et à Office 2019.) Pour plus d'informations sur l'utilisation des fichiers `.admx` et `.adml`, consultez Comment créer et gérer le magasin central des modèles d'administration de stratégie de groupe dans Windows de la documentation Microsoft.

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 le fichier de modèle d'administration de stratégie de groupe pour Office

1. Téléchargez les fichiers de modèles d'administration (.admx/.adml) pour Office depuis le Centre de téléchargement Microsoft.
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 `office16.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 `office16.adml` dans le dossier `\\FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions\en-US`.

Pour configurer les paramètres de langue du GPO pour Office

1. Sur l'administration de votre annuaire WorkSpace ou sur l'instance Amazon EC2 jointe à votre WorkSpaces annuaire, ouvrez l'outil de gestion des politiques de groupe ()gpmc.msc.
2. Développez la forêt (Forêt : ***FQDN***).
3. Développez Domaines.
4. Développez votre FQDN (par exemple, `example.com`).
5. Sélectionnez votre FQDN, ouvrez le menu contextuel (clic droit) ou le menu Action, puis choisissez Créer un GPO dans ce domaine et le lier ici.
6. Nommez votre GPO (par exemple, **`Office`**).
7. Sélectionnez votre GPO, ouvrez le menu contextuel (clic droit) ou le menu Action, puis choisissez Modifier.
8. Dans l'éditeur de gestion des stratégies de groupe, choisissez Configuration utilisateur, Politiques, Définitions de politiques du modèle administratif (fichiers ADMX) extraites de l'ordinateur local, Microsoft Office 2016 et Préférences de langue.

   > **Note**
   >
   > Office 2016 et Office 2019 utilisent les mêmes paramètres GPO (étiquetés avec Office 2016). Si vous ne voyez pas l'option Définitions de politiques du modèle administratif (fichiers ADMX) extraites de l'ordinateur local sous Configuration utilisateur, Politiques, cela signifie que les fichiers `office16.admx` et `office16.adml` ne sont pas correctement installés sur votre contrôleur de domaine.

9. Dans Préférences de langue, spécifiez la langue que vous souhaitez utiliser pour les paramètres suivants. Assurez-vous de définir chaque paramètre à Activé, puis sélectionnez la langue de votre choix sous Options. Choisissez OK pour enregistrer chaque paramètre.

   - Langue d'affichage > Afficher l'aide en
   - Langue d'affichage > Afficher les menus et les boîtes de dialogue en
   - Langues d'édition > Langue d'édition principale

10. Fermez l'outil de gestion des stratégies de groupe lorsque vous avez terminé.

11. Les modifications des paramètres de stratégie de groupe 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 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 partir d'une invite de commande administrative, entrez gpupdate /force.

Option 3 : mettre à jour les paramètres du registre des langues Office sur votre WorkSpaces

Pour définir les paramètres de langue Office via le registre, mettez à jour les paramètres suivants du registre :

- HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Office \ 16.0 \ Common \ \ UILanguage LanguageResources
- HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Office \ 16.0 \ Common \ \ LanguageResources HelpLanguage

Pour ces paramètres, ajoutez une valeur de clé DWORD avec l'ID local (LCID) Office approprié. Par exemple, le LCID pour Anglais (États-Unis) est 1033. Les LCID étant des valeurs décimales, vous devez définir l'option Base pour la valeur DWORD à Décimal. Pour obtenir la liste des LCID Office, consultez la section Identifiants de langue et valeurs OptionState d'identifiant dans Office 2016 dans la documentation Microsoft.

Vous pouvez appliquer ces paramètres de registre à vos paramètres GPO ou à l' WorkSpaces aide d'un script de connexion.

Pour plus d'informations sur l'utilisation des paramètres de langue pour Office, consultez Personnalisation de la configuration et des paramètres des langues pour Office de la documentation Microsoft.

Ajoutez Office à votre BYOL existant WorkSpaces

Vous pouvez également ajouter un abonnement à Office à votre BYOL existant WorkSpaces en procédant comme suit.

- Gérez les applications (recommandé) : vous pouvez installer et configurer Microsoft Office, Microsoft Visio ou Microsoft Project 2021 sur vos applications existantes WorkSpaces. Pour plus d'informations, consultez Gestion des applications.

- Migrer un WorkSpace : après avoir créé un bundle BYOL avec Office installé, vous pouvez utiliser la fonctionnalité de WorkSpaces migration pour migrer votre BYOL existant WorkSpaces vers le bundle BYOL abonné à Office. Pour plus d'informations, consultez Migrer un WorkSpace.

> **Note**
>
> L'option de gestion des applications est disponible pour installer Microsoft Office 2021 et d'autres applications, telles que Microsoft Visio 2021 et Microsoft Project 2021 sur votre WorkSpaces. Pour installer Microsoft Office 2016 ou 2019 sur votre ordinateur WorkSpaces, utilisezMigrer un WorkSpace.

Migration entre les versions de Microsoft Office

Pour effectuer une migration d'une version de Microsoft Office à une autre, vous pouvez effectuer les opérations suivantes :

- Gérer les applications (recommandé) — Vous pouvez désinstaller la version originale d'Office et installer Office 2021 et d'autres applications, telles que Microsoft Visio 2021 et Microsoft Project 2021, sur votre version existante WorkSpaces. Par exemple, pour migrer de Microsoft Office 2019 vers Microsoft Office 2021, utilisez le flux de travail de gestion des applications pour désinstaller Microsoft Office 2019 et installer Microsoft Office 2021. Pour plus d'informations, consultez Gestion des applications.
- Migrer un WorkSpace — Pour migrer de Microsoft Office 2016 vers 2019 ou de Microsoft Office 2019 vers 2016, vous devez créer un bundle BYOL abonné à la version d'Office vers laquelle vous souhaitez migrer. Utilisez ensuite la fonctionnalité de WorkSpaces migration pour migrer votre BYOL WorkSpaces existant abonné à Office vers le bundle BYOL abonné à la version d'Office vers laquelle vous souhaitez migrer. Par exemple, pour migrer d'Office 2016 vers 2019, créez un bundle BYOL abonné à Office 2019. Utilisez ensuite la fonctionnalité de WorkSpaces migration pour migrer votre BYOL WorkSpaces existant abonné à Office 2016 vers le bundle BYOL abonné à Office 2019. Pour plus d'informations, consultez Migrer un WorkSpace.

Vous pouvez utiliser ces options pour migrer vos WorkSpaces abonnés à Microsoft Office AWS vers des applications Microsoft 365. Toutefois, la gestion des applications se limite à la désinstallation de Microsoft Office de votre WorkSpace. Vous devez apporter vos propres outils et programmes d'installation pour installer les applications Microsoft 365 sur votre WorkSpaces.

> **Note**
>
> À l'aide de la gestion des applications, vous pouvez installer ou désinstaller Microsoft Office, Microsoft Visio ou MicrosoftProject 2021 sur votre WorkSpaces. Pour les versions de Microsoft Office 2016 ou 2019, vous pouvez uniquement les supprimer de votre WorkSpaces. Pour installer Microsoft Office 2016 ou 2019 sur votre ordinateur WorkSpaces, migrez un WorkSpace.

Pour en savoir plus sur la migration, consultez Migrer un WorkSpace.

Désabonnement d'Office

Pour vous désabonner d'Office, vous pouvez effectuer les opérations suivantes :

- Gérer les applications (recommandé) - Vous pouvez désinstaller Microsoft Office et d'autres applications telles que Microsoft Visio et Microsoft Project de votre WorkSpaces. Pour plus d'informations, consultez Gestion des applications.
- Migrer un WorkSpace : vous pouvez créer un bundle BYOL qui n'est pas abonné à Office. Utilisez ensuite la fonctionnalité de WorkSpaces migration pour migrer votre BYOL existant WorkSpaces vers le bundle BYOL qui n'est pas abonné à Office. Pour plus d'informations, consultez Migrer un WorkSpace.

Mises à jour Office

Si vous vous êtes abonné à Office via AWS, les mises à jour Office sont incluses dans vos mises à jour Windows régulières. Pour rester à jour de tous les correctifs et mises à jour de sécurité, nous vous recommandons de mettre à jour régulièrement vos images de base BYOL.

Étape 1 : Vérifiez l'éligibilité de votre compte au BYOL à l'aide de la console Amazon WorkSpaces

Avant de pouvoir activer l'option BYOL pour votre compte, vous devez passer par un processus de vérification afin de confirmer votre éligibilité. Tant que vous n'aurez pas suivi ce processus, l'option Enable BYOL ne sera pas disponible dans votre WorkSpaces console Amazon.

> **Note**
>
> Le processus de vérification prend au moins un jour ouvrable et peut être plus long si vous souhaitez associer deux ou plusieurs AWS comptes compatibles BYOL afin qu'ils utilisent le même matériel sous-jacent.

Pour vérifier l'éligibilité de votre compte au BYOL à l'aide de la console Amazon WorkSpaces

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Paramètres du compte, puis sous Bring your own license (BYOL), choisissez Afficher les paramètres WorkSpaces BYOL. Si votre compte n'est actuellement pas éligible à l'option BYOL, un message vous fournit des indications sur la procédure à suivre. Pour commencer, contactez votre responsable de AWS compte ou votre représentant commercial, ou contactez le AWS Support Centre. Votre contact vérifiera votre éligibilité à l'option BYOL.

   Pour déterminer votre éligibilité à l'option BYOL, votre contact vous demandera certaines informations. Par exemple, vous pouvez être invité à répondre aux questions suivantes.

   - Avez-vous examiné et accepté les exigences BYOL répertoriées précédemment ?
   - Dans quelles AWS régions avez-vous besoin que votre compte soit activé pour BYOL ?
   - Combien de BYOL WorkSpaces prévoyez-vous de déployer par AWS région ?
   - Quel est votre plan de montée en puissance ?
   - Achetez-vous WorkSpaces auprès d'un revendeur ?
   - De quels types de bundle avez-vous besoin pour BYOL ?
   - Votre organisation possède-t-elle d'autres AWS comptes activés pour le BYOL dans la même région ? Dans l'affirmative, souhaitez-vous associer ces comptes afin qu'ils utilisent le même matériel sous-jacent ?

     Si les comptes sont liés, le nombre total de comptes WorkSpaces déployés sur ces comptes est agrégé afin de déterminer votre éligibilité au BYOL. Sachez que l'association des comptes demande davantage de temps. Si vous souhaitez associer les comptes, soyez prêt à fournir les numéros de compte à votre contact.
3. Une fois votre éligibilité au BYOL confirmée, vous pouvez passer à l'étape suivante, qui consiste à activer le BYOL pour votre compte dans la console Amazon WorkSpaces .

Étape 2 : Activez BYOL pour votre compte BYOL à l'aide de la console Amazon WorkSpaces

Pour activer l'option BYOL pour votre compte, vous devez définir une interface réseau de gestion. Cette interface est connectée à un réseau de WorkSpaces gestion Amazon sécurisé. Il est utilisé pour le streaming interactif de l' WorkSpace ordinateur de bureau vers WorkSpaces les clients Amazon et pour permettre WorkSpaces à Amazon de gérer le WorkSpace.

> **Note**
>
> Vous ne devez effectuer les étapes de cette procédure qu'une seule fois par région afin d'activer BYOL pour votre compte.

Pour activer BYOL pour votre compte à l'aide de la console Amazon WorkSpaces

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Paramètres du compte, puis sous Bring your own license (BYOL), choisissez Afficher les paramètres WorkSpaces BYOL.
3. Sur la page Paramètres du compte, sous Apportez votre propre licence (BYOL), choisissez Activer BYOL.

   Si l'option Activer BYOL ne s'affiche pas, cela signifie que votre compte n'est pas éligible actuellement. Pour plus d'informations, consultez Étape 1 : Vérifiez l'éligibilité de votre compte au BYOL à l'aide de la console Amazon WorkSpaces .
4. Sous Bring Your Own License (Réutilisez vos licences - BYOL), dans la zone Management network interface IP address range (Plage d'adresses IP d'interface de réseau de gestion), choisissez une plage d'adresses IP, puis choisissez Display available CIDR blocks (Afficher les blocs d'adresses CIDR disponibles).

   Amazon WorkSpaces recherche et affiche les plages d'adresses IP disponibles sous forme de blocs CIDR (Classless Classless Inter-Domain Routing) IPv4, dans la plage que vous spécifiez. Si vous avez besoin d'une plage d'adresses IP spécifique, vous pouvez modifier la plage de recherche.

> **Important**
>
> Une fois que vous avez spécifié une plage d'adresses IP, vous ne pouvez plus la modifier. Assurez-vous de spécifier une plage d'adresses IP qui ne soit pas en conflit avec les plages utilisées par votre réseau interne. Si vous avez des questions concernant la fourchette à spécifier, contactez votre responsable de AWS compte ou votre représentant commercial, ou contactez le AWS Support Centre avant de continuer.

5. Sélectionnez le bloc d'adresse CIDR de votre choix dans la liste des résultats, puis choisissez Enable BYOL (Activer BYOL).

   Ce processus peut prendre plusieurs heures. Lors de WorkSpaces l'activation de votre compte pour BYOL, passez à l'étape suivante.

Étape 3 : Exécuter le PowerShell script BYOL Checker sur une machine virtuelle Windows

Une fois que vous avez activé BYOL pour votre compte, vous devez confirmer que votre machine virtuelle répond aux exigences pour BYOL. Pour ce faire, procédez comme suit pour télécharger et exécuter le script WorkSpaces BYOL Checker PowerShell . Le script effectue une série de tests sur la machine virtuelle que vous prévoyez d'utiliser pour créer votre image.

> **Important**
>
> La machine virtuelle doit réussir tous les tests avant que vous ne puissiez l'utiliser pour BYOL.

Pour télécharger le script BYOL Checker

Avant de télécharger et d'exécuter le script BYOL 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 BYOL Checker à l'adresse https://tools.amazonworkspaces.com/BYOLChecker.zip vers votre dossier `Downloads`.
2. Dans votre dossier `Downloads`, créez un dossier `BYOL`.

3. Récupérez les fichiers dans `BYOLChecker.zip` et copiez-les dans le dossier `Downloads\BYOL`.
4. Supprimez le dossier `Downloads\BYOLChecker.zip` afin de ne conserver que les fichiers récupérés.

Effectuez les étapes suivantes pour exécuter le script BYOL Checker.

Pour exécuter le script BYOL Checker

1. Depuis le bureau Windows, ouvrez Windows PowerShell. Cliquez sur le bouton Démarrer de Windows, cliquez avec le bouton droit sur Windows PowerShell, puis sélectionnez Exécuter en tant qu'administrateur. Si le Contrôle des comptes d'utilisateur vous invite à choisir si vous souhaitez PowerShell apporter des modifications à votre appareil, choisissez Oui.
2. À l'invite de PowerShell commande, accédez au répertoire dans lequel se trouve le script BYOL 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 BYOL 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 BYOL Checker :

   ```
   .\BYOLChecker.ps1
   ```
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 Commencer les 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, `BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` et `ImageInfo.text`. Ces fichiers se trouvent dans le répertoire qui contient les fichiers de script BYOL Checker.

    > **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 le tests, vous obtenez un message Validation Successful (Validation réussie). Passez en revue les paramètres régionaux de la machine virtuelle affichés dans l'outil. Pour mettre à jour les paramètres régionaux, suivez les instructions suivantes dans la documentation Microsoft et exécutez de nouveau le script BYOL Checker.
12. Arrêtez la machine virtuelle et créez un instantané de celle-ci.
13. Redémarrez la machine virtuelle. Choisissez Run Sysprep. Si Sysprep aboutit, la machine virtuelle que vous avez exportée après l'Step 12 peut être importée dans Amazon Elastic Compute Cloud (Amazon EC2). Dans le cas contraire, passez en revue les journaux Sysprep, revenez à l'instantané pris à l'Step 12, résolvez les problèmes signalés, prenez un nouvel instantané et exécutez de nouveau le script BYOL Checker.

    Le fait que les packages Modern AppX ne soient pas désinstallés pour tous les utilisateurs constitue la raison la plus fréquente de l'échec de Sysprep. Utilisez l'Remove-AppxPackage PowerShell applet de commande pour supprimer les packages AppX.
14. Après avoir créé votre image avec succès, vous pouvez supprimer le compte WorkSpaces_BYOL.

Liste des messages et corrections d'erreurs

L'importation BYOL requiert Powershell 4.0 ou une version ultérieure. La version installée de n' PowerShell est pas prise en charge.

PowerShell la version 4.0 ou ultérieure doit être installée. Pour plus d'informations, consultez Microsoft Windows PowerShell.

L'importation BYOL ne prend pas en charge les systèmes sur lesquels une version active de Microsoft Office est installée.

Microsoft Office doit être désinstallé avant l'importation. Pour plus d'informations, consultez Désinstaller Office d'un PC.

L'importation BYOL nécessite un système sans agent PCoIP.

Désinstallez l'agent PCoIP. Pour plus d'informations sur la désinstallation de l'agent PCoIP, consultez Uninstalling the Teradici PCoIP Software Client for 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 Modifier les paramètres TCP/IP.

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.

Seuls les lecteurs C et D peuvent être présents sur un WorkSpace périphérique utilisé pour importer une image. 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 outils VMware.

Les outils VMware doivent être désinstallés. Pour plus d'informations, consultez Uninstalling and manually installing VMware Tools in 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 réinitialisé.

Le nombre Image Rearm ne doit pas être égal à 0. 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 `cscript C:\Windows\System32\slmgr.vbs /dlv`, puis appuyez sur la touche Entrée.

3. Pour définir le nombre de réinitialisation à une valeur autre que 0. Pour plus d'informations, consultez Utiliser Sysprep (généralisation) sur une installation Windows.

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 ByolChecker 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.

Étape 4 : Exporter la machine virtuelle depuis l'environnement de virtualisation

Pour créer une image pour BYOL, vous devez d'abord exporter la machine virtuelle à partir de votre environnement de virtualisation. La machine virtuelle doit se trouver sur un seul volume avec une taille maximale de 70 Go et au moins 10 Go d'espace libre. Pour plus d'informations, reportez-vous à la documentation de votre environnement de virtualisation et à la section Exportation de votre machine virtuelle à partir de son environnement de virtualisation dans le Guide de l'utilisateur de VM Import/Export.

Étape 5 : Importer la machine virtuelle comme image dans Amazon EC2

Après avoir exporté votre machine virtuelle, vérifiez les prérequis pour l'importation des systèmes d'exploitation Windows à partir d'une machine virtuelle. Prenez les mesures appropriées le cas échéant. Pour plus d'informations, consultez Prérequis VM Import/Export.

> **Note**
>
> L'importation d'une machine virtuelle avec un disque chiffré n'est pas prise en charge. Si vous avez opté pour le chiffrement par défaut pour les volumes Amazon Elastic Block Store

(Amazon EBS), vous devez désélectionner cette option avant d'importer votre machine virtuelle.

Importez votre machine virtuelle dans Amazon EC2 en tant qu'Amazon Machine Image (AMI). Utilisez l'une des méthodes suivantes :

- Utilisez la commande import-image avec l' AWS CLI. Pour plus d'informations, consultez import-image du site AWS CLI Command Reference.
- Utilisez l'opération d'API ImportImage. Pour plus d'informations, consultez ImportImagele manuel Amazon EC2 API Reference.

Pour plus d'informations, consultez Importation d'une machine virtuelle en tant qu'image dans le document VM Import/Export User Guide.

Étape 6 : Création d'une image BYOL à l'aide de la console WorkSpaces

Procédez comme suit pour créer une image WorkSpaces BYOL.

> **Note**
>
> Pour effectuer cette procédure, vérifiez que vous disposez des autorisations AWS Identity and Access Management (IAM) nécessaires pour :
>
> - Appelle WorkSpaces **`ImportWorkspaceImage`**.
> - Appeler la fonction **`DescribeImages`** Amazon EC2 sur l'image Amazon EC2 que vous souhaitez utiliser pour créer l'image BYOL.
> - Appeler la fonction **`ModifyImageAttribute`** Amazon EC2 sur l'image Amazon EC2 que vous souhaitez utiliser pour créer l'image BYOL. Assurez-vous que les autorisations de lancement sur l'image Amazon EC2 ne sont pas restreintes. L'image doit pouvoir être partagée tout au long du processus de création d'image BYOL.
>
> Pour un exemple de politique IAM spécifique au BYOL WorkSpaces, voir. Gestion des identités et des accès pour WorkSpaces Pour plus d'informations sur l'utilisation des autorisations IAM, consultez Modification des autorisations pour un utilisateur IAM dans le Guide de l'utilisateur IAM.

Pour créer un Graphics.g4dn, GraphicsPro .g4dn, Graphics ou un GraphicsPro bundle à partir de votre image, contactez le AWS Support Centre pour que votre compte soit ajouté à la liste des autorisations. Une fois que votre compte figure dans la liste des autorisations, vous pouvez utiliser la AWS CLI import-workspace-image commande pour ingérer les fichiers Graphics.g4dn, GraphicsPro .g4dn, Graphics ou image. GraphicsPro Pour plus d'informations, consultez import-workspace-imagele manuel de référence des AWS CLI commandes.

Pour créer une image à partir de la machine virtuelle Windows

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Images.
3. Choisissez Créer une image BYOL.
4. Sur la page Créer une image BYOL, procédez comme suit :

   - Pour l'ID AMI, cliquez sur le lien Console EC2, puis choisissez l'image Amazon EC2 que vous avez importée comme décrit dans la section précédente (Étape 5 : Importer la machine virtuelle comme image dans Amazon EC2). Le nom de l'image doit commencer par `ami-`, suivi de l'identifiant de l'AMI (par exemple, `ami-1234567e`).
   - Dans le champ Nom de l'image, saisissez le nom unique de l'image.
   - Dans le champ Description de l'image, saisissez la description qui vous permettra d'identifier rapidement l'image.
   - Pour Type d'instance, choisissez le type de bundle approprié (Regular, Graphics.G4DN, Graphics ou GraphicsPro), selon le protocole que vous souhaitez utiliser pour votre image, PCoIP ou WorkSpaces Streaming Protocol (WSP). Si vous souhaitez créer un bundle GraphicsPro .g4dn, choisissez Graphics.g4dn. Pour les ensembles non compatibles avec le GPU (ensembles autres que Graphics.G4DN, .g4dn, Graphics ou), GraphicsPro choisissez Regular. GraphicsPro

     > **Note**
     >
     > Graphics.g4dn, GraphicsPro .g4dn, Graphics et GraphicsPro images peuvent être créés uniquement pour le protocole PCoIP pour le moment.

- (Facultatif) Pour Sélectionner des applications, choisissez la version de Microsoft Office à laquelle vous souhaitez vous abonner. Pour plus d'informations, consultez Ajout de Microsoft Office à votre image BYOL.
- (Facultatif) Pour Balises, choisissez Ajouter une nouvelle balise pour associer des balises à cette image. Pour plus d'informations, consultez Balisage des ressources WorkSpaces.

5. Choisissez Créer une image BYOL.

   Pendant la création de votre image, son état dans la page Images de la console est En attente. Le processus d'ingestion BYOL prend au moins 90 minutes. Si vous êtes aussi abonné à Office, attendez-vous à ce que le processus prenne au moins 3 heures.

   Si la validation de l'image n'aboutit pas, la console affiche un code d'erreur. Lorsque la création de l'image est terminée, l'état passe à Available (Disponible).

Étape 7 : Créer un bundle personnalisé à partir de l'image BYOL

Une fois votre image BYOL créée, vous pouvez l'utiliser pour créer une solution groupée personnalisée. Pour plus d'informations, consultez Création d'une WorkSpaces image personnalisée et d'un bundle.

Étape 8 : Enregistrez un répertoire dédié pour WorkSpaces

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

Pour enregistrer un annuaire pour WorkSpaces

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Sélectionnez l'annuaire et choisissez Actions, Register (Enregistrer).
4. Dans la boîte de dialogue Enregistrer le répertoire, pour Activer le répertoire dédié WorkSpaces, sélectionnez Oui.
5. Choisissez Register (S'inscrire).

Si vous avez déjà enregistré un AWS Managed Microsoft AD annuaire ou un répertoire AD Connector WorkSpaces qui ne fonctionne pas sur du matériel dédié, vous pouvez configurer un nouveau AWS Managed Microsoft AD répertoire ou un répertoire AD Connector à cette fin. Vous pouvez également

désenregistrer le répertoire, puis le réenregistrer en tant que répertoire dédié. WorkSpaces Pour ce faire, procédez comme suit.

> **Note**
>
> Vous ne pouvez effectuer cette procédure que si aucun WorkSpaces n'est associé au répertoire.

Pour désenregistrer un annuaire et le réenregistrer pour un répertoire dédié WorkSpaces

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Mettre fin à l'existant WorkSpaces.
3. Dans le volet de navigation, choisissez Directories (Annuaires).
4. Sélectionnez l'annuaire et choisissez Actions, Annuler l'enregistrement.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Annuler l'enregistrement.
6. Sélectionnez de nouveau l'annuaire et choisissez Actions, Register (Enregistrer).
7. Dans la boîte de dialogue Enregistrer le répertoire, pour Activer le répertoire dédié WorkSpaces, sélectionnez Oui.
8. Choisissez Register (S'inscrire).

Étape 9 : Lancez votre BYOL WorkSpaces

Après avoir enregistré un répertoire pour WorkSpaces Dedicated, vous pouvez lancer votre BYOL WorkSpaces dans ce répertoire. Pour plus d'informations sur le lancement WorkSpaces, consultezLancement d'un bureau virtuel avec WorkSpaces.

Surveillez votre WorkSpaces

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 plus d'informations, consultez Surveillez vos CloudWatch indicateurs WorkSpaces d'utilisation.

CloudWatch Évènements

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 plus d'informations, consultez Surveillez votre WorkSpaces utilisation d'Amazon EventBridge.

CloudTrail journaux

AWS CloudTrail fournit un enregistrement des actions réalisées par un utilisateur, un rôle ou un service AWS 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 CloudTrailenregistre les événements de connexion réussis et infructueux pour les utilisateurs de cartes à puce. Pour plus d'informations, consultez Compréhension des événements de connexion AWS pour les utilisateurs de carte 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

Moniteur Internet utilise les données de connectivité qu'AWS capture à partir de son empreinte réseau mondial pour calculer une référence de performance et de disponibilité pour le trafic 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.

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 métriques 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.

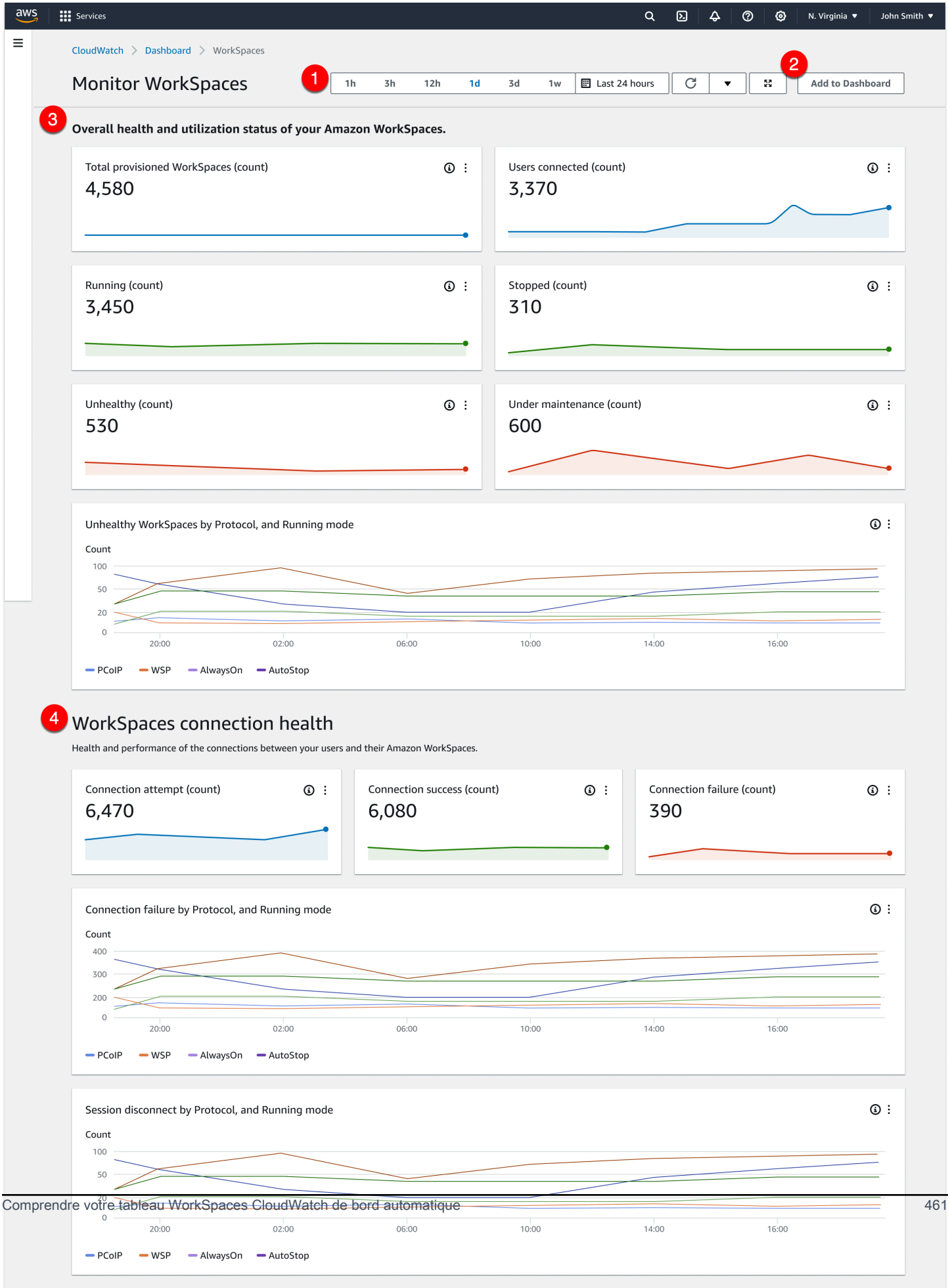
Pour utiliser le tableau de bord WorkSpaces CloudWatch automatique

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. Choisissez 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.


aws
Services
N. Virginia
John Smith
CloudWatch
Dashboard
WorkSpaces
Monitor WorkSpaces
1
1h
3h
12h
1d
3d
1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

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' WorkSpace instances 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 plus d'informations, consultez Exigences relatives à l'adresse IP et au port pour WorkSpaces.

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 eux WorkSpaces a renvoyé à un état de santé.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

`Unhealthy` [1]	Le numéro WorkSpaces renvoyait à un état insalubre.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

Métrique	Description	Dimensions	Statistiques	Unités

`ConnectionAttempt` [2]	Nombre de tentatives de connexion.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

`ConnectionSuccess` [2]	Nombre de connexions ayant réussi.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

`ConnectionFailure` [2]	Nombre de connexions ayant échoué.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			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`
			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`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Milliseconde (temps)

`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`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

Métrique	Description	Dimensions	Statistiques	Unités

`UserConnected` [3]	Le nombre de WorkSpaces ceux auxquels un utilisateur est connecté.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

`Stopped`	Le nombre d' WorkSpaces entre eux sont arrêtés.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, Somme, Maximum, Minimum et Exemples de données	Nombre

`Maintenance` [4]	Le nombre d'entre WorkSpace s eux sont en cours de maintenance.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			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
`TrustedDeviceCertificateDaysBeforeExpiration` [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`
			Moyenne, maximale, minimale	Pourcentage

`MemoryUsage`	Pourcentage de mémoire de la machine utilisé.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, maximale, minimale	Pourcentage

`RootVolumeDiskUsage`	Pourcentage du volume du disque racine utilisé.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, maximale, minimale	Pourcentage

Métrique	Description	Dimensions	Statistiques	Unités

`UserVolumeDiskUsage`	Pourcentage du volume de disque utilisateur utilisé.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, maximale, minimale	Pourcentage

`UDPPacketLossRate` [7]	Pourcentage de paquets abandonnés entre le client et la passerelle.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, maximale, minimale, échantillons de données	Pourcentage

`UpTime`	Le temps écoulé depuis le dernier redémarrage d'un WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Moyenne, maximale, minimale, échantillons de données	Secondes

[1] 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 établies 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 colis.

- Sur PCoIP : mesure la perte moyenne de paquets à la passerelle par le client.
- Sur WSP : mesure la perte moyenne de colis entre le client et 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-XXXXXXXXX` .
`RunningMode`	Filtre les données métriques en fonction WorkSpaces de 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 `wsb-XXXXXXXXXX` .
`ComputeType`	Filtre les données métriques WorkSpaces selon le type de calcul.

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-statisticscommande.

```
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 du protocole de WorkSpaces streaming (WSP) 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 Zero PCoIP, il s'agit de l'adresse IP du client auth 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 partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
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.

Compréhension des événements de connexion AWS pour les utilisateurs de carte 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 le nom de chaque événement de connexion CloudTrail et son but.

Nom de l'événement	But de l'événement
`CredentialChallenge`	Indique que la connexion AWS a exigé de l'utilisateur qu'il réponde à une demande d'informations d'identification spécifique, et précise les informations `CredentialType` requises (par exemple, SMARTCARD).
`CredentialVerification`	Indique que l'utilisateur a tenté de répondre à une demande `CredentialChallenge` spécifique, et précise si ces informations d'identification lui ont permis de se connecter ou non.
`UserAuthentication`	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.

Le tableau suivant présente d'autres champs de données d'événements utiles contenus dans des événements CloudTrail de connexion spécifiques.

Nom de l'événement	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
`AuthWorkflowID`	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.	`CredentialChallenge`, `CredentialVerification`, `UserAuthentication`	« AuthWorkflowID » : « 9de74b32-8362-4a01-a524-de21df59fd83"

Nom de l'événement	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
`CredentialType`	Indique que l'utilisateur a tenté de répondre à une demande `CredentialChallenge` spécifique, et précise si ces informations d'identification lui ont permis de se connecter ou non.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	« CredentialType » : « SMARTCARD » (valeurs possibles aujourd'hui : SMARTCARD)
`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 de scénarios de connexion AWS

Les exemples suivants illustrent la séquence d'événements CloudTrail 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.

Événement 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 de l'événement 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 de l'événement 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.

Événement 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",
    "awaRegion": "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 de l'événement 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"
    }
}
```

Continuité des activités pour Amazon WorkSpaces

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 plus d'informations, consultez Résilience dans 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 WorkSpaces à leur 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 bénéficier 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 Amazon WorkSpaces
- Résilience multirégionale pour Amazon WorkSpaces

Redirection entre régions pour Amazon 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 région de basculement que vous avez spécifiée lorsqu'ils ne peuvent pas accéder à leur zone de basculement WorkSpaces dans la AWS 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

- Prérequis
- Limites
- 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

Prérequis

- 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 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.

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.

Limites

- 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.
- Lorsque vous utilisez la redirection entre régions, les données utilisateur ne sont pas conservées d'une région WorkSpaces à l'autre. Pour garantir que les utilisateurs puissent accéder à leurs fichiers depuis différentes régions, nous vous recommandons de configurer Amazon WorkDocs pour vos WorkSpaces utilisateurs, si Amazon WorkDocs est pris en charge dans votre région principale et dans votre région de basculement. Pour plus d'informations sur Amazon WorkDocs, consultez Amazon WorkDocs Drive dans le guide d' WorkDocs administration Amazon. Pour plus d'informations sur l'activation d'Amazon WorkDocs pour vos WorkSpace utilisateurs, consultez Enregistrement d'un annuaire avec WorkSpaces etActivation d'Amazon WorkDocs pour AWS Managed Microsoft AD. Pour plus d'informations sur la manière dont WorkSpaces les utilisateurs

peuvent configurer Amazon WorkDocs sur leur compte WorkSpaces, consultez la section Intégrer avec WorkDocs dans le guide de WorkSpaces l'utilisateur Amazon.

- 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 AWSrégions 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

En utilisant le même compte AWS, créez des alias de connexion dans chaque région principale et de basculement où vous souhaitez configurer la redirection entre régions.

Pour créer un alias de connexion

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
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 compte AWS. 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 compte AWS 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 compte AWS dans la même région AWS. 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 peut être associé à un seul répertoire par région AWS. Si vous partagez un alias de connexion avec un autre compte AWS, 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 compte AWS

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans l'angle supérieur droit de la console, sélectionnez la région AWS dans laquelle vous voulez partager l'alias de connexion avec un autre compte AWS.
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/annuler le partage de l'alias de connexion, sous Partager avec un compte, entrez l'ID du compte AWS 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 pouvez associer un alias de connexion à un seul répertoire par région AWS. Si vous avez partagé un alias de connexion avec un autre compte AWS, un seul compte (votre compte ou le compte partagé) peut associer l'alias à un répertoire dans cette région.

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
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 l'annuaire 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 `wsca-`.

Pour rechercher l'identifiant de connexion d'une association d'alias de connexion

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
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 dans le cadre de 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 à ajouter à ***`votre_nom_de_domaine`***, 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 à ajouter à ***votre_nom_de_domaine***.

Exemple : Pour configurer l'enregistrement de basculement pour votre région de basculement

1. Sous Enregistrements de basculement à ajouter à ***votre_nom_de_domaine***, 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 à ajouter à ***votre_nom_de_domaine***.

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 qui est automatiquement envoyé pour un nouveau message 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre. WorkSpaces
3. Dans le volet de navigation, choisissez 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 WorkSpaces de leur 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans l'angle supérieur droit de la console, sélectionnez la région AWS contenant l'alias de connexion que vous voulez 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans l'angle supérieur droit de la console, sélectionnez la région AWS contenant l'alias de connexion dont vous voulez 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 compte AWS. 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 plus d'informations, consultez Considérations de sécurité si vous arrêtez d'utiliser la redirection entre régions.

Pour supprimer un alias de connexion

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans l'angle supérieur droit de la console, sélectionnez la région AWS contenant l'alias de connexion que vous voulez 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`.

```
{
  "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.

```
{
  "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 pour Amazon 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

- Prérequis
- Limites
- 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

Prérequis

- 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, consultezLancement d'un bureau virtuel avec 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 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, NVMe et PV sur votre système principal WorkSpaces. 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 AWSpour les instances Windows, et Mettre à niveau les pilotes PV sur les instances Windows.
- Assurez-vous de mettre régulièrement à jour les agents EC2Config, EC2Launch et EC2Launch V2 vers les dernières versions. Vous devez le faire au moins une fois tous les 6 mois. Pour plus d'informations, consultez Mettre à jour EC2Config et EC2Launch.
- 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 plus d'informations, consultez 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

Limites

- 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 (Ireland) 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 WorkSpaces, Ubuntu ou compatible avec le GPU WorkSpaces (par exemple Graphics GraphicsPro, 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+ABC12D) 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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre. WorkSpaces
3. Dans le volet de navigation, choisissez WorkSpaces.
4. Sélectionnez celui pour lequel WorkSpace vous souhaitez créer un mode veille 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 à l'adresse https://console.aws.amazon.com/workspaces/.
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 à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le coin supérieur droit de la console, sélectionnez la AWS région principale de votre. WorkSpaces
3. Dans le volet de navigation, choisissez 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 plus d'informations sur la sauvegarde des données utilisateur, contactez AWS 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.

Sécurité dans Amazon WorkSpaces

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les 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 conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à WorkSpaces, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS 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 lorsque vous utilisez WorkSpaces. Elle explique comment configurer WorkSpaces pour atteindre vos objectifs en matière de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS pour vous aider à surveiller et sécuriser vos ressources WorkSpaces.

Table des matières

- Protection des données sur Amazon WorkSpaces
- Gestion des identités et des accès pour WorkSpaces
- Validation de conformité pour Amazon WorkSpaces
- Résilience dans Amazon WorkSpaces
- Sécurité de l'infrastructure dans 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 responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. 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 en savoir plus 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 AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (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.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des 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 FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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 Name (Nom). Cela inclut lorsque vous travaillez avec WorkSpaces ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez 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, consultezConfiguration d'Amazon WorkSpaces pour l'autorisation FedRAMP ou la conformité SRG pour le Département de la Défense (DoD) des États-Unis.

Chiffrement au repos

Vous pouvez chiffrer les volumes de stockage pour votre WorkSpaces utilisation de AWS KMS AWS Key Management Service Key from. Pour plus d'informations, consultez Instances WorkSpace chiffrées.

Lorsque vous créez WorkSpaces avec des volumes chiffrés, WorkSpaces utilisez 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 Chiffrement Amazon EBS dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Chiffrement en transit

Pour PCoIP, les données en transit sont chiffrées à l'aide du chiffrement TLS 1.2 et de la signature de requêtes SigV4. Le protocole PCoIP 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 PCoIP pour Windows WorkSpaces, soit en modifiant les paramètres de sécurité PCoIP dans le fichier pour Amazon Linux. `pcoip-agent.conf` WorkSpaces

Pour en savoir plus sur l'administration des politiques de groupe pour Amazon WorkSpaces, consultez Configuration des paramètres de sécuritéGérez votre Windows WorkSpaces. Pour en savoir plus sur la modification du fichier `pcoip-agent.conf`, consultez Contrôlez le comportement de l'agent PCoIP sur Amazon Linux WorkSpaces, ainsi que la section PCoIP Security Settings dans la documentation Teradici.

Pour le protocole de WorkSpaces streaming (WSP), les données de streaming et de contrôle en transit sont cryptées à l'aide du cryptage DTLS 1.2 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 disposent pas d'autorisations pour les ressources et les opérations WorkSpaces. Pour permettre aux utilisateurs IAM de gérer des ressources WorkSpaces, vous devez créer une politique IAM qui leur donne explicitement les autorisations, et attacher cette politique aux utilisateurs ou groupes IAM qui requièrent ces autorisations.

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. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du 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 du 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.

Pour plus d'informations sur les politiques IAM, consultez Politiques et autorisations dans le Guide de l'utilisateur IAM.

WorkSpaces crée également un rôle IAM, `workspaces_DefaultRole`, qui permet au service WorkSpaces d'accéder aux ressources requises.q

Pour plus d'informations sur IAM, consultez Gestion des identités et des accès (IAM) et le Guide de l'utilisateur IAM. Vous pouvez trouver les ressources, actions et clés de contexte de condition spécifiques aux WorkSpaces à utiliser dans les politiques d'autorisation IAM dans la page Actions, ressources et clés de condition pour Amazon WorkSpaces du 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.

> **Note**
>
> Amazon WorkSpaces ne prend pas en charge l'attribution d'informations d'identification IAM dans un WorkSpace (par exemple avec un profil d'instance).

Table des matières

- Exemples de politiques
- Spécification de ressources WorkSpaces dans une politique IAM
- Création du rôle workspaces_DefaultRole
- Création de la fonction du service AmazonWorkspaceSpacesPCAAccess
- Politiques gérées par AWS pour WorkSpaces

Exemples de politiques

Les exemples suivants illustrent des déclarations de politique que vous pouvez utiliser pour contrôler les autorisations accordées aux utilisateurs IAM sur Amazon WorkSpaces.

Example 1 : Exécution de toutes les tâches WorkSpaces

La déclaration de politique suivante accorde à un utilisateur IAM l'autorisation d'effectuer toutes les tâches WorkSpaces, y compris la création et la gestion des annuaires. Elle accorde également l'autorisation d'exécuter la procédure de configuration rapide.

Bien qu'Amazon WorkSpaces prenne totalement en charge les éléments `Action` et `Resource` lors de l'utilisation de l'API et des outils de ligne de commande, pour pouvoir utiliser Amazon WorkSpaces depuis AWS Management Console, un utilisateur IAM doit disposer des autorisations pour les actions et ressources suivantes :

- Action : `workspaces:*"` et `"ds:*"`
- Ressources : `"Resource": "*"`

L'exemple de politique suivant montre comment autoriser un utilisateur IAM à utiliser Amazon WorkSpaces depuis AWS Management Console.

```
{
  "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",
        "workdocs:RegisterDirectory",
```

```
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Example 2 : Exécution des tâches spécifiques à un espace de travail

La déclaration de politique suivante accorde à un utilisateur IAM l'autorisation d'effectuer des tâches spécifiques à WorkSpace, comme le lancement et la suppression d'instances WorkSpaces. Dans la déclaration de stratégie, l'action `ds:*` accorde de larges autorisations, avec un contrôle complet sur tous les objets des services d'annuaire dans le compte.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Pour accorder également à l'utilisateur la possibilité d'activer Amazon WorkDocs dans les instances WorkSpaces, ajoutez l'opération `workdocs` comme indiqué dans l'exemple suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

Pour accorder également aux utilisateur la possibilité d'utiliser l'assistant de lancement d'instance WorkSpace, ajoutez les opérations `kms` comme indiqué dans l'exemple suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3 : Exécution de toutes les tâches WorkSpaces pour les instances WorkSpaces BYOL

La déclaration de politique suivante accorde à un utilisateur IAM l'autorisation d'effectuer toutes les tâches WorkSpaces, y compris les tâches Amazon EC2 nécessaires à la création de WorkSpaces Apportez votre propre licence (BYOL).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "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",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Spécification de ressources WorkSpaces dans une politique IAM

Pour spécifier une ressource d'instance WorkSpace dans l'élément `Resource` de la déclaration de politique, utilisez l'Amazon Resource Name (ARN) de la ressource. Vous contrôlez l'accès aux ressources des instances WorkSpaces en octroyant ou en refusant les autorisations d'utiliser les actions d'API spécifiées dans l'élément `Action` de votre déclaration de politique IAM. WorkSpaces définit les ARN pour les instances WorkSpaces, les bundles, les groupes IP et les annuaires.

ARN d'espace de travail

La syntaxe d'un ARN WorkSpace est celle de l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

region

Région dans laquelle se trouve l'instance WorkSpace (par exemple, `us-east-1`).

account_id

ID du compte AWS, sans trait d'union (par exemple, `123456789012`).

identificateur_espace de travail

ID de l'instance WorkSpace (par exemple, `ws-a1bcd2efg`).

Voici le format de l'élément `Resource` d'une déclaration de stratégie qui identifie une instance WorkSpace spécifique.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

Vous pouvez utiliser le caractère générique * pour spécifier toutes les instances WorkSpaces qui appartiennent à un compte spécifique dans une région spécifique.

ARN d'image

La syntaxe d'un ARN d'image WorkSpace est celle de l'exemple suivant.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

region

Région dans laquelle se trouve l'image d'instance WorkSpace (par exemple, `us-east-1`).

account_id

ID du compte AWS, sans trait d'union (par exemple, `123456789012`).

bundle_identifier

ID de l'image d'instance WorkSpace (par exemple, `wsi-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_identifier"
```

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_identifier
```

region

Région dans laquelle se trouve l'instance WorkSpace (par exemple, `us-east-1`).

account_id

ID du compte AWS, sans trait d'union (par exemple, `123456789012`).

bundle_identifier

ID de bundle de l'instance WorkSpace (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_identifier"
```

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_identifier
```

region

Région dans laquelle se trouve l'instance WorkSpace (par exemple, `us-east-1`).

account_id

ID du compte AWS, sans trait d'union (par exemple, `123456789012`).

ipgroup_identifier

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_identifier"
```

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_identifier
```

region

Région dans laquelle se trouve l'instance WorkSpace (par exemple, `us-east-1`).

account_id

ID du compte AWS, sans trait d'union (par exemple, `123456789012`).

directory_identifier

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_identifier"
```

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_identifier
```

region

Région dans laquelle se trouve l'alias de connexion (par exemple,`us-east-1`).

account_id

ID du compte AWS, sans trait d'union (par exemple, `123456789012`).

connectionalias_identifier

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_identifier"
```

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 une instance de WorkSpace à l'aide de AWS Management Console, et il accorde à Amazon WorkSpaces l'autorisation d'accéder à des ressources AWS 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 l'outil AWS Management Console, puis ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
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 Attacher des stratégies d'autorisation sélectionnez les politiques gérées par AWS, AmazonWorkSpacesServiceAccess et AmazonWorkSpacesSelfServiceAccess.
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 Next: Tags (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. Dans la page Summary (Récapitulatif) du rôle workspaces_defaultRole, choisissez l'onglet Trust relationships (Relations d'approbation) .
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 Update Trust Policy (Mettre à jour la politique d'approbation).

Création de la fonction du service AmazonWorkspaceSpacesPCAAccess

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 de AWS Management Console, et il accorde à Amazon WorkSpaces l'autorisation d'accéder aux ressources AWS Private CA 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 la fonction du service AmazonWorkspaceSpacesPCAAccess à l'aide de AWS CLI

1. Créez un fichier JSON nommé `AmazonWorkSpacesPCAAccess.json` avec le texte suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Ajustez le chemin de `AmazonWorkSpacesPCAAccess.json` selon vos besoins, et exécutez les commandes AWS CLI suivantes pour créer la fonction du service et associer la politique gérée AmazonWorkspaceSpacesPCAAccess.

```
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
```

Politiques gérées par AWS pour WorkSpaces

L'utilisation de politiques gérées par AWS rend l'ajout d'autorisations à des utilisateurs, à des groupes et à des rôles plus facile que d'écrire 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. Pour démarrer rapidement, vous pouvez utiliser les politiques gérées par AWS. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre compte AWS. Pour plus d'informations sur les politiques gérées AWS, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Les services AWS assurent la maintenance et la mise à jour des politiques gérées AWS. Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS 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 très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. En revanche, ils ne suppriment pas les autorisations d'une politique gérée par AWS, ce qui fait que les mises à jour de politique n'interrompent pas vos autorisations existantes.

En outre, AWS prend en charge des politiques gérées pour des fonctions professionnelles couvrant plusieurs services. Par exemple, la politique `ReadOnlyAccess` gérée par AWS donne accès en lecture seule à l'ensemble des services et des ressources AWS. 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 Politiques gérées par AWS pour les fonctions de tâches dans le Guide de l'utilisateur IAM.

Politique gérée par AWS : AmazonWorkSpacesAdmin

Cette politique permet d'accéder aux actions d'administration Amazon WorkSpaces. Elle fournit les autorisations suivantes :

- `workspaces` : permet d'effectuer des actions d'administration sur les ressources WorkSpaces.
- `kms` : permet d'accéder à la liste et à la description des clés KMS, ainsi qu'à la liste des alias.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

Politique gérée par AWS : AmazonWorkspacePCAAccess

Cette politique gérée permet d'accéder aux ressources de l'autorité de certification privée (CA privée) AWS Certificate Manager de votre compte AWS pour une authentification par certificat. Elle est incluse dans le rôle AmazonWorkspaceSpacesPCAAccess et fournit les autorisations suivantes :

- `acm-pca` : permet d'accéder à une CA privée AWS pour gérer l'authentification par certificats.

```
{
  "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": "*"
        }
      }
    }
  ]
}
```

Politique gérée par AWS : AmazonWorkspaceSelfServiceAccess

Cette politique donne accès au service Amazon WorkSpaces pour effectuer des actions WorkSpaces en libre-service initiées par un utilisateur. Elle est incluse dans le rôle `workspaces_DefaultRole` et fournit les autorisations suivantes :

- `workspaces` : permet l'accès aux capacités de gestion des instances WorkSpaces en libre-service pour les utilisateurs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Politique gérée parAWS : AmazonWorkSpacesServiceAccess

Cette politique offre au compte client un accès au service Amazon WorkSpaces pour le lancement d'une instance WorkSpace. Elle est incluse dans le rôle `workspaces_DefaultRole` et fournit les autorisations suivantes :

- `ec2` : permet de gérer les ressources Amazon EC2 associées à une instance WorkSpace, telles que les interfaces réseau.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Mises à jour des politiques gérées par AWS sur les instances WorkSpaces

Consultez les informations concernant les mises à jour des politiques gérées par AWS pour les instances WorkSpaces depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
the section called “AmazonWorkSpacesAdmin” – Mise à jour de politique	WorkSpaces a ajouté l'action `workspaces:RestoreWorkspace` à la politique gérée Amazon WorkSpacesAdmin, en accordant aux administrateurs l'accès pour restaurer les instances WorkSpaces.	25 juin 2023

Modification	Description	Date
the section called "AmazonWorkspacesPCAAccess" - Ajout d'une nouvelle politique	WorkSpaces a ajouté une nouvelle politique gérée pour accorder l'autorisation `acm-pca` de gérer une CA privée AWS afin de gérer l'authentification par certificat.	18 novembre 2022
Début du suivi des modifications par WorkSpaces	WorkSpaces a commencé à suivre les modifications apportées aux politiques gérées WorkSpaces.	1er mars 2021

Validation de conformité pour Amazon WorkSpaces

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon WorkSpaces dans le cadre de plusieurs programmes de conformité AWS. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour obtenir une liste des services AWS concernés par des programmes de conformité spécifiques, consultez Services AWS concernés par le programme de conformité. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports d'audit externes avec AWS Artifact. Pour plus d'informations, consultez Téléchargement de rapports dans AWS Artifact.

Pour plus d'informations sur WorkSpaces et FedRAMP, consultez Configuration d'Amazon WorkSpaces pour l'autorisation FedRAMP ou la conformité SRG pour le Département de la Défense (DoD) des États-Unis.

Quand vous utilisez WorkSpaces, votre responsabilité en matière de conformité est déterminée par la sensibilité de vos données, les objectifs de conformité de votre société, ainsi que par la législation et la réglementation en vigueur. AWS fournit les ressources suivantes pour faciliter le respect de la conformité :

- Guides de démarrage rapide concernant la sécurité et la conformité: ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de référence axés sur la sécurité et la conformité sur AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services : ce livre blanc (en anglais) décrit comment les entreprises peuvent utiliser AWS pour créer des applications HIPAA conformes.
- Ressources de conformité AWS : cet ensemble de manuels et de guides peut s'appliquer à votre secteur et à votre emplacement.
- Evaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : le service AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce service AWS fournit une vue complète de l'état de la sécurité au sein d'AWS, ce qui vous permet de vérifier votre conformité aux normes et aux bonnes pratiques de sécurité du secteur.

Résilience dans Amazon WorkSpaces

L'infrastructure mondiale d'AWS repose sur les régions et les zones de disponibilité AWS. 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 les régions et les zones de disponibilité AWS, consultez AWS Infrastructure mondiale.

Amazon WorkSpaces propose également une fonctionnalité de redirection entre régions, qui fonctionne avec les stratégies de routage de basculement de votre système de nom de domaine (DNS) afin de rediriger les utilisateurs vers d'autres WorkSpaces dans une autre région AWS lorsque leurs instances WorkSpaces principales ne sont pas disponibles. Pour plus d'informations, consultez Redirection entre régions pour Amazon WorkSpaces.

Sécurité de l'infrastructure dans Amazon WorkSpaces

En tant que service géré, Amazon WorkSpaces est protégé par la sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez les appels d'API AWS publiés pour accéder aux instances WorkSpaces via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous 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.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Isolement de réseau

Un Virtual Private Cloud (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée dans le cloud AWS. Vous pouvez déployer vos instances WorkSpaces dans un sous-réseau privé de votre VPC. Pour plus d'informations, consultez Configurer un VPC pour 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 l'accès à vos instances WorkSpaces aux périphériques de confiance dotés de certificats valides. Pour plus d'informations, consultez Restreindre WorkSpaces l'accès aux appareils fiables.

Isolation sur les hôtes physiques

Les différentes instances WorkSpaces sur un même hôte physique sont isolées les unes des autres par l'intermédiaire de l'hyperviseur. C'est comme si elles se trouvaient sur des hôtes physiques distincts. Lorsqu'une instance WorkSpace est supprimée, la mémoire qui lui est allouée est nettoyée (remise à zéro) par l'hyperviseur avant d'être allouée à une nouvelle instance WorkSpace.

Autorisation des utilisateurs professionnels

Avec WorkSpaces, les annuaires sont gérés via le serveur AWS 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 plus d'informations, consultez Gestion des annuaires pour les instances WorkSpaces.

Pour contrôler davantage l'accès à vos instances WorkSpaces, utilisez l'authentification multi-facteurs. Pour plus d'informations, consultez les informations sur la façon d'activer l'authentification multifactorielle pour les services AWS.

Effectuer des demandes d'API Amazon WorkSpaces via un point de terminaison d'interface VPC

Au lieu de vous connecter via Internet, vous pouvez vous connecter directement à des points de terminaison d'API Amazon WorkSpaces via un point de terminaison d'interface de votre cloud privé virtuel (VPC). Lorsque vous utilisez un point de terminaison d'interface VPC, la communication entre votre VPC et le point de terminaison d'API Amazon WorkSpaces est gérée entièrement au sein du réseau AWS.

> **Note**
>
> Cette fonctionnalité ne peut être utilisée que pour la connexion aux points de terminaison de l'API WorkSpaces. Pour la connexion à WorkSpaces à l'aide des clients WorkSpaces, une connexion Internet est requise, comme décrit dans Exigences relatives à l'adresse IP et au port pour WorkSpaces.

Les points de terminaison d'API Amazon WorkSpaces prennent en charge les points de terminaison d'interface Amazon Virtual Private Cloud (Amazon VPC) optimisés par AWS PrivateLink. Chaque

point de terminaison VPC est représenté par une ou plusieurs interfaces réseau (également appelées interfaces réseau Elastic, ou ENI) avec des adresses IP privées dans vos sous-réseaux VPC.

Le point de terminaison d'interface VPC connecte directement votre VPC au point de terminaison d'API Amazon WorkSpaces, sans passerelle Internet, périphérique NAT, connexion VPN ni connexion AWS Direct Connect. Les instances de votre VPC ne nécessitent pas d'adresses IP publiques pour communiquer avec le point de terminaison d'API Amazon WorkSpaces.

Vous pouvez créer un point de terminaison d'interface pour vous connecter à Amazon WorkSpaces soit avec les commandes de AWS Management Console, soit avec celle de AWS Command Line Interface (AWS CLI). Pour obtenir des instructions, consultez Création d'un point de terminaison d'interface.

Une fois que vous avez créé le point de terminaison d'un VPC, vous utiliser les exemples suivants de commandes d'interface de ligne de commande (CLI) qui emploient le paramètre `endpoint-url` pour spécifier des points de terminaison d'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 Amazon WorkSpaces que la CLI et Amazon WorkSpaces utilisent par défaut (https://api.workspaces.*Région*.amazonaws.com) constitue le point de terminaison de votre VPC.

Le point de terminaison de l'API Amazon WorkSpaces prend en charge les points de terminaison VPC dans toutes les régions AWS où Amazon VPC et Amazon WorkSpaces sont tous deux disponibles. Amazon WorkSpaces prend en charge les appels vers toutes ses API publiques à l'intérieur de votre VPC.

Pour en savoir plus sur AWS PrivateLink, veuillez consulter Documentation AWS PrivateLink. 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 afficher la liste des points de terminaison d'API Amazon WorkSpaces par région, consultez les Points de terminaison d'API WorkSpaces.

> **Note**
>
> Les points de terminaison d'API Amazon WorkSpaces avec AWS PrivateLink ne sont pas pris en charge pour les points de terminaison d'API Amazon WorkSpaces FIPS (Federal Information Processing Standard).

Création d'une stratégie de point de terminaison d'un VPC pour Amazon WorkSpaces

Vous pouvez créer une stratégie pour les points de terminaison d'un VPC Amazon pour Amazon WorkSpaces, dans laquelle vous pouvez spécifier :

- 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 Guide de l'utilisateur Amazon VPC.

> **Note**
>
> Les stratégies de point de terminaison d'un VPC ne sont pas prises en charge pour les points de terminaison Amazon WorkSpaces FIPS.

L'exemple suivant de stratégie de point de terminaison VPC spécifie que tous les utilisateurs ayant accès au point de terminaison de l'interface VPC sont autorisés à invoquer 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 :

- Invocation de points de terminaison hébergés par Amazon WorkSpaces autres que `ws-f9abcdefg`.
- Exécution d'une action sur une ressource autre que celle spécifiée (ID WorkSpace : `ws-f9abcdefg`).

> **Note**
>
> Dans cet exemple, les utilisateurs peuvent encore entreprendre d'autres actions d'API Amazon WorkSpaces depuis l'extérieur du VPC. Pour restreindre les appels d'API à ceux provenant du VPC, consultez Gestion des identités et des accès pour WorkSpaces pour plus d'informations sur l'utilisation de stratégies basées sur l'identité afin de contrôler l'accès aux points de terminaison d'API Amazon WorkSpaces.

Connexion de votre réseau privé à votre VPC

Pour appeler l'API Amazon WorkSpaces via votre VPC, vous devez vous connecter depuis une instance située dans le VPC, ou connecter votre réseau privé à votre VPC à l'aide de AWS Virtual Private Network (AWS VPN) ou de AWS Direct Connect. Pour plus d'informations consultez Connexions VPN dans le Guide de l'utilisateur Amazon Virtual Private Cloud. Pour obtenir des informations sur AWS Direct Connect, consultez Création d'une connexion dans le Guide de l'utilisateur AWS Direct Connect.

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 plus d’informations, consultez Maintenance des instances WorkSpaces.

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.

Résoudre les problèmes 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 PCoIP
- 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 fournisseur de services Internet 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. »
- Mes utilisateurs du client plume PCoIP reçoivent l'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 plume PCoIP
- 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 fédérent 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 basée sur des certificats et sont invités à saisir le mot de passe soit sur le WorkSpaces client, soit 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

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 PCoIP

Pour remplacer le shell par défaut pour Linux WorkSpaces, consultezRemplacer 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 PCoIP.

Si vous utilisez une version non prise en charge de l'agent PCoIP, 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 jour votre agent PCoIP avec la dernière version

1. Ouvrez la WorkSpaces console à l'adresse https://console.aws.amazon.com/workspaces/.
2. Dans le volet de navigation, choisissez 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 à`AVAILABLE`. Pour plus d'informations sur le mode `ADMIN_MAINTENANCE`, consultez Maintenance manuelle.

Pour modifier le statut d'un WorkSpace en`ADMIN_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 plus d'informations, consultez Activez les connexions SSH pour votre Linux WorkSpaces.
6. Pour mettre à jour l'agent PCoIP, 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` inStep 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 PCoIP, contactez le Support AWS .

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 affecter automatiquement des adresses IPv6 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. A la place, désactivez ce paramètre et spécifiez les adresses IPv6 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 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.

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 PCoIP. Vérifiez les éléments suivants :

- Ce message s'affiche si le service PCoIP 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 PCoIP 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 : *Nom de domaine*\Ordinateurs de domaine

  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 : *Nom de domaine*\Utilisateurs de 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 Amazon WorkSpaces Web Access.

> **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 (WSP). 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 des groupes de contrôle d'accès IP sont configurés WorkSpace dans l'annuaire, mais que 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.

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 fournisseur de services Internet 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 utiliser le protocole de WorkSpaces streaming (WSP), 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 autorité de certification racine de confiance sur les systèmes d'exploitation 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

- Clients plume PCoIP – 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
- Clients plume PCoIP
- 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/ us-iso-eastus-isob-east 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. Ouvrez 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 aux CA racine approuvées pour le domaine à l'aide d'une stratégie de groupe. Pour plus d'informations, consultez Use Policy to Distribute Certificates.

Clients plume PCoIP

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.

Mes utilisateurs du client plume PCoIP reçoivent l'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 plume PCoIP peuvent voir s'afficher des erreurs d'échec du certificat. Pour configurer NTP, consultez Configuration du client plume PCoIP pour les instances WorkSpaces.

Les imprimantes USB et autres périphériques USB ne fonctionnent pas pour les clients plume PCoIP

À partir de la version 20.10.4 de l'agent PCoIP, 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 périphériques PCoIP zéro client pour se connecter à leur. WorkSpaces

Si vous WorkSpaces utilisez la version 20.10.4 ou ultérieure de l'agent PCoIP, les périphériques USB ne fonctionneront pas avec les périphériques clients PCoIP 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 client plume PCoIP

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 \ PCoIP \ pcoip_admin

   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 \ PCoIP \ pcoip_admin_defaults

   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 plus d'informations, consultez Configuration d'Android pour les Chromebooks.

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 WorkSpaces.

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 WorkSpaces.

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 WorkSpaces groupe 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), Policies (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 plus d'informations, consultez Fournissez un accès à Internet depuis votre WorkSpace.

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. WorkSpace Une fois qu'une adresse IP élastique a été attribuée à un WorkSpace, celui-ci WorkSpace conserve la même adresse IP publique (sauf si elle WorkSpace 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 d'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 les WorkSpace 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 n'est pas en bon état WorkSpace, 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 Reconstruisez-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 PCoIP 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` 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 protocole de WorkSpaces streaming (WSP). Ils ne s'appliquent qu'à ceux WorkSpaces qui sont configurés pour PCoIP.
> - 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 comportera 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 (ENI) 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.

Seconde	Nombre de demandes envoyées	Nombre net de demandes autorisé	Détails
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 disponibl e pendant la seconde 6 en raison de la limite de débit constant de deux appels par seconde.
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 fédérent 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 SAm AccountName de l'utilisateur Active Directory. En outre, l'élément Attribute dont l'`PrincipalTag:Email`attribut 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 basée sur des certificats et sont invités à saisir le mot de passe soit sur le WorkSpaces client, soit 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 basée sur des certificats est prise en charge par les packs Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) 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 Private CA le certificat ou AWS Private CA n'a pas émis le certificat. Vérifiez AWS CloudTrail pour déterminer si un certificat a été émis. Pour plus d'informations, consultez 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 Prérequis.

- Le certificat n'est pas fiable. Pour plus d'informations, reportez-vous à l'étape 7, « Publier l'autorité de certification dans Active Directory » dansPrérequis. 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 AWS Support pour vider le cache avant l'expiration du certificat (24 heures). Pour plus d'informations, consultez le Centre AWS 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 de la rubrique Prérequis.
- 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 Prérequis.
- Pour vérifier s'il existe des autorités de certification obsolètes dans le domaine ou la forêt, exécutez `PKIVIEW.msc` l'autorité de certification pour vérifier. S'il existe des CA périmés, 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' WorkSpaces instance. 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 AWS Support. Pour plus d'informations, consultez le Centre AWS 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, consultez Créer avec des VPC dans le même compte et dans des régions différentes.

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 que vous WorkSpaces êtes en mesure d'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.

Politique de fin de vie des applications client Amazon WorkSpaces

La politique de fin de vie (EOL) d'Amazon WorkSpaces s'applique à certaines versions majeures (et à toutes leurs versions mineures) du client Amazon WorkSpaces qui ne sont plus prises en charge et dont la compatibilité avec les versions plus récentes n'est plus testée.

Le cycle de vie d'une version du client WorkSpaces comporte trois phases : prise en charge générale, conseils techniques et fin de vie (EOL). La phase de prise en charge générale commence à la date de sortie publique initiale d'un client WorkSpaces et dure pendant une période déterminée. Pendant la phase de prise en charge générale, l'équipe du support WorkSpaces 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 client WorkSpaces.

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 client WorkSpaces. Elles ne sont pas implémentées pour les anciennes versions. Au cours de la phase d'assistance technique, si un correctif est nécessaire, AWS planifie ce correctif pour la prochaine version accessible au public, et vous pourrez passer à la dernière version de WorkSpaces 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 ni maintenance n'est fournie. AWS arrête de tester les problèmes de compatibilité. Pour bénéficier d'une assistance continue, vous devez effectuer une mise à niveau vers la dernière version du client WorkSpaces.

Consultez ce tableau pour plus d'informations sur la prise en charge de versions spécifiques.

Client Windows	Prise en charge générale	Conseils techniques	Fin de vie
2.x	2018	31 mars 2023	31 août 2023

Client Linux	Prise en charge générale	Conseils techniques	Fin de vie
4.x pour Ubuntu 18.04	12 août 2021	31 mars 2023	31 août 2023
3.x pour Ubuntu 18.04	25 novembre 2019	31 mars 2023	31 août 2023

Client macOS	Prise en charge générale	Conseils techniques	Fin de vie
2.x	2019	31 mars 2023	31 août 2023
1.x	2018	31 mars 2023	31 août 2023

Client iPad	Prise en charge générale	Conseils techniques	Fin de vie
1.x	2018	31 mars 2023	31 août 2023

Client Android	Prise en charge générale	Conseils techniques	Fin de vie
2.x	2019	31 mars 2023	31 août 2023
1.x	2018	31 mars 2023	31 août 2023

Web Access	Prise en charge générale		
Google Chrome	Version actuelle, plus les deux versions principales les plus récentes		

Web Access	Prise en charge générale				
Firefox	Version actuelle, plus les deux versions principales les plus récentes				
Microsoft Edge	Version actuelle, plus les deux versions principales les plus récentes				

Clients non pris en charge

Les clients WorkSpaces suivants ne sont pas pris en charge.

Système d'exploitation	Version du client	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
Windows	5.11	3 juillet 2023	1er octobre 202	1er octobre 202	Non pris en charge en raison de problèmes de qualité
Windows	5.10	19 juin 2023	1er octobre 202	1er octobre 202	Non pris en charge en raison de problèmes de qualité
Windows	5.9	9 mai 2023	1er octobre 202	1er octobre 202	Non pris en charge en raison de

Système d'exploitation	Version du client	Prise en charge générale	Conseils techniques	Fin de vie	Remarques
					problèmes de qualité

Question fréquentes concernant la fin de vie (EOL)

J'utilise une version d'un client WorkSpaces qui a atteint sa fin de vie. Que dois-je faire pour passer à une version prise en charge ?

Accédez à la page de téléchargement du client WorkSpaces pour télécharger et installer une version entièrement compatible de WorkSpaces.

Puis-je utiliser une version du client WorkSpaces qui a atteint sa fin de vie avec un client WorkSpace compatible ?

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 de client qui a atteint sa fin de vie, contactez l'équipe d'assistance AWS pour plus d'informations.

J'utilise une version d'un client WorkSpaces qui a atteint sa fin de vie. 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 de client WorkSpaces compatible 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 fournit pas de support pour les clients

WorkSpaces qui utilisent des systèmes d'exploitation ayant atteint leur date de fin de vie. Utilisez un système d'exploitation pris en charge pour être sûr de bénéficier d'une assistance concernant vos clients WorkSpaces.

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
WorkSpaces	1	Le nombre maximum de personnes WorkSpaces présentes sur ce compte dans la région actuelle.	Oui
Graphismes WorkSpaces	0	Le nombre maximum de graphiques WorkSpaces dans ce compte dans la région actuelle. **Note** Le bundle Graphics ne sera plus pris	Oui

Ressource	Par défaut	Description	Ajustable
		en charge après le 30 novembre 2023. Nous vous recommandons de migrer votre offre groupée WorkSpaces vers Graphics.G4DN. Pour plus d'informations, consultez Migrer un WorkSpace.	
Carte graphique. G4DN WorkSpaces	0	Le nombre maximum de Graphics.G4DN WorkSpaces dans ce compte dans la région actuelle.	Oui
GraphicsPro WorkSpaces	0	Le nombre maximum de personnes GraphicsPro WorkSpaces présentes sur ce compte dans la région actuelle.	Oui

Ressource	Par défaut	Description	Ajustable
GraphicsPro.g4dn WorkSpaces	0	Le nombre maximum de GraphicsPro .g4dn WorkSpaces dans ce compte dans la région actuelle.	Oui
Veille WorkSpaces	0	Le nombre maximum de personnes WorkSpaces présentes sur ce compte dans la région actuelle.	Oui
Bundles	50	Nombre maximal de bundles pour ce compte dans la région actuelle. Ce quota s'appliqu e uniquement aux bundles personnal isés, et non aux bundles publics.	Non
Alias de connexion	20	Nombre maximal d'alias de connexion pour ce compte dans la région actuelle.	Non

Ressource	Par défaut	Description	Ajustable
Annuaires	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
Images	40	Nombre maximal d'images pour ce compte dans la région actuelle.	Oui
Groupes de contrôles d'accès IP	100	Nombre maximal de contrôles d'accès IP pour ce compte dans la région actuelle.	Non
Groupes de contrôle d'accès IP par annuaire	25	Nombre maximal de groupes de contrôle d'accès IP par annuaire pour ce compte dans la région actuelle.	Non
Règles par groupe de contrôle d'accès IP	10	Nombre maximal de règles par groupe de contrôle d'accès IP pour ce compte dans la région actuelle.	Non

Limitation d'API

Le débit autorisé est de deux appels par seconde. Pour plus d'informations sur les quotas de limitation, consultez Erreurs ThrottlingException.

WorkSpaces Versions de l'agent hôte du protocole de streaming (WSP)

L'agent hôte du protocole de WorkSpaces streaming (WSP) 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 protocole de WorkSpaces streaming (WSP), 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 WSP. L'agent hôte WSP est également mis à jour automatiquement pendant la période 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 ci-après décrit les modifications apportées à chaque version de l'agent hôte WSP.

Version	Date	Modifications
• 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 améliorat ions de performances
• Windows WorkSpaces - 2.0.0.1425	22 février 2024	• Ajout de la prise en charge des demandes de WebAuthn redirecti on 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

Version	Date	Modifications
		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 améliorat ions 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.
• 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 améliorat ions de performances

Version	Date	Modifications
• Windows WorkSpaces - 2.0.0.1164	13 octobre 2023	• Ajout de la prise en charge de VSync dans 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 améliorat ions de performances
• 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 reconnexions plus rapides après une interruption • Correctifs de bogues et améliorat ions de performances

Version	Date	Modifications
• 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
• 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 synchronisation A/V et aux claviers japonais • Amélioration de la fiabilité du programme d'installation WSP

Version	Date	Modifications
• 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 l'agent hôte, consultez Quel client et quels systèmes d'opération hôtes sont supportés par la version la plus récente de WSP ?.
- Pour plus d'informations sur la mise à jour de la version de votre agent hôte, consultez Si j'ai déjà un fournisseur de services WorkSpace Internet, comment le mettre à jour ? .

- Pour les notes de mise à jour de la version du client macOS de WSP, consultez les notes de mise à jour 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 de WSP, consultez les notes de version dans la section du Guide de l' WorkSpaces utilisateur consacrée aux applications clientes WorkSpaces Windows.

Prise en charge de l'extension du kit SDK par WSP

Le protocole de streaming Amazon WorkSpaces (WSP) repose sur la technologie NICE DCV, qui offre un accès à distance haute performance aux instances WorkSpaces pour un large éventail de charges de travail et de cas d'utilisation. Grâce au kit SDK d'extension NICE DCV, les développeurs peuvent personnaliser l'expérience WorkSpaces WSP pour les utilisateurs finaux, y compris :

- 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, consultez la documentation du kit SDK d'extension NICE DCV (langue française non garantie). Vous pouvez trouver le kit SDK lui-même dans le référentiel GitHub du SDK d'extension NICE DCV. En outre, vous pouvez également trouver des exemples d'intégration du kit SDK dans le référentiel GitHub d'exemples de kit SDK d'extension NICE DCV.

Les éléments suivants sont pris en charge par les instances WorkSpaces.

- Protocole de streaming : WSP (WorkSpaces Streaming Protocol)
- Client WorkSpaces Windows : Windows 5.9.0.4110 et versions ultérieures

> **Note**
>
> Les clients WorkSpaces Android, iOS et Web Access ne prennent pas en charge le kit SDK d'extension NICE DCV.

- WorkSpaces pris en charge : serveurs Windows, Linux et Ubuntu

Historique de la documentation WorkSpaces

Le tableau suivant décrit les modifications importantes apportées au service WorkSpaces et au Guide d'administration Amazon WorkSpaces depuis le 1er janvier 2018. Nous mettons aussi la documentation à jour régulièrement pour prendre en compte les commentaires qui nous sont envoyés.

Pour recevoir des notifications concernant ces mises à jour, vous pouvez vous abonner au flux RSS WorkSpaces.

Modification	Description	Date
Mise à jour de la politique gérée par AmazonWorkSpacesAdmin	WorkSpaces a ajouté l'action workspaces:RestoreWorkspace à la politique gérée Amazon WorkSpacesAdmin, en accordant aux administrateurs l'accès pour restaurer les instances WorkSpaces.	17 juillet 2023
Prise en charge de l'extension du kit SDK par WSP	Grâce au kit SDK d'extension NICE DCV, les développeurs peuvent personnaliser l'expérience WorkSpaces WSP pour les utilisateurs finaux.	25 mai 2023
Versions de l'agent hôte WSP (WorkSpaces Streaming Protocol)	Informations de version WSP (WorkSpaces Streaming Protocol).	8 mai 2023
Lancement d'Amazon WorkSpaces dans la région AWS GovCloud (US, côte est)	Amazon WorkSpaces est disponible dans la région AWS GovCloud (US, côte est).	3 mai 2023
Prise en charge des webcams par Amazon WorkSpaces	Amazon WorkSpaces prend désormais en charge l'audio/vidéo (AV) en temps réel en	5 avril 2021

	redirigeant de façon fluide l'entrée vidéo de la webcam locale vers les bureaux WorkSpaces Windows via WSP (WorkSpaces Streaming Protocol).	
Prise en charge des cartes à puce par Amazon WorkSpaces avec l'application client WorkSpaces macOS	Vous pouvez désormais utiliser l'application client Amazon WorkSpaces macOS avec les cartes à puce CAC (Common Access Card) et PIV (Personal Identity Verification). La prise en charge des cartes à puce est disponible sur les instances WorkSpaces via WSP (WorkSpaces Streaming Protocol).	5 avril 2021
API de gestion des offres groupées Amazon WorkSpaces	Des API de gestion des offres groupées Amazon WorkSpaces sont maintenant disponibles. Ces actions d'API prennent en charge les opérations de création, de suppression et d'association d'images pour les offres groupées WorkSpaces.	15 mars 2021
Lancement d'Amazon WorkSpaces dans la région Asie-Pacifique (Mumbai)	Amazon WorkSpaces est disponible dans la Région Asie-Pacifique (Mumbai).	8 mars 2021

Protocole de streaming WorkSpaces (WSP)	WSP (WorkSpaces Streaming Protocol) est désormais disponible pour les instances WorkSpaces sous licence (Windows Server 2016) et basées sur Windows 10 BYOL dans tous les types d'offres groupées, à l'exception de Graphics et GraphicsPro. WSP est également disponible pour les instances WorkSpaces Linux dans la région AWS GovCloud (US, côte ouest).	1er décembre 2020
Cartes à puce	Amazon WorkSpaces prend désormais en charge l'authentification par carte à puce pré-session (connexion) et en cours de session pour les instances WorkSpaces Windows et Linux dans la région AWS GovCloud (US, côte ouest).	1er décembre 2020
Partage d'images personnalisées	Vous pouvez partager des images d'instances WorkSpaces personnalisées entre des comptes AWS. Une fois l'image partagée, le compte destinataire peut la copier et l'utiliser pour créer des offres groupées afin de lancer de nouvelles instances WorkSpaces.	1er octobre 2020

Redirection entre régions	Vous pouvez maintenant utiliser la fonctionnalité de redirection entre régions avec vos stratégies de routage DNS (Domain Name System) pour rediriger les utilisate urs vers d'autres espaces de travail lorsque leurs instances WorkSpaces principales ne sont pas disponibles.	10 septembre 2020
Abonnement à Microsoft Office 2016 ou 2019 pour les instances WorkSpaces BYOL	Vous pouvez désormais vous abonner à Microsoft Office Professionnel 2016 ou 2019 fourni par AWS dans les instances WorkSpace s Windows Apportez votre propre licence (BYOL).	3 septembre 2020
Automatisation BYOL dans la région Chine (Ningxia)	Vous pouvez exploiter les fonctionnalités d'automat isation Apportez votre propre licence (BYOL) afin de simplifier le processus d'utilisation des licences de bureau Windows 10 pour vos instances WorkSpaces dans la région Chine (Ningxia).	2 avril 2020

Vérificateur d'image	L'outil Vérificateur d'image vous aide à déterminer si votre instance WorkSpace Windows répond aux exigences de création d'image. L'outil de vérification d'image effectue une série de tests sur l'instanc e WorkSpace que vous souhaitez utiliser pour créer votre image et fournit des conseils sur la façon de résoudre les problèmes détectés.	30 mars 2020
Migration d'instances WorkSpaces	La fonctionnalité de migration Amazon WorkSpaces vous permet de migrer une instance WorkSpace d'un groupe à un autre, tout en conservant les données sur le volume utilisate ur. Vous pouvez utiliser cette fonctionnalité pour migrer des instances WorkSpace s de l'expérience de bureau Windows 7 vers l'expérie nce de bureau Windows 10. Vous pouvez également utiliser cette fonctionnalité pour migrer des instances WorkSpaces d'un groupe public ou personnalisé vers un autre.	9 janvier 2020

Intégration de PrivateLink pour les API Amazon WorkSpaces	Au lieu de vous connecter via Internet, vous pouvez vous connecter directement à des points de terminaison d'API Amazon WorkSpaces via un point de terminaison d'interface de votre cloud privé virtuel (VPC). Lorsque vous utilisez un point de terminaison d'interface VPC, la communication entre votre VPC et le point de terminaison d'API Amazon WorkSpaces est gérée entièrement au sein du réseau AWS.	25 novembre 2019
Client Linux pour Amazon WorkSpaces	Les utilisateurs peuvent désormais utiliser le client Linux pour accéder à leurs espaces de travail.	25 novembre 2019
Lancement d'Amazon WorkSpaces dans la région Chine (Ningxia)	Amazon WorkSpaces est disponible dans la région Chine (Ningxia).	13 novembre 2019
Restauration des instances WorkSpaces à leur dernier état sain connu	Vous pouvez utiliser la fonctionnalité de restauration pour restaurer une instance WorkSpace à son dernier état sain connu.	18 septembre 2019

Chiffrement de points de terminaison FIPS	Pour être en conformité avec le Federal Risk and Authorization Management Program (FedRAMP) ou avec le Cloud Computing Security Requirements Guide (SRG) du Département de la Défense des États-Unis (DoD), vous devez configurer Amazon WorkSpaces pour utiliser le chiffrement des points de terminaison FIPS (Federal Information Processing Standards) au niveau de l'annuaire.	12 septembre 2019
Copie d'images d'instances WorkSpaces	Vous pouvez copier vos images dans la même région ou d'une région à une autre.	le 27 juin 2019
Capacités de gestion d'instances WorkSpaces en libre-service pour les utilisateurs	Vous pouvez activer différentes capacités de gestion d'instances WorkSpaces en libre-service. Les utilisateurs bénéficient ainsi d'un plus grand contrôle sur leur expérience.	19 novembre 2018
Automatisation BYOL	Vous pouvez exploiter les fonctionnalités d'automatisation BYOL (Réutilisez vos licences) afin de simplifier le processus d'utilisation des licences de bureau Windows 7 pour vos instances WorkSpaces.	16 novembre 2018

Bundles PowerPro et GraphicsPro	Les offres groupées PowerPro et GraphicsPro sont désormais disponibles pour les instances WorkSpaces.	le 18 octobre 2018
Surveillance des connexions réussies aux instances WorkSpaces	Vous pouvez utiliser des événements d'Amazon CloudWatch Events pour surveiller les connexions WorkSpace réussies et y répondre.	17 septembre 2018
Accès web pour les instances WorkSpaces Windows 10	Les utilisateurs peuvent désormais utiliser le client Web Access pour accéder à une instance WorkSpace exécutant l'expérience de bureau Windows 10.	24 août 2018
Connexion par URI	Vous pouvez utiliser les URI (Uniform Resource Identifier) pour fournir aux utilisateurs l'accès à leurs instances WorkSpaces.	31 juillet 2018
Instances WorkSpaces Amazon Linux	Vous pouvez allouer des instances WorkSpaces Amazon Linux aux 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 instances WorkSpaces.	30 avril 2018

Mises à niveau sur place	Vous pouvez mettre à niveau vos instances WorkSpaces Windows 10 BYOL vers une version plus récente de Windows 10.	9 mars 2018

Mises à jour antérieures

Le tableau suivant décrit les ajouts importants apportés au service Amazon WorkSpaces et à sa documentation avant le 1er janvier 2018.

Modification	Description	Date
Options de calcul flexibles	Vous pouvez faire basculer vos instances WorkSpaces entre les bundles Value, Standard, Performance et Power	22 décembre 2017
Stockage configurable	Vous pouvez configurer la taille des volumes racine et utilisateur pour vos instances WorkSpaces lorsque vous les lancez et augmenter la taille de ces volumes par la suite.	22 décembre 2017
Contrôle de l'accès aux appareils	Vous pouvez spécifier les types d'appareils ayant accès aux instances WorkSpaces. De plus, vous pouvez restreindre l'accès aux instances WorkSpaces aux appareils approuvés (plus connus sous le nom d'appareils gérés).	le 19 juin 2017
Approbations entre forêts	Vous pouvez établir une relation d'approbation entre votre annuaire AWS Managed Microsoft AD et votre domaine Microsoft Active Directory sur site, puis allouer des instances WorkSpaces aux utilisateurs du domaine sur site.	9 février 2017
Offres Windows Server 2016	WorkSpaces propose des offres groupées alimentées par Windows Server 2016,	29 novembre 2016

Modification	Description	Date
	qui incluent un environnement de bureau Windows 10.	
Web Access	Vous pouvez accéder à vos instances WorkSpaces Windows à partir d'un navigateur Web avec WorkSpaces Web Access.	le 18 novembre 2016
Instances WorkSpaces à l'heure	Vous pouvez configurer vos espaces de travail pour que les utilisateurs soient facturés à l'heure.	le 18 août 2016
Windows 10 BYOL	Vous pouvez réutiliser vos licences de bureau Windows 10 sur vos instances WorkSpaces (BYOL).	21 juillet 2016
Prise en charge du balisage	Vous pouvez utiliser des balises pour gérer et suivre vos instances WorkSpaces.	17 mai 2016
Enregistrements sauvegardés	Chaque fois que vous entrez un nouveau code d'enregistrement, le client WorkSpaces le stocke. Vous pouvez ainsi plus facilement basculer entre des instances WorkSpaces de différents annuaires ou régions.	28 janvier 2016
Windows 7 BYOL, client Chromebook, chiffrement d'instance WorkSpace	Vous pouvez utiliser votre licence de bureau Windows 7 dans vos instances WorkSpace s (BYOL), utiliser le client Chromebook et le chiffrement d'instance WorkSpace.	1 octobre 2015
Surveillance Amazon CloudWatch	Ajout d'informations sur la surveillance CloudWatch	28 avril 2015
Reconnexion de session automatique	Ajout d'informations sur la fonctionnalité de reconnexion de session automatique dans les applications client de bureau WorkSpaces.	31 mars 2015

Modification	Description	Date
Adresses IP publiques	Vous pouvez automatiquement attribuer une adresse IP publique à vos instances WorkSpaces.	23 janvier 2015
Lancement de WorkSpaces dans la région Asie-Pacifique (Singapour)	Amazon 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 instance WorkSpace personnalisée et une offre d'instance WorkSpace personnalisée à partir de l'image.	28 octobre 2014
Prise en charge du client PCoIP Zero	Vous pouvez accéder à des appareils client plume WorkSpaces PCoIP.	15 octobre 2014
Lancement de WorkSpaces dans la région Asie-Pacifique (Tokyo)	Amazon WorkSpaces est disponible dans la région Asie-Pacifique (Tokyo).	26 août 2014
Prise en charge d'une imprimante locale	Vous pouvez activer la prise en charge d'une imprimante locale pour votre instance WorkSpaces.	26 août 2014
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 d'organisation (OU) dans laquelle sont placés vos comptes de machine WorkSpace et un domaine distinct dans lequel vos comptes de machine WorkSpace sont créés.	le 7 juillet 2014

Modification	Description	Date
Ajout de groupes de sécurité	Vous pouvez ajouter un groupe de sécurité à vos instances WorkSpaces.	le 7 juillet 2014
Lancement de WorkSpaces dans la région Asie-Pacifique (Sydney)	Amazon WorkSpaces est disponible dans la région Asie-Pacifique (Sydney).	15 mai 2014
Lancement de WorkSpaces dans la région Europe (Irlande)	Amazon WorkSpaces est disponible dans la région Europe (Irlande).	5 mai 2014
Version bêta publique	Amazon WorkSpaces est disponible dans une 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.