Bonnes pratiques pour le déploiement des WorkSpaces applications Amazon

Bonnes pratiques pour le déploiement des WorkSpaces applications Amazon:

Table of Contents

Bonnes pratiques pour le déploiement des WorkSpaces applications Amazon

Date de publication : 19 janvier 2022 (Révisions du document)

Résumé

Ce livre blanc présente un ensemble de bonnes pratiques pour le déploiement d'Amazon WorkSpaces Applications. Le paper traite de la conception d'Amazon Virtual Private Cloud (VPC), de la création et de la gestion d'images, de la personnalisation de la flotte et des stratégies de mise à l'échelle automatique de la flotte. Il inclut les méthodes de connexion utilisateur, l'authentification et l'intégration à Microsoft Active Directory. Ce paper contient également des recommandations pour la conception de la sécurité, de la surveillance et de l'optimisation des coûts des WorkSpaces applications.

Ce livre blanc a été écrit pour permettre un accès rapide aux informations pertinentes. Il est destiné aux ingénieurs réseau, aux spécialistes de la fourniture d'applications, aux ingénieurs d'annuaires ou aux ingénieurs de sécurité.

Introduction

Amazon WorkSpaces Applications est un service de streaming d'applications entièrement géré qui fournit aux utilisateurs un accès instantané à leurs applications de bureau où qu'ils se trouvent. WorkSpaces Applications gère les AWS ressources nécessaires pour héberger et exécuter vos applications. Il évolue automatiquement et fournit un accès à vos utilisateurs à la demande. WorkSpaces Les applications permettent aux utilisateurs finaux d'accéder aux applications dont ils ont besoin sur l'appareil de leur choix, avec une expérience utilisateur réactive, identique à celle des applications installées en mode natif.

Les sections suivantes fournissent des informations sur Amazon WorkSpaces Applications, 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. Lors du déploiement WorkSpaces d'applications pour les utilisateurs finaux, il est important de mettre en œuvre les meilleures pratiques afin d'offrir une expérience utilisateur exceptionnelle. De plus, les entreprises de toutes tailles bénéficient d'une optimisation des coûts qui réduit les coûts opérationnels mensuels.

Concepts clés

Pour tirer le meilleur parti des WorkSpaces applications, familiarisez-vous avec les concepts suivants :

- Image — Une image est un modèle d'instance préconfiguré. Une image contient des applications que vous pouvez diffuser à vos utilisateurs, ainsi que des paramètres Windows et des applications par défaut pour permettre à vos utilisateurs de démarrer rapidement avec leurs applications. AWS fournit des images de base que vous pouvez utiliser pour créer des images qui incluent vos propres applications. Vous ne pouvez pas modifier le nom d'une image après sa création. Pour ajouter d'autres applications, mettre à jour des applications existantes ou modifier des paramètres d'image, vous devez créer une image. Vous pouvez copier vos images sur d'autres Régions AWSsites ou les partager avec d'autres Compte AWS personnes de la même région.
- Générateur d'images : un générateur d'images est une machine virtuelle que vous utilisez pour créer une image. Vous pouvez lancer un générateur d'images et vous y connecter à l'aide de la console WorkSpaces Applications. Une fois que vous êtes connecté à un Image Builder, vous pouvez installer, ajouter et tester vos applications, puis utiliser l'Image Builder pour créer une image. Vous pouvez lancer de nouveaux Image Builders en utilisant les images privées que vous possédez.
- Flotte : une flotte est composée d'instances de flotte (également appelées instances de streaming) qui exécutent l'image que vous spécifiez. Vous pouvez définir le nombre d'instances de streaming souhaité pour votre flotte et configurer des politiques pour adapter automatiquement votre flotte en fonction de la demande. Notez que chaque utilisateur a besoin d'une instance.
- Pile : une pile se compose d'un parc associé, de politiques d'accès utilisateur et de configurations de stockage. Vous configurez une pile pour démarrer le streaming d’applications vers les utilisateurs.
- Instance de streaming : une instance de streaming (également appelée instance de flotte) est une instance Amazon Elastic Compute Cloud (Amazon EC2) mise à la disposition d'un seul utilisateur pour le streaming d'applications. Une fois la session de l'utilisateur terminée, l'instance est interrompue par Amazon EC2.

Conception en VPC

Directives de conception

Déployez WorkSpaces des applications dans un VPC dédié. Lors de la conception du VPC WorkSpaces des applications, dimensionnez-le en fonction de la croissance prévue. Réservez la capacité des adresses IP pour les nouveaux cas d'utilisation et pour les zones de disponibilité (AZ) supplémentaires qui pourraient être ajoutées ultérieurement. L'un des points fondamentaux de la conception des WorkSpaces applications est qu'un seul utilisateur peut utiliser une instance d' WorkSpaces applications. Lorsque vous allouez de l'espace IP, considérez un utilisateur comme une adresse IP par instance WorkSpaces d'applications. Avec WorkSpaces Applications, il est possible pour un utilisateur de consommer plusieurs instances WorkSpaces d'applications. Par conséquent, la planification de l'espace IP doit également tenir compte des cas d'utilisation qui nécessitent des instances WorkSpaces d'applications supplémentaires.

Bien que la taille maximale d'un Inter-Domain routage sans classe VPC (CIDR) soit de /16, il est AWS recommandé de ne pas surallouer les adresses IP privées. Il est possible d'étendre la taille du VPC grâce à des CIDR supplémentaires, mais cela a une limite ; par conséquent, allouez ce qui est nécessaire dès le départ.

Si le déploiement WorkSpaces des applications est joint à un domaine Active Directory, le DNS du domaine doit être configuré pour les options DHCP définies pour le VPC. Le serveur de noms de domaine doit spécifier les adresses IP DNS qui font autorité pour le domaine Active Directory ou le DNS doit transmettre les demandes DNS aux instances DNS faisant autorité pour le domaine Active Directory. En outre, le VPC doit avoir `enableDnsHostnames` et `EnableDnsSupport` être configuré.

Zones de disponibilité

Une zone de disponibilité (AZ) est un ou plusieurs centres de données discrets dotés d'une alimentation, d'un réseau et d'une connectivité redondants dans un Région AWS. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l’échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Amazon WorkSpaces Applications ne nécessite qu'un seul sous-réseau pour le lancement d'une flotte. La meilleure pratique consiste à configurer au moins deux zones de disponibilité, un sous-réseau par zone de disponibilité unique. Pour optimiser la mise à l'échelle automatique de votre

flotte, utilisez plus de deux zones de disponibilité. La mise à l'échelle horizontale présente l'avantage supplémentaire d'ajouter de l'espace IP dans les sous-réseaux pour favoriser la croissance, ce qui est décrit dans la section suivante de ce document consacrée au dimensionnement des sous-réseaux. L'AWS Management Console ne permet de spécifier que deux sous-réseaux lors de la création d'une flotte. Utilisez la AWS Command Line Interface(AWS CLI) ou AWS CloudFormation pour autoriser plus de deux ID de sous-réseau.

Dimensionnement des sous-réseaux

Dédiez des sous-réseaux aux flottes d' WorkSpaces applications pour permettre une flexibilité dans les politiques de routage et la liste de contrôle d'accès au réseau. Les Stacks auront probablement des besoins en ressources distincts. Par exemple, les WorkSpaces applications Stacks peuvent avoir des exigences d'isolation qui cèdent la place à des ensembles de règles distincts. Lorsque plusieurs flottes Amazon WorkSpaces Applications utilisent les mêmes sous-réseaux, assurez-vous que la somme de la capacité maximale de toutes les flottes ne dépasse pas le nombre total d'adresses IP disponibles.

Si la capacité maximale de toutes les flottes d'un même sous-réseau peut ou a dépassé le nombre total d'adresses IP disponibles, migrez les flottes vers des sous-réseaux dédiés. Cela empêche les événements de dimensionnement automatique d'épuiser l'espace IP alloué. Si la capacité totale d'un parc dépasse l'espace IP alloué aux sous-réseaux assignés, utilisez l'API ou la AWS CLI pour « mettre à jour le parc » pour attribuer d'autres sous-réseaux. Pour plus d'informations, consultez les quotas Amazon VPC et comment les augmenter.

Il est recommandé d'augmenter le nombre de sous-réseaux, en dimensionnant les sous-réseaux en conséquence tout en réservant la capacité nécessaire à l'augmentation de la capacité de votre VPC. En outre, assurez-vous que le maximum du parc d' WorkSpaces applications ne dépasse pas l'espace IP total alloué par les sous-réseaux. Pour chaque sous-réseau AWS, cinq adresses IP sont réservées lors du calcul de la quantité totale d'espace IP. L'utilisation de plus de deux sous-réseaux et la mise à l'échelle horizontale présentent plusieurs avantages, tels que :

- Résilience accrue en cas de défaillance d'une zone de disponibilité
- Débit accru grâce à la mise à l'échelle automatique des instances de flotte
- Utilisation plus efficace des adresses IP privées, évitant ainsi de brûler des adresses IP

Lorsque vous dimensionnez des sous-réseaux pour Amazon WorkSpaces Applications, prenez en compte le nombre total de sous-réseaux et le pic de simultanéité attendu en cas de pic d'utilisation. Cela peut être surveillé en utilisant (`InUseCapacity`) plus la capacité réservée

(`AvailableCapacity`) pour une flotte. Dans Amazon WorkSpaces Applications, la somme des instances du parc d' WorkSpaces applications consommées et disponibles pour être consommées est étiquetée. `ActualCapacity` Pour dimensionner correctement l'espace IP total, prévoyez l'espace requis `ActualCapacity` et divisez-le par le nombre de sous-réseaux, moins un sous-réseau pour la résilience, attribué à la flotte.

Par exemple, si le nombre maximum prévu d'instances de flotte en période de pointe est de 1 000 et que l'exigence commerciale est de faire preuve de résilience en cas de défaillance d'une zone de disponibilité, 3 x/23 sous-réseaux répondent aux exigences techniques et commerciales.

- /23 = 512 hôtes — 5 réservés = 507 instances de flotte par sous-réseau
- 3 sous-réseaux — 1 sous-réseau = 2 sous-réseaux
- 2 sous-réseaux x 507 instances de flotte par sous-réseau = 1 014 instances de flotte en période de pointe

Exemple de dimensionnement de sous-réseau

Bien que 2 sous-réseaux /22 puissent également satisfaire à la résilience, tenez compte des points suivants :

- Au lieu de réserver 1 536 adresses IP, l'utilisation de deux AZ entraîne la réservation de 2 048 adresses IP, gaspillant ainsi des adresses IP qui pourraient être affectées à d'autres fonctions.
- Si une zone de disponibilité devient inaccessible, la capacité de faire évoluer les instances de flotte est limitée par le débit d'une zone de zone de disponibilité. Cela peut prolonger la durée de`PendingCapacity`.

Routage des sous-réseaux

Il est recommandé de créer des sous-réseaux privés pour les instances d' WorkSpaces applications, en les acheminant vers l'Internet public via un VPC centralisé pour le trafic sortant. Le trafic entrant pour le streaming WorkSpaces des sessions Applications est géré via le service Amazon WorkSpaces Applications via Streaming Gateway : vous n'avez pas besoin de configurer de sous-réseaux publics pour cela.

Intra-Region connectivité

Pour les instances de parc d' WorkSpaces applications jointes à un domaine Active Directory, configurez les contrôleurs de domaine Active Directory dans un VPC Shared Services dans chacune d'elles. Région AWS Les sources d'Active Directory peuvent être des contrôleurs de domaine basés sur Amazon EC2 ou AWS Microsoft Managed AD. Le routage entre les services partagés et WorkSpaces les VPC d'applications peut se faire via une connexion d'appairage VPC ou une passerelle de transit. Bien que les passerelles de transit résolvent la complexité du routage à grande échelle, il existe un certain nombre de raisons pour lesquelles l'appairage VPC est préférable dans la plupart des contextes :

- Le peering VPC est une connexion directe entre les deux VPC (aucun saut supplémentaire).
- Il n'y a aucun frais horaire, juste le taux de transfert de données standard entre les zones de disponibilité.
- Il n'y a aucune limite de bande passante.
- Support pour accéder aux groupes de sécurité entre les VPC.

Cela est particulièrement vrai si WorkSpaces les instances d'applications se connectent à des serveurs de and/or fichiers d'infrastructure d'applications avec de grands ensembles de données dans un VPC de service partagé. En optimisant le chemin d'accès à ces ressources fréquemment

consultées, la connexion d'appairage VPC est préférée, même dans les conceptions où tous les autres routages VPC et Internet sont effectués via une passerelle de transit.

Trafic Internet sortant

Alors que le routage direct vers les services partagés est principalement optimisé par le biais d'une connexion de peering, le trafic sortant pour les WorkSpaces applications peut être conçu en créant un point de sortie Internet unique à partir de plusieurs VPC à l'aide de Transit Gateway AWS . Dans une conception multi-VPC, il est courant de disposer d'un VPC dédié qui contrôle tout le trafic Internet sortant. Grâce à cette configuration, les passerelles de transit bénéficient d'une plus grande flexibilité et d'un meilleur contrôle du routage sur les tables de routage standard associées aux sous-réseaux. Cette conception prend également en charge le routage transitif sans complexité supplémentaire et élimine le besoin de passerelles de traduction d'adresses réseau (NAT) redondantes ou d'instances NAT dans chaque VPC.

Une fois que tout le trafic Internet sortant est centralisé dans un VPC unique, les passerelles NAT ou les instances NAT constituent un choix de conception courant. Pour déterminer ce qui convient le mieux à votre organisation, consultez le guide d'administration permettant de comparer les passerelles NAT et les instances NAT. AWS Network Firewall peut étendre la protection au-delà des niveaux du groupe de sécurité et du contrôle d'accès au réseau en protégeant au niveau de la route et en proposant des règles apatrides et dynamiques des couches 3 à 7 du modèle OSI. Pour plus d'informations, reportez-vous à la section Modèles de déploiement pour AWS Network Firewall. Si votre organisation a choisi un produit tiers doté de fonctionnalités avancées telles que le filtrage d'URL, déployez le service dans votre VPC Internet sortant. Cela peut remplacer les passerelles NAT ou les instances NAT. Suivez les directives fournies par le fournisseur tiers.

On-premises

Lorsque la connectivité aux ressources locales est requise, en particulier pour les instances d' WorkSpaces applications jointes à Active Directory, établissez une connexion hautement résiliente via AWS Direct Connect.

Points de terminaison d’un VPC

Point de terminaison VPC Amazon S3

De nombreux déploiements d'Amazon WorkSpaces Applications nécessitent la persistance de l'état utilisateur via les dossiers de base et les paramètres des applications. Activez les communications

privées avec ces sites Amazon Simple Storage Service (Amazon S3), afin d'éviter d'utiliser l'Internet public. Vous pouvez y parvenir par le biais d'une passerelle de point de terminaison VPC. Une passerelle de point de terminaison VPC est préférable à une passerelle AWS PrivateLink pour Amazon S3 pour les raisons suivantes :

- Il est optimisé en termes de coûts pour les exigences d'accès au réseau des WorkSpaces applications
- L'accès au compartiment Amazon S3 n'est pas requis depuis les ressources locales
- Un document de politique personnalisé peut être utilisé pour restreindre l'accès uniquement à partir des instances WorkSpaces d'applications

Une fois que vous avez créé la passerelle de point de terminaison VPC, il est recommandé de sécuriser la connexion privatisée en créant une politique personnalisée. La politique personnalisée commence par l'Amazon Resource Name (ARN) du rôle Identity and Access Management du service WorkSpaces Applications. Spécifiez explicitement les actions S3 requises pour la persistance de l'état utilisateur.

> **Note**
>
> L'exemple suivant de la `Resources` section indique d'abord le chemin du dossier de base de l'état et le chemin des paramètres de l'application ensuite.

Example

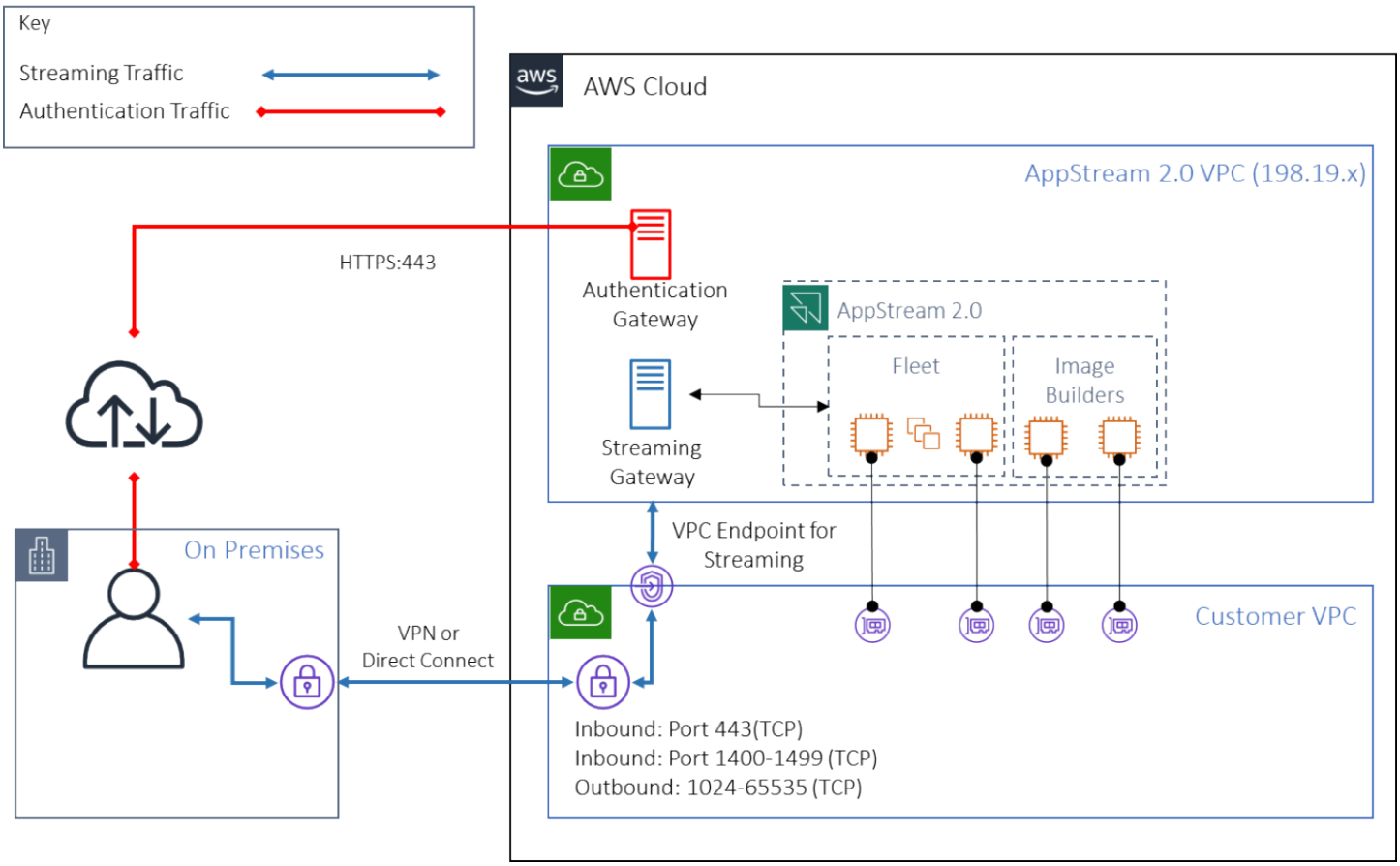
Point de terminaison VPC de l'interface API Amazon WorkSpaces Applications

Dans les scénarios de conception où les commandes d'API et de CLI destinées à Amazon WorkSpaces Applications proviennent de votre VPC, privatisez ces appels programmatiques via un point de terminaison VPC d'interface.

Point de terminaison VPC de l'interface de streaming Amazon WorkSpaces Applications

Bien qu'il soit possible d'acheminer le trafic de streaming d'Amazon WorkSpaces Applications via un point de terminaison VPC d'interface, utilisez cette configuration avec prudence. Le comportement

de streaming par défaut via l'Internet public est la méthode de diffusion la plus efficace et la plus performante pour le trafic de streaming d'Amazon WorkSpaces Applications.



Point de terminaison VPC de l'interface de streaming Amazon WorkSpaces Applications

Comme le montre la figure précédente, l'Internet public est le moyen le plus efficace d'accéder aux passerelles de streaming Amazon WorkSpaces Applications. Le routage via le VPC géré par le client et le réseau ajoutent de la complexité et de la latence. Cela ajoute également les frais de transfert de données Direct Connect.

> **Note**
>
> Seul le streaming est pris en charge par le point de terminaison VPC, et l'authentification doit toujours avoir lieu via l'Internet public. Les accès prérequis tels que le fournisseur d'identité Sign-On (IdP) SAML unique (SSO) restent une exigence accessible uniquement via l'Internet public.

Création et gestion d'images

Lorsque vous lancez un parc ou un générateur d'images dans WorkSpaces Applications, vous devez sélectionner l'une des images de base des WorkSpaces applications. Les administrateurs peuvent ensuite s'appuyer sur l'image de base pour ajouter leurs propres applications et paramètres de configuration.

Lors de la création d'une image, des considérations essentielles doivent être prises en compte pour garantir le fonctionnement correct et sécurisé des applications. En outre, il existe des considérations de conception quant à la manière dont cette image sera conservée.

Création d'une image d' WorkSpaces applications

Lorsque vous créez une nouvelle image, il est important de prendre en compte les points suivants :

- Système d’exploitation
- Applications
- Profil utilisateur
- Sécurité
- Performance
- Version d'agent
- Image Assistant CLI

Création d'une image d' WorkSpaces applications

En novembre 2021, WorkSpaces Applications a lancé la prise en charge d'Amazon Linux 2. Avec cette annonce, WorkSpaces Applications prend désormais en charge quatre types de plateformes :

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Amazon Linux 2

Il est possible que vous deviez choisir une plate-forme particulière en fonction des exigences de votre application (par exemple, si votre application nécessite Windows, Amazon Linux 2 ne sera pas une

option). Au-delà des exigences de l'application, reportez-vous à la matrice de comparaison suivante pour vous aider à choisir le type de plate-forme le mieux adapté à votre cas d'utilisation et à votre environnement :

Tableau 1 — Types de plateformes, quand les utiliser et prix

Types de plateforme	Quand l’utiliser	Tarification de la flotte*
Windows Server (2012 R2, 2016 ou 2019)	Votre application ne peut être exécutée que sous Windows (et elle ne prend pas en charge Amazon Linux 2). Vous souhaitez joindre un domaine à vos instances de streaming. Vous souhaitez utiliser la stratégie de groupe existante sur vos instances de streaming d' WorkSpace s applications (Linux ne respecte pas la stratégie de groupe, mais vous pouvez utiliser des scripts de session pour automatiser la configura tion au démarrage d'une session). Vous utiliserez Desktop View et vos utilisate urs préféreront l'expérience de bureau Windows. Vous préférez utiliser l'applica tion Image Assistant, qui fournit un assistant étape par étape, pour créer votre catalogue d'applications et votre image. Actuellem ent, vous devez créer votre image Amazon Linux 2 à l'aide des commandes du	Frais RDS SAL (Microsoft Remote Desktop Services Subscriber Access License) de 4,19$ par mois pour chaque utilisateur unique**, auxquels s'ajoutent les éléments suivants : 1. 0,10$ de l'heure pour les Always-On flottes On-Demand 2. 0,15$ de l'heure pour les flottes élastiques

Types de plateforme	Quand l'utiliser	Tarification de la flotte*
	terminal (consultez ce didacticiel pour plus d'informations). Vous souhaitez utiliser la persistance des paramètres de l'application. L'activation de la persistance des paramètres de l'application n'est actuellement pas prise en charge pour les Linux-based piles.	
Amazon Linux 2	Vous souhaitez profiter d'instances de streaming à moindre coût et éviter les frais de licence RDS SAL. Vos applications sont compatibles avec Amazon Linux 2	Les instances Linux sont moins coûteuses que les instances Windows. Avec Linux, vous ne payez aucun frais RDS SAL et les frais horaires suivants : 1. 0,084$ de l'heure pour les flottes Always-On On-Demand 2. 0,112 USD de l'heure pour les flottes Elastic

* Basé sur stream.standard.medium dans la région de Virginie du Nord

** Les clients éligibles peuvent apporter leur propre licence afin d'éliminer les frais AWS RDS SAL. Consultez la page de tarification des WorkSpaces applications pour plus de détails. Les clients du secteur de l'éducation peuvent également bénéficier d'une offre spéciale. Les écoles, les universités et certaines institutions publiques peuvent bénéficier d'une réduction des frais d'utilisation de Microsoft RDS SAL.

Applications

Avant d'installer des applications, il est important de passer en revue les exigences des applications, telles que les dépendances des applications et les exigences matérielles. Après avoir correctement

installé les applications sur les instances du générateur d'images, assurez-vous de changer d'utilisateur et de tester les applications dans le contexte de l'utilisateur de test.

Lorsque vous planifiez le déploiement de votre application, prenez en compte les points de terminaison et les quotas du service. Nettoyez également les fichiers d'installation et d'assistance pour optimiser l'espace total sur le lecteur C avant de créer une image. Pour rappel, les instances WorkSpaces Applications disposent d'un volume fixe de 200 Go. L'optimisation de l'espace disque après les installations est une bonne pratique pour garantir que le volume de taille fixe n'est jamais dépassé.

Si vous souhaitez modifier le catalogue d'applications auxquelles vos utilisateurs peuvent accéder en temps réel, le framework d'applications dynamique fournit des opérations d'API. Les applications gérées par les fournisseurs d'applications dynamiques peuvent se situer dans l'image, ou elles peuvent être hors instance, par exemple à partir d'un partage de fichiers Windows ou d'une application de technologie de virtualisation. Cette fonctionnalité nécessite un parc d' WorkSpaces applications joint à un domaine Microsoft Active Directory. Pour plus d'informations, reportez-vous à la section Utilisation d'Active Directory avec WorkSpaces des applications.

Blocs d'applications

Les blocs d'applications représentent le script de configuration et les fichiers d'application nécessaires au lancement des applications que vos utilisateurs utiliseront. Le disque dur virtuel (VHD) peut être n'importe quel objet d'Amazon S3. Il est recommandé que la taille de cet objet soit inférieure à 1,5 Go, car il doit être entièrement téléchargé avant que l'utilisateur puisse accéder à l'application.

Optimisation des blocs d'applications

Pour les Windows-based flottes, il est recommandé de créer un fichier VHDX pour contenir votre application. Pour les Linux-based flottes, il est recommandé de créer une image (IMG). Ces disques virtuels doivent être créés aussi petits que possible pour héberger les fichiers de l'application. Les disques virtuels peuvent être compressés pour réduire encore leur taille. Dans le script de configuration, vous devez décompresser le disque avant de le monter. L'exemple de script PowerShell d'installation Windows inclut la fonctionnalité de décompression. Il existe un compromis entre l'extension d'une archive (zip) et la vitesse de téléchargement. Certains tests peuvent être nécessaires pour trouver un équilibre offrant le temps de lancement d'application le plus rapide.

Mise à jour des applications

Les applications peuvent présenter des modifications mineures et majeures. Pour les mises à jour mineures, utilisez l'option Activer le contrôle de version sur le compartiment Amazon S3 qui héberge les fichiers de blocage de votre application. Ce paramètre permet aux administrateurs de revenir aux versions précédentes d'une application spécifique en modifiant la version de l'objet VHD de l'application en question sans modifier la configuration du bloc d'applications. Avec les mises à jour majeures, créez un nouveau bloc d'applications pour le VHD mis à jour. Cela permettra aux administrateurs de séparer les modifications majeures des applications au niveau du bloc d'applications par opposition au niveau du versionnement, ce qui fournit une approche plus organisée pour la gestion administrative des applications.

Personnalisation du profil utilisateur

Amazon WorkSpaces Applications est, de par sa conception, une solution d'application et de bureau non persistante. Lorsqu'une session utilisateur est interrompue, les modifications apportées au système et à l'utilisateur le sont également. Activez la persistance des paramètres de l'application uniquement lorsque cela est nécessaire. Cela peut alourdir le processus d'ouverture de session et entraîner des considérations financières pour le stockage S3 requis.

Dans les situations où la persistance des paramètres de l'application est requise, il est AWS recommandé de sécuriser cette connexion par le biais d'une politique personnalisée et d'un point de terminaison de passerelle VPC S3. Évaluez la taille globale des paramètres de l'application et minimisez les paramètres enregistrés dans la persistance des paramètres de l'application afin d'optimiser les coûts et les performances.

La personnalisation du profil utilisateur peut être configurée sur une instance d' WorkSpaces Applications Image Builder. Cela inclut l'ajout et la modification de clés de registre, l'ajout de fichiers et d'autres configurations spécifiques à l'utilisateur. Dans l'assistant d'image des WorkSpaces applications, il est possible de créer un profil utilisateur. Le modèle de profil utilisateur est alors copié dans le profil utilisateur par défaut. Une fois l'image déployée dans une flotte, les utilisateurs finaux qui diffusent des sessions depuis la flotte verront leur profil utilisateur créé à partir du profil utilisateur par défaut. Il est important d'envisager de minimiser la taille du profil utilisateur, en particulier lorsque la persistance des paramètres de l'application est activée. Par défaut, la taille maximale de VHDx pour le profil utilisateur est de 1 Go. Chaque fois qu'une session de streaming démarre, un fichier VHDx de profil utilisateur est téléchargé depuis un compartiment S3. Cela augmente le temps de préparation de la session de streaming et présente un risque de dépassement de la limite, ce qui entraînera l'échec du montage du profil utilisateur à l'aide du fichier vHDx.

Pour les cas d'utilisation nécessitant un profil utilisateur supérieur à 1 Go, AWS recommande d'utiliser d'autres méthodes pour stocker les profils. Par exemple, en utilisant des profils d'itinérance ou des conteneurs de profils FSLogix sur un stockage partagé tel qu'Amazon FSx for Windows File Server. Pour plus d'informations, consultez Utiliser Amazon FSx for Windows File Server et FSLogix pour optimiser la persistance des paramètres des applications sur Amazon Applications. WorkSpaces

Sécurité

Les développeurs doivent prendre en compte différentes mesures de sécurité. WorkSpaces Les administrateurs d'applications sont responsables de l'installation et de la maintenance des mises à jour du système d'exploitation Windows, de vos applications et de leurs dépendances. Pour obtenir des conseils supplémentaires sur la mise à jour des images de base, reportez-vous à la section Conserver l'image de vos WorkSpaces applications Up-to-Date pour obtenir des conseils supplémentaires sur la mise à jour des images de base.

Par défaut, WorkSpaces Applications permet aux utilisateurs ou aux applications de démarrer n'importe quel programme sur l'instance, au-delà de ce qui est spécifié dans le catalogue d'applications d'imagerie. Cela est utile lorsque votre application s'appuie sur une autre application dans le cadre d'un flux de travail, mais que vous ne souhaitez pas que l'utilisateur puisse démarrer directement cette application dépendante. Par exemple, votre application démarre le navigateur pour fournir des instructions d'aide à partir du site Web du fournisseur de l'application, mais vous ne souhaitez pas que l'utilisateur démarre le navigateur directement. Dans certains cas, vous souhaiterez peut-être contrôler les applications qui peuvent être lancées sur les instances de streaming. Microsoft AppLocker est un logiciel de contrôle des applications qui utilise des politiques de contrôle explicites pour activer ou désactiver les applications qu'un utilisateur peut exécuter.

Les logiciels antivirus peuvent nuire aux sessions de streaming et aux instances du générateur d'images. AWS recommande de ne pas activer les mises à jour automatiques pour le logiciel antivirus. Pour plus d'informations sur Windows Defender, reportez-vous à la section Logiciel antivirus.

Performance

Avant de créer une nouvelle image, il est important de tester les applications en tant qu'utilisateur de test. Les tests en tant qu'utilisateur de test vous permettent de vous assurer que les applications peuvent s'exécuter dans un contexte utilisateur non administrateur. Vérifiez également les performances des applications et l'expérience utilisateur à l'aide d'outils intégrés tels que le

gestionnaire de tâches et le moniteur de performances. Il est recommandé de surveiller l'utilisation des ressources telles que le processeur, la mémoire et la mémoire du processeur graphique. En cas de contrainte liée au processeur, à la mémoire ou aux ressources de mémoire du processeur graphique, envisagez de mettre à niveau le type d'instance. Pour améliorer les performances :

- Désactiver les fenêtres contextuelles du navigateur
- Désactiver la sécurité améliorée d'IE

WorkSpaces Sélection de la version de l'agent d'applications

Lorsque vous créez une nouvelle image, vous pouvez choisir d'utiliser le dernier logiciel d'agent d' WorkSpaces applications ou de ne pas le mettre à jour. Chaque version du logiciel de l'agent d' WorkSpaces applications inclut des corrections de bogues et des améliorations de fonctionnalités. Conservez votre image à l'aide des logiciels les plus récents. Passez en revue les mécanismes correspondants dans la section Mises à jour des images de ce document.

Vous pouvez choisir l'option Utiliser le dernier agent. Cette option garantit qu'au démarrage, le dernier agent WorkSpaces d'applications est toujours installé. Cependant, des modifications inattendues peuvent affecter l'expérience utilisateur, et une mise à jour de l'agent peut augmenter le délai de démarrage d'une instance. La mise à jour d'une image de base nécessite une recréation de l'image. Il est également important d'effectuer des tests avant de déployer l'image mise à jour en production afin de minimiser le temps de démarrage.

Interface de ligne de commande (CLI) d'Image Assistant

Pour les développeurs qui souhaitent automatiser ou créer par programmation des images d' WorkSpaces applications, utilisez l'interface de ligne de commande Image Assistant. Ceci est disponible sur les générateurs d'images dotés du logiciel d'agent d' WorkSpaces applications publié le 26 juillet 2019 ou après cette date. La présentation générale suivante décrit le processus de création par programmation d'une image d' WorkSpaces applications :

1. Utilisez l’automatisation d’installation de votre application pour installer les applications requises sur votre mage Builder. Cette installation peut inclure des applications que vos utilisateurs lanceront, des dépendances, et des applications en arrière-plan.
2. Déterminez les fichiers et les dossiers à optimiser.
3. Le cas échéant, utilisez l'opération Image Assistant `add-application` CLI pour spécifier les métadonnées de l'application et le manifeste d'optimisation pour l'image WorkSpaces Applications.

4. Pour spécifier des applications supplémentaires pour l'image WorkSpaces Applications, répétez les étapes 1 à 3 pour chaque application selon les besoins.
5. Le cas échéant, utilisez l'opération Image Assistant `update-default-profile` CLI pour remplacer le profil Windows par défaut et créer l'application par défaut et les paramètres Windows pour vos utilisateurs.
6. Utilisez l'opération d'interface de ligne de commande `create-image` d'Image Assistant pour créer l'image.

Pour plus d'informations, reportez-vous à la section Création d'une image d' WorkSpaces application par programmation à l'aide des opérations de la CLI de l'Assistant Image.

Gérer l'expérience de streaming des utilisateurs

Personnalisation à l'aide de scripts de session

WorkSpaces Les applications fournissent des scripts de session sur instance. Vous pouvez les utiliser pour exécuter vos propres scripts personnalisés lorsque des événements spécifiques surviennent au cours des sessions de streaming des utilisateurs. Par exemple, vous pouvez utiliser des scripts personnalisés pour préparer l'environnement de vos WorkSpaces applications avant le début des sessions de streaming de vos utilisateurs. Vous pouvez également utiliser les scripts personnalisés pour nettoyer les instances de streaming après que les utilisateurs ont terminé leur session.

Spécifiez les scripts de session dans une image d' WorkSpaces applications. Pour plus d'informations sur la configuration des scripts de session, consultez la section du guide d'administration sur l'utilisation de scripts de session pour gérer l'expérience utilisateur. Utilisés avec un partage réseau ou un profil Gestion des identités et des accès AWS(IAM), vous pouvez utiliser des scripts de session pour récupérer des scripts supplémentaires depuis un emplacement de stockage. Grâce à ces scripts supplémentaires, vous pouvez optimiser davantage l'expérience utilisateur. Cela permet de minimiser le nombre d'images et de flottes nécessaires pour fournir des environnements applicatifs à vos utilisateurs.

Utilisation de la stratégie de groupe Active Directory

Si vous envisagez d'utiliser WorkSpaces des flottes d'applications dans un domaine Active Directory, vous pouvez utiliser des objets de politiques de groupe (GPO) pour gérer l'expérience utilisateur. Les

GPO peuvent être attribués à l'unité organisationnelle (UO) dans laquelle les instances WorkSpaces d'applications sont créées. Pour simplifier la création d'images, lancez l'image d' WorkSpaces applications de base dans une unité d'organisation qui bloque l'héritage. Cela permet d'éviter que d'autres politiques de domaine n'aient un impact sur l'expérience utilisateur WorkSpaces des applications. Le déploiement de chaque flotte dans son unité d'organisation dédiée, avec des GPO uniques établissant l'environnement, permet de tirer parti des avantages consolidés de la gestion des images des WorkSpaces applications.

Un exemple d'utilisation de la stratégie de groupe consiste à spécifier un ensemble d'images différentes pages d'accueil Internet Explorer pour chaque parc d' WorkSpaces applications.

mises à jour des images

L'application de correctifs logiciels est essentielle à la sécurité et aux performances des ressources informatiques. L'application fréquente de correctifs figure parmi les meilleures pratiques dans le pilier de sécurité du Well-Architected Framework.

Lorsque votre image est créée et déployée, quatre catégories de logiciels nécessitent l'application de correctifs à votre image d' WorkSpaces applications :

- Applications et dépendances : vous êtes responsable de l'application des correctifs aux applications et aux dépendances de vos images.
- Système d'exploitation Microsoft Windows : vous êtes responsable de l'installation et de la maintenance des mises à jour pour Windows.
- Composants logiciels : il s'agit de pilotes, d'agents et d'autres logiciels nécessaires au fonctionnement WorkSpaces des applications (par exemple, l' CloudWatchagent Amazon). WorkSpaces Les applications publient régulièrement de nouvelles images de base contenant de nouveaux agents et pilotes. Vous pouvez reconstruire votre image à l'aide de la dernière base afin d'adapter les composants logiciels de leurs images à la dernière ligne de base. Le processus de reconstruction d'une image sur la base la plus récente peut être long et fastidieux lorsqu'il existe de nombreuses applications ou lorsque les installations d'applications sont complexes.
- WorkSpaces Agent d'applications : vous pouvez choisir Toujours utiliser la dernière version de l'agent dans Image Assistant. Avec cette option, les instances de streaming lancées à partir de l'image utilisent automatiquement la dernière version de l'agent.

Vous pouvez maintenir l'image de vos WorkSpaces applications à jour en effectuant l'une des opérations suivantes :

- Mettre à jour une image à l'aide des mises à jour d'image des WorkSpaces applications gérées : cette méthode de mise à jour fournit les dernières mises à jour du système d'exploitation Windows et des pilotes, ainsi que le dernier logiciel de l'agent d' WorkSpaces applications. Cette méthode gérée met à jour les composants du service et du système d'exploitation Microsoft, mais elle ne vous permet pas de mettre à jour les composants de votre application. Il est recommandé d'utiliser cette méthode lorsque les installations d'applications sont complexes ou nécessitent une configuration manuelle.
- Mettre à jour le logiciel de l'agent d' WorkSpaces applications à l'aide de versions d'image WorkSpaces des applications gérées : cette méthode de mise à jour fournit le dernier logiciel de l'agent d' WorkSpaces applications. Cette méthode vous permet de mettre à jour les composants de votre application.

Personnalisation de la flotte

Type de flotte

Lors de la création d'une flotte, les clients doivent choisir un type de flotte. Chaque type de flotte offre des avantages différents en termes d'expérience utilisateur, de coûts et de frais de maintenance. Quel que soit le type de parc choisi, chaque option prend en charge les types de plateformes Windows et Linux, ainsi que la vue Desktop ou la vue Application.

Les clients peuvent désormais choisir parmi les types de flotte suivants :

- Always-On— Ce type de flotte permet aux utilisateurs d'accéder instantanément à leurs applications. Toutes les instances actives de votre flotte vous seront facturées, même si aucun utilisateur n'utilise d'applications de streaming.
- On-Demand— Sélectionnez ce type de flotte pour optimiser vos coûts de streaming. Avec une flotte à la demande, les utilisateurs bénéficieront d'une heure de début de session d'environ une à deux minutes. Toutefois, les frais d'instance de streaming ne vous seront facturés que lorsque les utilisateurs sont connectés, ainsi qu'un petit tarif horaire pour chaque instance du parc qui n'est pas une application de streaming.
- Elastic — Les flottes élastiques peuvent être utilisées pour des applications qui ne nécessitent pas d'installation et peuvent être exécutées à partir d'un disque dur virtuel (VHD). Les flottes élastiques ne prennent pas en charge WorkSpaces les images d'applications et ne nécessitent pas de politiques de dimensionnement. Vous n'êtes facturé que pour la durée d'une session de streaming.

Tableau 2 — Types de flottes Amazon WorkSpaces Applications

Type de flotte	Quand l’utiliser	Expérience utilisateur	Modèle de tarification	Remarques
Always-On	Vos utilisateurs ont besoin d'un accès instantané aux applications lorsqu'il	Accès instantané aux applications	Vous payez le plein tarif pour chaque instance disponible dans votre	Prend en charge les politiques d'image et de mise à l'échelle personnalisées.

Type de flotte	Quand l’utiliser	Expérience utilisateur	Modèle de tarification	Remarques
	s démarrent une session. Vous n'aurez pas de capacité excédentaire significative dans votre flotte, peut-être parce que vos habitudes d'utilisation sont prévisibles et que vous pouvez contrôler les coûts de manière fiable grâce à des politiques de dimension nement.		parc (qu'elle soit utilisée ou non pour une session).	

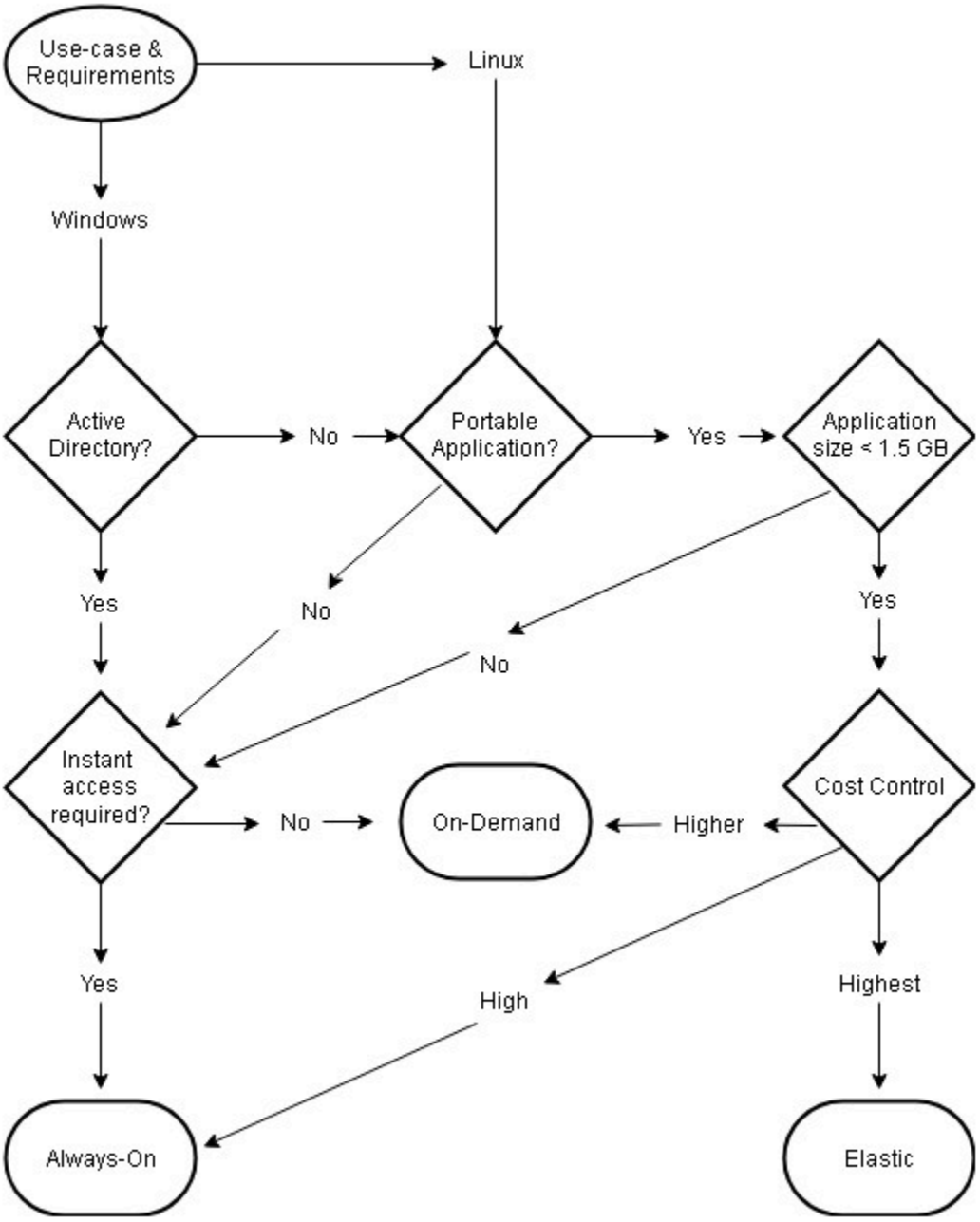
Type de flotte	Quand l'utiliser	Expérience utilisateur	Modèle de tarification	Remarques
On-Demand	Vous devez conserver une capacité excédentaire significative dans vos flottes. Vous souhaitez bénéficier de l'environnement le plus rentable possible et ne voulez pas payer le prix fort pour la capacité inutilisé e. Vos utilisate urs peuvent attendre une à deux minutes pour accéder à leurs applicati ons après avoir démarré une session. Vous utilisez des types d'instances plus important s. Le coût horaire d'une instance en cours d'exécuti on est bien plus élevé que le coût	Les utilisateurs attendent une à deux minutes pour accéder à leurs applicati ons après le démarrage d'une session.	Vous payez le plein tarif uniquement pour les instances de streaming avec une session active, puis un petit coût horaire pour les instances inactives.	Prend en charge les politiques d'image et de mise à l'échelle personnalisées.

Type de flotte	Quand l’utiliser	Expérience utilisateur	Modèle de tarification	Remarques
	de l'instance arrêtée.			

Type de flotte	Quand l'utiliser	Expérience utilisateur	Modèle de tarification	Remarques
Elasticité	La taille de votre application et de ses dépendances est inférieure à 1,5 Go environ. Chaque fois qu'un utilisateur démarre une session dans un parc Elastic, le fichier de votre disque dur virtuel (VHD) doit être téléchargé depuis Amazon S3 dans la session. Par conséquent, des fichiers VHD plus volumineux (c'est-à-dire d'une taille supérieure à 1,5 Go) nuiront à l'expérience utilisateur final. Votre application est portable. En d'autres termes, votre application et toutes ses dépendances peuvent être placées sur un	L'utilisateur attend entre 45 secondes et 3 minutes pour accéder aux applications après le démarrage de la session (le temps d'attente dépend de la taille du disque dur virtuel).	Vous n'êtes facturé que pour la durée d'une session de streaming. Comme il n'existe aucun concept d'instances inactives dans les flottes Elastic, vous n'avez aucun frais à payer pour les instances non utilisées.	Ne prend pas en charge les images personnalisées (le client fournit un VHD avec les applications) ni les politiques de dimensionnement. Supports `stream.standard.small` et `stream.standard.medium` instances actuels. Si votre cas d'utilisation nécessite un autre type d'instance, veuillez contacter l'équipe chargée de votre AWS compte.

Type de flotte	Quand l’utiliser	Expérience utilisateur	Modèle de tarification	Remarques
	disque dur virtuel et lancées à partir d'instanc es de streaming associées à un domaine VHD.You ne nécessitant pas (la jonction de domaine n'est actuellement pas disponible avec les flottes Elastic). Vous souhaitez payer uniquement pour les sessions actives (c'est-à-dire ne pas payer pour la capacité inutilisé e de votre flotte). Vos utilisateurs peuvent attendre 45 secondes ou plus pour accéder à leurs applicati ons après le démarrage d'une session. Vous voulez qu'AWS gère le dimension			

Type de flotte	Quand l'utiliser	Expérience utilisateur	Modèle de tarification	Remarques
	nement pour vous (aucune politique de dimension nement à gérer).			



Types de flotte, cas d'utilisation et exigences

Dimensionnement de la flotte

Capacité minimale et mise à l'échelle planifiée

Lors du dimensionnement de votre parc d' WorkSpaces applications, plusieurs facteurs se répercutent directement sur l'expérience utilisateur et les coûts. La valeur saisie pour la capacité

minimale garantit que le nombre d'instances d' WorkSpaces applications sera rarement inférieur à cette valeur. Après la fin d'une session d' WorkSpaces applications, si le nombre total d'instances d' WorkSpaces applications est inférieur à la valeur de capacité minimale, une nouvelle instance de flotte démarre. Comme toujours, il est important de se rappeler qu'une instance d' WorkSpaces applications correspond directement à une session utilisateur, ce qui influence directement la valeur de la capacité minimale.

La saisie d'une valeur pour la capacité minimale supérieure à la simultanéité prévue entraîne une augmentation des coûts, bien que l'expérience utilisateur n'en soit pas affectée. Une valeur trop faible entraîne de faibles coûts, mais a un impact sur l'expérience utilisateur lorsque le nombre total de demandes dépasse la capacité disponible. Les administrateurs remarqueront des erreurs de « capacité insuffisante » dans ce type de situation. Par exemple, attendre de `PendingCapacity` devenir `AvailableCapacity` est une utilisation inefficace du temps de l'utilisateur lorsque le nombre de connexions prévues en début de journée est une valeur constante prévisible.

Commencez par une capacité minimale adaptée aux heures creuses habituelles, puis utilisez une politique de dimensionnement planifié pour réinitialiser efficacement la capacité minimale avant le début de la journée de travail. N'oubliez pas de créer une autre politique de dimensionnement planifié pour ramener la capacité minimale aux heures creuses. Pour plus d'informations sur les politiques de dimensionnement et sur la manière de les mettre en œuvre, reportez-vous à la section Stratégies d'auto-scaling de la flotte de ce document.

Capacité maximale et quotas de service

La définition de la capacité maximale peut sembler arbitraire, mais lorsqu'elle est correctement prévue et définie, elle optimise la consommation et le coût totaux des ressources. Une valeur saisie supérieure au quota de service pour le parc d' WorkSpaces applications de votre parc d'applications Compte AWS peut sembler valide, mais lorsque des événements de dimensionnement automatique tentent de dimensionner les ressources au maximum de leur capacité, ils ne sont pas lancés, car la valeur de capacité maximale dépasse le quota de service disponible. Assurez-vous qu'une demande de quota de service est déposée pour la capacité maximale souhaitée afin de garantir que le dimensionnement automatique fonctionne comme prévu par votre organisation.

Le coût est un autre élément important à prendre en compte lors de la définition d'une valeur de capacité maximale. Pour plus d'informations, reportez-vous à la section Optimisation des coûts avec le choix du type de flotte de ce document.

Choix de l'affichage du bureau ou de l'affichage des applications

Le choix d'une vue d'application ou d'une vue de bureau n'a aucun impact sur les performances ou les coûts. Une seule vue est accessible à la fois par parc WorkSpaces d'applications. Vous pouvez modifier l'option Stream view. Planifiez ce changement pendant les heures creuses, car la modification de la vue du stream nécessite un redémarrage de la flotte.

Il n'existe pas de meilleure pratique unique pour l'affichage des flux. L'impact des options d'affichage des flux est résumé comme suit :

- Rapports détaillés sur l'utilisation des applications via la fonctionnalité Rapports d'utilisation pour les administrateurs
- Expérience globale et flux de travail pour les utilisateurs finaux (par exemple, un poste de travail complet répond-il aux besoins du cas d'utilisation ou la seule visualisation des applications suffira-t-elle ?).

Vue du bureau

Dans les cas d'utilisation où tout le flux de travail de l'utilisateur est effectué en session, Desktop View simplifie l'expérience utilisateur en centralisant toutes les applications dans un seul environnement. Desktop View peut offrir une expérience utilisateur plus cohérente pour les déploiements de plus de 3 à 5 applications nécessitant une intégration au système d'exploitation (OS). Desktop View est efficace lorsque vous gérez deux environnements séparés et distincts. Par exemple, un utilisateur peut avoir accès simultanément à un environnement de bureau de production et de pré-production pour valider les modifications apportées à la mise en page, à la configuration et à l'accès aux applications.

WorkSpaces Les rapports d'utilisation des applications créent un rapport quotidien sur les applications pour Desktop View. Le résultat obtenu pour l'application est simplement « bureau », mappé directement à la session WorkSpaces Applications. Pour plus d'informations, reportez-vous à la section Surveillance de l'utilisation des utilisateurs de ce document.

Afficher uniquement les applications

La vue Applications uniquement est également efficace lorsque la pile WorkSpaces Applications est destinée à fournir quelques applications requises par intermittence. Dans les environnements de kiosque, la diffusion des applications est verrouillée de manière sécurisée via Application View. Avec Application View, WorkSpaces Applications remplace le shell Windows par défaut par un shell personnalisé. Ce shell personnalisé ne présente que les applications en cours d'exécution, minimisant ainsi la surface d'attaque du système d'exploitation.

Dans les cas d'utilisation où WorkSpaces les applications sont utilisées pour améliorer l'environnement de bureau d'une organisation existante, l'affichage Applications uniquement est préférable. Déployez le client WorkSpaces Applications Windows en mode application natif afin de minimiser la confusion chez les utilisateurs en permettant l'utilisation complète des raccourcis clavier.

Amazon WorkSpaces Applications Usage Reports crée un rapport quotidien sur les applications à consulter. Pour des rapports plus précis sur l'utilisation des applications et des exécutions, envisagez une solution tierce pour établir des rapports au niveau du système d'exploitation. Vous pouvez utiliser Microsoft AppLocker en mode reporting ou envisager des solutions disponibles dans le AWS Marketplace, telles que Stratusphere UX de Liquidware.

Gestion des identités et des accès AWS configuration des rôles

Si une charge de travail nécessite que les utilisateurs finaux des WorkSpaces applications accèdent à d'autres AWS services depuis leur session, il est recommandé de déléguer l'accès à l'aide de rôles Gestion des identités et des accès AWS (IAM). Les rôles IAM peuvent être directement associés à la session de votre utilisateur final par le biais de l'attribution au niveau de la flotte. Pour connaître les meilleures pratiques supplémentaires relatives à l'utilisation de rôles IAM avec WorkSpaces des applications, consultez cette section du guide de l'administrateur.

Utilisation d'informations d'identification statiques

Certaines charges de travail peuvent nécessiter des entrées statiques pour les clés d'accès IAM au lieu de les hériter du rôle attaché. Il existe deux méthodes pour recevoir ces informations d'identification. La première méthode consiste à stocker les clés d'accès dans un AWS service, puis à donner à vos utilisateurs finaux un accès IAM explicite pour extraire cette valeur spécifique du service. Deux exemples de mécanismes de stockage de clés d'accès utilisent AWS Secrets Managerou AWS SSM Parameter Store. La deuxième méthode consiste à utiliser le fournisseur d'informations d'identification WorkSpaces Applications pour accéder aux clés d'accès

du rôle attaché. Cela peut être fait en invoquant le fournisseur d'informations d'identification et en analysant la sortie pour votre clé d'accès et votre clé secrète. Voici un exemple de la manière d'effectuer cette PowerShell action.

```
$CMD = 'C:\Program Files\Amazon\Photon\PhotonRoleCredentialProvider
\PhotonRoleCredentialProvider.exe'
$role = 'Machine'

$output = & $CMD --role=$role
$parsed = $output | ConvertFrom-Json

$access_key = $parsed.AccessKeyId
$secret_key = $parsed.SecretAccessKey
$session_token = $parsed.SessionToken
```

Protection du compartiment S3 de vos WorkSpaces applications

Si la charge de travail de vos WorkSpaces applications est configurée avec la persistance des and/or applications dans le dossier d'accueil, il est recommandé de protéger le compartiment Amazon S3 dans lequel les données persistantes sont stockées contre tout accès non autorisé ou toute suppression accidentelle. La première couche de protection consiste à ajouter une politique de compartiment Amazon S3 afin d'empêcher la suppression accidentelle du compartiment. Le deuxième niveau de protection consiste à ajouter une politique de compartiment conforme au principe du moindre privilège. L'alignement sur le principe peut être effectué en autorisant uniquement l'accès au bucket aux parties nécessaires.

Stratégies de mise à l'échelle automatique des flottes

Comprendre les instances WorkSpaces d'applications

WorkSpaces Les instances de parc d'applications ont un ratio utilisateur/instance de parc de 1:1. Cela signifie que chaque utilisateur dispose de sa propre instance de streaming. Le nombre d'utilisateurs que vous connectez simultanément déterminera la taille de la flotte.

Politiques de mise à l’échelle

WorkSpaces Les flottes d'applications sont lancées dans un groupe Application Auto Scaling. Cela permet à la flotte d'évoluer en fonction de l'utilisation pour répondre à la demande. Au fur et à mesure que l'utilisation augmente, le parc s'agrandit, et lorsque les utilisateurs se déconnectent, le parc s'agrandit à nouveau. Ceci est contrôlé par la définition de politiques de dimensionnement. Vous pouvez définir des politiques de mise à l'échelle planifiée, de mise à l'échelle par étapes et de suivi des cibles. Pour plus d'informations sur ces politiques de dimensionnement, consultez Fleet Auto Scaling for Amazon WorkSpaces Applications.

Mise à l’échelle par étapes

Ces politiques augmentent ou diminuent la capacité de la flotte d'un pourcentage de la taille actuelle de la flotte ou d'un nombre spécifique d'instances. Les politiques de dimensionnement des étapes sont déclenchées par CloudWatch les métriques des WorkSpaces applications de `Capacity UtilizationAvailable Capacity`, ou`Insufficient Capacity Errors`.

Lorsque vous utilisez des politiques de dimensionnement par étapes, il est AWS recommandé d'ajouter un pourcentage de capacité et non un nombre fixe d'instances. Cela garantit que vos actions de mise à l'échelle sont proportionnelles à la taille de votre flotte. Cela vous aidera à éviter les situations dans lesquelles vous augmentez trop lentement (parce que vous avez ajouté un petit nombre d'instances par rapport à la taille de votre flotte) ou trop de situations lorsque votre flotte est petite.

Suivi des cibles

Cette politique définit un niveau d'utilisation de la capacité pour la flotte. La mise à l'échelle automatique des applications crée et gère les CloudWatch alarmes qui déclenchent la politique de

dimensionnement. Cela permet d'augmenter ou de supprimer la capacité nécessaire pour maintenir le parc à la valeur cible spécifiée ou à un niveau proche de celle-ci. Pour garantir la disponibilité des applications, votre parc évolue proportionnellement à l'indicateur aussi vite que possible, mais de manière plus progressive. Lorsque vous configurez le suivi des cibles, tenez compte du temps de recharge pour vous assurer que le scale-out et le scale-in se produisent aux intervalles souhaités.

Le suivi des cibles est efficace dans les situations de taux de désabonnement élevés. Le churn se produit lorsqu'un grand nombre d'utilisateurs démarrent ou terminent des sessions en peu de temps. Vous pouvez identifier le taux de désabonnement en examinant CloudWatch les indicateurs de votre flotte. Les périodes pendant lesquelles votre flotte a une capacité en attente non nulle sans modification (ou avec très peu de changement) de la capacité souhaitée indiquent qu'un taux de désabonnement élevé est probable. Dans les situations où le taux de désabonnement est élevé, configurez des politiques de suivi des cibles dans lesquelles (100 — pourcentage d'utilisation cible) est supérieur au taux de désabonnement sur une période de 15 minutes. Par exemple, si 10 % de votre flotte doit être résiliée en 15 minutes en raison de la rotation des utilisateurs, fixez un objectif d'utilisation de la capacité de 90 % ou moins pour compenser le taux de désabonnement élevé.

Scheduled-based mise à échelle

Ces politiques vous permettent de définir la capacité de flotte souhaitée en fonction d'un calendrier chronologique. Cette politique est efficace lorsque vous comprenez le comportement de connexion et que vous pouvez prévoir l'évolution de la demande.

Par exemple, au début de la journée de travail, vous pouvez vous attendre à ce que 100 utilisateurs demandent des connexions de streaming à 9 h 00. Vous pouvez configurer une politique de dimensionnement planifiée pour fixer la taille minimale du parc à 100 à 8 h 40. Cela permet de créer des instances de flotte et de les rendre disponibles au début de la journée de travail, et de permettre à 100 utilisateurs de se connecter en même temps. Vous pouvez ensuite définir une autre politique planifiée pour étendre la flotte à un minimum de dix à 17 heures. Cela vous permet de réduire les coûts, car la demande de sessions en dehors des heures de bureau est moindre que pendant la journée de travail.

Politiques de mise à l'échelle en production

Vous pouvez choisir de combiner différents types de politiques de dimensionnement dans un seul parc afin de définir des politiques de dimensionnement précises adaptées au comportement de vos utilisateurs. Dans l'exemple précédent, vous pouvez combiner la politique de dimensionnement planifiée avec les politiques de suivi des cibles ou de dimensionnement par étapes pour maintenir un niveau d'utilisation spécifique. La combinaison d'une mise à l'échelle planifiée et d'une mise à

l'échelle basée sur le suivi des cibles peut contribuer à réduire l'impact d'une forte augmentation des niveaux d'utilisation lorsque la capacité est requise immédiatement.

Les utilisateurs connectés à des sessions de streaming lorsqu'une politique de dimensionnement modifie le nombre d'instances souhaité ne sont pas affectés par le scale-in ou le scale-out. Les politiques de dimensionnement ne mettront pas fin aux sessions de streaming existantes. Les sessions existantes se poursuivront sans interruption jusqu'à ce que l'utilisateur mette fin à la session ou jusqu'à ce qu'une politique de temporisation du parc soit établie.

La surveillance de l'utilisation des WorkSpaces applications à l'aide de CloudWatch métriques peut vous aider à optimiser vos politiques de dimensionnement au fil du temps. Par exemple, il est courant de surprovisionner les ressources lors de la configuration initiale et vous pouvez assister à de longues périodes de faible utilisation. Par ailleurs, si le parc est sous-approvisionné, vous risquez de rencontrer des erreurs liées à une utilisation élevée de la capacité et à une « capacité insuffisante ». L'examen CloudWatch des métriques peut vous aider à ajuster vos politiques de dimensionnement afin d'atténuer ces erreurs. Pour plus d'informations et des exemples de politiques de dimensionnement des WorkSpaces applications que vous pouvez utiliser, consultez la section Adapter vos flottes Amazon WorkSpaces Applications.

Bonnes pratiques pour la conception de politiques à grande échelle

Combinez les politiques de dimensionnement

De nombreux clients choisissent de combiner différents types de politiques de dimensionnement au sein d'un même parc afin d'accroître la puissance et la flexibilité d'Auto Scaling in WorkSpaces Applications. Par exemple, vous pouvez configurer une politique de dimensionnement planifié pour augmenter le minimum de votre flotte à 6 h 00 en prévision du début de la journée de travail des utilisateurs, et pour diminuer le minimum de flotte à 16 h 00 avant que les utilisateurs ne cessent de travailler. Vous pouvez associer cette politique de dimensionnement planifiée à des politiques de suivi des cibles ou de dimensionnement par étapes afin de maintenir un niveau d'utilisation spécifique et d'augmenter ou de réduire au cours de la journée pour faire face à une utilisation intensive. La combinaison d'une mise à l'échelle planifiée et d'une mise à l'échelle basée sur le suivi des cibles peut contribuer à réduire l'impact d'une forte augmentation des niveaux d'utilisation lorsque la capacité est requise immédiatement.

Évitez d'augmenter le taux de désabonnement

Déterminez si votre flotte est susceptible de connaître un taux de désabonnement élevé en raison de votre cas d'utilisation. Le churn se produit lorsqu'un grand nombre d'utilisateurs démarrent puis terminent des sessions dans un court laps de temps. Cela peut se produire lorsque de nombreux utilisateurs accèdent simultanément à une application de votre flotte pendant quelques minutes seulement avant de se déconnecter.

Dans de telles situations, la taille de votre flotte peut être bien inférieure à la capacité souhaitée, car les instances se terminent lorsque les utilisateurs mettent fin à leurs sessions. Les politiques de dimensionnement par étapes peuvent ne pas ajouter d'instances assez rapidement pour compenser le taux de désabonnement et, par conséquent, votre flotte se retrouve bloquée à une certaine taille.

Vous pouvez identifier le taux de désabonnement en examinant CloudWatch les indicateurs de votre flotte. Les périodes pendant lesquelles la capacité en attente de votre flotte est différente de zéro sans modification (ou avec très peu de changement) de la capacité souhaitée indiquent qu'un taux de désabonnement élevé est probable. Pour tenir compte des situations de taux de désabonnement élevés, appliquez des politiques de dimensionnement du suivi des cibles et

choisissez une utilisation cible de telle sorte que (100 — pourcentage d'utilisation cible) soit supérieur au taux de désabonnement sur une période de 15 minutes. Par exemple, si 10 % de votre parc doit être supprimé dans un délai de 15 minutes en raison de la rotation des utilisateurs, fixez un objectif d'utilisation de la capacité de 90 % ou moins pour compenser le taux de désabonnement élevé.

Comprendre le taux de provisionnement maximal

Les clients qui gèrent des flottes d' WorkSpaces applications pour un grand nombre d'utilisateurs devraient envisager de fixer des limites de débit. Cette limite aura un impact sur la rapidité avec laquelle les instances peuvent être ajoutées à une flotte ou à toutes les flottes d'un Compte AWS.

Il y a deux limites à prendre en compte :

- Pour un seul parc, WorkSpaces les applications approvisionnent au maximum 20 instances par minute.
- Pour une seule instance Compte AWS, WorkSpaces Applications approvisionne au rythme de 60 instances par minute (avec une rafale de 100 instances par minute).

Si plus de trois flottes sont mises à l'échelle en parallèle, la limite de taux de provisionnement des comptes est partagée entre ces flottes (par exemple, six flottes évoluant en parallèle peuvent chacune approvisionner jusqu'à 10 instances par minute). Tenez également compte du temps nécessaire à une instance de streaming donnée pour terminer le provisionnement en réponse à un événement de dimensionnement. Pour les flottes qui ne sont pas associées à un domaine Active Directory, ce délai est généralement de 15 minutes. Pour les flottes associées à un domaine Active Directory, cela peut prendre jusqu'à 25 minutes.

Compte tenu de ces contraintes, considérez les exemples suivants :

- Si vous souhaitez faire passer un parc unique de 0 à 1 000 instances, le provisionnement prendra 50 minutes (1 000 instances/20 instances par minute), puis 15 à 25 minutes supplémentaires pour que toutes les instances soient disponibles pour les utilisateurs finaux, soit un total de 65 à 75 minutes.
- Si vous souhaitez faire passer simultanément trois flottes de 0 à 333 instances (pour un total de 999 instances dans le Compte AWS), il faudra environ 17 minutes (999/60instances par minute) pour que toutes les flottes terminent le provisionnement, puis 15 minutes supplémentaires pour que ces instances soient disponibles pour les utilisateurs finaux, soit un total de 32 à 42 minutes.

Utiliser plusieurs zones de disponibilité

Choisissez plusieurs AZ dans la région pour le déploiement de votre flotte. Lorsque vous sélectionnez plusieurs AZ pour votre flotte, vous augmentez la probabilité que votre flotte soit en mesure d'ajouter des instances en réponse à un événement de dimensionnement. La CloudWatch métrique PendingCapacity est un point de départ pour évaluer dans quelle mesure la conception de la flotte AZ est optimisée dans le cadre de déploiements de flottes de grande envergure. Une valeur élevée et soutenue pour PendingCapacity peut indiquer la nécessité d'étendre la mise à l'échelle horizontale (entre les AZ). Pour plus d'informations, consultez la section Surveillance des ressources WorkSpaces des applications Amazon.

Par exemple, si le dimensionnement automatique tente de fournir des instances pour augmenter la taille de votre flotte et que la capacité de l'AZ sélectionnée est insuffisante, le dimensionnement automatique ajoutera des instances dans les autres AZ que vous avez spécifiées pour votre flotte. Pour plus d'informations sur les zones de disponibilité et la conception WorkSpaces des applications, reportez-vous à la section Zones de disponibilité de ce document.

Surveiller les mesures d'erreur de capacité insuffisante

L' « erreur de capacité insuffisante » est une CloudWatch métrique pour les flottes WorkSpaces d'applications. Cette métrique indique le nombre de demandes de session rejetées en raison d'un manque de capacité.

Lorsque vous modifiez vos politiques de dimensionnement, il est utile de créer une CloudWatch alarme pour vous avertir en cas d'erreur de capacité insuffisante. Cela vous permet d'ajuster rapidement vos politiques de dimensionnement afin d'optimiser la disponibilité pour les utilisateurs. Le guide d'administration décrit en détail les étapes à suivre pour surveiller WorkSpaces les ressources de vos applications.

Méthodes de connexion

Lorsqu'ils diffusent des sessions dans WorkSpaces Applications, les utilisateurs disposent de deux méthodes de connexion :

- Accès au navigateur Web : tous les HTML5-capable navigateurs sont pris en charge. Aucun plug-in ou téléchargement n'est requis.
- WorkSpaces Applications : client Windows

Il est recommandé de prendre en compte les fonctionnalités et les appareils requis pour le cas d'utilisation de votre utilisateur afin de déterminer quel navigateur ou appareil répond le mieux à ses besoins.

> **Note**
>
> WorkSpaces Les applications ne sont pas prises en charge sur les appareils dont la résolution d'écran est inférieure à 1 024 x 768 pixels.

Fonctionnalité récapitulative et prise en charge des appareils

Tableau 3 — Résumé des fonctionnalités et des appareils pris en charge

	Accès au navigateur Web	WorkSpaces Applications : client Windows
Moniteur multiple (résolution jusqu'à 2k)	Pris en charge	Pris en charge
Moniteur multiple (résolution jusqu'à 4k)	N/A	Pris en charge
Support pour tablette de dessin	Pris en charge*	Pris en charge
Support pour appareils à écran tactile	Pris en charge	N/A

	Accès au navigateur Web	WorkSpaces Applications : client Windows
Prise en charge des périphériques USB	N/A	Pris en charge
Raccourcis clavier	Pris en charge	Pris en charge
Décalage relatif de la souris	Pris en charge	Pris en charge
Transfert de fichiers	Pris en charge	Pris en charge
Redirection de l'imprimante locale	N/A	Pris en charge
Redirection du lecteur local	N/A	Pris en charge
Web-cam soutien	Pris en charge	Pris en charge

*Google Chrome et Mozilla Firefox uniquement

Accès au navigateur Web

WorkSpaces L'accès au navigateur Web des applications permet d'accéder aux applications sans qu'il soit nécessaire d'installer un client dédié. Les utilisateurs peuvent se connecter à l'aide d'un HTML5-capable navigateur compatible. Aucun plugin ou extension de navigateur n'est requis.

L'accès par navigateur Web offre un large choix de systèmes d'exploitation et de types de terminaux.

WorkSpaces Client d'applications pour Windows

Le client WorkSpaces Applications pour Windows est une application que vous installez sur votre PC Windows. Cette application fournit des fonctionnalités supplémentaires qui ne sont pas disponibles lorsque vous accédez aux WorkSpaces applications à l'aide d'un navigateur Web. Par exemple, le client WorkSpaces Applications vous permet d'effectuer les opérations suivantes :

- Utilisez plus de deux moniteurs ou une résolution 4K
- Utilisez vos appareils USB avec des applications diffusées via WorkSpaces Applications

- Accédez à vos disques et dossiers locaux pendant vos sessions de streaming
- Redirigez les tâches d'impression de votre application de streaming vers une imprimante connectée à votre ordinateur local
- Utilisez votre webcam locale pour les conférences vidéo et audio dans le cadre de vos sessions de streaming
- Utilisez les raccourcis clavier dans les applications auxquelles vous accédez pendant vos sessions de streaming
- Interagissez avec vos applications de streaming à distance de la même manière que vous interagissez avec les applications installées localement

WorkSpaces Modes de connexion client aux applications

Le client WorkSpaces Applications propose deux modes de connexion : le mode application native et le mode classique. Le mode de connexion que vous choisissez détermine les options qui seront disponibles pendant le streaming d'application, ainsi que le fonctionnement et l'affichage de vos applications de streaming. Les administrateurs peuvent contrôler la capacité des utilisateurs à passer du mode application natif au mode classique.

- Le mode classique diffuse les applications dans la fenêtre de session WorkSpaces Applications. Cela est similaire à la façon dont les utilisateurs finaux diffusent des applications dans un navigateur Web. Utilisez le mode classique si les utilisateurs finaux préfèrent diffuser des applications de la même manière que les navigateurs, tout en utilisant des fonctionnalités supplémentaires telles que la connexion pour les fichiers locaux et la redirection d'imprimantes. Le mode classique est le mode de connexion par défaut recommandé. Le mode classique est le seul mode pris en charge pour Desktop View.
- Le mode application native permet aux utilisateurs finaux de travailler avec des applications de streaming à distance de la même manière que les autres applications installées localement. Si les utilisateurs finaux ont l'habitude de travailler avec des applications installées localement, le mode d'application natif offre une expérience fluide. L'application de diffusion à distance fonctionne à peu près de la même manière qu'une application installée localement. L'icône de l'application s'affiche dans la barre des tâches de votre PC local, exactement comme les icônes de vos applications locales. Contrairement aux icônes de vos applications locales, les icônes de vos applications de streaming en mode application native incluent le logo WorkSpaces Applications. Le mode d'application natif est le mode de connexion recommandé lorsque les utilisateurs souhaitent utiliser les raccourcis clavier des applications et passer facilement d'une application locale à une application distante individuelle à l'aide de raccourcis clavier.

Déploiement et gestion des clients

Les utilisateurs peuvent installer le client WorkSpaces Applications eux-mêmes, ou les administrateurs peuvent installer le client WorkSpaces Applications pour eux en exécutant PowerShell des scripts à distance ou en reconditionnant le client WorkSpaces Applications avec des paramètres personnalisés.

Vous devez qualifier les périphériques USB que vous voulez autoriser vos utilisateurs à utiliser avec leur session de streaming. Si leur périphérique USB n'est pas qualifié, il ne sera pas détecté par WorkSpaces les applications et ne pourra pas être partagé avec la session. Une fois leurs appareils qualifiés, vos utilisateurs doivent les partager avec les WorkSpaces applications chaque fois qu'ils démarrent une nouvelle session de streaming.

Lors du déploiement du client WorkSpaces Applications à grande échelle, il est AWS recommandé d'utiliser l'outil de déploiement d'entreprise. L'outil de déploiement d'entreprise inclut les fichiers d'installation du client WorkSpaces Applications et un modèle d'administration de stratégie de groupe.

Domaines personnalisés

Lors du déploiement d' WorkSpaces applications par programmation, il est possible de créer un domaine personnalisé qui peut fournir aux utilisateurs une expérience familière pour les sessions de streaming. Dans les déploiements d'applications IDP SAML 2.0, il est important WorkSpaces de souligner que l'accès des utilisateurs commence au niveau de l'IdP, et non des applications. WorkSpaces Les utilisateurs n'ont pas besoin WorkSpaces d'URL d'applications, car celles-ci sont fournies par l'IdP après authentification. Par conséquent, les noms de domaine personnalisés ne sont pas requis pour les déploiements d'IdP SAML 2.0.

Authentification

Avec WorkSpaces Applications, l'authentification peut avoir lieu en dehors d'Amazon WorkSpaces Applications ou dans le cadre du service WorkSpaces Applications. La sélection de la manière dont l'authentification aura lieu pour le déploiement de vos WorkSpaces applications est une considération fondamentale de votre conception. Il n'est pas rare qu'une entreprise déploie plusieurs WorkSpaces applications pour différents cas d'utilisation. Chaque cas d'utilisation peut avoir une méthode d'authentification différente.

Il existe trois types de méthodes d'authentification pour les WorkSpaces applications :

- SAML 2.0
- Groupe d'utilisateurs
- Programmatique

Déterminer la méthode optimisée

Amazon WorkSpaces Applications est conçu pour être flexible afin de s'appliquer à la plupart des exigences de conception organisationnelle. Lors de la détermination de la méthode d'authentification optimisée, il est recommandé de prendre en compte les objectifs et les finalités des utilisateurs du service, ainsi que les politiques et procédures de l'organisation.

Voici quelques exemples de combinaison de cas d'utilisation avec des objectifs organisationnels.

Tableau 4 — Cas d'utilisation avec objectifs organisationnels

Exemple	Description	Authentification
Des instances de flotte jointes à un domaine sont requises	Les applications installées sur l'image WorkSpaces Applications ne sont accessibles qu'aux ressources jointes au domaine.	SAML 2.0
Intégration poussée avec les services Microsoft	Dépendance organisationnelle vis-à-vis du développement de politiques de groupe Microsoft	SAML 2.0

Exemple	Description	Authentification
	et d'une infrastructure principal e	
Entreprise unique existante Sign-on (SSO)	Tous les nouveaux services doivent tirer parti d'une solution SSO d'entreprise dotée de plusieurs processus de reporting et de sécurité établis.	SAML 2.0
Support des cartes à puce pour les applications	Cartes à puce (telles que la vérification d'identité privée et les cartes d'accès communes) pour l'authentification en cours de session pour les applicati ons diffusées via un lecteur de carte à puce.	SAML 2.0
Main-d'œuvre saisonnière avec personnel temporaire	Quelques mois par an, les travailleurs temporaires se voient attribuer un petit ensemble de demandes qui n'incluent pas les ressource s internes nécessaires pour mener à bien leurs activités.	Groupe d'utilisateurs
Support informatique limité	Petites entreprises comptant moins de 50 utilisateurs et disposant d'un personnel informatique limité, qui cherchent à réduire les coûts liés à la gestion d'un fournisse ur d'identité (IdP)	Groupe d'utilisateurs

Exemple	Description	Authentification
Fournisseur de logiciels indépendant (ISV)	Solution propriétaire conçue par votre organisation qui inclut les droits et l'authent ification des utilisateurs, en étendant WorkSpaces les applications dans le cadre de votre solution. *	Programmatique
Vitrine technologique	Environnement totalemen t éphémère présentant une technologie propriétaire dans le cadre d'une visite guidée de votre solution, sans qu'il soit nécessaire de stocker les informations utilisateur.	Programmatique
Expérience de site Web interactive	Rendez votre site Web interactif avec des applications Windows en streaming. **	Programmatique

*Consultez les fournisseurs de logiciels : diffusez vos applications sur n'importe quel appareil utilisateur pour plus d'informations.

**Reportez-vous à la section Intégrer des sessions de streaming d' WorkSpaces applications pour plus d'informations.

Si votre organisation a un cas d'utilisation ou une politique qui n'est pas répertoriée dans les exemples donnés précédemment, il est recommandé de prévoir l'état final souhaité de la consommation du flux de travail des WorkSpaces applications afin de garantir que la solution d'authentification n'entre pas en conflit avec cet état.

Configuration de votre fournisseur d'identité

SAML 2.0

Le langage SAML (Security Assertion Markup Language) 2.0 est une option de déploiement courante permettant aux utilisateurs d'utiliser AWS des ressources. Différents fournisseurs d'identité SAML 2.0 tiers prennent en charge les WorkSpaces applications. Que WorkSpaces les ressources de vos applications soient jointes à un domaine ou non, l'IdP SAML 2.0 vous oblige à utiliser IAM.

Comme la plupart IdPs génèrent un fichier metadata.xml unique avec des attributs SAML spécifiques pour chaque application SAML, chaque pile d' WorkSpaces applications nécessite un rôle entretenant une relation de confiance avec l'IdP SAML et une politique dotée d'une autorisation unique sur AppStream:Stream avec des conditions répondant aux exigences de l'IdP SAML et de l'ARN de la pile d'applications. WorkSpaces

Le guide WorkSpaces d'administration des applications fournit un exemple de configuration pour la conception d'une pile d' WorkSpaces applications unique. Pour les déploiements à piles multiples, reportez-vous aux étapes facultatives d'utilisation du catalogue d'applications multi-piles SAML 2.0.

Groupe d'utilisateurs

L'onglet Groupe d'utilisateurs dans WorkSpaces Applications est une option valide pour de petites démonstrations de concepts. Il est recommandé d'éviter les groupes d'utilisateurs pour tous les cas d'utilisation et toutes les organisations qui utilisent des WorkSpaces applications pour fournir des applications de production.

Il est important de noter à propos des groupes d'utilisateurs que les adresses e-mail des utilisateurs font la distinction entre majuscules et minuscules ; il est donc recommandé de s'assurer que les utilisateurs sont formés à la saisie correcte des informations d'identification des utilisateurs.

URL de diffusion

Pour les déploiements qui appellent des ressources d' WorkSpaces applications à partir d'un service centralisé (généralement des ISV), l'authentification programmatique repose sur le fait qu'une application effectue des appels programmatiques afin de transmettre des informations de manière dynamique et de créer une session d' WorkSpaces applications AWS pour ses utilisateurs. Utilisez la méthode d'authentification API (communément appelée « programmatique ») lorsque vous créez des URL de streaming à l'aide de l'opération CreateStreamingURL. L'utilisateur

qui passe l'`CreateStreamingURL`appel doit utiliser un utilisateur ou un rôle valide autorisé pour`appstream:CreateStreamingURL`.

Lors de la création de la politique d'accès programmatique, il est recommandé de sécuriser l'accès en spécifiant l'ARN exact de la pile d' WorkSpaces applications dans la section Ressources à la place du « * » par défaut. Par exemple :

Example

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appstream:createStreamingURL"
            ],
            "Resource": "arn:aws:appstream:us-east-1:031421429609:stack/
BestPracticesStack"
        }
    ]
}
```

> **Note**
>
> Vous pouvez rapidement récupérer les ARN de vos WorkSpaces applications Stacks à l'aide de l'API Describe Stacks ou de l'AWS CLI.

WorkSpaces Les instances d'applications doivent démarrer en tant qu'instances génériques. Grâce aux informations qui lui sont transmises par l'application, l'instance WorkSpaces Applications établit l'environnement en utilisant le contexte de session pour rendre les choses dynamiques pour l'utilisateur.

Bien que les GPO locaux puissent être utilisés pour spécifier les paramètres lors de la connexion de l'utilisateur, le contexte de session est une bonne pratique lors de l'utilisation `CreateStreamingURL` et de la transmission d'attributs clés tels que l'ID client ou les paramètres de connexion à la base de données, à utiliser dans la session WorkSpaces Applications.

Admissibilité à la demande

WorkSpaces Les applications peuvent créer dynamiquement le catalogue d'applications présenté aux utilisateurs. Les droits des applications sont basés sur les attributs SAML 2.0 ou à l'aide d' WorkSpaces Applications Dynamic Application Framework.

Attribute-based les droits d'application utilisant SAML 2.0 sont recommandés dans la plupart des scénarios. Pour gérer la livraison des packages d'applications, il est recommandé d'utiliser Dynamic Application Framework.

Intégration à Microsoft Active Directory

Les générateurs d'images et les flottes Amazon WorkSpaces Applications peuvent être intégrés à Microsoft Active Directory. Cela vous permet de fournir une méthode centralisée pour l'authentification et l'autorisation des utilisateurs et d'appliquer des politiques de groupe Active Directory aux instances d' WorkSpaces applications jointes à un domaine. L'utilisation de flottes d' WorkSpaces applications associées à un domaine offre les mêmes avantages administratifs qu'un environnement sur site. Cela inclut la gestion centralisée des partages de fichiers réseau, des droits des applications utilisateur, des profils d'itinérance, de l'accès aux imprimantes et d'autres paramètres basés sur des politiques.

Lors de l'intégration d'un environnement d' WorkSpaces applications à Active Directory, il est important de noter que l'authentification initiale auprès de la pile d' WorkSpaces applications est toujours gérée par un SAML2.0 IdP. Une fois que l'utilisateur est authentifié auprès de l'IdP, lorsqu'il lance une session, il doit saisir son mot de passe de domaine ou une authentification par carte à puce pour le domaine Active Directory.

Lors de la conception de l'environnement des services de domaine Active Directory (ADDS) qui sera utilisé avec WorkSpaces les applications, deux options de service et de nombreux scénarios de déploiement sont disponibles. Assurez-vous également que le réseau WorkSpaces des applications est examiné avec le propriétaire de la topologie de votre site Active Directory.

Options de service

Active Directory peut également être déployé à l'aide de AWS Managed Microsoft Active Directory (AD). AWS Managed Microsoft AD est un service entièrement géré qui vous permet d'exécuter Microsoft Active Directory. Microsoft Active Directory peut également être utilisé dans un environnement auto-hébergé, exécuté sur EC2 ou sur site.

Scénarios de déploiement

Les scénarios de déploiement répertoriés ci-dessous sont des options d'intégration couramment utilisées et recommandées pour WorkSpaces les applications avec Microsoft Managed AD ou Active Directory autogéré par un client. Tous les diagrammes d'architecture répertoriés ci-dessous utilisent les constructions principales d'Amazon.

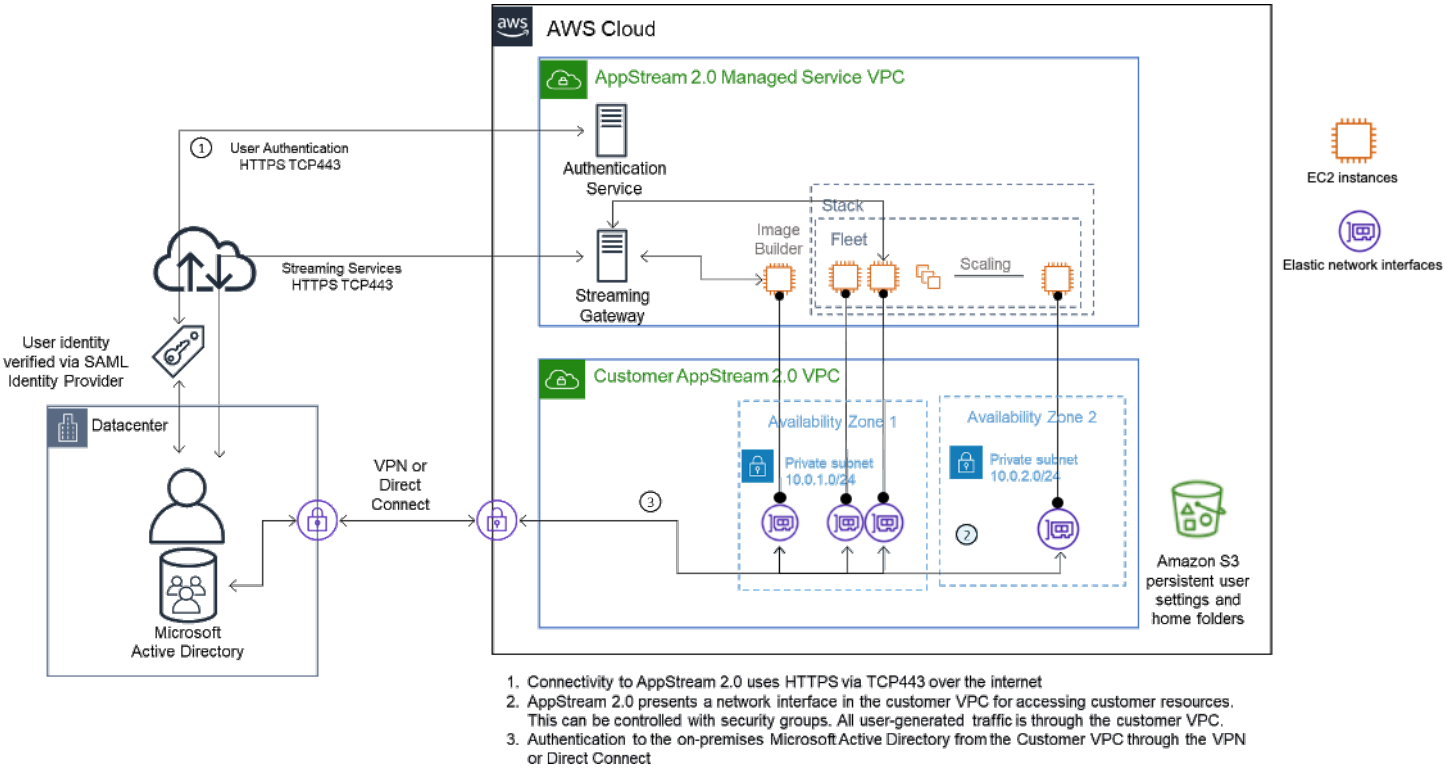
- Amazon Virtual Private Cloud (VPC) — Création d'un Amazon VPC dédié aux services d' WorkSpaces applications avec au moins quatre sous-réseaux privés répartis sur quatre zones

de disponibilité. Deux des sous-réseaux privés sont utilisés pour les flottes d' WorkSpaces applications et les générateurs d'images. Les deux sous-réseaux restants sont utilisés pour les contrôleurs de domaine sur EC2 ou Microsoft Managed AD).

- Ensemble d'options DHCP (Dynamic Host Configuration Protocol) : fournit une norme pour transmettre les informations de configuration au parc d' WorkSpaces applications et aux générateurs d'images qui seront fournis dans le VPC. Le jeu d'options DHCP est défini au niveau du VPC. Il permet aux clients de définir un nom de domaine et des paramètres DNS spécifiques qui seront utilisés avec les WorkSpaces applications instanciées lors de leur mise en service.
- AWS Services d'annuaire — Amazon Microsoft Managed AD peut être déployé sur deux sous-réseaux privés qui seront utilisés conjointement avec les charges de travail WorkSpaces des applications.
- WorkSpaces Flottes d'applications : les flottes WorkSpaces d'applications ou les générateurs d'images sont hébergés dans le AWS VPC géré. Chaque instance WorkSpaces d'applications possède deux interfaces réseau élastiques (ENI). L'interface principale (`eth0`) est utilisée à des fins de gestion et pour négocier la connexion de l'utilisateur final à l'instance via la passerelle de streaming. L'interface secondaire (`eth1`) est injectée dans le VPC client et peut être utilisée pour accéder à d'autres ressources dans le VPC sur mesure ou sur site.

Scénario 1 : services de domaine Active Directory (ADDS) déployés sur site

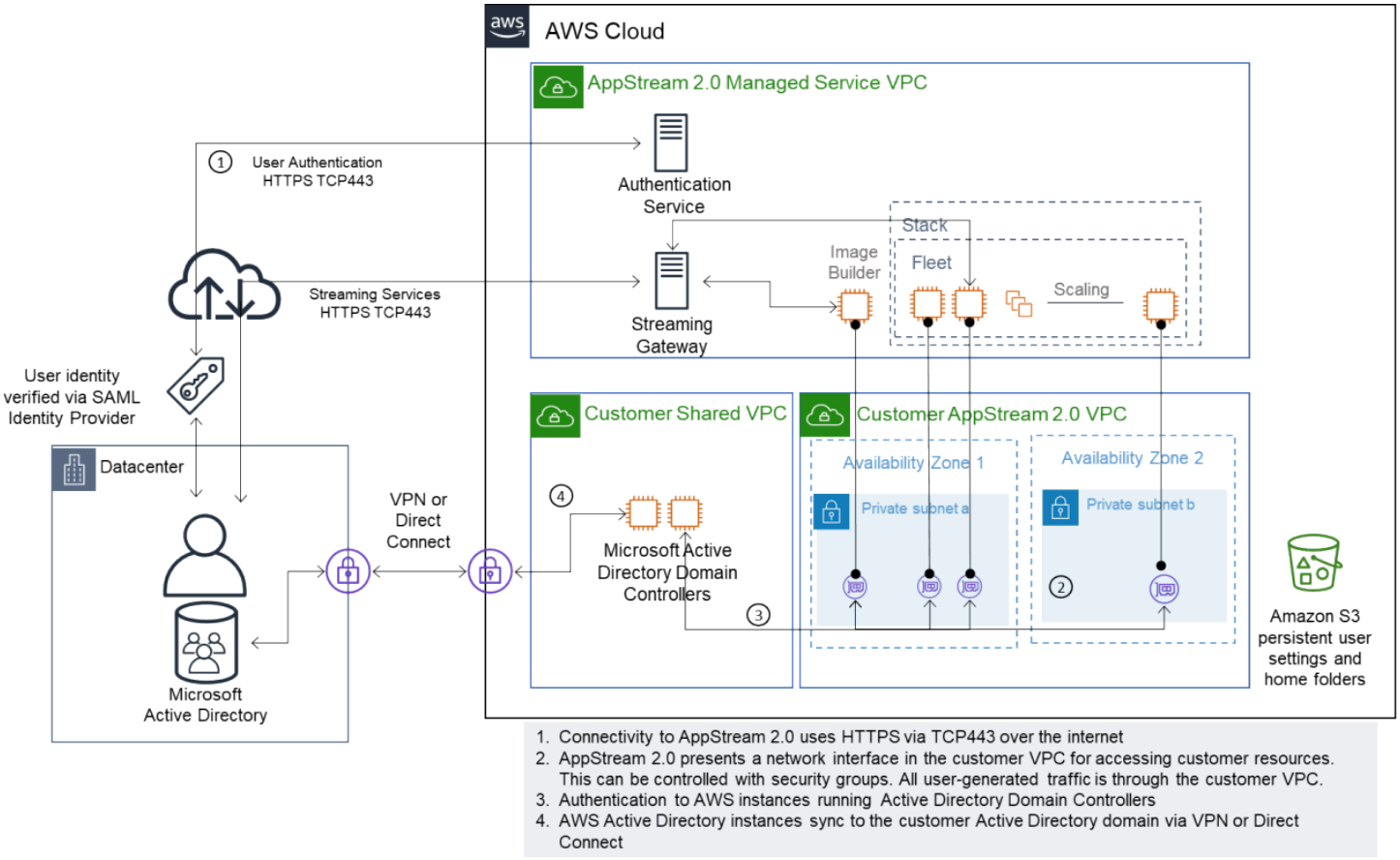
Tout le trafic d'authentification passe par la connexion VPN ou Direct Connect entre le VPC du client et la passerelle client. L'avantage de ce scénario est l'avantage d'utiliser un environnement AD peut-être déjà déployé sans avoir à fournir de contrôleurs de domaine supplémentaires dans le VPC du client. L'inconvénient est la dépendance exclusive au VPN ou à Direct Connect pour authentifier et autoriser les utilisateurs du parc d' WorkSpaces applications. En cas de problème de connectivité réseau, le parc WorkSpaces d'applications ou les constructeurs d'images seront directement affectés. La fourniture de deux tunnels VPN ou de connexions Direct Connect avec des chemins différents atténue ce risque potentiel.



Scénario 1 — Services de domaine Active Directory (ADDS) déployés sur site

Scénario 2 : étendre les services de domaine actifs (ADDS) à AWS VPC client

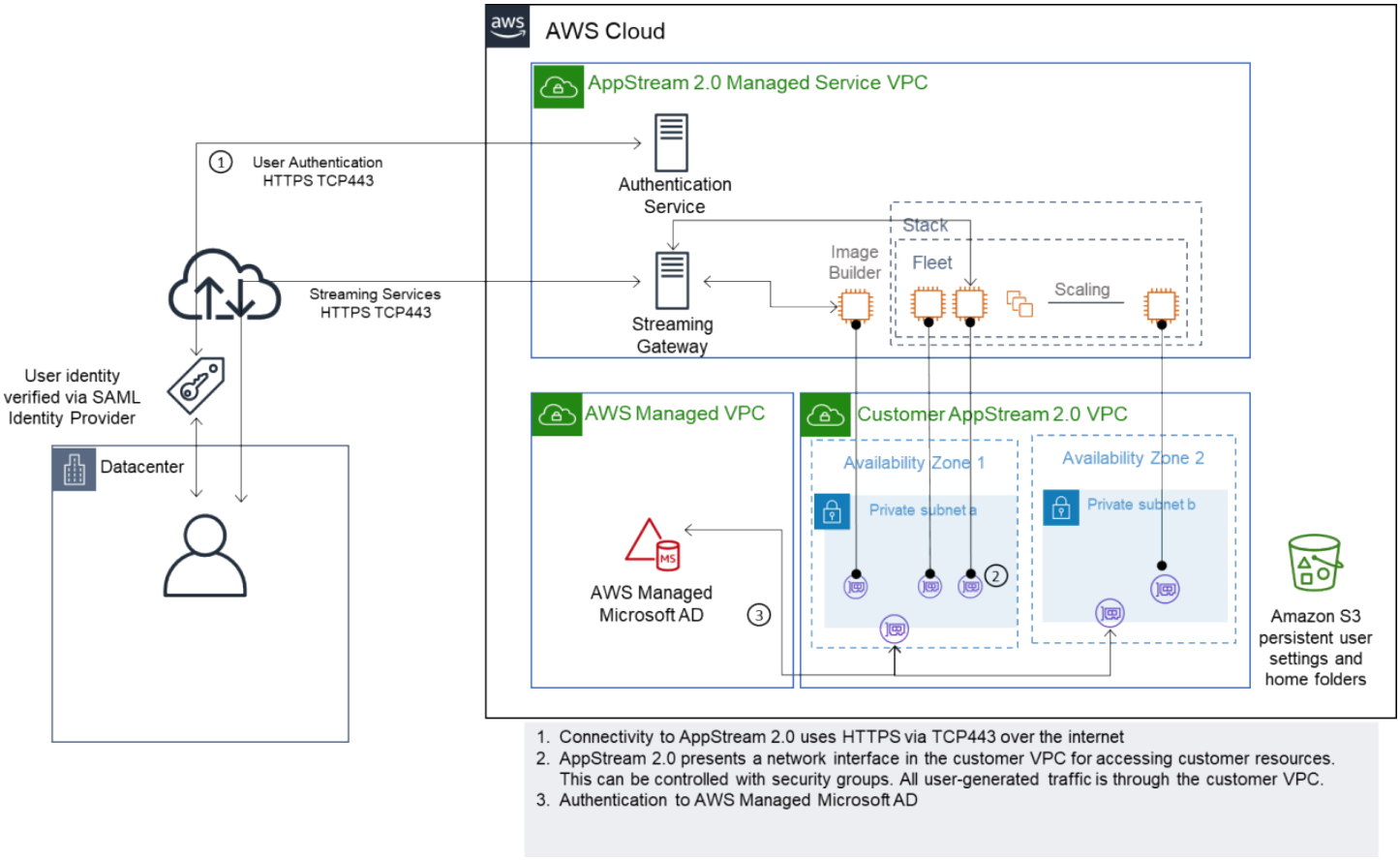
L'Active Directory est étendu au VPC de votre client. Un site Active Directory doit être créé pour les nouveaux contrôleurs de domaine dans le VPC du client. Le trafic d'authentification est acheminé vers les contrôleurs de domaine du VPC du AWS client au lieu de passer par la connexion VPN ou Direct Connect.



Scénario 2 — Étendre les services de domaine actifs au cloud privé virtuel AWS du client

Scénario 3 : AWS Microsoft Active Directory géré

AWS Managed Microsoft AD est déployé dans AWS Cloud et est utilisé comme domaine d'identité et de ressources pour les flottes d' WorkSpaces applications et les générateurs d'images.



Scénario 3 — Active Directory AWS géré

Topologie du site Active Directory Service

La topologie d'un site de service Active Directory est une représentation logique de votre réseau physique.

Une topologie de site vous aide à acheminer efficacement les requêtes des clients et le trafic de réplication Active Directory. Une topologie de site bien conçue et bien entretenue permet à votre organisation de bénéficier des avantages suivants :

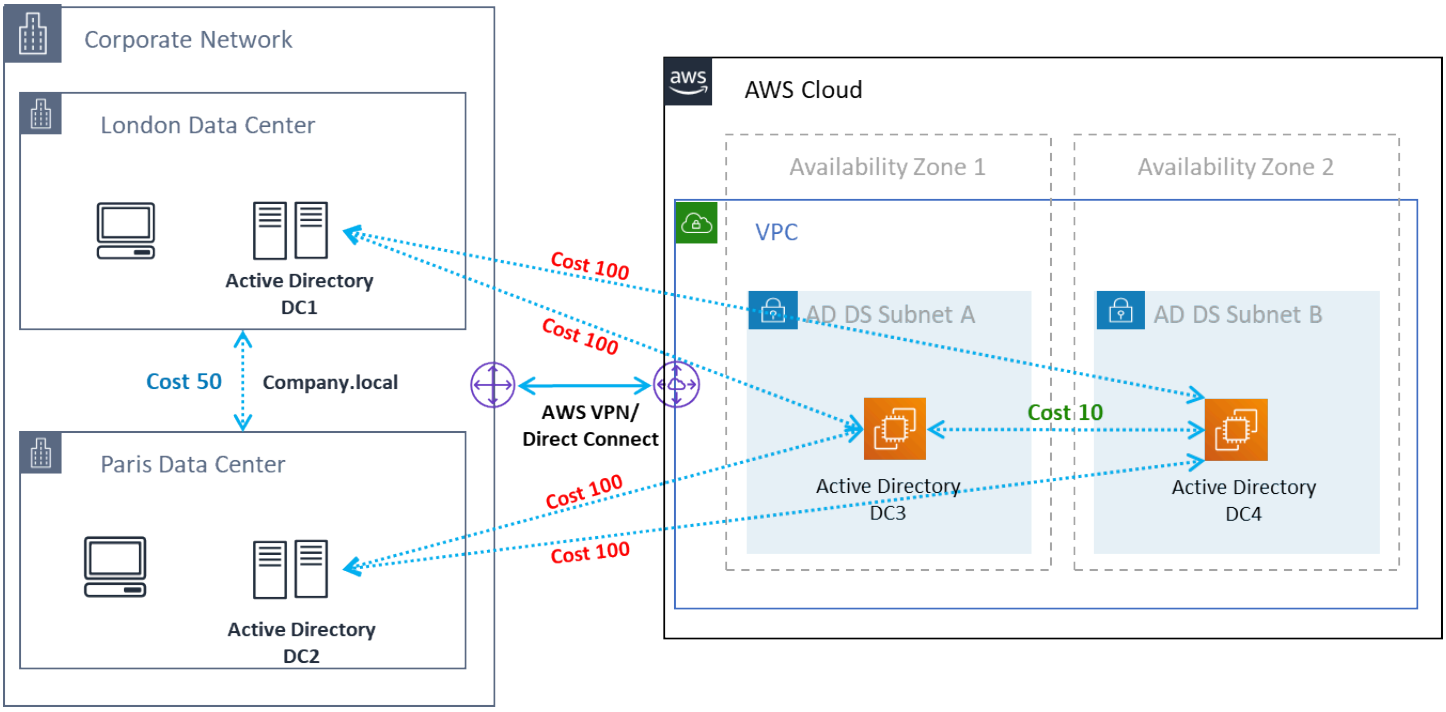
- Minimisez le coût de réplication des données Active Directory lors de la synchronisation entre les données sur site et. AWS Cloud
- Optimisez la capacité des ordinateurs clients à localiser les ressources les plus proches, telles que les contrôleurs de domaine. Cela permet de réduire le trafic réseau sur les liaisons réseau étendues (WAN) lentes, d'améliorer les processus d'ouverture et de fermeture de session et d'accélérer les opérations d'accès aux ressources.

Lorsque vous WorkSpaces introduisez les services Applications, assurez-vous que les plages d'adresses utilisées pour les sous-réseaux des instances d' WorkSpaces applications sont attribuées au site correspondant à votre environnement.

Pour les scénarios 1 et 2, les sites et les services sont des composants essentiels à la meilleure expérience utilisateur en termes de temps de connexion et de temps d'accès aux ressources Active Directory.

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.

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



Sites et services Active Directory : affinité avec les clients

> **Tip**
>
> La meilleure pratique consiste à définir le coût élevé des liens entre les sites AD DS sur site et le cloud AWS. La figure précédente est un exemple des coûts que vous devez attribuer aux liens du site (coût 100) pour garantir une affinité client indépendante du site.

Pour plus d'informations sur la topologie du site, reportez-vous à la section Conception de la topologie du site.

Unités organisationnelles Active Directory

AWS recommande de stocker les unités organisationnelles (UO) configurées dans un seul objet WorkSpaces Applications Directory Config. Il est recommandé que chaque pile d' WorkSpaces applications dispose de sa propre unité d'organisation. Cela vous donne la flexibilité d'avoir des GPO spécifiques par pile. Assurez-vous que les unités d'organisation sont dédiées aux objets informatiques des WorkSpaces applications afin d'éviter de mélanger WorkSpaces Applications-specific les politiques avec les bureaux locaux. Envisagez d'utiliser des sous-unités d'exploitation pour chaque unité dans Région AWS laquelle vous déployez WorkSpaces des applications.

Nettoyage d'objets informatiques Active Directory

WorkSpaces Les instances d'applications sont éphémères. Un parc crée et réutilise des objets informatiques Active Directory au fur et à mesure que les flottes s'agrandissent et s'intensifient.

AWS recommande de créer un processus de nettoyage AD pour supprimer les objets informatiques Active Directory obsolètes qui peuvent exister après la suppression d'un parc d' WorkSpaces applications.

Sécurité

Chez Amazon Web Services (AWS), la sécurité dans le cloud est la priorité principale. La sécurité et la conformité sont une responsabilité partagée entre le client AWS et le client. Pour plus d'informations, reportez-vous au modèle de responsabilité partagée. En tant que client d' AWS and WorkSpaces Applications, il est important de mettre en œuvre des mesures de sécurité sur différentes couches telles que le stack, le parc, l'image et le réseau.

En raison de son caractère éphémère, WorkSpaces les applications sont souvent préférées en tant que solution sécurisée à la livraison d'applications et de postes de travail. Déterminez si les solutions antivirus courantes dans les déploiements Windows sont pertinentes dans vos cas d'utilisation pour un environnement prédéfini et purgé à la fin d'une session utilisateur. L'antivirus alourdit les instances virtualisées, ce qui en fait une bonne pratique pour limiter les activités inutiles. Par exemple, l'analyse du volume système (qui est éphémère) au démarrage n'améliore pas la sécurité globale des WorkSpaces applications.

Les deux questions clés relatives aux WorkSpaces applications de sécurité sont centrées sur :

- La persistance de l'état utilisateur au-delà de la session est-elle une exigence ?
- Quel niveau d'accès doit avoir un utilisateur au cours d'une session ?

Sécurisation des données persistantes

Les déploiements d' WorkSpaces applications peuvent nécessiter la persistance de l'état utilisateur sous une forme ou une autre. Il peut s'agir de conserver des données pour des utilisateurs individuels ou de conserver des données à des fins de collaboration à l'aide d'un dossier partagé. WorkSpaces Le stockage des instances d'applications est éphémère et ne comporte aucune option de chiffrement.

WorkSpaces Les applications assurent la persistance de l'état utilisateur via les dossiers personnels et les paramètres des applications dans Amazon S3. Certains cas d'utilisation nécessitent un meilleur contrôle de la persistance de l'état utilisateur. Dans ces cas d'utilisation, il est AWS recommandé d'utiliser un partage de fichiers SMB (Server Message Block).

État et données de l'utilisateur

Étant donné que la plupart des applications Windows fonctionnent de manière optimale et sécurisée lorsqu'elles sont colocalisées avec des données d'application créées par l'utilisateur, il est

recommandé de conserver ces données au même Région AWS titre que les flottes d' WorkSpaces applications. Le chiffrement de ces données est une bonne pratique. Le comportement par défaut du dossier personnel de l'utilisateur consiste à chiffrer les fichiers et les dossiers au repos à l'aide des clés de S3-managed chiffrement Amazon fournies par les services de gestion des AWS clés (AWS KMS). Il est important de noter que les utilisateurs AWS administratifs ayant accès à la AWS console ou au compartiment Amazon S3 pourront accéder directement à ces fichiers.

Dans les conceptions qui nécessitent une cible SMB (Server Message Block) à partir d'un partage de fichiers Windows pour stocker les fichiers et dossiers utilisateur, le processus est automatique ou nécessite une configuration.

Tableau 5 — Options de sécurisation des données utilisateur

Cible pour les PME	Encryption-at-rest	Encryption-in-transit	Antivirus (antivirus)
FSx for Windows File Server	Automatique via AWS KMS	Chiffrement automatique via le chiffrement des PME	L'AV installé sur une instance distante effectue un scan sur le lecteur mappé
Passerelle de fichiers, AWS Storage Gateway	Par défaut, toutes les données stockées AWS Storage Gateway dans S3 sont chiffrées côté serveur avec Amazon S3-Managed Encryption Keys ()SSE-S3. Vous pouvez éventuellement configurer différents types de passerelles pour chiffrer les données stockées avec AWS Key Management Service (KMS)	Toutes les données transférées entre tout type d'appliance passerelle et le AWS stockage sont cryptées à l'aide du protocole SSL.	L'AV installé sur une instance distante effectue un scan sur le lecteur mappé
EC2-based Serveurs de fichiers Windows	Activer le chiffrement EBS	PowerShell; `Set-SmbServer`	L'AV installé sur le serveur effectue un

Cible pour les PME	Encryption-at-rest	Encryption-in-transit	Antivirus (antivirus)
		`Configuration - EncryptData $True`	scan sur les disques locaux

Sécurité des terminaux et antivirus

La brève nature éphémère des instances Amazon WorkSpaces Applications et le manque de persistance des données obligent à adopter une approche différente pour garantir que l'expérience utilisateur et les performances ne soient pas compromises par des activités qui seraient requises sur un poste de travail persistant. Les agents Endpoint Security sont installés dans WorkSpaces les images des applications lorsqu'il existe une politique organisationnelle ou lorsqu'ils sont utilisés avec une entrée de données externes, par exemple des e-mails, des entrées de fichiers, une navigation Web externe.

Supprimer les identifiants uniques

Les agents Endpoint Security peuvent disposer d'un identifiant global unique (GUID) qui doit être réinitialisé lors du processus de création des instances du parc. Les fournisseurs disposent d'instructions sur l'installation de leurs produits sous forme d'images, qui garantissent la génération d'un nouveau GUID pour chaque instance générée à partir d'une image.

Pour vous assurer que le GUID n'est pas généré, installez l'agent Endpoint Security comme dernière action avant d'exécuter l'assistant WorkSpaces Applications pour générer l'image.

Optimisation des performances

Les fournisseurs de solutions de sécurité des terminaux fournissent des commutateurs et des paramètres qui optimisent les performances des WorkSpaces applications. Les paramètres varient selon les fournisseurs et se trouvent dans leur documentation, généralement dans une section sur le VDI. Certains paramètres courants incluent, sans toutefois s'y limiter, les suivants :

- Désactivez les scans de démarrage pour vous assurer que les temps de création, de démarrage et de connexion des instances sont minimisés
- Désactiver les scans programmés pour éviter les scans inutiles
- Désactiver les caches de signatures pour empêcher l'énumération des fichiers
- Activer les paramètres d'E/S optimisés pour le VDI

- Exclusions requises par les applications pour garantir les performances

Les fournisseurs de solutions de sécurité des terminaux fournissent des instructions d'utilisation avec des environnements de bureau virtuels qui optimisent les performances.

- Support de numérisation Trend Micro Office pour l'infrastructure de bureau virtuel - Apex One/ OfficeScan (trendmicro.com)
- CrowdStrike et comment installer le CrowdStrike Falçon dans le centre de données
- Sophos et Sophos Central Endpoint : comment effectuer une installation sur une image dorée pour éviter les doublons d'identité et Sophos Central : meilleures pratiques lors de l'installation de points de terminaison Windows dans des environnements de bureau virtuels
- McAfee et le provisionnement et le déploiement d'McAfee agents sur les systèmes d'infrastructure de bureau virtuel
- Microsoft Endpoint Security et configuration de l'antivirus Microsoft Defender pour les machines VDI non persistantes - Microsoft Tech Community

Exclusions de numérisation

Si un logiciel de sécurité est installé dans WorkSpaces les instances d'applications, il ne doit pas interférer avec les processus suivants.

Tableau 6 — Processus WorkSpaces des applications Les logiciels de sécurité ne doivent pas interférer avec les processus suivants.

Service	Processus
AmazonCloudWatchAgent	« C:\Program Files \ Amazon \ AmazonClo udWatchAgent \ start-amazon- cloudwatch-agent.exe »
AmazonssMagent	« C:\Program Files \ Amazon \ SSM \ amazon-ssm-agent.exe »
NICE DCV	« C:\Program Files \ NICE \ DCV \ Server \ bin \ dcvserver.exe » "C:\Program Files \ NICE \ DCV \ Server \ bin \ dcvagent.exe »

Service	Processus
WorkSpaces Applications	« C : \ ProgramFiles \ Amazon \ AppStream 2 \ StorageConnector \ StorageConnector.exe » Dans le dossier « C:\Program Files \ Amazon \ Photon \ » «. \ Agent \ PhotonAgent.exe » «. \ Agent \ s5cmd.exe » ".\WebServer\PhotonAgentWebServer.exe" ".\CustomShell\PhotonWindowsAppSwitcher.exe" ".\CustomShell\PhotonWindowsCustomShell.exe" ".\CustomShell\PhotonWindowsCustomShellBackground.exe"

Dossiers

Si un logiciel de sécurité est installé dans WorkSpaces les instances d'applications, il ne doit pas interférer avec les dossiers suivants :

Example

```
C:\Program Files\Amazon\*
C:\ProgramData\Amazon\*
C:\Program Files (x86)\AWS Tools\*
C:\Program Files (x86)\AWS SDK for .NET\*
C:\Program Files\NICE\*
C:\ProgramData\NICE\*
C:\AppStream\*
C:\Program Files\Internet Explorer\*
C:\Program Files\nodejs\
```

Hygiène des consoles de sécurité des terminaux

Amazon WorkSpaces Applications créera de nouvelles instances uniques chaque fois qu'un utilisateur se connecte au-delà des délais d'inactivité et de déconnexion. Les instances porteront un nom unique et s'accumuleront dans les consoles de gestion de la sécurité des terminaux. Le fait de configurer la suppression des machines anciennes et inutilisées âgées de plus de 4 jours (ou moins selon les délais d'expiration des sessions des WorkSpaces applications) réduira le nombre d'instances expirées dans la console.

Exclusions de réseau

La plage du réseau de gestion des WorkSpaces applications (`198.19.0.0/16`) et les ports et adresses suivants ne doivent être bloqués par aucune solution de sécurité/pare-feu ou antivirus au sein des instances d' WorkSpaces applications.

Tableau 7 — Ports dans les instances de streaming WorkSpaces des applications, les logiciels de sécurité ne doivent pas interférer avec

Port	Utilisation
8300, 3128	Ceci est utilisé pour établir la connexion de streaming
8000	Ceci est utilisé pour gérer l'instance de streaming par WorkSpaces Applications
8443	Ceci est utilisé pour gérer l'instance de streaming par WorkSpaces Applications
53	DNS

Tableau 8 — Adresses des services gérés des WorkSpaces applications avec lesquelles les logiciels de sécurité ne doivent pas interférer

Port	Utilisation
169,254,169,123	NTP
169,254,169,249	Service de licence NVIDIA GRID
169,254,169,250	KMS
169,254,169,251	KMS
169,254,169,253	DNS
169,254,169,254	Métadonnées

Sécurisation d'une session WorkSpaces d'applications

Limiter les contrôles des applications et du système d'exploitation

WorkSpaces Les applications permettent à l'administrateur de spécifier exactement quelles applications peuvent être lancées à partir de la page Web en mode streaming d'applications. Cela ne garantit toutefois pas que seules les applications spécifiées peuvent être exécutées.

Les utilitaires et applications Windows peuvent être lancés via le système d'exploitation par des moyens supplémentaires. AWS recommande d'utiliser Microsoft AppLocker pour s'assurer que seules les applications dont votre organisation a besoin peuvent être exécutées. Les règles par défaut doivent être modifiées, car elles accordent à tous l'accès aux chemins d'accès aux répertoires critiques du système.

> **Note**
>
> Windows Server 2016 et 2019 nécessitent l'exécution du service Windows Application Identity pour appliquer AppLocker les règles. L'accès aux WorkSpaces applications depuis Applications utilisant Microsoft AppLocker est détaillé dans le Guide d'administration WorkSpaces des applications.

Pour les instances de flotte associées à un domaine Active Directory, utilisez des objets de stratégie de groupe (GPO) pour fournir des paramètres utilisateur et système afin de sécuriser l'accès des utilisateurs aux applications et aux ressources.

Pare-feu et routage

Lors de la création d'un parc d' WorkSpaces applications, des sous-réseaux et un groupe de sécurité doivent être attribués. Des listes de contrôle d'accès réseau (NACL) et des tables de routage sont déjà attribuées aux sous-réseaux. Vous pouvez associer jusqu'à cinq groupes de sécurité lors du lancement d'un nouveau générateur d'images ou lors de la création d'une nouvelle flotte. Les groupes de sécurité peuvent avoir jusqu'à cinq attributions à partir des groupes de sécurité existants. Pour chaque groupe de sécurité, vous ajoutez des règles qui contrôlent le trafic réseau sortant et entrant depuis et vers vos instances

Une NACL est une couche de sécurité optionnelle pour votre VPC qui agit comme un pare-feu sans état pour contrôler le trafic entrant et sortant d'un ou de plusieurs sous-réseaux. Vous pouvez définir des listes ACL réseau à l'aide de règles similaires à vos groupes de sécurité afin d'ajouter une couche de sécurité supplémentaire à votre VPC. Pour plus d'informations sur les différences entre les groupes de sécurité et les ACL réseau, consultez la page de comparaison des groupes de sécurité et des NACL.

Lors de la conception et de l'application des règles du groupe de sécurité et de la NACL, tenez compte des Well-Architected meilleures pratiques d'AWS en matière de privilège minimal. Le principe du moindre privilège consiste à n'accorder que les autorisations nécessaires à l'exécution d'une tâche.

Pour les clients disposant d'un réseau privé haut débit connectant leur environnement sur site à AWS (via AWS Direct Connect), vous pouvez envisager d'utiliser les points de terminaison VPC pour les WorkSpaces applications, ce qui signifie que le trafic de streaming sera acheminé via la connectivité de votre réseau privé plutôt que via l'Internet public. Pour plus d'informations sur ce sujet, consultez la section Point de terminaison VPC de l'interface de streaming d' WorkSpaces applications de ce document.

Prévention des pertes de données

Nous examinerons deux types de prévention des pertes de données.

Contrôles de transfert de données entre le client et l'instance d' WorkSpaces applications

Tableau 9 — Conseils pour contrôler l'entrée et la sortie des données

Réglage	Options	Conseils
Presse-papiers	• Copier et coller sur une session à distance uniquement • Copier uniquement sur un appareil local • Désactivé	La désactivation de ce paramètre ne désactive pas le copier-coller dans la session. S'il est nécessaire de copier des données dans la session, choisissez Coller uniquement dans une session distante afin de minimiser le risque de fuite de données.
Transfert de fichiers	• Charger et télécharger • Upload uniquement • Téléchargement uniquement • Désactivé	Évitez d'activer ce paramètre pour éviter les fuites de données.
Imprimer sur un appareil local	• Activé • Désactivé	Si l'impression est requise, utilisez des imprimantes mappées en réseau contrôlées et surveillées par votre organisation.

Tenez compte des avantages de la solution de transfert de données organisationnelle existante par rapport aux paramètres de la pile. Ces configurations ne sont pas conçues pour remplacer une solution complète de transfert de données sécurisé.

Contrôle du trafic sortant de l'instance d' WorkSpaces applications

Lorsque la perte de données est préoccupante, il est important de couvrir les accès auxquels un utilisateur peut accéder une fois qu'il est dans son instance d' WorkSpaces applications. À quoi ressemble le chemin de sortie (ou de sortie) du réseau ? Il est courant que l'utilisateur final dispose d'un accès Internet public au sein de son instance d' WorkSpaces applications. Il convient donc d'envisager de placer une solution de filtrage de contenu WebProxy ou une solution de filtrage de contenu sur le chemin réseau. Les autres considérations incluent une application antivirus locale et

d'autres mesures de sécurité des terminaux au sein de l'instance WorkSpaces Applications (voir la section « Sécurité des terminaux et antivirus » pour plus d'informations).

Utilisation AWS services

Gestion des identités et des accès AWS

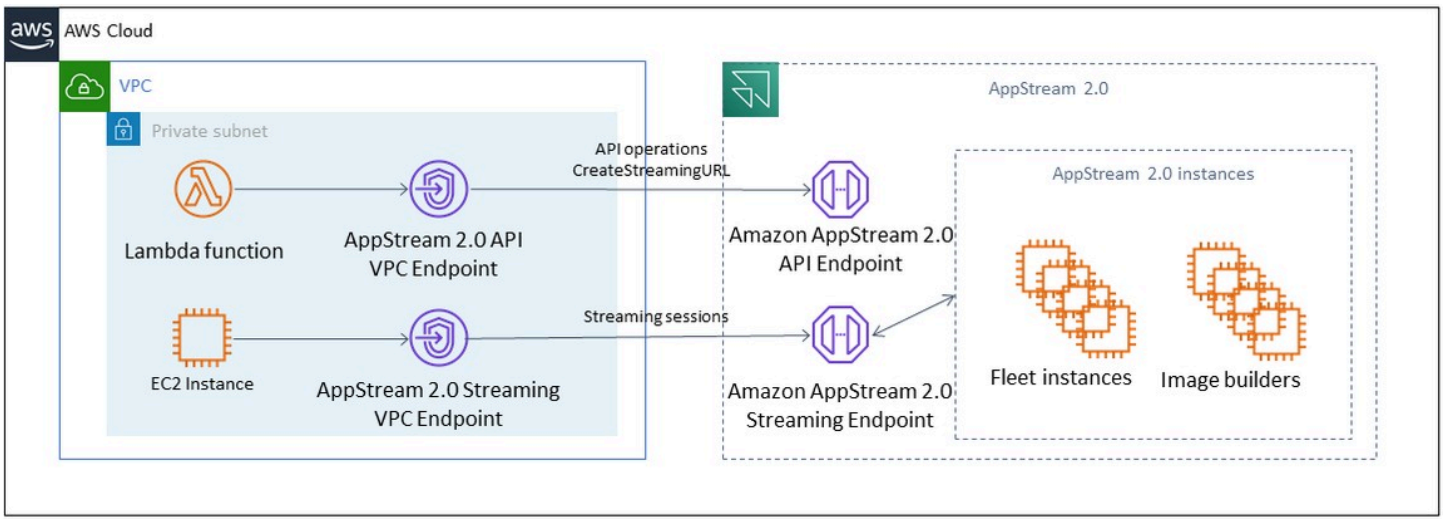
L'utilisation d'un rôle IAM pour accéder aux AWS services, et le fait d'être spécifique dans la politique IAM qui y est associée, est une bonne pratique qui garantit que seuls les utilisateurs des sessions WorkSpaces Applications y ont accès sans gérer d'informations d'identification supplémentaires. Suivez les meilleures pratiques relatives à l'utilisation des rôles IAM avec les WorkSpaces applications.

Créez des politiques IAM pour protéger les compartiments Amazon S3 créés pour conserver les données utilisateur à la fois dans les dossiers personnels et dans les paramètres des applications. Cela empêche l'accès des administrateurs autres que les administrateurs d'WorkSpaces applications.

Points de terminaison d’un VPC

Un point de terminaison VPC permet des connexions privées entre votre VPC et les services pris en charge et les services AWS de point de terminaison VPC alimentés par. AWS PrivateLink AWS PrivateLink est une technologie qui vous permet d'accéder à des services de manière privée en utilisant des adresses IP privées. Le trafic entre votre VPC et les autres services ne quitte pas le réseau Amazon. Si l'accès public à Internet n'est requis que pour les AWS services, les points de terminaison VPC suppriment complètement le besoin de passerelles NAT et de passerelles Internet.

Dans les environnements où les routines d'automatisation ou les développeurs nécessitent d'effectuer des appels d'API pour les WorkSpaces applications, créez un point de terminaison VPC d'interface pour les opérations de l'API WorkSpaces des applications. Par exemple, s'il existe des instances EC2 dans des sous-réseaux privés sans accès public à Internet, un point de terminaison VPC pour l'API WorkSpaces Applications peut être utilisé pour appeler des opérations d'API d' WorkSpaces applications telles que l'URL. CreateStreaming Le schéma suivant montre un exemple de configuration dans lequel l'API d' WorkSpaces applications et les points de terminaison VPC de streaming sont utilisés par des fonctions Lambda et des instances EC2.



Point de terminaison d'un VPC

Le point de terminaison VPC de streaming vous permet de diffuser des sessions via un point de terminaison VPC. Le point de terminaison de l'interface de streaming gère le trafic de streaming au sein de votre VPC. Le trafic de streaming inclut les pixels, l'USB, l'entrée utilisateur, l'audio, le presse-papiers, le chargement et le téléchargement de fichiers et le trafic d'imprimante. Pour utiliser le point de terminaison VPC, le paramètre du point de terminaison VPC doit être activé dans la pile Applications. WorkSpaces Cela constitue une alternative à la diffusion en continu de sessions utilisateur sur Internet public à partir de sites disposant d'un accès limité à Internet et qui bénéficieraient d'un accès via une instance Direct Connect. Le streaming de sessions utilisateur via un point de terminaison VPC nécessite les éléments suivants :

- Les groupes de sécurité associés au point de terminaison de l'interface doivent autoriser l'accès entrant aux ports (TCP) et aux ports `443` `1400-1499` (TCP) à partir de la plage d'adresses IP à partir de laquelle vos utilisateurs se connectent.
- La liste de contrôle d'accès réseau pour les sous-réseaux doit autoriser le trafic sortant des ports réseau éphémères `1024-65535` (TCP) vers la plage d'adresses IP à partir de laquelle vos utilisateurs se connectent.
- La connectivité Internet est nécessaire pour authentifier les utilisateurs et fournir les ressources Web dont WorkSpaces les applications ont besoin pour fonctionner.

Pour en savoir plus sur la restriction du trafic aux AWS services dotés d' WorkSpaces applications, consultez le guide d'administration pour la création et le streaming à partir de points de terminaison VPC.

Lorsqu'un accès public complet à Internet est requis, il est recommandé de désactiver la configuration de sécurité renforcée (ESC) d'Internet Explorer sur Image Builder. Pour plus d'informations, consultez le guide WorkSpaces d'administration des applications pour désactiver la configuration de sécurité renforcée d'Internet Explorer.

Reprise après sinistre

Amazon AppStream 2.0 a intégré la redondance dans un maximum de trois zones de disponibilité. Cela signifie que si un utilisateur dispose d'une session active dans une zone de disponibilité dégradée, il peut simplement se déconnecter et se reconnecter, ce qui lui réservera une session dans une zone de disponibilité saine en supposant que vous en ayez la capacité. Bien que cela assure une haute disponibilité au sein de la région, cela ne constitue pas une solution de reprise après sinistre si le service rencontre des problèmes au niveau régional.

Pour fournir un plan de reprise après sinistre aux utilisateurs de vos WorkSpaces applications, vous devez d'abord créer un environnement d' WorkSpaces applications dans votre région secondaire. Du point de vue de la conception, cet environnement doit disposer de connexions redondantes avec votre environnement sur site, le cas échéant, et ne doit pas dépendre de la région principale. Par exemple, si votre parc d' WorkSpaces applications est joint à un domaine, vous devez disposer de contrôleurs de domaine supplémentaires dans la région secondaire avec des sites et des services configurés. Du point de vue WorkSpaces des applications, cet environnement doit comporter les mêmes paramètres de flotte et de stack que ceux que vous avez dans votre région principale. La flotte elle-même doit exécuter votre même image de base, qui peut être copiée dans votre région secondaire via la console ou par programmation. Si les applications qui s'exécutent dans le cadre de vos sessions WorkSpaces Applications ont une dépendance dorsale liée à votre région principale, celle-ci doit également bénéficier d'une redondance régionale afin de garantir que les utilisateurs puissent toujours accéder au backend de l'application en cas de panne de la région principale. Vos limites de niveau de service dans votre région de destination doivent correspondre à celles de votre région principale.

Routage des identités

Il existe deux méthodes distinctes pour fournir l'accès aux applications dans un scénario de reprise après sinistre. À un niveau élevé, les deux méthodes diffèrent selon la manière dont les utilisateurs sont dirigés vers la région de basculement. La première méthode est exécutée avec une seule configuration d'application WorkSpaces Applications dans votre IdP et la seconde méthode consiste à avoir deux configurations d'application distinctes.

Méthode 1 : modification de l'état du relais de votre application

Lorsque les utilisateurs se connectent aux WorkSpaces applications depuis un fournisseur d'identité (IdP), après leur authentification, ils sont redirigés vers une URL spécifique qui correspond à la région

et à la pile auxquelles ils sont censés avoir accès. Pour plus d'informations sur l'URL de l'état du relais, consultez le guide d'administration WorkSpaces des applications Amazon. L'administrateur peut configurer une pile interrégionale basée sur la même image d' WorkSpaces applications que la région principale vers laquelle les utilisateurs peuvent basculer. L'administrateur peut contrôler ce basculement en mettant simplement à jour l'URL de l'état du relais pour qu'elle pointe vers la pile de basculement. Pour que cette méthode fonctionne correctement, les politiques IAM associées devront refléter l'accès aux deux piles : primaire et basculement. Pour plus de détails sur la façon dont ces politiques IAM doivent être configurées, consultez l'exemple de stratégie suivant.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "appstream:Stream",
            "Resource": [
                "arn:aws:appstream:us-east-1:190836837966:stack/StackName",
                "arn:aws:appstream:us-east-1:190836837966:stack/StackName"
            ],
            "Condition": {
                "StringEquals": {
                    "appstream:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

Méthode 2 : Configuration de deux WorkSpaces applications au sein de votre IdP

Cette méthode nécessite que l'administrateur crée deux applications distinctes pour les WorkSpaces applications au sein de l'IdP. Ils peuvent ensuite soit présenter les deux applications et laisser l'utilisateur choisir où aller, soit lock/hide une application jusqu'au moment du basculement. Cette méthode est mieux adaptée au cas d'utilisation consistant à avoir des utilisateurs internationaux qui se déplacent souvent. Ces utilisateurs doivent diffuser depuis le point de terminaison le

plus proche. Le fait d'avoir les deux applications assignées leur donne la possibilité de choisir l'application configurée pour la région la plus proche. Cela peut également être automatisé. Pour plus d'informations, consultez ce billet de blog.

Persistance du stockage

Lorsque vous utilisez les fonctionnalités de persistance des données incluses dans WorkSpaces les applications, telles que la persistance des applications et la synchronisation du dossier de base, vous devez répliquer ces données dans votre zone de basculement. Ces fonctionnalités stockent les données persistantes dans un compartiment Amazon S3 dans la région WorkSpaces Applications donnée. Pour que les données soient conservées d'une région à l'autre, vous devez répliquer toutes les modifications apportées au bucket source vers le bucket WorkSpaces Applications de la région de basculement. Cela peut être fait avec les fonctionnalités natives d'Amazon S3, telles que la réplication entre régions d'Amazon S3. Les données persistantes de chaque utilisateur résideront dans un dossier contenant son nom d'utilisateur haché. Étant donné que le nom d'utilisateur sera haché dans la même région, le simple fait de répliquer les données assurera la persistance des données dans votre région secondaire. Pour plus d'informations sur les compartiments Amazon S3 utilisés par WorkSpaces les applications, consultez ce guide.

Contrôle

Utilisation des tableaux de bord

La surveillance de l'utilisation de la flotte est une activité régulière qui peut être effectuée au moyen de CloudWatch métriques et de la création d'un tableau de bord. Vous pouvez également utiliser l'onglet Utilisation du parc depuis la console WorkSpaces Applications. Surveillez régulièrement l'utilisation de votre flotte, car le comportement des utilisateurs n'est pas toujours prévisible et la demande peut même dépasser une planification initiale de premier ordre. Une liste complète des métriques et des dimensions des WorkSpaces applications se CloudWatch trouve dans le guide d'administration WorkSpaces des applications sous Surveillance des ressources.

Anticiper la croissance

Chaque fois qu'il y a un saut important`PendingCapacity`, un événement de mise à l'échelle automatique se produit. Il est important de le confirmer `AvailableCapacity` et d'`PendingCapacity`avoir une relation inverse lorsque de nouvelles instances du parc d' WorkSpaces applications deviennent disponibles pour héberger des sessions utilisateur. Créez une CloudWatch alarme `InsufficientCapacityError` pour chaque parc d' WorkSpaces applications afin d'avertir les administrateurs afin de garantir que le dimensionnement automatique ne soit pas inférieur à la demande.

Si la demande dépasse la capacité et que les valeurs `InsufficientCapacityError` métriques sont courantes, envisagez d'augmenter la capacité minimale par le biais d'une politique de dimensionnement planifié pour le début de la journée de travail. En outre, adoptez une deuxième politique de dimensionnement planifié afin de réduire la capacité minimale une fois la demande satisfaite. N'oubliez pas que la réduction de la valeur de la capacité minimale n'a aucune incidence sur les sessions existantes. La réduction de la capacité minimale avant la fin de la journée de travail permet efficacement à l'échelle de fonctionner comme prévu en abaissant la valeur de`ActualCapacity`. Cela permet d'optimiser les coûts.

Si la demande est constamment imprévisible, utilisez la politique de dimensionnement de Target Tracking pour vous assurer que le parc d' WorkSpaces applications est suffisant `AvailableCapacity` pour répondre à la demande tout en déterminant les modèles d'utilisation. Continuez à surveiller car Target Tracking utilise un pourcentage de la consommation du parc. À mesure que le nombre total d'instances de flotte augmente, le nombre total d'instances de flotte

inutilisées se multiplie. Cela peut devenir un gaspillage à moins que la capacité maximale ne soit fixée à une valeur prudente. Utilisez plusieurs types de politiques de dimensionnement (par exemple, le suivi planifié et le suivi des cibles) pour trouver un équilibre entre fiabilité et optimisation des coûts.

Surveillance de l'utilisation par les utilisateurs

Surveillance des utilisateurs uniques, car cela entraîne un coût sous forme de frais d'utilisation. Ces frais d'utilisation sont dus aux licences d'accès aux abonnés (SAL) d'Image Assistant (RDS). L'évaluation des utilisateurs uniques peut être effectuée soit par le biais de rapports provenant de l'IdP où l'authentification est effectuée, soit par le biais de rapports d'utilisation.

Les rapports d'utilisation sont stockés sous forme de `.csv` fichiers séparés dans votre compartiment S3, que vous pouvez télécharger et analyser à l'aide d'outils de business intelligence (BI) tiers. Vous pouvez analyser vos données d'utilisation AWS sans télécharger vos rapports ou créer des rapports sur des plages de dates personnalisées sans concaténer plusieurs fichiers. `.csv` Par exemple, vous pouvez utiliser Amazon Athena et Amazon Quick pour créer des rapports personnalisés et des visualisations des données d'utilisation de vos WorkSpaces applications.

Journaux d'événements persistants des applications et Windows

Lorsqu'une session d'instance d' WorkSpaces applications est terminée, l'instance est terminée. Cela signifie que tous les journaux d'événements d'applications et de Windows utilisés pendant la session sont perdus. S'il est nécessaire de conserver ces journaux d'événements d'applications et de Windows, l'une des méthodes consiste à utiliser Amazon Data Firehose pour les transmettre en temps réel à S3 et à effectuer une recherche avec Amazon OpenSearch Service (OpenSearch Service). Si les requêtes ne sont pas susceptibles d'être fréquentes, pour optimiser les coûts, utilisez Amazon Athena pour effectuer des recherches plutôt que d'exécuter Amazon OpenSearch Service.

Réseau d'audit et activité administrative

Si ce n'est pas déjà fait, il est recommandé AWS CloudTrailde le configurer Compte AWS avec Amazon WorkSpaces Applications. Pour auditer spécifiquement les appels d'API d' WorkSpaces applications, utilisez la source d'événements du filtre avec une valeur de`appstream.amazonaws.com`.

Activez les journaux de flux VPC pour auditer l'accès aux ressources gérées par le client. Les journaux de flux VPC peuvent être publiés dans CloudWatch Logs pour effectuer des requêtes lorsqu'un audit est requis.

La surveillance de l'allocation des adresses IP des sous-réseaux est importante à mesure que WorkSpaces les flottes d'applications augmentent. Créez un rapport sur l'attribution des adresses IP en exécutant la CLI describe-subnets pour signaler les adresses IP disponibles dans chaque sous-réseau attribué aux flottes. Assurez-vous que votre entreprise dispose d'une capacité d'adresses IP suffisante pour répondre à la demande de toutes les flottes fonctionnant à pleine capacité.

Optimisation des coûts

L'optimisation des coûts vise à éviter les coûts inutiles. Les sujets clés incluent la compréhension et le contrôle de l'utilisation de l'argent, ainsi que le choix du nombre de types de ressources le plus approprié et le plus correct. Analysez les dépenses au fil du temps et adaptez-les aux besoins de l'entreprise. Les ressources d' WorkSpaces applications suivantes entraînent des frais de paiement à l'utilisation :

- Always-On instances de flotte
- On-Demand instances de flotte
- On-Demand frais d'instance interrompus
- Instances Image Builder
- Frais d'utilisation

Pour obtenir les informations tarifaires actuelles, consultez le AWS site Web pour connaître les tarifs WorkSpaces d'Amazon Applications.

Conception de déploiements WorkSpaces d'applications rentables

La première étape de la planification et de la conception du déploiement des WorkSpaces applications consiste à utiliser un outil de tarification simple pour estimer la base de référence de vos AWS frais liés à votre utilisation. Indiquez le nombre total d'utilisateurs, l'utilisation simultanée réelle par heure, le type d'instance et l'utilisation du parc, et l'outil de tarification estime votre prix par utilisateur. Il indique également les économies de prix estimées lorsque vous utilisez une On-Demand flotte au lieu d'une Always-On flotte.

Les clients apprécient le modèle de tarification des WorkSpaces applications qui consiste à ne payer que pour les instances qu'elles fournissent pour répondre aux besoins de streaming de leurs utilisateurs. Ce modèle est différent de leurs environnements de streaming d'applications existants. Ils sont généralement basés sur le provisionnement en cas de pic de capacité, même pendant les nuits, les week-ends et les jours fériés, lorsque la charge est plus faible. L'outil de tarification Amazon AppStream 2.0 fournit uniquement une estimation de vos frais AWS liés à votre utilisation des WorkSpaces applications, et n'inclut aucune taxe susceptible de s'appliquer. Vos frais réels dépendent de divers facteurs, notamment de votre utilisation réelle des services AWS.

L'outil de tarification des WorkSpaces applications est fourni sous forme de feuille de calcul Microsoft Excel ou OpenOffice Calc qui vous permet de saisir des informations de base sur votre parc, puis

fournit une estimation des coûts pour l'environnement des WorkSpaces applications pour les flottes à la demande et en permanence en fonction de vos habitudes d'utilisation. Vous pouvez simuler les coûts en fonction des tendances d'utilisation historiques ou prévues. Les flottes élastiques évitent à l'administrateur de prévoir l'utilisation, de créer et de gérer des politiques de dimensionnement et des images grâce à l'intégration de ces fonctionnalités. Les flottes élastiques et les instances fonctionnant sous Amazon Linux 2 (tous les types de flotte) sont facturées pour la durée de la session de streaming, en secondes, avec un minimum de 15 minutes.

Optimisation des coûts grâce au choix du type d'instance

Pour les instances de fleet et de générateur d'images, vous pouvez choisir une gamme de familles et de types d'instances différents pour votre application.

Tests auprès des utilisateurs finaux : l'étape suivante consiste à déployer le parc d' WorkSpaces applications auprès d'un groupe d'utilisateurs pilotes afin de les tester afin de valider notre choix de type d'instance. Il est important de demander aux utilisateurs pilotes de tester tous leurs flux de travail réguliers et intensifs afin de capturer des mesures relatives à la mémoire, au processeur et aux graphiques afin que vous puissiez capturer des indicateurs de performance de base. Le groupe pilote doit contenir les différents rôles d'utilisateur qui utilisent l'application afin de garantir que vous la testez à partir de plusieurs expériences utilisateur. Les tests d'acceptation par les utilisateurs vous permettent de recueillir des commentaires sur l'expérience des sessions de streaming. Lors de la création ou de la mise à jour d'une pile, il est possible d'utiliser une URL de commentaires personnalisée. Les utilisateurs sont redirigés vers cette URL après avoir cliqué sur le lien Envoyer des commentaires pour envoyer des commentaires sur leur expérience de streaming d'applications. En cas de problème de performance, utilisez les indicateurs de performance de Windows pour analyser les contraintes en matière de ressources. Par exemple, si le type d'instance de flotte actuel stream.standard.medium affiche une contrainte de ressources, mettez-le à niveau vers stream.standard.large. À l'inverse, si les indicateurs de performance indiquent des niveaux élevés de sous-utilisation des ressources, envisagez de rétrograder le type d'instance.

Optimisation des coûts grâce au choix du type de flotte

Lors de la création d'un nouveau parc d' WorkSpaces applications, les développeurs doivent choisir un type de flotte Always- On ou un type de On-Demand flotte. Lors du choix du type d'instance du point de vue de la tarification, il est important de comprendre comment WorkSpaces Applications gère les instances de flotte. Pour les Always-On flottes, les instances de flotte restent en état de fonctionnement. Par conséquent, lorsque les utilisateurs essaient de diffuser des sessions, les instances de flotte sont toujours prêtes à démarrer des sessions de streaming.

Pour les On-Demand flottes, une fois les instances de flotte lancées, elles sont maintenues à l'état arrêté. Les frais d'instance interrompus sont inférieurs aux frais d'instance de fonctionnement, ce qui peut contribuer à réduire les coûts. Les instances On-Demand de flotte doivent être démarrées à partir d'un état arrêté. Un utilisateur doit attendre environ deux minutes pour que sa session de streaming soit disponible.

Les flottes élastiques sont de bons candidats pour les applications autonomes qui peuvent être installées sur des disques durs virtuels enregistrés dans un bucket Amazon Simple Storage Service (Amazon S3). Les flottes élastiques peuvent encore réduire les coûts dans certains cas d'utilisation en raison de la facturation à la seconde facturée uniquement pour la durée du streaming. Le taux dépend du type et de la taille de l'instance ainsi que du système d'exploitation que vous choisissez lors de la création du parc.

Si les utilisateurs finaux ont besoin d'instances de flotte pendant les heures de bureau, il est préférable de conserver les mêmes sessions de streaming. En effet, les instances de flotte sont facturées à l'heure, et chaque fois qu'une nouvelle session de streaming démarre, cela entraîne des frais supplémentaires pour les instances de flotte.

Tableau 10 — Comparaison des types de parcs d' WorkSpaces applications

Type de flotte	Avantages	Considérations
Always-On	Moins de temps d'attente pour les sessions de streaming	Les utilisateurs paient les frais d'instance horaires, car il n'existe aucune option permettant de maintenir les instances à l'état arrêté.
On-Demand	Réduction des coûts car les instances restent à l'état arrêté	Temps d'attente plus long pour les sessions de streaming
Elasticité	Per-second la facturation peut être utile pour les cas d'utilisation qui ont des modèles d'utilisation sporadiques pour les applications pouvant être installées sur un disque dur virtuel	À mesure que la taille du disque dur virtuel de l'application augmente, le temps nécessaire pour le monter sur une instance de streaming peut être long

WorkSpaces Les applications surveillent l'utilisation de votre flotte et ajustent automatiquement la capacité de votre flotte afin de répondre à la demande de vos utilisateurs au moindre coût possible. Les ajustements de capacité sont effectués en fonction des politiques de dimensionnement que vous définissez, en fonction de l'utilisation actuelle ou en fonction d'un calendrier. Passez régulièrement en revue les indicateurs d'utilisation de la flotte pour vérifier que les politiques de dimensionnement de la flotte ne prévoient pas de niveaux élevés de capacité inutilisée.

Politiques de mise à l’échelle

Fleet Auto Scaling vous permet d'optimiser les ressources de votre flotte en évitant de surcharger les ressources en attendant que les utilisateurs se connectent. Les administrateurs peuvent ajuster la taille de la flotte en fonction des différentes utilisations afin de répondre à la demande des utilisateurs. Utilisez CloudWatch WorkSpaces les indicateurs du parc d'applications ou des outils de surveillance tiers pour en savoir plus sur l'activité des utilisateurs et configurer des politiques de dimensionnement afin d'étendre ou de réduire WorkSpaces les flottes d'applications en fonction de l'utilisation prévue. Les journaux des utilisateurs sont un mécanisme essentiel pour mieux comprendre l'utilisation réelle. Ces informations peuvent être utilisées pour modifier dynamiquement la taille du parc en fonction d'Auto Scaling.

Dans de nombreux cas, WorkSpaces les flottes d'applications sont créées en fonction du nombre maximum d'utilisateurs et ne sont pas ajustées en fonction des différents moments de la journée et de la semaine, tels que les nuits et les week-ends. Souvent, le nombre d'utilisateurs simultanés des applications diffusées en continu est inférieur au nombre total d'utilisateurs, en particulier lorsque les utilisateurs ont la possibilité de travailler à distance. Il est important de tenir compte de ces facteurs lors de la projection des modèles d'utilisation. La surestimation entraîne un surprovisionnement des instances d' WorkSpaces applications, ce qui entraîne des coûts supplémentaires. Pour obtenir une configuration optimale, vous devrez peut-être combiner une ou plusieurs politiques de dimensionnement planifiées avec des politiques de dimensionnement externe.

Pour en savoir plus sur la mise en œuvre des politiques de dimensionnement, consultez Scaling your Amazon AppStream 2.0 fleet.

Frais d'utilisation

Des frais d'utilisation sont facturés par utilisateur et par mois dans chaque cas Région AWS où les utilisateurs diffusent des applications à partir d'instances du parc d' WorkSpaces applications. Au lieu de générer des ID utilisateur différents, utilisez des ID utilisateur cohérents pour les utilisateurs

WorkSpaces des applications. Aucuns frais d'utilisation ne sont facturés lors de la connexion à des générateurs d'images.

Les écoles, les universités et certaines institutions publiques peuvent bénéficier d'une réduction des frais d'utilisation de Microsoft RDS SAL de 0,44$ par utilisateur et par mois. Pour connaître les conditions de qualification, reportez-vous aux termes et documents relatifs aux licences Microsoft.

Si vous possédez Microsoft License Mobility, vous pouvez peut-être apporter vos propres licences d'accès client (CAL) Microsoft RDS et les utiliser avec Amazon WorkSpaces Applications. Si vous êtes couvert par votre propre licence, vous n'aurez pas à payer de frais d'utilisation mensuels. Pour plus d'informations sur la possibilité d'utiliser vos licences Microsoft RDS CAL existantes avec Amazon WorkSpaces Applications, consultez les instructions relatives à la mobilité des AWS licences ou consultez votre représentant des licences Microsoft.

Utilisation d'Image Builder

WorkSpaces Les instances d'Applications Image Builder sont facturées à l'heure. Les frais d'instance d'Image Builder incluent le calcul, le stockage et tout trafic réseau utilisé par le protocole de streaming. Toutes les instances Image Builder en cours d'exécution sont facturées aux frais d'instance applicables. Ces frais sont basés sur le type et la taille de l'instance, même lorsqu'aucun administrateur n'est connecté.

Pour optimiser les coûts, il est recommandé d'arrêter une instance Image Builder lorsqu'elle n'est pas utilisée. CloudWatch Les règles relatives aux événements peuvent être utilisées pour planifier une tâche quotidienne, telle que l'appel d'une fonction Lambda pour arrêter les instances du générateur d'images.

Vous pouvez maintenir l'image de vos WorkSpaces applications à jour en utilisant des mises à jour d'image d' WorkSpaces applications gérées. Cette méthode de mise à jour fournit les dernières mises à jour du système d'exploitation Windows et des pilotes, ainsi que le dernier logiciel d'agent d' WorkSpaces applications. Lorsque vous utilisez cette méthode pour mettre à jour des images, un Image Builder est automatiquement démarré et arrêté dans le cadre du processus de service géré.

Conclusion

Avec WorkSpaces Applications, vous pouvez facilement ajouter vos applications de bureau existantes AWS et permettre à vos utilisateurs de les diffuser instantanément. Les utilisateurs de Windows peuvent utiliser le client WorkSpaces Applications ou un navigateur HTML5-capable Web pour le streaming des applications. Vous pouvez conserver une seule version de chacune de vos applications, ce qui facilite leur gestion. Les utilisateurs peuvent accéder à tout moment aux dernières versions des applications. Vos applications s'exécutent sur des ressources AWS informatiques et les données ne sont jamais stockées sur les appareils des utilisateurs, ce qui signifie qu'ils bénéficient toujours d'une expérience sécurisée et performante.

Contrairement aux solutions sur site traditionnelles pour le streaming d'applications de bureau, WorkSpaces Applications propose une tarification à l'utilisation, sans investissement initial ni infrastructure à entretenir. Vous pouvez évoluer instantanément et à l'échelle mondiale, afin de garantir à vos utilisateurs une expérience exceptionnelle en permanence.

Amazon WorkSpaces Applications 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 contributeurs à ce document incluent :

- Andrew Wood, architecte de solutions senior, Amazon Web Services
- Andrew Morgan, spécialiste EUC SA, Amazon Web Services
- Arun PC, spécialiste senior de l'EUC SA, Amazon Web Services
- Asriel Agronin, architecte de solutions senior, Amazon Web Services
- Dustin Shelton, spécialiste principal de l'EUC SA, Amazon Web Services
- Jeremy Schiefer, architecte de solutions senior, Amazon Web Services
- Navi Magee, architecte de solutions principale, Amazon Web Services
- Pete Fergus, ingénieur principal du support cloud, Amazon Web Services
- Phil Persson, spécialiste principal de l'EUC SA, Amazon Web Services
- Richard Spaven, spécialiste principal de l'EUC SA, Amazon Web Services
- Spencer DeBrosse, architecte de solutions senior, Amazon Web Services
- Stephen Stetler, architecte de solutions senior, Amazon Web Services
- Taka Matsumoto, ingénieur principal du support cloud, Amazon Web Services
- Vasant Sirsat, spécialiste principal de l'EUC SA, Amazon Web Services

Suggestions de lecture

Pour en savoir plus, voir :

- Guide d'administration WorkSpaces des applications Amazon
- Référence WorkSpaces d'API Amazon Applications
- Utilisez Amazon FSx for Windows File Server et FSLogix pour optimiser la persistance des paramètres des applications sur Amazon Applications WorkSpaces
- Surveillance des WorkSpaces applications Amazon avec Amazon ElasticSearch et Amazon Firehose
- Analysez vos rapports d'utilisation WorkSpaces des applications Amazon à l'aide d'Amazon Athena et d'Amazon Quick
- Faites évoluer vos flottes WorkSpaces d'applications Amazon
- Utilisation AppLocker de Microsoft pour gérer l'expérience applicative sur Amazon WorkSpaces Applications
- Utilisation d'un domaine personnalisé avec Amazon WorkSpaces Applications
- Comment utiliser mes propres licences d'accès client Microsoft RDS avec WorkSpaces des applications ?
- Outil de tarification des WorkSpaces applications Amazon
- Créez une version d'essai logicielle en ligne avec des WorkSpaces applications
- Créez un portail SaaS avec Amazon WorkSpaces Applications

Révisions du document

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

Modification	Description	Date
Document mis à jour	Mises à jour pour inclure les flottes élastiques, les droits d'application basés sur les tributs, le catalogue d'applications multi-stack, les flottes basées sur Linux, les entrées et sorties de données, la reprise après sinistre et d'autres mises à jour.	14 juin 2022
Document mis à jour	Version HTML publiée.	19 janvier 2022
Publication initiale	Livre blanc publié.	8 juin 2021

Avis

Les clients sont tenus de procéder à leur propre évaluation indépendante des informations contenues dans ce 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. AWSles 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.

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.