Bonnes pratiques de déploiement d'Amazon WorkSpaces

Accès au réseau, services d'annuaire et sécurité

Juillet 2016

Mentions légales

Ce document est fourni à titre informatif uniquement. Il présente l'offre de produits et les pratiques actuelles d'AWS à la date de publication de ce document, des informations qui sont susceptibles d'être modifiées sans avis préalable. Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document et chaque client est responsable de son utilisation des produits ou services AWS, chacun étant fourni « en l'état », sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Ce document ne crée pas de garanties, représentations, engagements contractuels, conditions ou assurances à l'encontre d'AWS, de ses affiliés, fournisseurs ou donneurs de licence. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun contrat et ne modifie aucun contrat entre AWS et ses clients.

Table des matières

Résumé 4
Introduction 4
Configuration requise pour WorkSpaces 5
Considérations sur le réseau 6
Conception du VPC 7
Flux de trafic 9
Exemple d'une configuration type 12
AWS Directory Service 18
Scénarios de déploiement AD DS 18
Considérations relatives à la conception 28
Authentification multi-facteurs (MFA) 34
Sécurité 36
Chiffrement en transit 36
Interfaces réseau 38
Groupe de sécurité WorkSpaces 39
WorkSpaces chiffrés 41
Surveillance et journalisation à l'aide d'Amazon CloudWatch 43
Métriques Amazon CloudWatch pour WorkSpaces 43
Dépannage 45
AD Connector ne pas se connecter à Active Directory 45
Comment vérifier la latence vers la région AWS la plus proche 46
Conclusion 46
Collaborateurs 47
Suggestions de lecture 47

Résumé

Ce livre blanc expose un certain nombre de bonnes pratiques pour le déploiement d'Amazon WorkSpaces. Il présente quelques considérations sur le réseau et aborde les services d'annuaire et l'authentification utilisateur, ainsi que la sécurité, la supervision et la journalisation.

Ce document est divisé en quatre catégories pour vous aider à retrouver plus rapidement les informations pertinentes. Il est destiné aux ingénieurs spécialisés dans les réseaux, les services d'annuaire ou la sécurité.

Introduction

Amazon WorkSpaces est un service de calcul de bureau géré et exécuté dans le cloud. Avec Amazon WorkSpaces, vous n'avez plus besoin d'acquérir ou de déployer du matériel, ni d'installer des logiciels complexes. Ce service offre une expérience de bureau en quelques clics sur l'AWS Management Console, à l'aide de l'interface de ligne de commande (CLI) AWS ou en utilisant les API. Amazon WorkSpaces vous permet de lancer un bureau en quelques minutes et de vous connecter à un logiciel de bureau, et d'y accéder, depuis un réseau local ou externe en toute sécurité, avec fiabilité et rapidement. Vous pouvez :

- Utiliser votre annuaire Microsoft Active Directory (AD) existant en utilisant AWS Directory Service : AD Connector.
- Transférer votre annuaire sur AWS Cloud.
- Créer un annuaire géré avec AWS Directory Service (Microsoft AD ou Simple AD), afin de gérer les utilisateurs et WorkSpaces.

De plus, vous pouvez utiliser votre serveur RADIUS local ou hébergé sur le cloud avec AD Connector afin de permettre à WorkSpaces de se servir de l'authentification MFA (multi-factor authentication).

Vous pouvez automatiser la mise en service d'Amazon WorkSpaces en utilisant la CLI ou l'API, ce qui vous permet d'intégrer Amazon WorkSpaces à vos flux de travail de mise en service existants.

En termes de sécurité, outre le chiffrement réseau intégré fourni par le service WorkSpaces, vous pouvez également activer le chiffrement au repos pour WorkSpaces (voir WorkSpaces chiffré dans la section consacrée à la sécurité).

Vous pouvez déployer des applications sur WorkSpaces à l'aide de vos outils locaux existants, par exemple Microsoft System Center Configuration Manager (SCCM), ou en utilisant Amazon WorkSpaces Application Manager (Amazon WAM).

Les sections suivantes fournissent des détails sur Amazon WorkSpaces, expliquent le fonctionnement du service, décrivent ce dont vous avez besoin pour le lancer et exposent les options et fonctionnalités disponibles.

Configuration requise pour WorkSpaces

Le service Amazon WorkSpaces a besoin de trois composants pour pouvoir être déployé :

- **Application cliente WorkSpaces**. Un appareil client pris en charge par Amazon WorkSpaces. Vous trouverez une liste complète ici : Plateformes et appareils pris en charge.

  Vous pouvez également utiliser des appareils Zero Client PCoIP (Personal Computer over Internet Protocol) pour vous connecter à WorkSpaces. Pour obtenir une liste des appareils disponibles, consultez Appareils Zero Client PCoIP pour Amazon WorkSpaces.

- **Un service d'annuaire pour authentifier les utilisateurs et leur donner accès à leur WorkSpace**. Amazon WorkSpaces fonctionne actuellement avec AWS Directory Service et Active Directory. Vous pouvez utiliser votre serveur local Active Directory avec AWS Directory Service afin de prendre en charge vos informations d'identification utilisateur professionnelles avec WorkSpaces.

- **Amazon Virtual Private Cloud (Amazon VPC) dans lequel exécuter vos Amazon WorkSpaces**. Vous aurez besoin de deux sous-réseaux au minimum pour un déploiement de WorkSpaces car chaque structure AWS Directory Service requiert deux sous-réseaux dans un déploiement Multi-AZ.

Considérations sur le réseau

Chaque WorkSpace est associé à un Amazon VPC et à une structure AWS Directory Service spécifiques que vous avez utilisés pour le créer. Toutes les structures AWS Directory Service (Simple AD, AD Connector et Microsoft AD) ont besoin de deux sous-réseaux pour fonctionner, un dans chaque zone de disponibilité. Les sous-réseaux sont constamment affiliés à une structure Directory Service et ils ne peuvent pas être modifiés une fois l'AWS Directory Service créé. Il est donc impératif que vous définissiez la taille de réseau appropriée avant de créer la structure Directory Service. Lors de la création des sous-réseaux, prêtez attention aux points suivants :

- De combien de WorkSpaces aurez-vous besoin dans le temps ? Quelle est la croissance prévue ?
- Aux besoins de quels types d'utilisateurs devez-vous répondre ?
- Combien de domaines Active Directory connecterez-vous ?
- Où résident vos comptes utilisateur professionnels ?

Amazon vous 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. Ces réponses sont utiles lorsque vous devez limiter l'accès à certaines applications ou ressources. Les personas d'utilisateur définis peuvent vous aider à segmenter et à limiter l'accès à l'aide d'AWS Directory Service, des listes de contrôle d'accès réseau, des tables de routage et des groupes de sécurité VPC. Chaque structure AWS Directory Service utilise deux sous-réseaux et applique les mêmes paramètres à tous les WorkSpaces lancés depuis la structure. Par exemple, vous pouvez utiliser un groupe de sécurité qui s'applique à tous les WorkSpaces associés à un AD Connector afin de spécifier si l'authentification MFA est nécessaire ou si l'utilisateur final peut bénéficier d'un accès administrateur local à son WorkSpace.

> **Remarque** Chaque AD Connector est connecté à une unité d'organisation (UO) Microsoft Active Directory. Vous devez créer votre Directory Service de façon à tenir compte des personas d'utilisateur pour pouvoir bénéficier de cette capacité.

Cette section décrit les bonnes pratiques pour définir la taille de votre VPC et de vos sous-réseaux, le flux de trafic et les implications pour la conception des services d'annuaire.

Conception du VPC

Voici quelques points dont il est important de tenir compte lors de la conception du VPC, des sous-réseaux, des groupes de sécurité, des stratégies de routage et des ACL réseau pour vos Amazon WorkSpaces afin de créer un environnement WorkSpaces évolutif, sûr et facile à gérer.

- **VPC**. Nous vous recommandons d'utiliser un VPC distinct propre à votre déploiement WorkSpaces. L'utilisation d'un VPC distinct vous permet de spécifier la gouvernance et les protections de sécurité pour vos WorkSpaces en créant une séparation du trafic.
- **Services d'annuaire**. Chaque structure AWS Directory Service requiert deux sous-réseaux qui permettent d'obtenir un service d'annuaire extrêmement disponible réparti entre les zones de disponibilité Amazon.
- **Taille du sous-réseau**. Les déploiements de WorkSpaces sont liés à une structure d'annuaire et résident sur les mêmes sous-réseaux VPC que l'AWS Directory Service sélectionné. Quelques points clés :
  - Les tailles de sous-réseau sont définitives et ne peuvent pas être modifiées. Veillez donc à prévoir suffisamment de place pour la croissance future.
  - Vous pouvez spécifier un groupe de sécurité par défaut pour l'AWS Directory Service que vous avez sélectionné. Le groupe de sécurité s'applique à tous les WorkSpaces associés à la structure AWS Directory Service concernée.
  - Vous pouvez avoir plusieurs AWS Directory Service qui utilisent le même sous-réseau.

Tenez compte de l'évolution prévue lors de la conception de votre VPC. Par exemple, vous pouvez ajouter des composants de gestion tels qu'un serveur antivirus, un serveur de gestion de correctifs ou un serveur Active Directory ou RADIUS MFA. Pensez à prévoir des adresses IP supplémentaires lors de la conception de votre VPC afin de pouvoir répondre à ce type de demande.

Pour des conseils et des informations approfondis sur la conception du VPC et la taille des sous-réseaux, consultez la présentation **re:Invent** Comment Amazon.com migre vers Amazon WorkSpaces.

Interfaces réseau

Chaque WorkSpace dispose de deux interfaces réseau élastiques (ENI), d'une interface réseau de gestion (eth0) et d'une interface réseau principale (eth1). AWS utilise l'interface réseau de gestion afin de gérer le WorkSpace. Il s'agit de l'interface sur laquelle la connexion du client se termine. 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'adresses privées sur un réseau capable de communiquer avec votre VPC WorkSpaces.

Pour obtenir une liste des plages d'IP privées utilisées par région, consultez Détails sur Amazon WorkSpaces.

> **Remarque** Les Amazon WorkSpaces et leurs interfaces réseau de gestion associées ne résident pas dans votre VPC et vous ne pouvez pas visualiser l'interface réseau de gestion ou l'ID d'instance Amazon Elastic Compute Cloud (Amazon EC2) sur votre AWS Management Console (voir Figure 4, Figure 5 et Figure 6). Toutefois, vous pouvez afficher et modifier les paramètres du groupe de sécurité de votre interface réseau principale (eth1) sur l'AWS Management Console. De plus, l'interface réseau principale de chaque WorkSpace n'est pas prise en compte pour les limites de ressource ENI Amazon EC2. Pour les déploiements à grande échelle des WorkSpaces, vous devez ouvrir un ticket de support via l'AWS Management Console afin d'augmenter vos limites ENI.

Flux de trafic

Vous pouvez diviser le trafic Amazon WorkSpace en deux composants principaux :

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

Au cours de la prochaine section, nous allons aborder ces deux composants.

Appareil client vers le WorkSpace

L'appareil qui exécute le client Amazon WorkSpaces, quel que soit son emplacement (local ou distant), utilise les deux mêmes ports pour la connectivité au service WorkSpaces. Le client utilise HTTPS sur le port 443 pour toutes les informations d'authentification et de session, et il utilise le port 4172 (port PCoIP) avec TPC et UDP pour le streaming de pixels vers un WorkSpace donné et pour les contrôles d'intégrité du réseau. Le trafic sur les deux ports est chiffré. Le trafic du port 443 est utilisé pour les informations d'authentification et de session. Ce port utilise TLS pour le chiffrement du trafic. Le trafic du streaming de pixels utilise le chiffrement AES-256-bits pour la communication entre le client et eth0 du WorkSpace, via la passerelle de streaming. Pour plus d'informations, consultez la section Sécurité plus loin dans ce document.

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

Le client Amazon WorkSpaces dispose d'une vérification intégrée de l'état du réseau. Cet utilitaire indique aux utilisateurs si leur réseau prendra en charge une connexion à l'aide d'un indicateur d'état situé dans la partie inférieure droite de l'application. Vous pouvez accéder à un affichage plus détaillé de l'état du réseau en sélectionnant **Network** dans la partie inférieure droite du client. Le résultat de cette sélection est illustré à la figure 1.

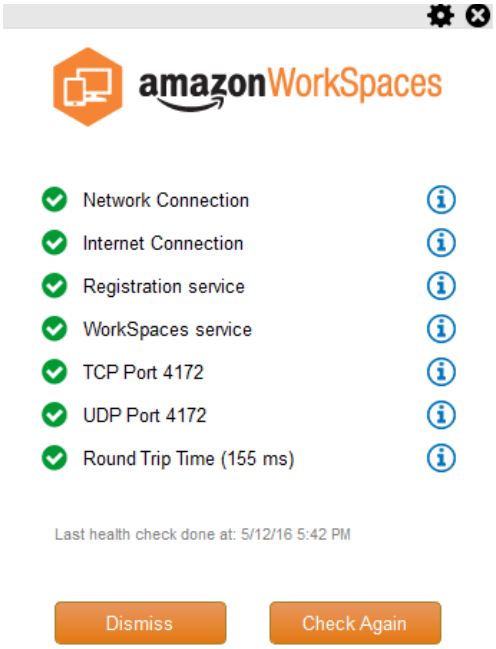

Figure 1 : Client WorkSpaces – Vérification de l'état du réseau

Un utilisateur lance une connexion entre son client et le service WorkSpaces en entrant ses informations de connexion pour l'annuaire utilisé par la structure Directory Service, généralement votre annuaire d'entreprise. Les informations de connexion sont envoyées via HTTPS aux passerelles d'authentification du service Amazon WorkSpaces dans la région où se trouve le WorkSpace. La passerelle d'authentification du service Amazon WorkSpaces transmet ensuite le trafic à la structure du service AWS Directory Service associée à votre WorkSpace. Par exemple, lors de l'utilisation de l'AD Connector, ce dernier transmet la demande d'authentification directement à votre service Active Directory, qui peut se trouver sur site ou sur un VPC AWS (voir Scénarios de déploiement AD DS). L'AD Connector ne stocke aucune information d'authentification et fonctionne comme un proxy sans état. C'est pourquoi il est impératif que l'AD Connector ait une connectivité vers un serveur Active Directory. L'AD Connector détermine à quel serveur Active Directory il se connecte 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. Si la validation MFA échoue, les informations de connexion de l'utilisateur sont transmises à votre AWS Directory Service.

Une fois l'utilisateur authentifié, le trafic de streaming commence par utiliser le port 4172 (port PCoIP) via la passerelle de streaming AWS vers le WorkSpace. Les informations relatives à la session sont échangées via HTTPS au cours de la session. Le trafic de streaming utilise la première ENI sur le WorkSpace (eth0 sur le WorkSpace) qui ne soit pas connectée à votre VPC. La connexion réseau de la passerelle de streaming vers l'ENI est gérée par AWS. En cas d'échec de connexion des passerelles de streaming vers l'ENI de streaming des WorkSpaces, un événement CloudWatch est généré (voir Surveillance ou journalisation à l'aide d'Amazon CloudWatch dans ce livre blanc).

Le volume des données transmises entre le service Amazon WorkSpaces et le client dépend du niveau d'activité des pixels. Afin de proposer une expérience optimale aux utilisateurs, nous recommandons une durée de boucle inférieure à 100 ms entre le client WorkSpaces et la région AWS où se trouvent les WorkSpaces. En règle générale, cela signifie que votre client WorkSpaces se trouve à moins de 3 200 km de la région qui héberge le WorkSpace. Nous proposons une page Web Connection Health Check que vous pouvez consulter pour déterminer la région AWS optimale à laquelle vous pouvez vous connecter pour le service Amazon WorkSpaces.

Service Amazon WorkSpaces vers VPC

Une fois qu'une connexion a été authentifiée d'un client vers un WorkSpace et que le trafic de streaming a été lancé, le client WorkSpaces affiche un bureau Windows (votre WorkSpace) connecté à votre VPC, et votre réseau doit indiquer que vous avez établi cette connexion. L'ENI principale du WorkSpace, identifiée comme eth1, reçoit une adresse IP du service DHCP (Dynamic Host Configuration Protocol) fourni par votre VPC, généralement depuis les mêmes sous-réseaux que ceux de votre AWS Directory Service. L'adresse IP reste avec le WorkSpace pendant toute la durée de vie de celui-ci. L'ENI qui se trouve dans votre VPC a accès à toutes les ressources du VPC et à tous les réseaux connectés à votre VPC (via l'appairage de VPC, une connexion AWS Direct Connect ou une connexion VPN).

L'accès de l'ENI à vos ressources réseau est déterminé par le groupe de sécurité par défaut (consultez des informations supplémentaires sur les groupes de sécurité ici) qu'AWS Directory Service configure pour chaque WorkSpace et par tout groupe de sécurité supplémentaire attribué à l'ENI. Vous pouvez ajouter des groupes de sécurité à l'ENI qui fait face à votre VPC comme vous le souhaitez, à l'aide de l'AWS Management Console ou de la CLI. Outre les groupes de sécurité, vous pouvez utiliser votre pare-feu basé sur les hôtes préféré sur un WorkSpace spécifique afin de limiter l'accès réseau aux ressources au sein du VPC.

La Figure 4 à la section Scénarios de déploiement AD DS, plus loin dans ce livre blanc, illustre le flux de trafic décrit précédemment.

Exemple d'une configuration type

Prenons l'exemple d'un scénario avec deux types d'utilisateur et un AWS Directory Service qui utilise un Active Directory centralisé pour l'authentification des utilisateurs :

- **Personnel ayant besoin d'un accès complet, partout** (par exemple, les employés à temps plein). Ces utilisateurs bénéficieront d'un accès complet à Internet et au réseau interne, et ils passeront à travers un pare-feu du VPC vers le réseau local.
- **Personnel devant uniquement avoir un accès limité depuis le réseau de l'entreprise** (par exemple, les sous-traitants et les consultants). Ces utilisateurs disposent d'un accès limité à Internet via un serveur proxy (vers des sites Web spécifiques) dans le VPC. Ils auront un accès réseau limité dans le VPC et vers le réseau local.

Vous souhaitez donner aux employés à temps plein la possibilité de bénéficier d'un accès administrateur local sur leur WorkSpace afin d'installer les logiciels et vous voulez mettre en place l'authentification à deux facteurs avec MFA. Vous souhaitez également octroyer aux employés à temps plein un accès continu à Internet depuis leur WorkSpace.

Pour les sous-traitants, vous souhaitez bloquer l'accès admin local afin qu'ils puissent utiliser uniquement des applications préinstallées spécifiques. Vous souhaitez appliquer des contrôles d'accès réseau très stricts via des groupes de sécurité pour ces WorkSpaces. Vous devez ouvrir les ports 80 et 443 à certains sites Web internes uniquement et vous souhaitez bloquer leur accès à Internet.

Dans le cadre de ce scénario, vous avez deux types de personas d'utilisateur totalement différents, avec des exigences différentes pour l'accès de réseau et de bureau. Il est généralement recommandé de gérer et de configurer leurs WorkSpaces différemment. Pour cela, vous devez créer deux AD Connector, un pour chaque persona d'utilisateur. Chaque AD Connector requiert deux sous-réseaux qui ont besoin d'un nombre suffisant d'adresses IP pour répondre à vos estimations de croissance de l'utilisation des WorkSpaces.

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

Voici quelques informations complémentaires sur ce scénario :

- Les sous-réseaux AWS VPC doivent être privés afin que le trafic tel que l'accès Internet puisse être contrôlé via une passerelle NAT ou un serveur Proxy-NAT dans le cloud, ou être réacheminé via votre système de gestion du trafic local.
- Un pare-feu est en place pour tout le trafic VPC destiné au réseau local.
- Le serveur Microsoft Active Directory et les serveurs MFA RADIUS sont locaux (voir Scénario 1 : Utilisation d'AD Connector pour traiter par proxy l'authentification vers AD DS **sur site**) ou font partie de l'implémentation d'AWS Cloud (voir les scénarios 2 et 3, Scénarios de déploiement AD DS).

Etant donné que tous les WorkSpaces bénéficieront d'une forme d'accès à Internet et étant donné qu'ils seront hébergés dans un sous-réseau privé, vous devez également créer des sous-réseaux publics pouvant accéder à Internet via une passerelle Internet. Vous aurez besoin d'une passerelle NAT pour les employés à temps plein afin de leur permettre d'accéder à Internet et d'un serveur Proxy-NAT pour les consultants et les sous-traitants afin de limiter leur accès à certains sites Web internes. Pour anticiper les pannes, prévoir une disponibilité élevée et limiter les frais de trafic entre zones de disponibilité, vous devez avoir deux passerelles NAT et des serveurs NAT ou proxy dans deux sous-réseaux différents d'un déploiement Multi-AZ. Les deux zones de disponibilité que vous sélectionnez comme sous-réseaux publics doivent correspondre aux deux zones de disponibilité que vous utilisez pour vos sous-réseaux WorkSpaces dans des régions ayant plus de deux zones de disponibilité. Vous pouvez acheminer le trafic de chaque zone de disponibilité WorkSpaces vers le sous-réseau public correspondant afin de limiter les frais de trafic entre plusieurs zones de disponibilité et de faciliter la gestion. La figure 2 illustre la configuration du VPC.

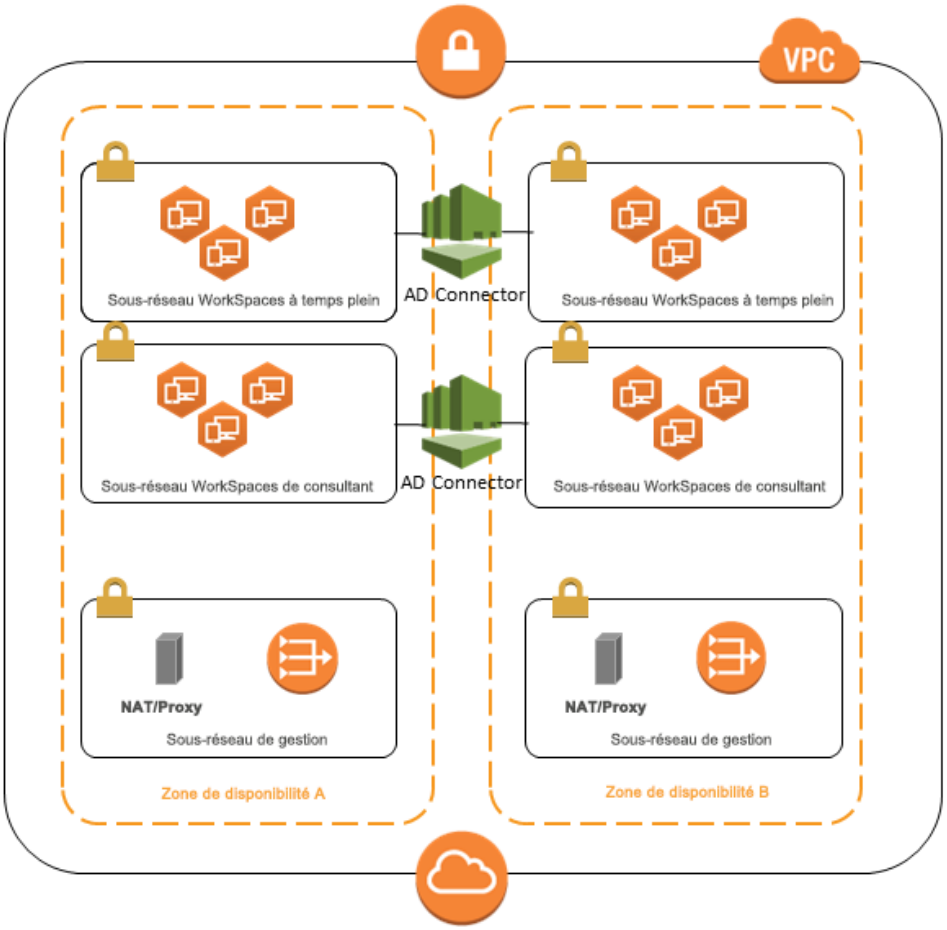

Figure 2 : Conception générale du VPC

Les informations suivantes décrivent la configuration des deux types de WorkSpaces décrits précédemment.

- **Employés à temps plein :** Sur Amazon WorkSpaces Management Console, sélectionnez l'option **Directories** dans la barre de menus, puis sélectionnez le répertoire contenant les employés à temps plein et choisissez **Local Administrator Setting**. Lorsque vous activez cette option, tout WorkSpace qui vient d'être créé bénéficie de privilèges d'administrateur locaux. Pour octroyer un accès Internet, vous devez configurer NAT (Network Address Translation) pour un accès Internet sortant à partir de votre VPC. Pour activer MFA, vous devez spécifier un serveur RADIUS, des IP serveur, des ports et une clé prépartagée.

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

- **Sous-traitants et consultants :** Dans Amazon WorkSpaces Management Console, désactivez **Internet Access** et **Local Administrator Setting**. Ajoutez ensuite un groupe de sécurité sous la section de paramètres **Security Group** pour appliquer un groupe de sécurité à tous les nouveaux WorkSpaces créés sous ce répertoire.

  Pour les WorkSpaces de consultants, limitez le trafic sortant et entrant vers les WorkSpaces en appliquant un groupe de sécurité par défaut via les paramètres AD Connector à tous les WorkSpaces associés à AD Connector. Le groupe de sécurité empêchera tout accès sortant depuis les WorkSpaces vers tous les éléments autres que le trafic HTTP et HTTPS, et le trafic sortant vers RDP à partir du sous-réseau Helpdesk dans le réseau sur site.

Remarque : Le groupe de sécurité s'applique uniquement à l'ENI se trouvant dans le VPC (eth1 sur le WorkSpace), et l'accès au WorkSpace depuis le client WorkSpaces n'est pas restreint en raison d'un groupe de sécurité. La figure 3 illustre la conception de VPC WorkSpaces finale décrite précédemment.

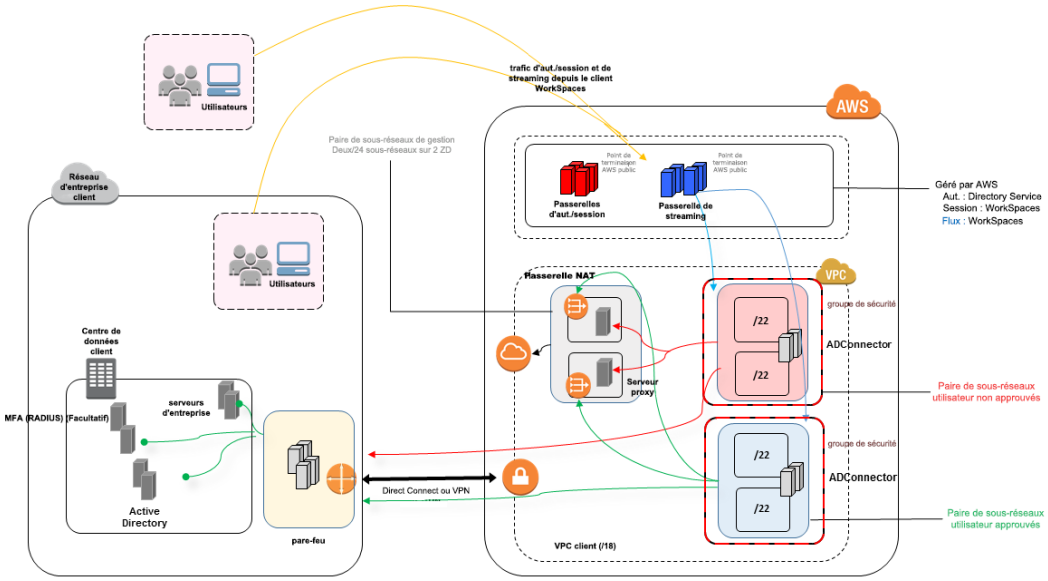

Figure 3 : Conception WorkSpaces avec des personas d'utilisateur

AWS Directory Service

Comme indiqué dans l'introduction, Amazon WorkSpaces repose sur AWS Directory Service. Avec AWS Directory Service, vous pouvez créer trois types d'annuaires. Les deux premiers en direct dans le cloud AWS :

- AWS Directory Service pour Microsoft Active Directory (Enterprise Edition), ou **Microsoft AD**, qui est géré par Microsoft Active Directory, avec Windows Server 2012 R2.
- **Simple AD**, un service d'annuaire géré autonome, compatible Microsoft Active Directory avec Samba 4.

Le troisième, **AD Connector,** est une passerelle d'annuaire qui vous permet de traiter par proxy les demandes d'authentification et les recherches d'utilisateur ou de groupe vers votre Microsoft Active Directory sur site existant.

La section suivante décrit les flux de communication pour l'authentification entre le service de courtier Amazon WorkSpaces et AWS Directory Service, de bonnes pratiques pour implémenter WorkSpaces avec AWS Directory Service, et des concepts avancés comme MFA. Nous présentons également des concepts d'architecture d'infrastructure pour Amazon WorkSpaces à grande échelle, des exigences relatives à Amazon VPC, et AWS Directory Service, y compris l'intégration aux services de domaine Active Directory (AD DS) Microsoft sur site.

Scénarios de déploiement AD DS

Amazon WorkSpaces repose sur AWS Directory Service, et une conception et un déploiement corrects du service d'annuaire sont essentiels. Les trois scénarios suivants sont basés sur le guide de démarrage rapide des *services de domaine Active Directory Microsoft*, qui détaille les bonnes pratiques en termes d'options de déploiement pour AD DS, en particulier pour l'intégration à WorkSpaces. La section *Considérations relatives à la conception* de ce chapitre aborde les exigences particulières et les bonnes pratiques d'utilisation d'AD Connector pour WorkSpaces, qui fait partie intégrante du concept de la conception WorkSpaces globale.

- **Scénario 1 : Utilisation d'AD Connector pour traiter par proxy l'authentification vers AD DS sur site.** Dans ce scénario, la connectivité réseau (VPN/Direct Connect (DX)) est mise en place vers le client avec toute l'authentification traitée par proxy via AWS Directory Service (AD Connector) vers les services AD DS sur site du client.
- **Scénario 2 : Extension d'AD DS sur site dans AWS (réplica).** Ce scénario est similaire au scénario 1, mais ici, un réplica des services AD DS du client est déployé sur AWS combiné à AD Connector, ce qui réduit la latence des demandes d'authentification/de requête vers AD DS et le catalogue global AD DS.
- **Scénario 3 : Déploiement isolé autonome d'AWS Directory Service dans le cloud AWS.** Il s'agit d'un scénario isolé et celui-ci n'inclut pas la connectivité retour vers le client pour l'authentification. Cette approche utilise AWS Directory Service (Microsoft AD) et AD Connector. Même si ce scénario ne repose pas sur une connectivité vers le client pour l'authentification, il prévoit d'exécuter le trafic applicatif si nécessaire via VPN ou DX.

Scénario 1 : Utilisation d'AD Connector pour traiter par proxy l'authentification vers AD DS sur site

Ce scénario est destiné aux clients qui ne souhaitent pas étendre leurs services AD DS sur site à AWS ou pour lesquels un nouveau déploiement d'AD DS n'est pas envisageable. La Figure 4 : AD Connector vers Active Directory sur site décrit globalement chacun des composants et illustre le flux d'authentification utilisateur.

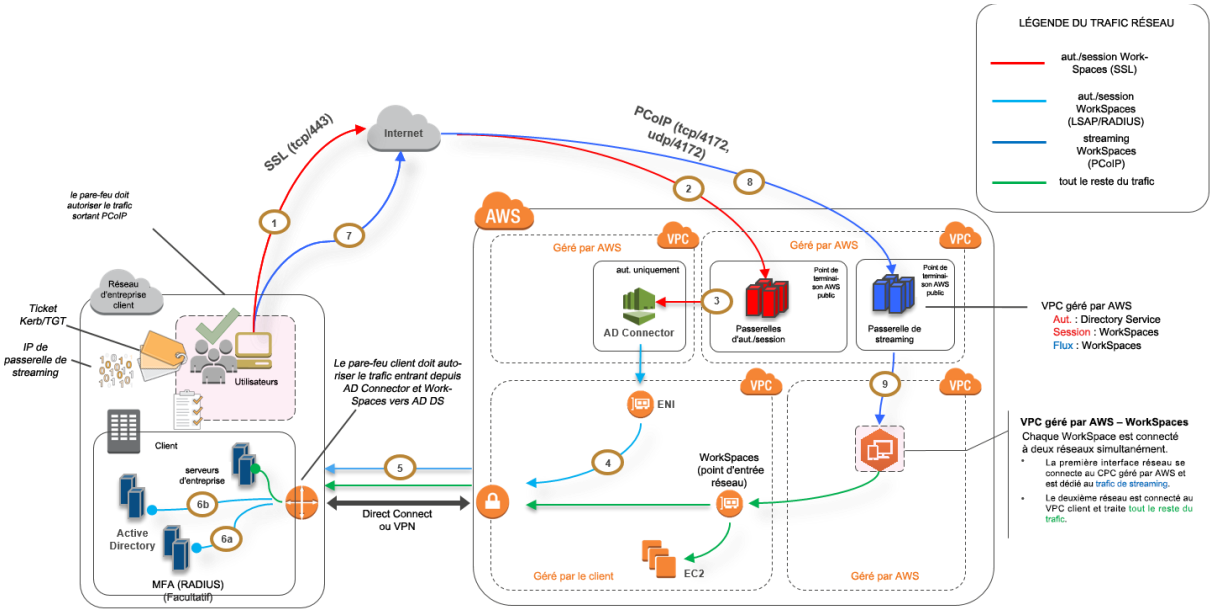

Figure 4 : AD Connector vers Active Directory sur site

Dans ce scénario, AWS Directory Service (AD Connector) est utilisé pour toute l'authentification utilisateur ou MFA qui est traitée par proxy via AD Connector vers les services AD DS sur site du client (Figure 5). Pour plus de détails sur les protocoles ou le chiffrement utilisés pour le processus d'authentification, consultez la section Sécurité de ce livre blanc.

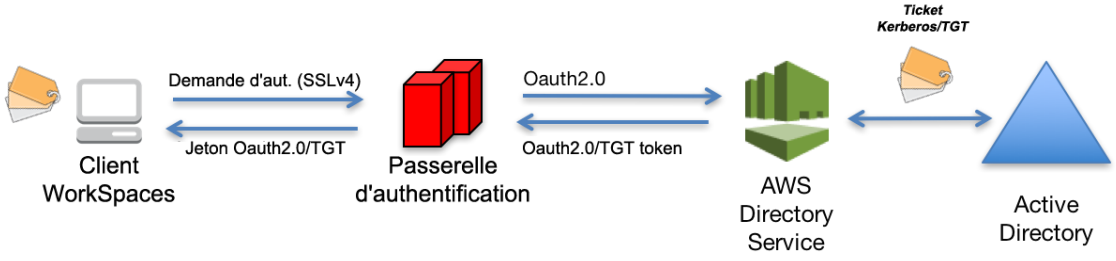

Figure 5 : Authentification utilisateur via la passerelle d'authentification

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

Cette architecture utilise la structure ou les composants suivants.

Amazon Web Services :

- **Amazon VPC :** Création d'un Amazon VPC avec au moins deux sous-réseaux privés s'étendant sur deux zones de disponibilité.
- **Jeu d'options DHCP :** Création d'un jeu d'options DHCP Amazon VPC. Cela permet la définition de noms de domaine spécifiés par le client et de serveurs de nom de domaine (DNS) (services sur site). (Pour plus d'informations, consultez la page relative aux jeux d'options DHCP.)
- **Passerelle privée virtuelle Amazon :** Activez la communication avec votre propre réseau via un tunnel VPN IPsec ou une connexion AWS Direct Connect.
- **AWS Directory Service** : AD Connector est déployé dans une paire de sous-réseaux privés Amazon VPC.
- **Amazon WorkSpaces :** Les WorkSpaces sont déployés dans les mêmes sous-réseaux privés qu'AD Connector (consultez Considérations relatives à la conception, AD Connector).

Client :

- **Connectivité réseau :** Points de terminaison VPN d'entreprise ou Direct Connect.
- **AD DS :** Services AD DS d'entreprise.
- **MFA (facultatif) :** Serveur RADIUS d'entreprise.
- **Appareils utilisateur final :** Appareils utilisateur final d'entreprise ou BYOL (par exemple, tablettes Windows, Mac, iPad ou Android, clients zéro, Chromebook), utilisés pour accéder au service Amazon WorkSpaces (consultez la page relative aux plateformes et appareils pris en charge).

Même si cette solution convient parfaitement aux clients qui ne souhaitent pas déployer AD DS dans le cloud, elle comporte quelques pièges.

- **Dépendance à la connectivité :** Si la connectivité vers le centre de données est perdue, aucun utilisateur ne pourra se connecter à ses WorkSpaces respectifs, et les connexions existantes resteront actives pendant la durée de vie Kerberos/TGT.
- **Latence :** Si une latence a lieu via la connexion (c'est plus souvent le cas avec VPN qu'avec DX), l'authentification WorkSpaces et toute activité liée à AD DS, comme l'application d'un objet Stratégie de groupe (GPO), prendront plus de temps.
- **Coûts du trafic :** Toute l'authentification doit passer par la liaison VPN ou DX ; elle dépend donc du type de connexion. Il s'agit d'un transfert de données sortantes depuis Amazon EC2 vers Internet ou d'un transfert de données sortantes (DX).

> **Remarque :** AD Connector est un service proxy. Il ne stocke pas ou ne met pas en cache des informations d'identification utilisateur. Toutes les demandes d'authentification, de recherche et de gestion sont traitées par votre Active Directory. Un compte avec des privilèges de délégation est requis dans votre service d'annuaire avec des droits permettant de lire toutes les informations utilisateur et de joindre un ordinateur au domaine.

Pour plus de détails sur la façon de configurer un utilisateur dans votre annuaire pour AD Connector, consultez la page relative à la délégation des privilèges de connexion.

En général, l'expérience WorkSpaces dépend fortement de l'élément 5 illustré à la Figure 4.

Scénario 2 : Extension d'AD DS sur site dans AWS (réplica)

Ce scénario est similaire au scénario 1. Par contre, dans le scénario 2, un réplica des services AD DS du client est déployé sur AWS combiné à AD Connector. Cela réduit la latence des demandes d'authentification ou de requête vers AD DS. La Figure 6 montre une vue globale de chacun des composants et du flux d'authentification utilisateur.

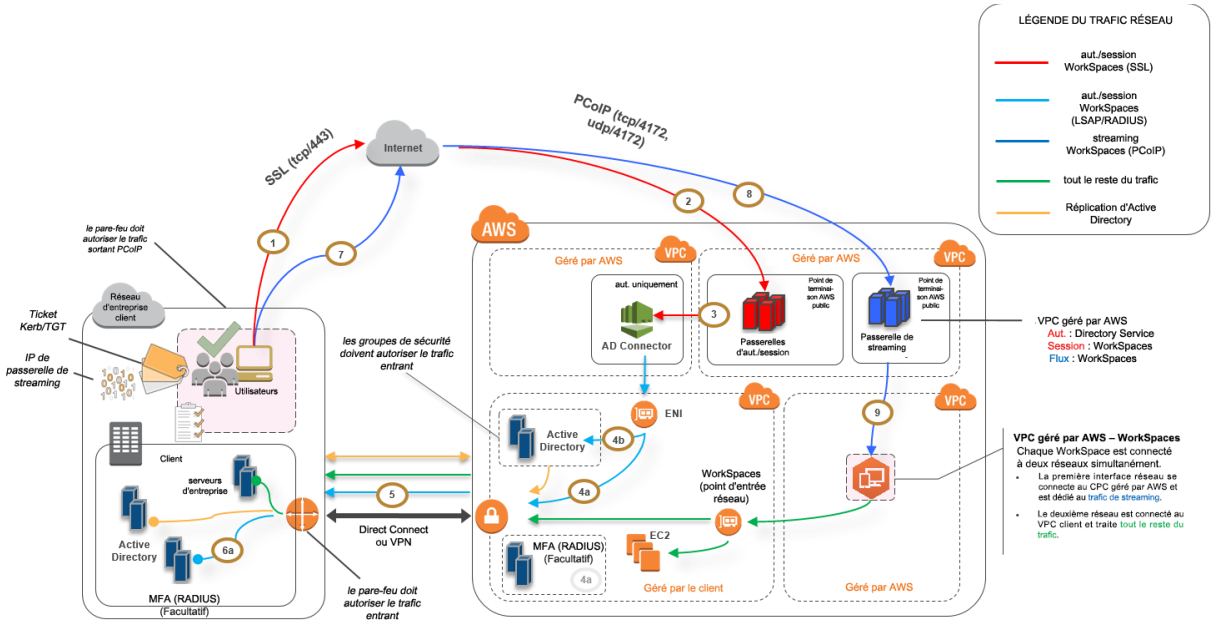

Figure 6 : Étendre les services Active Directory Domain du client au cloud

Comme dans le scénario 1, AD Connector est utilisé pour toute l'authentification utilisateur ou MFA, qui est ensuite traitée par proxy vers les services AD DS du client (Figure 5). Dans le scénario 2, les services AD DS du client sont déployés dans des zones de disponibilité sur des instances Amazon EC2 qui sont promues en contrôleurs de domaine dans la forêt Active Directory sur site du client, s'exécutant dans le cloud AWS. Chaque contrôleur de domaine est déployé dans des sous-réseaux privés VPC pour rendre AD DS hautement disponible dans le cloud AWS. Vous trouverez des bonnes pratiques pour le déploiement d'AD DS dans le cloud AWS dans la section Considérations relatives à la conception plus loin dans ce livre blanc.

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

Cette architecture utilise la structure ou les composants suivants.

Amazon Web Services :

- **Amazon VPC :** Création d'un Amazon VPC avec au moins quatre sous-réseaux privés s'étendant sur deux zones de disponibilité (deux pour les services AD DS du client, deux pour AD Connector ou WorkSpaces).
- **Jeu d'options DHCP :** Création d'un jeu d'options DHCP Amazon VPC. Cela vous permet de définir un nom de domaine spécifié par le client et des DNS (AD DS local). (Pour plus d'informations, consultez la page relative aux jeux d'options DHCP.)
- **Passerelle privée virtuelle Amazon :** Activez la communication avec votre propre réseau via un tunnel VPN IPsec ou une connexion AWS Direct Connect.
- **Amazon EC2 :**

— Des contrôleurs de domaine AD DS d'entreprise client sont déployés sur des instances Amazon EC2 dans des sous-réseaux VPC privés dédiés.

— Serveur RADIUS « facultatifs » du client pour MFA.

- AWS Directory Services : AD Connector est déployé dans une paire de sous-réseaux privés Amazon VPC.
- **Amazon WorkSpaces :** Les WorkSpaces sont déployés dans les mêmes sous-réseaux privés qu'AD Connector (consultez Considérations relatives à la conception, AD Connector).

Client :

- **Connectivité réseau :** Points de terminaison de VPN d'entreprise ou AWS Direct Connect.
- **AD DS :** AD DS d'entreprise (requis pour la réplication).
- **MFA « facultatif » :** Serveur RADIUS d'entreprise.

Appareils utilisateur final : Appareils utilisateur final d'entreprise ou BYOL (par exemple, tablettes Windows, Mac, iPad ou Android, clients zéro, Chromebook), utilisés pour accéder au service Amazon WorkSpaces (consultez la page relative aux plateformes et appareils pris en charge).

À la différence du scénario 1, cette solution ne présente pas les mêmes pièges. WorkSpaces et AWS Directory Service n'ont pas de dépendance à la connectivité mise en place.

- **Dépendance à la connectivité :** Si la connectivité vers le centre de données du client est perdue, les utilisateurs finaux peuvent continuer à travailler, car l'authentification et la fonctionnalité MFA « facultative » sont traitées en local.
- **Latence :** À l'exception du trafic de réplication (consultez *Considérations relatives à la conception :* Sites et services AD DS), toute l'authentification est locale et la latence est faible.
- **Coûts du trafic :** Dans ce scénario, l'authentification est locale et seule la réplication AD DS doit passer par la liaison VPN ou DX, ce qui réduit le transfert de données.

En général, l'expérience WorkSpaces dépend fortement de l'élément 5 illustré à la Figure 6. C'est encore plus le cas quand vous voulez faire évoluer WorkSpaces sur des milliers de bureaux, surtout pour les requêtes du catalogue global AD DS, car ce trafic reste local vers l'environnement WorkSpaces.

Scénario 3 : Déploiement isolé autonome d'AWS Directory Service dans le cloud AWS

Dans ce scénario, illustré à la Figure 7, AD DS est déployé dans cloud AWS au sein d'un environnement isolé autonome. AWS Directory Service est exclusivement utilisé dans ce scénario. Au lieu de gérer AD DS vous-même, vous vous appuyez 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.

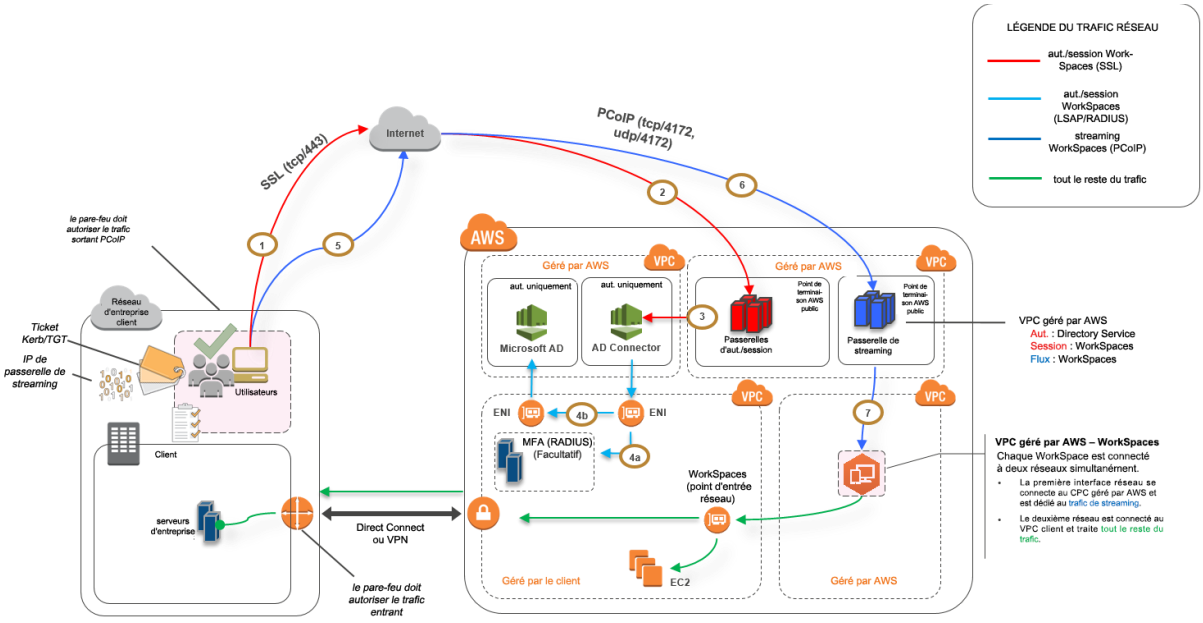

Figure 7 : Cloud uniquement - AWS Directory Services (Microsoft AD)

Comme dans le scénario 2, AD DS (Microsoft AD) est déployé dans des sous-réseaux dédiés s'étendant sur deux zones de disponibilité, ce qui rend AD DS hautement disponible dans le cloud AWS. En plus de Microsoft AD, AD Connector (dans les trois scénarios) est déployé pour l'authentification WorkSpaces ou MFA. Ceci assure la séparation des rôles ou des fonctions au sein de l'instance Amazon VPC, ce qui est une bonne pratique standard (consultez la section *Considérations relatives à la conception* : Réseau partitionné).

Le scénario 3 est une configuration complète standard qui fonctionne bien pour les clients qui souhaitent laisser AWS gérer le déploiement, l'application de correctifs (patch), la haute disponibilité et la surveillance d'AWS Directory Service. En raison de son mode d'isolation, outre les environnements de production, le scénario fonctionne bien également pour les environnements de preuve de concept ou d'atelier.

En plus du placement d'AWS Directory Service, la Figure 7 illustre le flux du trafic à partir d'un utilisateur vers un espace de travail et montre comment l'espace de travail interagit avec le serveur AD et le serveur MFA.

Cette architecture utilise la structure ou les composants suivants.

Amazon Web Services :

- **Amazon VPC :** Création d'un Amazon VPC avec au moins quatre sous-réseaux privés s'étendant sur deux zones de disponibilité (deux pour AD DS *Microsoft AD*, deux pour AD Connector ou WorkSpaces). « *Séparation des rôles.* »
- **Jeu d'options DHCP :** Création d'un jeu d'options DHCP Amazon VPC. Cela vous permet de définir un nom de domaine spécifié par le client et des DNS (Microsoft AD). Pour plus d'informations, consultez la page relative aux jeux d'options DHCP.
- **Facultatif : Passerelle privée virtuelle Amazon :** Activez la communication avec votre propre réseau via un tunnel VPN IPsec (VPN) ou une connexion AWS Direct Connect. À utiliser pour l'accès aux systèmes principaux sur site.
- **AWS Directory Service :** Microsoft AD déployé dans une paire de sous-réseaux VPC dédiés (service géré AD DS).
- **Amazon EC2 :** Serveurs RADIUS d'entreprise « facultatif » du client pour MFA.
- **AWS Directory Services :** AD Connector est déployé dans une paire de sous-réseaux privés Amazon VPC.
- **Amazon WorkSpaces :** Les WorkSpaces sont déployés dans les mêmes sous-réseaux privés qu'AD Connector (consultez Considérations relatives à la conception, AD Connector).

Client :

- **Facultatif : Connectivité réseau :** Points de terminaison VPN d'entreprise ou AWS Direct Connect.
- **Appareils utilisateur final :** Appareils utilisateur final d'entreprise ou BYOL (par exemple, tablettes Windows, Mac, iPad ou Android, clients zéro, Chromebook), utilisés pour accéder au service Amazon WorkSpaces (consultez la page relative aux plateformes et appareils pris en charge).

Tout comme le scénario 2, cette solution n'a pas de problème de dépendance ou de connectivité vers le centre de données sur site du client, de latence, ou de coûts de transfert sortant des données (sauf là où l'accès Internet est activé pour WorkSpaces au sein du VPC) car, il s'agit, de par sa conception, d'un scénario isolé ou de cloud uniquement.

Considérations relatives à la conception

Un déploiement AD DS fonctionnel dans le cloud AWS nécessite une bonne compréhension des concepts Active Directory et des services AWS spécifiques. Dans cette section, nous aborderons des considérations de conception clés lors du déploiement d'AD DS pour WorkSpaces, des bonnes pratiques VPC pour AWS Directory Service, des exigences liées à DHCP et DNS, des caractéristiques d'AD Connector, et des sites et services Active Directory.

Conception du VPC

Comme indiqué dans la section Considérations relatives au réseau de ce document et documenté précédemment pour les scénarios 2 et 3, il est conseillé de déployer AD DS dans le cloud AWS au sein d'une paire de sous-réseaux privés dédiés s'étendant sur deux zones de disponibilité, et séparés des sous-réseaux AD Connector ou WorkSpaces. Cette structure offre un accès hautement disponible et à faible latence aux services AD DS pour WorkSpaces, tout en appliquant les bonnes pratiques standard de séparation de rôles ou fonctions au sein d'Amazon VPC.

La Figure 8 illustre la séparation d'AD DS et d'AD Connector dans des sous-réseaux privés dédiés (scénario 3). Dans cet exemple, tous les services résident dans le même Amazon VPC.

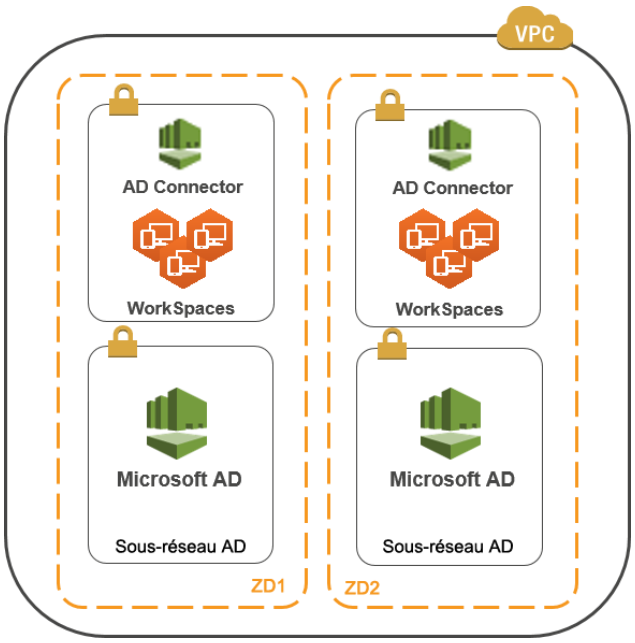

Figure 8 : Séparation réseau AD DS

La figure 9 illustre une conception similaire à celle du scénario 1. Par contre, dans ce scénario, la partie sur site réside dans un Amazon VPC dédié.

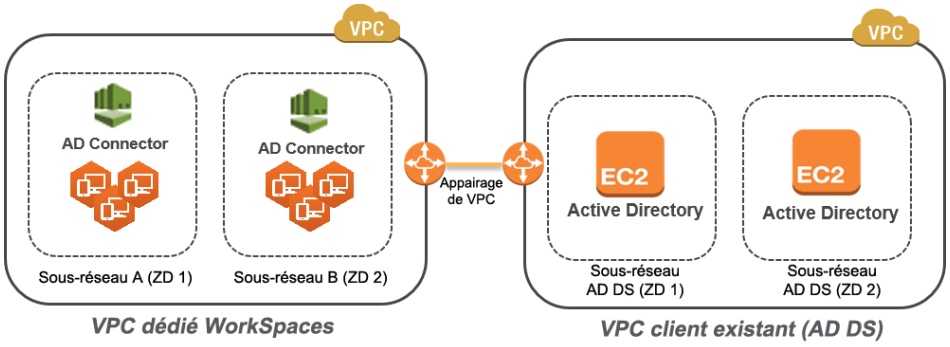

Figure 9 : VPC WorkSpaces dédié

> **Remarque :** Pour les clients disposant d'un déploiement AWS existant dans lequel AD DS est utilisé, nous vous recommandons de placer vos WorkSpaces dans un VPC dédié et d'utiliser l'appairage de VPC pour les communications AD DS.

En plus de la création de sous-réseaux privés dédiés pour AD DS, les contrôleurs de domaine et les serveurs membres ont besoin de plusieurs règles de groupe de sécurité afin d'autoriser le trafic pour des services comme la réplication AD DS, l'authentification utilisateur, les services de temps Windows et le système de fichiers distribué (DFS).

> **Remarque :** La bonne pratique consiste à restreindre les règles de groupe de sécurité requises aux sous-réseaux privés WorkSpaces et, dans le cas du scénario 2, à autoriser des communications AD DS bidirectionnelles sur site vers/depuis le cloud AWS, comme illustré dans le tableau suivant.

Protocole	Port	Utilisation	Destination
tcp	53, 88, 135, 139, 389, 445, 464, 636	Aut. (principale)	Active Directory (centre de données privé ou EC2)*
tcp	49152 – 65535	Ports élevés RPC	Active Directory (centre de données privé ou EC2)**
tcp	3268-3269	Approbations	Active Directory (centre de données privé ou EC2)*
tcp	9389	Microsoft Windows PowerShell distant (facultatif)	Active Directory (centre de données privé ou EC2)*
udp	53, 88, 123, 137, 138, 389, 445, 464	Aut. (principale)	Active Directory (centre de données privé ou EC2)*
udp	1812	Aut. (MFA) (facultatif)	RADIUS (centre de données privé ou EC2)*

* Consultez la page relative aux exigences de port Active Directory et de services de domaine Active Directory

**Consultez la page de présentation des services et des exigences de ports réseau pour Windows

Pour accéder à des conseils étape par étape pour l'implémentation de règles, consultez Ajout de règles à un groupe de sécurité dans le *Guide de l'utilisateur Amazon Elastic Compute Cloud*.

Conception VPC : DHCP et DNS

Avec un Amazon VPC, les services DHCP sont fournis par défaut pour vos instances. Par défaut, chaque VPC fournit un serveur DNS interne qui est accessible via le routage CIDR (Classless Inter-Domain Routing) + 2 espaces d'adressage, et est affecté à toutes les instances via un jeux d'options DHCP par défaut.

Les jeux d'options DHCP sont utilisés au sein d'un Amazon VPC pour définir des options d'étendue, comme le nom de domaine ou les serveurs de noms devant être transmis à vos instances via DHCP. La fonctionnalité correcte de services Windows au sein de votre VPC dépend de ces options d'étendue DHCP. Vous devez donc les définir correctement. Dans chacun des scénarios définis précédemment, vous devez créer et affecter votre propre étendue définissant vos nom de domaine et serveurs de noms. Cela garantit que les instances Windows jointes au domaine ou les espaces de travail WorkSpaces sont configurés pour utiliser le DNS Active Directory. Le tableau suivant est un exemple de jeu personnalisé d'options d'étendue DHCP devant être créé pour que WorkSpaces et AWS Directory Services fonctionnent correctement.

Paramètre	Valeur
Nom de balise	Crée une balise avec la clé = **name** et **value** définie sur une chaîne spécifique Exemple : exampleco.com
Nom de domaine	exampleco.com
Serveurs de noms de domaine	Adresses de serveur DNS, séparées par des virgules Exemple : 10.0.0.10, 10.0.1.10
Serveurs NTP	Laissez ce champ vide
Serveurs de noms NetBIOS	Entrez les mêmes adresses IP séparées par des virgules que les serveurs de noms de domaine Exemple : 10.0.0.10, 10.0.1.10
Type de nœud NetBIOS	2

Pour plus de détails sur la création d'un jeu d'options DHCP personnalisé et son association à votre Amazon VPC, consultez Utilisation de jeux d'options DHCP dans le *Guide de l'utilisateur Amazon Virtual Private Cloud*.

Dans le scénario 1, l'étendue DHCP serait le DNS sur site ou AD DS. Par contre, dans le scénario 2 ou 3, ce serait le service d'annuaire déployé en local (AD DS sur Amazon EC2 ou AWS Directory Services : Microsoft AD). Nous vous avons recommandé de faire de chaque contrôleur de domaine qui réside dans le cloud AWS un catalogue global et un serveur DNS intégré Directory.

Active Directory : Sites et services

Pour le scénario 2, les sites et services sont des composants stratégiques pour le fonctionnement correct d'AD DS. La topologie de site contrôle la réplication Active Directory entre les contrôleurs de domaine au sein du même site et au-delà des limites du site. Dans le scénario 2, au moins deux sites sont présents, sur site et AWS WorkSpaces dans le cloud. La définition de la topologie de site correcte garantit l'affinité client, ce qui signifie que les clients (dans le cas présent, les WorkSpaces) utilisent leur contrôleur de domaine local préféré.

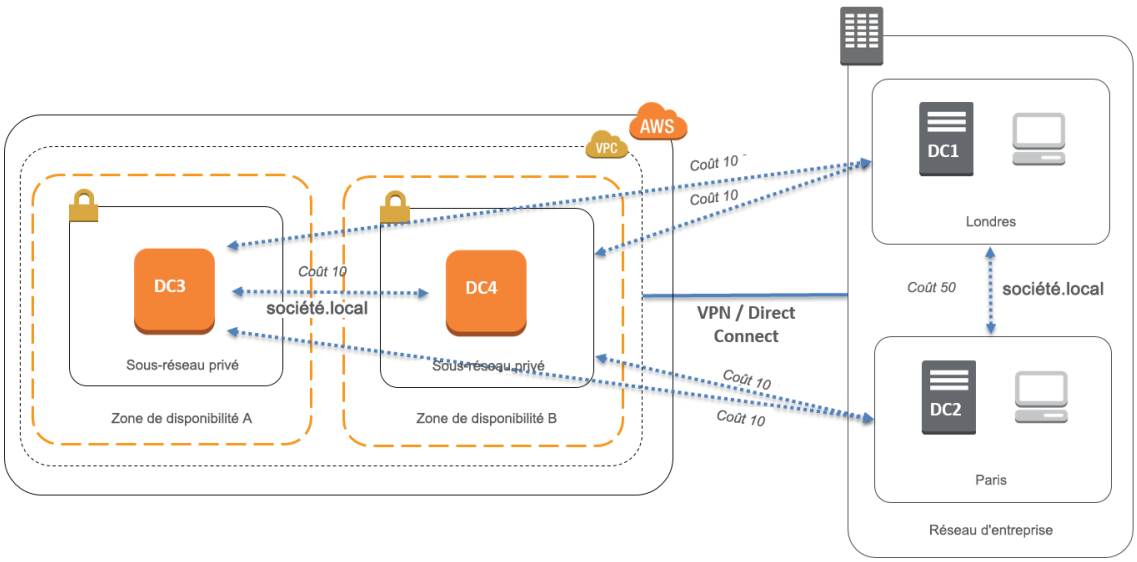

Figure 10 : Sites et services Active Directory : affinité client

> **Bonne pratique** Définissez un coût élevé pour les liaisons de site entre vos services AD DS sur site et le cloud AWS. La Figure 10 est un exemple des coûts à affecter aux liaisons de site (coût 100) pour assurer une affinité client indépendante des sites.

Ces associations contribuent à garantir que ce trafic (comme 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 contribue à garantir une faible latence et un trafic inter-liaisons.

Authentification multi-facteurs (MFA)

L'implémentation de MFA nécessite que l'infrastructure WorkSpaces utilise AD Connector comme AWS Directory Service et dispose d'un serveur RADIUS. Même si ce document n'aborde pas le déploiement d'un serveur RADIUS, la section précédente, Scénarios de déploiement AD DS décrit le placement de RADIUS dans chaque scénario.

MFA – Authentification à deux facteurs

Amazon WorkSpaces prend en charge MFA via AWS Directory Service : AD Connector et un serveur RADIUS *détenu par le client*. Une fois MFA activé, les utilisateurs doivent fournir un **nom utilisateur**, un **mot de passe** et un **code MFA** au client WorkSpaces pour l'authentification sur leurs bureaux WorkSpaces respectifs.

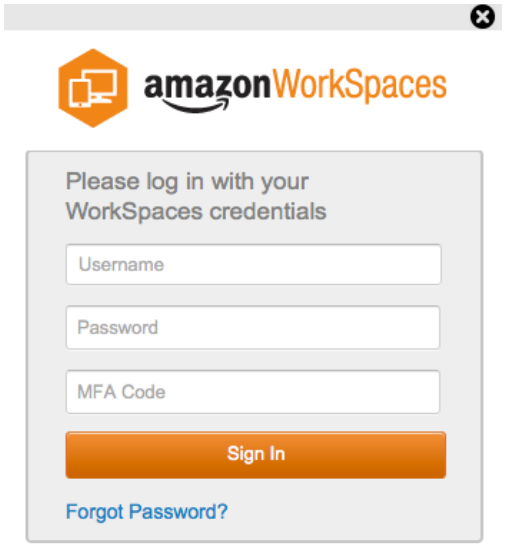

Figure 11 : Client WorkSpaces avec MFA activé

> **Règle obligatoire :** L'implémentation de l'authentification MFA nécessite que vous utilisiez AD Connector. AD Connector ne prend pas en charge l'authentification MFA « par utilisateur » sélective, car il s'agit d'un paramètre AD Connector global. Si vous avez besoin d'une l'authentification MFA « par utilisateur » sélective, vous devez séparer les utilisateurs par AD Connector.

WorkSpaces MFA nécessite un ou plusieurs serveurs RADIUS. En général, il s'agit de solutions existantes (par exemple, RSA), ou les serveurs peuvent être déployés au sein de votre VPC (voir Scénarios de déploiement AD DS). Si vous déployez une nouvelle solution RADIUS, il existe plusieurs implémentations dans le secteur aujourd'hui, par exemple, FreeRADIUS et des services de cloud comme Duo Security.

Vous trouverez une liste de prérequis pour implémenter MFA dans le *guide d'administration Amazon WorkSpaces* dans la section relative à la préparation d'un réseau pour un annuaire AD Connector Directory. Le processus de configuration de votre AD Connector pour MFA est décrit dans la section relative à la gestion d'un annuaire AD Connector Directory pour l'authentification multi-facteurs, dans le *guide d'administration Amazon WorkSpaces*.

Sécurité

Cette section explique comment sécuriser les données à l'aide du chiffrement quand vous utilisez des services Amazon WorkSpaces. Nous décrivons le chiffrement en transit et au repos, ainsi que l'utilisation de groupes de sécurité pour protéger l'accès réseau aux WorkSpaces. Vous trouverez des informations supplémentaires sur l'authentification (notamment la prise en charge de MFA) dans la section AWS Directory Service.

Chiffrement en transit

Amazon WorkSpaces utilise le chiffrement pour protéger la confidentialité à différentes étapes de la communication (en transit) et protéger les données au repos (WorkSpaces chiffrés). Les processus de chaque étape du chiffrement utilisés par Amazon WorkSpaces en transit sont décrits dans les sections suivantes. Pour plus d'informations sur le chiffrement au repos, consultez la section WorkSpaces chiffrés plus loin dans ce livre blanc.

Enregistrement et mises à jour

L'application de client de bureau communique avec Amazon pour les mises à jour et l'enregistrement à l'aide de 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 https. A la fin de cette étape, si l'authentification aboutit, la passerelle d'authentification renvoie un jeton OAuth 2.0 au client de bureau via la même connexion https.

> **Remarque :** L'application de 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 à AWS Directory Service. La communication de la passerelle d'authentification vers AWS Directory Service a lieu via HTTPS. Les informations d'identification utilisateur ne sont donc pas transmises sous forme de texte clair.

Authentification - AD Connector

AD Connector utilise Kerberos pour établir une communication authentifiée avec AD sur site afin de pouvoir se connecter à LDAP et exécuter les requêtes LDAP ultérieures. Actuellement, AWS Directory Service ne prend pas en charge LDAP avec TLS (LDAP). Toutefois, les informations d'identification utilisateur ne sont jamais transmises sous forme de texte clair. Pour plus de sécurité, il est possible de connecter votre VPC WorkSpaces à votre réseau sur site (où vos services AD résident) à l'aide d'une connexion VPN. Lors de l'utilisation d'une connexion VPN hardware AWS, vous configurez le chiffrement en transit à l'aide d'IPSEC standard (IKE et IPSEC SAs) avec des clé chiffrement symétrique 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 1 ; 1,2,5, 14-18, 22, 23 et 24 pour la phase 2) à l'aide de PFS.

Étape de courtier

Après avoir reçu le jeton OAuth 2.0 (de la passerelle d'authentification si l'authentification a abouti), le client de bureau interroge les services Amazon WorkSpaces (Broker Connection Manager) à l'aide de HTTPS. Le client de bureau s'authentifie en envoyant le jeton OAuth 2.0 et, suite à ceci, le client recevra les informations de point de terminaison de la passerelle de streaming.

Étape de streaming

Le client de bureau demande l'ouverture d'une session PCoIP avec la passerelle de streaming (à l'aide du jeton OAuth 2.0). La session est chiffrée avec le chiffrement aes256 et utilise le port PCoIP pour le contrôle des communications (c'est-à-dire, 4172/tcp).

A l'aide du jeton OAuth 2.0, la passerelle de streaming demande les informations WorkSpaces spécifiques à l'utilisateur au service WorkSpaces, via https.

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

Le WorkSpace initie ensuite une demande d'authentification vers l'AWS Directory Service configuré, à l'aide de l'authentification Kerberos standard.

Une fois le 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 votre bureau WorkSpaces sur l'interface de gestion est établie via UDP 55002. (Consultez la documentation Amazon Workspaces pour accéder aux détails relatifs à Amazon WorkSpaces. Le port UDP sortant initial est 55002.) La connexion de streaming, utilisant les ports 4172 (tcp et udp), est chiffrée à l'aide des chiffrements AES 128 et 256 bits, mais par défaut sur 128 bits. Vous pouvez activement changer ceci en 256 bits via l'objet Stratégie de groupe (GPO) Active Directory spécifique à PCoIP (pcoip.adm).

Interfaces réseau

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

L'interface réseau principale assure la connectivité vers les ressources à l'intérieur de votre VPC, comme l'accès à AWS Directory Service, Internet et votre réseau d'entreprise. Il est possible d'attacher des groupes de sécurité à l'interface réseau principale (comme vous le feriez pour toute ENI). Du point de vue conceptuel, nous différencions les groupes de sécurité attachés à cette ENI en fonction du périmètre du déploiement : groupe de sécurité WorkSpaces et groupes de sécurité ENI.

Interface réseau de gestion

Vous ne pouvez pas contrôler l'interface réseau de gestion via des groupes de sécurité. Par contre, vous pouvez tirer parti d'un pare-feu basé sur l'hôte sur votre WorkSpace pour bloquer des ports ou contrôler l'accès. Nous ne recommandons pas d'appliquer des restrictions sur l'interface réseau de gestion. Si vous décidez d'ajouter des règles de pare-feu basées sur l'hôte pour gérer cette interface, vous devez laisser quelques ports ouverts pour que le service WorkSpaces puisse gérer l'état de santé et l'accessibilité au WorkSpace, comme défini dans le guide d'administration Amazon WorkSpaces.

Groupe de sécurité WorkSpaces

Un groupe de sécurité par défaut est créé par AWS Directory Service et est attaché automatiquement à tous les WorkSpaces qui font partie de cet annuaire spécifique.

Comme avec tout autre groupe de sécurité, il est possible de modifier les règles d'un groupe de sécurité WorkSpaces. Les résultats prennent effet immédiatement une fois les modifications appliquées.

Il est également possible de modifier le groupe de sécurité WorkSpaces par défaut attaché à un AWS Directory Service en changeant l'association de groupe de sécurité WorkSpaces.

> **Remarque :** Un groupe de sécurité nouvellement associé ne sera attaché qu'aux WorkSpaces crées ou reconstruits après la modification.

Groupes de sécurité ENI

Comme l'interface réseau principale est une ENI classique, vous pouvez gérer sa configuration à l'aide des différents outils de gestion AWS (consultez Elastic Network Interfaces (ENI)). En particulier, recherchez l'adresse IP de WorkSpace (sur la page WorkSpaces de la console Amazon WorkSpaces), puis utilisez cette adresse IP comme filtre pour trouver l'ENI correspondante (dans la section Interfaces réseau de la console Amazon EC2).

Une fois que vous avez trouvé l'ENI, vous pouvez gérer directement les groupes de sécurité à partir de là. Lorsque vous affectez manuellement des groupes de sécurité à l'interface réseau principale, tenez compte des exigences des ports d'Amazon WorkSpaces, comme indiqué dans la section des détails relatifs à Amazon WorkSpaces.

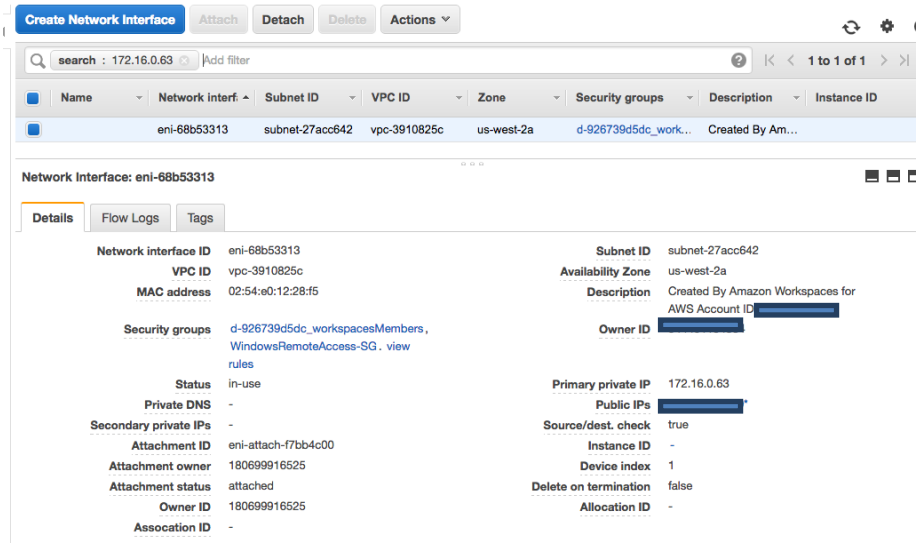

Figure 12 : Gestion des associations de groupe de sécurité

WorkSpaces chiffrés

A chaque espace de travail Amazon WorkSpace sont alloués un volume racine (disque C:) et un volume utilisateur (disque D:). La fonction de WorkSpaces chiffrés vous permet de chiffrer l'une des volumes ou les deux.

Qu'est-ce qui est chiffré ?

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

Quand le chiffrement a-t-il lieu ?

Vous devez spécifier le chiffrement pour un WorkSpace lors de son lancement (sa création). Les volumes WorkSpaces peuvent être chiffrés uniquement au moment du lancement : après le lancement, vous ne pouvez plus modifier le statut de chiffrement d'un volume. La Figure 13 montre la page de la console Amazon WorkSpaces permettant de choisir le chiffrement au lancement d'un nouveau WorkSpace.

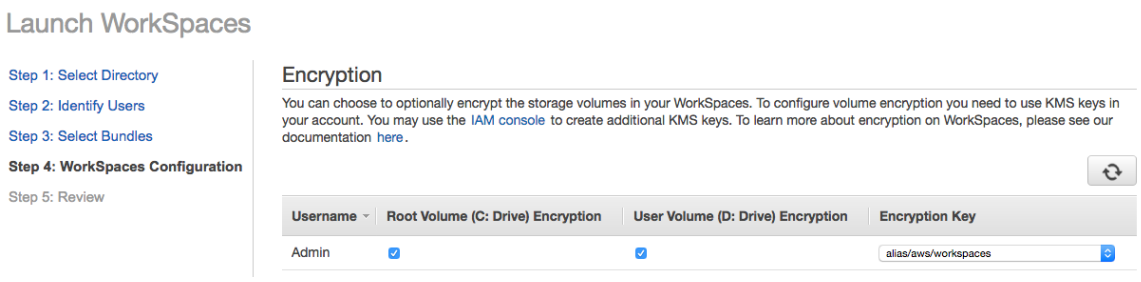

Figure 13 : Chiffrement de volumes WorkSpaces

Comment un nouveau WorkSpace est-il chiffré ?

Vous pouvez choisir l'option de WorkSpaces chiffrés à partir de la console Amazon WorkSpaces ou de la CLI AWS, ou à l'aide de l'API Amazon WorkSpaces lorsque vous lancez un nouveau WorkSpace.

Pour chiffrer les volumes, Amazon WorkSpaces utilise une clé principale du client (CMK) d'AWS Key Management Service (KMS). Une clé CMK AWS KMS est créée la première fois qu'un WorkSpace est lancé dans une région (les clés CMK ont une portée de niveau région). Vous pouvez également créer une clé CMK gérée client à utiliser avec des WorkSpaces chiffrés. La clé CMK permet de chiffrer les clés de données utilisées par le service Amazon WorkSpaces pour chiffrer les volumes (au sens strict, ce sera le service Amazon Elastic Block Store (Amazon EBS) qui chiffrera les volumes). Chaque clé CMK permet de chiffrer des clés pour jusqu'à 30 WorkSpaces.

> **Remarque :** La création d'images personnalisées à partir d'un WorkSpace chiffré n'est pas actuellement prise en charge. De plus, la mise en service de WorkSpaces lancés avec le chiffrement de volume racine activé peut prendre jusqu'à une heure.

Vous trouverez une description détaillée du processus de chiffrement sur la page de présentation du chiffrement Amazon WorkSpaces à l'aide d'AWS KMS. Pour plus d'informations sur les clés principales client AWS KMS et les clés de données, consultez la page relative aux concepts AWS Key Management Service.

Surveillance et journalisation à l'aide d'Amazon CloudWatch

La surveillance fait partie intégrante de toute infrastructure, qu'il s'agisse d'un réseau, de serveurs ou de journaux. Les clients qui déploient Amazon WorkSpaces doivent surveiller leurs déploiements, en particulier, la santé globale et le statut de connexion des différents WorkSpaces.

Métriques Amazon CloudWatch pour WorkSpaces

Les métriques CloudWatch pour WorkSpaces sont conçues pour donner aux administrateurs des informations supplémentaires sur la santé globale et le statut de connexion des différents WorkSpaces. Les métriques sont disponibles par WorkSpace ou regroupées pour tous les WorkSpaces d'une organisation au sein d'un annuaire donné (*AD Connector, voir la section relative à l'identité*).

Ces métriques, comme toutes les métriques CloudWatch, peuvent être affichées dans AWS Management Console (figure 13), consultées via les API CloudWatch, et surveillées par des alarmes CloudWatch et des outils tiers.

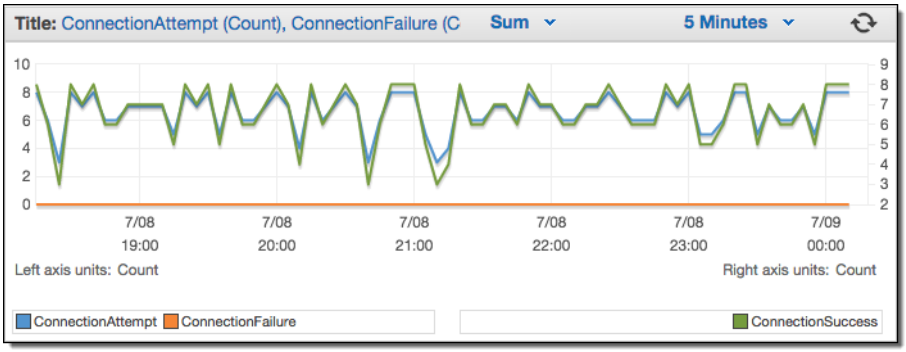

Figure 14: Métriques CloudWatch – ConnectionAttempt/ConnectionFailure

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

- **Available** : Les WorkSpaces qui répondent à un contrôle de statut sont comptés dans cette métrique.

- **Unhealthy** : Les WorkSpaces qui ne répondent pas au même contrôle de statut sont comptés dans cette métrique.
- **ConnectionAttempt** : Nombre de tentatives de connexion effectuées vers un WorkSpace.
- **ConnectionSuccess** : Nombre de tentatives de connexion réussies.
- **ConnectionFailure** : Nombre de tentatives de connexion ayant échoué.
- **SessionLaunchTime** : Temps pris pour initier une session, tel que mesuré par le client WorkSpaces.
- **InSessionLatency** : Temps aller-retour entre le client WorkSpaces et les WorkSpaces, tel que mesuré et signalé par le client.
- **SessionDisconnect** : Nombre de sessions initiées par l'utilisateur et fermées automatiquement.

De plus, des alarmes peuvent être créées, comme illustré à la figure 15.

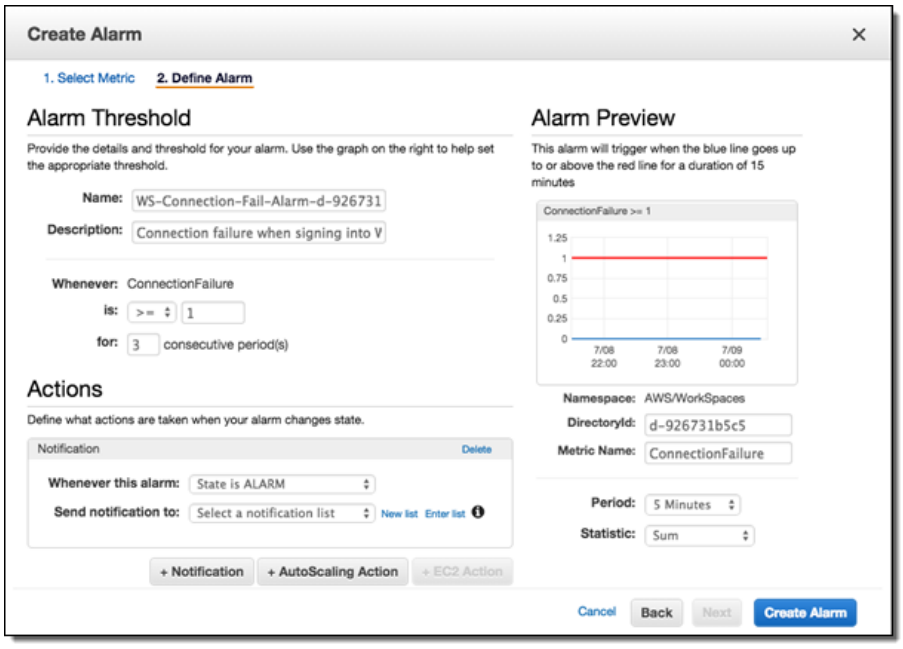

Figure 15 : Créer une alarme CloudWatch pour les erreurs de connexion WorkSpaces

Dépannage

Les problèmes courants d'administration et client, tels que « Je vois le message d'erreur suivant : « Your device is not able to connect to the WorkSpaces Registration service » (Votre appareil ne peut pas se connecter au service d'enregistrement de WorkSpaces) ou « Can't connect to a WorkSpace with an interactive logon banner » (Impossible de se connecter à une bannière de connexion interactive) peuvent être trouvés sur les pages de dépannage de client et d'administration du *guide d'administration Amazon WorkSpaces*.

AD Connector ne pas se connecter à Active Directory

Pour qu'AD Connector se connecte à votre annuaire sur site, le pare-feu pour tout votre réseau sur site doit avoir certains ports ouverts vers les CIDR pour les deux sous-réseaux du VPC (voir AD Connector). Pour vérifier si ces conditions sont satisfaites, exécutez les étapes suivantes :

Pour vérifier la connexion

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

```
DirectoryServicePortTest.exe -d <nom_domaine> -ip <adresse_IP_serveur> -tcp
"53,88,135,139,389,445,464,636,49152" -udp "53,88,123,137,138,389,445,464"
<nom_domaine>
```

<*nom_domaine*>

Nom de domaine complet utilisé pour tester les niveaux fonctionnels de la forêt et du domaine. Si vous excluez le nom de domaine, les niveaux fonctionnels ne seront pas testés.

<*adresse_IP_serveur*>

Adresse IP d'un contrôleur de domaine dans votre domaine sur site. Les ports seront testés sur cette adresse IP. Si vous excluez l'adresse IP, les ports ne seront pas testés.

Ceci déterminera si les ports nécessaires sont ouverts du VPC vers votre domaine. L'application de test vérifie également les niveaux fonctionnels minimum de la forêt et du domaine.

Comment vérifier la latence vers la région AWS la plus proche

En octobre 2015, Amazon WorkSpaces a lancé le site Web Connection Health Check. Ce site Web vérifie rapidement si vous pouvez obtenir tous les services requis pour utiliser WorkSpaces. Il effectue également une vérification des performances de chaque région AWS dans laquelle des services WorkSpaces s'exécutent et permet aux utilisateurs de savoir laquelle serait la plus rapide pour eux.

Conclusion

Nous constatons une évolution stratégique de l'informatique utilisateur final alors que les organisations s'efforcent de devenir plus agiles, de mieux protéger leurs données et d'aider leurs employés à être plus productifs. De nombreux avantages déjà réalisés avec le cloud computing s'appliquent également à l'informatique utilisateur final. En déplaçant leurs bureaux vers le cloud AWS avec Amazon WorkSpaces, les organisations peuvent rapidement évoluer au fur et à mesure qu'elles ajoutent des employés, améliorer leurs procédures de sécurité en conservant les données en dehors des appareils et offrir à leurs collaborateurs un bureau portable accessible depuis n'importe où, sur l'appareil de leur choix.

Amazon WorkSpaces est conçu pour s'intégrer à des systèmes et processus informatiques existants, et ce livre blanc décrit les bonnes pratiques pour cette intégration. Si vous suivez les instructions de ce livre blanc, vous bénéficiez d'un déploiement de bureau dans le cloud économique pouvant suivre l'évolution de votre entreprise sur l'infrastructure globale d'AWS.

Collaborateurs

Les personnes suivantes ont contribué à ce document :

- Justin Bradley, Architecte de solutions, Amazon Web Services
- Mahdi Sajjadpour, Consultant senior, AWS Professional Services
- Mauricio Munoz, Architecte de solutions, Amazon Web Services

Suggestions de lecture

Pour obtenir de l'aide, consultez les ressources suivantes :

- Troubleshooting AWS Directory Service Administration Issues
- Troubleshooting Amazon WorkSpaces Administration Issues
- Troubleshooting Amazon WorkSpaces Client Issues
- Amazon WorkSpaces Administration Guide
- Amazon WorkSpaces Developer Guide
- Supported Platforms and Devices
- How Amazon WorkSpaces Uses AWS KMS
- AWS CLI Command Reference – workspaces
- Monitoring Amazon WorkSpaces Metrics