Guide de l'administrateur

Amazon WorkSpaces Thin Client

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon WorkSpaces Thin Client: Guide de l'administrateur

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Qu'est-ce que la console d'administration Amazon WorkSpaces Thin Client ? 1
Est-ce votre première utilisation ? 1
Architecture 1
Configuration de la console d'administration Amazon WorkSpaces Thin Client 4
Inscrivez-vous à AWS 4
Créer un utilisateur IAM 4
Commencer à utiliser votre console d'administration VDI pour Amazon WorkSpaces Thin Client 6
Configuration de WorkSpaces Personal pour WorkSpaces Thin Client 6
Avant de commencer 7
Étape 1 : Vérifiez que votre système possède les fonctionnalités WorkSpaces personnelles requises 7
Étape 2 : utilisez la configuration avancée pour lancer votre WorkSpace 8
Continuité des activités 9
Configuration de WorkSpaces pools pour WorkSpaces Thin Client 10
Avant de commencer 10
Création d'un WorkSpaces pool 11
Configuration de l'accès aux clients WorkSpaces légers 14
Configuration de la AppStream version 2.0 pour Amazon WorkSpaces Thin Client 14
Étape 1 : Vérifiez que votre système répond aux fonctionnalités requises AppStream 2.0 15
Étape 2 : Configurez vos AppStream stacks 2.0 16
Configuration d'Amazon WorkSpaces Secure Browser pour Amazon WorkSpaces Thin Client 16
Étape 1 : Vérifiez que votre système répond aux fonctionnalités requises par Amazon WorkSpaces Secure Browser 17
Étape 2 : configurer les portails WorkSpaces Secure Browser 17
Démarrage de la console d'administration du WorkSpaces Thin Client 18
Régions couvertes 18
Lancement de la console d'administration WorkSpaces Thin Client 19
Utilisation de la console d'administration WorkSpaces Thin Client 20
Environnements 21
Liste des environnements 21
Détails de l'environnement 23
Création d'un environnement 27
Modification d'un environnement 30

Suppression d'un environnement ... 31
Appareils ... 32
Liste des périphériques ... 32
Détails de l'appareil ... 35
Modification du nom d'un appareil ... 42
Réinitialisation et annulation de l'inscription d'un appareil ... 42
Archivage d'un appareil ... 42
Suppression d'un appareil ... 43
Exportation des détails d'un appareil ... 43
Mises à jour de logiciels ... 43
Mise à jour de l'environnement logiciel ... 44
Mise à jour du logiciel de l'appareil ... 45
WorkSpaces Versions du logiciel Thin Client ... 45
Utilisation de balises sur les ressources WorkSpaces Thin Client ... 59
Sécurité ... 63
Protection des données ... 63
Chiffrement des données ... 65
Chiffrement au repos ... 66
Chiffrement en transit ... 80
Gestion des clés ... 81
Confidentialité du trafic professionnel sur Internet ... 81
Gestion des identités et des accès ... 81
Public ciblé ... 82
Authentification par des identités ... 82
Gestion des accès à l’aide de politiques ... 86
Comment Amazon WorkSpaces Thin Client fonctionne avec IAM ... 89
Exemples de politiques basées sur l’identité ... 97
AWS politiques gérées ... 102
Résolution des problèmes ... 107
Résilience ... 110
Analyse et gestion des vulnérabilités ... 110
Surveillance ... 112
CloudTrail journaux ... 112
CloudTrail événements liés aux données ... 114
CloudTrail événements de gestion ... 115
CloudTrail exemples d'événements ... 115

AWS CloudFormation ressources 120
WorkSpaces Thin Client et AWS CloudFormation modèles 120
En savoir plus sur AWS CloudFormation 120
AWS PrivateLink 122
Considérations 122
Création d’un point de terminaison d’interface 122
Création d’une politique de point de terminaison 123
Historique de la documentation 125
..... cxxviii

Qu'est-ce que la console d'administration Amazon WorkSpaces Thin Client ?

Avec la console d'administration Amazon WorkSpaces Thin Client, les administrateurs peuvent gérer les environnements et les appareils WorkSpaces Thin Client via un portail WorkSpaces Thin Client. À partir de cette console Web, les administrateurs peuvent créer des environnements, gérer des appareils et définir des paramètres pour les utilisateurs de WorkSpaces Thin Client au sein de leur réseau.

Les environnements de bureau virtuels que vous utilisez pour WorkSpaces Thin Client doivent être créés ou modifiés dans leur propre console.

> **Important**
>
> Pour que la console d'administration WorkSpaces Thin Client fonctionne correctement, votre système doit d'abord répondre à des exigences spécifiques. Ces exigences sont répertoriées dans Prérequis et configurations.

Rubriques

- Est-ce votre première utilisation ?
- Architecture

Est-ce votre première utilisation ?

Si vous utilisez la console d'administration WorkSpaces Thin Client pour la première fois, nous vous recommandons de commencer par lire les sections suivantes :

- Démarrage de la console d'administration du WorkSpaces Thin Client
- Utilisation de la console d'administration WorkSpaces Thin Client

Architecture

Chaque client WorkSpaces léger est associé à un fournisseur d'interface de bureau virtuel (VDI). WorkSpaces Thin Client prend en charge trois fournisseurs VDI :

- Amazon WorkSpaces
- AppStream 2.0
- Navigateur Amazon WorkSpaces Secure

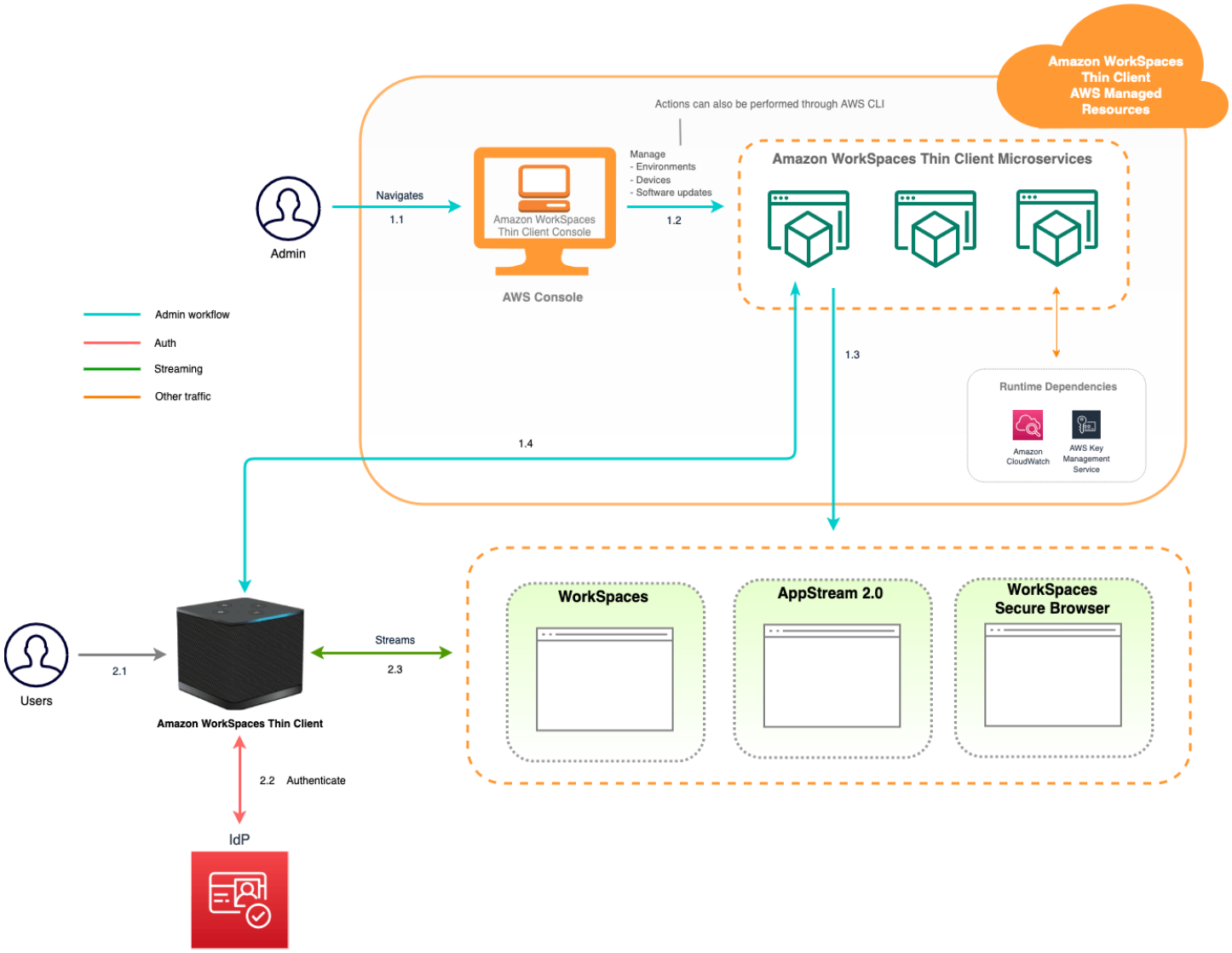
Selon le VDI utilisé, les informations relatives à votre client WorkSpaces léger sont accessibles et gérées via des répertoires pour Secure Browser WorkSpaces, des piles pour AppStream 2.0 et des points de terminaison de portail Web pour WorkSpaces Secure Browser.

Pour plus d'informations sur Amazon WorkSpaces, consultez Commencer la configuration WorkSpaces rapide. Les annuaires sont gérés via le AWS Directory Service, qui propose les options suivantes : Simple AD, AD Connector ou AWS Directory Service pour Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD. Pour plus d'informations, consultez le Guide d'administration AWS Directory Service.

Pour plus d'informations sur la AppStream version 2.0, consultez Get Started with Amazon AppStream 2.0 : Configuration avec des exemples d'applications. AppStream La version 2.0 gère les AWS ressources nécessaires pour héberger et exécuter vos applications, évolue automatiquement et fournit un accès à vos utilisateurs à la demande. AppStream La version 2.0 permet aux utilisateurs d'accéder aux applications dont ils ont besoin sur l'appareil de leur choix, avec une expérience utilisateur réactive et fluide, identique à celle des applications installées en mode natif.

Pour plus d'informations sur WorkSpaces Secure Browser, consultez Getting started with Amazon WorkSpaces Secure Browser. Amazon WorkSpaces Secure Browser est un service à la demande, entièrement géré, basé sur Linux, conçu pour faciliter l'accès sécurisé des navigateurs aux sites Web internes et aux applications (software-as-a-serviceSaaS). Accédez au service à partir des navigateurs web existants, sans les contraintes administratives de la gestion de l’infrastructure, les logiciels clients spécialisés ou les solutions de réseau privé virtuel (VPN).

Le schéma suivant montre l'architecture de WorkSpaces Thin Client.


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
AWS Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
Admin workflow
Auth
Streaming
Other traffic
1.4
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
2.2 Authenticate
IdP

Configuration de la console d'administration Amazon WorkSpaces Thin Client

Rubriques

- Inscrivez-vous à AWS
- Créer un utilisateur IAM

Inscrivez-vous à AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d’inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l’utilisateur racine a accès à l’ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l’utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

Créer un utilisateur IAM

Afin de créer un utilisateur administrateur, choisissez l'une des options suivantes :

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des identifiants à court terme pour accéder à AWS. Telles sont les meilleures pratiques en matière de sécurité. Pour plus d'informations sur les bonnes pratiques, veuillez consulter Security best practices in IAM (français non garanti) dans le Guide de l'utilisateur IAM.	Suivre les instructions de la section Mise en route dans le AWS IAM Identity Center Guide de l'utilisateur.	Configurez l'accès par programmation en configurant le AWS CLI à utiliser AWS IAM Identity Center dans le guide de l'AWS Command Line Interface utilisateur.
Dans IAM (Non recommandé)	Utiliser des identifiants à long terme pour accéder à AWS.	Suivez les instructions de la section Créer un utilisateur IAM pour un accès d'urgence dans le guide de l'utilisateur IAM.	Configurez l'accès programmatique en gérant les clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

Commencer à utiliser votre VDI pour Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client est un appareil client léger économique conçu pour fonctionner avec les services informatiques des utilisateurs AWS finaux afin de vous fournir un accès instantané et sécurisé aux applications et aux bureaux virtuels.

Choisissez une infrastructure de bureau virtuel (VDI) et configurez-la pour qu'elle fonctionne avec WorkSpaces Thin Client.

> **Important**
>
> Pour que la console d'administration WorkSpaces Thin Client fonctionne correctement, votre système doit d'abord répondre à des exigences spécifiques. Ces exigences sont répertoriées dans la procédure de configuration de chaque fournisseur de bureau virtuel.

WorkSpaces Thin Client nécessite des configurations logicielles spécifiques, en fonction de votre fournisseur de bureau virtuel.

Rubriques

- Configuration de WorkSpaces Personal pour WorkSpaces Thin Client
- Configuration de WorkSpaces pools pour WorkSpaces Thin Client
- Configuration de la AppStream version 2.0 pour Amazon WorkSpaces Thin Client
- Configuration d'Amazon WorkSpaces Secure Browser pour Amazon WorkSpaces Thin Client

Configuration de WorkSpaces Personal pour WorkSpaces Thin Client

Pour que WorkSpaces Thin Client soit utilisé avec Amazon WorkSpaces Personal, votre service doit être configuré pour accéder aux WorkSpaces annuaires. Les annuaires Amazon WorkSpaces Personal sont répertoriés en fonction de leur nom sur la page d'environnement WorkSpaces Thin Client Create de AWS la console.

> **Note**
>
> Les configurations doivent être effectuées avant d'utiliser la console pour la première fois. Il n'est pas recommandé de modifier les fonctionnalités requises après avoir commencé à utiliser la console.

Avant de commencer

Assurez-vous de disposer d'un AWS compte pour créer ou administrer un WorkSpace. Les utilisateurs de l'appareil n'ont toutefois pas besoin d'un AWS compte pour se connecter et utiliser leur WorkSpaces.

Passez en revue et comprenez les concepts suivants avant de procéder à votre configuration :

- Lorsque vous lancez un WorkSpace, sélectionnez un WorkSpace bundle. Pour plus d'informations, consultez Amazon WorkSpaces Bundles.
- Lorsque vous lancez un WorkSpace, sélectionnez le protocole que vous souhaitez utiliser avec votre offre groupée. Pour plus d'informations, consultez Protocoles pour Amazon WorkSpaces Personal.
- Lorsque vous lancez un WorkSpace, spécifiez les informations de profil de chaque utilisateur, y compris le nom d'utilisateur et l'adresse e-mail. Les utilisateurs complètent leur profil en créant un mot de passe. Les informations concernant WorkSpaces et les utilisateurs sont stockées dans un répertoire. Pour plus d'informations, voir Gérer les annuaires pour les WorkSpaces utilisateurs personnels.
- Lorsque vous lancez un WorkSpace, activez et configurez l'accès Web du client WorkSpaces léger. Pour plus d'informations, voir Configurer un client WorkSpaces léger

Étape 1 : Vérifiez que votre système possède les fonctionnalités WorkSpaces personnelles requises

Pour que la console d'administration WorkSpaces Thin Client fonctionne correctement avec Amazon WorkSpaces Personal, votre système doit répondre aux exigences spécifiques suivantes. Ce tableau répertorie toutes ces fonctionnalités prises en charge et leurs exigences.

Fonctionnalité	Exigence
Accès web	Activées
Système d'exploitation pris en charge	• Windows 10 • Windows 10 (Apportez votre propres licence) • Windows 11 • Windows 11 (Apportez votre propres licence)
Offres groupées prises en charge	• Microsoft Power avec Windows 10 (basé sur Server 2016, 2019 et 2022) • Microsoft Power avec Windows 10 (basé sur Server 2016, 2019 et 2022) avec Office • Microsoft PowerPro avec Windows 10 (basé sur Server 2016, 2019 et 2022) • Microsoft PowerPro avec Windows 10 (basé sur Server 2016, 2019 et 2022) avec Office • Microsoft Performance avec Windows 10 (basé sur Server 2016, 2019 et 2022) • Microsoft Performance avec Windows 10 (basé sur Server 2016, 2019 et 2022) avec Office
Protocole pris en charge	DCV uniquement

Étape 2 : utilisez la configuration avancée pour lancer votre WorkSpace

Pour utiliser la configuration avancée pour lancer votre WorkSpace

1. Ouvrez la WorkSpaces console à l'adressehttps://console.aws.amazon.com/workspaces/v2/home/.
2. Choisissez l'un des types d'annuaire suivants, puis cliquez sur Suivant :
   - AWS Microsoft AD géré
   - Simple AD
   - AD Connector

3. Saisissez les informations de l'annuaire.
4. Choisissez deux sous-réseaux au sein d'un VPC dans deux zones de disponibilité différentes. Pour plus d'informations, consultez Configuration d'un VPC avec des sous-réseaux publics.
5. Vérifiez les informations de votre répertoire et choisissez Créer un répertoire.

Continuité des activités

WorkSpaces Thin Client fournit un support pour la continuité des activités dans le cadre d'un plan de continuité des activités (BCP). WorkSpaces La continuité des activités de Thin Client est uniquement disponible pour une utilisation avec WorkSpaces Personal. Pour plus d'informations sur la continuité des activités, consultez Business continuity for WorkSpaces Personal dans le guide d' WorkSpaces administration Amazon.

Prérequis

Pour que la continuité des activités fonctionne sur WorkSpaces Thin Client, les conditions préalables suivantes doivent être remplies :

- Pour WorkSpaces la redirection entre régions, le service DNS et les politiques de routage ont été configurés. Pour les configurer, consultez Configurer votre service DNS et configurer les politiques de routage DNS.
- Pour WorkSpaces la résilience multirégionale — Une réserve WorkSpaces a été créée. Pour créer cela, consultez la section Créer une réserve WorkSpace.
- Un alias de connexion dans la région à l'aide de WorkSpaces Thin Client. Pour vérifier votre région, consultez la section Régions couvertes.

Configuration de la continuité des activités pour WorkSpaces Thin Client

Pour activer WorkSpaces Personal DR sur Amazon WorkSpaces Thin Client, vous devez configurer des alias de connexion pour qu'ils soient mappés à l'environnement à l'aide du SDK.

Exemple d'explication documentaire sur la configuration de la reprise après sinistre :

Example

Exemple de commande utilisant la AWS CLI pour créer un nouvel environnement à l'aide d'un alias de WorkSpaces connexion pour le poste de travail de streaming :

```
aws workspaces-thin-client create-environment --region region --desktop-arn/
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

*wsca-id*Remplacez-le par votre alias de connexion WorkSpaces personnel. L'ID de l'alias de WorkSpaces connexion se trouve dans la console WorkSpaces de gestion ou dans le SDK.

L'expérience de l'utilisateur final

Une fois la continuité des activités configurée, les appareils doivent être enregistrés et actifs au cours des 15 derniers jours. Ensuite, si les services de gestion des clients WorkSpaces légers deviennent indisponibles, les utilisateurs peuvent rester connectés à leurs sessions pendant 24 heures au maximum. Dans ces conditions, l'appareil ne recevra pas de mises à jour logicielles, n'échangera pas d'informations de posture et ne pourra pas être activé. L'entrée de périphérique correspondante dans la console WorkSpaces Thin Client n'affichera pas les informations les plus récentes.

Si les services de gestion des appareils WorkSpaces Thin Client restent indisponibles au-delà de 24 heures, le message d'erreur suivant s'affiche :

« Une erreur s'est produite. Veuillez réessayer. Si le problème persiste, contactez votre administrateur informatique. (Code d'erreur : 3006). »

Configuration de WorkSpaces pools pour WorkSpaces Thin Client

Pour que WorkSpaces Thin Client soit utilisé avec Amazon WorkSpaces Pools, votre fournisseur d'identité (IdP) SAML 2.0 doit être configuré pour accéder WorkSpaces au répertoire Pools. Les annuaires Amazon WorkSpaces Pools sont un pool non persistant WorkSpaces attribué à un groupe d'utilisateurs.

> **Note**
>
> Les configurations doivent être effectuées avant d'utiliser la console pour la première fois.

Avant de commencer

Assurez-vous de disposer d'un AWS compte pour créer ou administrer un WorkSpace. Les utilisateurs de l'appareil n'ont toutefois pas besoin d'un AWS compte pour se connecter et utiliser leur WorkSpaces.

Passez en revue et comprenez les concepts répertoriés dans la section Before you Begin Using Active Directory with WorkSpaces Pools du guide d' WorkSpaces administration Amazon avant de procéder à votre configuration.

Création d'un WorkSpaces pool

Configurez et créez un pool à partir duquel les applications utilisateur sont lancées et diffusées en continu.

> **Note**
>
> Vous devez créer un répertoire avant de créer un WorkSpaces pool. Pour plus d'informations, consultez Configurer SAML 2.0 et créer un répertoire de répertoires WorkSpaces Pools.

Pour configurer et créer un pool

1. Ouvrez la WorkSpaces console à l'adressehttps://console.aws.amazon.com/workspaces/v2/home/.
2. Dans le volet de navigation WorkSpaces, choisissez Pools.
3. Choisissez Create WorkSpaces Pools.
4. Sous Intégration (facultatif), vous pouvez choisir de me recommander des options en fonction de mon cas d'utilisation pour obtenir des recommandations sur le type que WorkSpaces vous souhaitez utiliser. Vous pouvez ignorer cette étape si vous savez que vous souhaitez utiliser des WorkSpaces pools.
5. Sous Configurer WorkSpaces, entrez les informations suivantes :
   - Dans Nom, entrez un identifiant de nom unique pour le pool. Les caractères spéciaux ne sont pas autorisés.
   - Dans Description, entrez une description du pool (256 caractères maximum).
   - Pour Bundle, choisissez parmi les options suivantes le type de bundle que vous souhaitez utiliser pour votre WorkSpaces.
     - Utiliser un WorkSpaces pack de base — Choisissez l'un des packs dans le menu déroulant. Pour plus d'informations sur le type de bundle que vous avez sélectionné, choisissez Bundle details. Pour comparer les forfaits proposés pour les pools, choisissez Comparer tous les forfaits.

- Utilisez votre propre bundle personnalisé : choisissez un bundle que vous avez créé précédemment. Pour créer un ensemble personnalisé, voir Création d'une WorkSpaces image personnalisée et d'un ensemble pour WorkSpaces Personal.

  > **Note**
  >
  > Le BYOL n'est actuellement pas disponible pour les WorkSpaces piscines.

- Pour Durée maximale de la session en minutes, choisissez la durée maximale pendant laquelle une session de streaming peut rester active. Si les utilisateurs sont toujours connectés à une instance de streaming cinq minutes avant que cette limite ne soit atteinte, ils sont invités à enregistrer tous les documents ouverts avant d'être déconnectés. Une fois ce délai écoulé, l'instance est résiliée et remplacée par une nouvelle instance. La durée maximale de session que vous pouvez définir dans la console WorkSpaces Pools est de 5760 minutes (96 heures). La durée maximale de session que vous pouvez définir à l'aide de l'API et de la CLI WorkSpaces Pools est de 432 000 secondes (120 heures).
- Pour Disconnect timeout in minutes (Délai avant déconnexion en minutes), choisissez la durée pendant laquelle une session de streaming doit rester active après la déconnexion des utilisateurs. Si les utilisateurs essaient de se reconnecter à la session de streaming après une déconnexion ou une interruption réseau dans cet intervalle de temps, ils sont connectés à leur session précédente. Sinon, ils sont connectés à une nouvelle session avec une nouvelle instance de streaming.
- Si un utilisateur met fin à la session en choisissant Fin de session ou Déconnexion dans la barre d'outils du pool, le délai de déconnexion ne s'applique pas. Au lieu de cela, l'utilisateur est invité à enregistrer les documents ouverts, puis il est immédiatement déconnecté de l'instance de streaming. L'instance que l'utilisateur utilisait est ensuite supprimée.
- Pour Idle disconnect timeout in minutes (Délai d'inactivité avant déconnexion en minutes), choisissez la durée pendant laquelle les utilisateurs peuvent rester inactifs avant d'être déconnectés de leur session de streaming et avant le début de l'intervalle Disconnect timeout in minutes (Délai avant déconnexion en minutes). Les utilisateurs sont avertis avant d'être déconnectés en raison de leur inactivité. S'ils essaient de se reconnecter à la session de streaming avant que l'intervalle de temps spécifié dans Délai avant déconnexion en minutes se soit écoulé, ils sont connectés à leur session précédente. Sinon, ils sont connectés à une nouvelle session avec une nouvelle instance de streaming. Si vous définissez la valeur sur 0, celle-ci est désactivée. Lorsque cette valeur est désactivée, les utilisateurs ne sont pas déconnectés en raison de leur inactivité.

> **Note**
>
> Les utilisateurs sont considérées comme inactifs lorsqu'ils arrêtent de se servir du clavier ou de la souris lors de leur session de streaming. Pour les pools joints à un domaine, le compte à rebours pour le délai d'inactivité de déconnexion ne commence que lorsque les utilisateurs se connectent à l'aide du mot de passe de leur domaine Active Directory ou à l'aide d'une carte à puce. Les chargements et téléchargements, les entrées audio, les sorties audio, et les modifications de pixels ne sont pas considérés comme une activité de l'utilisateur. Si les utilisateurs continuent d'être inactifs après que l'intervalle de temps défini par Délai d'inactivité avant déconnexion en minutes se soit écoulé, ils sont déconnectés.

- Pour les politiques de capacité planifiée (facultatif), choisissez Ajouter une nouvelle capacité planifiée. Indiquez les dates et heures de début et de fin auxquelles vous devez fournir le nombre minimum et maximum d'instances pour votre pool en fonction du nombre minimum d'utilisateurs simultanés attendus.
- Pour les politiques de dimensionnement manuel (facultatif), spécifiez les politiques de dimensionnement que les pools doivent utiliser pour augmenter ou diminuer la capacité de votre pool. Développez les politiques de dimensionnement manuel pour ajouter de nouvelles politiques de dimensionnement.

  > **Note**
  >
  > La taille de votre piscine est limitée par la capacité minimale et maximale que vous avez spécifiée.

  - Choisissez Ajouter de nouvelles politiques de scalabilité et entrez les valeurs pour ajouter des instances spécifiées si l'utilisation de la capacité spécifiée est inférieure ou supérieure à la valeur de seuil spécifiée.
  - Choisissez Ajouter une nouvelle échelle dans les politiques et entrez les valeurs pour supprimer les instances spécifiées si l'utilisation de la capacité spécifiée est inférieure ou supérieure à la valeur de seuil spécifiée.
- Pour les balises, spécifiez la valeur de paire de clés que vous souhaitez utiliser. Une clé peut être une catégorie générale, comme un « projet », un « propriétaire » ou un « environnement » avec des valeurs associées spécifiques.

6. Sur la page Sélectionner un répertoire, choisissez le répertoire que vous avez créé. Pour créer un répertoire, choisissez Create directory. Pour plus d'informations, consultez la section Gérer les annuaires pour les WorkSpaces pools.
7. Choisissez Create WorkSpace Pool.

Configuration de l'accès aux clients WorkSpaces légers

Pour configurer l'accès Web pour que les WorkSpaces pools utilisent WorkSpaces Thin Client, vous devez utiliser la AWS commande land interface.

1. Installez ou mettez à jour le AWS Command Line Interface.
2. Configurez vos AWS CLI paramètres.
3. Ouvrez le AWS CLI.
4. Exécutez la commande suivante en `REGION` remplaçant `WORKSPACES_DIRECTORY_ID` et en saisissant les informations appropriées :

```
aws workspaces modify-workspace-access-properties --resource-
id WORKSPACES_DIRECTORY_ID  --workspace-access-properties
 '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

Configuration de la AppStream version 2.0 pour Amazon WorkSpaces Thin Client

AppStream Les instances 2.0 seront répertoriées en fonction des noms de Stack et nécessiteront la configuration d'une URL de connexion IdP sur la page de création d'un environnement. Étant donné que l'authentification SAML pour AppStream 2.0 ne prend en charge que l'authentification initiée, l'administrateur devra saisir manuellement l'URL de connexion correcte.

> **Note**
>
> Les configurations doivent être effectuées avant d'utiliser la console pour la première fois. Il n'est pas recommandé de modifier les fonctionnalités requises après avoir commencé à utiliser la console.

Étape 1 : Vérifiez que votre système répond aux fonctionnalités requises AppStream 2.0

Pour que la console d'administration WorkSpaces Thin Client fonctionne correctement avec la AppStream version 2.0, votre système doit répondre aux exigences spécifiques suivantes. Ce tableau répertorie toutes ces fonctionnalités prises en charge et leurs exigences.

Fonctionnalité	Exigence
Fournisseur d'identité	Accédez à la section Configuration de SAML dans le guide de l'administrateur AppStream 2.0 pour créer un fournisseur d'identité. Lorsque vous êtes invité à créer une console d'environnement, entrez votre URL de connexion IDP.
Système d’exploitation	Windows
Type de plateforme	Windows Server (2012 R2, 2016 ou 2019)
Presse-papiers	Désactiver Configuré au niveau de la pile AppStream 2.0
Transfert de fichiers	Désactiver Configuré au niveau de la pile AppStream 2.0
Imprimer sur un appareil local	Désactiver Configuré au niveau de la pile AppStream 2.0

L'exigence de verrouillage de l'écran via l'authentification SAML sur AppStream 2.0 est également prise en charge. Le pool d'utilisateurs et les mécanismes d'authentification programmatique ne sont pas pris en charge sur WorkSpaces Thin Client.

Étape 2 : Configurez vos AppStream stacks 2.0

Pour diffuser vos applications, la AppStream version 2.0 nécessite un environnement comprenant un parc associé à une pile et au moins une image d'application. Suivez ces étapes pour configurer une flotte et une pile et permettre aux utilisateurs d'accéder à la pile. Si ce n'est pas déjà fait, nous vous recommandons d'essayer les procédures décrites dans Get Started with AppStream 2.0 : Configuration avec des exemples d'applications.

Si vous souhaitez créer une image à utiliser, voir Tutoriel : Création d'une image AppStream 2.0 personnalisée à l'aide de la console AppStream 2.0.

Si vous avez l'intention de joindre une flotte à un domaine Active Directory, configurez votre domaine Active Directory avant d'exécuter les étapes ci-dessous. Pour plus d'informations, consultez la section Utilisation d'Active Directory avec AppStream 2.0.

Tâches

- Créer une flotte
- Créer une pile
- Fournir l'accès aux utilisateurs
- Nettoyer les ressources

Configuration d'Amazon WorkSpaces Secure Browser pour Amazon WorkSpaces Thin Client

Amazon WorkSpaces Secure Browser est basé sur les points de terminaison de son portail Web sur la page WorkSpaces Thin Client Create environment de AWS la console.

> **Note**
>
> Les configurations doivent être effectuées avant d'utiliser la console pour la première fois. Il n'est pas recommandé de modifier les fonctionnalités requises après avoir commencé à utiliser la console.

Étape 1 : Vérifiez que votre système répond aux fonctionnalités requises par Amazon WorkSpaces Secure Browser

Pour que WorkSpaces Thin Client Administrator Console fonctionne correctement avec Amazon WorkSpaces Secure Browser, votre système doit répondre aux exigences spécifiques suivantes. Ce tableau répertorie toutes ces fonctionnalités prises en charge et leurs exigences.

Fonctionnalité	Exigence
Presse-papiers	Désactiver
Transfert de fichiers	Désactiver
Imprimer sur un appareil local	Désactiver

> **Note**
>
> L'extension WorkSpaces Secure Browser pour l'authentification unique n'est actuellement pas prise en charge sur WorkSpaces Thin Client.

Étape 2 : configurer les portails WorkSpaces Secure Browser

WorkSpaces Thin Client fonctionne avec le VPC WorkSpaces Secure Browser dans une configuration spécifique :

1. Créez un VPC à l'aide du modèle AWS CodeBuild Cloudformation.
2. Configurez votre Fournisseur d'identité.
3. Créez un portail Amazon WorkSpaces Secure Browser.
4. Testez votre nouveau portail Amazon WorkSpaces Secure Browser.

Démarrage de la console d'administration du WorkSpaces Thin Client

WorkSpaces Le client léger est un appareil client léger économique conçu pour fonctionner avec les services informatiques des utilisateurs AWS finaux afin de vous fournir un accès instantané et sécurisé aux applications et aux bureaux virtuels.

Rubriques

- Régions couvertes
- Lancement de la console d'administration WorkSpaces Thin Client

Régions couvertes

WorkSpaces Thin Client est disponible dans les régions suivantes.

Seule la console d'administration WorkSpaces Thin Client est disponible dans ces régions. WorkSpaces Les appareils Thin Client ne sont actuellement disponibles qu'aux États-Unis, en Allemagne, en France, en Italie et en Espagne.

Nom de la région	Région	Point de terminaison	Lien vers la console
USA Est (Virginie du Nord)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
USA Ouest (Oregon)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
Asie-Pacifique (Mumbai)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home

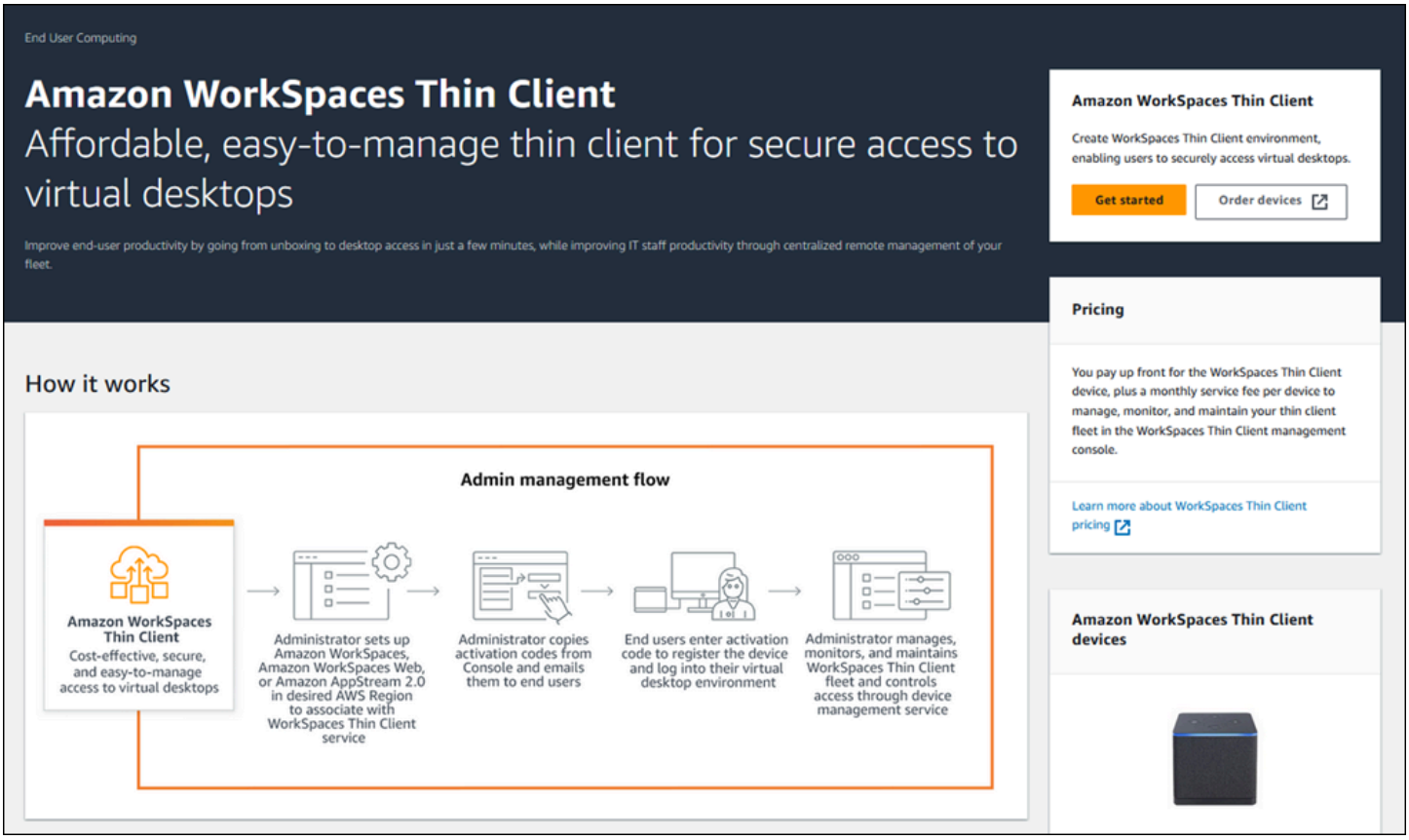
Nom de la région	Région	Point de terminaison	Lien vers la console
Europe (Irlande)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
Canada (Centre)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europe (Francfort)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europe (Londres)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

Lancement de la console d'administration WorkSpaces Thin Client

Lorsque vous avez un AWS compte, vous pouvez lancer la console d'administration et accéder à la console WorkSpaces Thin Client. Pour lancer la console, procédez comme suit :

1. Connectez-vous à votre AWS compte.
2. Accédez à la console WorkSpaces Thin Client.
3. Sélectionnez Premiers pas et vous serez dirigé vers Environnements.

Utilisation de la console d'administration WorkSpaces Thin Client



Bienvenue sur la console d'administration de WorkSpaces Thin Client !

À partir de là, vous pouvez gérer votre parc d'appareils et d'environnements WorkSpaces Thin Client pour votre équipe.

Pour plus d'informations concernant le dispositif WorkSpaces Thin Client, reportez-vous au Guide de l'utilisateur du WorkSpaces Thin Client.

C'est parti !

Rubriques

- Environnements
- Appareils
- Mises à jour de logiciels

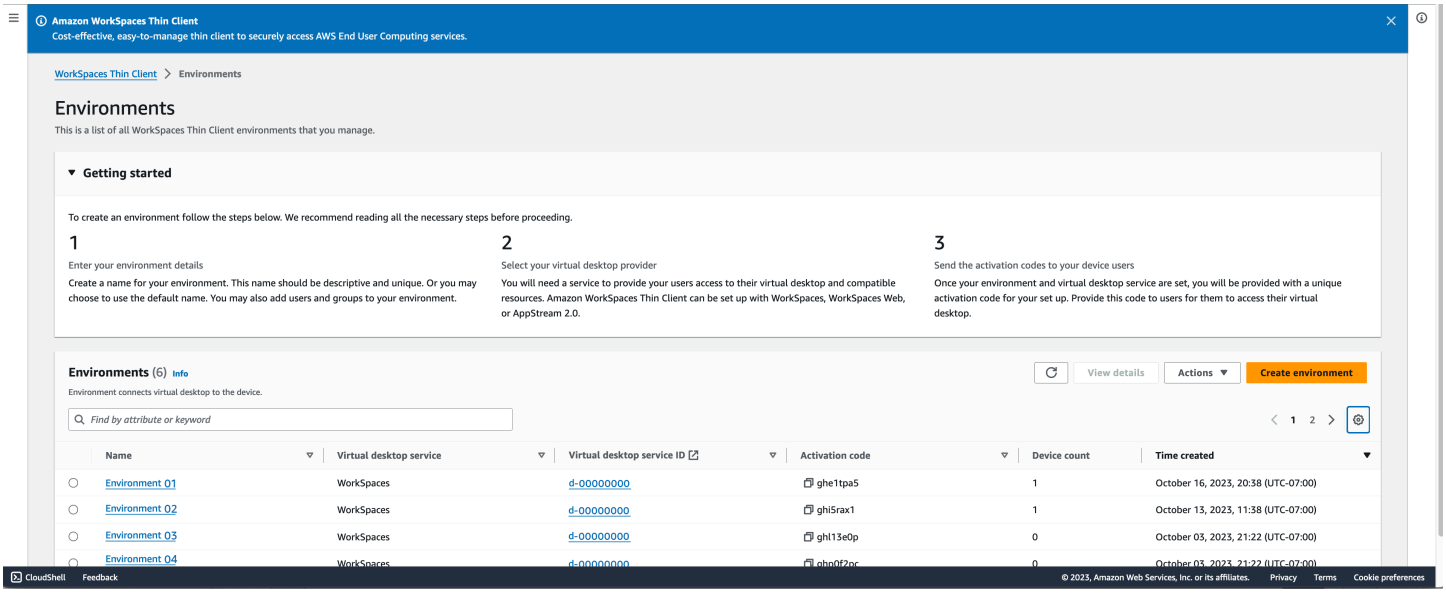
Environnements

Chaque appareil WorkSpaces Thin Client utilise un environnement de bureau virtuel individuel pour accéder à ses ressources en ligne. Les utilisateurs accèdent à cet environnement en utilisant l'un des fournisseurs de bureaux virtuels suivants :

- Amazon WorkSpaces
- AppStream 2.0
- Navigateur Amazon WorkSpaces Secure

Liste des environnements

Vous devez passer en revue un certain nombre de paramètres de votre environnement, ainsi que certaines mesures que vous pouvez prendre.



Informations contenues dans la liste des environnements

Les paramètres de votre environnement sont répertoriés pour votre examen. Le tableau suivant répertorie chaque élément du résumé et son fonctionnement.

Element	Description
Nom	Identifiant unique associé à cet environnement.

Element	Description
Service de bureau virtuel	Le fournisseur de bureau virtuel utilisé par cet environnement.
ID du service de bureau virtuel	Identifiant unique attribué par le fournisseur de services de bureau virtuel à cet environnement.
Code d'activation	Code utilisé par les utilisateurs finaux pour accéder à l'environnement de bureau virtuel.
Nombre d'appareils	Nombre de périphériques WorkSpaces Thin Client qui accèdent à cet environnement.
Heure de création	Date et heure de création de l'environnement.

Actions contenues dans la liste des environnements

Vous pouvez effectuer un certain nombre d'actions à partir d'ici. Sélectionnez l'une de ces options pour effectuer l'action correspondante.

Element	Description
Search	Effectue des recherches dans tous les environnements que vous gérez.
Actualiser	Actualise la liste des environnements.
View details (Afficher les détails)	Affiche les détails de l'environnement.
Actions	Ouvre une liste déroulante dans laquelle vous pouvez modifier ou supprimer un environnement.
Créer un environnement	Lance le processus de création d'un environnement.

Rubriques

- Détails de l'environnement
- Création d'un environnement
- Modification d'un environnement
- Suppression d'un environnement

Détails de l'environnement

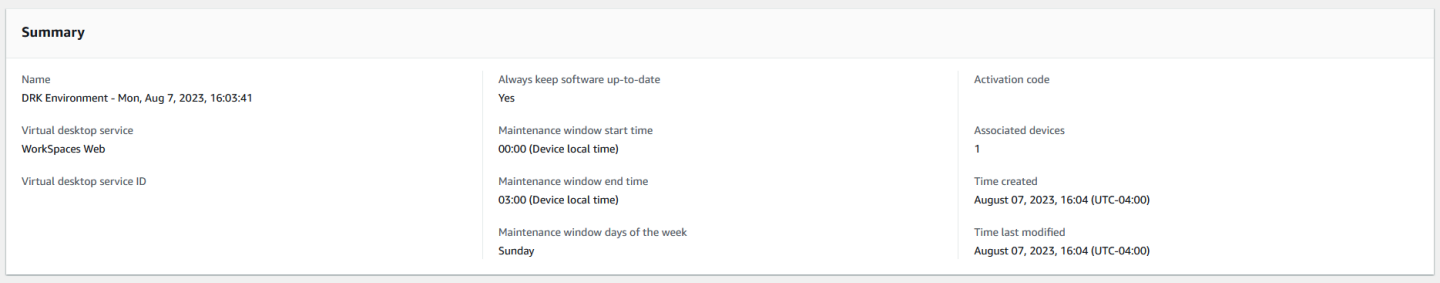
Lorsque vous sélectionnez un environnement, la console WorkSpaces Thin Client affiche les détails de cet environnement pour que vous puissiez les consulter. La console affiche également les informations relatives au fournisseur de bureau virtuel utilisé par cet environnement.

Rubriques

- Récapitulatif
- Détails sur l'environnement du bureau virtuel

Récapitulatif

La section Résumé fournit une vue d'ensemble des principales fonctionnalités de l'environnement WorkSpaces Thin Client. Le tableau suivant répertorie chaque élément du résumé et son fonctionnement.



Element	Description
Nom	Identifiant unique associé à cet environnement.
Service de bureau virtuel	Le fournisseur de bureau virtuel utilisé par cet environnement.
Nom du service de bureau virtuel	Identifiant unique attribué par le fournisseur de services de bureau virtuel à cet environnement.

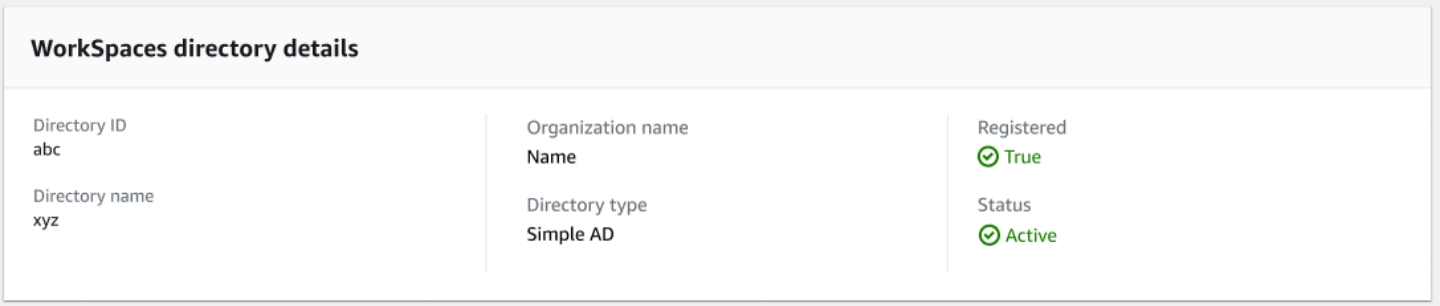
Element	Description
Code d'activation	Ce code est utilisé par les utilisateurs finaux pour accéder à l'environnement de bureau virtuel.
Conservez toujours le logiciel up-to-date	Ce paramètre active les mises à jour logicielles automatiques.
Heure de début de la fenêtre de maintenance	Heure à laquelle les mises à jour logicielles automatiques commencent chaque semaine.
Heure de fin de la fenêtre de maintenance	Heure hebdomadaire à laquelle les mises à jour logicielles automatiques se terminent.
Fenêtre de maintenance les jours de la semaine	Les jours où les mises à jour logicielles automatiques ont lieu.
Appareils associés	Nombre de périphériques WorkSpaces Thin Client qui accèdent à cet environnement.
Heure créée	Date et heure de création de cet environne ment.

Détails sur l'environnement du bureau virtuel

WorkSpaces Les environnements Thin Client sont exécutés sur une interface de bureau virtuel. Chaque interface possède un ensemble différent de paramètres qui contrôlent l'environnement dédié.

Informations sur l' WorkSpaces annuaire Amazon

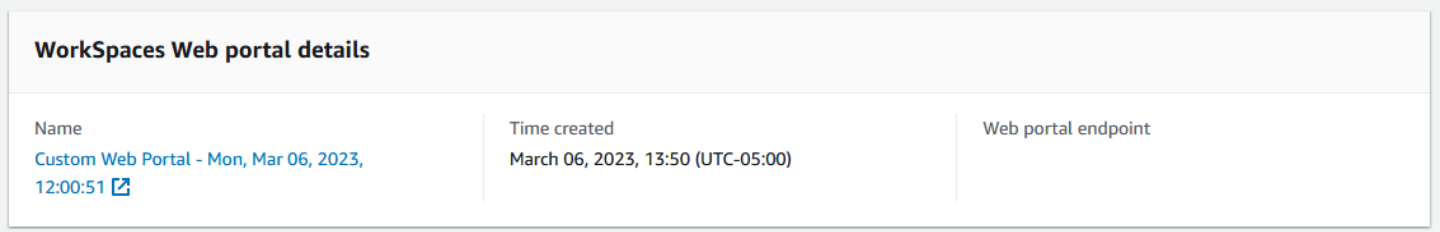
WorkSpaces Les environnements Thin Client exécutés sur Amazon WorkSpaces utilisent des annuaires pour créer et exécuter leurs bureaux virtuels. Le tableau suivant répertorie chaque élément dans ses détails et indique comment il fonctionne.



Element	Description
ID de l'annuaire	Le WorkSpaces répertoire Amazon associé à cet environnement.
Nom du répertoire	L'identifiant unique associé à cet WorkSpaces annuaire Amazon.
Nom de l'organisation	Le nom de l'organisation qui contrôle le WorkSpaces répertoire Amazon.
Type de répertoire	Format de l' WorkSpaces annuaire Amazon.
Membre	Si cet WorkSpaces annuaire Amazon est enregistré.
Statut	Si cet WorkSpaces annuaire Amazon est actif.

Détails du portail Amazon WorkSpaces Secure Browser

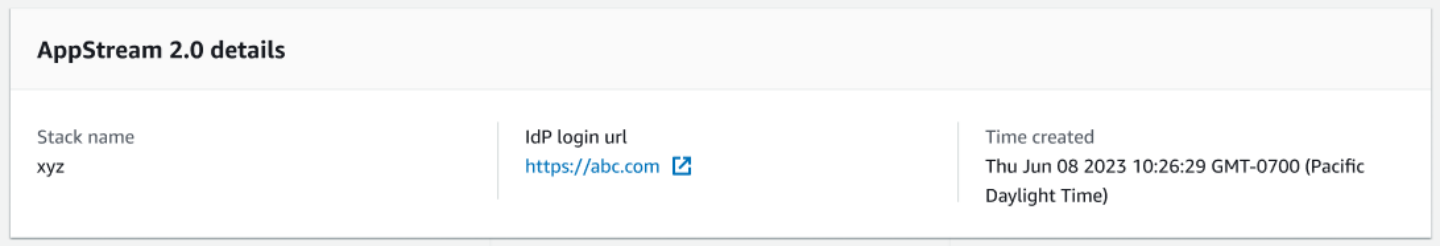
WorkSpaces Les environnements Thin Client exécutés sur Amazon WorkSpaces Secure Browser utilisent des portails Web pour créer et exécuter leurs bureaux virtuels. Le tableau suivant répertorie chaque élément dans ses détails et indique comment il fonctionne.



Element	Description
Nom	Identifiant unique associé à ce portail WorkSpaces Secure Browser.
Heure créée	Date et heure de création de ce portail WorkSpaces Secure Browser.
Point de terminaison du portail web	URL utilisée pour accéder à votre environne ment de bureau virtuel.

AppStream Détails de la version 2.0

WorkSpaces Les environnements Thin Client s'exécutent sur des piles d'informations AppStream 2.0 pour créer et exécuter leurs bureaux virtuels. Le tableau suivant répertorie chaque élément dans ses détails et indique comment il fonctionne.



Element	Description
Nom de la pile	Identifiant unique associé à cette pile AppStream 2.0.
URL de connexion à l'IdP	URL du fournisseur d'identité utilisée pour vous connecter et vous déconnecter de votre stack AppStream 2.0.
Heure créée	Date et heure de création de cette pile AppStream 2.0.

Création d'un environnement

Pour commencer, chaque appareil nécessite un service informatique pour l'utilisateur AWS final. WorkSpaces Thin Client utilise les services suivants :

- Amazon WorkSpaces via un répertoire attribué
- AppStream 2.0 via une pile assignée
- Amazon WorkSpaces Secure Browser via une adresse de portail Web

Vous devez attribuer un service à un environnement existant ou en créer un nouveau.

> **Note**
>
> WorkSpaces Thin Client affiche uniquement les bureaux virtuels de la même région.

Rubriques

- Étape 1 : saisissez les détails de votre environnement
- Étape 2 : sélectionnez votre fournisseur de bureau virtuel
- Étape 3 : envoyer le code d'activation aux utilisateurs de votre appareil

Étape 1 : saisissez les détails de votre environnement

1. Saisissez un nom pour votre environnement dans le champ Détails de l'environnement.
2. Pour configurer les correctifs logiciels automatiques, cochez la case Toujours conserver les logiciels up-to-date.

> **Note**
>
> Si les mises à jour logicielles automatiques ne sont pas activées, les appareils enregistrés dans cet environnement ne recevront pas de mises à jour logicielles tant que vous n'aurez pas effectué la mise à jour manuellement ou lorsque le logiciel arrivera à expiration et que le système force une mise à jour.
> De plus, la version du logiciel de l'appareil est déterminée par le système. Cette version n'est peut-être pas la plus récente.

3. Sélectionnez le moment où vous souhaitez planifier la fenêtre de maintenance pour votre environnement.

   - Appliquer une fenêtre de maintenance à l'échelle du système - Met automatiquement à jour le logiciel d'environnement à une heure déterminée chaque semaine.
   - Appliquer une fenêtre de maintenance personnalisée : définissez le jour et l'heure auxquels vous souhaitez que l'environnement logiciel soit mis à jour chaque semaine.

4. Sélectionnez un service de bureau virtuel.

   - Amazon WorkSpaces
   - Navigateur Amazon WorkSpaces Secure
   - AppStream 2.0

Étape 2 : sélectionnez votre fournisseur de bureau virtuel

Vous devez disposer d'un service permettant à vos utilisateurs d'accéder à leur bureau virtuel et à des ressources compatibles.

> **Important**
>
> Pour que la console WorkSpaces Thin Client Administrator fonctionne correctement, votre système doit répondre à des exigences spécifiques. Ces exigences sont répertoriées dans Prérequis et configurations.
> Assurez-vous que votre système répond à ces exigences avant de configurer votre console.

Utilisation d'Amazon WorkSpaces

Amazon WorkSpaces est un service de virtualisation de bureau entièrement géré pour Windows qui vous permet d'accéder aux ressources depuis n'importe quel appareil compatible.

1. Pour utiliser Amazon WorkSpaces, effectuez l'une des opérations suivantes :

   - Sélectionnez le répertoire que vous souhaitez utiliser pour votre environnement. Vous pouvez parcourir la liste déroulante ou effectuer une recherche dans les annuaires à l'aide du champ de recherche.

- Créez un répertoire en sélectionnant le bouton Créer un WorkSpaces répertoire. Pour plus d'informations sur la création de WorkSpaces répertoires, voir Gérer les annuaires pour WorkSpaces.

2. Cliquez sur le bouton Créer un environnement.

Lorsque vous créez votre environnement, vous pouvez toujours modifier les détails ultérieurement. Pour plus d'informations, consultez Modification d'un environnement.

Utilisation de la AppStream version 2.0

AppStream 2.0 est un service de streaming d'applications sécurisé et entièrement géré que vous pouvez utiliser pour diffuser des applications AWS de bureau depuis un navigateur Web.

> **Important**
>
> Pour créer un environnement AppStream 2.0, vous devez avoir `cli_follow_urlparam` défini sur`false`. Pour ce faire, procédez comme suit :
>
> - Pour un profil par défaut, exécutez `aws configure set cli_follow_urlparam false`.
> - Pour un profil avec un nom `ProfileName`, exécutez `aws configure set cli_follow_urlparam false --profile ProfileName`.

1. Pour configurer la AppStream version 2.0, effectuez l'une des opérations suivantes :

   - Sélectionnez la pile que vous souhaitez utiliser pour votre environnement. Vous pouvez soit parcourir la liste déroulante, soit effectuer une recherche dans les piles en utilisant le champ de recherche.
   - Créez une pile en sélectionnant le bouton Créer une pile. Pour plus d'informations sur la création de piles AppStream 2.0, consultez la section Créer une pile.

2. Saisissez les URL de connexion et de déconnexion de votre fournisseur d'identité dans le champ URL de connexion à l'IdP. Cela permet aux utilisateurs de se connecter et de se déconnecter de WorkSpaces Thin Client.
3. Cliquez sur le bouton Créer un environnement.

Après avoir créé votre environnement, vous pouvez toujours modifier les détails ultérieurement. Pour plus d'informations, consultez Modification d'un environnement.

Utilisation d'Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser est une WorkSpaces console peu coûteuse et entièrement gérée conçue pour fournir aux utilisateurs des charges de travail Web sécurisées et un accès aux applications SaaS (Software as a Service) dans les navigateurs Web existants.

1. Pour configurer Amazon WorkSpaces Secure Browser, effectuez l'une des opérations suivantes :
   - Sélectionnez le portail Web que vous souhaitez utiliser pour votre environnement. Vous pouvez parcourir la liste déroulante ou effectuer une recherche sur les portails Web à l'aide du champ de recherche.
   - Créez un portail Web en sélectionnant le bouton Créer un navigateur WorkSpaces sécurisé. Pour plus d'informations sur la création de portails Web WorkSpaces Secure Browser, consultez Configuration d'Amazon WorkSpaces Secure Browser.
2. Cliquez sur le bouton Créer un environnement.

Après avoir créé votre environnement, vous pouvez toujours modifier les détails ultérieurement. Pour plus d'informations, consultez Modification d'un environnement.

Étape 3 : envoyer le code d'activation aux utilisateurs de votre appareil

Après avoir configuré votre environnement et votre service de bureau virtuel, vous recevrez un code d'activation unique pour votre configuration sur la console AWS de gestion.

Fournissez ce code d'activation à n'importe quel utilisateur d'appareil WorkSpaces Thin Client, et il pourra l'utiliser pour accéder à son bureau virtuel.

Consultez le guide de l'utilisateur du client WorkSpaces léger pour plus d'informations sur la manière d'aider l'utilisateur de votre appareil à configurer son Amazon WorkSpaces Thin Client.

Modification d'un environnement

La console d'administration WorkSpaces Thin Client gère les environnements de bureau virtuels pour les utilisateurs individuels. À partir de cette console, vous pouvez modifier ou supprimer des environnements de bureau virtuels.

1. Sélectionnez l'environnement que vous souhaitez modifier.

   > **Note**
   >
   > Vous pouvez parcourir la liste déroulante ou effectuer une recherche dans les environnements à l'aide du champ de recherche.

2. Sélectionnez le bouton Actions.
3. Sélectionnez Modifier dans la liste déroulante. Vous serez dirigé vers la fenêtre Modifier l'environnement.
4. Modifiez l'un des éléments suivants :

   - Modifiez le nom de votre environnement dans le champ Nom de l'environnement.
   - Cochez la case correspondant aux détails des mises à jour logicielles pour les mises à jour automatiques des correctifs logiciels.
   - Modifiez le moment où vous souhaitez planifier la fenêtre de maintenance pour votre environnement.

5. Cliquez sur le bouton Modifier l'environnement.

Suppression d'un environnement

> **Note**
>
> Vous ne pouvez pas supprimer un environnement si des appareils y sont enregistrés. Tout d'abord, vous devez annuler l'inscription et supprimer tous les appareils d'un environnement.

1. Sélectionnez l'environnement que vous souhaitez supprimer. Vous pouvez parcourir la liste déroulante ou effectuer une recherche dans les environnements à l'aide du champ de recherche.
2. Sélectionnez le bouton Actions.
3. Sélectionnez Supprimer dans la liste déroulante. La fenêtre de confirmation de la suppression de l'environnement apparaît.
4. Saisissez « supprimer » dans le champ de confirmation.
5. Sélectionnez le bouton Supprimer.

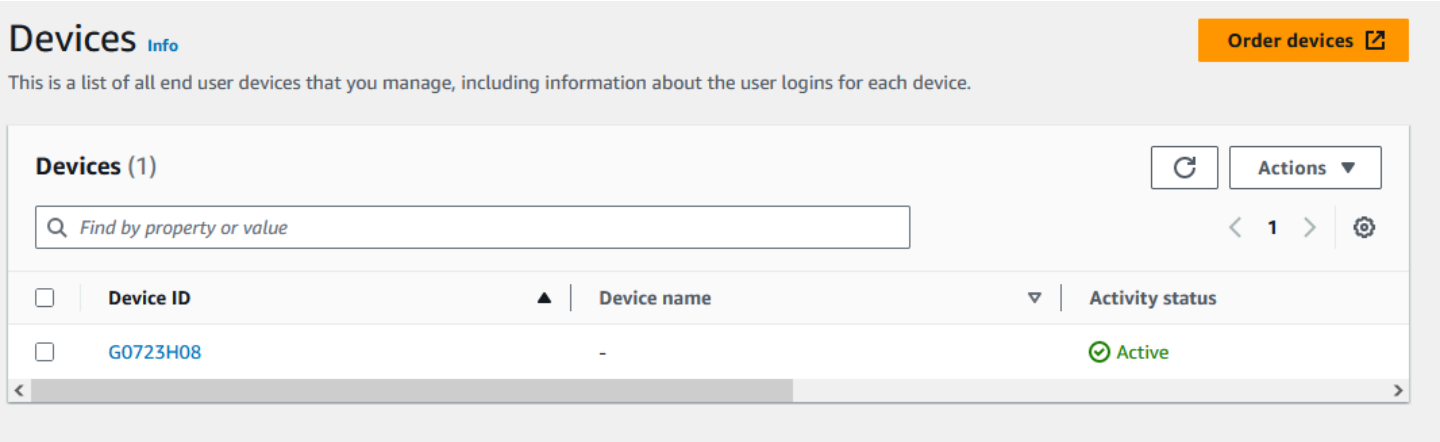
Appareils

Chaque utilisateur final de WorkSpaces Thin Client dispose d'un appareil dédié qui le connecte à ses environnements de bureau virtuels et à ses ressources en ligne. Ces appareils sont gérés via la console d'administration WorkSpaces Thin Client sur le AWS site.

À partir de cette console, vous pouvez commander des appareils pour votre équipe.

Liste des périphériques

Vous devez passer en revue un certain nombre de paramètres pour chaque appareil de votre réseau, ainsi que certaines mesures que vous pouvez prendre.



Informations contenues dans la liste des appareils

Les paramètres de votre appareil sont répertoriés à des fins de vérification. Le tableau suivant répertorie chaque élément du résumé et son fonctionnement.

Element	Description
Numéro de série de l'appareil	Numéro d'identification attribué à un appareil individuel.
Nom d’appareil	(facultatif) Le nom unique que vous attribuez à un appareil.
Dernière utilisation par	Le numéro d'identification de l'utilisateur accédant à l'appareil. Disponible uniquement lors de l'utilisation de WorkSpaces Personal.

Element	Description
État de l'activité	État actuel d'un appareil. Il existe deux états de statut : • Actif : connecté à un réseau au moins une fois au cours des sept derniers jours. • Inactif — Non connecté à un réseau au cours des sept derniers jours.
Statut d'inscription	Confirmation qu'un appareil a été configuré, qu'il est associé à ce compte AWS et qu'il fait partie d'un environnement spécifique. Il peut se trouver dans l'un des états suivants : • Enregistré — Il s'agit du statut par défaut. • Désenregistrement — L'appareil est en cours de réinitialisation et de désenregistrement. **Note** Vous pouvez supprimer un appareil s'il est en cours de désenregi strement. • Désenregistré — L'appareil a été désenregi stré avec succès. **Note** Vous ne pouvez supprimer un appareil que s'il est en état de désenregistrement ou de désenregi strement. • Archivé — L'appareil est archivé.

Element	Description
ID de l'environnement	Identifiant de l'environnement auquel ce périphérique est connecté.
Conformité logicielle	État de conformité du logiciel de l'appareil. Il existe deux états de statut : • Conforme • Non conforme

Actions contenues dans la liste des appareils

Vous pouvez effectuer un certain nombre d'actions à partir d'ici. Sélectionnez l'une de ces options pour effectuer l'action correspondante.

Element	Description
Search	Effectue des recherches sur tous les appareils que vous gérez.
Actualiser	Actualise la liste des appareils.
View details (Afficher les détails)	Affiche les détails de l'appareil.
Actions	Ouvre une liste déroulante dans laquelle vous pouvez effectuer les opérations suivantes : • Modifier le nom de l'appareil • Désenregistrer • Archivage • Suppression • Exporter les détails de l'appareil
Commander des appareils	Démarre le processus de commande des appareils.

Rubriques

- Détails de l'appareil
- Modification du nom d'un appareil
- Réinitialisation et annulation de l'inscription d'un appareil
- Archivage d'un appareil
- Suppression d'un appareil
- Exportation des détails d'un appareil

Détails de l'appareil

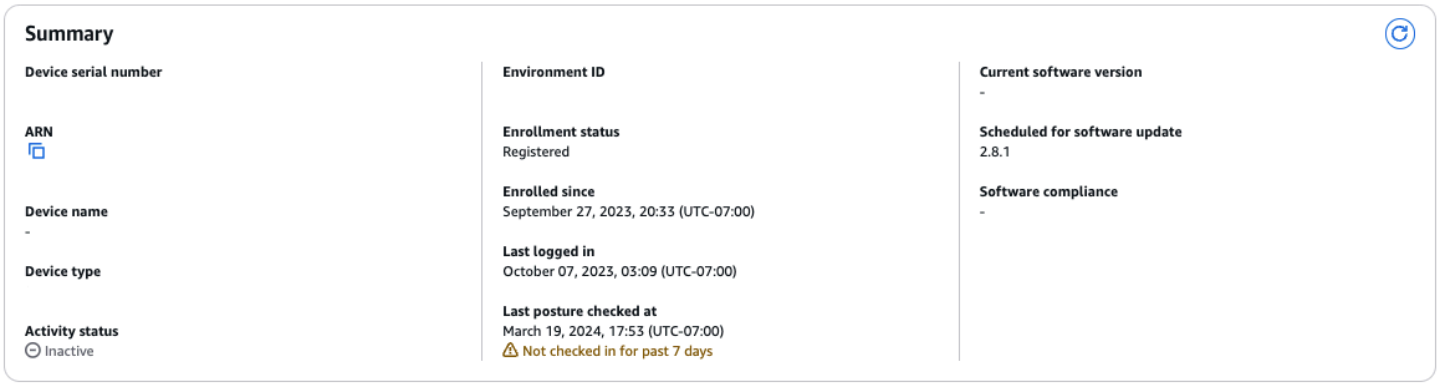
Lorsque vous sélectionnez un appareil, la console WorkSpaces Thin Client affiche les détails de cet appareil pour que vous puissiez les consulter. La console affiche également les détails relatifs au type de réseau de l'appareil et aux périphériques connectés.

Rubriques

- Récapitulatif
- Paramètres de l'appareil
- Activité de l'utilisateur

Récapitulatif

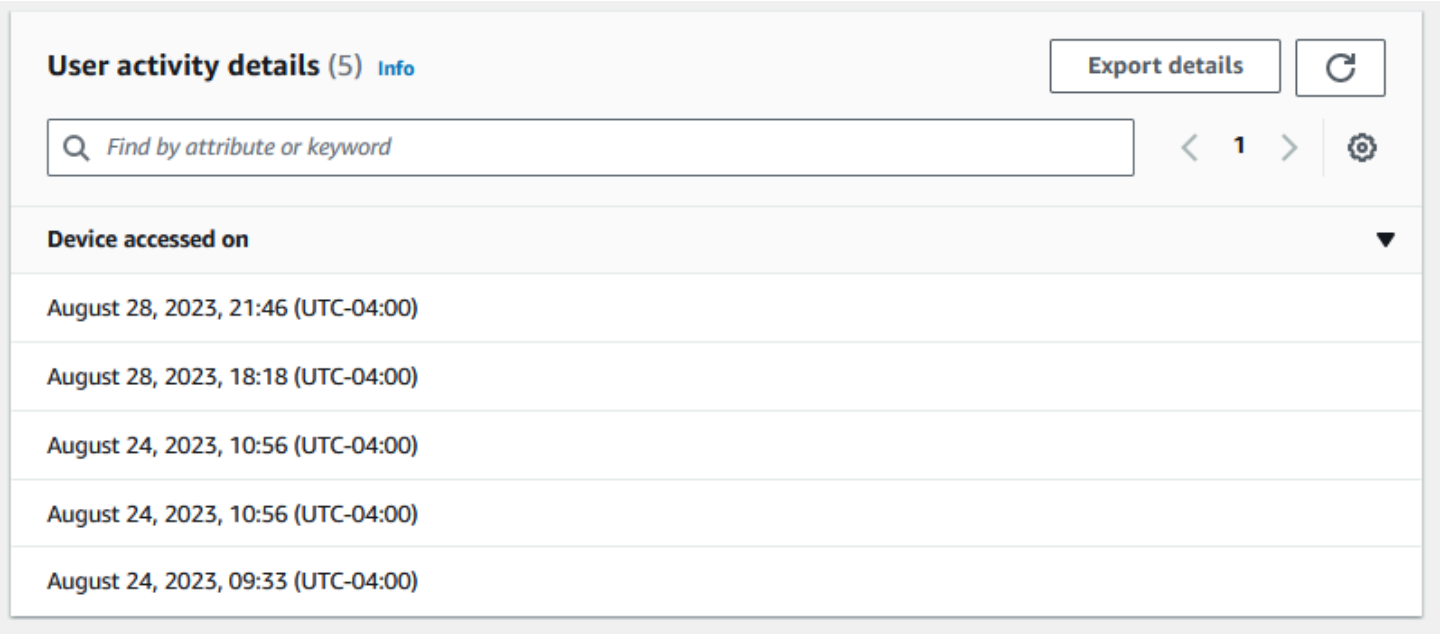
La section Résumé fournit une vue d'ensemble des principales fonctionnalités du dispositif WorkSpaces Thin Client. Le tableau suivant répertorie chaque élément du résumé et son fonctionnement.



Element	Description
Numéro de série de l'appareil	Numéro d'identification attribué à un appareil individuel.
ARN	L'identifiant unique de l'appareil au format Amazon Resource Name (ARN).
Nom d’appareil	Le nom que vous attribuez à un appareil. Si vous n'avez pas créé de nom, vous pouvez le nommer, ou il recevra un nom par défaut.
Type d'appareil	Type d'appareil de l'utilisateur final associé au compte.
État de l'activité	État actuel de cet appareil. Les deux états de statut sont les suivants : • Actif • Inactif
ID de l'environnement	Numéro d'identification de l'environnement utilisé par l'appareil.
Statut d'inscription	Confirmation qu'un appareil a été configuré, qu'il est associé à ce compte AWS et qu'il fait partie d'un environnement spécifique. Il peut se trouver dans l'un des quatre états suivants : • Enregistré — Il s'agit du statut par défaut. • Désenregistrement — L'appareil est en cours de réinitialisation et de désenregistrement. • Désenregistré — L'appareil a été désenregi stré avec succès.

Element	Description
	- Note Vous ne pouvez supprimer l'appareil que s'il est désenregistré ou archivé. - Archivé — Cet appareil a été marqué par l'administrateur comme n'étant pas actuellement en service.
Inscrit depuis	Date à laquelle l'appareil a été activé.
Dernière connexion	Date et heure de la dernière connexion.
Dernière posture vérifiée à	Date et heure du dernier enregistrement de l'appareil.
Version actuelle du logiciel	Version logicielle actuellement utilisée par cet appareil.
Mise à jour logicielle planifiée	Version logicielle planifiée sur l'appareil.
Conformité logicielle	Confirmation de la validité du jeu de logiciels. Il existe deux états de statut : - Conforme - Non conforme
Dernière utilisation par	Le numéro d'identification de l'utilisateur accédant à l'appareil. Disponible uniquement lors de l'utilisation de WorkSpaces Personal.

Journal utilisateur



Element	Description
Dernier accès à l'appareil	Date et heure de dernière utilisation de cet appareil.

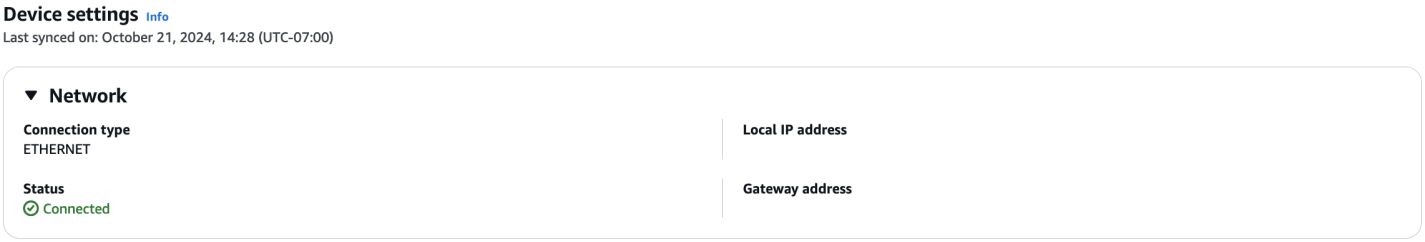
Paramètres de l'appareil

Les paramètres de votre appareil sont répertoriés à des fins de vérification. Le tableau suivant répertorie chaque élément et son fonctionnement.

> **Note**
>
> Les informations relatives aux paramètres de l'appareil sont mises à jour uniquement lorsque l'appareil est en ligne. Si l'appareil est hors ligne, il est possible que certaines informations ne soient plus à jour.

Titre et réseau

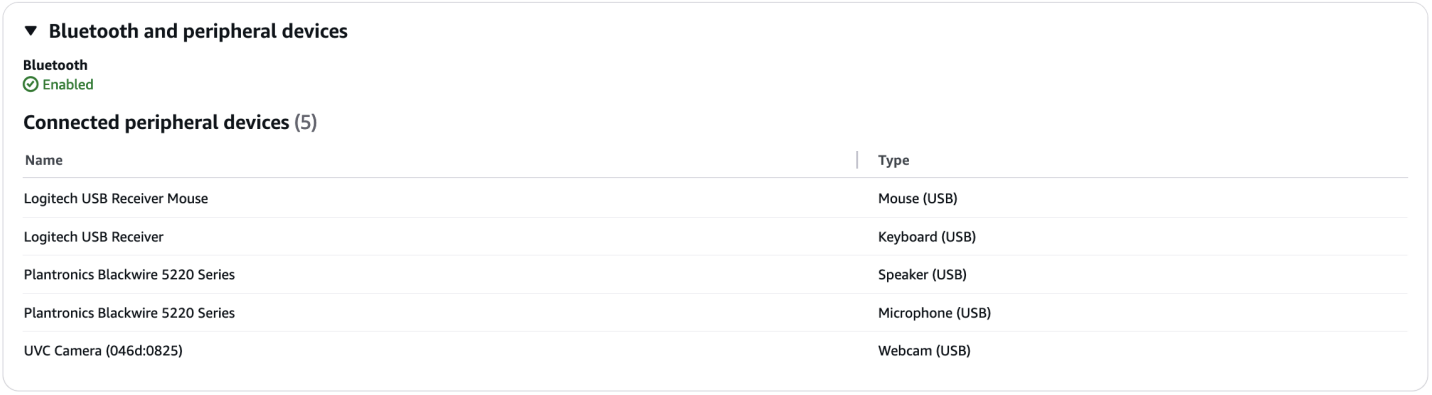
WorkSpaces Les détails du périphérique Thin Client fournissent une vue d'ensemble des connexions réseau de l'appareil. Le tableau suivant répertorie chaque élément et son fonctionnement.



Element	Description
Dernière synchronisation le	La date et l'heure des derniers paramètres de l'appareil sont synchronisés avec la console.
Type de connexion	Type de connexion réseau utilisé par l'apparei l. Le type de connexion peut être Ethernet ou Wifi.
Statut	État du réseau. Si l'appareil est actuellement connecté, ou s'il s'est connecté au cours des 20 dernières minutes, le statut sera affiché comme « connecté ». Si le réseau est déconnecté depuis plus de 20 minutes, l'état changera pour indiquer le temps écoulé depuis la dernière connexion de l'appareil à Internet, par exemple « dernière connexion il y a 20 minutes ».
Adresse IP locale	Adresse IP locale du réseau connecté.
Adresse de passerelle	Adresse de passerelle du réseau connecté.

Bluetooth et périphériques

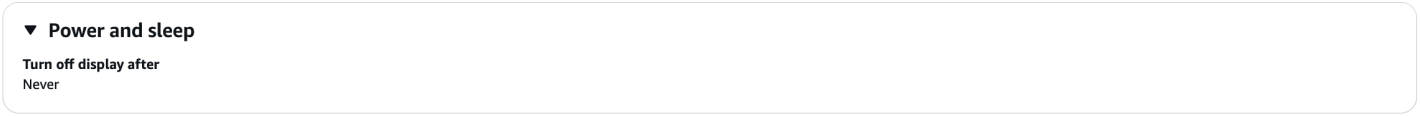
WorkSpaces Les détails de l'appareil Thin Client fournissent une liste de tous les périphériques connectés à un appareil. Le tableau suivant répertorie chaque élément et son fonctionnement.



Element	Description
Bluetooth	État Bluetooth de l'appareil. Les deux états de statut sont les suivants : • Activé • Désactivées
Appareils périphériques connectés	La liste des noms des périphériques connectés , tels que la souris Logitech, et le type de périphériques connectés, tels que Mouse (USB).

Alimentation et sommeil

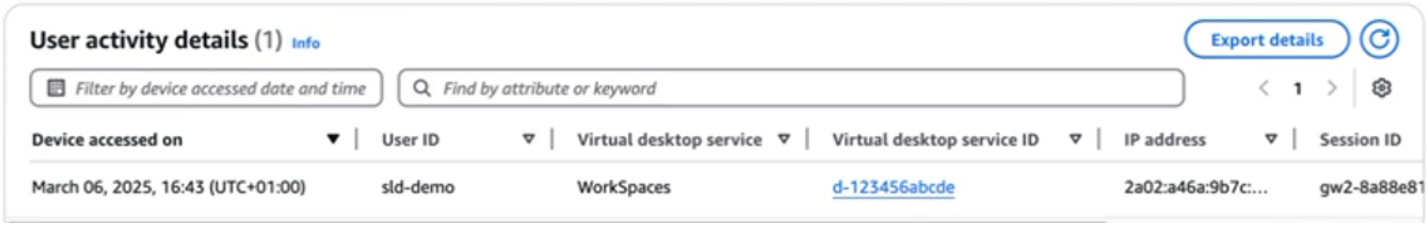
Chaque appareil WorkSpaces Thin Client dispose d'un mode d'économie d'énergie. Le tableau suivant répertorie l'état de ce mode.



Element	Description
Éteindre l'affichage après	Période d'inactivité après laquelle l'appareil éteint son écran.

Activité de l'utilisateur

Cet onglet affiche le journal des informations de configuration et d'utilisation d'un appareil spécifique. Le tableau suivant répertorie chaque élément de ce journal.



Element	Description
Appareil auquel on a accédé sur	Date et heure d'activation de l'appareil.
ID de l'utilisateur	Le numéro d'identification de l'utilisateur accédant à l'appareil.
Service de bureau virtuel	Le service de bureau virtuel utilisé par l'apparei l.
ID du service de bureau virtuel	Numéro d'identification du service de bureau virtuel associé à l'utilisateur.
Adresse IP	Le numéro d'identification de l'adresse IP accédant à l'appareil.
Type d'événement	Informations sur la façon dont l'appareil est utilisé.

> **Note**
>
> À l'exception de WorkSpaces Personal, VDIs n'afficher qu'un événement initié par la connexion.

Vous pouvez utiliser la barre de recherche située au-dessus du tableau pour trouver des informations spécifiques dans le tableau. Vous pouvez également filtrer les résultats du tableau par date et heure.

Vous pouvez exporter le tableau vers un fichier CSV en cliquant sur le bouton Exporter les détails.

Modification du nom d'un appareil

1. Sélectionnez l'appareil que vous souhaitez modifier. Vous pouvez soit parcourir la liste déroulante, soit rechercher un appareil en utilisant le champ de recherche.
2. Sélectionnez le bouton Actions.
3. Sélectionnez Modifier le nom de l'appareil dans la liste déroulante. La fenêtre Modifier le nom de l'appareil apparaît.
4. Saisissez le nouveau nom de l'appareil dans le champ de confirmation Nom de l'appareil.
5. Sélectionnez le bouton Enregistrer.

Réinitialisation et annulation de l'inscription d'un appareil

1. Sélectionnez l'appareil pour lequel vous souhaitez annuler l'inscription. Vous pouvez soit parcourir la liste déroulante, soit rechercher l'appareil en utilisant le champ de recherche.
2. Sélectionnez le bouton Actions.
3. Sélectionnez Désenregistrer dans la liste déroulante. La fenêtre Désenregistrer apparaît.
4. Saisissez « annuler l'inscription » dans le champ de confirmation.
5. Sélectionnez le bouton Annuler l'inscription.

> **Note**
>
> Le désenregistrement entraîne la déconnexion forcée de l'utilisateur et nécessite le redémarrage de son appareil WorkSpaces Thin Client au milieu d'une session.

Archivage d'un appareil

1. Sélectionnez l'appareil que vous souhaitez archiver. Vous pouvez soit parcourir la liste déroulante, soit rechercher l'appareil en utilisant le champ de recherche.
2. Sélectionnez le bouton Actions.
3. Sélectionnez Archiver dans la liste déroulante. La fenêtre Archive apparaît.
4. Saisissez « réinitialiser et archiver » dans le champ de confirmation.

5. Sélectionnez le bouton Réinitialiser et archiver.

> **Note**
>
> L'archivage d'un appareil déconnecte de force l'utilisateur et nécessite le redémarrage de son appareil WorkSpaces Thin Client au milieu d'une session.

Suppression d'un appareil

1. Sélectionnez l'appareil que vous souhaitez supprimer. Vous pouvez soit parcourir la liste déroulante, soit rechercher l'appareil en utilisant le champ de recherche.
2. Sélectionnez le bouton Actions.
3. Sélectionnez Supprimer dans la liste déroulante. La fenêtre Supprimer apparaît.
4. Saisissez « supprimer » dans le champ de confirmation.
5. Sélectionnez le bouton Supprimer.

Exportation des détails d'un appareil

1. Sélectionnez l'appareil à partir duquel vous souhaitez exporter les détails. Vous pouvez soit parcourir la liste déroulante, soit rechercher l'appareil en utilisant le champ de recherche.
2. Sélectionnez le bouton Actions.
3. Sélectionnez Exporter les détails de l'appareil dans la liste déroulante. Les informations relatives à l'appareil sélectionné sont téléchargées sous forme de feuille de calcul.

Mises à jour de logiciels

WorkSpaces Thin Client nécessite parfois des mises à jour logicielles qui introduisent de nouvelles fonctionnalités et appliquent des correctifs de sécurité. Ces mises à jour sont représentées par un ensemble de logiciels versionnés.

Un ensemble de logiciels peut contenir des mises à jour des applications logicielles ou du système d'exploitation du dispositif WorkSpaces Thin Client. À partir de cette console, vous pouvez choisir de mettre à jour le logiciel immédiatement ou de planifier une mise à jour automatique pendant la fenêtre de maintenance des environnements.

Reportez-vous à la section Ensembles logiciels de l'environnement WorkSpaces Thin Client pour obtenir la liste des ensembles logiciels publiés.

Rubriques

- Mise à jour de l'environnement logiciel
- Mise à jour du logiciel de l'appareil
- WorkSpaces Versions du logiciel Thin Client

Mise à jour de l'environnement logiciel

WorkSpaces Thin Client est un service informatique destiné aux utilisateurs AWS finaux qui permet aux utilisateurs d'accéder à des bureaux virtuels. Ces bureaux virtuels sont régulièrement mis à jour avec de nouveaux ensembles logiciels. Pour mettre à jour le logiciel d'environnement, procédez comme suit :

1. Sélectionnez le logiciel dans la liste Mises à jour logicielles disponibles. Pour obtenir la liste des ensembles logiciels, reportez-vous à la section Ensembles logiciels de l'environnement WorkSpaces Thin Client.
2. Cliquez sur le bouton Installer.
3. Sélectionnez Environnements en haut de la page.
4. Sélectionnez l'environnement à mettre à jour dans la liste de la section Environnements.
5. Sélectionnez le moment où vous souhaitez mettre à jour de l'environnement dans la section Planifier la mise à jour en choisissant l'une des options suivantes :

   - Mettre à jour le logiciel maintenant : démarre la mise à jour de l'environnement logiciel sur tous les appareils enregistrés.

     > **Note**
     >
     > La mise à jour du logiciel peut désormais interrompre toute session utilisateur active.

   - Mettre à jour le logiciel pendant la fenêtre de maintenance de chaque environnement : met à jour le logiciel d'environnement pendant la fenêtre de maintenance planifiée de l'environnement.
6. Cochez la case pour autoriser la mise à jour. Cette case doit être cochée pour que le logiciel soit mis à jour.

7. Sélectionnez le bouton Installer.

Mise à jour du logiciel de l'appareil

WorkSpaces Thin Client est un service informatique destiné aux utilisateurs AWS finaux qui fournit un appareil client léger qui connecte les utilisateurs à des bureaux virtuels dédiés. Ces appareils sont régulièrement mis à jour avec de nouveaux logiciels. Pour mettre à jour le logiciel de l'appareil, procédez comme suit :

1. Sélectionnez le logiciel dans la liste Mises à jour logicielles disponibles.
2. Sélectionnez le bouton Installer.
3. Sélectionnez Appareil en haut de la page.
4. Sélectionnez le ou les appareils à mettre à jour dans la liste de la section Appareils. Pour obtenir la liste des ensembles logiciels, reportez-vous à la section Ensembles logiciels de l'environnement WorkSpaces Thin Client.
5. Sélectionnez le moment où vous souhaitez mettre à jour de l'environnement dans la section Planifier la mise à jour en choisissant l'une des options suivantes :

   - Mettre à jour le logiciel maintenant : met immédiatement à jour le logiciel de l'appareil.

     > **Note**
     >
     > La mise à jour actuelle du logiciel peut interrompre toute session utilisateur active.

   - Mettre à jour le logiciel pendant la fenêtre de maintenance de chaque appareil : met à jour le logiciel d'environnement pendant la fenêtre de maintenance planifiée de l'appareil.
6. Cochez la case pour autoriser la mise à jour. Cette case doit être cochée pour que le logiciel soit mis à jour.
7. Sélectionnez le bouton Installer.

WorkSpaces Versions du logiciel Thin Client

WorkSpaces Thin Client est un service informatique destiné aux utilisateurs AWS finaux qui permet aux utilisateurs d'accéder à des bureaux virtuels sur un appareil. Ces appareils sont régulièrement mis à jour avec de nouveaux ensembles logiciels. Le tableau suivant décrit tous les ensembles de

logiciels publiés. Les administrateurs peuvent utiliser la console AWS de gestion pour consulter les ensembles de logiciels disponibles.

Set de logiciels	Date de publication	Modifications
2.17.0	30-7-2025	• Le hub USB enfichable UD-3900Z est désormais compatible avec Thin Client. WorkSpaces • Ajout du support pour les AltGr touches avec les claviers espagnols. • Correction du problème qui entraînait des entrées dupliquées pour l'activité de session utilisateur sur l'appareil. • Ajout du support pour la touche Entrée sur le clavier numérique. • Corrections et améliorations générales.
2.16,2	22-7-2025	• Correction du problème de sécurité critique CVE-2025-6558 de Chromium.
2.16.1	7-3-2025	• Correction du problème de sécurité critique CVE-2025-6554 de Chromium.
2.16.0	27/06/2025	• Notifications ajoutées pour la latence du réseau. • Ajout de la possibilité de récupérer si le deuxième moniteur s'assombrit pendant une session.

Set de logiciels	Date de publication	Modifications
		• Le problème lié au fait que les écrans affichaient un écran blanc ou ne s'étendai ent pas automatiquement une fois que l'appareil était sorti du mode veille a été résolu.
2.15.0	19/06/2025	• Ajout du support pour les claviers espagnols d'Amérique latine et anglais international. • Les utilisateurs finaux reçoivent des notifications lorsque l'appareil ne détecte pas l'activité du clavier ou de la souris pendant une période prolongée.
2.14.1	6-09-2025	• Correctif des problèmes de sécurité critiques liés au CVE-2025-5419 de Chromium.

Set de logiciels	Date de publication	Modifications
2.13.0	31-03-2025	• Les utilisateurs finaux verront l'enquête de satisfaction sur les produits sous forme de notification. • Ajoute la prise en charge des fonctionnalités d'avant-première pour le flux FIDO2 d'authentification. Voir les détails de FIDO2 pré-session. • L'appareil ne se mettra pas en veille audio/video s'il joue pendant la session. • Les utilisateurs finaux reçoivent des notifications lorsque le moniteur est connecté et déconnecté. • L'appareil collecte des informations de diagnostic à partir du système d'exploitation pour améliorer le service. • Résout un problème en raison duquel une date incorrecte était affichée dans les paramètres pour la date d'installation du logiciel.
2.14.0	29/04/2025	• Améliorations de l'utilisabilité et corrections de bogues.

Set de logiciels	Date de publication	Modifications
2.13.0	31-03-2025	• Les utilisateurs finaux verront l'enquête de satisfaction sur les produits sous forme de notification. • Ajoute la prise en charge des fonctionnalités d'avant-première pour le flux FIDO2 d'authentification. Voir les détails de FIDO2 pré-session. • L'appareil ne se mettra pas en veille audio/video s'il joue pendant la session. • Les utilisateurs finaux reçoivent des notifications lorsque le moniteur est connecté et déconnecté. • L'appareil collecte des informations de diagnostic à partir du système d'exploitation pour améliorer le service. • Résout un problème en raison duquel une date incorrecte était affichée dans les paramètres pour la date d'installation du logiciel.

Set de logiciels	Date de publication	Modifications
2.12.0	30-01-2025	• Résout un problème selon lequel l'utilisateur final était déconnecté de la session lorsqu'il appuyait sur le bouton de retour de la souris.
2.11.2	24-01-2025	• Résout un problème à cause duquel le son crépitait pendant les appels lorsque la souris bougeait d'un écran à l'autre.
2.11.1	27-12-2024	• Résout le problème d'extension automatique du double moniteur. • Améliorations mineures apportées à VoiceView l'étiquette.
2.11.0	19-12-2024	• WorkSpaces Thin Client prend désormais en charge VoiceView et Magnifier.
2.10.0	22-11-2024	• Les utilisateurs finaux peuvent utiliser un raccourci clavier pour réduire la barre d'outils de l'appareil.

Set de logiciels	Date de publication	Modifications
2.9.0	28-10-2024	• Les administrateurs peuvent désormais consulter les paramètres de l'appareil de leurs utilisateurs finaux dans AWS la console, sous la page des détails de l'apparei l d'un appareil spécifique. • WorkSpaces Thin Client prend désormais en charge un moniteur de résolution 2K pour un seul écran. • Les utilisateurs finaux peuvent voir les notifications relatives aux diagnostics du réseau sur leurs appareils WorkSpaces Thin Client. • L'utilisateur final peut désormais choisir de placer la barre d'outils de l'apparei l à gauche ou à droite selon ses préférences. • Correction d'un problème en raison duquel l'appareil n'installait pas les mises à jour logicielles pendant la période de veille ou d'inactiv ité.
2.8.1	26-09-2024	• Correction d'un problème critique à cause duquel le second moniteur ne pouvait pas être activé une fois que l'appareil était sorti du mode veille.

Set de logiciels	Date de publication	Modifications
2.8.0	09-06-2024	• Thin Client prend en charge les moniteurs dotés d'une résolution 4K. • Les utilisateurs peuvent se connecter à la session VDI même si les services de gestion des appareils WorkSpaces Thin Client sont temporairement indisponibles. • Correction d'un problème en raison duquel la section des détails de l'activité des utilisateurs de AWS la console affichait des entrées dupliquées. • Les utilisateurs finaux peuvent utiliser l' PrintScreen option lors du streaming WorkSpaces sur WorkSpaces Thin Client.
2.7.1	27-08-2024	• Corrections « zero-day » pour les problèmes de sécurité critiques relatifs aux CVE-2024-7971 et CVE-2024-7965 de Chromium.

Set de logiciels	Date de publication	Modifications
2.7.0	29/07/2024	• Améliorations des performances du deuxième moniteur. • Correction d'un problème en raison duquel la langue de la barre d'outils n'était pas affectée lors du changement de langue de l'appareil. • L'appareil collecte désormais des informations de diagnostic pour améliorer le service.
2.6.0	07-09-2024	• Les utilisateurs peuvent différer les mises à jour logicielles entrantes afin de pouvoir terminer leur travail sans interruption. • Les paramètres de l'appareil permettent aux utilisateurs d'oublier WiFi les réseaux enregistrés. • Améliorations des performances des audio/video appels pendant la session. • Certains paramètres utilisateur des sessions VDI sont conservés après le redémarrage de l'appareil.

Set de logiciels	Date de publication	Modifications
2.5.0	13/06/2024	• Correction d'un problème à cause duquel l'appareil affichait brièvement l'écran de configuration du clavier et de la souris au réveil avant le lancement de la session. • Le bouton Accueil de la barre d'outils de l'apparei l a été renommé en Se connecter. • Améliorations des performances des audio/ video appels pendant la session.
2.4.3	29/05/2024	• Solution « jour zéro » pour le problème de sécurité critique CVE-2024-5274 de Chromium.
2.4.2	17/05/2024	• Solution « jour zéro » pour le problème de sécurité critique CVE-2024-4947 de Chromium.

Set de logiciels	Date de publication	Modifications
2.4.1	15/05/2024	• Corrections « zero-day » pour les problèmes de sécurité critiques relatifs aux CVE-2024-4671 et CVE-2024-4761 de Chromium. • Le problème qui permettai t de cliquer avec le bouton droit sur les liens AWS et Privacy sur la page de WorkSpaces connexion pour ouvrir le navigateur en mode autonome a été résolu.
2.4.0	05-09-2024	• Correction d'un problème bloquant « accounts. google.com » et empêchant l'utilisation de Google Workspace comme IDP pour la session 2.0. AppStream • La barre d'outils des paramètres de l'appareil se réduit automatiquement en un clic dans n'importe quelle zone de l'écran.

Set de logiciels	Date de publication	Modifications
2.3.0	04-05-2024	• Les paramètres de l'appareil apparaissent dans une barre d'outils réduite permettant une meilleure utilisation de l'écran visible. • Les utilisateurs finaux peuvent désormais configurer la durée d'attente avant que l'appareil ne se mette en veille en cas d'inactivité. • Le problème d'affichage de l'URL « about:blank » sur le deuxième écran a été résolu. • Correction du problème qui provoquait un écran blanc lorsque l'affichage étendu était fermé. • Les niveaux de volume définis par les utilisateurs finaux sont désormais conservés après le redémarrage de l'appareil.
2.2.1	16/02/2024	• Correction d'un problème qui se produisait pendant le processus de connexion et qui empêchait les utilisateurs de se connecter à une connexion WorkSpaces configurée avec l'authentification SAML 2.0.

Set de logiciels	Date de publication	Modifications
2.2.0	02-08-2024	• Ajout du support pour les claviers ISO avec les langues anglaise (Royaume-Uni), française , allemande, italienne et espagnole.
2.1.2	26/01/2024	• Solution « jour zéro » pour le problème de sécurité critique CVE-2024-0519 de Chromium. • Amélioration de la latence de l'utilisateur final associée à la fonctionnalité de verrouillage. • Les points de terminaison internes orientés vers les appareils sont transférés vers le domaine « thinclien t* ».
2.1.1	21-12-2023	• Solution « jour zéro » pour le problème de sécurité critique CVE-2023-7024 de Chromium.
2.1.0	20-12-2023	• Ajoute un bouton d'accueil aux paramètres de l'apparei l et active la prise en charge des touches méta. Cela permet aux utilisateurs finaux d'invoquer l'écran de verrouillage en appuyant sur Meta+L.

Set de logiciels	Date de publication	Modifications
2.0.1	12-06-2023	• Solution « jour zéro » pour le problème de sécurité critique CVE-2024-6345 de Chromium.
2.0.0	15-11-2023	• Première version

Utilisation de balises sur les ressources WorkSpaces Thin Client

Vous pouvez organiser et gérer les ressources de votre client WorkSpaces léger en attribuant vos propres métadonnées à chaque ressource sous forme de balises. Vous spécifiez une clé et une valeur pour chaque balise. Une clé peut être une catégorie générale, comme un « projet », un « propriétaire » ou un « environnement » avec des valeurs associées spécifiques. Vous pouvez utiliser les balises comme moyen simple mais puissant de gérer les ressources AWS et d'organiser les données, y compris les données de facturation.

Lorsque vous ajoutez des balises à une ressource existante, elles n'apparaissent dans votre rapport de répartition des coûts que le premier jour du mois suivant. Par exemple, si vous ajoutez des balises à un appareil WorkSpaces Thin Client existant le 15 juillet, elles n'apparaîtront dans votre rapport de répartition des coûts que le 1er août. Pour plus d'informations, consultez la section Utilisation des balises de répartition des coûts dans le guide de l'utilisateur d'AWS Billing.

> **Note**
>
> Pour afficher les balises de ressources de vos clients WorkSpaces légers dans le Cost Explorer, vous devez activer les balises que vous avez appliquées à vos ressources de clients WorkSpaces légers en suivant les instructions de la section Activation des balises de répartition des coûts définies par l'utilisateur dans le guide de l'AWS Billing utilisateur. Les balises apparaissent 24 heures après l'activation, mais les valeurs associées à ces balises peuvent prendre 4 à 5 jours pour apparaître dans Cost Explorer. En outre, pour apparaître et fournir des données de coûts dans Cost Explorer, les ressources WorkSpaces Thin Client qui ont été balisées doivent être facturées pendant cette période. Cost Explorer affiche uniquement les données de coûts à partir du moment où les balises ont été activées. Aucune donnée historique n'est disponible pour le moment.

Ressources que vous pouvez baliser :

- Vous pouvez ajouter des balises aux ressources suivantes lorsque vous les créez : environnements WorkSpaces Thin Client.
- Vous pouvez ajouter des balises aux ressources existantes des types suivants : environnements WorkSpaces Thin Client, appareils et ensembles de logiciels.

- Vous pouvez configurer les balises d'un appareil dans un environnement pour qu'elles soient automatiquement appliquées lorsque vous enregistrez un appareil.

Restrictions liées aux étiquettes

- Nombre maximal de balises par ressource : 50
- Longueur de clé maximale : 128 caractères Unicode
- Longueur maximale de la valeur : 256 caractères Unicode
- Les clés et valeurs d'étiquette sont sensibles à la casse. Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : / @. N'utilisez pas d'espaces de début ou de fin.
- N'utilisez pas le `aws:` préfixe dans les noms ou les valeurs de vos balises, car il est réservé à AWS l'usage. Vous ne pouvez pas modifier ou supprimer des noms ou valeurs de balise ayant ce préfixe.

Pour gérer les balises d'un environnement existant à l'aide de la console

1. Ouvrez la console WorkSpaces Thin Client.
2. Sélectionnez l'environnement pour ouvrir sa page de détails
3. Choisissez Modifier.
4. Dans la section Balises, effectuez une ou plusieurs des opérations suivantes :
    - Pour ajouter une nouvelle balise, choisissez Ajouter une nouvelle balise , puis modifiez les valeurs pour Clé et Valeur.
    - Pour mettre à jour une balise, modifiez la valeur de Value.
    - Pour supprimer une étiquette, cliquez sur le bouton Supprimer à côté de la balise.
5. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer.

Pour gérer les tags d'un appareil existant à l'aide de la console

1. Ouvrez la console WorkSpaces Thin Client.
2. Sélectionnez l'appareil pour ouvrir sa page de détails.
3. Choisissez Tags.
4. Choisissez Gérer les balises.

5. Effectuez une ou plusieurs des actions suivantes :
   - Pour ajouter une nouvelle balise, choisissez Ajouter une nouvelle balise , puis modifiez les valeurs pour Clé et Valeur.
   - Pour mettre à jour une balise, modifiez la valeur de Value.
   - Pour supprimer une étiquette, cliquez sur le bouton Supprimer à côté de la balise.
6. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer.

Pour gérer les tags d'un nouvel appareil à l'aide de la console

1. Ouvrez la console WorkSpaces Thin Client.
2. Sélectionnez l'environnement pour ouvrir sa page de détails.
3. Choisissez Modifier.
4. Dans la section Balises de création d'appareils, effectuez une ou plusieurs des opérations suivantes :
   - Pour ajouter une nouvelle balise, choisissez Ajouter une nouvelle balise , puis modifiez les valeurs pour Clé et Valeur.
   - Pour mettre à jour une balise, modifiez la valeur de Value.
   - Pour supprimer une étiquette, cliquez sur le bouton Supprimer à côté de la balise.
5. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer.

Lorsqu'un appareil est créé, il est enregistré dans l'environnement et les balises de création de l'appareil sont appliquées. Cela ne se produit que lors de l'enregistrement d'un nouvel appareil. De plus, la balise `aws:thinclient:environment-id` système est appliquée avec l'identifiant d'environnement utilisé comme valeur.

Pour gérer les balises d'une mise à jour logicielle à l'aide de la console

1. Ouvrez la console WorkSpaces Thin Client.
2. Sélectionnez la mise à jour logicielle pour ouvrir sa page de détails.
3. Dans la section Tags, choisissez Gérer les tags.
4. Effectuez une ou plusieurs des actions suivantes :

- Pour ajouter une nouvelle balise, choisissez Ajouter une nouvelle balise , puis modifiez les valeurs pour Clé et Valeur.
- Pour mettre à jour une balise, modifiez la valeur de Value.
- Pour supprimer une étiquette, cliquez sur le bouton Supprimer à côté de la balise.

5. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer.

Sécurité dans Amazon WorkSpaces Thin Client

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon WorkSpaces Thin Client, consultez la section AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de WorkSpaces Thin Client. Les rubriques suivantes expliquent comment configurer WorkSpaces Thin Client pour atteindre vos objectifs de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de vos clients WorkSpaces légers.

Rubriques

- Protection des données dans Amazon WorkSpaces Thin Client
- Gestion des identités et des accès pour Amazon WorkSpaces Thin Client
- Résilience dans Amazon WorkSpaces Thin Client
- Analyse et gestion des vulnérabilités dans Amazon WorkSpaces Thin Client

Protection des données dans Amazon WorkSpaces Thin Client

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon WorkSpaces Thin Client. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure

mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec WorkSpaces Thin Client ou autre Services AWS à l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse

URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Amazon WorkSpaces Thin Client collecte et fournit des informations sur l'utilisation des appareils WorkSpaces Thin Client par les utilisateurs et leur interaction avec les services de bureau virtuel. Par exemple, la mémoire disponible, les diagnostics réseau, les informations réseau, la connectivité des appareils, les informations d'identification SAML, les informations d'identification des appareils et les rapports d'erreur. Ces informations sont utilisées pour vous fournir le service et peuvent être utilisées pour améliorer l'expérience utilisateur avec le service. En outre, uniquement pour vous fournir le service, les informations peuvent être transférées en dehors de la AWS région où les utilisateurs utilisent le service. Nous traitons ces informations conformément à l'avis AWS de confidentialité.

Rubriques

- Chiffrement des données
- Chiffrement des données au repos pour Amazon WorkSpaces Thin Client
- Chiffrement en transit
- Gestion des clés
- Confidentialité du trafic professionnel sur Internet

Chiffrement des données

WorkSpaces Thin Client collecte des données relatives à l'environnement et à la personnalisation des appareils, telles que les paramètres utilisateur, les identifiants des appareils, les informations relatives au fournisseur d'identité et les identifiants de bureau de diffusion en continu. WorkSpaces Thin Client collecte également les horodatages des sessions. Les données collectées sont stockées dans Amazon DynamoDB et Amazon S3. WorkSpaces Thin Client utilise AWS Key Management Service (KMS) pour le chiffrement.

Pour sécuriser votre contenu, suivez ces recommandations :

- Implémentez l'accès avec le moindre privilège et créez des rôles spécifiques à utiliser pour les actions des clients WorkSpaces légers.
- Protégez les données end-to-end en fournissant une clé gérée par le client, afin que WorkSpaces Thin Client puisse chiffrer vos données au repos avec les clés que vous fournissez.
- Soyez prudent lorsque vous partagez des codes d'activation d'environnement et des informations d'identification utilisateur :

  - Les administrateurs doivent se connecter à la console WorkSpaces Thin Client, et les utilisateurs doivent fournir des codes d'activation pour la configuration du WorkSpaces Thin Client. Utilisez les informations d'identification pour se connecter au poste de travail de streaming.
  - Toute personne disposant d'un accès physique peut configurer un client WorkSpaces léger, mais elle ne peut pas démarrer de session si elle ne dispose pas d'un code d'activation valide et d'informations d'identification utilisateur pour se connecter.
- Les utilisateurs peuvent mettre fin à leurs sessions de manière explicite en choisissant de verrouiller leur écran, de redémarrer ou d'éteindre l'appareil à l'aide de la barre d'outils de l'appareil. Cela supprime la session de l'appareil et efface les informations d'identification de session.

WorkSpaces Thin Client sécurise le contenu et les métadonnées par défaut en chiffrant toutes les données sensibles avec AWS KMS. En cas d'erreur lors de l'application des paramètres existants, l'utilisateur ne peut pas accéder aux nouvelles sessions et les appareils ne peuvent pas appliquer les mises à jour du logiciel.

Chiffrement des données au repos pour Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client fournit un chiffrement par défaut pour protéger les données sensibles des clients au repos en utilisant des clés de chiffrement AWS détenues par nos soins.

- AWS clés détenues : Amazon WorkSpaces Thin Client utilise ces clés par défaut pour chiffrer automatiquement les données personnelles identifiables. Vous ne pouvez pas consulter, gérer ou utiliser les clés que vous AWS possédez, ni auditer leur utilisation. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez Clés détenues par AWS dans le Guide du développeur AWS Key Management Service.

Le chiffrement des données au repos par défaut permet de réduire les frais opérationnels et la complexité liés à la protection des données sensibles. Dans le même temps, il vous permet de créer des applications sécurisées qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement.

Bien que vous ne puissiez pas désactiver cette couche de chiffrement ou sélectionner un autre type de chiffrement, vous pouvez ajouter une deuxième couche de chiffrement aux clés de chiffrement existantes détenues par AWS en choisissant une clé gérée par le client lors de la création de l'environnement de votre client léger :

- Clés gérées par le client : Amazon WorkSpaces Thin Client prend en charge l'utilisation d'une clé symétrique gérée par le client que vous créez, détenez et gérez afin d'ajouter une deuxième couche de chiffrement au chiffrement AWS détenu existant. Comme vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :
  - Établissement et gestion des stratégies de clé
  - Établissement et mise à jour de politiques IAM
  - Activation et désactivation des stratégies de clé
  - Rotation des matériaux de chiffrement de clé
  - Ajout de balises
  - Création d'alias de clé
  - Planification des clés pour la suppression

Pour plus d'informations, consultez Clés gérées par le client dans le Guide du développeur AWS Key Management Service.

Le tableau suivant résume la manière dont Amazon WorkSpaces Thin Client chiffre les données personnelles identifiables.

Type de données	Chiffrement par clé détenue par AWS	Chiffrement par clé gérée par le client (facultatif)
Nom de l'environnement WorkSpaces Nom de l'environnement Thin Client	Activées	Activées
Nom d'appareil WorkSpaces Nom du périphérique client léger	Activées	Activées
Activité de l'utilisateur WorkSpaces Activité des utilisateurs de Thin Client	Activées	Activées
Paramètres de l'appareil	Activées	Activées

Type de données	Chiffrement par clé détenue par AWS	Chiffrement par clé gérée par le client (facultatif)
WorkSpaces Paramètres du périphérique client léger		
Balises de création d'appareils WorkSpaces Balises de création de périphériques Thin Client Environment	Activées	Activées

> **Note**
>
> Amazon WorkSpaces Thin Client active automatiquement le chiffrement au repos en utilisant des clés AWS détenues pour protéger gratuitement les données personnelles identifiables. Toutefois, des frais AWS KMS s'appliquent pour l'utilisation d'une clé gérée par le client. Pour plus d'informations sur la tarification, consultez Tarification d'AWS Key Management Service.

Comment Amazon WorkSpaces Thin Client utilise AWS KMS

Amazon WorkSpaces Thin Client a besoin d'une politique clé pour que vous puissiez utiliser votre clé gérée par le client.

Amazon WorkSpaces Thin Client a besoin de la politique relative aux clés pour utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez `GenerateDataKey`des demandes à AWS KMS pour chiffrer les données.
- Envoyez `Decrypt`des demandes à AWS KMS pour déchiffrer les données chiffrées.

Vous pouvez supprimer l'accès du service à la clé gérée par le client à tout moment. Dans ce cas, Amazon WorkSpaces Thin Client ne pourra accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données. Par exemple, si vous essayez d'obtenir des détails d'environnement auxquels WorkSpaces Thin Client ne peut pas accéder, l'opération renvoie une `AccessDeniedException` erreur. En outre, le périphérique WorkSpaces Thin Client ne pourra pas utiliser un environnement WorkSpaces Thin Client.

Création d’une clé gérée par le client

Vous pouvez créer une clé symétrique gérée par le client à l'aide de l'AWS Management Console ou des opérations de l'API AWS KMS.

Pour créer une clé symétrique gérée par le client

Suivez les étapes de la rubrique Création d'une clé symétrique gérée par le client dans le Guide du développeur AWS Key Management Service.

Stratégie de clé

Les stratégies de clé contrôlent l’accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l’utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez Gestion de l'accès aux clés gérées par le client dans le Guide du développeur AWS AWS Key Management Service.

Pour utiliser votre clé gérée par le client avec vos ressources Amazon WorkSpaces Thin Client, les opérations d'API suivantes doivent être autorisées dans la politique relative aux clés :

- `kms:DescribeKey`— Fournit les informations clés gérées par le client afin qu'Amazon WorkSpaces Thin Client puisse valider la clé.
- `kms:GenerateDataKey` : autorise l'utilisation de la clé gérée par le client pour chiffrer les données.
- `kms:Decrypt` : autorise l'utilisation de la clé gérée par le client pour déchiffrer les données.

Voici des exemples de déclarations de politique que vous pouvez ajouter pour Amazon WorkSpaces Thin Client :

```
{
    "Statement":
    [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
```

```
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt
data",
            "Effect": "Allow",
            "Principal": {"Service": "thinclient.amazonaws.com"},
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:SourceArn":
                         "arn:aws:thinclient:region:111122223333:*",
                    "kms:EncryptionContext:aws:thinclient:arn":
                         "arn:aws:thinclient:region:111122223333:*"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
```

```
                "kms:Get*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur la spécification d'autorisations dans une stratégie, consultez le Guide du développeur AWS Key Management Service.

Pour plus d'informations sur la résolution des problèmes de clé d'accès, consultez le Guide du développeur AWS Key Management Service.

Spécification d'une clé gérée par le client pour WorkSpaces Thin Client

Vous pouvez spécifier une clé gérée par le client en tant que seconde couche de chiffrement pour les ressources suivantes :

- WorkSpaces Environnement client léger

Lorsque vous créez un environnement, vous pouvez spécifier la clé de données en fournissant un`kmsKeyArn`, qu'Amazon WorkSpaces Thin Client utilise pour chiffrer les données personnelles identifiables.

- `kmsKeyArn`— Identifiant de clé pour une clé gérée par le client AWS KMS. Fournit un ARN de clé.

Lorsqu'un nouveau périphérique client WorkSpaces léger est ajouté à l'environnement client WorkSpaces léger chiffré avec une clé gérée par le client, le périphérique client WorkSpaces léger hérite du paramètre de clé gérée par le client de l'environnement client WorkSpaces léger.

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données.

AWS KMS utilise le contexte de chiffrement comme données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, incluez le même contexte de chiffrement dans la demande.

Contexte de chiffrement Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client utilise le même contexte de chiffrement dans toutes les opérations cryptographiques AWS KMS, où la clé `aws:thinclient:arn` et la valeur sont le nom de ressource Amazon (ARN).

Le contexte de chiffrement de l'environnement est le suivant :

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

Le contexte de chiffrement de l'appareil est le suivant :

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

Utilisation du contexte de chiffrement pour la surveillance

Lorsque vous utilisez une clé symétrique gérée par le client pour chiffrer les données de votre environnement client WorkSpaces léger et de votre appareil, vous pouvez également utiliser le contexte de chiffrement dans les enregistrements et les journaux d'audit pour identifier la manière dont la clé gérée par le client est utilisée. Le contexte de chiffrement apparaît également dans les journaux générés par AWS CloudTrail ou Amazon CloudWatch Logs.

Utilisation du contexte de chiffrement pour contrôler l'accès à votre clé gérée par le client

Vous pouvez utiliser le contexte de chiffrement dans les stratégies de clé et les politiques IAM en tant que conditions pour contrôler l'accès à votre clé symétrique gérée par le client.

Vous trouverez ci-dessous des exemples de déclarations de stratégie de clé permettant d'accorder l'accès à une clé gérée par le client dans un contexte de chiffrement spécifique. La condition énoncée dans cette déclaration de stratégie exige que l'appel `kms:Decrypt` comporte une contrainte de contexte de chiffrement qui spécifie le contexte de chiffrement.

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
```

```
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

Surveillance de vos clés de chiffrement pour Amazon WorkSpaces Thin Client

Lorsque vous utilisez une clé gérée par le client AWS KMS avec vos ressources Amazon WorkSpaces Thin Client, vous pouvez utiliser AWS CloudTrail Amazon CloudWatch Logs pour suivre les demandes qu'Amazon WorkSpaces Thin Client envoie à AWS KMS.

Les exemples suivants sont AWS CloudTrail des événements permettant à`DescribeKey`, `GenerateDataKeyDecrypt`, de surveiller les opérations KMS appelées par Amazon WorkSpaces Thin Client pour accéder aux données chiffrées par votre clé gérée par le client :

Dans les exemples suivants, vous pouvez voir `encryptionContext` l'environnement du client WorkSpaces léger. Des CloudTrail événements similaires sont enregistrés pour le dispositif client WorkSpaces léger.

DescribeKey

Amazon WorkSpaces Thin Client utilise cette `DescribeKey` opération pour vérifier la clé gérée par le client AWS KMS.

L'exemple d'événement suivant enregistre l'opération `DescribeKey` :

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
```

```
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Amazon WorkSpaces Thin Client utilise cette `GenerateDataKey` opération pour chiffrer les données.

L'exemple d'événement suivant enregistre l'opération `GenerateDataKey` :

```
{
    "eventVersion": "1.09",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-04-08T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

GenerateDataKey (by service)

Lorsqu'Amazon WorkSpaces Thin Client utilise les `GenerateDataKey` informations enregistrées sur l'appareil, l'`GenerateDataKey`opération est utilisée pour chiffrer les données.

L'`GenerateDataKey`opération est autorisée dans la déclaration de politique clé de KMS avec le sid « Autoriser le service Amazon WorkSpaces Thin Client à chiffrer et déchiffrer les données ».

L'exemple d'événement suivant enregistre l' GenerateDataKey opération :

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
```

```
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces Thin Client utilise cette `Decrypt` opération pour déchiffrer les données.

L'exemple d'événement suivant enregistre l'opération `Decrypt` :

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
```

```
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
```

```
    "eventCategory": "Management"
}
```

Decrypt (by service)

Lorsque le périphérique client WorkSpaces léger accède aux informations relatives à l'environnement ou au périphérique, l'`Decrypt`opération est utilisée pour déchiffrer les données. L'`Decrypt`opération est autorisée dans la déclaration de politique clé de KMS avec le sid « Autoriser le service Amazon WorkSpaces Thin Client à chiffrer et déchiffrer les données ».

L'exemple d'événement suivant enregistre l'`Decrypt`opération, autorisée par le biais d'un `Grant` :

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```


En savoir plus

Les ressources suivantes fournissent des informations supplémentaires sur le chiffrement des données au repos :

- Pour plus d'informations sur les concepts de base d'AWS Key Management Service, consultez le Guide du développeur AWS Key Management Service.
- Pour plus d'informations sur les bonnes pratiques de sécurité pour AWS Key Management Service, consultez le Guide du développeur AWS Key Management Service.

Chiffrement en transit

WorkSpaces Thin Client chiffre les données en transit via HTTPS et TLS 1.2. Vous pouvez envoyer une demande à WorkSpaces Thin Client à l'aide de la console ou d'appels d'API directs. Les données de demande transférées sont cryptées en les envoyant via une connexion HTTPS ou TLS. Les données de demande peuvent être transférées depuis la AWS console, l'interface de ligne de AWS commande ou le AWS SDK vers le client WorkSpaces léger. Cela inclut également toutes les mises à jour logicielles de l'appareil.

Le chiffrement en transit est configuré par défaut, tout comme les connexions sécurisées (HTTPS, TLS).

Gestion des clés

Vous pouvez fournir votre propre clé AWS KMS gérée par le client pour chiffrer les informations de vos clients. Si vous ne fournissez pas de clé, WorkSpaces Thin Client utilise une clé AWS possédée. Vous pouvez définir votre clé à l'aide du AWS SDK.

Confidentialité du trafic professionnel sur Internet

Les administrateurs peuvent consulter les événements des sessions WorkSpaces Thin Client, notamment les heures de début et les informations relatives aux mises à jour logicielles en attente. Ces journaux sont chiffrés et transmis de manière sécurisée aux clients dans la console WorkSpaces Thin Client. Les informations sur les utilisateurs et d'autres détails sur les sessions de streaming individuelles pour ordinateur de bureau sont enregistrées par les services de bureau. Pour plus d'informations, voir Surveiller votre WorkSpaces, Monitoring and Reporting for AppStream 2.0 ou Journalisation des accès utilisateurs pour WorkSpaces le Web.

Gestion des identités et des accès pour Amazon WorkSpaces Thin Client

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources WorkSpaces Thin Client. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l’aide de politiques
- Comment Amazon WorkSpaces Thin Client fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour Amazon Thin Client WorkSpaces
- AWS politiques gérées pour Amazon WorkSpaces Thin Client
- Résolution des problèmes d'identité et d'accès à Amazon WorkSpaces Thin Client

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans WorkSpaces Thin Client.

Utilisateur du service : si vous utilisez le service WorkSpaces Thin Client pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités WorkSpaces Thin Client pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans WorkSpaces Thin Client, consultezRésolution des problèmes d'identité et d'accès à Amazon WorkSpaces Thin Client.

Administrateur du service — Si vous êtes responsable des ressources du WorkSpaces Thin Client dans votre entreprise, vous avez probablement un accès complet au WorkSpaces Thin Client. C'est à vous de déterminer les fonctionnalités et les ressources du WorkSpaces Thin Client auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec WorkSpaces Thin Client, consultezComment Amazon WorkSpaces Thin Client fonctionne avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à WorkSpaces Thin Client. Pour consulter des exemples de politiques basées sur l'identité des clients WorkSpaces légers que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Amazon Thin Client WorkSpaces

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains

services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette

ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d’autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d’autorisations : une limite d’autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d’autorisations qu’une politique basée sur l’identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d’autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l’identité d’une entité et de ses limites d’autorisation. Les politiques basées sur les ressources qui spécifient l’utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d’autorisations. Un refus explicite dans l’une de ces politiques annule l’autorisation. Pour plus d’informations sur les limites d’autorisations, consultez Limites d’autorisations pour des entités IAM dans le Guide de l’utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services

(SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations SCPs, voir Politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon WorkSpaces Thin Client fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à WorkSpaces Thin Client, découvrez quelles fonctionnalités IAM peuvent être utilisées avec WorkSpaces Thin Client.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon WorkSpaces Thin Client

Fonctionnalité IAM	WorkSpaces Assistance pour les clients légers
Politiques basées sur l'identité	Oui

Fonctionnalité IAM	WorkSpaces Assistance pour les clients légers
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble du fonctionnement du WorkSpaces Thin Client et AWS des autres services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Thin Client WorkSpaces

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité,

car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Exemples de politiques basées sur l'identité pour Thin Client WorkSpaces

Pour consulter des exemples de politiques basées sur l'identité des clients WorkSpaces légers, consultez. Exemples de politiques basées sur l'identité pour Amazon Thin Client WorkSpaces

Politiques basées sur les ressources au sein de Thin Client WorkSpaces

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L’ajout d’un principal intercompte à une politique basée sur les ressources ne représente qu’une partie de l’instauration de la relation d’approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l’entité. Toutefois, si une politique basée sur des ressources accorde l’accès à un principal dans le même compte, aucune autre politique basée sur l’identité n’est requise. Pour plus d’informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l’utilisateur IAM.

Actions politiques pour WorkSpaces Thin Client

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions du client WorkSpaces léger, consultez la section Actions définies par Amazon WorkSpaces Thin Client dans la référence d'autorisation du service.

Les actions de stratégie dans WorkSpaces Thin Client utilisent le préfixe suivant avant l'action :

```
thinclient
```

Pour spécifier plusieurs actions dans une seule instruction, séparez-les par des virgules, comme illustré dans l'exemple suivant :

```
"Action": [
      "thinclient:action1",
      "thinclient:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité des clients WorkSpaces légers, consultez. Exemples de politiques basées sur l'identité pour Amazon Thin Client WorkSpaces

Ressources relatives aux politiques pour WorkSpaces Thin Client

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources WorkSpaces Thin Client et leurs caractéristiques ARNs, consultez la section Ressources définies par Amazon WorkSpaces Thin Client dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon WorkSpaces Thin Client.

Pour consulter des exemples de politiques basées sur l'identité des clients WorkSpaces légers, consultez. Exemples de politiques basées sur l'identité pour Amazon Thin Client WorkSpaces

Clés de conditions de politique pour WorkSpaces Thin Client

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition des clients WorkSpaces légers, consultez la section Clés de condition pour Amazon WorkSpaces Thin Client dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon WorkSpaces Thin Client.

Pour consulter des exemples de politiques basées sur l'identité des clients WorkSpaces légers, consultez. Exemples de politiques basées sur l'identité pour Amazon Thin Client WorkSpaces

ACLs dans WorkSpaces Thin Client

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec client WorkSpaces léger

Prise en charge d'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d’informations sur ABAC, consultez Définition d’autorisations avec l’autorisation ABAC dans le Guide de l’utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

Utilisation d'informations d'identification temporaires avec WorkSpaces Thin Client

Prend en charge les informations d’identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d’identification temporaires lorsque vous vous connectez à la console en tant qu’utilisateur, puis changez de rôle. Pour plus d’informations sur le changement de rôle, consultez Passage d’un rôle utilisateur à un rôle IAM (console) dans le Guide de l’utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour WorkSpaces Thin Client

Prend en charge les sessions d’accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour WorkSpaces Thin Client

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités du WorkSpaces Thin Client. Modifiez les rôles de service uniquement lorsque WorkSpaces Thin Client fournit des instructions à cet effet.

Rôles liés à un service pour Thin Client WorkSpaces

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Amazon Thin Client WorkSpaces

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources WorkSpaces Thin Client. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par WorkSpaces Thin Client, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon WorkSpaces Thin Client dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console WorkSpaces Thin Client
- Accorder un accès en lecture seule à Thin Client WorkSpaces
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accorder un accès complet à WorkSpaces Thin Client

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources WorkSpaces Thin Client dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à

vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console WorkSpaces Thin Client

Pour accéder à la console Amazon WorkSpaces Thin Client, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources WorkSpaces Thin Client de votre Compte AWS. Si vous

créez une politique basée sur l’identité qui est plus restrictive que l’ensemble minimum d’autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l’accès à uniquement aux actions qui correspondent à l’opération d’API qu’ils tentent d’effectuer.

Accorder un accès en lecture seule à Thin Client WorkSpaces

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM de consulter une configuration WorkSpaces Thin Client, mais pas d'y apporter de modifications. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou le programme à l'aide de l'AWS CLI ou de l'API AWS.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
```

```
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accorder un accès complet à WorkSpaces Thin Client

Cet exemple montre comment créer une politique qui accorde un accès complet aux utilisateurs de WorkSpaces Thin Client IAM. Cette politique inclut les autorisations permettant d'effectuer toutes les actions du client WorkSpaces léger sur la console ou le programme à l'aide de l'AWS CLI ou de l'API AWS.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
```

```
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

AWS politiques gérées pour Amazon WorkSpaces Thin Client

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonWorkSpacesThinClientReadOnlyAccess

Vous pouvez associer la politique `AmazonWorkSpacesThinClientReadOnlyAccess` à vos identités IAM. Cette politique accorde des autorisations d'accès complètes au service WorkSpaces Thin Client et à ses dépendances. Pour plus d'informations sur cette stratégie gérée, consultez AmazonWorkSpacesThinClientReadOnlyAccessle guide de référence des politiques AWS gérées.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `thinclient`(WorkSpaces Thin Client) : autorise l'accès en lecture seule à toutes les actions du WorkSpaces Thin Client.
- `workspaces`(WorkSpaces) — Autorise les autorisations pour décrire les WorkSpaces répertoires et les alias de connexion. Ceci est utilisé pour vérifier que vos WorkSpaces ressources sont compatibles avec WorkSpaces Thin Client. Il est également utilisé pour afficher ces ressources dans la AWS console WorkSpaces Thin Client.
- `workspaces-web`(WorkSpaces Secure Browser) — Autorise les autorisations pour décrire les WorkSpaces Secure Browser portails et les paramètres utilisateur. Ceci est utilisé pour vérifier que vos WorkSpaces Secure Browser ressources sont compatibles avec WorkSpaces Thin Client. Il est également utilisé pour afficher ces ressources dans la AWS console WorkSpaces Thin Client.
- `appstream`(AppStream 2.0) — Autorise les autorisations pour décrire les piles AppStream 2.0. Ceci est utilisé pour vérifier que vos ressources AppStream 2.0 sont compatibles avec WorkSpaces Thin Client. Il est également utilisé pour afficher ces ressources dans la AWS console WorkSpaces Thin Client.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
}
```

AWS politique gérée : AmazonWorkSpacesThinClientFullAccess

Vous pouvez associer la politique `AmazonWorkSpacesThinClientFullAccess` à vos identités IAM. Cette politique accorde des autorisations d'accès complètes au service WorkSpaces Thin Client et à ses dépendances. Pour plus d'informations sur cette stratégie gérée, consultez AmazonWorkSpacesThinClientFullAccessle Guide de référence des politiques AWS gérées.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `thinclient`(WorkSpaces Thin Client) — Permet un accès complet à toutes les actions du WorkSpaces Thin Client.
- `workspaces`(WorkSpaces) — Autorise les autorisations pour décrire les WorkSpaces répertoires et les alias de connexion. Ceci est utilisé pour vérifier que vos WorkSpaces ressources sont compatibles avec WorkSpaces Thin Client. Il est également utilisé pour afficher ces ressources dans la AWS console WorkSpaces Thin Client.
- `workspaces-web`(WorkSpaces Secure Browser) — Autorise les autorisations pour décrire les WorkSpaces Secure Browser portails et les paramètres utilisateur. Ceci est utilisé pour vérifier que vos WorkSpaces Secure Browser ressources sont compatibles avec WorkSpaces Thin Client. Il est également utilisé pour afficher ces ressources dans la AWS console WorkSpaces Thin Client.
- `appstream`(AppStream 2.0) — Autorise les autorisations pour décrire les piles AppStream 2.0. Ceci est utilisé pour vérifier que vos ressources AppStream 2.0 sont compatibles avec WorkSpaces Thin Client. Il est également utilisé pour afficher ces ressources dans la AWS console WorkSpaces Thin Client.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
```

```
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
}
```

WorkSpaces Mises à jour des politiques AWS gérées par Thin Client

Modification	Description	Date
AmazonWorkSpacesThinClientReadOnlyAccess— Politique mise à jour	WorkSpaces Thin Client a mis à jour la politique pour inclure des autorisations de lecture limitées pour les détails de l'appareil et les alias de WorkSpaces connexion.	9 janvier 2025
AmazonWorkSpacesThinClientFullAccess— Politique mise à jour	WorkSpaces Thin Client a mis à jour la politique afin d'inclure des autorisations de lecture limitées pour les alias de WorkSpaces connexion.	9 janvier 2025

Modification	Description	Date
AmazonWorkSpacesThinClientReadOnlyAccess— Politique mise à jour	WorkSpaces Thin Client a mis à jour la politique pour inclure des autorisations de lecture limitées pour AppStream 2.0, WorkSpaces Web et WorkSpaces.	9 août 2024
AmazonWorkSpacesThinClientFullAccess : nouvelle politique	Fournit un accès complet à Amazon WorkSpaces Thin Client ainsi qu'un accès limité aux services connexes requis.	9 août 2024
AmazonWorkSpacesThinClientReadOnlyAccess : nouvelle politique	Fournit un accès en lecture seule à Amazon WorkSpaces Thin Client et à ses dépendances.	19 juillet 2024
WorkSpaces Thin Client a commencé à suivre les modifications	WorkSpaces Thin Client a commencé à suivre les modifications apportées AWS à ses politiques gérées.	19 juillet 2024

Résolution des problèmes d'identité et d'accès à Amazon WorkSpaces Thin Client

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec WorkSpaces Thin Client et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans WorkSpaces Thin Client
- Je veux afficher mes clés d'accès
- Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à WorkSpaces Thin Client

- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources WorkSpaces Thin Client

Je ne suis pas autorisé à effectuer une action dans WorkSpaces Thin Client

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-thin-client-device`* fictive, mais ne dispose pas des autorisations `thinclient:`*`ListDevices`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 thinclient:ListDevices on resource: my-thin-client-device
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la *`my-thin-client-device`* ressource en utilisant l'`thinclient:`*`ListDevices`*action.

Je veux afficher mes clés d'accès

Une fois les clés d'accès utilisateur IAM créées, vous pouvez afficher votre ID de clé d'accès à tout moment. Toutefois, vous ne pouvez pas revoir votre clé d'accès secrète. Si vous perdez votre clé d'accès secrète, vous devez créer une nouvelle paire de clés.

Les clés d'accès se composent de deux parties : un ID de clé d'accès (par exemple, `AKIAIOSFODNN7EXAMPLE`) et une clé d'accès secrète (par exemple, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). À l'instar d'un nom d'utilisateur et un mot de passe, vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour authentifier vos demandes. Gérez vos clés d'accès de manière aussi sécurisée que votre nom d'utilisateur et votre mot de passe.

> **Important**
>
> Ne communiquez pas vos clés d'accès à un tiers, même pour qu'il vous aide à trouver votre ID utilisateur canonique. Ce faisant, vous pourriez donner à quelqu'un un accès permanent à votre Compte AWS.

Lorsque vous créez une paire de clé d'accès, enregistrez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, vous devez ajouter de nouvelles clés d'accès pour votre utilisateur IAM. Vous pouvez avoir un maximum de deux clés d'accès. Si vous en avez déjà deux, vous devez supprimer une paire de clés avant d'en créer une nouvelle. Pour afficher les instructions, consultez Gestion des clés d'accès dans le Guide de l'utilisateur IAM.

Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à WorkSpaces Thin Client

Pour autoriser d'autres personnes à accéder à WorkSpaces Thin Client, vous devez accorder l'autorisation aux personnes ou aux applications qui ont besoin d'y accéder. Si vous utilisez AWS IAM Identity Center pour gérer des personnes et des applications, vous attribuez des ensembles d'autorisations aux utilisateurs ou aux groupes afin de définir leur niveau d'accès. Les ensembles d'autorisations créent et attribuent automatiquement des politiques IAM aux rôles IAM associés à la personne ou à l'application. Pour plus d'informations, consultez la section Ensembles d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

Si vous n'utilisez pas IAM Identity Center, vous devez créer des entités IAM (utilisateurs ou rôles) pour les personnes ou les applications qui ont besoin d'un accès. Vous devez ensuite associer une politique à l'entité qui lui accorde les autorisations appropriées dans WorkSpaces Thin Client. Une fois les autorisations accordées, fournissez les informations d'identification à l'utilisateur ou au développeur de l'application. Ils utiliseront ces informations d'identification pour y accéder AWS. Pour en savoir plus sur la création d'utilisateurs, de groupes, de politiques et d'autorisations IAM, consultez la section Identités, politiques et autorisations IAM dans le guide de l'utilisateur IAM.

Pour de plus amples informations, veuillez consulter Accorder un accès complet à WorkSpaces Thin Client.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources WorkSpaces Thin Client

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si WorkSpaces Thin Client prend en charge ces fonctionnalités, consultezComment Amazon WorkSpaces Thin Client fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Résilience dans Amazon WorkSpaces Thin Client

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, WorkSpaces Thin Client propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Analyse et gestion des vulnérabilités dans Amazon WorkSpaces Thin Client

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Amazon WorkSpaces Thin Client s'intègre de manière croisée à Amazon WorkSpaces, Amazon AppStream 2.0 et WorkSpaces Web. Consultez les liens suivants pour plus d'informations sur la gestion des mises à jour pour chacun de ces services :

- Gestion des mises à jour dans Amazon AppStream 2.0
- Gestion des mises à jour sur Amazon WorkSpaces
- Analyse de configuration et de vulnérabilité sur Amazon WorkSpaces Web

Surveillance d'Amazon WorkSpaces Thin Client

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon WorkSpaces Thin Client et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller WorkSpaces Thin Client, signaler un problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le AWS compte de votre compte et envoie les fichiers journaux au compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le AWS CloudTrail Guide de l'utilisateur .

Rubriques

- Journalisation des appels d'API Amazon WorkSpaces Thin Client à l'aide de AWS CloudTrail

Journalisation des appels d'API Amazon WorkSpaces Thin Client à l'aide de AWS CloudTrail

Amazon WorkSpaces Thin Client est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API pour WorkSpaces Thin Client sous forme d'événements. Les appels capturés incluent des appels provenant de la console WorkSpaces Thin Client et des appels de code vers les opérations de l'API WorkSpaces Thin Client. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à WorkSpaces Thin Client, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des détails supplémentaires.

Toutes les actions d'Amazon WorkSpaces Thin Client sont enregistrées CloudTrail et documentées dans le manuel Amazon WorkSpaces Thin Client API Reference. Par exemple, les appels au `CreateEnvironment` `DeleteDevice` et les `GetSoftwareSet` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d’identification d’utilisateur root ou d’utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d’identification de sécurité temporaires d’un rôle ou d’un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

WorkSpaces Événements liés aux données de Thin Client dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource (par exemple, l'enregistrement d'un appareil par un utilisateur final). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de ressources WorkSpaces Thin Client à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API. Pour plus d'informations sur la façon de journaliser les événements de données, consultez Journalisation des événements de données avec la AWS Management Console et Journalisation des événements de données avec l' AWS Command Line Interface dans le Guide de l'utilisateur AWS CloudTrail .

Le tableau suivant répertorie les types de ressources WorkSpaces Thin Client pour lesquels vous pouvez enregistrer des événements de données. La colonne Type d'événement de données

(console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur resources.type indique la **`resources.type`** valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide du ou. AWS CLI CloudTrail APIs La CloudTrail colonne Données APIs enregistrées indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
ThinClientDevice	`AWS::WorkSpacesThinClient::Device`	• RegisterDevice • UpdateDeviceDetails

Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les champs `eventName`, `readOnly` et `resources.ARN` afin de ne journaliser que les événements importants pour vous. Pour plus d'informations sur ces champs, voir AdvancedFieldSelector dans la Référence d'API AWS CloudTrail

WorkSpaces Événements de gestion des clients légers dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Amazon WorkSpaces Thin Client enregistre toutes les opérations du plan de contrôle du WorkSpaces Thin Client en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de contrôle Amazon WorkSpaces Thin Client auxquelles WorkSpaces Thin Client se connecte CloudTrail, consultez le manuel Amazon WorkSpaces Thin Client API Reference.

WorkSpaces Exemples d'événements pour clients légers

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre un CloudTrail événement illustrant l'`RegisterDevice`opération.

```
{
```

```
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-06-19T17:13:44Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "RegisterDevice",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "dsn": "G1X11X11111111XX",
        "activationCode": "xxx1xxx1",
        "model": "AFTGAZL"
      },
      "responseElements": null,
      "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
      "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
      "readOnly": false,
      "resources": [
        {
          "type": "AWS::ThinClient::Device",
          "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": false,
      "recipientAccountId": "111111111111",
      "eventCategory": "Data"
    }
```


L'exemple suivant montre un CloudTrail événement illustrant l'`UpdateDeviceDetails`opération.


```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-10-21T17:46:27Z",
```

```
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "UpdateDeviceDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
    "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
    "readOnly": false,
    "resources": [
      {
        "type": "AWS::ThinClient::Device",
        "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
      }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": false,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
      "settings": {
        "network": {
          "ethernet": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          },
          "networkInterfaceInUse": "ETHERNET",
          "wifi": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          }
        },
```

```
          "peripherals": {
            "bluetooth": {
              "enabledStatus": "ENABLED"
            },
            "keyboards": [
              {
                "name": "name",
                "type": "USB"
              }
            ],
            "mice": [
              {
                "name": "name",
                "type": "BLUETOOTH"
              }
            ],
            "sound": {
              "microphones": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ],
              "speakers": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ]
            },
            "webcams": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "USB"
              }
            ]
          },
          "powerAndSleep": {
            "sleepAfter": "FIFTEEN_MINUTES"
          }
        },
```

```
        "updatedAt": "2024-10-21T17:46:27.624Z"
      },
      "eventCategory": "Data"
    }
```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Création de ressources Amazon WorkSpaces Thin Client avec AWS CloudFormation

Amazon WorkSpaces Thin Client est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources. Ainsi, vous pouvez consacrer moins de temps à la création et à la gestion de vos ressources et de votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez (telles que les environnements), et AWS CloudFormation qui fournit et configure ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources WorkSpaces Thin Client de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis fournissez les mêmes ressources à plusieurs reprises dans plusieurs Comptes AWS régions.

WorkSpaces Thin Client et AWS CloudFormation modèles

Pour fournir et configurer des ressources pour WorkSpaces Thin Client et les services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés au format JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec les formats JSON ou YAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormation Guide de l'utilisateur.

WorkSpaces Thin Client prend en charge la création d'environnements dans AWS CloudFormation. Pour plus d'informations, notamment des exemples de modèles JSON et YAML pour les environnements, consultez la référence au type de ressource Amazon WorkSpaces Thin Client dans le guide de l'AWS CloudFormation utilisateur.

En savoir plus sur AWS CloudFormation

Pour en savoir plus AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- Référence d'API AWS CloudFormation

- AWS CloudFormation Guide de l'utilisateur de l'interface de ligne de commande

Accédez à Amazon WorkSpaces Thin Client à l'aide d'un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et Amazon WorkSpaces Thin Client. Vous pouvez accéder à WorkSpaces Thin Client en tant que VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder au WorkSpaces Thin Client.

Vous établissez cette connexion privée en créant un point de terminaison d'interface alimenté par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d’interface. Il s'agit d'interfaces réseau gérées par les demandeurs qui servent de point d'entrée pour le trafic destiné au WorkSpaces Thin Client.

Pour plus d’informations, consultez Accès aux Services AWS via AWS PrivateLink dans le Guide AWS PrivateLink .

Considérations relatives aux clients WorkSpaces légers

Avant de configurer un point de terminaison d'interface pour WorkSpaces Thin Client, consultez les considérations du AWS PrivateLink guide.

WorkSpaces Thin Client prend en charge les appels à toutes ses actions d'API via le point de terminaison de l'interface.

Création d'un point de terminaison d'interface pour WorkSpaces Thin Client

Vous pouvez créer un point de terminaison d'interface pour WorkSpaces Thin Client à l'aide de la console Amazon VPC ou du AWS Command Line Interface ()AWS CLI. Pour plus d’informations, consultez Création d’un point de terminaison d’interface dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour WorkSpaces Thin Client en utilisant le nom de service suivant :

```
com.amazonaws.region.thinclient.api
```

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API au WorkSpaces Thin Client en utilisant son nom DNS régional par défaut. Par exemple, `api.thinclient.us-east-1.amazonaws.com`.

Création d’une politique de point de terminaison pour votre point de terminaison d’interface

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d’interface. La politique de point de terminaison par défaut vous donne un accès complet à WorkSpaces Thin Client via le point de terminaison de l'interface. Pour contrôler l'accès accordé à WorkSpaces Thin Client depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux qui peuvent effectuer des actions (Comptes AWS, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

Pour plus d’informations, consultez Contrôle de l’accès aux services à l’aide de politiques de point de terminaison dans le Guide AWS PrivateLink .

Exemple : politique de point de terminaison VPC pour les actions des clients WorkSpaces légers

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison de votre interface, elle accorde l'accès aux actions WorkSpaces Thin Client répertoriées à tous les principaux sur toutes les ressources.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
```

```
        }
    ]
}
```

Historique des documents pour le guide de l'administrateur du client WorkSpaces léger

Le tableau suivant décrit l'historique de la documentation des versions du WorkSpaces Thin Client Administrator Guide.

Modification	Description	Date
AWS politique gérée : AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client a ajouté la version 2 de la politique AmazonWorkSpacesThinClientFullAccess gérée.	9 janvier 2025
AWS politique gérée : AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client a ajouté la version 3 des politiques AmazonWorkSpacesThinClientReadOnlyAccess gérées.	9 janvier 2025
Journalisation des appels d'API Amazon WorkSpaces Thin Client à l'aide de AWS CloudTrail Paramètres de l'appareil Chiffrement des données au repos pour Amazon WorkSpaces Thin Client	Ajout d'une nouvelle section pour les événements liés aux données. Ajout d'une nouvelle section pour les paramètres de l'appareil. Mise à jour des informations KMS dans la section relative au chiffrement des données au repos.	28 octobre 2024
Continuité des activités	Ajout d'une nouvelle section pour la continuité des activités et la reprise après sinistre.	6 septembre 2024

Modification	Description	Date
AWS politique gérée : AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client a ajouté une politique AmazonWorkSpacesThinClientFullAccess gérée.	9 août 2024
AWS politique gérée : AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client a ajouté la version 2 des politiques AmazonWorkSpacesThinClientReadOnlyAccess gérées.	9 août 2024
Configuration de WorkSpaces Personal pour WorkSpaces Thin Client	Mise à jour du pour le nouveau WorkSpaces personnel.	7 août 2024
Configuration de WorkSpaces pools pour WorkSpaces Thin Client	Ajout d'une nouvelle section pour les nouveaux WorkSpaces pools.	7 août 2024
AWS politique gérée : AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client a ajouté une politique AmazonWorkSpacesThinClientReadOnlyAccess gérée.	19 juillet 2024
AWS politiques gérées pour Amazon WorkSpaces Thin Client	Amazon WorkSpaces Thin Client a commencé à suivre les modifications.	19 juillet 2024
Configuration WorkSpaces pour Amazon WorkSpaces Thin Client	Mise à jour de la liste des systèmes d'exploitation.	12 février 2024

Modification	Description	Date
Configuration de la AppStream version 2.0 pour Amazon WorkSpaces Thin Client	Mise à jour de la procédure du fournisseur d'identité.	12 février 2024
Première version	Première version	26 novembre 2023

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.