AWS Livre blanc

Bonnes pratiques pour le déploiement WorkSpaces

Bonnes pratiques pour le déploiement WorkSpaces: AWS Livre blanc

Table of Contents

Résumé et introduction i
Résumé 1
Introduction 1
WorkSpaces exigences 3
Considérations relatives au réseau 4
Conception en VPC 5
Interfaces réseau 6
Flux de trafic 6
Appareil client pour WorkSpace 7
Amazon WorkSpaces Service vers VPC 9
Exemple de configuration typique 14
AWS Service de répertoire 18
Scénarios de déploiement d'AD DS 20
Rôle de l' AWS AD Connector avec WorkSpaces 21
L'importance de votre lien réseau AWS avec un Active Directory sur site 22
Utilisation de l'authentification multifactorielle avec WorkSpaces 23
Séparer le compte du domaine de ressources 23
Déploiements Active Directory de grande envergure 23
Utilisation de Microsoft Azure Active Directory ou des services de domaine Active Directory avec WorkSpaces 24
Dimensionnement de l'AD Connector avec WorkSpaces 24
Dimensionnement de AWS Managed Microsoft AD 25
Scénario 1 : utilisation du connecteur AD pour l'authentification par proxy auprès du service Active Directory local 25
AWS 27
Client 27
Scénario 2 : extension des services AD DS locaux à AWS (réplique) 28
AWS 30
Client 30
Scénario 3 : déploiement isolé autonome à l'aide du AWS Directory Service dans le cloud AWS 31
AWS 33
Client 33

Scénario 4 : AWS Microsoft AD et une confiance transitive bidirectionnelle vers les environnements locaux 34
AWS 35
Client 35
Scénario 5 : AWS Microsoft AD utilisant un Virtual Private Cloud (VPC) à services partagés 36
AWS 36
Client 37
Scénario 6 : AWS Microsoft AD, VPC à services partagés et confiance unidirectionnelle sur site 37
AWS 39
Client 40
Utilisation d'Active Directory AWS géré par plusieurs régions avec Amazon WorkSpaces 40
Architecture 41
Mise en œuvre 41
Considérations relatives à la conception 42
Conception en VPC 42
Conception de VPC : DHCP et DNS 45
Active Directory : sites et services 46
Protocole 47
Multi-Factor Authentication (MFA) 49
MFA — Authentification à deux facteurs 49
Reprise après sinistre/Continuité des activités 51
WorkSpaces Redirection entre régions 51
WorkSpaces Interface VPC Endpoint (AWS PrivateLink) — Appels d'API 54
Prise en charge des cartes à puce 55
Root CA 56
En cours de session 56
Avant la session 57
Déploiement du client 59
Sélection d'un point de WorkSpaces terminaison Amazon 61
Choisir un point de terminaison pour votre WorkSpaces 61
Client d'accès Web 63
WorkSpaces Balises Amazon 65
Gestion des balises 66
Quotas WorkSpaces de service Amazon 66
Automatiser le déploiement d'Amazon WorkSpaces 67

Méthodes WorkSpaces d'automatisation courantes 67
AWS CLI et API 67
AWS CloudFormation 67
Portail en libre-service WorkSpaces 68
Intégration à la gestion des services informatiques d'entreprise 68
WorkSpaces Bonnes pratiques en matière d'automatisation du déploiement 69
Correctifs WorkSpaces et mises à niveau sur place d'Amazon 69
WorkSpace entretien 70
Amazon Linux WorkSpaces 71
Conditions préalables et considérations relatives à l'application de correctifs pour Linux 71
Application de correctifs pour Amazon Windows 71
Mise à niveau sur place d'Amazon Windows 71
Conditions préalables à la mise à niveau sur place de Windows 72
Considérations relatives à la mise à niveau sur place de 72
Packs WorkSpaces de langue Amazon 73
Gestion des WorkSpaces profils Amazon 73
Redirection de dossiers 73
Bonnes pratiques 74
Chose à éviter 75
Autres considérations 75
Paramètres du profil 75
Politiques de groupe 75
WorkSpaces Volumes Amazon 76
WorkSpaces Journalisation Amazon 77
Conteneurs et sous-système Windows pour Linux sur Amazon WorkSpaces 79
Conteneurs et Amazon WorkSpaces 79
Sous-système Windows pour Linux 79
Amazon WorkSpaces Migrate 80
Framework Well-Architected 83
Excellence opérationnelle 83
Sécurité 83
Fiabilité 84
Optimisation des coûts 84
Sécurité 85
Chiffrement en transit 85
Inscription et mises à jour 85

Étape d'authentification 85
Authentification — Connecteur Active Directory (ADC) 86
Étape de courtier 86
Étape de diffusion 86
Interfaces réseau 87
Interface réseau de gestion 87
WorkSpaces groupes de sécurité 88
Groupes de sécurité ENI 89
Listes de contrôle d'accès réseau (ACL) 90
AWS Network Firewall 90
Scénarios de conception 91
Chiffré WorkSpaces 93
Qu'est-ce qui est chiffré ? 93
Quand le chiffrement a-t-il lieu ? 93
Comment est WorkSpace crypté un nouveau produit ? 94
Options de contrôle d'accès et appareils fiables 95
Groupes de contrôle d'accès IP 96
Surveillance ou journalisation à l'aide d'Amazon CloudWatch 96
CloudWatch Métriques Amazon pour WorkSpaces 97
Amazon CloudWatch Events pour WorkSpaces 98
YubiKey support pour Amazon WorkSpaces 99
Optimisation des coûts 84
Fonctionnalités de WorkSpace gestion en libre-service 102
Amazon WorkSpaces Cost Optimizer 103
Se désinscrire à l'aide de tags 104
Opter pour les régions 104
Déploiement dans un VPC existant 104
Résiliation de la période non utilisée WorkSpaces 104
Optimisation d'Amazon Connect pour Amazon WorkSpaces 105
Résolution des problèmes 107
AD Connector ne peut pas se connecter à Active Directory 107
Résolution des problèmes Une erreur de création d'image WorkSpace personnalisée 108
Résolution des problèmes liés à un système Windows WorkSpace marqué comme défectueux 109
Vérifier l'utilisation du processeur 109
Vérifiez le nom d'ordinateur du WorkSpace 110

Vérifiez les règles du pare-feu 110
Collecte d'un ensemble de journaux de WorkSpaces support pour le débogage 111
Journaux côté serveur du WSP 111
Journaux côté serveur PCoIP 112
WebAccess journaux côté serveur 113
Journaux côté client 113
Collecte automatisée de paquets de journaux côté serveur pour Windows 114
Comment vérifier la latence par rapport à la AWS région la plus proche 115
Conclusion 116
Collaborateurs 117
Suggestions de lecture 118
Révisions du document 119
Avis 121
AWS Glossaire 122
..... cxxiii

Bonnes pratiques pour le déploiement d'Amazon WorkSpaces

Date de publication : 1 juin 2022 (Révisions du document)

Résumé

Ce livre blanc présente un ensemble de bonnes pratiques pour le déploiement de. WorkSpaces Le livre blanc couvre les considérations relatives au réseau, aux services d'annuaire et à l'authentification des utilisateurs, à la sécurité, ainsi qu'à la surveillance et à la journalisation.

Ce livre blanc permet également un accès rapide aux informations pertinentes. Il est destiné aux ingénieurs réseau, aux ingénieurs d'annuaire ou aux ingénieurs de sécurité.

Introduction

Amazon WorkSpaces est un service informatique de bureau géré dans le cloud. Amazon WorkSpaces élimine le fardeau lié à l'achat ou au déploiement de matériel ou à l'installation de logiciels complexes, et fournit une expérience de bureau en quelques clics AWS Management Console, en utilisant l'interface de ligne de commande (CLIAWS) d'Amazon Web Services () ou en utilisant l'interface de programmation d'applications (API). Avec Amazon WorkSpaces, vous pouvez lancer un poste de travail Microsoft Windows ou Amazon Linux en quelques minutes, ce qui vous permet de vous connecter à votre logiciel de bureau et d'y accéder de manière sécurisée, fiable et rapide depuis votre site ou depuis un réseau externe. Vous pouvez :

- Tirez parti de votre Microsoft Active Directory (AD) existant sur site en utilisant AWS Directory Service : Active Directory Connector (AD Connector).
- Étendez votre annuaire au AWS Cloud.
- Créez un annuaire géré avec AWS Directory Service Microsoft AD ou Simple AD, pour gérer vos utilisateurs et WorkSpaces.
- Tirez parti de votre serveur RADIUS sur site ou hébergé dans le cloud avec AD Connector pour fournir une authentification multifactorielle (MFA) à votre. WorkSpaces

Vous pouvez automatiser le provisionnement d'Amazon à l'aide WorkSpaces de la CLI ou de l'API, ce qui vous permet d' WorkSpaces intégrer Amazon à vos flux de travail de provisionnement existants.

Pour des raisons de sécurité, outre le chiffrement réseau intégré fourni par le WorkSpaces service Amazon, vous pouvez également activer le chiffrement au repos pour votre WorkSpaces. Reportez-vous à la WorkSpacessection Chiffrée de ce document.

Vous pouvez déployer des applications sur votre WorkSpaces site à l'aide de vos outils locaux existants, tels que Microsoft System Center Configuration Manager (SCCM), Puppet Enterprise ou Ansible.

Les sections suivantes fournissent des informations sur Amazon WorkSpaces, expliquent le fonctionnement du service, décrivent ce dont vous avez besoin pour le lancer et vous indiquent les options et fonctionnalités que vous pouvez utiliser.

WorkSpaces exigences

Le WorkSpaces service Amazon nécessite trois composants pour réussir son déploiement :

- WorkSpaces application client — Un appareil client WorkSpaces compatible avec Amazon. Reportez-vous à Getting Started with your WorkSpace.

  Vous pouvez également utiliser les clients zéro d'ordinateur personnel sur protocole Internet (PCoIP) pour vous connecter à. WorkSpaces Pour obtenir la liste des appareils disponibles, consultez PCoIP Zero Clients pour Amazon. WorkSpaces
- Un service d'annuaire pour authentifier les utilisateurs et leur WorkSpace fournir un accès. Amazon travaille WorkSpaces actuellement avec AWS Directory Service et Microsoft AD. Vous pouvez utiliser votre serveur AD sur site avec AWS Directory Service pour prendre en charge vos informations d'identification d'utilisateur d'entreprise existantes auprès d'Amazon WorkSpaces.
- Amazon Virtual Private Cloud (Amazon VPC) sur lequel exécuter votre Amazon WorkSpaces — Vous aurez besoin d'au moins deux sous-réseaux pour un WorkSpaces déploiement Amazon, car chaque construction de AWS Directory Service nécessite deux sous-réseaux dans un déploiement multi-AZ.

Considérations relatives au réseau

Chacun WorkSpace est associé à la structure Amazon VPC et AWS Directory Service spécifique que vous avez utilisée pour le créer. Toutes les constructions de AWS Directory Service (Simple AD, AD Connector et Microsoft AD) nécessitent deux sous-réseaux pour fonctionner, chacun dans des zones de disponibilité (AZ) différentes. Les sous-réseaux sont affiliés de façon permanente à une structure de Directory Service et ne peuvent pas être modifiés une fois celle-ci créée. Pour cette raison, il est impératif de déterminer les bonnes tailles de sous-réseau avant de créer la structure des services d'annuaire. Prenez bien en compte les points suivants avant de créer les sous-réseaux :

- De combien en WorkSpaces aurez-vous besoin au fil du temps ?
- Quelle est la croissance attendue ?
- Quels types d'utilisateurs devrez-vous accueillir ?
- Combien de domaines AD allez-vous connecter ?
- Où se trouvent vos comptes d'entreprise ?

Amazon recommande de définir des groupes d'utilisateurs, ou personas, en fonction du type d'accès et de l'authentification utilisateur dont vous avez besoin dans le cadre de votre processus de planification. Les réponses à ces questions sont utiles lorsque vous devez limiter l'accès à certaines applications ou ressources. Les personas utilisateur définis peuvent vous aider à segmenter et à restreindre l'accès à l'aide de AWS Directory Service, de listes de contrôle d'accès réseau, de tables de routage et de groupes de sécurité VPC. Chaque construction de AWS Directory Service utilise deux sous-réseaux et applique les mêmes paramètres à tous ceux WorkSpaces qui sont lancés à partir de cette construction. Par exemple, vous pouvez utiliser un groupe de sécurité qui s'applique à toutes les WorkSpaces personnes connectées à un AD Connector pour spécifier si le MFA est requis ou si un utilisateur final peut disposer d'un accès administrateur local sur son WorkSpace

> **Note**
>
> Chaque AD Connector se connecte à votre Microsoft AD d'entreprise existant. Pour tirer parti de cette fonctionnalité et spécifier une unité organisationnelle (UO), vous devez créer votre Directory Service en tenant compte de vos profils d'utilisateur.

Conception en VPC

Cette section décrit les meilleures pratiques en matière de dimensionnement de votre VPC et de vos sous-réseaux, le flux de trafic et les implications pour la conception des services d'annuaire.

Voici quelques éléments à prendre en compte lors de la conception du VPC, des sous-réseaux, des groupes de sécurité, des politiques de routage et des listes de contrôle d'accès réseau (ACL) pour votre Amazon WorkSpaces afin de pouvoir créer votre WorkSpaces environnement en termes d'évolutivité, de sécurité et de facilité de gestion :

- VPC — Nous vous recommandons d'utiliser un VPC distinct spécialement pour votre déploiement. WorkSpaces Avec un VPC distinct, vous pouvez définir la gouvernance et les garde-fous de sécurité nécessaires pour votre entreprise en WorkSpaces créant une séparation du trafic.
- Services d'annuaire : chaque AWS Directory Service construction nécessite une paire de sous-réseaux fournissant un service d'annuaire hautement disponible réparti entre les AZ.
- Taille du sous-réseau : WorkSpaces les déploiements sont liés à une structure de répertoire et résident dans le même VPC que celui que vous avez choisi AWS Directory Service, mais ils peuvent se trouver dans des sous-réseaux VPC différents. Quelques considérations :
  - La taille des sous-réseaux est permanente et ne peut pas être modifiée. Vous devez laisser suffisamment de place à la croissance future.
  - Vous pouvez définir un groupe de sécurité par défaut pour votre choix AWS Directory Service. Le groupe de sécurité s'applique à tous WorkSpaces ceux qui sont associés à la AWS Directory Service construction spécifique.
  - Vous pouvez avoir plusieurs instances d' AWS Directory Service utilisation du même sous-réseau.

Pensez à vos projets futurs lors de la conception de votre VPC. Par exemple, vous souhaiterez peut-être ajouter des composants de gestion, tels qu'un serveur antivirus, un serveur de gestion des correctifs ou un serveur MFA AD ou RADIUS. Il vaut la peine de prévoir des adresses IP supplémentaires disponibles dans la conception de votre VPC pour répondre à ces exigences.

Pour obtenir des conseils et des considérations approfondis concernant la conception des VPC et le dimensionnement des sous-réseaux, reportez-vous à la présentation de re:Invent How Amazon.com is Moving to Amazon. WorkSpaces

Interfaces réseau

Chacune WorkSpaces possède deux interfaces réseau élastiques (ENI), une interface réseau de gestion (`eth0`) et une interface réseau principale (`eth1`). AWS utilise l'interface réseau de gestion pour gérer le WorkSpace : il s'agit de l'interface sur laquelle se termine votre connexion client. AWS utilise une plage d'adresses IP privées pour cette interface. Pour que le routage réseau fonctionne correctement, vous ne pouvez pas utiliser cet espace d'adressage privé sur un réseau capable de communiquer avec votre WorkSpaces VPC.

Pour obtenir la liste des plages d'adresses IP privées utilisées par région, consultez Amazon WorkSpaces Details.

> **Note**
>
> Amazon WorkSpaces et ses interfaces réseau de gestion associées ne résident pas dans votre VPC, et vous ne pouvez pas consulter l'interface réseau de gestion ou l'ID d'instance Amazon Elastic Compute Cloud (Amazon EC2) dans AWS Management Console votre (reportez-vous Figure 5 à, et). Figure 6 Figure 7 Toutefois, vous pouvez consulter et modifier les paramètres du groupe de sécurité de votre interface réseau principale (`eth1`) dans la console. L'interface réseau principale de chacun d'entre eux WorkSpace est prise en compte dans vos quotas de ressources ENI Amazon EC2. Pour les déploiements d'Amazon à grande échelle WorkSpaces, vous devez ouvrir un ticket d'assistance via le AWS Management Console pour augmenter vos quotas ENI.

Flux de trafic

Vous pouvez diviser le WorkSpaces trafic Amazon en deux composantes principales :

- Le trafic entre l'appareil client et le WorkSpaces service Amazon.
- Le trafic entre le WorkSpaces service Amazon et le trafic réseau du client.

La section suivante traite de ces deux composants.

Appareil client pour WorkSpace

Quel que soit son emplacement (sur site ou à distance), l'appareil exécutant le WorkSpaces client Amazon utilise les deux mêmes ports pour se connecter au WorkSpaces service Amazon. Le client utilise le port 443 (port HTTPS) pour toutes les informations relatives à l'authentification et à la session, et le port 4172 (port PCoIP), avec le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol), pour le streaming de pixels vers une donnée et les contrôles de santé du réseau. WorkSpace Le trafic sur les deux ports est crypté. Le trafic du port 443 est utilisé pour l'authentification et les informations de session et utilise le protocole TLS pour chiffrer le trafic. Le trafic de streaming de pixels utilise le cryptage AES-256 bits pour la communication entre le client et le WorkSpace, via la passerelle `eth0` de streaming. Vous trouverez de plus amples informations dans la Sécurité section de ce document.

Nous publions les plages d'adresses IP par région de nos passerelles de streaming PCoIP et de nos points de terminaison de contrôle de l'état du réseau. Vous pouvez limiter le trafic sortant sur le port 4172 depuis le réseau de votre entreprise vers la passerelle de AWS streaming et les points de terminaison de contrôle de l'état du réseau en autorisant uniquement le trafic sortant sur le port 4172 à destination des AWS régions spécifiques dans lesquelles vous utilisez Amazon. WorkSpaces Pour les plages d'adresses IP et les points de terminaison de vérification de l'état du réseau, reportez-vous à la section Plages d'adresses IP Amazon WorkSpaces PCoIP Gateway.

Le WorkSpaces client Amazon dispose d'une fonction intégrée de vérification de l'état du réseau. Cet utilitaire indique aux utilisateurs si leur réseau peut prendre en charge une connexion au moyen d'un indicateur d'état en bas à droite de l'application. La figure suivante montre une vue plus détaillée de l'état du réseau accessible en choisissant Réseau en haut à droite du client.

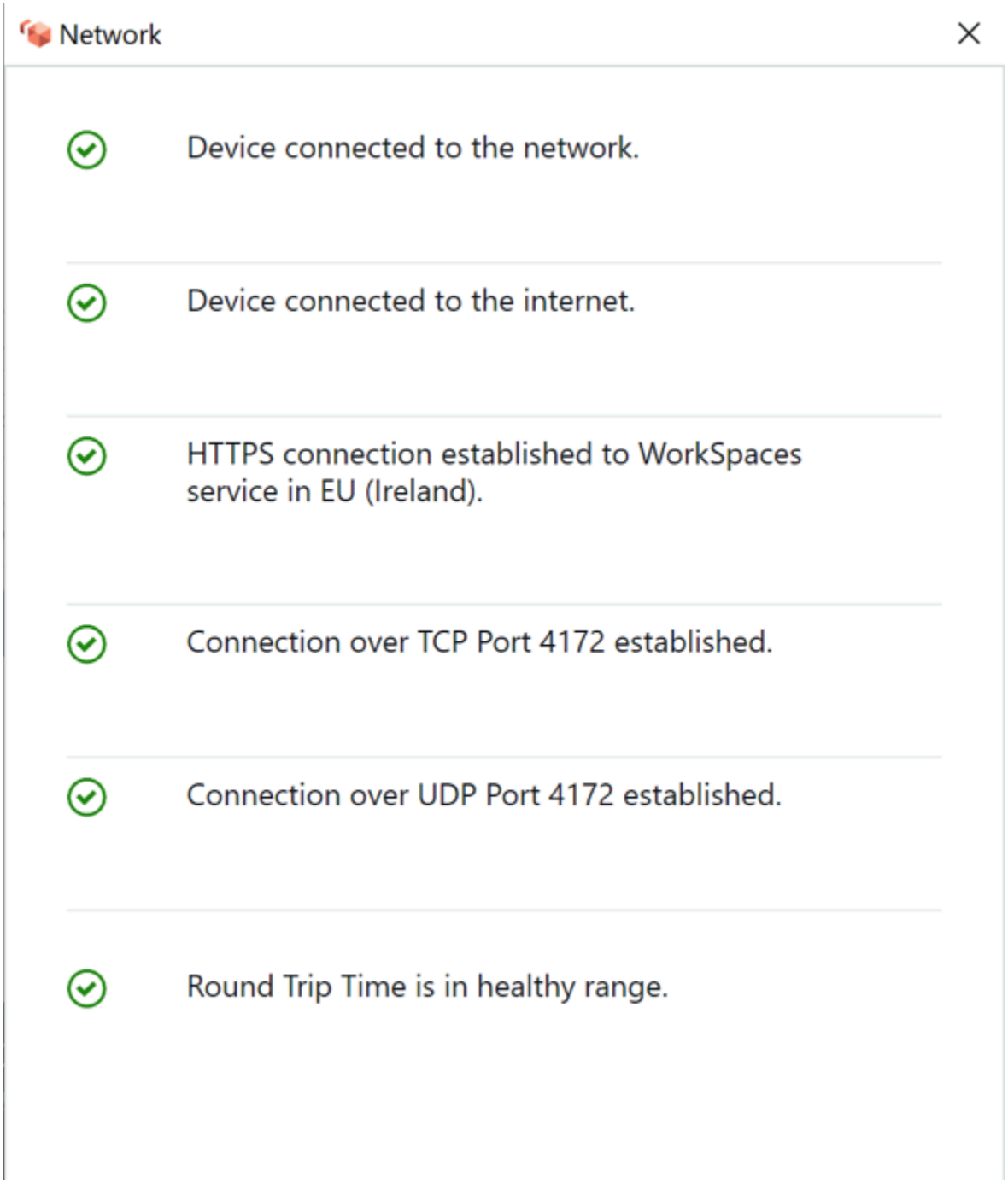

Figure 1 : WorkSpaces Client : vérification du réseau

Un utilisateur établit une connexion entre son client et le WorkSpaces service Amazon en fournissant ses informations de connexion pour le répertoire utilisé par la structure Directory Service, généralement son annuaire d'entreprise. Les informations de connexion sont envoyées via HTTPS aux passerelles d'authentification du WorkSpaces service Amazon dans la région où ils WorkSpace

se trouvent. La passerelle d'authentification du WorkSpaces service Amazon transmet ensuite le trafic à la structure de AWS Directory Service spécifique associée à votre WorkSpace.

Par exemple, lorsque vous utilisez l'AD Connector, celui-ci transmet la demande d'authentification directement à votre service AD, qui peut être sur site ou dans un AWS VPC. Pour plus d'informations, reportez-vous à la section Scénarios de déploiement AD DS de ce document. L'AD Connector ne stocke aucune information d'authentification et agit comme un proxy apatride. Par conséquent, il est impératif que l'AD Connector soit connecté à un serveur AD. L'AD Connector détermine le serveur AD auquel se connecter en utilisant les serveurs DNS que vous définissez lorsque vous créez l'AD Connector.

Si vous utilisez un AD Connector et que l'authentification MFA est activée sur l'annuaire, le jeton MFA est vérifié avant l'authentification du service d'annuaire. En cas d'échec de la validation MFA, les informations de connexion de l'utilisateur ne sont pas transmises à votre AWS Directory Service.

Une fois qu'un utilisateur est authentifié, le trafic de streaming démarre en utilisant le port 4172 (port PCoIP) via la passerelle de AWS streaming vers le. WorkSpace Les informations relatives à la session sont toujours échangées via HTTPS tout au long de la session. Le trafic de streaming utilise le premier ENI sur le WorkSpace (`eth0`sur le WorkSpace) qui n'est pas connecté à votre VPC. La connexion réseau entre la passerelle de streaming et l'ENI est gérée par AWS. En cas d'échec de connexion entre les passerelles de diffusion et l'ENI de WorkSpaces diffusion, un CloudWatch événement est généré. Pour plus d'informations, consultez la CloudWatch section Surveillance ou journalisation à l'aide d'Amazon de ce document.

La quantité de données envoyée entre le WorkSpaces service Amazon et le client dépend du niveau d'activité des pixels. Pour garantir une expérience optimale aux utilisateurs, nous recommandons que le temps d'aller-retour (RTT) entre le WorkSpaces client et la AWS région où vous vous WorkSpaces trouvez soit inférieur à 100 millisecondes (ms). Cela signifie généralement que votre WorkSpaces client est situé à moins de trois mille kilomètres de la région dans laquelle WorkSpace il est hébergé. La page Web Connection Health Check peut vous aider à déterminer la AWS région la plus optimale pour vous connecter au WorkSpaces service Amazon.

Amazon WorkSpaces Service vers VPC

Une fois qu'une connexion est authentifiée entre un client WorkSpace et qu'un trafic de streaming est initié, votre WorkSpaces client affiche un poste de travail Windows ou Linux (votre Amazon WorkSpace) connecté à votre cloud privé virtuel (VPC), et votre réseau doit indiquer que vous avez établi cette connexion. La WorkSpace principale Elastic Network Interface (ENI), identifiée

commeeth1, se verra attribuer une adresse IP par le service DHCP (Dynamic Host Configuration Protocol) fourni par votre VPC, généralement à partir des mêmes sous-réseaux que votre Directory AWS Service. L'adresse IP est conservée WorkSpace pendant toute la durée de vie du WorkSpace. L'ENI de votre VPC a accès à toutes les ressources du VPC et à tous les réseaux que vous avez connectés à votre VPC (via un peering VPC, une connexion ou une connexion VPN). AWS Direct Connect

L'accès de l'ENI aux ressources de votre réseau est déterminé par la table de routage du sous-réseau et du groupe de sécurité par défaut que votre AWS Directory Service configure pour chacun WorkSpace, ainsi que par tout groupe de sécurité supplémentaire que vous attribuez à l'ENI. Vous pouvez ajouter des groupes de sécurité à l'ENI faisant face à votre VPC à tout moment en utilisant le AWS Management Console ou. AWS CLI (Pour plus d'informations sur les groupes de sécurité, reportez-vous à la section Groupes de sécurité pour vous WorkSpaces.) Outre les groupes de sécurité, vous pouvez utiliser votre pare-feu hôte préféré sur un site donné WorkSpace pour limiter l'accès réseau aux ressources du VPC.

Il est recommandé de créer votre ensemble d'options DHCP avec les adresses IP du serveur DNS et les noms de domaine complets faisant autorité dans votre Active Directory et spécifiques à votre environnement, puis d'attribuer ces options DHCP personnalisées définies au VPC Amazon utilisé par Amazon. WorkSpaces Par défaut, Amazon Virtual Private Cloud (Amazon VPC) utilise le AWS DNS au lieu du DNS de votre service d'annuaire. L'utilisation d'un ensemble d'options DHCP garantit une résolution correcte des noms DNS et une configuration cohérente de vos serveurs de noms DNS internes, non seulement pour votre charge de travail ou instance de support WorkSpaces, mais également pour toute charge de travail ou instance de support que vous pourriez avoir planifiée pour votre déploiement.

Lorsque les options DHCP sont appliquées, il existe deux différences importantes dans la manière dont elles seront appliquées par rapport WorkSpaces à la manière dont elles sont appliquées aux instances EC2 traditionnelles :

- La première différence réside dans la manière dont les suffixes DNS de l'option DHCP seront appliqués. Les paramètres DNS de chacun WorkSpace sont configurés pour son adaptateur réseau, les options Ajouter les suffixes DNS principaux et spécifiques à la connexion et Ajouter les suffixes parents des suffixes DNS principaux étant activées. La configuration sera mise à jour avec le suffixe DNS configuré dans le AWS Directory Service que vous avez enregistré et auquel vous êtes associé WorkSpace par défaut. De même, si le suffixe DNS configuré dans le jeu d'options DHCP utilisé est différent, il sera ajouté et appliqué à tout suffixe associé. WorkSpaces

- La deuxième différence est que les adresses IP DNS de l'option DHCP configurées ne seront pas appliquées WorkSpace car le WorkSpaces service Amazon donne la priorité aux adresses IP des contrôleurs de domaine du répertoire configuré.

Vous pouvez également configurer une zone hébergée privée Route 53 pour prendre en charge un environnement DNS hybride ou partagé et obtenir une résolution DNS appropriée pour votre WorkSpaces environnement Amazon. Pour plus d'informations, reportez-vous aux options DNS du cloud hybride pour VPC et au DNS AWS hybride avec Active Directory.

> **Note**
>
> Chacun WorkSpace doit actualiser la table IP lors de l'application d'un ensemble d'options DHCP nouveau ou différent au VPC. Pour actualiser, vous pouvez exécuter ipconfig / renew ou redémarrer n'importe quel WorkSpace VPC configuré avec vos options DHCP mises à jour. Si vous utilisez AD Connector et que vous mettez à jour les adresses IP de vos adresses IP/contrôleurs de domaine connectés, vous devez ensuite mettre à jour la clé de `DomainJoinDNS` registre Skylight sur votre. WorkSpaces Il est recommandé de le faire via un GPO. Le chemin d'accès à cette clé de registre est`HKLM:\SOFTWARE\Amazon \Skylight`. La valeur de cette valeur n'`REG_SZ`est pas mise à jour si les paramètres DNS du connecteur AD sont modifiés, et les ensembles d'options DHCP VPC ne mettront pas non plus à jour cette clé.

La figure de la section Scénarios de déploiement AD DS de ce livre blanc montre le flux de trafic décrit.

Comme expliqué précédemment, le WorkSpaces service Amazon donne la priorité aux adresses IP des contrôleurs de domaine du répertoire configuré pour la résolution DNS et ignore les serveurs DNS configurés dans votre ensemble d'options DHCP. Si vous avez besoin d'un contrôle plus précis des paramètres de votre serveur DNS pour votre Amazon WorkSpaces, vous pouvez suivre les instructions relatives à la mise à jour des serveurs DNS pour Amazon figurant WorkSpaces dans le WorkSpaces guide Update DNS servers for Amazon du Amazon WorkSpaces Administration Guide.

Si vous WorkSpaces devez résoudre d'autres services et si vous utilisez les options DHCP par défaut définies avec votre VPC, le service DNS de votre contrôleur de domaine dans AWS ce VPC doit donc être configuré pour utiliser le transfert DNS, en pointant vers le serveur Amazon DNS avec l'adresse IP à la base de votre CIDR VPC plus deux ; en d'autres termes, si votre CIDR VPC est 10.0.0.0/24, vous configurez le transfert DNS pour utiliser le résolveur DNS Route 53 standard à 10.0.0.2.

Si vous avez WorkSpaces besoin d'une résolution DNS des ressources de votre réseau local, vous pouvez utiliser un point de terminaison sortant Route 53 Resolver, créer une règle de transfert Route 53 et associer cette règle aux VPC nécessitant cette résolution DNS. Si vous avez configuré le transfert sur le service DNS de votre contrôleur de domaine vers le résolveur DNS Route 53 par défaut de votre VPC, comme expliqué dans le paragraphe précédent, le processus de résolution DNS se trouve dans le guide de résolution des requêtes DNS entre VPC et dans le guide de votre réseau du guide du développeur Amazon Route 53.

Si vous utilisez les options DHCP définies par défaut et que vous avez besoin d'autres hôtes de vos VPC qui ne font pas partie de votre domaine Active Directory pour résoudre les noms d'hôtes dans votre espace de noms Active Directory, vous pouvez utiliser ce point de terminaison sortant Route 53 Resolver et ajouter une autre règle de transfert Route 53 qui transmet les requêtes DNS de votre domaine Active Directory à vos serveurs DNS Active Directory. Cette règle de transfert Route 53 devra être associée au point de terminaison sortant du résolveur Route 53 capable d'accéder à votre service DNS Active Directory, ainsi qu'à tous les VPC que vous souhaitez activer pour résoudre les enregistrements DNS dans votre domaine WorkSpaces Active Directory.

De même, un point de terminaison entrant Route 53 Resolver peut être utilisé pour autoriser la résolution DNS des enregistrements DNS de votre domaine WorkSpaces Active Directory à partir de votre réseau local.

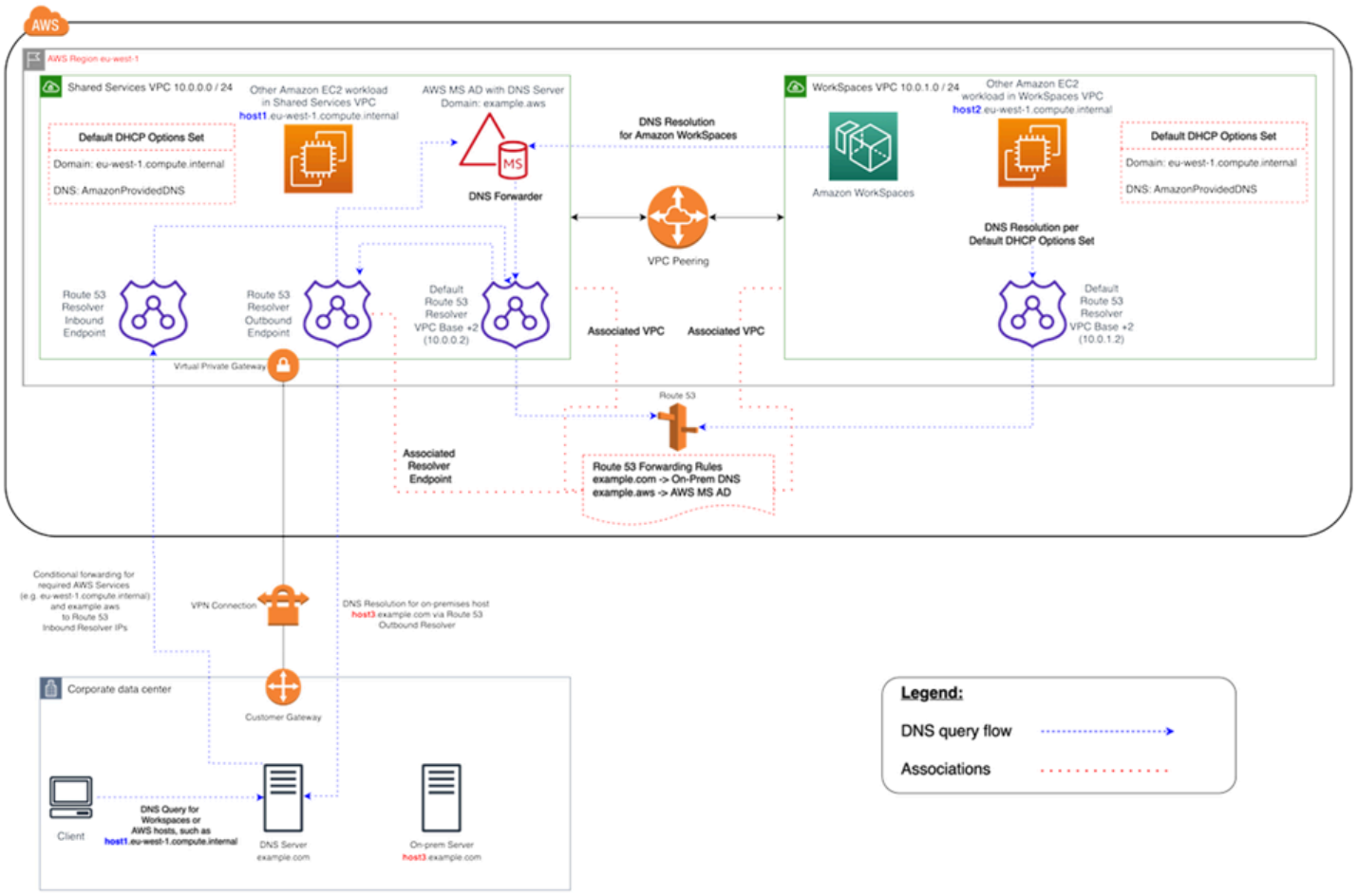

Figure 2 : Exemple de résolution WorkSpaces DNS avec les points de terminaison Route 53

- Votre Amazon WorkSpaces utilisera le service DNS AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) pour la résolution DNS. Le service AWS Managed Microsoft AD DNS résout le `example.aws` domaine et transmet toutes les autres requêtes DNS au résolveur DNS Route 53 par défaut à l'adresse IP de base VPC CIDR +2 pour activer la résolution DNS

  Le VPC Shared Services contient un point de terminaison Route 53 Outbound Resolver, qui est associé à deux règles de transfert Route 53. L'une de ces règles transmet les requêtes DNS pour le `example.com` domaine aux serveurs DNS locaux. La deuxième règle transmet les requêtes DNS pour votre AWS Managed Microsoft AD domaine `example.aws` à votre service DNS Active Directory dans le VPC Shared Services.

  Grâce à cette architecture, votre Amazon WorkSpaces sera en mesure de résoudre les requêtes DNS pour les éléments suivants :

  - Votre AWS Managed Microsoft AD domaine`example.aws`.
  - Les instances EC2 du domaine sont configurées avec votre ensemble d'options DHCP par défaut (par exemple,`host1.eu-west-1.compute.internal`) ainsi que d'autres AWS services ou points de terminaison.
  - Les hôtes et les services de votre domaine local, tels que`host3.example.com`.
- • Les autres charges de travail EC2 du VPC Shared Services (`host1.eu-west-1.compute.internal`) et du WorkSpaces VPC (`host2.eu-west-1.compute.internal`) peuvent utiliser les mêmes résolutions DNS que les vôtres WorkSpaces, à condition que les règles de transfert Route 53 soient associées aux deux VPC. Dans ce cas, la résolution DNS du `example.aws` domaine passera par le résolveur DNS Route 53 par défaut à l'adresse IP de base VPC CIDR +2, qui, selon les règles de transfert Route 53 configurées et associées, les transmettra via le point de terminaison sortant du résolveur Route 53 au WorkSpaces service DNS Active Directory.
- • Enfin, un client local peut également effectuer la même résolution DNS, puisque le serveur DNS local est configuré avec des redirecteurs conditionnels pour les `eu-west-1.compute.internal` domaines `example.aws` et, transférant les requêtes DNS pour ces domaines aux adresses IP des points de terminaison entrants du résolveur Route 53.

Exemple de configuration typique

Imaginons un scénario dans lequel vous avez deux types d'utilisateurs et où votre AWS Directory Service utilise un AD centralisé pour l'authentification des utilisateurs :

- Travailleurs qui ont besoin d'un accès complet depuis n'importe où (par exemple, les employés à plein temps) : ces utilisateurs auront un accès complet à Internet et au réseau interne, et ils passeront par un pare-feu entre le VPC et le réseau sur site.
- Travailleurs qui ne devraient avoir qu'un accès restreint depuis le réseau de l'entreprise (par exemple, les sous-traitants et les consultants) — Ces utilisateurs ont un accès Internet restreint via un serveur proxy à des sites Web spécifiques du VPC, et auront un accès réseau limité dans le VPC et au réseau sur site.

Vous souhaitez donner aux employés à temps plein la possibilité de disposer d'un accès administrateur local WorkSpace pour installer leurs logiciels, et vous aimeriez appliquer l'authentification à deux facteurs grâce à la MFA. Vous souhaitez également permettre aux employés à temps plein d'accéder à Internet sans restrictions de leur part WorkSpace.

Pour les sous-traitants, vous souhaitez bloquer l'accès des administrateurs locaux afin qu'ils ne puissent utiliser que des applications préinstallées spécifiques. Vous souhaitez appliquer des contrôles d'accès réseau restrictifs à l'aide de groupes de sécurité pour ces derniers WorkSpaces. Vous devez ouvrir les ports 80 et 443 uniquement à des sites Web internes spécifiques, et vous souhaitez bloquer complètement leur accès à Internet.

Dans ce scénario, il existe deux types de personas d'utilisateurs complètement différents avec des exigences différentes en matière d'accès au réseau et aux postes de travail. Il est recommandé de les gérer et de les configurer WorkSpaces différemment. Vous devrez créer deux connecteurs AD, un pour chaque personnage utilisateur. Chaque AD Connector nécessite deux sous-réseaux dotés de suffisamment d'adresses IP disponibles pour répondre à vos estimations de croissance de WorkSpaces l'utilisation.

> **Note**
>
> Chaque sous-réseau AWS VPC consomme cinq adresses IP (les quatre premières et la dernière) à des fins de gestion, et chaque AD Connector consomme une adresse IP dans chaque sous-réseau dans lequel il persiste.

Les autres considérations relatives à ce scénario sont les suivantes :

- AWS Les sous-réseaux VPC doivent être des sous-réseaux privés, afin que le trafic, tel que l'accès à Internet, puisse être contrôlé via une passerelle de traduction d'adresses réseau (NAT), un serveur proxy NAT dans le cloud ou redirigé via votre système de gestion du trafic sur site.
- Un pare-feu est en place pour tout le trafic VPC à destination du réseau sur site.
- Le serveur Microsoft AD et les serveurs MFA RADIUS sont soit sur site (voir Scénario 1 : Utilisation du connecteur AD pour l'authentification par proxy auprès des services AD DS locaux dans ce document), soit font partie de l'implémentation dans le AWS cloud (reportez-vous aux scénarios 2 et 3, Scénarios de déploiement AD DS, dans ce document).

Étant donné que tous WorkSpaces ont accès à Internet sous une forme ou une autre et qu'ils sont hébergés dans un sous-réseau privé, vous devez également créer des sous-réseaux publics qui peuvent accéder à Internet via une passerelle Internet. Vous avez besoin d'une passerelle NAT pour les employés à plein temps, leur permettant d'accéder à Internet, et d'un serveur proxy NAT pour les consultants et les sous-traitants, afin de limiter leur accès à des sites Web internes spécifiques. Pour planifier les défaillances, concevoir une haute disponibilité et limiter les frais de

trafic inter-AZ, vous devez disposer de deux passerelles NAT et de serveurs NAT ou proxy dans deux sous-réseaux différents dans un déploiement multi-AZ. Les deux zones de disponibilité que vous sélectionnez comme sous-réseaux publics correspondent aux deux zones de disponibilité que vous utilisez pour vos WorkSpaces sous-réseaux, dans les régions comportant plus de deux zones. Vous pouvez acheminer tout le trafic de chaque zone WorkSpaces de zone vers le sous-réseau public correspondant afin de limiter les frais de trafic inter-zones et de faciliter la gestion. La figure suivante montre la configuration du VPC.

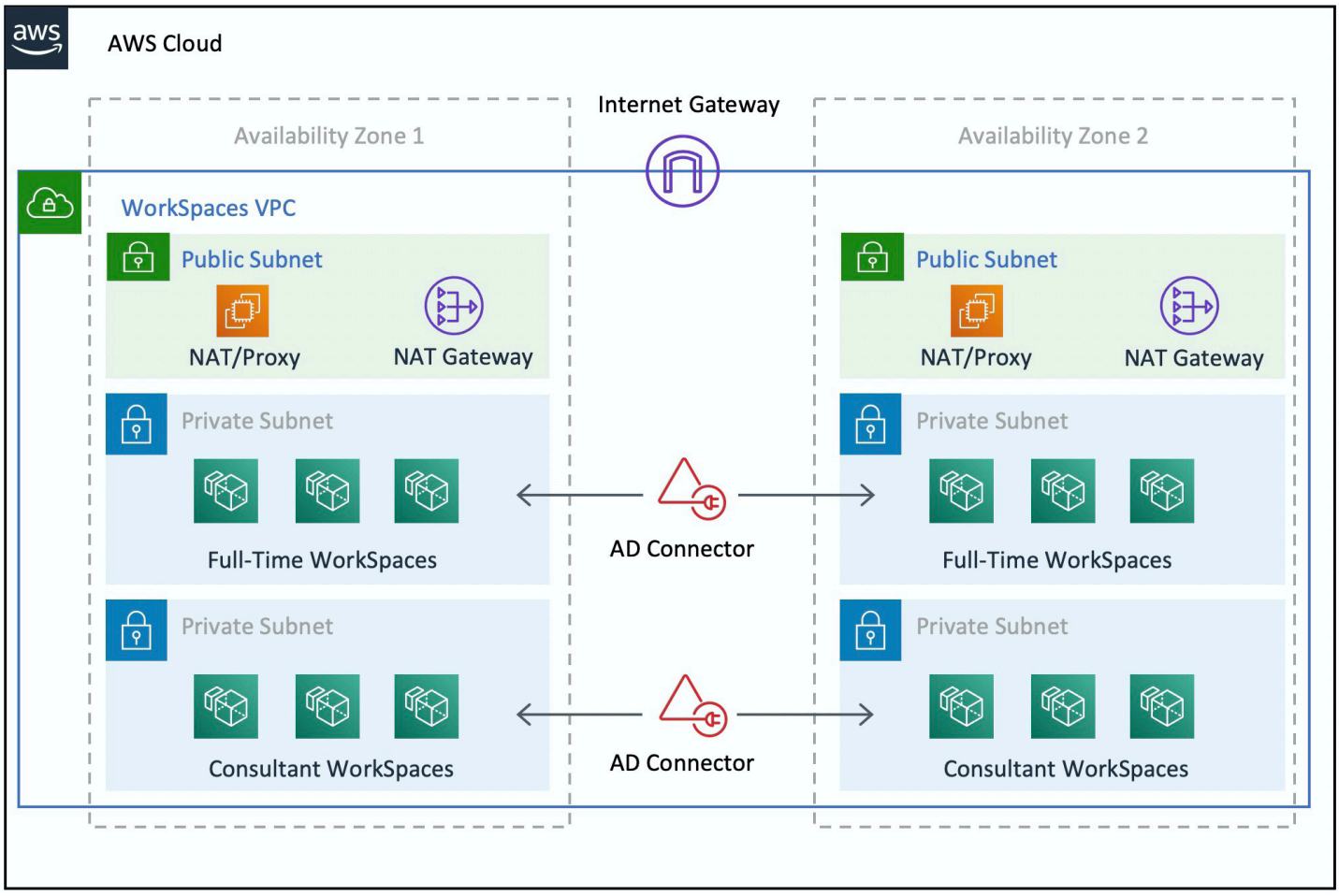

Figure 3 : conception de VPC de haut niveau

Les informations suivantes décrivent comment configurer les deux WorkSpaces types différents :

Pour configurer WorkSpaces pour les employés à temps plein :

1. Dans l'Amazon WorkSpaces Management Console, choisissez l'option Répertoires dans la barre de menu.
2. Choisissez l'annuaire qui héberge vos employés à temps plein.

3. Choisissez Local Administrator Setting.

En activant cette option, toute personne nouvellement créée WorkSpace aura des privilèges d'administrateur local. Pour accorder l'accès à Internet, configurez le NAT pour l'accès Internet sortant depuis votre VPC. Pour activer le MFA, vous devez spécifier un serveur RADIUS, des adresses IP de serveur, des ports et une clé pré-partagée.

Pour les employés à plein temps WorkSpaces, le trafic entrant vers le Remote Desktop Protocol (RDP) WorkSpace peut être limité au Remote Desktop Protocol (RDP) depuis le sous-réseau Helpdesk en appliquant un groupe de sécurité par défaut via les paramètres AD Connector.

Pour configurer WorkSpaces pour les sous-traitants et les consultants :

1. Dans la console WorkSpaces de gestion Amazon, désactivez l'accès à Internet et le paramètre d'administrateur local.
2. Ajoutez un groupe de sécurité dans la section des paramètres du groupe de sécurité pour appliquer un groupe de sécurité à tous les nouveaux groupes WorkSpaces créés dans ce répertoire.

Pour les consultants WorkSpaces, limitez le trafic sortant et entrant au en appliquant un groupe de sécurité WorkSpaces par défaut via les paramètres AD Connector à tous les utilisateurs WorkSpaces associés à l'AD Connector. Le groupe de sécurité empêche l'accès sortant depuis le trafic WorkSpaces vers autre chose que le trafic HTTP et HTTPS, et le trafic entrant vers RDP depuis le sous-réseau Helpdesk du réseau local.

> **Note**
>
> Le groupe de sécurité s'applique uniquement à l'ENI qui se trouve dans le VPC (`eth1`sur le WorkSpace), et l'accès à celui-ci WorkSpace depuis le WorkSpaces client n'est pas restreint en raison d'un groupe de sécurité. La figure suivante montre la conception finale du WorkSpaces VPC.

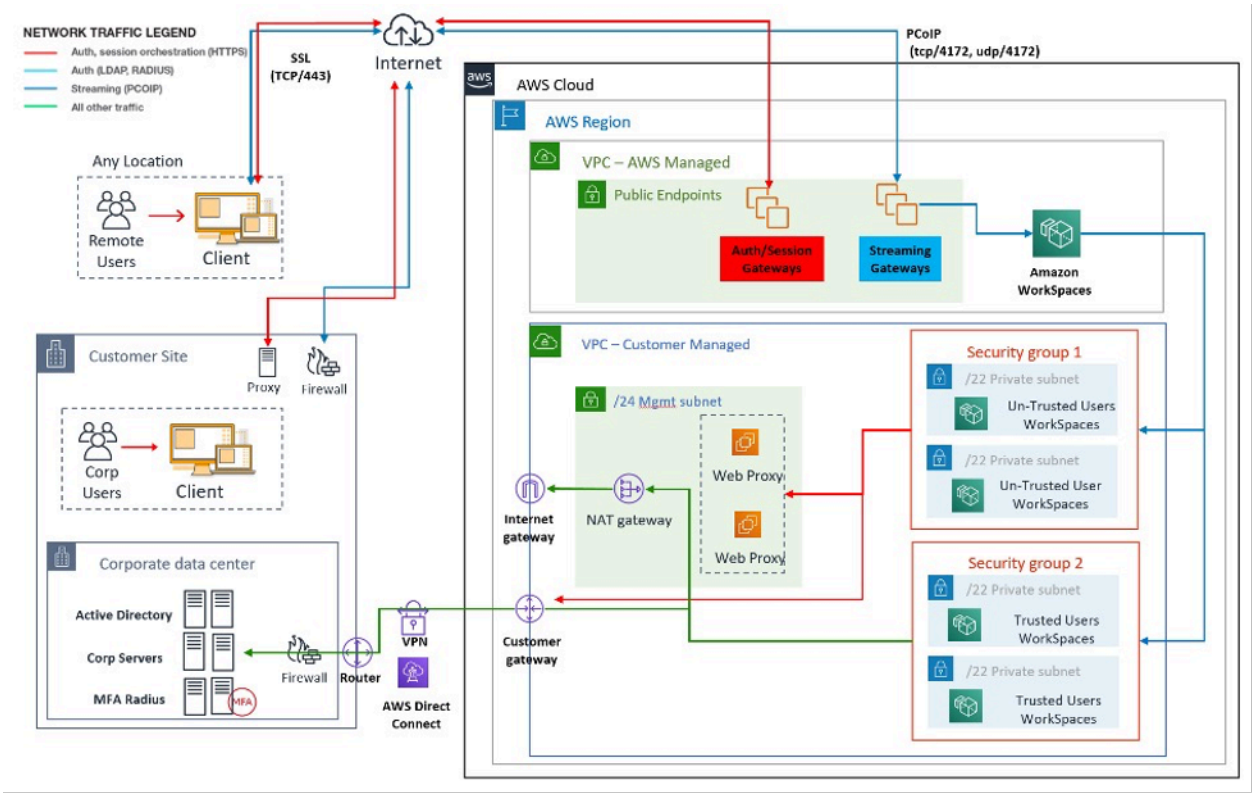

Figure 4 : WorkSpaces design avec personas d'utilisateur

AWS Service de répertoire

Comme indiqué dans l'introduction, AWS Directory Service est un composant essentiel d'Amazon WorkSpaces. Avec AWS Directory Service, vous pouvez créer trois types d'annuaires avec Amazon WorkSpaces :

- AWS Managed Microsoft AD est un Microsoft AD géré, alimenté par Windows Server 2012 R2. AWS Managed Microsoft AD est disponible en édition Standard ou Enterprise.
- Simple AD est un service d'annuaire géré autonome, compatible avec Microsoft AD, alimenté par Samba 4.
- AD Connector est un proxy d'annuaire permettant de rediriger les demandes d'authentification et les recherches d'utilisateurs ou de groupes vers votre Microsoft AD local existant.

La section suivante décrit les flux de communication pour l'authentification entre le service de WorkSpaces courtage Amazon et AWS Directory Service, les meilleures pratiques de mise en œuvre WorkSpaces avec AWS Directory Service et les concepts avancés, tels que le MFA. Il aborde également les concepts d'architecture d'infrastructure pour Amazon WorkSpaces à grande échelle,

les exigences relatives à Amazon VPC et AWS Directory Service, y compris l'intégration avec les services de domaine Microsoft AD (AD DS) sur site.

Scénarios de déploiement d'AD DS

Amazon WorkSpaces est soutenu par le service d' AWS annuaire, et la conception et le déploiement appropriés du service d'annuaire sont essentiels. Les six scénarios suivants s'appuient sur les services de domaine Active Directory présentés dans le guide de démarrage AWS rapide et décrivent les meilleures pratiques en matière d'options de déploiement pour AD DS lorsqu'ils sont utilisés avec Amazon WorkSpaces. La section Considérations relatives à la conception de ce document détaille les exigences spécifiques et les meilleures pratiques relatives à l'utilisation d'AD Connector pour WorkSpaces, ce qui fait partie intégrante du concept de WorkSpaces conception global.

- Scénario 1 : utilisation d'AD Connector pour l'authentification par proxy auprès d'AD DS sur site — Dans ce scénario, la connectivité réseau (VPN/Direct Connect) est en place avec le client, toutes les authentifications étant transmises par proxy via AWS Directory Service (AD Connector) à l'AD DS local du client.
- Scénario 2 : extension d'AD DS sur site à AWS (Replica) : ce scénario est similaire au scénario 1, mais ici, une réplique de l'AD DS du client est déployée AWS en combinaison avec AD Connector, réduisant ainsi le temps de latence des demandes d'authentification/de requête adressées à AD DS et au catalogue global AD DS.
- Scénario 3 : déploiement isolé autonome à l'aide du AWS Directory Service dans le AWS cloud — Il s'agit d'un scénario isolé qui n'inclut pas la connectivité vers le client pour l'authentification. Cette approche utilise AWS Directory Service (Microsoft AD) et AD Connector. Bien que ce scénario ne repose pas sur la connectivité avec le client pour l'authentification, il prévoit le trafic des applications lorsque cela est nécessaire via un VPN ou Direct Connect.
- Scénario 4 : AWS Microsoft AD et confiance transitive bidirectionnelle vers le service local — Ce scénario inclut le service géré AWS Microsoft AD (MAD) avec une confiance transitive bidirectionnelle vers la forêt Microsoft AD sur site.
- Scénario 5 : AWS Microsoft AD utilisant un VPC Shared Services — Ce scénario utilise Managed AWS Microsoft AD dans un VPC Shared Services pour être utilisé comme domaine d'identité pour plusieurs services (AWS Amazon EC2, Amazon WorkSpaces, etc.) tout en utilisant le connecteur AD pour transmettre par proxy les demandes d'authentification utilisateur LDAP (Lightweight Directory Access Protocol) aux contrôleurs de domaine AD.
- Scénario 6 : AWS Microsoft AD, Shared Services VPC et confiance unidirectionnelle avec AD sur site — Ce scénario est similaire au scénario 5, mais il inclut des domaines d'identité et de ressources disparates utilisant une approbation unidirectionnelle sur site.

Vous devez prendre en compte plusieurs points lors de la sélection de votre scénario de déploiement pour les services de domaine Active Directory (ADDS). Cette section explique le rôle de l'AD Connector auprès d'Amazon WorkSpaces et aborde certaines considérations importantes lors de la sélection d'un scénario de déploiement ADDS. Pour plus d'informations sur la conception et la planification d' AWSADDS, consultez le guide de AWS conception et de planification des services de domaine Active Directory.

Le rôle de l' AWS AD Connector auprès d'Amazon WorkSpaces

L'AWS AD Connector est un service d' AWS annuaire qui agit comme un service proxy pour un Active Directory. Il ne stocke ni ne met en cache les informations d'identification utilisateur, mais transmet les demandes d'authentification ou de recherche à votre Active Directory, sur site ou sur site. AWS À moins que vous ne l'utilisiez AWS Managed Microsoft AD, c'est également le seul moyen d'enregistrer votre Active Directory (sur site ou étendu à AWS) pour une utilisation avec Amazon WorkSpaces (WorkSpaces).

Un AD Connector peut pointer vers votre Active Directory local, vers un Active Directory étendu à AWS (contrôleurs de domaine AD sur Amazon EC2) ou vers un. AWS Managed Microsoft AD

L'AD Connector joue un rôle important dans la plupart des scénarios de déploiement décrits dans les sections suivantes. L'utilisation de l'AD Connector WorkSpaces offre de nombreux avantages :

- Lorsqu'ils sont dirigés vers l'Active Directory de votre entreprise, il permet à vos utilisateurs d'utiliser leurs informations d'identification professionnelles existantes pour se connecter à WorkSpaces d'autres services, tels qu'Amazon WorkDocs.
- Vous pouvez appliquer de manière cohérente les politiques de sécurité existantes (expiration des mots de passe, verrouillage des comptes, etc.), que vos utilisateurs accèdent aux ressources de votre infrastructure sur site ou dans une infrastructure telle que. AWS Cloud WorkSpaces
- L'AD Connector permet une intégration simple à votre infrastructure MFA existante basée sur Radius afin de fournir un niveau de sécurité supplémentaire.
- Il permet de séparer vos utilisateurs. Par exemple, il permet de configurer un certain nombre d' WorkSpaces options par unité commerciale ou par personne, étant donné que plusieurs connecteurs AD peuvent pointer vers les mêmes contrôleurs de domaine (serveurs DNS) d'Active Directory pour l'authentification des utilisateurs :
  - Domaine cible ou unité organisationnelle pour une application ciblée des objets de stratégie de groupe (GPO) Active Directory

- Différents groupes de sécurité pour contrôler le flux de trafic vers/depuis WorkSpaces
- Différentes options de contrôle d'accès (appareils clients autorisés) et groupes de contrôle d'accès IP (limite d'accès aux plages d'adresses IP)
- Activation sélective des autorisations d'administrateur local
- Différentes autorisations en libre-service
- Application sélective de l'authentification multifactorielle (MFA)
- Placement de vos interfaces réseau WorkSpaces élastiques (ENI) dans différents VPC ou sous-réseaux à des fins d'isolation

Les connecteurs AD multiples permettent également de prendre en charge un plus grand nombre d'utilisateurs, si vous atteignez la limite de performance d'un seul connecteur AD, petit ou grand. Reportez-vous à la Dimensionnement de AWS Managed Microsoft AD section pour plus de détails.

L'utilisation d'AD Connector WorkSpaces est gratuite, à condition que vous ayez au moins un WorkSpaces utilisateur actif dans un petit AD Connector et au moins 100 WorkSpaces utilisateurs actifs dans un grand AD Connector. Pour plus d'informations, consultez la page de tarification des services d'AWS annuaire.

L'importance de votre lien réseau AWS avec un Active Directory sur site

WorkSpaces repose sur la connectivité à votre Active Directory. Par conséquent, la disponibilité du lien réseau vers votre Active Directory est de la plus haute importance. Par exemple, si votre liaison réseau dans le scénario 1 est en panne, vos utilisateurs ne pourront pas s'authentifier et ne pourront donc pas utiliser leur WorkSpaces.

Si un Active Directory sur site doit être utilisé dans le cadre du scénario, vous devez tenir compte de la résilience, de la latence et du coût du trafic de votre liaison réseau. AWS Dans un WorkSpaces déploiement multirégional, cela peut impliquer plusieurs liaisons réseau dans différentes AWS régions, ou plusieurs liaisons réseau avec AWS Transit Gateway un peering établi entre elles pour acheminer votre trafic AD vers le VPC connecté à votre AD sur site. Ces considérations relatives aux liens réseau s'appliquent à la plupart des scénarios décrits dans les sections suivantes, mais elles sont particulièrement importantes pour les scénarios dans lesquels votre trafic AD en provenance des connecteurs AD WorkSpaces doit traverser le lien réseau pour atteindre votre Active Directory sur site. Le scénario 1 met en évidence certaines des mises en garde.

Utilisation de l'authentification multifactorielle avec WorkSpaces

Si vous envisagez d'utiliser la Multi-Factor Authentication (MFA) WorkSpaces avec, vous devez utiliser un AD AWS Connector ou AWS Managed Microsoft AD un AD Connector, car seuls ces services autorisent l'enregistrement de l'annuaire à utiliser WorkSpaces et à configurer RADIUS. Pour le placement de vos serveurs RADIUS, les considérations relatives aux liaisons réseau abordées dans la L'importance de votre lien réseau AWS avec un Active Directory sur site section s'appliquent.

Séparer le compte du domaine de ressources

Pour des raisons de sécurité ou pour une meilleure gestion, il peut être souhaitable de séparer le domaine du compte du domaine des ressources. Par exemple, placez les objets WorkSpaces informatiques dans un domaine de ressources distinct, tandis que les utilisateurs font partie du domaine du compte. Une telle implémentation peut être utilisée pour permettre à une organisation partenaire de gérer l' WorkSpacesutilisation des politiques de groupe AD dans le domaine des ressources, sans pour autant renoncer au contrôle ni accorder l'accès au domaine du compte. Cela peut être accompli en utilisant deux Active Directory avec un Active Directory Trust configuré. Les sections suivantes traitent de cette question plus en détail :

- Scénario 4 : AWS Microsoft AD et une confiance transitive bidirectionnelle vers les environnements locaux
- Scénario 6 : AWS Microsoft AD, VPC à services partagés et confiance unidirectionnelle sur site

Déploiements Active Directory de grande envergure

Vous devez vous assurer qu'Active Directory Sites & Services est configuré en conséquence. Cela est particulièrement important si votre Active Directory est composé d'un grand nombre de contrôleurs de domaine situés dans différentes zones géographiques. Votre Windows WorkSpaces utilise le mécanisme standard de Microsoft pour découvrir son contrôleur de domaine pour le site Active Directory auquel il est affecté. Ce processus DC Locator repose sur le DNS et peut être considérablement prolongé si une longue liste de contrôleurs de domaine dont la priorité et le poids ne sont pas spécifiques est renvoyée au début du processus DC Locator. Plus important encore, si WorkSpaces vous êtes « épinglé » sur un contrôleur de domaine sous-optimal, toutes les communications ultérieures avec ce contrôleur de domaine peuvent être affectées par une latence réseau accrue et une réduction de la bande passante lorsque vous traversez des liaisons réseau étendues. Cela ralentira toute communication avec le contrôleur de domaine, y compris le traitement d'un nombre potentiellement important d'objets de stratégie de groupe (GPO) et

les transferts de fichiers depuis le contrôleur de domaine. En fonction de la topologie du réseau, cela peut également augmenter vos coûts de mise en réseau, car les données échangées entre WorkSpaces les contrôleurs de domaine peuvent emprunter inutilement un chemin réseau plus coûteux. Reportez-vous aux Considérations relatives à la conception sections Conception en VPC et pour obtenir des conseils sur le DHCP et le DNS dans le cadre de la conception de votre VPC, ainsi que sur les sites et services Active Directory.

Utilisation de Microsoft Azure Active Directory ou des services de domaine Active Directory avec WorkSpaces

Si vous avez l'intention d'utiliser Microsoft Azure Active Directory avec WorkSpaces, vous pouvez utiliser Azure AD Connect pour synchroniser votre identité avec votre Active Directory local ou avec votre Active Directory sur AWS (contrôleur de domaine sur Amazon EC2 AWS Managed Microsoft AD ou). Toutefois, cela ne vous permettra pas de WorkSpaces rejoindre votre Azure Active Directory. Pour plus d'informations, consultez la documentation Microsoft Hybrid Identity dans la documentation Microsoft Azure.

Si vous souhaitez vous connecter WorkSpaces à Azure Active Directory, vous devez déployer les services de domaine Microsoft Azure Active Directory (Azure AD DS), établir une connectivité entre Azure AWS et Azure et utiliser un connecteur AWS AD pointant vers vos contrôleurs de domaine Azure AD DS. Pour plus d'informations sur la façon de configurer cela, consultez le billet de blog Ajouter votre WorkSpaces compte à Azure AD à l'aide des services de domaine Azure Active Directory.

Lorsque vous utilisez AWS Directory Service s with WorkSpaces, vous devez tenir compte de la taille de votre WorkSpaces déploiement et de sa croissance attendue afin de déterminer la taille AWS Directory Service appropriée. Cette section fournit des conseils sur le dimensionnement AWS Directory Service à utiliser avec WorkSpaces. Nous vous recommandons également de consulter les meilleures pratiques pour AD Connector et les meilleures pratiques pour les AWS Managed Microsoft AD sections du Guide d'AWS Directory Service administration.

Dimensionnement de l'AD Connector avec WorkSpaces

Le connecteur Active Directory (AD Connector) est disponible en deux tailles, petite et grande. Bien qu'aucune limite d'utilisateur ou de connexion ne soit imposée, nous recommandons d'utiliser un petit AD Connector pour un maximum de 500 utilisateurs WorkSpaces autorisés, et un AD Connector de grande taille pour un maximum de 5 000 utilisateurs WorkSpaces autorisés. Vous pouvez répartir la charge des applications sur plusieurs AD Connector afin de répondre à vos besoins en termes de

performances. Par exemple, si vous devez prendre en charge 1 500 WorkSpaces utilisateurs, vous pouvez répartir le vôtre de WorkSpaces manière égale sur trois petits AD Connector, chacun prenant en charge 500 utilisateurs. Si tous vos utilisateurs résident dans le même domaine, l'AD Connector peut tous pointer vers le même ensemble de serveurs DNS résolvant votre domaine Active Directory.

Remarque : si vous avez commencé avec un petit AD Connector et que votre WorkSpaces déploiement s'étoffe au fil du temps, vous pouvez créer un ticket d'assistance pour faire passer la taille de votre AD Connector de petite taille à grande afin de prendre en charge le plus grand nombre d'utilisateurs WorkSpaces autorisés.

Dimensionnement de AWS Managed Microsoft AD

AWS Managed Microsoft ADvous permet d'exécuter Microsoft Active Directory en tant que service géré. Vous pouvez choisir entre l'édition Standard et l'édition Enterprise lorsque vous lancez le service. L'édition Standard est recommandée pour les petites et moyennes entreprises comptant jusqu'à 5 000 utilisateurs et prend en charge environ 30 000 objets de répertoire, tels que des utilisateurs, des groupes et des ordinateurs. L'édition Enterprise est conçue pour prendre en charge jusqu'à 500 000 objets de répertoire et propose également une fonctionnalité supplémentaire, telle que la réplication multirégionale.

Si vous devez prendre en charge plus de 500 000 objets d'annuaire, envisagez de déployer des contrôleurs de domaine Microsoft Active Directory sur Amazon EC2. Pour le dimensionnement de ces contrôleurs de domaine, reportez-vous au document de planification des capacités pour les services de domaine Active Directory de Microsoft.

Scénario 1 : utilisation du connecteur AD pour l'authentification par proxy auprès du service Active Directory local

Ce scénario s'adresse aux clients qui ne souhaitent pas étendre leur service AD sur site à ou pour lesquels un nouveau déploiement d'AD DS n'est pas une option. AWS La figure suivante montre, à un niveau élevé, chacun des composants et le flux d'authentification utilisateur.

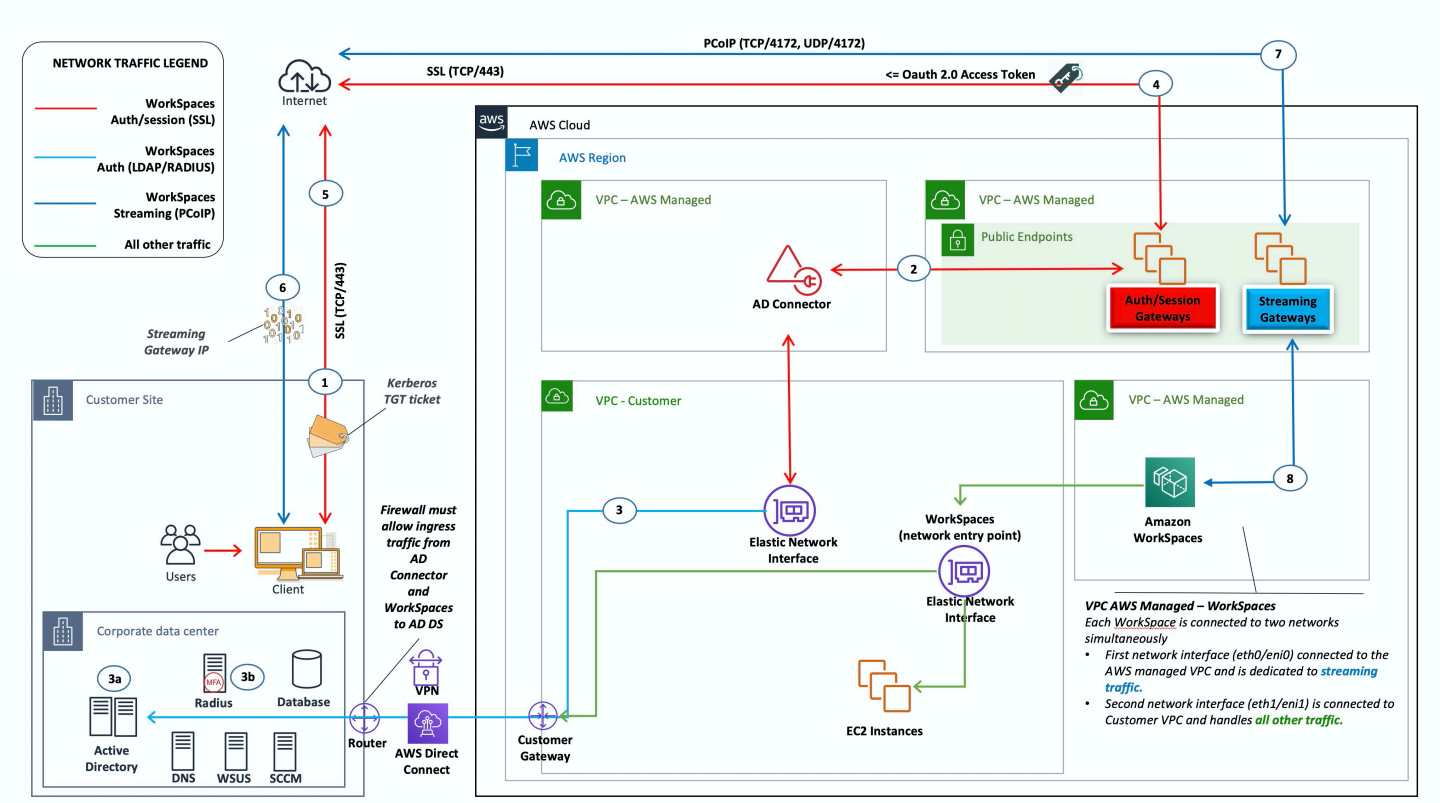

Figure 5 : AD Connector vers Active Directory sur site

Dans ce scénario, le AWS Directory Service (AD Connector) est utilisé pour toutes les authentifications utilisateur ou MFA transmises par proxy via l'AD Connector à l'AD DS sur site du client (détaillé dans la figure suivante). Pour plus de détails sur les protocoles ou le cryptage utilisés pour le processus d'authentification, reportez-vous à la Sécurité section de ce document.

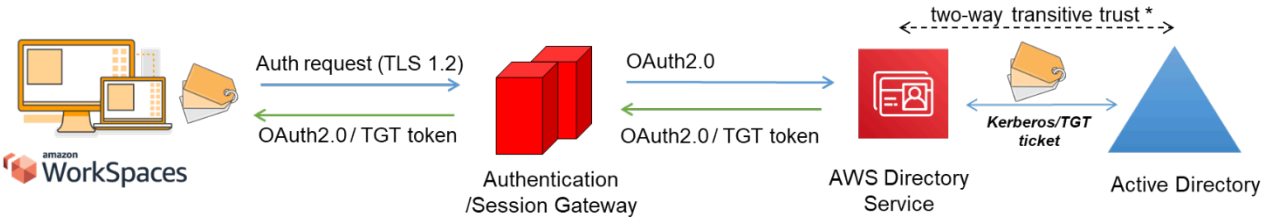

Figure 6 : Authentification des utilisateurs via la passerelle d'authentification

Le scénario 1 montre une architecture hybride dans laquelle le client possède peut-être déjà des ressources AWS, ainsi que des ressources dans un centre de données sur site accessible via Amazon WorkSpaces. Le client peut tirer parti de ses serveurs AD DS et RADIUS sur site existants pour l'authentification des utilisateurs et l'authentification MFA.

Cette architecture utilise les composants ou constructions suivants :

AWS

- Amazon VPC — Création d'un Amazon VPC avec au moins deux sous-réseaux privés répartis sur deux AZ.
- Ensemble d'options DHCP : création d'un ensemble d'options DHCP Amazon VPC. Cela permet de définir des noms de domaine et des serveurs de noms de domaine (DNS) (services sur site) spécifiés par le client. Pour plus d'informations, reportez-vous aux ensembles d'options DHCP.
- Amazon Virtual Private Gateway — Activez la communication avec votre propre réseau via un tunnel VPN IPSec ou une AWS Direct Connect connexion.
- AWS Directory Service — AD Connector est déployé dans une paire de sous-réseaux privés Amazon VPC.
- Amazon WorkSpaces : WorkSpaces sont déployés dans les mêmes sous-réseaux privés que l'AD Connector. Pour plus d'informations, reportez-vous à la section Active Directory : Sites et services de ce document.

Client

- Connectivité réseau : points de terminaison VPN d'entreprise ou Direct Connect.
- AD DS — AD DS d'entreprise.
- MFA (facultatif) : serveur RADIUS d'entreprise.
- Appareils destinés aux utilisateurs finaux : appareils destinés aux utilisateurs finaux destinés aux entreprises ou aux appareils BYOL (tels que Windows, Mac, iPad, tablettes Android, clients zéro et Chromebooks) utilisés pour accéder au service Amazon. WorkSpaces Consultez cette liste d'applications clientes pour les appareils et les navigateurs Web pris en charge.

Bien que cette solution soit idéale pour les clients qui ne souhaitent pas déployer AD DS dans le cloud, elle comporte certaines réserves :

- Dépendance accordée à la connectivité : en cas de perte de connectivité au centre de données, les utilisateurs ne peuvent pas se connecter à leurs serveurs respectifs WorkSpaces, et les connexions existantes resteront actives pendant toute la durée de vie du ticket Kerberos/Ticket Grant Ticket (TGT).

- Latence — Si la latence existe via la connexion (c'est davantage le cas avec un VPN qu'avec Direct Connect), l' WorkSpaces authentification et toute activité liée à AD DS, telle que l'application de la politique de groupe (GPO), prendront plus de temps.
- Coûts liés au trafic — Toutes les authentifications doivent passer par le VPN ou le lien Direct Connect, et cela dépend donc du type de connexion. Il s'agit soit d'un transfert de données sortant d'Amazon EC2 vers Internet, soit d'un transfert de données sortant (Direct Connect).

> **Note**
>
> AD Connector est un service proxy. Il ne stocke ni ne met en cache les informations d'identification des utilisateurs. Au lieu de cela, toutes les demandes d'authentification, de recherche et de gestion sont gérées par votre AD. Un compte doté de privilèges de délégation est requis dans votre service d'annuaire et autorisé à lire toutes les informations utilisateur et à associer un ordinateur au domaine.

En général, l' WorkSpaces expérience dépend fortement du processus d'authentification Active Directory illustré dans la figure précédente. Dans ce scénario, l'expérience WorkSpaces d'authentification dépend fortement de la liaison réseau entre l'AD du client et le WorkSpaces VPC. Le client doit s'assurer que le lien est hautement disponible.

Scénario 2 : extension des services AD DS locaux à AWS (réplique)

Ce scénario est similaire au scénario 1. Toutefois, dans ce scénario, une réplique de l'AD DS du client est déployée AWS en combinaison avec AD Connector. Cela réduit la latence des demandes d'authentification ou de requête adressées à AD DS s'exécutant sur Amazon Elastic Compute Cloud (Amazon EC2). La figure suivante montre une vue globale de chacun des composants et du flux d'authentification utilisateur.

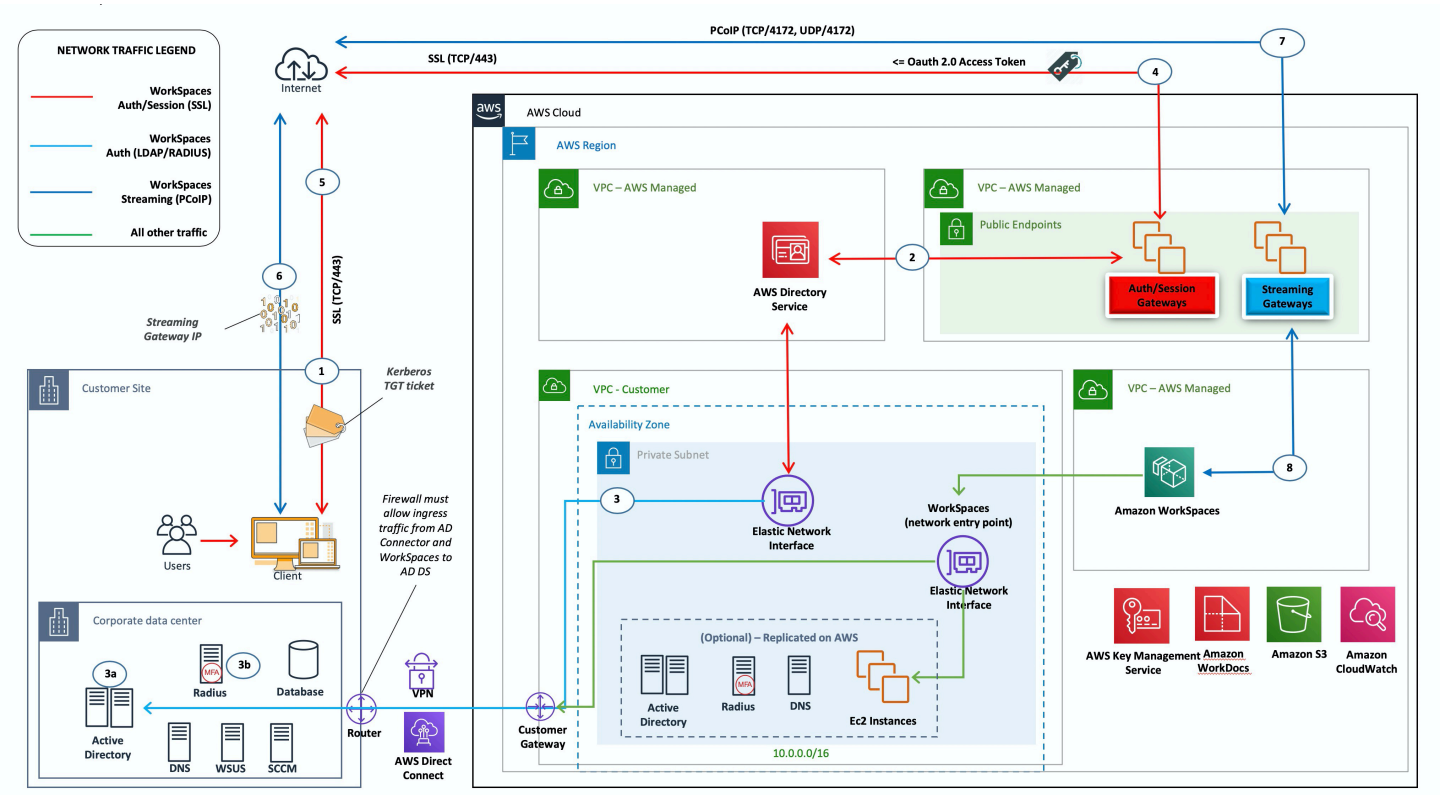

Figure 7 : Étendre le domaine Active Directory du client au cloud

Comme dans le scénario 1, AD Connector est utilisé pour toutes les authentifications utilisateur ou MFA, qui sont à leur tour transmises par proxy aux services de domaine Active Directory du client (voir la figure précédente). Dans ce scénario, les services de domaine Active Directory du client sont déployés sur des instances Amazon EC2 qui sont promues en tant que contrôleurs de domaine dans la forêt AD locale du client, s'exécutant dans le cloud. AWS Chaque contrôleur de domaine est déployé dans des sous-réseaux privés VPC afin de rendre AD DS hautement disponible dans le cloud. AWS Pour connaître les meilleures pratiques relatives au déploiement d'AD DS sur AWS, reportez-vous à la section Considérations relatives à la conception de ce document.

Une fois les WorkSpaces instances déployées, elles ont accès aux contrôleurs de domaine basés sur le cloud pour des services d'annuaire et un DNS sécurisés à faible latence. Tout le trafic réseau, y compris les communications AD DS, les demandes d'authentification et la réplication AD, est sécurisé soit au sein des sous-réseaux privés, soit via le tunnel VPN du client ou Direct Connect.

Cette architecture utilise les composants ou constructions suivants :

AWS

- Amazon VPC — Création d'un Amazon VPC avec au moins quatre sous-réseaux privés répartis sur deux AZ : deux pour les services de domaine Active Directory du client, deux pour AD Connector ou Amazon. WorkSpaces
- Ensemble d'options DHCP : création d'un ensemble d'options DHCP Amazon VPC. Cela permet au client de définir un nom de domaine et des DNS (AD DS local) spécifiés. Pour plus d'informations, reportez-vous à la section Ensembles d'options DHCP.
- Amazon Virtual Private Gateway — Activez la communication avec un réseau appartenant au client via un tunnel ou une connexion VPN IPSec. AWS Direct Connect
- Amazon EC2
  - Contrôleurs de domaine AD DS d'entreprise cliente déployés sur des instances Amazon EC2 dans des sous-réseaux VPC privés dédiés.
  - Serveurs RADIUS client (facultatif) pour le MFA sur des instances Amazon EC2 dans des sous-réseaux VPC privés dédiés.
- AWS Services d'annuaire — AD Connector est déployé dans une paire de sous-réseaux privés Amazon VPC.
- Amazon WorkSpaces : WorkSpaces sont déployés dans les mêmes sous-réseaux privés que l'AD Connector. Pour plus d'informations, reportez-vous à la section Active Directory : Sites et services de ce document.

Client

- Connectivité réseau : VPN ou AWS Direct Connect terminaux d'entreprise.

- AD DS : AD DS d'entreprise (requis pour la réplication).

- MFA (facultatif) : serveur RADIUS d'entreprise.
- Appareils utilisateur final : appareils destinés aux utilisateurs finaux professionnels ou BYOL (tels que Windows, Mac, iPad, tablettes Android, clients zéro et Chromebooks) utilisés pour accéder au service Amazon. WorkSpaces Consultez la liste des applications clientes pour les appareils et navigateurs Web pris en charge. Cette solution ne présente pas les mêmes inconvénients que le scénario 1. Amazon WorkSpaces et AWS Directory Service ne comptent pas sur la connectivité en place.

- Recours à la connectivité — En cas de perte de connectivité avec le centre de données du client, les utilisateurs finaux peuvent continuer à travailler car l'authentification et le MFA optionnel sont traités localement.
- Latence — À l'exception du trafic de réplication, toutes les authentifications sont locales et à faible latence. Reportez-vous à la section Active Directory : Sites et services de ce document.
- Coûts liés au trafic — Dans ce scénario, l'authentification est locale, seule la réplication AD DS devant passer par le VPN ou le lien Direct Connect, ce qui réduit le transfert de données.

En général, l' WorkSpaces expérience est améliorée et ne dépend pas fortement de la connectivité aux contrôleurs de domaine locaux, comme le montre la figure précédente. C'est également le cas lorsqu'un client souhaite s'adapter WorkSpaces à des milliers de postes de travail, en particulier en ce qui concerne les requêtes du catalogue global AD DS, car ce trafic reste local dans l' WorkSpaces environnement.

Scénario 3 : déploiement isolé autonome à l'aide du AWS Directory Service dans le cloud AWS

Dans ce scénario, illustré dans la figure suivante, AD DS est déployé dans le AWS cloud dans un environnement isolé autonome. AWS Directory Service est utilisé exclusivement dans ce scénario. Au lieu de gérer entièrement les services AD DS, les clients peuvent compter sur AWS Directory Service pour des tâches telles que la création d'une topologie d'annuaire hautement disponible, la surveillance des contrôleurs de domaine et la configuration des sauvegardes et des instantanés.

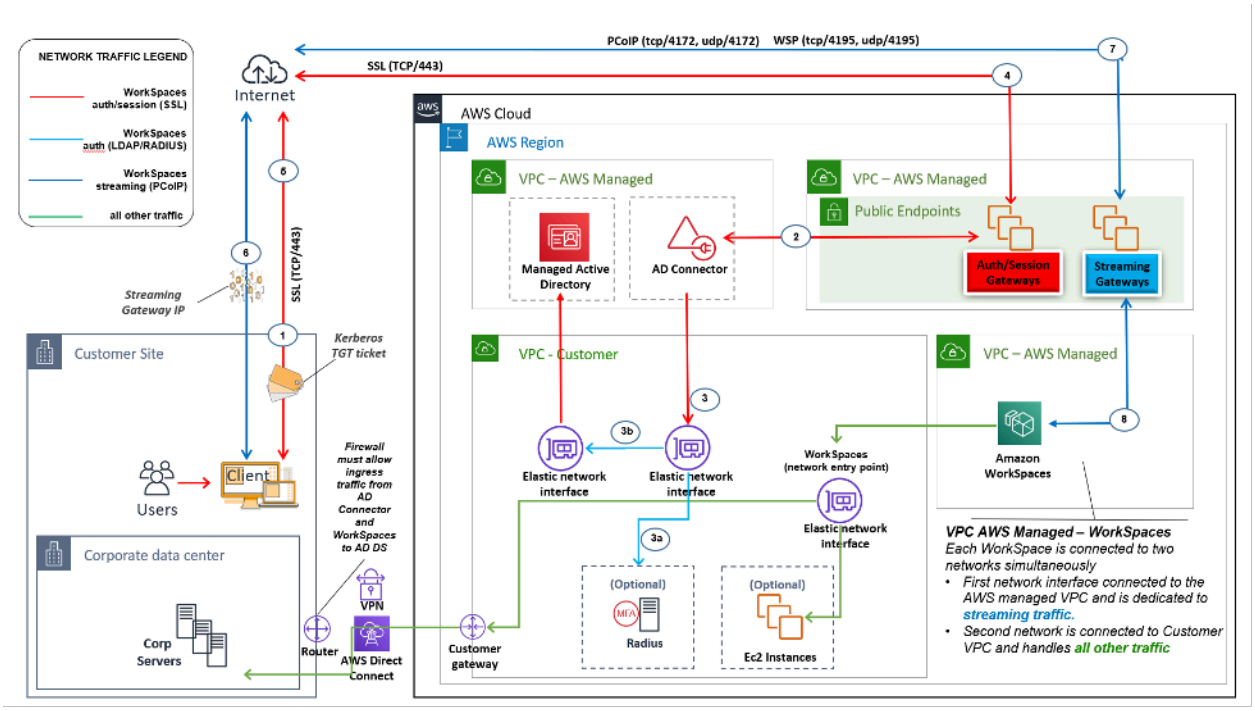

Figure 8 : Cloud uniquement : services d' AWS annuaire (Microsoft AD)

Comme dans le scénario 2, l'AD DS (Microsoft AD) est déployé dans des sous-réseaux dédiés qui s'étendent sur deux AZ, ce qui rend AD DS hautement disponible dans le AWS cloud. Outre Microsoft AD, AD Connector (dans les trois scénarios) est déployé pour WorkSpaces l'authentification ou le MFA. Cela garantit la séparation des rôles ou des fonctions au sein d'Amazon VPC, ce qui est une bonne pratique standard. Pour plus d'informations, reportez-vous à la section Considérations relatives à la conception de ce document.

Le scénario 3 est une configuration standard complète qui convient aux clients qui souhaitent AWS gérer le déploiement, les correctifs, la haute disponibilité et la surveillance du AWS Directory Service. Le scénario fonctionne également bien pour les validations de concepts, les laboratoires et les environnements de production en raison de son mode d'isolation.

Outre le placement de AWS Directory Service, cette figure montre le flux de trafic d'un utilisateur vers un espace de travail et la manière dont l'espace de travail interagit avec le serveur AD et le serveur MFA.

Cette architecture utilise les composants ou constructions suivants.

AWS

- Amazon VPC — Création d'un Amazon VPC avec au moins quatre sous-réseaux privés répartis sur deux AZ : deux pour AD DS, Microsoft AD, deux pour AD Connector ou. WorkSpaces
- Ensemble d'options DHCP : création d'un ensemble d'options DHCP Amazon VPC. Cela permet au client de définir un nom de domaine et un DNS (Microsoft AD) spécifiques. Pour plus d'informations, reportez-vous aux ensembles d'options DHCP.
- Facultatif : passerelle privée virtuelle Amazon — Activez la communication avec un réseau appartenant au client via un tunnel VPN (VPN) ou une connexion IPSec. AWS Direct Connect À utiliser pour accéder aux systèmes principaux sur site.
- AWS Directory Service : Microsoft AD est déployé dans une paire dédiée de sous-réseaux VPC (service géré AD DS).
- Amazon EC2 — Serveurs RADIUS « facultatifs » du client pour le MFA.
- AWS Services d'annuaire — AD Connector est déployé dans une paire de sous-réseaux privés Amazon VPC.
- Amazon WorkSpaces : WorkSpaces sont déployés dans les mêmes sous-réseaux privés que l'AD Connector. Pour plus d'informations, reportez-vous à la section Active Directory : Sites et services de ce document.

Client

- Facultatif : connectivité réseau — VPN d'entreprise ou AWS Direct Connect terminaux.
- Appareils utilisateur final : appareils destinés aux utilisateurs finaux professionnels ou BYOL (tels que Windows, Mac, iPad, tablettes Android, clients zéro et Chromebooks) utilisés pour accéder au service Amazon. WorkSpaces Consultez cette liste d'applications clientes pour les appareils et les navigateurs Web pris en charge.

Tout comme le scénario 2, ce scénario ne pose aucun problème en termes de dépendance à la connectivité au centre de données sur site du client, de latence ou de coûts de transfert de données sortantes (sauf lorsque l'accès à Internet est activé WorkSpaces au sein du VPC) car, de par sa conception, il s'agit d'un scénario isolé ou uniquement basé sur le cloud.

Scénario 4 : AWS Microsoft AD et une confiance transitive bidirectionnelle vers les environnements locaux

Dans ce scénario, illustré dans la figure suivante, AWS Managed AD est déployé dans le AWS cloud, avec une confiance transitive bidirectionnelle envers l'AD sur site du client. Les utilisateurs WorkSpaces sont créés dans Managed AD, l'AD Trust permettant d'accéder aux ressources dans l'environnement local.

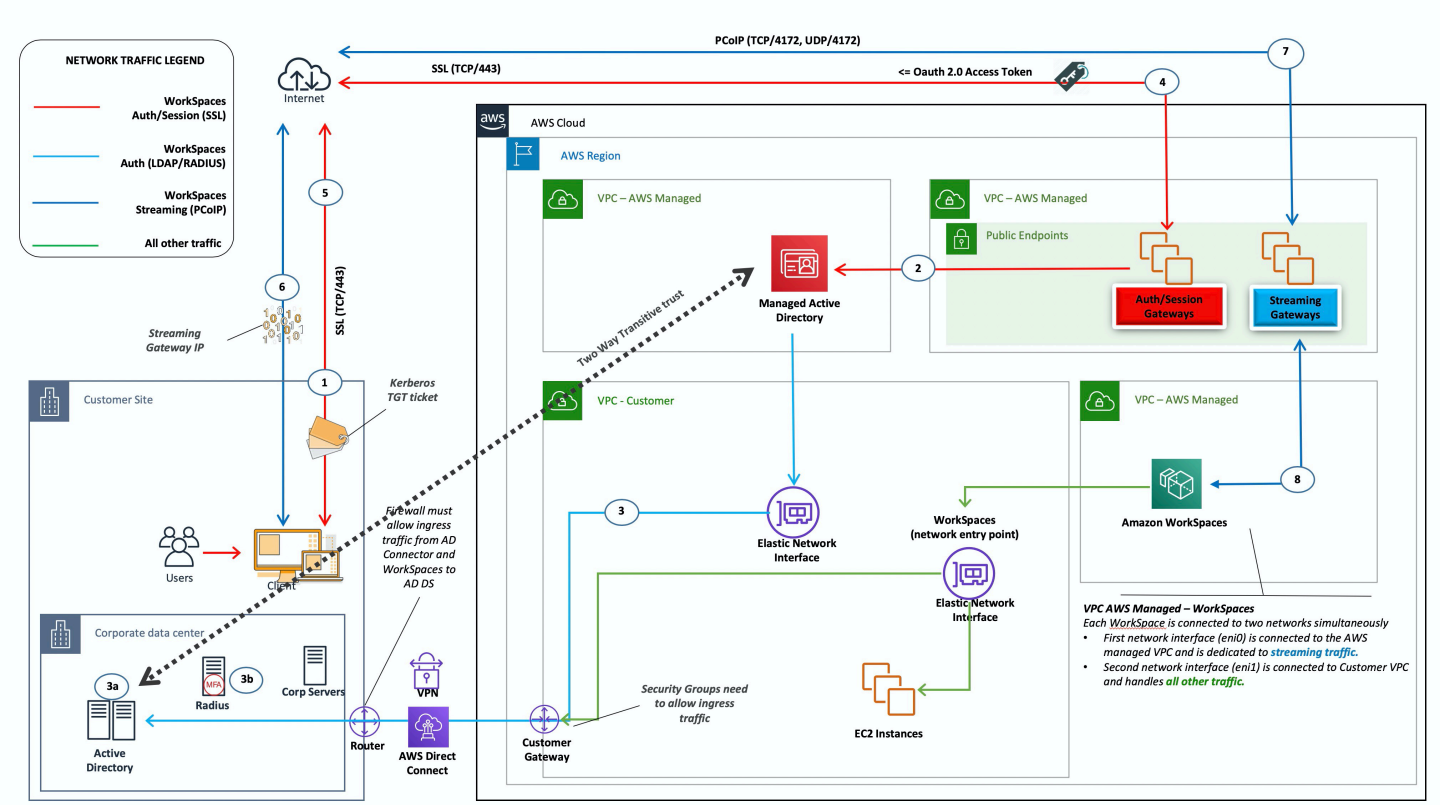

Figure 9 : AWS Microsoft AD et une confiance transitive bidirectionnelle vers les environnements locaux

Comme dans le scénario 3, l'AD DS (Microsoft AD) est déployé dans des sous-réseaux dédiés qui s'étendent sur deux AZ, ce qui rend AD DS hautement disponible dans le AWS cloud.

Ce scénario convient parfaitement aux clients qui souhaitent disposer d'un AWS Directory Service entièrement géré, y compris le déploiement, l'application de correctifs, la haute disponibilité et la surveillance de leur AWS cloud. Ce scénario permet également aux WorkSpaces utilisateurs d'accéder à des ressources associées à AD sur leurs réseaux existants. Ce scénario nécessite la mise en place d'une approbation de domaine. Les groupes de sécurité et les règles de pare-feu doivent autoriser la communication entre les deux annuaires actifs.

Outre le placement de AWS Directory Service, la figure précédente décrit le flux de trafic d'un utilisateur vers un espace de travail, ainsi que la manière dont l'espace de travail interagit avec le serveur AD et le serveur MFA.

Cette architecture utilise les composants ou constructions suivants.

AWS

- Amazon VPC — Création d'un Amazon VPC avec au moins quatre sous-réseaux privés répartis sur deux AZ : deux pour AD DS, Microsoft AD, deux pour AD Connector ou. WorkSpaces
- Ensemble d'options DHCP : création d'un ensemble d'options DHCP Amazon VPC. Cela permet au client de définir un nom de domaine et un DNS (Microsoft AD) spécifiques. Pour plus d'informations, reportez-vous aux ensembles d'options DHCP.
- Facultatif : passerelle privée virtuelle Amazon — Activez la communication avec un réseau appartenant au client via un tunnel VPN (VPN) ou une connexion IPSec. AWS Direct Connect À utiliser pour accéder aux systèmes principaux sur site.
- AWS Directory Service : Microsoft AD est déployé dans une paire dédiée de sous-réseaux VPC (service géré AD DS).

- Amazon EC2 — Serveurs RADIUS optionnels pour le client pour le MFA.
- Amazon WorkSpaces : WorkSpaces sont déployés dans les mêmes sous-réseaux privés que l'AD Connector. Pour plus d'informations, reportez-vous à la section Active Directory : Sites et services de ce document.

Client

- Connectivité réseau : VPN ou AWS Direct Connect terminaux d'entreprise.
- Appareils utilisateur final : appareils destinés aux utilisateurs finaux professionnels ou BYOL (tels que Windows, Mac, iPad, tablettes Android, clients zéro et Chromebooks) utilisés pour accéder au service Amazon. WorkSpaces Consultez la liste des applications clientes pour les appareils et navigateurs Web pris en charge.

Cette solution nécessite une connectivité au centre de données sur site du client pour permettre au processus de confiance de fonctionner. Si WorkSpaces les utilisateurs utilisent des ressources sur le réseau local, les coûts de latence et de transfert des données sortantes doivent être pris en compte.

Scénario 5 : AWS Microsoft AD utilisant un Virtual Private Cloud (VPC) à services partagés

Ce scénario, illustré dans la figure suivante, implique le déploiement d'un AD AWS géré dans le AWS cloud, fournissant des services d'authentification pour les charges de travail déjà hébergées AWS ou prévues dans le cadre d'une migration plus large. La meilleure pratique recommandée est d'installer Amazon WorkSpaces dans un VPC dédié. Les clients doivent également créer une unité AD OU spécifique pour organiser les objets WorkSpaces informatiques.

Pour effectuer un déploiement WorkSpaces avec un VPC à services partagés hébergeant Managed AD, déployez un AD Connector (ADC) avec un compte de service ADC créé dans Managed AD. Le compte de service nécessite des autorisations pour créer des objets informatiques dans l' WorkSpacesunité d'organisation désignée dans les services partagés Managed AD.

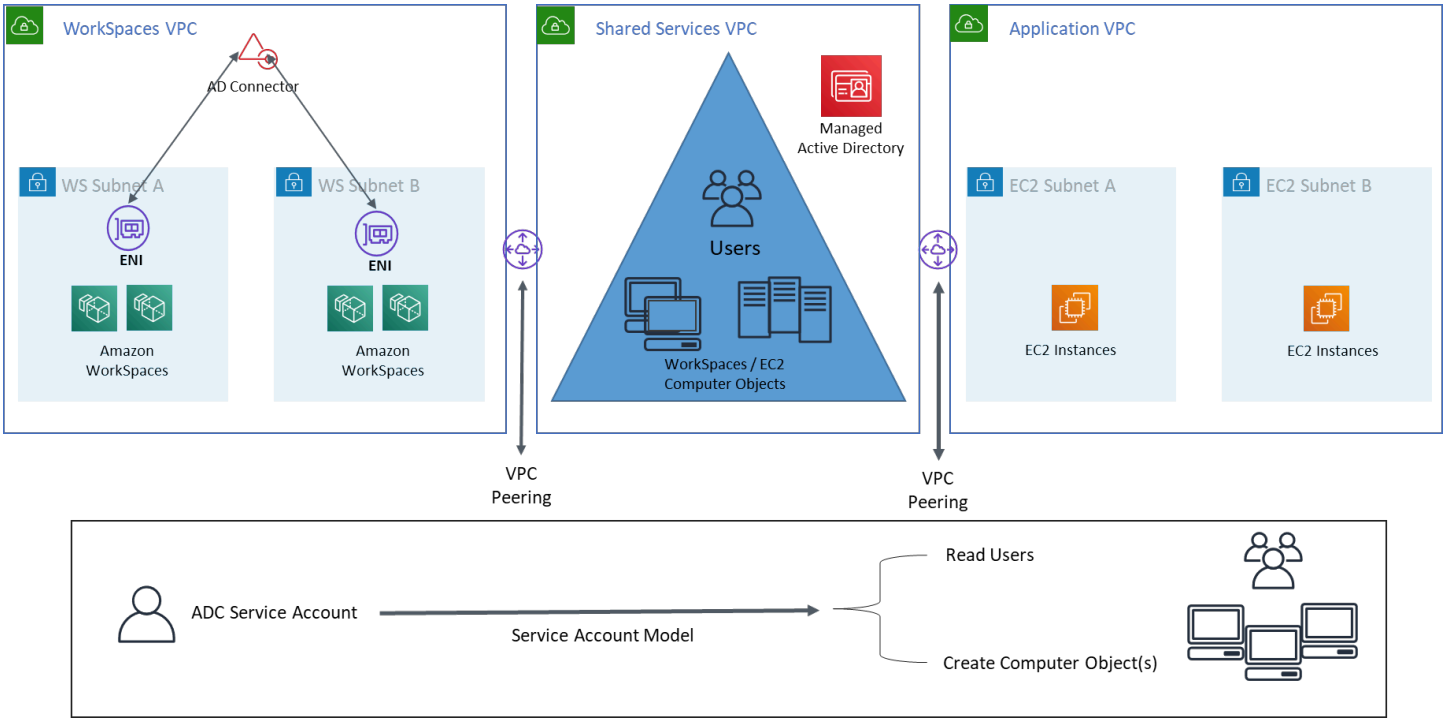

Figure 10 : AWS Microsoft AD utilisant un VPC à services partagés

Cette architecture utilise les composants ou constructions suivants.

AWS

- Amazon VPC — Création d'un Amazon VPC avec au moins deux sous-réseaux privés répartis sur deux AZ (deux pour AD Connector et). WorkSpaces

- Ensemble d'options DHCP : création d'un ensemble d'options DHCP Amazon VPC. Cela permet au client de définir un nom de domaine et un DNS (Microsoft AD) spécifiques. Pour plus d'informations, reportez-vous aux ensembles d'options DHCP.
- Facultatif : passerelle privée virtuelle Amazon — Activez la communication avec un réseau appartenant au client via un tunnel VPN (VPN) ou une connexion IPSec. AWS Direct Connect À utiliser pour accéder aux systèmes principaux sur site.
- AWS Directory Service : Microsoft AD déployé dans une paire dédiée de sous-réseaux VPC (AD DS Managed Service), AD Connector
- AWS Transit Gateway/VPC Peering : activez la connectivité entre le VPC Workspaces et le VPC Shared Services
- Amazon EC2 — Serveurs RADIUS optionnels pour le client pour le MFA.
- Amazon WorkSpaces : WorkSpaces sont déployés dans les mêmes sous-réseaux privés que l'AD Connector. Pour plus d'informations, reportez-vous à la section Active Directory : Sites et services de ce document.

Client

- Connectivité réseau : VPN ou AWS Direct Connect terminaux d'entreprise.
- Appareils utilisateur final : appareils destinés aux utilisateurs finaux professionnels ou BYOL (tels que Windows, Mac, iPad, tablettes Android, clients zéro et Chromebooks) utilisés pour accéder au service Amazon. WorkSpaces Consultez la liste des applications clientes pour les appareils et navigateurs Web pris en charge.

Scénario 6 : AWS Microsoft AD, VPC à services partagés et confiance unidirectionnelle sur site

Ce scénario, comme illustré dans la figure suivante, utilise un Active Directory local existant pour les utilisateurs et introduit un Active Directory géré distinct dans le AWS cloud pour héberger les objets informatiques associés au WorkSpaces. Ce scénario permet de gérer les objets informatiques et les politiques de groupe Active Directory indépendamment de l'Active Directory d'entreprise.

Ce scénario est utile lorsqu'un tiers souhaite gérer Windows pour WorkSpaces le compte d'un client, car il permet au tiers de définir et de contrôler les WorkSpaces politiques qui lui sont associées, sans qu'il soit nécessaire de lui accorder l'accès à l'AD du client. Dans ce scénario, une unité

organisationnelle (UO) Active Directory spécifique est créée pour organiser les objets WorkSpaces informatiques dans Shared Services AD.

> **Note**
>
> Amazon Linux a WorkSpaces besoin d'une confiance bidirectionnelle pour pouvoir être créés.

Pour déployer Windows WorkSpaces avec les objets informatiques créés dans le VPC Shared Services hébergeant Managed Active Directory en utilisant des utilisateurs du domaine d'identité du client, déployez un connecteur Active Directory (ADC) référençant l'AD de l'entreprise. Utilisez un compte de service ADC créé dans l'AD d'entreprise (domaine d'identité) doté d'autorisations déléguées pour créer des objets informatiques dans l'unité organisationnelle (UO) configurée pour Windows WorkSpaces dans l'AD géré par Shared Services et disposant d'autorisations de lecture sur l'Active Directory d'entreprise (domaine d'identité).

Pour garantir que la fonction Domain Locator est en mesure d'authentifier WorkSpaces les utilisateurs sur le site AD souhaité pour le domaine d'identité, nommez les sites AD des deux domaines pour les WorkSpaces sous-réseaux Amazon de la même manière, conformément à la documentation de Microsoft. Il est recommandé d'avoir à la fois des contrôleurs de domaine AD de domaine d'identité et de domaine de services partagés dans la même AWS région qu'Amazon WorkSpaces.

Pour obtenir des instructions détaillées sur la configuration de ce scénario, consultez le guide de mise en œuvre pour configurer une confiance unidirectionnelle pour Amazon WorkSpaces avec AWS Directory Services

Dans ce scénario, nous établissons une confiance transitive unidirectionnelle entre le AWS Managed Microsoft AD VPC Shared Services et l'AD sur site. La figure 11 montre le sens de la confiance et de l'accès, ainsi que la manière dont l' AWS AD Connector utilise le compte de service AD Connector pour créer des objets informatiques dans le domaine des ressources.

Une approbation forestière est utilisée conformément aux recommandations de Microsoft pour garantir que l'authentification Kerberos est utilisée dans la mesure du possible. WorkSpaces Vous recevez des objets de stratégie de groupe (GPO) de votre domaine de ressources dans le AWS Managed Microsoft AD. De plus, vous WorkSpaces effectuez une authentification Kerberos avec votre domaine d'identité. Pour que cela fonctionne de manière fiable, il est recommandé d'étendre votre domaine d'identité AWS comme indiqué ci-dessus. Pour plus de détails, nous vous suggérons

de consulter le guide de mise en AWS Directory Service œuvre Deploy Amazon WorkSpaces using a One-Way Trust Resource Domain with One-Way.

L'AD Connector et le vôtre WorkSpaces doivent tous deux être en mesure de communiquer avec les contrôleurs de domaine de votre domaine d'identité et de votre domaine de ressources. Pour plus d'informations, consultez les exigences en matière d'adresse IP et de port WorkSpaces dans le guide d' WorkSpaces administration Amazon.

Si vous utilisez plusieurs connecteurs AD, il est recommandé que chacun d'eux utilise son propre compte de service AD Connector.

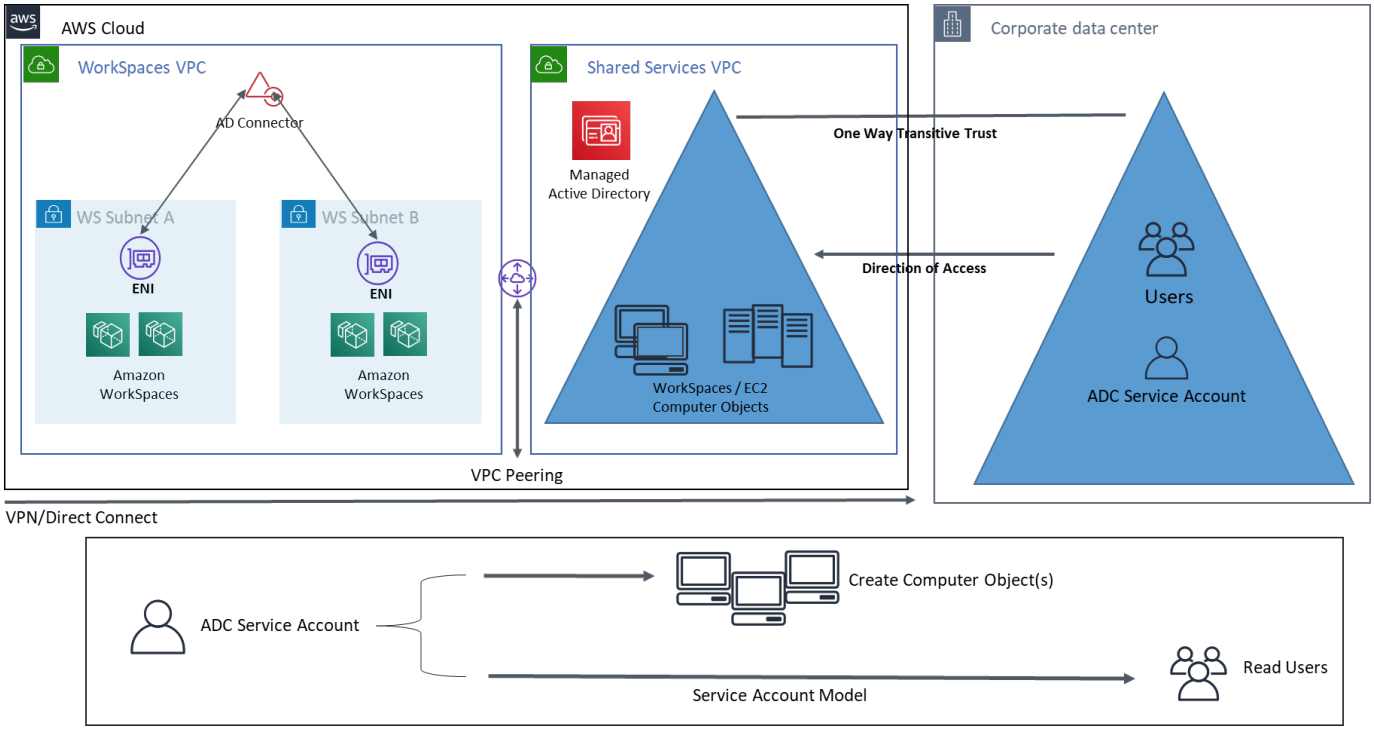

Figure 11 : AWS Microsoft, VPC à services partagés et confiance unidirectionnelle envers AD sur site

Cette architecture utilise les composants ou constructions suivants :

AWS

- Amazon VPC — Création d'un Amazon VPC avec au moins deux sous-réseaux privés répartis sur deux AZ : deux pour AD Connector et. WorkSpaces
- Ensemble d'options DHCP : création d'un ensemble d'options DHCP Amazon VPC. Cela permet au client de définir un nom de domaine et un DNS (Microsoft AD) spécifiques. Pour plus d'informations, reportez-vous aux ensembles d'options DHCP.

- Facultatif : passerelle privée virtuelle Amazon — Activez la communication avec un réseau appartenant au client via un tunnel VPN (VPN) ou une connexion IPSec. AWS Direct Connect À utiliser pour accéder aux systèmes principaux sur site.
- AWS Directory Service : Microsoft AD est déployé dans une paire dédiée de sous-réseaux VPC (AD DS Managed Service), AD Connector.
- Transit Gateway/VPC Peering : activez la connectivité entre le VPC Workspaces et le VPC Shared Services.
- Amazon EC2 — Serveurs RADIUS « facultatifs » du client pour le MFA.
- Amazon WorkSpaces : WorkSpaces sont déployés dans les mêmes sous-réseaux privés que l'AD Connector. Pour plus d'informations, reportez-vous à la section Active Directory : Sites et services de ce document.

Client

- Connectivité réseau : VPN ou AWS Direct Connect terminaux d'entreprise.
- Appareils utilisateur final : appareils destinés aux utilisateurs finaux professionnels ou BYOL (tels que Windows, Mac, iPad, tablettes Android, clients zéro et Chromebooks) utilisés pour accéder au service Amazon. WorkSpaces Consultez cette liste d'applications clientes pour les appareils et les navigateurs Web pris en charge.

Utilisation d'Active Directory AWS géré par plusieurs régions avec Amazon WorkSpaces

AWS Directory Service for Microsoft Active Directory (MAD) est un service Microsoft Active Directory (AD) entièrement géré qui peut être associé à Amazon WorkSpaces. Les clients choisissent AWS Managed Microsoft AD car il intègre une haute disponibilité, une surveillance et des sauvegardes. AWS L'édition Managed Microsoft AD Enterprise ajoute la possibilité de configurer la réplication multirégionale. Cette fonctionnalité configure automatiquement la connectivité réseau interrégionale, déploie des contrôleurs de domaine et réplique toutes les données Active Directory dans plusieurs régions, garantissant ainsi que les charges de travail Windows et Linux résidant dans ces régions peuvent se connecter à AWS MAD et l'utiliser avec une faible latence et des performances élevées. Les régions MAD répliquées ne peuvent pas être enregistrées directement auprès de celles-ci WorkSpaces, mais un répertoire MAD répliqué peut être enregistré WorkSpaces en configurant un AD Connector (ADC) pour qu'il pointe vers vos contrôleurs de domaine répliqués.

La meilleure pratique lors du déploiement de connecteurs AD avec MAD consiste à créer un connecteur AD pour chaque unité commerciale de votre WorkSpaces environnement. Cela vous permettra d'aligner chaque unité commerciale sur une unité organisationnelle spécifique au sein d'Active Directory. Vous pouvez ensuite attribuer des objets de stratégie de groupe AD au niveau de l'unité organisationnelle qui correspondent directement à l'unité commerciale en question.

Architecture

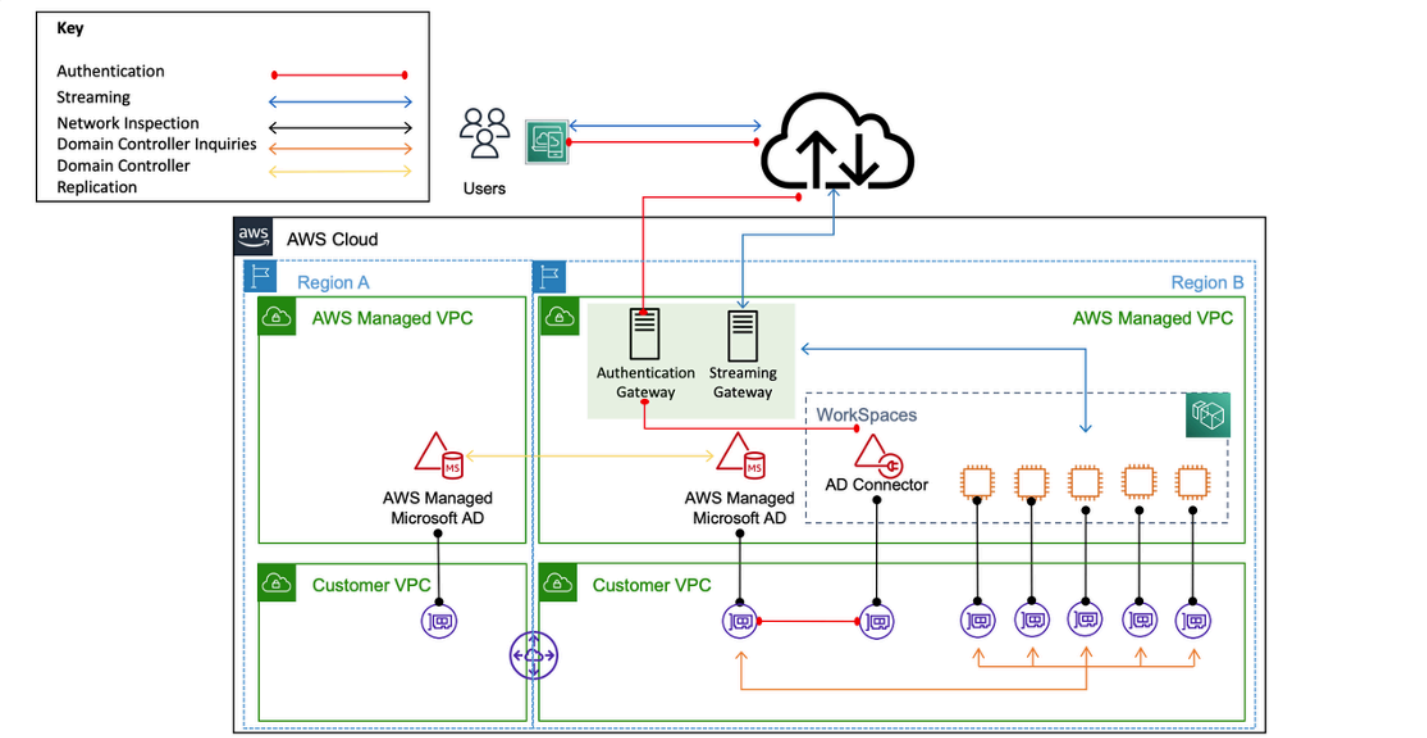

Figure 12 : Exemple d'architecture pour enregistrer une région MAD répliquée dans un WorkSpace

Mise en œuvre

Pour enregistrer votre région MAD répliquée dans WorkSpaces, vous devez créer un connecteur AD pointé vers les adresses IP de votre contrôleur de domaine MAD. Vous pouvez trouver les adresses IP de vos contrôleurs de domaine MAD en accédant au volet de navigation de la console AWS Directory Service, en sélectionnant Directories, puis en choisissant le bon ID de répertoire. Pour créer ces connecteurs AD, suivez ce guide. Une fois qu'ils sont créés, vous pouvez les enregistrer pour WorkSpaces. Avant de procéder WorkSpaces au déploiement dans votre nouvelle région, assurez-vous d'avoir mis à jour le jeu d'options DHCP de votre VPC.

Considérations relatives à la conception

Un déploiement AD DS fonctionnel dans le AWS cloud nécessite une bonne compréhension des concepts d'Active Directory et des AWS services spécifiques. Cette section aborde les principales considérations de conception lors du déploiement d'AD DS pour Amazon WorkSpaces, les meilleures pratiques en matière de VPC en matière de AWS Directory Service, les exigences DHCP et DNS, les spécificités de l'AD Connector, ainsi que les sites et services AD.

Conception en VPC

Comme indiqué précédemment dans la section Considérations relatives au réseau de ce document et comme décrit précédemment pour les scénarios 2 et 3, les clients doivent déployer AD DS dans le AWS cloud dans une paire dédiée de sous-réseaux privés, répartis sur deux AZ, et séparés de l'AD Connector ou des WorkSpaces sous-réseaux. Cette structure fournit un accès à haute disponibilité et à faible latence aux services AD DS WorkSpaces, tout en respectant les meilleures pratiques standard en matière de séparation des rôles ou des fonctions au sein d'Amazon VPC.

La figure suivante montre la séparation d'AD DS et d'AD Connector en sous-réseaux privés dédiés (scénario 3). Dans cet exemple, tous les services résident dans le même Amazon VPC.

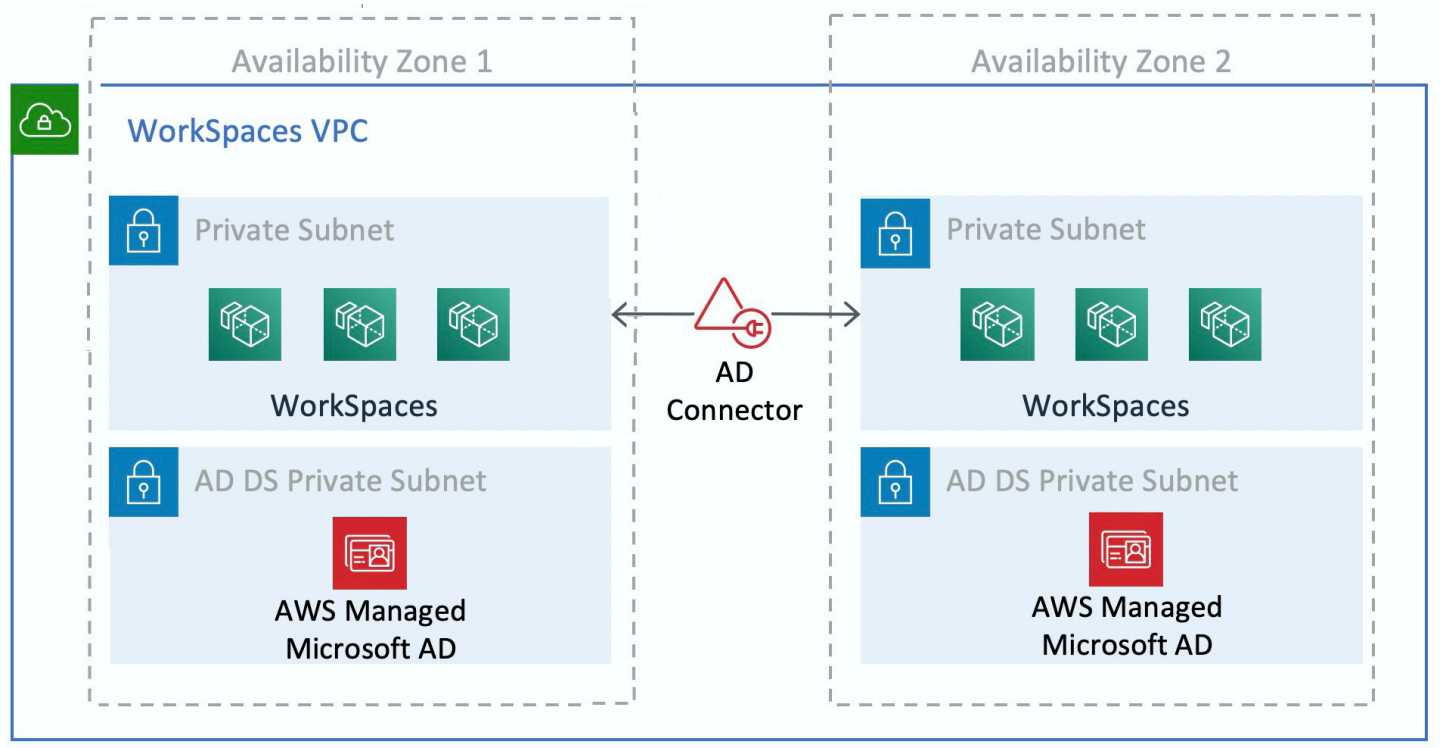

Figure 13 : Séparation du réseau AD DS

La figure suivante montre une conception similaire au scénario 1 ; toutefois, dans ce scénario, la partie locale réside dans un Amazon VPC dédié.

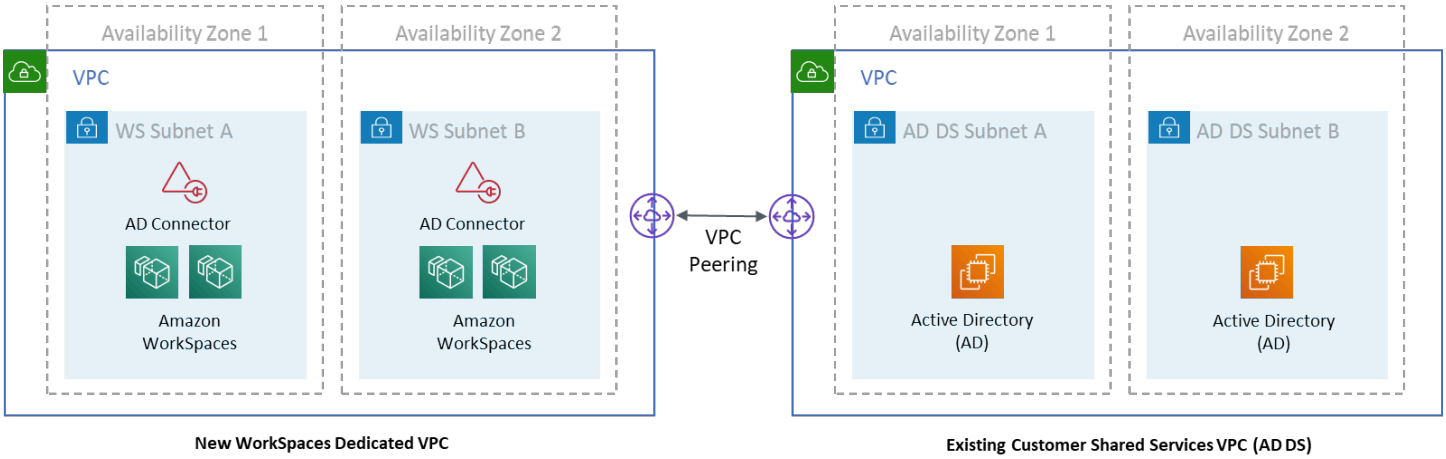

Figure 14 : WorkSpaces VPC dédié

> **Note**
>
> Pour les clients disposant d'un AWS déploiement existant dans lequel AD DS est utilisé, il est recommandé de le localiser WorkSpaces dans un VPC dédié et d'utiliser le peering VPC pour les communications AD DS.

Outre la création de sous-réseaux privés dédiés pour les services AD DS, les contrôleurs de domaine et les serveurs membres nécessitent plusieurs règles de groupe de sécurité pour autoriser le trafic pour les services, tels que la réplication AD DS, l'authentification des utilisateurs, les services Windows Time et le système de fichiers distribué (DFS).

> **Note**
>
> La meilleure pratique consiste à limiter les règles de groupe de sécurité requises aux sous-réseaux WorkSpaces privés et, dans le cas du scénario 2, à autoriser les communications AD DS bidirectionnelles sur site vers et depuis le AWS cloud, comme indiqué dans le tableau suivant.

Tableau 1 — Communications AD DS bidirectionnelles vers et depuis le cloud AWS

Protocole	Port	Utiliser	Destination
TCP	53, 88, 135, 139, 389, 445, 464, 636	Auth (principal)	Active Directory (centre de données privé ou Amazon EC2) *
TCP	49152 — 65535	Ports RPC à haut débit	Active Directory (centre de données privé ou Amazon EC2) **
TCP	3268-3269	Fiducies	Active Directory (centre de données privé ou Amazon EC2) *
TCP	9389	Microsoft Windows à distance PowerShell (facultatif)	Active Directory (centre de données privé ou Amazon EC2) *
UDP	53, 88, 123, 137, 138, 389, 445, 464	Auth (principal)	Active Directory (centre de données privé ou Amazon EC2) *
UDP	1812	Auth (MFA) (facultatif)	RADIUS (centre de données privé ou Amazon EC2) *

Pour plus d'informations, reportez-vous à la section Exigences relatives aux ports d'Active Directory et aux services de domaine Active Directory, à la présentation des services et aux exigences relatives aux ports réseau pour Windows

Pour step-by-step obtenir des conseils sur la mise en œuvre des règles, reportez-vous à la section Ajouter des règles à un groupe de sécurité dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

Conception de VPC : DHCP et DNS

Avec un Amazon VPC, les services DHCP (Dynamic Host Configuration Protocol) sont fournis par défaut pour vos instances. Par défaut, chaque VPC fournit un serveur DNS (Domain Name System) interne accessible via l'espace d'adressage CIDR (Classless Inter-Domain Routing) +2, et attribué à toutes les instances via un ensemble d'options DHCP par défaut.

Les ensembles d'options DHCP sont utilisés au sein d'un Amazon VPC pour définir les options d'étendue, telles que le nom de domaine ou les serveurs de noms qui doivent être transmis aux instances du client via DHCP. Le bon fonctionnement des services Windows au sein d'un VPC client dépend de cette option d'étendue DHCP. Dans chacun des scénarios définis précédemment, les clients créent et attribuent leur propre étendue qui définit le nom de domaine et les serveurs de noms. Cela garantit que les instances Windows jointes au domaine WorkSpaces sont configurées pour utiliser le DNS AD.

Le tableau suivant est un exemple d'un ensemble personnalisé d'options d'étendue DHCP qui doivent être créées pour qu'Amazon WorkSpaces et AWS Directory Services fonctionnent correctement.

Tableau 2 — Ensemble personnalisé d'options d'étendue DHCP

Paramètre	Valeur
Identification de nom	Crée une balise avec key = nom et valeur définies sur une chaîne spécifique Exemple : example.com
Nom de domaine	example.com
Serveurs de noms de domaine	Adresse du serveur DNS, séparée par des virgules Exemple : 192.0.2.10, 192.0.2.21
Serveurs NTP	Laissez ce champ vide

Paramètre	Valeur
Serveur de nom NetBIOS	Entrez les mêmes adresses IP séparées par des virgules que pour les serveurs de noms de domaine Exemple : 192.0.2.10, 192.0.2.21
Type de nœud NetBIOS	2

Pour en savoir plus sur la création d'un ensemble d'options DHCP personnalisé et son association à un Amazon VPC, reportez-vous à la section Utilisation des ensembles d'options DHCP du guide de l'utilisateur Amazon Virtual Private Cloud.

Dans le scénario 1, l'étendue DHCP serait le DNS ou AD DS sur site. Toutefois, dans les scénarios 2 ou 3, il s'agirait du service d'annuaire déployé localement (AD DS sur Amazon EC2 ou AWS Directory Services : Microsoft AD). Il est recommandé que chaque contrôleur de domaine résidant dans le AWS cloud soit un catalogue global et un serveur DNS intégré à un annuaire.

Active Directory : sites et services

Dans le scénario 2, les sites et les services sont des composants essentiels au bon fonctionnement d'AD DS. La topologie du site contrôle la réplication AD entre les contrôleurs de domaine au sein d'un même site et au-delà des limites du site. Dans le scénario 2, au moins deux sites sont présents : sur site et Amazon WorkSpaces dans le cloud.

La définition de la topologie de site correcte garantit l'affinité avec les clients, ce qui signifie que les clients (dans ce cas WorkSpaces) utilisent leur contrôleur de domaine local préféré.

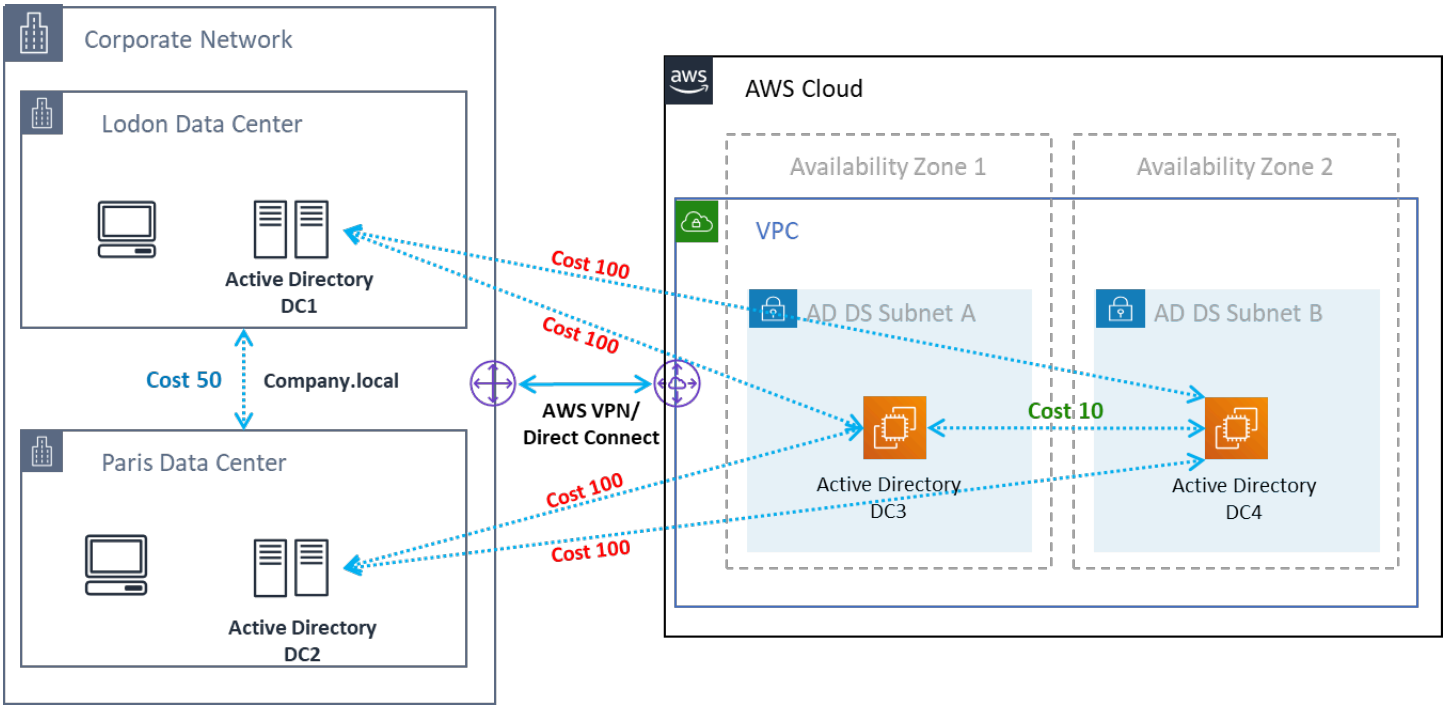

Figure 15 : Sites et services Active Directory : affinité avec les clients

Bonne pratique : définissez le coût élevé des liens de site entre les services AD DS locaux et le AWS cloud. La figure suivante est un exemple des coûts à attribuer aux liens du site (coût 100) pour garantir une affinité client indépendante du site.

Ces associations permettent de garantir que le trafic, tel que la réplication AD DS et l'authentification du client, utilise le chemin le plus efficace vers un contrôleur de domaine. Dans le cas des scénarios 2 et 3, cela permet de réduire la latence et le trafic de liaisons croisées.

Protocole

Amazon WorkSpaces Streaming Protocol (WSP) est un protocole de streaming natif dans le cloud qui permet une expérience utilisateur cohérente sur des distances mondiales et sur des réseaux peu fiables. WSP dissocie le protocole du en déléguant l'analyse métrique, le WorkSpaces codage, l'utilisation et la sélection des codecs. WSP utilise le port TCP/UDP 4195. Au moment de décider d'utiliser ou non le protocole WSP, il convient de répondre à plusieurs questions clés avant le déploiement. Veuillez vous référer à la matrice de décision ci-dessous :

Question	WSP	PCoIP
Les WorkSpaces utilisateurs identifiés auront-ils besoin d'un système audio/vidéo bidirecti onnel ?	•	
Aucun client ne sera-t-il utilisé comme point de terminaison distant (appareil local) ?		•
Windows ou macOS seront-ils utilisés pour les terminaux distants ?	•	•
Ubuntu 18.04 sera-t-il utilisé comme point de terminaison distant ?		•
Les utilisateurs accèderont-ils à Amazon WorkSpaces via un accès Web ?		•
La prise en charge des cartes à puce avant ou pendant la session (PIC/CAC) est-elle nécessaire ?	•	
Sera-t-il WorkSpaces utilisé dans la région de Chine (Ningxia) ?		•
Une pré-authentification par carte à puce ou une assistanc e en cours de session seront-elles nécessaires ?	•	
Les utilisateurs finaux utilisent-ils des connexions peu fiables,	•	

Question	WSP	PCoIP
à latence élevée ou à faible bande passante ?		

Les questions précédentes sont essentielles pour déterminer le protocole à utiliser. Des informations supplémentaires sur les cas d'utilisation du protocole recommandés peuvent être consultées ici. Le protocole utilisé peut également être modifié ultérieurement à l'aide de la fonctionnalité Amazon WorkSpaces Migrate. Plus d'informations sur l'utilisation de cette fonctionnalité peuvent être consultées ici.

Lors d'un déploiement WorkSpaces à l'aide du WSP, les passerelles WSP doivent être ajoutées à une liste d'autorisation pour garantir la connectivité au service. De plus, pour les utilisateurs qui se connectent à un WorkSpaces WSP, le temps d'aller-retour (RTT) doit être inférieur à 250 ms pour de meilleures performances. Les connexions avec un RTT compris entre 250 ms et 400 ms seront dégradées. Si la connexion de l'utilisateur est constamment dégradée, il est recommandé de déployer un Amazon WorkSpaces dans la région prise en charge la plus proche de l'utilisateur final, si possible.

Multi-Factor Authentication (MFA)

La mise en œuvre de la MFA WorkSpaces nécessite qu'Amazon soit configuré avec un connecteur Active Directory (AD Connector) ou Managed AWS Microsoft AD (MAD) comme service d'annuaire, et qu'il dispose d'un serveur RADIUS accessible en réseau par le service d'annuaire. Simple Active Directory ne prend pas en charge le MFA.

Reportez-vous à la section précédente, qui traite des considérations relatives au déploiement d'Active Directory et des services d'annuaire pour AD, ainsi que des options de conception RADIUS dans chaque scénario.

MFA — Authentification à deux facteurs

Une fois l'authentification MFA activée, les utilisateurs doivent fournir leur nom d'utilisateur, leur mot de passe et leur code MFA au WorkSpaces client pour l'authentification sur leurs postes de travail respectifs. WorkSpaces

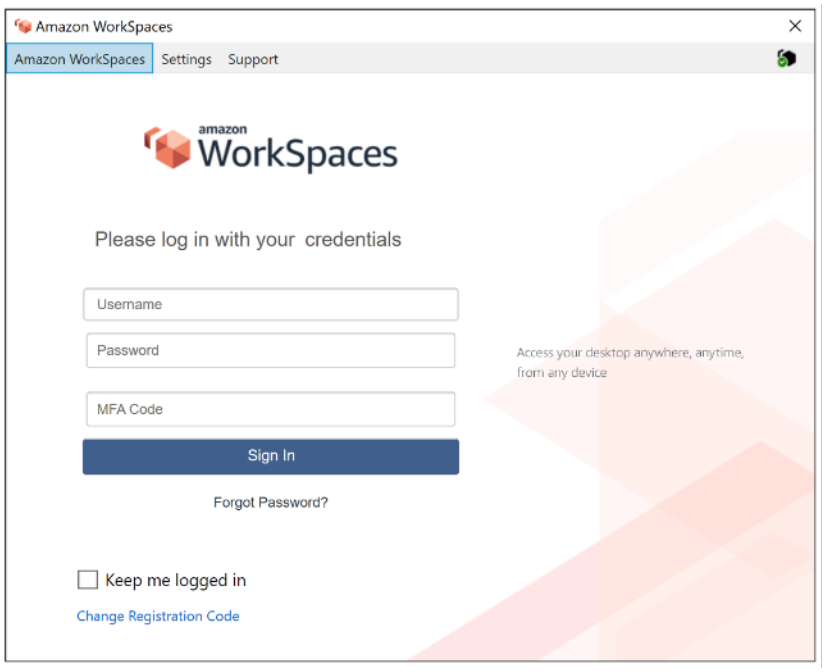

Figure 16 : WorkSpaces client avec MFA activée

> **Note**
>
> Le AWS Directory Service ne prend pas en charge le MFA sélectif par utilisateur ou contextuel : il s'agit d'un paramètre global par annuaire. Si une MFA sélective « par utilisateur » est requise, les utilisateurs doivent être séparés par un AD Connector, qui peut pointer vers la même source Active Directory.

WorkSpaces La MFA nécessite un ou plusieurs serveurs RADIUS. Il s'agit généralement de solutions existantes que vous avez peut-être déjà déployées, par exemple RSA ou Gemalto. Les serveurs RADIUS peuvent également être déployés au sein de votre VPC sur des instances EC2 (reportez-vous à la section Scénarios de déploiement AD DS de ce document pour connaître les options architecturales). Si vous déployez une nouvelle solution RADIUS, plusieurs implémentations existent, telles que FreeRADIUS, ainsi que des offres SaaS telles que Duo Security ou Okta MFA.

Il est recommandé de tirer parti de plusieurs serveurs RADIUS pour garantir la résilience de votre solution en cas de panne. Lorsque vous configurez votre Directory Service pour le MFA, vous pouvez saisir plusieurs adresses IP en les séparant par une virgule (par exemple, 192.0.0.0,192.0.0.12). La fonctionnalité MFA des services d'annuaire essaiera la première adresse IP spécifiée et passera à la deuxième adresse IP si la connectivité réseau ne peut pas être établie avec la première. La configuration de RADIUS pour une architecture à haute disponibilité est propre à chaque ensemble

de solutions, mais la principale recommandation est de placer les instances sous-jacentes de votre fonctionnalité RADIUS dans différentes zones de disponibilité. Duo Security est un exemple de configuration. Pour Okta MFA, vous pouvez déployer plusieurs agents de serveur Okta RADIUS de la même manière.

Pour connaître les étapes détaillées relatives à l'activation de votre AWS Directory Service pour le MFA, reportez-vous aux sections AD Connector et Managed AWS Microsoft AD.

Reprise après sinistre/Continuité des activités

WorkSpaces Redirection entre régions

Amazon WorkSpaces est un service régional qui fournit un accès à distance aux postes de travail aux clients. En fonction des exigences en matière de continuité des activités et de reprise après sinistre (BC/DR), certains clients ont besoin d'un basculement fluide vers une autre région où le WorkSpaces service est disponible. Cette exigence BC/DR peut être satisfaite à l'aide de l'option de redirection WorkSpaces entre régions. Il permet aux clients d'utiliser un nom de domaine complet (FQDN) comme code d' WorkSpaces enregistrement.

Il est important de déterminer à quel moment une redirection vers une région de basculement doit avoir lieu. Les critères de cette décision doivent être basés sur la politique de votre entreprise, mais doivent inclure l'objectif de temps de reprise (RTO) et l'objectif de point de reprise (RPO). La conception d'une architecture WorkSpaces Well-Architected doit inclure le risque de défaillance du service. La tolérance temporelle pour le rétablissement normal des activités commerciales sera également prise en compte dans la décision.

Lorsque vos utilisateurs finaux se connectent WorkSpaces avec un FQDN comme code WorkSpaces d'enregistrement, un enregistrement DNS TXT contenant un identifiant de connexion déterminant le répertoire enregistré vers lequel l'utilisateur sera dirigé est résolu. La page d'accueil de connexion du WorkSpaces client sera ensuite présentée en fonction du répertoire enregistré associé à l'identifiant de connexion renvoyé. Cela permet aux administrateurs de diriger leurs utilisateurs finaux vers différents WorkSpaces répertoires en fonction de vos politiques DNS pour le FQDN. Cette option peut être utilisée avec des zones DNS publiques ou privées, en supposant que les zones privées peuvent être résolues à partir de la machine cliente. La redirection entre régions peut être manuelle ou automatisée. Ces deux basculements peuvent être réalisés en modifiant l'enregistrement TXT contenant l'identifiant de connexion pour qu'il pointe vers le répertoire souhaité.

Lorsque vous développez votre stratégie BC/DR, il est important de prendre en compte les données utilisateur, car l'option de redirection WorkSpaces entre régions ne synchronise aucune donnée

utilisateur, pas plus qu'elle ne synchronise vos images. WorkSpaces Vos WorkSpaces déploiements dans différentes AWS régions sont des entités indépendantes. Vous devrez donc prendre des mesures supplémentaires pour garantir que vos WorkSpaces utilisateurs puissent accéder à leurs données lors d'une redirection vers une région secondaire. De nombreuses options sont disponibles pour la réplication des données utilisateur WorkSpaces, telles que Windows FSx (DFS Share) ou des utilitaires tiers pour synchroniser les volumes de données entre les régions. De même, vous devez vous assurer que votre région secondaire a accès aux WorkSpaces images requises, par exemple en copiant les images d'une région à l'autre. Pour plus d'informations, consultez la section Redirection entre régions pour Amazon WorkSpaces dans le guide d' WorkSpaces administration Amazon et l'exemple dans le schéma.

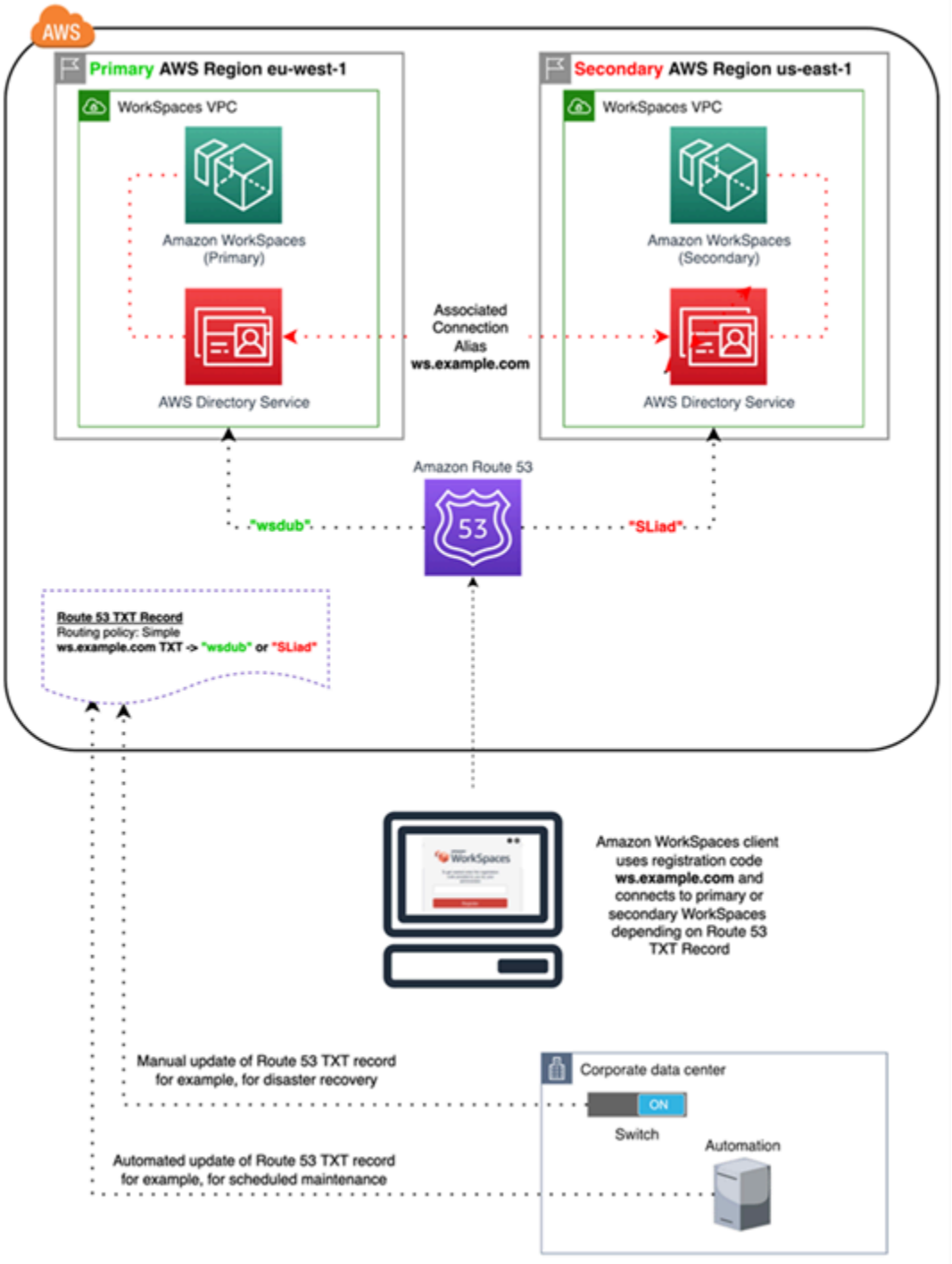

Figure 17 : Exemple de redirection WorkSpaces entre régions avec Amazon Route 53

WorkSpaces Interface VPC Endpoint (AWS PrivateLink) — Appels d'API

Les API WorkSpaces publiques d'Amazon sont prises en charge sur AWS PrivateLink. AWS PrivateLink augmente la sécurité des données partagées avec des applications basées sur le cloud en réduisant l'exposition des données à l'Internet public. WorkSpaces Le trafic d'API peut être sécurisé au sein d'un VPC à l'aide d'un point de terminaison d'interface, qui est une interface elastic network dotée d'une adresse IP privée issue de la plage d'adresses IP de votre sous-réseau qui sert de point d'entrée pour le trafic destiné à un service pris en charge. Cela vous permet d'accéder de manière privée aux services WorkSpaces API en utilisant des adresses IP privées.

L'utilisation PrivateLink avec des API WorkSpaces publiques vous permet également d'exposer en toute sécurité les API REST aux ressources uniquement de votre VPC ou à celles connectées à vos centres de données via. AWS Direct Connect

Vous pouvez restreindre l'accès à certains Amazon VPC et points de terminaison VPC, et activer l'accès entre comptes en utilisant des politiques spécifiques aux ressources.

Assurez-vous que le groupe de sécurité associé à l'interface réseau du point de terminaison autorise la communication entre l'interface réseau du point de terminaison et les ressources de votre VPC qui communiquent avec le service. Si le groupe de sécurité restreint le trafic HTTPS entrant (port 443) provenant des ressources du VPC, il se peut que vous ne puissiez pas envoyer de trafic via l'interface réseau du point de terminaison. Un point de terminaison d'interface prend uniquement en charge le trafic TCP.

- Les points de terminaison prennent en charge le trafic IPv4 uniquement.
- Quand vous créez un point de terminaison, vous pouvez lui attacher une stratégie de point de terminaison qui contrôle l'accès au service auquel vous vous connectez.
- Vous êtes soumis à un quota pour le nombre de points de terminaison que vous pouvez créer par VPC.
- Les points de terminaison ne sont pris en charge que dans la même région. Vous ne pouvez pas créer de point de terminaison entre un VPC et un service dans une autre région.

Créer une notification pour recevoir des alertes sur les événements du point de terminaison de l'interface : vous pouvez créer une notification pour recevoir des alertes pour des événements spécifiques qui se produisent sur le point de terminaison de votre interface. Afin de créer une

notification, vous devez lui associer une rubrique Amazon SNS. Vous pouvez vous inscrire à la rubrique SNS pour recevoir une notification par e-mail quand un événement de point de terminaison se produit.

Créez une politique pour les points de terminaison VPC pour Amazon WorkSpaces — Vous pouvez créer une politique pour les points de terminaison Amazon VPC pour Amazon WorkSpaces afin de spécifier les éléments suivants :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Connectez votre réseau privé à votre VPC — Pour appeler l' WorkSpaces API Amazon via votre VPC, vous devez vous connecter depuis une instance située à l'intérieur du VPC, ou connecter votre réseau privé à votre VPC à l'aide d'un réseau privé virtuel (VPN) Amazon ou. AWS Direct Connect Pour plus d'informations sur Amazon VPN, reportez-vous à la section Connexions VPN du guide de l'utilisateur Amazon Virtual Private Cloud. Pour plus d'informations AWS Direct Connect, reportez-vous à la section Création d'une connexion dans le Guide de AWS Direct Connect l'utilisateur.

Pour plus d'informations sur l'utilisation de l' WorkSpaces API Amazon via un point de terminaison d'interface VPC, consultez la section Sécurité de l'infrastructure sur Amazon. WorkSpaces

Prise en charge des cartes à puce

La prise en charge des cartes à puce est disponible pour Microsoft Windows et Amazon Linux WorkSpaces. La prise en charge des cartes à puce via Common Access Card (CAC) et la vérification d'identité personnelle (PIV) sont exclusivement disponibles WorkSpaces via Amazon via le protocole de WorkSpaces streaming (WSP). La prise en charge des cartes à puce par WSP WorkSpaces offre un niveau de sécurité accru pour authentifier les utilisateurs sur des points de terminaison de connexion approuvés par l'organisation avec du matériel spécifique sous la forme de lecteurs de cartes à puce. Il est important de se familiariser d'abord avec l'étendue du support disponible pour les cartes à puce et de déterminer comment les cartes à puce fonctionneront dans les WorkSpaces déploiements existants et futurs.

Il est recommandé de déterminer quel type de support de carte à puce est requis, qu'il s'agisse d'une authentification pré-session ou d'une authentification en cours de session. L'authentification de pré-session n'est disponible qu'au moment de la rédaction de cet article en AWS GovCloud (USA

Ouest), USA Est (Virginie du Nord), USA Ouest (Oregon), Europe (Irlande), Asie-Pacifique (Tokyo) et Asie-Pacifique (Sydney). L'authentification par carte à puce en cours de session est généralement disponible sous réserve de certaines considérations, telles que :

- Votre entreprise possède-t-elle une infrastructure de cartes à puce intégrée à Windows Active Directory ?
- Votre répondeur OCSP (Online Certificate Status Protocol) est-il accessible sur Internet ?
- Les certificats utilisateur sont-ils émis avec le nom d'utilisateur principal (UPN) dans le champ Nom alternatif du sujet (SAN) ?
- D'autres considérations sont détaillées dans les sections en cours de session et de pré-session.

La prise en charge des cartes à puce est activée par le biais de la stratégie de groupe. Il est recommandé d'ajouter le modèle d'administration Amazon WorkSpaces Group Policy pour WSP au magasin central de votre domaine Active Directory utilisé par Amazon WorkSpaces Directory (s). Lors de l'application de cette politique à un WorkSpaces déploiement Amazon existant, tous WorkSpaces auront besoin de la mise à jour de la politique de groupe et d'un redémarrage pour que la modification prenne effet pour tous les utilisateurs, car il s'agit d'une politique informatique.

Root CA

La nature de la portabilité du WorkSpaces client et de l'utilisateur Amazon nécessite de fournir à distance un certificat d'autorité de certification racine tiers au magasin de certificats racine approuvé de chaque appareil utilisé par les utilisateurs pour se connecter à leur Amazon. WorkSpaces Les contrôleurs de domaine AD et les appareils utilisateur équipés de cartes à puce doivent faire confiance aux autorités de certification racines. Consultez les directives fournies par Microsoft pour activer les autorités de certification tierces pour plus d'informations sur les exigences exactes.

Dans les environnements joints à un domaine AD, ces appareils répondent à cette exigence grâce à une stratégie de groupe distribuant des certificats d'autorité de certification racine. Dans les scénarios où Amazon WorkSpaces Client est utilisé à partir d' non-domain-joined appareils, un autre mode de livraison pour les autorités de certification racine tierces doit être déterminé, tel qu'Intune.

En cours de session

L'authentification en cours de session simplifie et sécurise l'authentification des applications une fois que les sessions WorkSpaces utilisateur Amazon ont déjà commencé. Comme indiqué

précédemment, le comportement par défaut d'Amazon WorkSpaces désactive les cartes à puce et doit être activé via la politique de groupe. Du point de vue de WorkSpaces l'administration d'Amazon, la configuration est spécifiquement requise pour les applications qui transmettent l'authentification (telles que les navigateurs Web). Aucune modification n'est requise pour les connecteurs AD et les annuaires.

La plupart des applications nécessitant une prise en charge de l'authentification en cours de session se font via des navigateurs Web tels que Mozilla Firefox et Google Chrome. Mozilla Firefox nécessite une configuration limitée pour la prise en charge des cartes à puce en cours de session. Amazon Linux WSP WorkSpaces nécessite une configuration supplémentaire pour la prise en charge des cartes à puce en cours de session pour Mozilla Firefox et Google Chrome.

Il est recommandé de s'assurer que les autorités de certification racines sont chargées dans le magasin de certificats personnels de l'utilisateur avant le dépannage, car le WorkSpaces client Amazon n'est peut-être pas autorisé à accéder à l'ordinateur local. En outre, utilisez OpenSC pour identifier les appareils à carte à puce lors de la résolution de tout problème d'authentification en cours de session suspecté avec des cartes à puce. Enfin, un répondeur OCSP (Online Certificate Status Protocol) est recommandé pour améliorer le niveau de sécurité de l'authentification des applications par le biais d'un contrôle de révocation des certificats.

Avant la session

Support pour l'authentification de présession : le WorkSpaces client Windows version 3.1.1 ou ultérieure, ou le WorkSpaces client macOS version 3.1.5 ou ultérieure. L'authentification de présession par carte à puce est fondamentalement différente de l'authentification standard, car l'utilisateur doit s'authentifier en insérant la carte à puce et en saisissant un code PIN. Avec ce type d'authentification, la durée des sessions de l'utilisateur est limitée par la durée de vie du ticket Kerberos. Un guide d'installation complet est disponible ici.

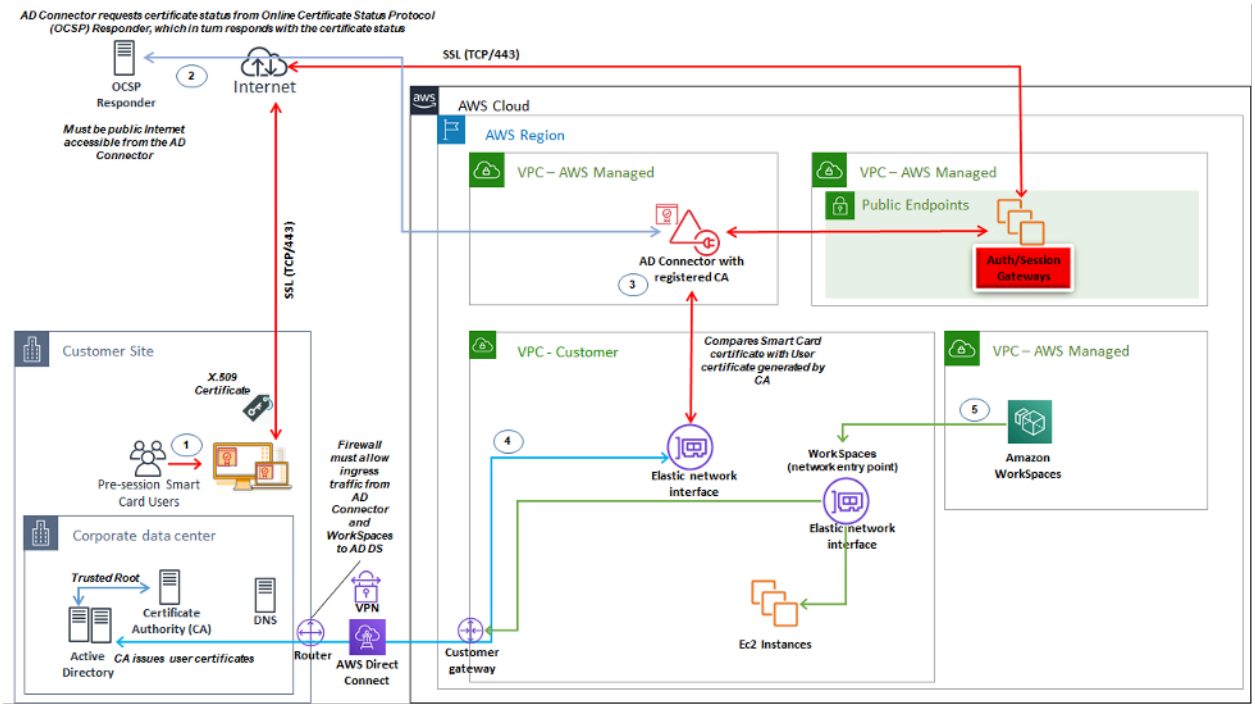

Figure 18 : Présentation de l'authentification de pré-session

1. L'utilisateur ouvre WorkSpaces le client Amazon, insère une carte à puce et saisit son code PIN. Le code PIN est utilisé par Amazon WorkSpaces Client pour déchiffrer le certificat X.509, qui est transmis par proxy à l'AD Connector via la passerelle d'authentification.
2. AD Connector valide le certificat X.509 par rapport à l'URL du répondeur OCSP accessible au public spécifiée dans les paramètres du répertoire pour s'assurer que le certificat n'a pas été révoqué.
3. Si le certificat est valide, le WorkSpaces client Amazon poursuit le processus d'authentification en demandant à l'utilisateur de saisir son code PIN une seconde fois pour déchiffrer le certificat X.509 et le connecter par proxy à l'AD Connector, où il est ensuite mis en correspondance avec les certificats racine et intermédiaire de l'AD Connector à des fins de validation.
4. Une fois que la validation du certificat est réussie, Active Directory est utilisé par l'AD Connector pour authentifier l'utilisateur et un ticket Kerberos est créé.
5. Le ticket Kerberos est transmis à l'Amazon de l'utilisateur WorkSpace pour s'authentifier et démarrer la session WSP.

Le répondeur OCSP doit être accessible au public car la connexion s'effectue via le réseau AWS géré et non via le réseau géré par le client. Il n'y a donc aucun routage vers des réseaux privés à cette étape.

La saisie du nom de l'utilisateur n'est pas obligatoire car les certificats utilisateur présentés à AD Connector incluent le userPrincipalName (UPN) de l'utilisateur dans le champ subjectAltName (SAN) du certificat. Il est recommandé d'automatiser la mise à jour des objets utilisateur AD de tous les utilisateurs qui ont besoin d'une authentification préalable à la session à l'aide de cartes à puce afin de s'authentifier avec le nom d'utilisateur UPN prévu dans le certificat utilisé PowerShell, plutôt que de le faire individuellement dans les consoles de gestion Microsoft.

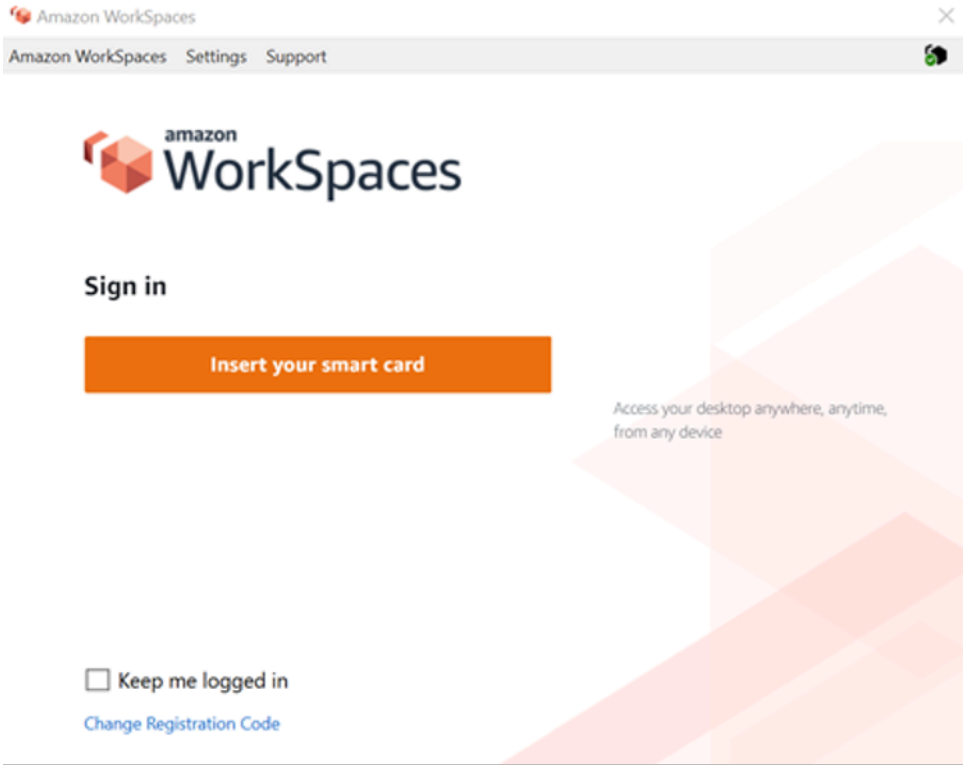

Figure 19 : console de WorkSpaces connexion

Déploiement du client

Le WorkSpaces client Amazon (version 3.X+) utilise des fichiers de configuration standardisés qui peuvent être utilisés par les administrateurs pour préconfigurer le client de leurs utilisateurs. WorkSpaces Le chemin des deux principaux fichiers de configuration se trouve à l'adresse suivante :

Système d’exploitation	Chemin du fichier de configuration
Windows	C:\Users\USERNAME \ AppData \ Local \ Amazon Web Services \ Amazon WorkSpaces

Système d'exploitation	Chemin du fichier de configuration
macOS	/Utilisateurs/Nom d'utilisateur/Bibliothèque/Support des applications/Amazon Web Services/Amazon WorkSpaces
Linux (Ubuntu 18.04)	/home/Ubuntu/.local/share/Amazon Web Services/Amazon/ WorkSpaces

Dans ces chemins, vous trouverez les deux fichiers de configuration. Le premier fichier de configuration est UserSettings .json, qui définira des éléments tels que l'enregistrement actuel, la configuration du proxy, le niveau de journalisation et la possibilité d'enregistrer la liste d'enregistrement. Le deuxième fichier de configuration est RegistrationList .json. Ce fichier contiendra toutes les informations de WorkSpaces répertoire que le client pourra utiliser pour mapper vers le WorkSpaces répertoire approprié. La préconfiguration du RegistrationList fichier .json remplira tous les codes d'enregistrement dans le client pour l'utilisateur.

> **Note**
>
> Si vos utilisateurs utilisent la version 2.5.11 du WorkSpaces client, proxy.cfg sera utilisé pour les paramètres du proxy client et client_settings.ini définira le niveau de journalisation ainsi que la possibilité d'enregistrer la liste d'enregistrement. Le paramètre de proxy par défaut utilisera ce qui est défini dans le système d'exploitation.

Ces fichiers étant standardisés, les administrateurs peuvent télécharger le WorkSpaces client, définir tous les paramètres applicables, puis envoyer les mêmes fichiers de configuration à tous les utilisateurs finaux. Pour que les paramètres prennent effet, le client doit être démarré une fois les nouvelles configurations définies. Si vous modifiez la configuration pendant que le client est en cours d'exécution, aucune des modifications ne sera définie dans le client.

Le dernier paramètre pouvant être défini pour les WorkSpaces utilisateurs est la mise à jour automatique du client Windows. Cela n'est pas contrôlé par les fichiers de configuration mais par le registre Windows. Lorsqu'une nouvelle version du client sort, vous pouvez créer une clé de registre pour ignorer cette version. Cela peut être défini en créant une chaîne de noms d'entrées de registre SkipThisVersion avec la valeur du numéro de version complet dans le chemin ci-dessous : Computer \ HKEY_CURRENT_USER \ Software \ Amazon Web Services. LLC \ Amazon

WorkSpaces \ WinSparkle Cette option est également disponible pour macOS ; toutefois, la configuration se trouve dans un fichier plist qui nécessite un logiciel spécial pour être modifiée. Si vous souhaitez toujours effectuer cette action, vous pouvez le faire en ajoutant une SkippedVersion entrée SU dans le domaine com.amazon.workspaces situé à l'adresse : /Users/Username/Library/Preferences

Sélection d'un point de WorkSpaces terminaison Amazon

Choisir un point de terminaison pour votre WorkSpaces

Amazon prend WorkSpaces en charge plusieurs terminaux, qu'il s'agisse d'ordinateurs de bureau Windows, d'iPads ou de Chromebooks. Vous pouvez télécharger les WorkSpaces clients Amazon disponibles sur le site Web Amazon Workspaces. Choisir le point de terminaison adapté à vos utilisateurs est une décision importante. Si vos utilisateurs ont besoin d'un système audio/vidéo bidirectionnel et qu'ils utiliseront le protocole de WorkSpaces streaming, ils doivent utiliser le client Windows ou macOS. Pour tous les clients, assurez-vous que les adresses IP et les ports répertoriés dans la section Exigences relatives aux adresses IP et aux ports pour Amazon WorkSpaces ont été explicitement configurés pour garantir que le client peut se connecter au service. Voici quelques considérations supplémentaires pour vous aider à choisir un terminal :

- Windows — Pour utiliser le WorkSpaces client Amazon Windows, le client 4.x doit exécuter l'ordinateur de bureau Microsoft Windows 8.1, Windows 10 64 bits requis. Les utilisateurs peuvent installer le client uniquement pour leur profil utilisateur sans privilèges administratifs sur la machine locale. Les administrateurs système peuvent déployer le client sur des points de terminaison gérés à l'aide de Group Policy, de Microsoft Endpoint Manager Configuration Manager (MEMCM) ou d'autres outils de déploiement d'applications utilisés dans un environnement. Le client Windows prend en charge un maximum de quatre écrans et une résolution maximale de 3840 x 2160.
- macOS — Pour déployer le dernier WorkSpaces client macOS Amazon, les appareils macOS doivent exécuter macOS 10.12 (Sierra) ou une version ultérieure. Vous pouvez déployer une ancienne version du WorkSpaces client pour vous connecter à PCoIP WorkSpaces si le terminal exécute OSX 10.8.1 ou version ultérieure. Le client macOS prend en charge jusqu'à deux moniteurs de résolution 4K ou quatre moniteurs de résolution WUXGA (1920 x 1200).
- Linux — Le client Amazon WorkSpaces Linux nécessite Ubuntu 18.04 (AMD64) 64 bits pour fonctionner. Si vos terminaux Linux n'exécutent pas cette version du système d'exploitation, le client Linux n'est pas pris en charge. Avant de déployer des clients Linux ou de fournir aux utilisateurs leur code d'enregistrement, assurez-vous d'activer l'accès au client Linux au niveau du WorkSpaces répertoire, car il est désactivé par défaut et les utilisateurs ne pourront pas se

connecter à partir de clients Linux tant qu'il ne sera pas activé. Le client Linux prend en charge jusqu'à deux moniteurs de résolution 4K ou quatre moniteurs de résolution WUXGA (1920 x 1200).

- iPad — L'application client Amazon WorkSpaces iPad prend en charge le protocole PCoIP WorkSpaces. Les iPad compatibles sont l'iPad2 ou version ultérieure avec iOS 8.0 ou version ultérieure, l'iPad Retina avec iOS 8.0 et version ultérieure, l'iPad Mini avec iOS 8.0 et version ultérieure, et l'iPad Pro avec iOS 9.0 et version ultérieure. Assurez-vous que l'appareil à partir duquel les utilisateurs se connecteront répond à ces critères. L'application cliente pour iPad prend en charge de nombreux gestes différents. (Consultez la liste complète des gestes pris en charge.) L'application client Amazon WorkSpaces iPad prend également en charge le Swiftpoint GT et ProPoint PadPoint les souris. Le Swiftpoint TRACPOINT PenPoint et les GoPoint souris ne sont pas pris en charge.
- Android/Chromebook — Lorsque vous souhaitez déployer un appareil Android ou un Chromebook comme point de terminaison pour vos utilisateurs finaux, vous devez tenir compte de quelques considérations. Assurez-vous que WorkSpaces les utilisateurs auxquels se connecteront sont PCoIP WorkSpaces, car ce client ne prend en charge que le PCoIP. WorkSpaces Ce client ne prend en charge qu'un seul affichage. Si les utilisateurs ont besoin d'un support multi-écrans, utilisez un autre point de terminaison. Si vous souhaitez déployer un Chromebook, assurez-vous que le modèle que vous déployez prend en charge l'installation d'applications Android. La prise en charge complète des fonctionnalités n'est prise en charge que sur le client Android, et non sur l'ancien client Chromebook. Cela n'est généralement pris en compte que pour les Chromebooks fabriqués avant 2019. Le support Android est fourni pour les tablettes et les téléphones tant qu'Android exécute OS 4.4 ou version ultérieure. Cependant, il est recommandé que l'appareil Android exécute OS 9 ou une version ultérieure pour utiliser le dernier client WorkSpace Android. Si vos Chromebooks exécutent la version WorkSpaces client 3.0.1 ou supérieure, vos utilisateurs peuvent désormais profiter des fonctionnalités de libre-service. WorkSpaces En outre, en tant qu'administrateur, vous pouvez utiliser des certificats d'appareils sécurisés pour restreindre l' WorkSpaces accès aux appareils sécurisés dotés de certificats valides.
- Accès Web — Les utilisateurs peuvent accéder à leur Windows WorkSpaces depuis n'importe quel endroit à l'aide d'un navigateur Web. Cette solution convient parfaitement aux utilisateurs qui doivent utiliser un appareil verrouillé ou un réseau restrictif. Au lieu d'utiliser une solution d'accès à distance traditionnelle et d'installer l'application client appropriée, les utilisateurs peuvent visiter le site Web pour accéder à leurs ressources de travail. Les utilisateurs peuvent utiliser le WorkSpaces Web Access pour se connecter à non-graphics-based Windows PCoIP WorkSpaces exécutant Windows 10 ou Windows Server 2016 avec Desktop Experience. Les utilisateurs doivent se connecter à l'aide de Chrome 53 ou version ultérieure, ou de Firefox 49 ou version ultérieure. Pour les applications basées sur WSP WorkSpaces, les utilisateurs peuvent utiliser le WorkSpaces

Web Access pour se connecter à des applications Windows non graphiques. WorkSpaces Ces utilisateurs doivent se connecter à l'aide de Microsoft Edge 91 ou version ultérieure ou de Google Chrome 91 ou version ultérieure. La résolution d'écran minimale prise en charge est de 960 x 720 avec une résolution maximale prise en charge de 2560 x 1600. L'utilisation de plusieurs moniteurs n'est pas prise en charge. Pour une expérience utilisateur optimale, dans la mesure du possible, il est recommandé aux utilisateurs d'utiliser une version du système d'exploitation du client.

- Client PCoIP zéro — Vous pouvez déployer des clients PCoIP zéro pour les utilisateurs finaux auxquels WorkSpaces PCoIP leur est ou sera attribué. Le client Tera2 zero doit disposer d'une version de microprogramme 6.0.0 ou ultérieure pour se connecter directement au. WorkSpace Pour utiliser l'authentification multifactorielle avec Amazon WorkSpaces, l'appareil client Tera2 zero doit exécuter la version 6.0.0 ou ultérieure du microprogramme. Support et dépannage du matériel zéro client doivent être effectués auprès du fabricant.
- Système d'exploitation IGEL — Vous pouvez utiliser le système d'exploitation IGEL sur les terminaux pour vous connecter à PCoIP, à condition WorkSpaces que la version du microprogramme soit 11.04.280 ou supérieure. Les fonctionnalités prises en charge correspondent à celles du client Linux existant aujourd'hui. Avant de déployer des clients IGEL OS ou de fournir aux utilisateurs leur code d'enregistrement, assurez-vous d'activer l'accès au client Linux au niveau du WorkSpaces répertoire, car il est désactivé par défaut et les utilisateurs ne pourront pas se connecter depuis les clients IGEL OS tant qu'il ne sera pas activé. Le client LGel OS prend en charge jusqu'à deux moniteurs de résolution 4K ou quatre moniteurs de résolution WUXGA (1920 x 1200).

Client d'accès Web

Conçu pour les appareils verrouillés, le client Web Access permet d'accéder à Amazon WorkSpaces sans qu'il soit nécessaire de déployer un logiciel client. Le client Web Access est recommandé uniquement dans les environnements où Amazon WorkSpaces utilise le système d'exploitation Windows et est utilisé pour des flux de travail utilisateur limités, tels qu'un environnement de kiosque. La plupart des cas d'utilisation bénéficient de l'ensemble de fonctionnalités disponibles auprès du WorkSpaces client Amazon. Le client Web Access n'est recommandé que dans des cas d'utilisation spécifiques où les appareils et les restrictions du réseau nécessitent une autre méthode de connexion.

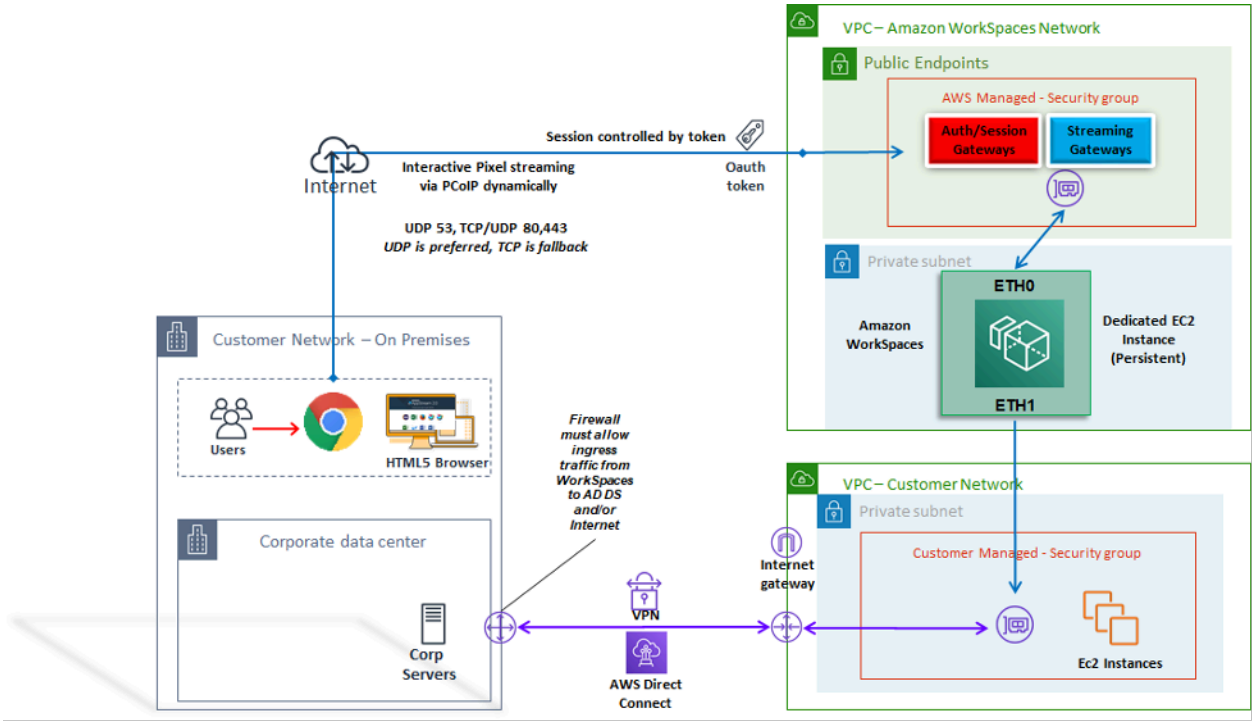

Figure 20 : Architecture du client d'accès Web

Comme le montre le schéma, le client Web Access a des exigences réseau différentes pour diffuser la session aux utilisateurs. Web Access est disponible pour Windows à WorkSpaces l'aide du protocole PCoIP ou WSP. Le DNS et le HTTP/HTTPS sont nécessaires pour l'authentification et l'enregistrement auprès des WorkSpaces passerelles. Pour WorkSpaces utiliser le protocole WSP, une connexion directe UDP/TCP 4195 doit être ouverte aux plages d'adresses IP de la passerelle WSP. Le trafic de streaming n'est pas alloué à un port fixe comme c'est le cas pour le WorkSpaces client Amazon complet ; il est plutôt alloué de manière dynamique. Le protocole UDP est préférable pour le trafic en continu ; toutefois, le navigateur Web revient au protocole TCP lorsque le protocole UDP est restreint. Dans les environnements où le port TCP/UDP 4172 est bloqué et ne peut pas être débloqué en raison de restrictions organisationnelles, le client Web Access fournit une méthode de connexion alternative aux utilisateurs.

Par défaut, le client Web Access est désactivé au niveau du répertoire. Pour permettre aux utilisateurs d'accéder à leur Amazon WorkSpaces via un navigateur Web, utilisez le AWS Management Console pour mettre à jour les paramètres du répertoire ou utilisez l'WorkspaceAccessProperties API par programmation pour les modifier en Allow DeviceTypeWeb . En outre, l'administrateur doit s'assurer que les paramètres de stratégie de groupe n'entrent pas en conflit avec les exigences de connexion.

WorkSpaces Balises Amazon

```
Tags enable you to associate metadata with AWS resources. Tags can be used with Amazon
 WorkSpaces to registered directories,
  bundles, IP Access Control Groups, or images. Tags assist with cost allocation to
 internal cost centers. Before using tags with Amazon WorkSpaces,
  refer to the Tagging Best Practices whitepaper.

Tag restrictions
```

- Nombre maximal de balises par ressource : 50
- Longueur de clé maximale : 127 caractères Unicode
- Longueur de valeur maximale : 255 caractères Unicode
- Les clés et les valeurs des balises 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 : ou aws:workspaces : dans les noms ou les valeurs de vos balises, car ils sont réservés à l'usage. AWS Vous ne pouvez pas modifier ni supprimer les noms ou valeurs de balise ayant ces préfixes.

Ressources que vous pouvez baliser

- Vous pouvez ajouter des balises aux ressources suivantes lorsque vous les créez : WorkSpaces images importées et groupes de contrôle d'accès IP.
- Vous pouvez ajouter des balises aux ressources existantes des types suivants : annuaires enregistrés WorkSpaces, ensembles personnalisés, images et groupes de contrôle d'accès IP.

  Utilisation de l'étiquette de répartition des coûts

Pour afficher vos balises de WorkSpaces ressources dans le Cost Explorer, activez les balises que vous avez appliquées à vos WorkSpaces ressources en suivant les instructions de la section Activation des balises de répartition des coûts définies par l'utilisateur dans le guide de l'utilisateur de AWS Billing and Cost Management and Cost Management.

Bien que les balises apparaissent 24 heures après l'activation, les valeurs associées à ces balises peuvent prendre quatre à cinq jours pour apparaître dans Cost Explorer, pour apparaître et fournir des données de coûts dans Cost Explorer. Les WorkSpaces ressources balisées doivent être

facturées pendant cette période. Cost Explorer 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.

Gestion des balises

Pour mettre à jour les balises d'une ressource existante à l'aide de AWS CLI, utilisez les commandes create-tags et delete-tags. Pour les mises à jour groupées et pour automatiser la tâche sur un grand nombre de WorkSpaces ressources, Amazon WorkSpaces ajoute la prise en charge de AWS Resource Groups Tag Editor. AWS Resource Groups L'éditeur de balises vous permet d'ajouter, de modifier ou de supprimer des AWS balises dans vos ressources WorkSpaces ainsi que dans vos autres AWS ressources.

Quotas WorkSpaces de service Amazon

Les Quotas de Service facilitent la recherche de la valeur d'un quota spécifique, également appelé limite. Vous pouvez également consulter tous les quotas pour un service donné.

Pour consulter vos quotas pour WorkSpaces

1. Accédez à la console Service Quotas.
2. Dans le volet de navigation de gauche, sélectionnez AWS services.
3. Sélectionnez Amazon dans WorkSpaces la liste ou saisissez Amazon WorkSpaces dans le champ de recherche à l'avance.
4. Pour afficher des informations supplémentaires sur un quota, telles que sa description et le nom de ressource Amazon (ARN), choisissez le nom du quota.

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, des quotas par défaut (également appelés limites) sont définis en fonction du nombre de ressources que vous pouvez créer.

Vous pouvez utiliser la console Service Quotas pour consulter les Quotas de Service par défaut ou pour demander des augmentations de quota pour des quotas ajustables.

Pour plus d'informations, reportez-vous aux sections Affichage des quotas de service et Demande d'augmentation des quotas du Guide de l'utilisateur des quotas de service.

Automatiser le déploiement d'Amazon WorkSpaces

Avec Amazon WorkSpaces, vous pouvez lancer un poste de travail Microsoft Windows ou Amazon Linux en quelques minutes, vous connecter à votre logiciel de bureau et y accéder depuis un réseau local ou externe de manière sécurisée, fiable et rapide. Vous pouvez automatiser le provisionnement d'Amazon WorkSpaces pour WorkSpaces intégrer Amazon à vos flux de travail de provisionnement existants.

Méthodes WorkSpaces d'automatisation courantes

Les clients peuvent utiliser un certain nombre d'outils pour permettre un WorkSpaces déploiement rapide d'Amazon. Les outils peuvent être utilisés pour simplifier la gestion WorkSpaces, réduire les coûts et créer un environnement agile capable d'évoluer et d'évoluer rapidement.

AWS CLI et API

Il existe des opérations WorkSpaces d'API Amazon que vous pouvez utiliser pour interagir avec le service en toute sécurité et à grande échelle. Toutes les API publiques sont disponibles avec le AWS CLI SDK et les outils pour PowerShell, tandis que les API privées telles que la création d'images ne sont disponibles que via le AWS Management Console. Lorsque vous envisagez la gestion opérationnelle et le libre-service commercial pour Amazon WorkSpaces, tenez compte du fait que WorkSpaces les API nécessitent une expertise technique et des autorisations de sécurité pour être utilisées.

Les appels d'API peuvent être effectués à l'aide du AWS SDK. AWS Tools for Windows PowerShell et AWS Tools for PowerShell Core sont des PowerShell modules basés sur les fonctionnalités exposées par le AWS SDK pour .NET. Ces modules vous permettent de scripter des opérations sur les AWS ressources à partir de la ligne de PowerShell commande et de les intégrer aux outils et services existants. Par exemple, les appels d'API peuvent vous permettre de gérer automatiquement le WorkSpaces cycle de vie en intégrant AD pour le provisionnement et la mise hors service en WorkSpaces fonction de l'appartenance d'un utilisateur au groupe AD.

AWS CloudFormation

AWS CloudFormation vous permet de modéliser l'ensemble de votre infrastructure dans un fichier texte. Ce modèle devient la source unique de vérité pour votre infrastructure. Cela vous permet de standardiser les composants d'infrastructure utilisés au sein de votre entreprise, de garantir la conformité des configurations et d'accélérer le dépannage.

AWS CloudFormation provisionne vos ressources de manière sûre et reproductible, ce qui vous permet de créer et de reconstruire votre infrastructure et vos applications. Vous pouvez l'utiliser CloudFormation pour mettre en service et mettre hors service des environnements, ce qui est utile lorsque vous souhaitez créer et mettre hors service plusieurs comptes de manière répétitive. Lorsque vous envisagez la gestion opérationnelle et le libre-service commercial pour Amazon WorkSpaces, considérez que leur utilisation AWS CloudFormationnécessite une expertise technique et des autorisations de sécurité.

Portail en libre-service WorkSpaces

Les clients peuvent utiliser des commandes d' WorkSpaces API intégrées et d'autres AWS services pour créer un portail WorkSpaces en libre-service. Cela permet aux clients de rationaliser le processus de déploiement et de récupération WorkSpaces à grande échelle. À l'aide d'un WorkSpaces portail, vous pouvez permettre à votre personnel de configurer son propre WorkSpaces flux de travail d'approbation intégré qui ne nécessite aucune intervention informatique pour chaque demande. Cela réduit les coûts opérationnels informatiques, tout en aidant les utilisateurs finaux à démarrer WorkSpaces plus rapidement. Le flux de travail d'approbation intégré supplémentaire simplifie le processus d'approbation sur ordinateur pour les entreprises. Un portail dédié peut offrir un outil automatisé pour le provisionnement des postes de travail cloud Windows ou Linux, permettre aux utilisateurs de reconstruire, redémarrer ou migrer leurs ordinateurs WorkSpace, ainsi que de permettre la réinitialisation des mots de passe.

Vous trouverez des exemples guidés de création de WorkSpaces portails en libre-service dans la section Lectures complémentaires de ce document. AWS Les partenaires fournissent des portails WorkSpaces de gestion préconfigurés via le AWS Marketplace.

Intégration à la gestion des services informatiques d'entreprise

À mesure que les entreprises adoptent Amazon WorkSpaces comme solution de bureau virtuel à grande échelle, il est nécessaire de mettre en œuvre des systèmes de gestion des services informatiques (ITSM) ou de les intégrer. L'intégration ITSM permet de proposer des offres en libre-service pour le provisionnement et les opérations. Le Service Catalog vous permet de gérer de manière centralisée les AWS services couramment déployés et les produits logiciels fournis. Ce service aide votre entreprise à respecter des exigences cohérentes en matière de gouvernance et de conformité, tout en permettant aux utilisateurs de déployer uniquement les AWS services approuvés dont ils ont besoin. Le Service Catalog peut être utilisé pour proposer une offre de gestion du cycle de vie en libre-service pour WorkSpaces Amazon à partir d'outils de gestion des services informatiques tels que. ServiceNow

WorkSpaces Bonnes pratiques en matière d'automatisation du déploiement

Vous devez prendre en compte les principes de Well Architected en matière de sélection et de conception de l'automatisation WorkSpaces du déploiement.

- Conception axée sur l'automatisation : conception de manière à permettre le moins d'interventions manuelles possible dans le processus afin de garantir la répétabilité et l'évolutivité.
- Conception axée sur l'optimisation des coûts : en créant et en récupérant automatiquement WorkSpaces, vous pouvez réduire les efforts administratifs nécessaires pour fournir des ressources et empêcher les ressources inutilisées ou inutilisées de générer des coûts inutiles.
- Conception axée sur l'efficacité : minimisez les ressources nécessaires à la création et à la terminaison WorkSpaces. Dans la mesure du possible, offrez des fonctionnalités de libre-service de niveau 0 à l'entreprise afin d'améliorer son efficacité.
- Conception axée sur la flexibilité : créez un mécanisme de déploiement cohérent capable de gérer plusieurs scénarios et d'évoluer avec le même mécanisme (personnalisé à l'aide de cas d'utilisation et d'identifiants de profil balisés).
- Conception axée sur la productivité — Concevez vos WorkSpaces opérations de manière à permettre l'autorisation et la validation correctes pour ajouter ou supprimer des ressources.
- Conception axée sur l'évolutivité : le modèle pay-as-you Go WorkSpaces utilisé par Amazon permet de réaliser des économies en créant des ressources selon les besoins et en les supprimant lorsqu'elles ne sont plus nécessaires.
- Conception axée sur la sécurité — Concevez vos WorkSpaces opérations de manière à permettre l'autorisation et la validation correctes pour ajouter ou supprimer des ressources.
- Conception axée sur la soutenabilité — Concevez vos WorkSpaces opérations de manière à permettre la mise en place de mécanismes et de processus de soutien et de rétablissement non invasifs.

Correctifs WorkSpaces et mises à niveau sur place d'Amazon

Avec Amazon WorkSpaces, vous pouvez gérer les correctifs et les mises à jour à l'aide d'outils tiers existants, tels que Microsoft System Center Configuration Manager (SCCM), Puppet Enterprise ou Ansible. Le déploiement sur place des correctifs de sécurité maintient généralement un cycle de correctifs mensuel, avec des processus supplémentaires pour l'escalade ou le déploiement

rapide. Toutefois, dans le cas de mises à niveau du système d'exploitation ou de mises à jour de fonctionnalités sur place, des considérations spéciales sont souvent nécessaires.

WorkSpace entretien

Amazon WorkSpaces dispose d'une fenêtre de maintenance par défaut au cours de laquelle les mises à jour de l' WorkSpaces agent Amazon et toutes les mises à jour du système d'exploitation disponibles sont WorkSpace installées. WorkSpaces ne sera pas disponible pour les connexions utilisateur pendant la période de maintenance planifiée.

- AlwaysOn WorkSpaces la fenêtre de maintenance par défaut est de 00h00 à 04h00, dans le fuseau horaire du WorkSpace, chaque dimanche matin.

- La redirection de fuseau horaire est activée par défaut et peut remplacer la fenêtre par défaut pour qu'elle corresponde au fuseau horaire local de l'utilisateur.
- Vous pouvez désactiver la redirection de fuseau horaire pour Windows à WorkSpaces l'aide de la stratégie de groupe. Vous pouvez désactiver la redirection de fuseau horaire pour Linux à l'aide WorkSpaces de la configuration de l'agent PCoIP.

- AutoStop WorkSpaces sont lancés automatiquement une fois par mois pour installer les mises à jour importantes. À compter du troisième lundi du mois, et pendant deux semaines au maximum, le créneau de maintenance est ouvert chaque jour de 00h00 à 05h00 environ, dans le fuseau horaire de la AWS Région pour le. WorkSpace Il WorkSpace peut être maintenu n'importe quel jour pendant la période de maintenance.

- Bien que vous ne puissiez pas modifier le fuseau horaire utilisé pour la maintenance AutoStop WorkSpaces, vous pouvez désactiver la fenêtre de maintenance pour votre AutoStop WorkSpaces.

- Les fenêtres de maintenance manuelle peuvent être définies en fonction de votre calendrier préféré en définissant l'état du sur WorkSpace ADMIN_MAINTENANCE.

- La AWS CLI commande modify-workspace-statepeut être utilisée pour modifier l' WorkSpace état en ADMIN_MAINTENANCE.

Amazon Linux WorkSpaces

Pour connaître les considérations, les conditions requises et les modèles suggérés pour gérer les mises à jour et les correctifs sur les images WorkSpaces personnalisées Amazon Linux, consultez le livre blanc Meilleures pratiques pour préparer vos images Amazon WorkSpaces pour Linux.

Conditions préalables et considérations relatives à l'application de correctifs pour Linux

- Les référentiels Amazon Linux sont hébergés dans des compartiments Amazon Simple Storage Service (Amazon S3) accessibles via des points de terminaison publics accessibles à Internet ou des points de terminaison privés. Si votre Amazon Linux WorkSpaces n'a pas accès à Internet, veuillez suivre ce processus pour rendre les mises à jour accessibles : Comment puis-je mettre à jour yum ou installer des packages sans accès à Internet sur mes instances EC2 exécutant Amazon Linux 1 ou Amazon Linux 2 ?
- Vous ne pouvez pas configurer la fenêtre de maintenance par défaut pour Linux WorkSpaces. Si la personnalisation de cette fenêtre est requise, le processus de maintenance manuelle peut être utilisé.

Application de correctifs pour Amazon Windows

Par défaut, votre système Windows est configuré pour recevoir WorkSpaces les mises à jour de Windows Update qui nécessitent un accès Internet depuis votre WorkSpaces VPC. Pour configurer vos propres mécanismes de mise à jour automatique pour Windows, reportez-vous à la documentation de Windows Server Update Services (WSUS) et de Configuration Manager.

Mise à niveau sur place d'Amazon Windows

- 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 mis à niveau à partir d'une version précédente (mise à niveau de fonctionnalité/de version Windows). Toutefois, les mises à jour cumulatives ou de sécurité de Windows sont prises en charge par le processus de création et de capture d' WorkSpaces images.

- Les images personnalisées de Windows 10 Bring Your Own License (BYOL) doivent commencer par la dernière version prise en charge de Windows sur une machine virtuelle comme source du

processus d'importation BYOL : reportez-vous à la documentation d'importation BYOL pour plus de détails.

Conditions préalables à la mise à niveau sur place de Windows

- Si vous avez reporté ou suspendu les mises à niveau de Windows 10 à l'aide de la stratégie de groupe Active Directory ou du SCCM, activez les mises à niveau du système d'exploitation pour votre Windows 10. WorkSpaces
- S'il s' WorkSpace agit d'un AutoStop WorkSpace, modifiez le AutoStop délai à au moins trois heures pour tenir compte de la fenêtre de mise à niveau.
- Le processus de mise à niveau sur place recrée le profil utilisateur en créant une copie de l'utilisateur par défaut (C:\Users\Default). N'utilisez pas le profil utilisateur par défaut pour effectuer des personnalisations. Il est recommandé de personnaliser le profil utilisateur via des objets de stratégie de groupe (GPO) à la place. Les personnalisations effectuées via les GPO 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 relatives à la mise à niveau sur place de

- Le processus de mise à niveau sur place utilise deux scripts de registre (enable-inplace-upgrade.ps1 et update-pvdrivers.ps1) pour apporter les modifications nécessaires à votre compte et permettre au processus Windows Update de s'exécuter. WorkSpaces 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.
- Une fois la mise à niveau sur place déployée, vous devez restaurer les profils utilisateur sur le lecteur D pour vous assurer de pouvoir reconstruire ou migrer le vôtre WorkSpaces et pour éviter tout problème potentiel lié à la redirection des dossiers du shell utilisateur. Vous pouvez le faire en utilisant la clé de registre PostUpgradeRestoreProfileOnD, comme expliqué sur la page de référence de mise à niveau BYOL.

Packs WorkSpaces de langue Amazon

WorkSpaces Les offres Amazon qui fournissent l'expérience de bureau Windows 10 sont disponibles en anglais (États-Unis), en français (Canada), en coréen et en japonais. Cependant, vous pouvez inclure des modules linguistiques supplémentaires pour l'espagnol, l'italien, le portugais et de nombreuses autres options linguistiques. Pour plus d'informations, reportez-vous à Comment créer une nouvelle WorkSpace image Windows avec une langue client autre que l'anglais ? .

Gestion des WorkSpaces profils Amazon

Amazon WorkSpaces sépare le profil utilisateur du système d'exploitation (OS) de base en redirigeant toutes les écritures de profil vers un volume Amazon Elastic Block Store (Amazon EBS) distinct. Dans Microsoft Windows, le profil utilisateur est stocké dans D:\Users\username. Dans Amazon Linux, le profil utilisateur est stocké dans /home. Le volume EBS est automatiquement capturé toutes les 12 heures. L'instantané est automatiquement stocké dans un compartiment S3 AWS géré, à utiliser en cas de reconstruction ou de restauration d'un Amazon WorkSpace .

Pour la plupart des entreprises, il est préférable de disposer de snapshots automatiques toutes les 12 heures par rapport au déploiement de postes de travail existant, qui ne prévoit aucune sauvegarde pour les profils utilisateur. Toutefois, les clients peuvent avoir besoin d'un contrôle plus précis des profils utilisateur ; par exemple, migration d'un ordinateur de bureau vers WorkSpaces un nouveau système d'AWS exploitation/région, prise en charge de la reprise après sinistre, etc. D'autres méthodes de gestion des profils sont disponibles pour Amazon WorkSpaces.

Redirection de dossiers

Bien que la redirection de dossiers soit une considération de conception courante dans les architectures d'infrastructure de bureau virtuel (VDI), elle ne constitue pas une bonne pratique, ni même une exigence courante dans les WorkSpaces conceptions Amazon. Cela s'explique par le fait qu'Amazon WorkSpaces est une solution de bureau en tant que service (DaaS) persistante, avec des données d'application et d'utilisateur persistantes prêtes à l'emploi.

Il existe des scénarios spécifiques dans lesquels la redirection de dossiers pour les dossiers de l'interface utilisateur (par exemple, D:\Users\username\Desktop redirigé vers \ \ Server \ RedirectionShare $ \ username \ Desktop) est requise, tels que l'objectif de point de restauration immédiat (RPO) pour les données de profil utilisateur dans les environnements de reprise après sinistre (DR).

Bonnes pratiques

Les meilleures pratiques suivantes sont répertoriées pour une redirection de dossiers robuste :

- Hébergez les serveurs de fichiers Windows dans la même AWS région et dans la même région que celles dans WorkSpaces lesquelles Amazon est lancé.
- Assurez-vous que les règles entrantes du groupe de sécurité AD incluent le groupe de sécurité du serveur de fichiers Windows ou les adresses IP privées ; sinon, assurez-vous que le pare-feu local autorise le même trafic basé sur les ports TCP et UDP.
- Assurez-vous que les règles entrantes du groupe de sécurité du serveur de fichiers Windows incluent le protocole TCP 445 (SMB) pour tous les groupes de sécurité Amazon WorkSpaces .
- Créez un groupe de sécurité AD pour les WorkSpaces utilisateurs d'Amazon afin d'autoriser les utilisateurs à accéder au partage de fichiers Windows.
- Utilisez l'espace de noms DFS (DFS-N) et la réplication DFS (DFS-R) pour garantir que votre partage de fichiers Windows est agile, qu'il n'est pas lié à un serveur de fichiers Windows en particulier et que toutes les données utilisateur sont automatiquement répliquées entre les serveurs de fichiers Windows.
- Ajoutez « $ » à la fin du nom du partage pour masquer les données utilisateur du partage hébergeant les données utilisateur lorsque vous parcourez les partages réseau dans l'Explorateur Windows.
- Créez le partage de fichiers en suivant les instructions de Microsoft relatives aux dossiers redirigés : Déployer la redirection de dossiers avec des fichiers hors connexion. Suivez attentivement les instructions relatives aux autorisations de sécurité et à la configuration des GPO.
- Si votre WorkSpaces déploiement Amazon est basé sur Bring Your Own License (BYOL), vous devez également spécifier la désactivation des fichiers hors ligne en suivant les instructions de Microsoft : Désactiver les fichiers hors ligne sur des dossiers redirigés individuels.
- Installez et exécutez la déduplication des données (communément appelée « déduplication ») si votre serveur de fichiers Windows est Windows Server 2016 ou une version ultérieure afin de réduire la consommation de stockage et d'optimiser les coûts. Reportez-vous aux sections Installation et activation de la déduplication des données et Exécution de la déduplication des données.
- Sauvegardez les partages de fichiers de votre serveur de fichiers Windows à l'aide des solutions de sauvegarde organisationnelles existantes.

Chose à éviter

- N'utilisez pas de serveurs de fichiers Windows accessibles uniquement via une connexion réseau étendu (WAN), car le protocole SMB n'est pas conçu pour cette utilisation.
- N'utilisez pas le même partage de fichiers Windows que celui utilisé pour les répertoires de base afin de réduire les risques que les utilisateurs suppriment accidentellement leurs dossiers User Shell.
- Bien qu'il soit recommandé d'activer le service Volume Shadow Copy (VSS) pour faciliter les restaurations de fichiers, cela ne supprime pas à lui seul la nécessité de sauvegarder les partages de fichiers du serveur de fichiers Windows.

Autres considérations

- Amazon FSx for Windows File Server propose un service géré pour les partages de fichiers Windows et simplifie la charge opérationnelle liée à la redirection de dossiers, y compris les sauvegardes automatiques.
- Utilisez AWS Storage Gateway for SMB File Share pour sauvegarder vos partages de fichiers s'il n'existe aucune solution de sauvegarde organisationnelle existante.

Paramètres du profil

Politiques de groupe

L'une des meilleures pratiques courantes dans les déploiements de Microsoft Windows en entreprise consiste à définir les paramètres de l'environnement utilisateur par le biais des paramètres GPO (Group Policy Object) et GPP (Group Policy Preferences). Les paramètres tels que les raccourcis, les mappages de lecteurs, les clés de registre et les imprimantes sont définis via la console de gestion des politiques de groupe. Les avantages liés à la définition de l'environnement utilisateur par le biais des GPO incluent, sans toutefois s'y limiter :

- Gestion centralisée de la configuration
- Profil utilisateur défini par l'appartenance à un groupe de sécurité AD ou le placement de l'unité organisationnelle
- Protection contre la suppression des paramètres
- Automatisez la création et la personnalisation des profils dès la première connexion

- Facilité de mise à jour future

> **Note**
>
> Suivez les meilleures pratiques de Microsoft pour optimiser les performances des politiques de groupe.

Les politiques de groupe relatives aux bannières de connexion interactives ne doivent pas être utilisées car elles ne sont pas prises en charge sur Amazon WorkSpaces. Les bannières sont présentées sur le WorkSpaces client Amazon par le biais de demandes d' AWS assistance. En outre, les appareils amovibles ne doivent pas être bloqués par le biais d'une politique de groupe, car ils sont obligatoires pour Amazon WorkSpaces.

Les GPO peuvent être utilisés pour gérer Windows WorkSpaces. Pour plus d'informations, reportez-vous à la section Gérer vos fenêtres WorkSpaces.

WorkSpaces Volumes Amazon

Chaque WorkSpaces instance Amazon contient deux volumes : un volume du système d'exploitation et un volume utilisateur.

- Amazon Windows WorkSpaces — Le lecteur C : \ est utilisé pour le système d'exploitation (OS) et le lecteur D : \ est le volume utilisateur. Le profil utilisateur se trouve sur le volume utilisateur (documentsAppData, images, téléchargements, etc.).
- Amazon Linux WorkSpaces — Avec un Amazon Linux WorkSpace, le volume système (/dev/xvda1) est monté en tant que dossier racine. Le volume utilisateur est destiné aux données utilisateur et aux applications ; /dev/xvdf1 se monte sous la forme /home.

Pour les volumes du système d'exploitation, vous pouvez sélectionner une taille de départ pour ce lecteur de 80 Go ou 175 Go. Pour les volumes utilisateur, vous pouvez sélectionner une taille de départ de 10 Go, 50 Go ou 100 Go. La taille des deux volumes peut être augmentée jusqu'à 2 To selon les besoins ; toutefois, pour augmenter le volume utilisateur au-delà de 100 Go, le volume du système d'exploitation doit être de 175 Go. Les changements de volume ne peuvent être effectués qu'une fois toutes les six heures par volume. Pour plus d'informations sur la modification de la taille du WorkSpaces volume, reportez-vous à la WorkSpace section Modifier un du Guide d'administration.

WorkSpaces bonnes pratiques en matière de volumes

Lors de la planification d'un WorkSpaces déploiement Amazon, il est recommandé de prendre en compte les exigences minimales relatives à l'installation du système d'exploitation, aux mises à niveau sur place et aux applications principales supplémentaires qui seront ajoutées à l'image sur le volume du système d'exploitation. En ce qui concerne le volume utilisateur, il est recommandé de commencer par une allocation de disque plus petite et d'augmenter progressivement la taille du volume utilisateur selon les besoins. La réduction de la taille des volumes de disque réduit le coût d'exploitation du WorkSpace.

> **Note**
>
> La taille d'un volume peut être augmentée, mais elle ne peut pas être diminuée.

WorkSpaces Journalisation Amazon

Dans un WorkSpaces environnement Amazon, de nombreuses sources de journaux peuvent être capturées pour résoudre les problèmes et surveiller les WorkSpaces performances globales.

Amazon WorkSpaces Client 3.x Sur chaque WorkSpaces client Amazon, les journaux des clients se trouvent dans les répertoires suivants :

- Windows : %LOCALAPPDATA% \ Amazon Web Services \ Amazon \ logs WorkSpaces
- macOS — ~/Bibliothèque/"Support des applications » /"Amazon Web Services » /"Amazon » /logs WorkSpaces
- Linux (Ubuntu 18.04 ou version ultérieure) — /opt/workspacesclient/workspacesclient

Dans de nombreux cas, des informations de diagnostic ou de débogage peuvent être nécessaires pour une WorkSpaces session côté client. Les journaux clients avancés peuvent également être activés en ajoutant un « -l3 » au fichier exécutable des espaces de travail. Par exemple :

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

WorkSpaces Service Amazon

Le WorkSpaces service Amazon est intégré à Amazon CloudWatch Metrics, CloudWatch Events et CloudTrail. Cette intégration permet de connecter les données de performance et les appels d'API au AWS service central.

Lorsque vous gérez un WorkSpaces environnement Amazon, il est important de surveiller en permanence certains CloudWatch indicateurs afin de déterminer l'état de santé général de l'environnement. Métriques

Bien que d'autres CloudWatch métriques soient disponibles pour Amazon WorkSpaces (voir Monitor Your WorkSpaces Using CloudWatch Metrics), les trois métriques suivantes vous aideront à maintenir la disponibilité de l' WorkSpaceinstance :

- Insalubre — Le nombre d'articles WorkSpaces renvoyés à un état insalubre.
- SessionLaunchTime— Le temps nécessaire pour démarrer une WorkSpaces session.
- InSessionLatency— Le temps de trajet aller-retour entre le WorkSpaces client et le. WorkSpace

Pour plus d'informations sur les options de WorkSpaces journalisation, consultez Logging Amazon WorkSpaces API Calls by Using CloudTrail. Les CloudWatch événements supplémentaires aideront à capturer l'adresse IP côté client de la session utilisateur, le moment où l'utilisateur s'est connecté à la WorkSpaces session et le point de terminaison utilisé pendant la connexion. Tous ces détails aident à isoler ou à identifier les problèmes signalés par les utilisateurs lors des sessions de dépannage.

> **Note**
>
> Certaines CloudWatch métriques ne sont disponibles qu'avec AWS Managed AD.

Conteneurs et sous-système Windows pour Linux sur Amazon WorkSpaces

Conteneurs et Amazon WorkSpaces

L'informatique destinée aux utilisateurs finaux est souvent sollicitée par les clients qui souhaitent gérer des charges de travail liées à des conteneurs avec Amazon WorkSpaces. Bien que cela soit possible, il ne s'agit pas de la solution préférée ou recommandée. Les clients qui souhaitent tirer parti des économies potentielles en termes de coûts et d'exploitation liés aux conteneurs sont vivement invités à évaluer Amazon Elastic Container Service (Amazon ECS) et/ou Amazon Elastic Kubernetes Service (Amazon EKS).

Dans les cas où les exigences du client imposent d'activer les conteneurs à l'aide d'Amazon WorkSpaces, un guide technique a été publié pour permettre l'utilisation de Docker. Les clients doivent être informés que cela nécessite d'autres services de suivi et que les coûts et la complexité augmentent par rapport aux services de conteneurs natifs découplés.

Sous-système Windows pour Linux

Avec le lancement de Windows Server 2019 en tant que système d'exploitation sous-jacent d'Amazon WorkSpaces, les clients ont hâte de mettre en œuvre le sous-système Windows pour Linux (WSL), en particulier le WSL2. WSL2 invoquant une machine virtuelle (Hyper-V) pour exécuter ses fonctions, il ne peut pas fonctionner sur Amazon WorkSpaces, qui est géré par des hyperviseurs. AWS Les clients doivent savoir que seul le WSL1 sera disponible pour cette raison et comprendre les différences entre le WSL1 et le WSL2.

Amazon WorkSpaces Migrate

La fonctionnalité Amazon WorkSpaces Migrate vous permet d'intégrer les données de votre volume d'utilisateurs dans un nouveau bundle. Vous pouvez utiliser cette fonctionnalité pour :

- Passez WorkSpaces de l'expérience Windows 7 à l'expérience de bureau Windows 10.
- Migrez d'un PCoIP WorkSpace vers un protocole de WorkSpaces streaming (WSP). WorkSpace
- Migrez WorkSpaces d'un bundle public ou personnalisé à un autre. Par exemple, vous pouvez migrer des ensembles compatibles GPU (graphiques et GraphicsPro) vers des ensembles non compatibles avec le GPU, et vice versa.

Processus de migration

Avec WorkSpaces migrate, vous pouvez spécifier le WorkSpaces bundle cible. Le processus de migration recrée le volume WorkSpace en utilisant un nouveau volume racine à partir de l'image du bundle cible et le volume utilisateur à partir du dernier instantané du volume utilisateur d'origine. Un nouveau profil utilisateur est généré lors de la migration pour une meilleure compatibilité. Les données de votre ancien profil utilisateur qui ne peuvent pas être déplacées vers le nouveau profil sont stockées dans un dossier .NotMigrated.

Pendant la migration, les données du volume utilisateur (lecteur D) sont préservées, mais toutes les données du 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. NotMigrated suffixe, et un nouveau profil utilisateur est créé.

Le processus de migration prend jusqu'à une heure par migration WorkSpace. En outre, si le flux de travail de migration ne parvient pas à terminer le processus, le service rétablira automatiquement son état d'origine avant la WorkSpace migration, minimisant ainsi tout risque de perte de données.

Toutes les balises attribuées à l'original WorkSpace sont reportées lors de la migration. Le mode de fonctionnement du WorkSpace est préservé. La personne migrée WorkSpace possède un nouvel WorkSpace identifiant, un nouveau nom d'ordinateur et une nouvelle adresse IP. Procédure de migration

Vous pouvez effectuer la migration WorkSpaces via la WorkSpaces console Amazon, à l' AWS CLI aide de la commande migrate-workspace ou de l'API Amazon WorkSpaces . Toutes les demandes

de migration sont mises en file d'attente et le service limite automatiquement le nombre total de demandes de migration s'il y en a trop. Limites de migration

- Vous ne pouvez pas migrer vers un bundle d'expérience de bureau Windows 7 public ou personnalisé.
- Vous ne pouvez pas migrer vers des bundles BYOL Windows 7.
- Vous ne pouvez migrer le BYOL WorkSpaces que vers d'autres bundles BYOL.
- Vous ne pouvez pas migrer un bundle WorkSpace créé à partir de bundles publics ou personnalisés vers un bundle BYOL.
- 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 tant 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.
- WorkSpaces ne peuvent pas être migrés lorsqu'ils sont en mode ADMIN_MAINTENANCE.

Coût

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.

WorkSpaces meilleures pratiques en matière de migration

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 vous référer à 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 de leur WorkSpaces compte et ne se reconnectent qu'une fois le processus de migration terminé.
- Assurez-vous que le statut du WorkSpaces fichier que vous souhaitez migrer est DISPONIBLE, STOPPÉ 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.

Framework Well-Architected

AWS Well-Architected aide les architectes du cloud à créer une infrastructure sécurisée, performante, résiliente et efficace pour leurs applications et leurs charges de travail. Il décrit les concepts clés, les principes de conception et les meilleures pratiques architecturales pour la conception et l'exécution de charges de travail dans le cloud. Il repose sur cinq piliers essentiels :

- Excellence opérationnelle
- Sécurité
- Fiabilité
- Efficacité des performances
- Optimisation des coûts

Lors de l'architecture d'un WorkSpaces environnement Amazon, il est important d'évaluer ces piliers clés afin de déterminer le niveau de maturité du déploiement et de découvrir des fonctionnalités supplémentaires pouvant être utilisées avec Amazon WorkSpaces. Bien qu'il existe des directives générales pour le cadre AWS Well-Architect, voici quelques questions clés qui peuvent être incluses dans la phase de planification de votre WorkSpaces déploiement afin de garantir que chacun des cinq piliers est pris en compte.

Général

- Quel est le moteur commercial de ce projet ?

Excellence opérationnelle

- Comment répartissez-vous le contrôle d'accès entre les utilisateurs et les différents groupes d'administrateurs ?

Sécurité

1. Quelles sont les exigences de sécurité et de conformité à prendre en compte WorkSpaces pour opérer ?
2. Existe-t-il des restrictions concernant le routage vers des adresses IP externes ?

3. Les WorkSpaces ports requis sont-ils autorisés à passer par le pare-feu de l'entreprise ?
4. L'authentification multifactorielle est-elle ou sera-t-elle utilisée dans le cadre de ce déploiement ?
5. Combien d'identités d'utilisateurs et de demandes d'autorisation faites-vous aujourd'hui ?

Fiabilité

1. Quelle est la politique de conservation des données pour les ordinateurs de bureau ?
2. Qu'est-ce que l'objectif de point de restauration (RPO) pour les données des utilisateurs finaux ?
3. Quel est l'objectif de temps de restauration (RTO) pour les données des utilisateurs finaux ?

Optimisation des coûts

1. WorkSpaces Les packs ont-ils été adaptés au cas utilisateur et aux applications ?
2. Les utilisateurs WorkSpaces consommeront-ils plus de 82 heures par mois ?

Bien que les questions ci-dessus ne constituent pas une liste exhaustive des éléments à prendre en compte, elles fournissent des conseils généraux pour vous aider à déployer Well-Architected Amazon. WorkSpaces

Sécurité

Cette section explique comment sécuriser les données à l'aide du chiffrement lors de l'utilisation WorkSpaces des services Amazon. Il décrit le chiffrement en transit et au repos, ainsi que l'utilisation de groupes de sécurité pour protéger l'accès réseau au WorkSpaces. Cette section fournit également des informations sur la façon de contrôler l'accès aux appareils finaux à WorkSpaces l'aide de périphériques sécurisés et de groupes de contrôle d'accès IP.

Vous trouverez des informations supplémentaires sur l'authentification (y compris le support MFA) dans le AWS Directory Service dans cette section.

Chiffrement en transit

Amazon WorkSpaces utilise la cryptographie pour protéger la confidentialité à différentes étapes de la communication (en transit) et également pour protéger les données au repos (cryptées WorkSpaces). Les processus de chaque étape du chiffrement utilisé par Amazon pendant WorkSpaces le transport sont décrits dans les sections suivantes.

Pour plus d'informations sur le chiffrement au repos, reportez-vous à la WorkSpaces section Chiffrée de ce document.

Inscription et mises à jour

L'application cliente de bureau communique avec Amazon pour les mises à jour et l'enregistrement via HTTPS.

Étape d'authentification

Le client de bureau initie l'authentification en envoyant des informations d'identification à la passerelle d'authentification. La communication entre le client de bureau et la passerelle d'authentification utilise le protocole HTTPS. À la fin de cette étape, si l'authentification réussit, la passerelle d'authentification renvoie un jeton OAuth 2.0 au client de bureau, via la même connexion HTTPS.

> **Note**
>
> L'application client de bureau prend en charge l'utilisation d'un serveur proxy pour le trafic du port 443 (HTTPS), pour les mises à jour, l'enregistrement et l'authentification.

Après avoir reçu les informations d'identification du client, la passerelle d'authentification envoie une demande d'authentification au AWS Directory Service. La communication entre la passerelle d'authentification et le AWS Directory Service s'effectue via HTTPS, de sorte qu'aucun identifiant utilisateur n'est transmis en texte clair.

Authentification — Connecteur Active Directory (ADC)

AD Connector utilise Kerberos pour établir une communication authentifiée avec AD sur site, afin de pouvoir se lier à LDAP et exécuter les requêtes LDAP suivantes. Le support LDAPS côté client dans ADC est également disponible pour chiffrer les requêtes entre Microsoft AD et Applications. AWS Avant d'implémenter la fonctionnalité LDAPS côté client, passez en revue les conditions requises pour le LDAPS côté client.

Le AWS Directory Service prend également en charge le protocole LDAP avec TLS. Aucune information d'identification utilisateur n'est transmise en texte clair à aucun moment. Pour une sécurité accrue, il est possible de connecter un WorkSpaces VPC au réseau local (où réside AD) à l'aide d'une connexion VPN. Lorsqu'ils utilisent une connexion VPN AWS matérielle, les clients peuvent configurer le chiffrement en transit en utilisant les normes IPSEC (Internet Key Exchange (IKE) et IPSEC SaS) avec des clés de chiffrement symétriques AES-128 ou AES-256, SHA-1 ou SHA-256 pour le hachage d'intégrité et des groupes DH (2,14-18, 22, 23 et 24 pour la phase 2) en utilisant une confidentialité directe (PFS)).

Étape de courtier

Après avoir reçu le jeton OAuth 2.0 (depuis la passerelle d'authentification, si l'authentification a réussi), le client de bureau interroge les WorkSpaces services Amazon (Broker Connection Manager) via HTTPS. Le client de bureau s'authentifie en envoyant le jeton OAuth 2.0 et, par conséquent, le client reçoit les informations de point de terminaison de la passerelle de streaming. WorkSpaces

Étape de diffusion

Le client de bureau demande l'ouverture d'une session PCoIP avec la passerelle de streaming (à l'aide du jeton OAuth 2.0). Cette session est cryptée en AES-256 et utilise le port PCoIP pour le contrôle des communications (4172/TCP).

À l'aide du jeton OAuth2.0, la passerelle de streaming demande les WorkSpaces informations spécifiques à l'utilisateur au WorkSpaces service Amazon, via HTTPS.

La passerelle de streaming reçoit également le TGT du client (qui est chiffré à l'aide du mot de passe de l'utilisateur du client) et, en utilisant le transfert Kerberos TGT, la passerelle initie une connexion Windows sur le, en utilisant le TGT Kerberos récupéré par l' WorkSpaceutilisateur.

Il lance WorkSpace ensuite une demande d'authentification auprès du AWS Directory Service configuré, en utilisant l'authentification Kerberos standard.

Une fois WorkSpace connecté avec succès, le streaming PCoIP démarre. La connexion est initiée par le client sur le port TCP 4172 avec le trafic de retour sur le port UDP 4172. De plus, la connexion initiale entre la passerelle de streaming et un WorkSpaces poste de travail via l'interface de gestion se fait via le protocole UDP 55002. (Reportez-vous à la documentation pour connaître les exigences en matière d'adresse IP et de port pour Amazon WorkSpaces. Le port UDP sortant initial est 55002.) La connexion de streaming, utilisant les ports 4172 (TCP et UDP), est cryptée à l'aide de chiffrements AES 128 et 256 bits, mais par défaut, 128 bits. Les clients peuvent modifier activement ce paramètre en 256 bits, soit en utilisant les paramètres de stratégie de groupe AD spécifiques à PCoIP pour Windows WorkSpaces, soit avec le fichier pcoip-agent.conf pour Amazon Linux. WorkSpaces Pour plus d'informations sur l'administration des politiques de groupe pour Amazon WorkSpaces, consultez la documentation.

Interfaces réseau

Chaque Amazon WorkSpace possède deux interfaces réseau, appelées interface réseau principale et interface réseau de gestion.

L'interface réseau principale fournit la connectivité aux ressources du VPC du client, telles que l'accès au AWS Directory Service, à Internet et au réseau d'entreprise du client. Il est possible d'associer des groupes de sécurité à cette interface réseau principale. Conceptuellement, les groupes de sécurité attachés à cette ENI sont différenciés en fonction de l'étendue du déploiement : groupe de WorkSpaces sécurité et groupes de sécurité ENI.

Interface réseau de gestion

L'interface réseau de gestion ne peut pas être contrôlée par le biais de groupes de sécurité ; toutefois, les clients peuvent utiliser un pare-feu basé sur l'hôte WorkSpaces pour bloquer les ports ou contrôler l'accès. Nous ne recommandons pas d'appliquer des restrictions à l'interface du réseau de gestion. Si un client décide d'ajouter des règles de pare-feu basées sur l'hôte pour gérer cette interface, quelques ports doivent être ouverts afin que le WorkSpaces service Amazon puisse gérer l'état et l'accessibilité du. WorkSpace Pour plus d'informations, reportez-vous à la section Interfaces réseau du guide d'administration d'Amazon Workspaces.

WorkSpaces groupes de sécurité

Un groupe de sécurité par défaut est créé par AWS Directory Service et est automatiquement attaché à tous WorkSpaces ceux qui appartiennent à ce répertoire spécifique.

Amazon WorkSpaces, comme de nombreux autres AWS services, utilise des groupes de sécurité. Amazon WorkSpaces crée deux groupes AWS de sécurité lorsque vous enregistrez un annuaire auprès du WorkSpaces service. Un pour les contrôleurs de répertoire DirectoryID_Controllers et un pour WorkSpaces le répertoire DirectoryID_WorkspacesMembers. Ne supprimez aucun de ces groupes de sécurité, sinon vous WorkSpaces serez affaibli. Par défaut, la sortie du groupe de sécurité WorkSpaces Membres est ouverte à 0.0.0.0/0. 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. Lorsque vous associez plusieurs groupes de sécurité à un WorkSpaces annuaire, WorkSpaces regroupez les règles de chaque groupe de sécurité en un seul 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, reportez-vous à la section Groupes de sécurité pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Pour plus d'informations sur l'ajout d'un groupe de sécurité à un WorkSpaces répertoire ou à un répertoire existant WorkSpace, consultez le guide de l'WorkSpaces administrateur.

Certains clients souhaitent restreindre les ports et les destinations par lesquels le WorkSpaces trafic peut sortir. Pour limiter le trafic sortant du WorkSpaces, vous devez vous assurer de laisser les ports spécifiques nécessaires aux communications de service ; sinon, vos utilisateurs ne pourront pas se connecter à leur WorkSpaces.

WorkSpaces utiliser l'Elastic Network Interface (ENI) dans le VPC du client pour communiquer avec les contrôleurs de domaine lors de la WorkSpace connexion. Pour permettre à vos utilisateurs de s'y connecter WorkSpaces correctement, vous devez autoriser les ports suivants à accéder à vos contrôleurs de domaine ou aux plages d'adresses CIDR qui incluent vos contrôleurs de domaine dans le groupe de sécurité _WorkspacesMembers.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- TCP/UDP 389 — LDAP

- TCP/UDP 445 - SMB
- TCP 3268-3269 - Catalogue global
- TCP/UDP 464 - Modification du mot de passe Kerberos
- TCP 139 - Netlogon
- UDP 137-138 - Netlogon
- UDP 123 - NTP
- Ports éphémères TCP/UDP 49152-65535 pour RPC

Si vous WorkSpaces devez accéder à d'autres applications, à Internet ou à d'autres emplacements, vous devez autoriser ces ports et destinations en notation CIDR au sein du groupe de sécurité _WorkspacesMembers. Si vous n'ajoutez pas ces ports et destinations, ils n'atteindront rien d'autre que les ports listés ci-dessus. WorkSpaces Enfin, par défaut, un nouveau groupe de sécurité n'a aucune règle de trafic entrant. Par conséquent, aucun trafic entrant issu d'un autre hôte de votre instance n'est autorisé tant que vous n'avez pas ajouté des règles entrantes au groupe de sécurité. Les étapes ci-dessus ne sont requises que si vous souhaitez limiter la sortie WorkSpaces ou verrouiller les règles d'entrée uniquement aux ressources ou aux plages d'adresses CIDR qui devraient y avoir accès.

> **Note**
>
> Un nouveau groupe de sécurité associé ne sera attaché qu'aux groupes WorkSpaces créés ou reconstruits après la modification.

Groupes de sécurité ENI

L'interface réseau principale étant une ENI classique, elle peut être gérée à l'aide AWS des différents outils de gestion. Pour plus d'informations, reportez-vous à Elastic Network Interfaces. Accédez à l'adresse WorkSpace IP (WorkSpaces sur la page de la WorkSpaces console Amazon), puis utilisez cette adresse IP comme filtre pour trouver l'ENI correspondant (dans la section Interfaces réseau de la console Amazon EC2).

Une fois l'ENI localisé, il peut être géré directement par les groupes de sécurité. Lorsque vous attribuez manuellement des groupes de sécurité à l'interface réseau principale, tenez compte des exigences en matière de port d'Amazon WorkSpaces. Pour plus d'informations, reportez-vous à la section Interfaces réseau du guide d'administration d'Amazon Workspaces.

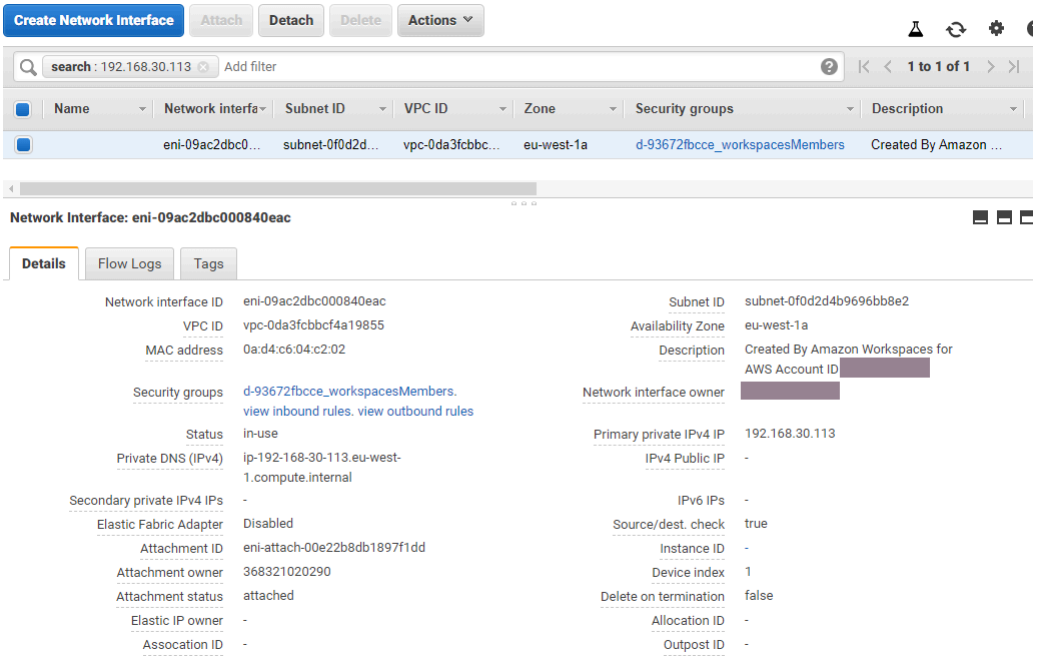

Figure 21 : WorkSpaces client avec MFA activée

Listes de contrôle d'accès réseau (ACL)

En raison de la complexité accrue de la gestion d'un autre pare-feu, les ACL réseau sont couramment utilisées dans des déploiements très complexes et ne constituent généralement pas une bonne pratique. Comme les ACL réseau sont attachées aux sous-réseaux du VPC, leur fonction se concentre sur la couche 3 (réseau) du modèle OSI. Amazon WorkSpaces étant conçu sur les services d'annuaire, deux sous-réseaux doivent être définis. Les ACL réseau sont gérées séparément des services d'annuaire, et il est fort probable qu'une ACL réseau soit attribuée à un seul des sous-réseaux WorkSpaces « assignés ».

Lorsqu'un pare-feu sans état est requis, les listes de contrôle d'accès réseau constituent une bonne pratique en matière de sécurité. Assurez-vous que toutes les modifications apportées aux ACL réseau au-delà des paramètres par défaut sont validées par sous-réseau, conformément à la meilleure pratique. Si les ACL réseau ne fonctionnent pas comme prévu, pensez à utiliser les journaux de flux VPC pour analyser le trafic.

AWS Network Firewall

AWS Network Firewall offre des fonctionnalités allant au-delà de celles proposées par les groupes de sécurité natifs et les ACL réseau, mais moyennant un coût. Lorsque les clients ~~ont~~ demandé

la possibilité de renforcer la sécurité des connexions réseau, telles que l'inspection des noms de serveur (SNI) pour les sites Web basés sur HTTPS, la détection et la prévention des intrusions et une liste d'autorisation et de refus pour les noms de domaine, ils ont dû trouver d'autres pare-feux sur le. AWS Marketplace La complexité du déploiement de ces pare-feux présentait des défis qui dépassaient les compétences des administrateurs EUC standard. AWS Network Firewall offre une AWS expérience native tout en activant les protections des couches 3 à 7. L'utilisation de AWS Network Firewall en conjonction avec NAT Gateway est une bonne pratique lorsque les entreprises ne disposent d'aucun autre moyen (licences sur site existantes pour les pare-feux tiers pouvant être transférés vers le cloud ou équipes distinctes qui gèrent les pare-feux exclues) pour couvrir toutes les protections du réseau EUC. NAT Gateway est également gratuit avec AWS Network Firewall.

Les déploiements de AWS Network Firewall sont conçus sur la base de la conception EUC existante. Les conceptions à VPC unique permettent d'obtenir une architecture simplifiée avec des sous-réseaux pour les points de terminaison du pare-feu et des considérations distinctes relatives au routage des sorties Internet, tandis que les conceptions à VPC multiples tirent parti d'un VPC d'inspection consolidé avec points de terminaison pare-feu et passerelles de transit.

Scénarios de conception

Scénario 1 : verrouillage de base de l'instance

Le groupe WorkSpaces de sécurité par défaut n'autorise aucun trafic entrant, car les groupes de sécurité sont refusés par défaut et dotés d'un état. Cela signifie qu'aucune configuration supplémentaire ne doit être configurée pour sécuriser davantage les WorkSpaces instances elles-mêmes. Tenez compte des règles sortantes qui autorisent tout le trafic, et déterminez si cela correspond au cas d'utilisation. Par exemple, il peut être préférable de refuser tout le trafic sortant vers le port 443, quelle que soit l'adresse, ainsi que les plages d'adresses IP spécifiques adaptées aux cas d'utilisation des ports, telles que 389 pour LDAP, 636 pour LDAPS, 445 pour SMB, entre autres ; notez toutefois que la complexité de l'environnement peut nécessiter plusieurs règles et qu'il est donc préférable de le faire via des ACL réseau ou un dispositif de pare-feu.

Scénario 2 : Exceptions entrantes

Bien qu'il ne s'agisse pas d'une exigence constante, il peut arriver que le trafic réseau soit initié en provenance de WorkSpaces. Par exemple, le triage des instances lorsque le WorkSpaces client ne peut pas se connecter nécessite une autre connectivité à distance. Dans ces cas, il est préférable d'activer temporairement le protocole TCP 3389 entrant pour le groupe de sécurité du client ENI WorkSpace du client.

Un autre scénario est celui des scripts organisationnels qui exécutent des commandes pour les fonctions d'inventaire ou d'automatisation, initiées par une instance centralisée. La sécurisation du trafic sur ce port à partir de ces instances centralisées spécifiques sur le trafic entrant peut être configurée de manière permanente. Toutefois, il est recommandé de le faire sur le groupe de sécurité supplémentaire attaché à la configuration du répertoire, car il peut être appliqué à plusieurs déploiements dans le AWS compte.

Enfin, certains trafics réseau ne sont pas basés sur l'état et nécessiteront que des ports éphémères soient spécifiés dans les exceptions entrantes. Si les requêtes et les scripts échouent, il est recommandé d'autoriser les ports éphémères, au moins temporairement, tout en déterminant la cause première de la panne de connectivité.

Scénario 3 : inspection d'un seul VPC

Les déploiements simplifiés WorkSpaces (tels qu'un VPC unique sans plan de dimensionnement) ne nécessitent pas de VPC distinct pour l'inspection. La connexion à d'autres VPC peut donc être simplifiée grâce au peering VPC. Cependant, des sous-réseaux distincts pour les points de terminaison du pare-feu doivent être créés avec le routage configuré vers ces points de terminaison ainsi que le routage de sortie Internet Gateway (IGW), qui n'aurait pas besoin d'être configuré autrement. Les déploiements existants peuvent ne pas disposer de l'espace IP disponible si tous les sous-réseaux utilisent l'intégralité du bloc d'adresse CIDR VPC. Dans ces cas, le scénario 4 peut être plus efficace car le déploiement a déjà dépassé sa conception initiale.

Scénario 4 : Inspection centralisée

Souvent préféré dans le cadre de plusieurs déploiements EUC dans une même AWS région, ce qui simplifie l'administration des règles statiques et apatrides du pare-feu AWS réseau. Les homologues VPC existants seront remplacés par des passerelles de transit, car cette conception nécessite l'utilisation de pièces jointes Transit Gateway ainsi que le routage d'inspection qui ne peut être configuré que via ces pièces jointes. Un plus grand contrôle est également exercé sur cette configuration, ce qui permet une sécurité allant au-delà de l' WorkSpaces expérience par défaut.

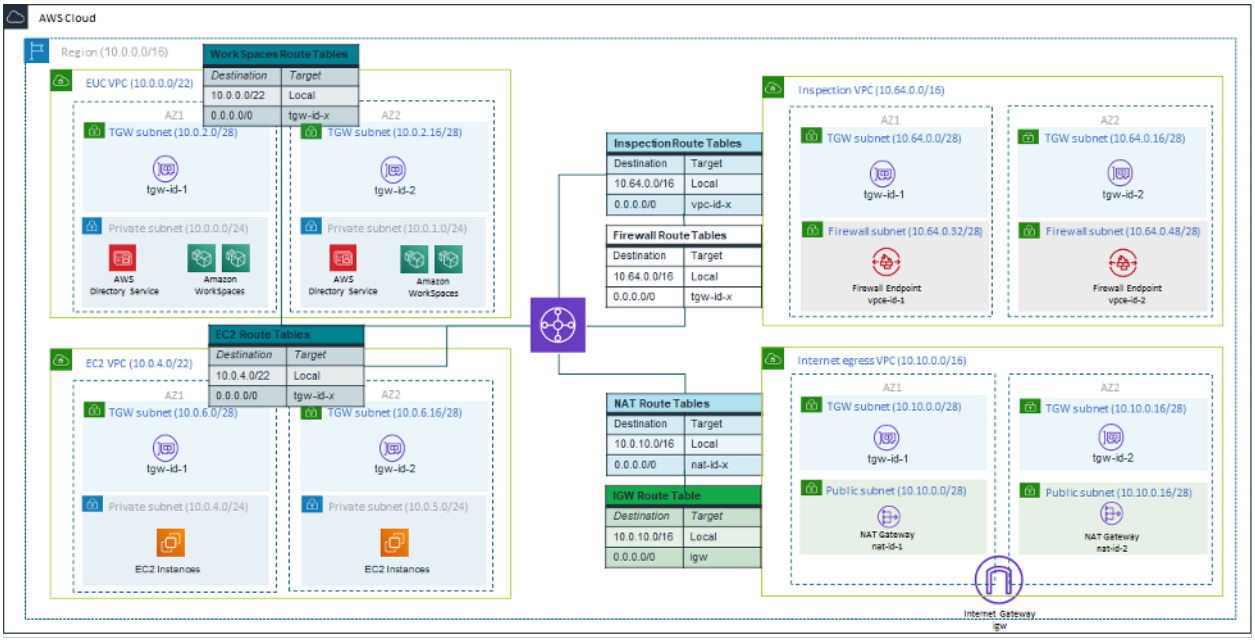

Figure 22 : Exemple d'architecture utilisant les pièces jointes Transit Gateway

Chiffré WorkSpaces

Chaque Amazon WorkSpace est approvisionné avec un volume racine (C : lecteur pour Windows WorkSpaces, racine pour Amazon Linux WorkSpaces) et un volume utilisateur (D : lecteur pour Windows WorkSpaces, /home pour Amazon Linux WorkSpaces). La WorkSpaces fonction cryptée permet de chiffrer un ou les deux volumes.

Qu'est-ce qui est chiffré ?

Les données stockées au repos, les entrées/sorties (E/S) du disque vers le volume et les instantanés créés à partir de volumes chiffrés sont tous chiffrés.

Quand le chiffrement a-t-il lieu ?

Le chiffrement d'un WorkSpace doit être spécifié lors du lancement (création) du WorkSpace. WorkSpaces les volumes ne peuvent être chiffrés qu'au moment du lancement : après le lancement, l'état de chiffrement des volumes ne peut pas être modifié. La figure suivante montre la page de WorkSpaces console Amazon permettant de choisir le chiffrement lors du lancement d'un nouveau système WorkSpace.

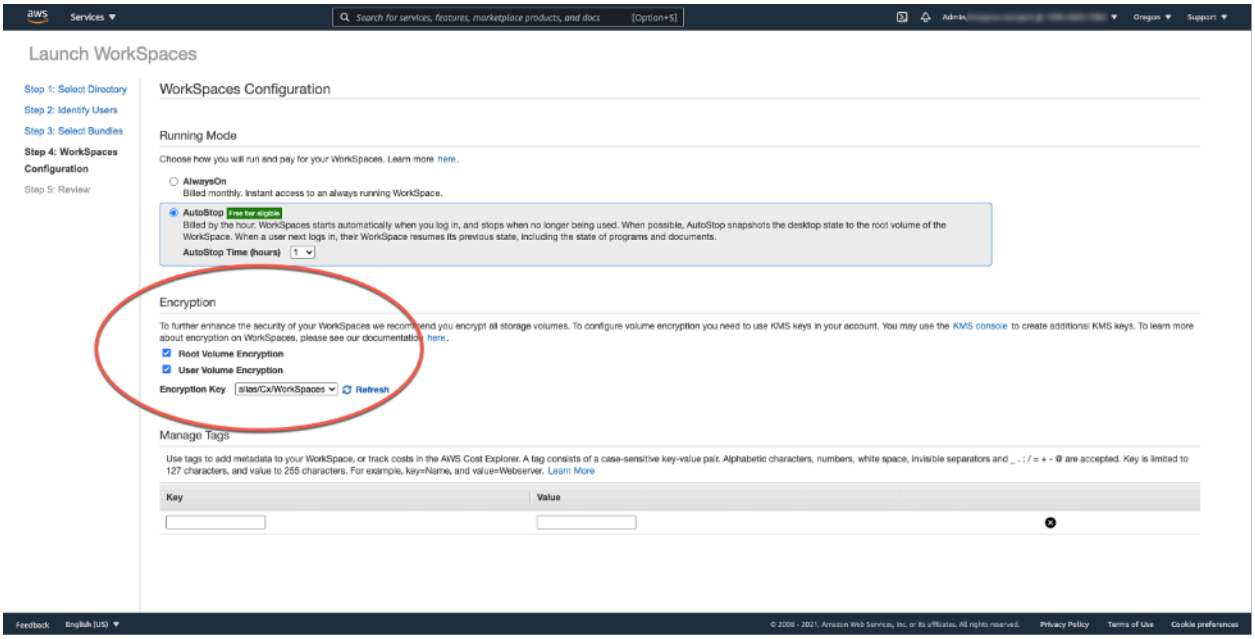

Figure 23 : Chiffrement des volumes WorkSpace racines

Comment est WorkSpace crypté un nouveau produit ?

Un client peut choisir l' WorkSpaces option Encrypted depuis la WorkSpaces console Amazon ou en utilisant l' WorkSpaces API Amazon lorsqu'il lance une nouvelle application WorkSpace. AWS CLI

Pour chiffrer les volumes, Amazon WorkSpaces utilise une clé CMK provenant de AWS Key Management Service ()AWS KMS. Une clé AWS KMS CMK par défaut est créée la première fois qu'une clé WorkSpace est lancée dans une région. (Les CMK ont une portée régionale.)

Un client peut également créer une clé CMK gérée par le client à utiliser avec le chiffrement. WorkSpaces Le CMK est utilisé pour chiffrer les clés de données utilisées par le WorkSpaces service Amazon pour chiffrer chacun des volumes. WorkSpace (Au sens strict, c'est Amazon EBS qui chiffrera les volumes). Pour connaître les limites CMK actuelles, reportez-vous à la section Quotas de AWS KMS ressources.

> **Note**
>
> La création d'images personnalisées à partir d'une image cryptée n' WorkSpace est pas prise en charge. En outre, le provisionnement d'un produit WorkSpaces lancé avec le chiffrement du volume racine activé peut prendre jusqu'à une heure.

Pour une description détaillée du processus de WorkSpaces chiffrement, reportez-vous à la section Comment Amazon l' WorkSpaces utilise AWS KMS. Réfléchissez à la manière dont l'utilisation de CMK sera surveillée pour garantir qu'une demande de chiffrement WorkSpace est traitée correctement. Pour plus d'informations sur AWS KMS les clés et les clés de données, consultez la AWS KMS page.

Options de contrôle d'accès et appareils fiables

Amazon WorkSpaces propose aux clients des options leur permettant de gérer les appareils clients auxquels ils peuvent accéder WorkSpaces. Les clients peuvent limiter WorkSpaces l'accès aux appareils fiables uniquement. L'accès à WorkSpaces peut être autorisé à partir de macOS et de PC Microsoft Windows à l'aide de certificats numériques. Il peut également autoriser ou bloquer l'accès pour les clients iOS, Android, Chrome OS, Linux et Zero, ainsi que pour le client WorkSpaces Web Access. Grâce à ces fonctionnalités, il peut encore améliorer la posture de sécurité.

Les options de contrôle d'accès sont activées pour les nouveaux déploiements afin que les utilisateurs puissent y accéder WorkSpaces depuis des clients sous Windows, macOS, iOS, Android, ChromeOS et Zero Clients. L'accès via Web Access ou un WorkSpaces client Linux n'est pas activé par défaut pour un nouveau WorkSpaces déploiement et devra être activé.

Si l'accès aux données d'entreprise à partir d'appareils sécurisés (également appelés appareils administrés) est limité, WorkSpaces l'accès peut être limité aux appareils sécurisés dotés de certificats valides. Lorsque cette fonctionnalité est activée, Amazon WorkSpaces utilise une 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.

Un support fiable pour les appareils est disponible pour les clients suivants :

- Application Amazon WorkSpaces Android Client sur Google Play qui fonctionne sur les appareils Android et Chrome OS compatibles avec Android
- Application Amazon WorkSpaces macOS Client exécutée sur des appareils macOS
- Application Amazon WorkSpaces Windows Client exécutée sur des appareils Windows

Pour plus d'informations sur le contrôle des appareils autorisés à accéder WorkSpaces, reportez-vous à la section Restreindre WorkSpaces l'accès aux appareils fiables.

> **Note**
>
> Les certificats pour appareils fiables s'appliquent uniquement aux clients Amazon WorkSpaces Windows, macOS et Android. Cette fonctionnalité ne s'applique pas au client Amazon WorkSpaces Web Access, ni aux clients tiers, y compris, mais sans s'y limiter, au logiciel Teradici PCoIP et aux clients mobiles, aux clients Teradici PCoIP zéro, aux clients RDP et aux applications de bureau à distance.

Groupes de contrôle d'accès IP

À l'aide de groupes de contrôle basés sur les adresses IP, les clients peuvent définir et gérer des groupes d'adresses IP fiables, et autoriser les utilisateurs à accéder à leurs adresses WorkSpaces uniquement lorsqu'ils sont connectés à un réseau fiable. Cette fonctionnalité permet aux clients de mieux contrôler leur niveau de sécurité.

Des groupes de contrôle d'accès IP peuvent être ajoutés au niveau du WorkSpaces répertoire. Il existe deux manières de commencer à utiliser les groupes de contrôle d'accès IP.

- Page Contrôles d'accès IP — À partir de la console de WorkSpaces gestion, des groupes de contrôle d'accès IP peuvent être créés sur la page Contrôles d'accès IP. Des règles peuvent être ajoutées à ces groupes en saisissant les adresses IP ou les plages d'adresses IP à partir desquelles il est WorkSpaces possible d'accéder. Ces groupes peuvent ensuite être ajoutés aux annuaires sur la page Détails de la mise à jour.
- API d'espace de travail : les WorkSpaces API peuvent être utilisées pour créer, supprimer et afficher des groupes, créer ou supprimer des règles d'accès, ou pour ajouter et supprimer des groupes dans des annuaires.

Pour une description détaillée de l'utilisation des groupes de contrôle d'accès IP dans le cadre du processus de WorkSpaces chiffrement Amazon, reportez-vous à la section Groupes de contrôle d'accès IP pour vous WorkSpaces.

Surveillance ou journalisation à l'aide d'Amazon CloudWatch

La surveillance du réseau, des serveurs et des journaux fait partie intégrante de toute infrastructure. Les clients qui déploient Amazon WorkSpaces doivent surveiller leurs déploiements, en particulier l'état de santé général et l'état de connexion de chacun WorkSpaces.

CloudWatch Métriques Amazon pour WorkSpaces

CloudWatch metrics for WorkSpaces est conçu pour fournir aux administrateurs des informations supplémentaires sur l'état de santé général et l'état de connexion d'un individu WorkSpaces. Les métriques sont disponibles par WorkSpace ou agrégées pour tous les membres WorkSpaces d'une organisation au sein d'un annuaire donné.

Ces métriques, comme toutes les CloudWatch métriques, peuvent être consultées dans le AWS Management Console (illustré dans la figure suivante), accessibles via les CloudWatch API et surveillées par des CloudWatch alarmes et des outils tiers.

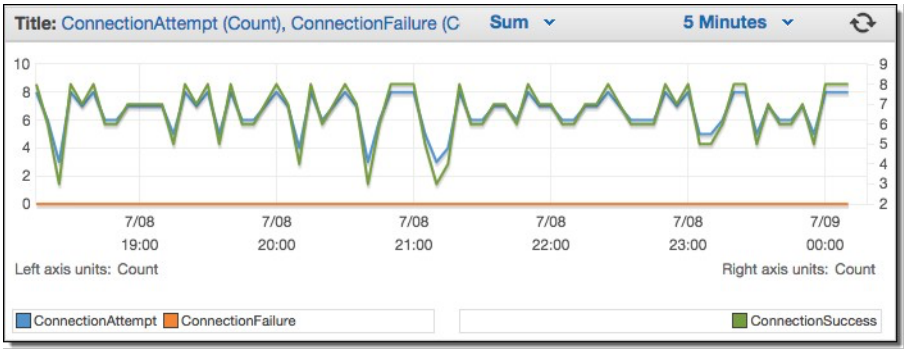

Figure 24 : CloudWatch mesures ConnectionAttempt :/ ConnectionFailure

Par défaut, les mesures suivantes sont activées et sont disponibles sans frais supplémentaires :

- Disponible : WorkSpaces les réponses à une vérification de statut sont prises en compte dans cette métrique.
- Malsain : WorkSpaces ceux qui ne répondent pas à la même vérification de statut sont pris en compte dans cette métrique.
- ConnectionAttempt— Le nombre de tentatives de connexion effectuées vers un WorkSpace.
- ConnectionSuccess— Le nombre de tentatives de connexion réussies.
- ConnectionFailure— Le nombre de tentatives de connexion infructueuses.
- SessionLaunchTime— Le temps nécessaire pour démarrer une session, tel que mesuré par le WorkSpaces client.
- InSessionLatency— Le temps de trajet aller-retour entre le WorkSpaces client et WorkSpaces, tel que mesuré et indiqué par le client.
- SessionDisconnect— Le nombre de sessions initiées par l'utilisateur et fermées automatiquement.

En outre, des alarmes peuvent être créées, comme le montre la figure suivante.

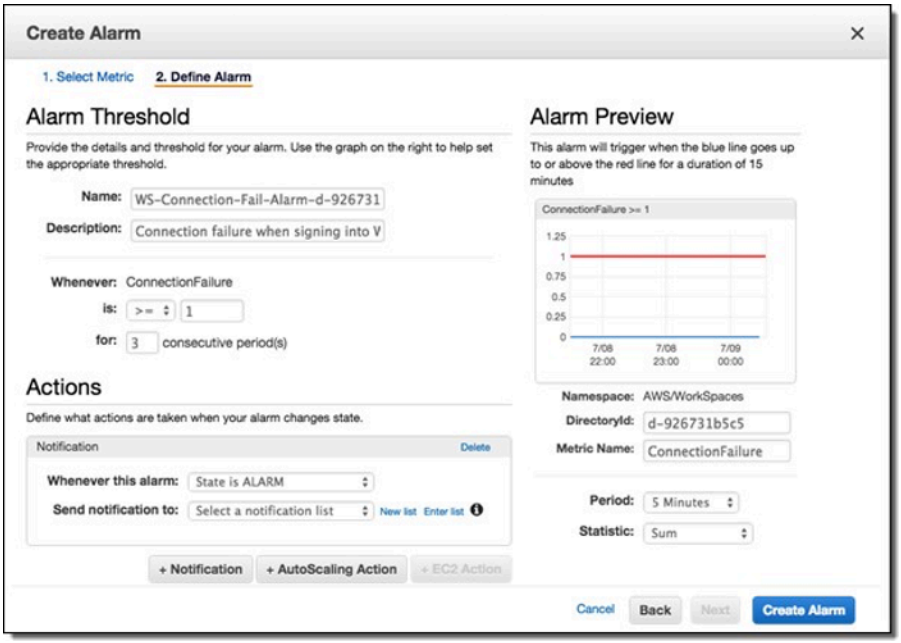

Figure 25 : Création CloudWatch d'une alarme en cas d'erreur de WorkSpaces connexion

Amazon CloudWatch Events pour WorkSpaces

Les événements d'Amazon CloudWatch Events peuvent être utilisés pour afficher, rechercher, télécharger, archiver, analyser et répondre aux connexions réussies à WorkSpaces. Le service peut surveiller les adresses IP WAN des clients, le système d'exploitation, l' WorkSpaces identifiant et les informations d'identifiant de répertoire auxquelles les utilisateurs se WorkSpaces connectent. Par exemple, il peut 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' CloudWatch événement d'WorkSpaces accès.
- Utilisez les contrôles de stratégie pour bloquer l'accès aux fichiers et applications à partir d'adresses IP non autorisées.

Pour plus d'informations sur l'utilisation d' CloudWatch Events, consultez le guide de l'utilisateur Amazon CloudWatch Events. Pour en savoir plus sur les CloudWatch événements pour WorkSpaces, reportez-vous à la section Surveiller votre WorkSpaces utilisation de Cloudwatch Events.

YubiKey support pour Amazon WorkSpaces

Afin d'ajouter une couche de sécurité supplémentaire, les clients choisissent souvent de sécuriser les outils et les sites avec une authentification multifactorielle. Certains clients choisissent de le faire avec un Yubico YubiKey. Amazon WorkSpaces prend en charge à la fois les codes d'accès à usage unique (OTP) et le protocole d'authentification FIDO U2F avec. YubiKeys

Amazon prend WorkSpaces actuellement en charge le mode OTP, et aucune étape supplémentaire n'est requise de la part d'un administrateur ou d'un utilisateur final pour utiliser un YubiKey avec OTP. L'utilisateur peut le connecter YubiKey à son ordinateur, s'assurer que le clavier est focalisé dans le WorkSpace (en particulier dans le champ où l'OTP doit être saisi) et toucher le contact doré duYubiKey. L'OTP YubiKey sera automatiquement saisi dans le champ sélectionné.

Pour utiliser le mode FIDO U2F avec YubiKey et WorkSpaces, des étapes supplémentaires sont nécessaires. Assurez-vous que vos utilisateurs disposent de l'un de ces YubiKey modèles pris en charge afin d'utiliser la redirection U2F avec : WorkSpaces

- YubiKey 4
- YubiKey 5 NFC
- YubiKey 5 Nano
- YubiKey 5C
- YubiKey 5C Nano
- YubiKey 5 NFC

Pour activer la redirection USB pour YubiKey U2F

Par défaut, la redirection USB est désactivée pour PCoIP WorkSpaces ; pour utiliser le mode U2F avec YubiKeys, vous devez l'activer.

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).

2. Sur une instance d'administration d'annuaire WorkSpace ou 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. Pour permettre à l'utilisateur de modifier vos paramètres, choisissez Overridable Administrator Defaults. Sinon, choisissez Not Overridable Administrator Defaults.
4. Ouvrez le paramètre Activer/désactiver l'USB dans la session PCOIP.
5. Choisissez Activé, puis OK.
6. Ouvrez le paramètre Configurer les règles relatives aux périphériques USB autorisés et non autorisés par PCoIP.
7. Choisissez Activé, puis sous Entrer le tableau d'autorisation USB (10 règles maximum), configurez les règles de la liste d'autorisation du périphérique USB.
   a. 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 le `1xxxxyyyy` suivant : VID au format hexadécimal et `yyyy` PID au format hexadécimal. `xxxx` Dans cet exemple, 1050 est le VID et 0407 le PID. Pour plus de valeurs YubiKey USB, reportez-vous à la section Valeurs d'identification YubiKey USB.
8. Sous Entrez le tableau d'autorisation USB (dix règles maximum), configurez les règles de la liste de blocage de votre périphérique USB.
   a. 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, reportez-vous à Teradici PCoIP Standard Agent pour Windows

9. Choisissez OK.
10. 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 Amazon, sélectionnez le WorkSpace, puis choisissez Actions, Redémarrer WorkSpaces).

b. Dans une invite de commande administrative, entrez gpupdate /force.

11. Une fois le réglage pris en compte, tous les périphériques USB pris en charge pourront être redirigés, WorkSpaces sauf si des restrictions sont configurées via le paramètre des règles relatives aux périphériques USB.

Une fois que vous avez activé la redirection USB pour YubiKey U2F, vous pouvez utiliser le mode Fido U2F. YubiKey

Optimisation des coûts

Fonctionnalités de WorkSpace gestion en libre-service

Sur Amazon WorkSpaces, les fonctionnalités WorkSpace de gestion en libre-service peuvent être activées pour permettre aux utilisateurs de mieux contrôler leur expérience. Permettre aux utilisateurs de disposer de fonctionnalités en libre-service peut réduire la charge de travail de votre personnel de support informatique pour Amazon WorkSpaces. Lorsque les fonctionnalités de libre-service sont activées, les utilisateurs peuvent effectuer une ou plusieurs des tâches suivantes directement depuis leur client Windows, macOS ou Linux pour Amazon WorkSpaces :

- Mettre en cache leurs informations d'identification sur leur client. Cela permet aux utilisateurs de se reconnecter à leur WorkSpace sans avoir à saisir à nouveau leurs informations d'identification.
- Redémarrez leur WorkSpace.
- Augmentez la taille des volumes root et utilisateur sur leur WorkSpace.
- Modifiez le type de calcul (bundle) de leur WorkSpace.
- Changez le mode de fonctionnement de leur WorkSpace.
- Reconstruisez leur WorkSpace.

L'octroi aux utilisateurs des options de redémarrage et de reconstruction n'a aucune incidence financière permanente pour leur WorkSpaces. Les utilisateurs doivent savoir qu'une reconstruction les WorkSpace WorkSpace rendra indisponibles pendant une heure au maximum, au cours du processus de reconstruction.

Les options permettant d'augmenter la taille des volumes, de modifier le type de calcul et de changer de mode d'exécution peuvent entraîner des WorkSpaces coûts supplémentaires. L'une des meilleures pratiques consiste à activer le libre-service afin de réduire la charge de travail de l'équipe d'assistance. Le libre-service pour les éléments à coût supplémentaire doit être autorisé dans le cadre d'un processus de flux de travail garantissant l'obtention de l'autorisation pour les frais supplémentaires. Cela peut se faire par le biais d'un portail en libre-service dédié ou par intégration avec les services de gestion des services informatiques (ITSM) existants, tels que. WorkSpaces ServiceNow

Pour plus d'informations, reportez-vous à la section Activation WorkSpace des fonctionnalités de gestion en libre-service pour vos utilisateurs. Pour un exemple décrivant l'activation d'un portail

structuré pour le libre-service des utilisateurs, reportez-vous à Automatiser Amazon WorkSpaces avec un portail en libre-service.

Amazon WorkSpaces Cost Optimizer

La solution Amazon WorkSpaces Cost Optimizer analyse toutes vos données d' WorkSpaces utilisation d'Amazon. En fonction de votre utilisation, il convertit automatiquement WorkSpace l'option de facturation la plus rentable (horaire ou mensuelle). Cette solution vous aide à surveiller votre WorkSpace utilisation et à optimiser les coûts. Elle permet de fournir et de configurer automatiquement les AWS services nécessaires pour analyser l'utilisation toutes les 24 heures et convertir les données individuelles WorkSpaces. AWS CloudFormation La dernière version, 2.4, donne aux clients la flexibilité de déployer la solution dans un VPC existant, de la configurer en option pour la région et la terminaison. Il a également amélioré la précision des calculs des heures de facturation WorkSpaces et amélioré les métadonnées des rapports. Si vous avez déjà déployé une version antérieure (v2.2.1 ou inférieure) de cette solution, suivez la documentation de la pile de mise à jour pour mettre à jour la pile Amazon WorkSpaces Cost Optimizer CloudFormation afin d'obtenir la dernière version du framework de la solution.

Le mode de fonctionnement d'un WorkSpace détermine sa disponibilité et sa facturation immédiates. Voici le mode de WorkSpaces fonctionnement actuel :

AlwaysOn— À utiliser lorsque vous payez un abonnement mensuel fixe pour une utilisation illimitée de WorkSpaces. Ce mode est idéal pour les utilisateurs qui utilisent leur WorkSpace poste de travail principal et qui ont besoin d'un accès instantané à un ordinateur en cours d'exécution WorkSpace à tout moment.

AutoStop— À utiliser lorsque vous payez WorkSpaces à l'heure. Avec ce mode, WorkSpaces arrêtez après une période d'inactivité spécifiée et l'état des applications et des données est enregistré. Pour définir l'heure d'arrêt automatique, utilisez AutoStop le paramètre Heure (heures). Ce mode est idéal pour les utilisateurs qui n'ont besoin que d'un accès à temps partiel à leur WorkSpaces.

Une bonne pratique consiste à surveiller l'utilisation et à définir le mode de fonctionnement d' WorkSpacesAmazon de manière à ce qu'il soit le plus rentable à l'aide d'une solution telle que l'Amazon WorkSpaces Cost Optimizer. Cette solution déploie une règle Amazon CloudWatch Events qui appelle une AWS Lambdafonction toutes les 24 heures.

Cette solution peut convertir un modèle WorkSpaces de facturation individuelle d'un modèle de facturation horaire à un modèle de facturation mensuelle n'importe quel jour après avoir atteint le

seuil. Si la solution convertit une WorkSpace facturation horaire en facturation mensuelle, elle ne WorkSpace reconvertit pas la facturation horaire avant le début du mois suivant, et uniquement si l'utilisation était inférieure au seuil. Cependant, le modèle de facturation peut être modifié manuellement à tout moment à l'aide de l' WorkSpaces API Amazon AWS Management Console ou Amazon. Le AWS CloudFormation modèle de la solution inclut des paramètres qui exécuteront ces conversions et permettront d'exécuter la solution en mode d'exécution à sec afin de fournir des rapports contenant les recommandations.

Se désinscrire à l'aide de tags

Pour empêcher la solution de convertir un modèle de facturation WorkSpace entre deux modèles, appliquez une balise de ressource à l' WorkSpace aide de la clé de balise Skip_Convert et de toute valeur de balise. Cette solution enregistrera les balises WorkSpaces, mais ne les convertira pas WorkSpaces. Supprimez le tag à tout moment pour reprendre la conversion automatique WorkSpace. Pour plus de détails, consultez Amazon WorkSpaces Cost Optimizer.

Opter pour les régions

Par défaut, cette solution surveille toutes les AWS régions disponibles WorkSpaces en recherchant les annuaires enregistrés auprès d'Amazon sur WorkSpaces le même AWS compte. Vous pouvez fournir une liste séparée par des AWS virgules des régions que vous souhaitez surveiller dans le paramètre d'entrée Liste des AWS régions afin de limiter les régions à surveiller.

Déploiement dans un VPC existant

Cette solution nécessite un VPC pour exécuter la tâche ECS. Par défaut, la solution crée un nouveau VPC, mais vous pouvez le déployer dans un VPC existant en fournissant les ID de sous-réseau et l'ID de groupe de sécurité dans le cadre du paramètre d'entrée. Votre sous-réseau actuel dispose d'une route vers Internet pour que la tâche ECS extrait l'image Docker hébergée dans un référentiel Amazon ECR public.

Résiliation de la période non utilisée WorkSpaces

Cette solution vous permet de résilier les WorkSpaces articles non utilisés le dernier jour du mois lorsque tous les critères sont remplis. Vous pouvez activer cette fonctionnalité en modifiant le paramètre TerminateUnusedWorkSpacesd'entrée par rapport au CloudFormation modèle. Une bonne pratique consiste à exécuter cette fonctionnalité en mode Dry Run pendant quelques mois et à consulter les rapports mensuels pour vérifier les informations WorkSpaces marquées pour résiliation.

Optimisation d'Amazon Connect pour Amazon WorkSpaces

L'expérience utilisateur pour les agents des centres de contact doit être une priorité absolue, car si leur son est dégradé, cela crée une mauvaise expérience d'appel pour le client qu'ils servent. Lorsque vous exécutez une solution de centre de contact sur un poste de travail distant, les performances audio seront toujours affectées de manière mesurable lorsque le trafic vocal n'est pas prioritaire par rapport à la connexion réseau. Cet impact est dû au fait que le son circule du point de terminaison audio vers la session virtuelle, puis qu'il est compressé via le protocole de streaming pour être transmis à l'utilisateur final. Ce routage supplémentaire entraîne une dégradation des performances audio en raison de l'engorgement du réseau.

Une approche pour éviter ce comportement consiste à séparer le son de la session, ce qui signifie que toutes les ressources de l'agent du centre de contact restent en session tandis que le flux audio reste en dehors de la session. Cette division permet à l'audio d'être diffusé du point de terminaison audio directement vers l'utilisateur final, tandis que toutes les autres ressources d'appel, y compris les informations personnelles consultées par l'agent, restent dans une session sécurisée. Cette optimisation audio est considérée comme une bonne pratique car elle garantit que l'expérience d'appel du client est aussi bonne que possible.

Amazon Connect propose une API Streams qui permet aux administrateurs de personnaliser leur panneau de contrôle des contacts (CCP) pour répondre aux besoins de leur entreprise. L'une des options dont dispose un administrateur est de contrôler si le CCP personnalisé peut recevoir du son pour l'appel. Ces paramètres nous permettent de configurer un CCP divisé, un CCP uniquement audio en dehors de la session et un CCP sans support pour les sessions en cours. Une fois que les administrateurs ont configuré ces CCP personnalisés, ils peuvent tirer parti de l'optimisation audio d'Amazon Connect pour WorkSpaces. Les CCP étant fournis dans le navigateur, ce paramètre permet aux administrateurs de fournir leur URL CCP uniquement audio au répertoire. WorkSpaces Une fois configuré, lorsque les agents du centre de contact WorkSpaces Connect s'authentifient avec succès WorkSpaces, le WorkSpaces client ouvre automatiquement l'URL CCP uniquement audio fournie dans le navigateur local par défaut de l'agent. Cette action permet à l'audio de circuler directement vers la machine locale de l'agent tandis que le CCP sans support gère tout le reste de la session sécurisée. WorkSpaces

Schéma de l'architecture

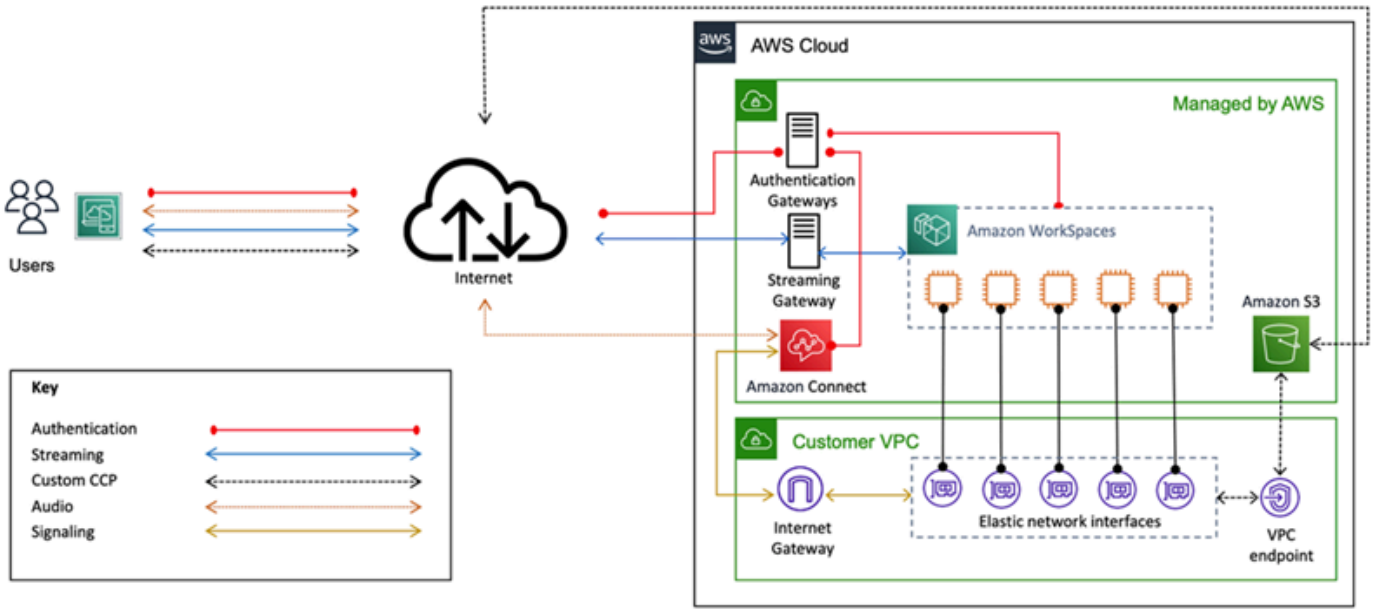

Figure 26 — Amazon Connect et schéma WorkSpaces d'architecture

Résolution des problèmes

Les problèmes courants liés à l'administration et aux clients, tels que les messages d'erreur tels que « Votre appareil ne parvient pas à se connecter au service WorkSpaces d'enregistrement » ou « Impossible de se connecter WorkSpace à une bannière de connexion interactive », figurent sur les pages de résolution des problèmes des clients et des administrateurs du guide d' WorkSpaces administration Amazon.

Rubriques

- AD Connector ne peut pas se connecter à Active Directory
- Résolution des problèmes Une erreur de création d'image WorkSpace personnalisée
- Résolution des problèmes liés à un système Windows WorkSpace marqué comme défectueux
- Collecte d'un ensemble de journaux de WorkSpaces support pour le débogage
- Comment vérifier la latence par rapport à la AWS région la plus proche

AD Connector ne peut pas se connecter à Active Directory

Pour qu'AD Connector puisse se connecter à l'annuaire local, le pare-feu du réseau local doit disposer de certains ports ouverts aux CIDR pour les deux sous-réseaux du VPC. Reportez-vous au scénario 1 : Utilisation d'AD Connector pour l'authentification par proxy auprès du service Active Directory sur site. Pour vérifier si ces conditions sont remplies, effectuez les opérations suivantes.

Pour tester la connexion, procédez comme suit :

1. Lancez une instance Windows dans le VPC et connectez-vous à celle-ci via RDP. Les étapes restantes sont effectuées sur l'instance VPC.
2. Téléchargez et décompressez l'application de DirectoryServicePortTesttest. Le code source et les fichiers de projet Microsoft Visual Studio sont inclus pour modifier l'application de test, si vous le souhaitez.
3. À partir d'une invite de commande Windows, exécutez l'application de DirectoryServicePortTest test avec les options suivantes :

```
DirectoryServicePortTest.exe -d <domain_name>
```

```
-ip <server_IP_address> -tcp "53,88,135,139,389,445,464,636,49152" -udp
 "53,88,123,137,138,389,445,464" <domain_name>
```

<domain_name>— Le nom de domaine complet, utilisé pour tester les niveaux fonctionnels de la forêt et du domaine. Si le nom de domaine est exclu, les niveaux fonctionnels ne seront pas testés.

< Server_IP_Address> — Adresse IP d'un contrôleur de domaine dans le domaine local. Les ports sont testés par rapport à cette adresse IP. Si l'adresse IP est exclue, les ports ne seront pas testés.

Ce test détermine si les ports nécessaires sont ouverts entre le VPC et le domaine. L'application de test vérifie également les niveaux fonctionnels minimaux de forêt et de domaine.

Résolution des problèmes Une erreur de création d'image WorkSpace personnalisée

Si un système Windows ou Amazon Linux WorkSpace a été lancé et personnalisé, une image personnalisée peut être créée à partir de celui-ci WorkSpace. Une image personnalisée contient le système d'exploitation, le logiciel d'application et les paramètres du WorkSpace.

Consultez les conditions requises pour créer une image personnalisée Windows ou les exigences pour créer une image personnalisée Amazon Linux. La création d'images nécessite que toutes les conditions préalables soient remplies avant que la création d'image puisse commencer.

Pour vérifier que 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 WorkSpace moment où une image est créée et fournit des conseils sur la manière de résoudre les problèmes détectés. Pour obtenir des informations détaillées, reportez-vous à la section Installation et configuration du vérificateur d'images.

Une fois tous WorkSpace les tests réussis, un message « Validation réussie » apparaît. Vous pouvez désormais créer un bundle personnalisé. Dans le cas contraire, résolvez les problèmes susceptibles d'entraîner des échecs de test et des avertissements, et répétez le processus d'exécution du vérificateur d'images jusqu'à ce qu'il WorkSpace réussisse tous les tests. Toutes les défaillances et tous les avertissements doivent être résolus avant qu'une image puisse être créée.

Pour plus d'informations, suivez les conseils pour résoudre les problèmes détectés par le vérificateur d'images.

Résolution des problèmes liés à un système Windows WorkSpace marqué comme défectueux

Le WorkSpaces service Amazon vérifie régulièrement l'état de santé d'un WorkSpace en lui envoyant une demande de statut. Le WorkSpace est marqué comme étant en mauvais état si aucune réponse n'est reçue WorkSpace en temps opportun. Les causes courantes de ce problème sont les suivantes :

- Une application sur le WorkSpace bloque la connexion réseau entre le WorkSpaces service Amazon et le WorkSpace.
- Utilisation élevée du processeur sur le WorkSpace.
- Le nom de l'ordinateur WorkSpace est modifié.
- L'agent ou le service qui répond au WorkSpaces service Amazon n'est pas en cours d'exécution.

Les étapes de dépannage suivantes peuvent WorkSpace rétablir le bon état :

- Tout d'abord, redémarrez-le WorkSpace depuis la WorkSpaces console Amazon. Si le redémarrage WorkSpace ne résout pas le problème, utilisez le protocole RDP ou connectez-vous à un Amazon Linux WorkSpace via SSH.
- Si le WorkSpace n'est pas accessible par un autre protocole, reconstruisez-le WorkSpace depuis la WorkSpaces console Amazon.
- Si aucune WorkSpaces connexion ne peut être établie, vérifiez les points suivants :

Vérifier l'utilisation du processeur

Utilisez Open Task Manager pour déterminer si l'utilisation du processeur WorkSpace est élevée. Si tel est le cas, essayez l'une des étapes de dépannage suivantes pour résoudre le problème :

1. Arrêtez tout service consommant une grande quantité de CPU.
2. Redimensionnez le WorkSpace pour un type de calcul supérieur à celui actuellement utilisé.
3. Redémarrez le WorkSpace.

> **Note**
>
> Pour diagnostiquer une utilisation élevée du processeur et obtenir des conseils si les étapes ci-dessus ne permettent pas de résoudre le problème d'utilisation élevée du processeur, reportez-vous à Comment diagnostiquer une utilisation élevée du processeur sur mon instance Windows EC2 lorsque mon processeur n'est pas limité ?

Vérifiez le nom d'ordinateur du WorkSpace

Si le nom de l'ordinateur de l'espace de travail a été modifié, redonnez-lui le nom d'origine :

1. Ouvrez la WorkSpaces console Amazon, puis agrandissez le champ Unhealthy WorkSpace pour afficher les détails.
2. Copiez le nom de l'ordinateur.
3. Connectez-vous au RDP à l' WorkSpace aide du protocole RDP.
4. Ouvrez une invite de commande, puis entrez le nom d'hôte pour afficher le nom actuel de l'ordinateur.
   a. Si le nom correspond au nom de l'ordinateur indiqué à l'étape 2, passez à la section de dépannage suivante.
   b. Si les noms ne correspondent pas, entrez sysdm.cpl pour ouvrir les propriétés du système, puis suivez les étapes restantes de cette section.
5. Choisissez Modifier, puis collez le nom de l'ordinateur indiqué à l'étape 2.
6. Entrez les informations d'identification de l'utilisateur du domaine si vous y êtes invité.
7. Confirmez que l'état SkyLightWorkspaceConfigServiceest en cours d'exécution
   a. Dans Services, vérifiez que le WorkSpace service SkyLightWorkspaceConfigService est en cours d'exécution. Si ce n'est pas le cas, lancez le service.

Vérifiez les règles du pare-feu

Vérifiez que le pare-feu Windows et tout pare-feu tiers en cours d'exécution disposent de règles autorisant les ports suivants :

- TCP entrant sur le port 4172 : établissez la connexion de streaming.
- UDP entrant sur le port 4172 : diffusion des entrées utilisateur.

- TCP entrant sur le port 8200 : gérez et configurez le. WorkSpace
- UDP sortant sur le port 55002 : diffusion PCoIP.

Si le pare-feu utilise le filtrage sans état, ouvrez les ports éphémères 49152-65535 pour autoriser les communications de retour.

Si le pare-feu utilise le filtrage dynamique, le port éphémère 55002 est déjà ouvert.

Collecte d'un ensemble de journaux de WorkSpaces support pour le débogage

Lors de la résolution WorkSpaces des problèmes, il est nécessaire de rassembler le bundle de journaux auprès de l'hôte concerné WorkSpace et auprès de l'hôte sur lequel le WorkSpaces client est installé. Il existe deux catégories fondamentales de journaux :

- Journaux côté serveur : dans ce scénario, il s' WorkSpace agit du serveur, ce sont donc des journaux qui vivent sur lui-même. WorkSpace
- Journaux côté client : se connecte à l'appareil que l'utilisateur final utilise pour se connecter au. WorkSpace

- Seuls les clients Windows et macOS rédigent des journaux localement.
- Aucun client et les clients iOS ne se connectent pas.
- Les journaux Android sont chiffrés sur le stockage local et téléchargés automatiquement vers l'équipe d'ingénierie du WorkSpaces client. Seule cette équipe peut consulter les journaux des appareils Android.

Journaux côté serveur du WSP

Tous les composants du WSP écrivent leurs fichiers journaux dans l'un des deux dossiers suivants :

- Emplacement principal : `C:\ProgramData\Amazon\WSP\` et `C:\ProgramData\NICE\dcv\log\`
- Emplacement de l'archive : `C:\ProgramData\Amazon\WSP\TRANSMITTED\`

Modification de la verbosité des fichiers journaux sous Windows

Vous pouvez configurer le niveau de verbosité du fichier journal pour WSP Windows WorkSpaces à grande échelle en configurant le paramètre de stratégie de groupe au niveau de verbosité du journal.

Pour modifier la verbosité du fichier journal pour un individu WorkSpaces, configurez la `h_log_verbosity_options` clé à l'aide de l'éditeur de registre Windows :

1. Ouvrez l'Éditeur du Registre Windows en tant qu'administrateur.
2. Accédez à `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. Si la `WSP` clé n'existe pas, cliquez avec le bouton droit de la souris, choisissez Nouveau > Clé et nommez-la`WSP`.
4. Accédez à `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP`.
5. Si la `h_log_verbosity_options` valeur n'existe pas, cliquez avec le bouton droit de la souris, choisissez Nouveau > DWORD et nommez-la`h_log_verbosity_options`.
6. Cliquez sur le nouveau `h_log_verbosity_options` DWORD et remplacez la valeur par l'un des nombres suivants en fonction du niveau de verbosité requis :
   - 0 — Erreur
   - 1 — Avertissement
   - 2 — Informations
   - 3 — Déboguer
7. Choisissez OK, puis fermez l'Éditeur du Registre Windows.
8. Redémarrez le WorkSpace.

Journaux côté serveur PCoIP

Tous les composants PCoIP écrivent leurs fichiers journaux dans l'un des deux dossiers suivants :

- Emplacement principal : `C:\ProgramData\Teradici\PCoIPAgent\logs`
- Emplacement de l'archive : `C:\ProgramData\Teradici\logs`

Lorsque vous travaillez AWS Support sur un problème complexe, il est parfois nécessaire de mettre l'agent du serveur PCoIP en mode de journalisation détaillée. Pour l'activer, procédez comme suit :

1. Ouvrez la clé de registre suivante : `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin_defaults`
2. Dans la `pcoip_admin_defaults` clé, créez le DWORD 32 bits suivant : `pcoip.event_filter_mode`
3. Définissez la valeur `pcoip.event_filter_mode` de « `3` » (Dec ou Hex).

À titre de référence, il s'agit des seuils de journalisation qui peuvent être définis dans ce DWORD.

- 0 — (CRITIQUE)
- 1 — (ERREUR)
- 2 — (INFORMATIONS)
- 3 — (Débogage)

Si le `pcoip_admin_default` DWORD n'existe pas, le niveau de journalisation est défini 2 par défaut. Il est recommandé de restaurer la valeur de 2 dans le DWORD une fois que celui-ci n'a plus besoin de journaux détaillés, car ils sont beaucoup plus volumineux et consomment inutilement de l'espace disque.

WebAccess journaux côté serveur

Pour PCoIP et WSP (version 1.0+) WorkSpaces, le client WorkSpaces Web Access utilise le service STXHD. Les journaux de WorkSpaces Web Access sont stockés à l'adresse`C:\ProgramData\Amazon\Stxhd\Logs`.

Pour WSP (version 2.0+) WorkSpaces, les journaux de WorkSpaces Web Access sont stockés dans. `C:\ProgramData\Amazon\WSP\`

Journaux côté client

Ces journaux proviennent du WorkSpaces client auquel l'utilisateur se connecte, ils se trouvent donc sur l'ordinateur de l'utilisateur final. Les emplacements des fichiers journaux pour Windows et Mac sont les suivants :

- Windows : `"%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\Logs"`
- macOS : `~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs`
- Linux : `~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs`

Pour aider à résoudre les problèmes que les utilisateurs peuvent rencontrer, activez la journalisation avancée qui peut être utilisée sur n'importe quel WorkSpaces client Amazon. La journalisation avancée est activée pour chaque session client suivante jusqu'à ce qu'elle soit désactivée.

1. Avant de se connecter au WorkSpace, l'utilisateur final doit activer la journalisation avancée pour son WorkSpaces client.
2. L'utilisateur final doit ensuite se connecter comme d'habitude, utiliser le sien et tenter de reproduire le problème. WorkSpace
3. 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.

Ce paramètre est conservé jusqu'à ce qu'il soit explicitement désactivé. Une fois que l'utilisateur a réussi à reproduire le problème lié à la connexion détaillée, ce paramètre doit être désactivé, car il génère des fichiers journaux volumineux.

Collecte automatisée de paquets de journaux côté serveur pour Windows

Le `Get-WorkSpaceLogs.ps1` script est utile pour rassembler rapidement un ensemble de journaux côté serveur pour. AWS Support Le script peut être demandé AWS Support en le demandant dans un dossier d'assistance :

1. Connectez-vous à l' WorkSpace aide du client ou du protocole RDP (Remote Desktop Protocol).
2. Lancez une invite de commande administrative (exécutée en tant qu'administrateur).
3. Lancez le script depuis l'invite de commande à l'aide de la commande suivante :

```
powershell.exe -NoLogo -ExecutionPolicy RemoteSigned -NoProfile -File "C:\Program
 Files\Amazon\WorkSpacesConfig\Scripts\Get-WorkSpaceLogs.ps1"
```

4. Le script crée un ensemble de journaux sur le bureau de l'utilisateur.

   Le script crée un fichier zip contenant les dossiers suivants :

   - C — Contient les fichiers provenant de Program Files, Program Files (x86) et Windows relatifs à Skylight ProgramData, EC2Config, Teradici, à l'observateur d'événements et aux journaux Windows (Panther et autres).

- CliXML — Contient des fichiers XML qui peuvent être importés dans Powershell à des `Import-CliXML` fins de filtrage interactif. Reportez-vous à Import-Clixml.
- Config — Journaux détaillés pour chaque vérification effectuée
- ScriptLogs— Journaux relatifs à l'exécution du script (non pertinents pour l'investigation, mais utiles pour débugger le rôle du script).
- tmp —Dossier temporaire (il doit être vide).
- Traces — Capture de paquets effectuée lors de la collecte du journal.

Comment vérifier la latence par rapport à la AWS région la plus proche

Le site Web Connection Health Check vérifie rapidement si tous les services requis utilisant Amazon sont WorkSpaces accessibles. Il vérifie également les performances de chaque AWS région dans laquelle Amazon WorkSpaces est disponible et indique aux utilisateurs laquelle sera la plus rapide.

Conclusion

Il y a un changement stratégique dans l'informatique destinée aux utilisateurs finaux, les entreprises s'efforçant d'être plus agiles, de mieux protéger leurs données et d'aider leurs employés à être plus productifs. Bon nombre des avantages déjà obtenus grâce au cloud computing s'appliquent également à l'informatique destinée aux utilisateurs finaux. En déplaçant leurs postes de travail Windows ou Linux vers le AWS cloud avec Amazon WorkSpaces, les entreprises peuvent rapidement évoluer au fur et à mesure qu'elles ajoutent des employés, améliorer leur niveau de sécurité en protégeant les données des appareils et offrir à leurs employés un ordinateur de bureau portable, accessible depuis n'importe où, en utilisant l'appareil de leur choix.

Amazon WorkSpaces est conçu pour être intégré aux systèmes et processus informatiques existants, et ce livre blanc décrit les meilleures pratiques pour ce faire. En suivant les directives de ce livre blanc, vous pouvez déployer des postes de travail dans le cloud à moindre coût, capables d'évoluer en toute sécurité avec votre entreprise sur l'infrastructure AWS mondiale.

Collaborateurs

Les personnes qui ont contribué à ce document incluent :

- Andrew Morgan, architecte de solutions EUC, Amazon Web Services
- Don Scott, consultant spécialisé senior de l'EUC, Amazon Web Services
- Klaus Becker, architecte de solutions spécialiste senior de l'EUC, Amazon Web Services
- Naviero Magee, architecte de solutions principal, Amazon Web Services
- Robert Fountain, consultant spécialisé EUC, Amazon Web Services
- Stephen Stetler, architecte de solutions EUC senior, Amazon Web Services

Suggestions de lecture

Pour plus d'informations, reportez-vous à :

- Guide d' WorkSpaces administration d'Amazon
- Guide WorkSpaces du développeur Amazon
- WorkSpaces Clientèle d'Amazon
- Gestion d'Amazon Linux 2 (Amazon WorkSpaces avec AWS OpsWorks pour Puppet Enterprise)
- Personnalisation d'Amazon Linux WorkSpace
- Comment améliorer la sécurité LDAP dans AWS Directory Service avec le protocole LDAPS côté client
- Utilisez Amazon CloudWatch Events avec Amazon WorkSpaces et AWS Lambda pour une meilleure visibilité de votre flotte
- Comment Amazon WorkSpaces utilise AWS KMS
- AWS CLI Référence de commande — WorkSpaces
- Surveillance des WorkSpaces métriques Amazon
- Environnement de bureau MATE
- Résolution des problèmes liés à l'administration du AWS Directory Service
- Résolution des problèmes d' WorkSpaces administration d'Amazon
- Résolution des problèmes liés aux WorkSpaces clients Amazon
- Automatisez Amazon WorkSpaces grâce à un portail en libre-service

Révisions du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

Modification	Description	Date
Mise à jour mineure	Contenu mis à jour pour les services d'annuaire AD, la reprise après sinistre, la continuité des activités et la redirection entre régions. Ajout WorkSpaces et optimisation audio d'Amazon Connect. Mises à jour mineures du formatage.	26 mai 2022
Mise à jour mineure	Corrigez le langage non inclusif.	6 avril 2022
Livre blanc mis à jour	Contenu mis à jour	24 mars 2022
Livre blanc mis à jour	Contenu mis à jour pour AWS Network Firewall, les annuaires MAD Replicated, YubiKey Support, Containers, WSLv1, Smart Card Support, WorkSpaces Service Quota et Trusted Devices.	20 décembre 2021
Livre blanc mis à jour	Contenu mis à jour pour le protocole de WorkSpace s streaming, l'authent ification par carte à puce, les diagrammes, les déploieme nts de clients, la sélection des appareils finaux et l'accès au Web	28 avril 2021

Livre blanc mis à jour	Contenu mis à jour	1er décembre 2020
Livre blanc mis à jour	Contenu mis à jour depuis la première publication et ajout de nouveaux diagrammes.	1er mai 2020
Publication initiale	Publié pour la première fois.	1er juillet 2016

Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de AWS produits et les pratiques actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations AWS de ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne les modifie pas.

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

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.