aws

Administratorhandbuch

Amazon WorkSpaces

Amazon WorkSpaces: Administratorhandbuch

Table of Contents

Was ist Amazon WorkSpaces?

Mit Amazon WorkSpaces können Sie virtuelle, Cloud-basierte Microsoft Windows-, Amazon Linux- oder Ubuntu Linux-Desktops für Ihre Benutzer bereitstellen, die als bezeichnet werdenWorkSpaces. WorkSpaces Dadurch entfällt die Notwendigkeit, Hardware zu erwerben und bereitzustellen oder komplexe Software zu installieren. Sie können nach Ihren Bedürfnissen Benutzer schnell und bequem hinzufügen oder entfernen. Benutzer können auf ihre virtuellen Desktops von mehreren Geräten oder Web-Browsern aus zugreifen.

Weitere Informationen finden Sie unter Amazon WorkSpaces.

Features

- Wählen Sie Ihr Betriebssystem (Windows, Amazon Linux, Ubuntu Linux) und dann eine von verschiedenen Hardware- und Software-Konfigurationen sowie AWS-Regionen aus. Weitere Informationen finden Sie unter Amazon WorkSpaces -Pakete und the section called “Erstellen eines benutzerdefinierten Abbilds und Pakets”.
- Wählen Sie Ihr Protokoll aus: PCoIP oder WorkSpaces Streaming Protocol (WSP). Weitere Informationen finden Sie unter Protokolle für Amazon WorkSpaces.
- Stellen Sie eine Verbindung zu Ihrem her WorkSpace und nehmen Sie es von rechts dort auf, wo Sie aufgehört haben. WorkSpaces bietet ein dauerhaftes Desktop-Erlebnis.
- WorkSpaces bietet die Flexibilität einer monatlichen oder stündlichen Fakturierung für WorkSpaces. Weitere Informationen finden Sie unter -WorkSpaces Preise.
- Bei Windows-Desktops können Sie Ihre eigenen Lizenzen und Anwendungen nutzen oder diese über den AWS Marketplace für Desktopanwendungen erwerben.
- Erstellen Sie ein eigenständiges verwaltetes Verzeichnis für Ihre Benutzer oder verbinden Sie Ihre mit WorkSpaces Ihrem On-Premises-Verzeichnis, damit Ihre Benutzer ihre vorhandenen Anmeldeinformationen verwenden können, um nahtlosen Zugriff auf Unternehmensressourcen zu erhalten. Weitere Informationen finden Sie unter Verzeichnisse.
- Verwenden Sie dieselben Tools, um zu verwalten WorkSpaces , die Sie für die Verwaltung von On-Premises-Desktops verwenden.
- Verwenden Sie die Multi-Faktor-Authentifizierung (MFA) für ein höheres Maß an Sicherheit.
- Verwenden Sie AWS Key Management Service (AWS KMS) zum Verschlüsseln von gespeicherten Daten, Festplatten-E/A-Vorgängen und Volume-Snapshots.

- Steuern Sie die IP-Adressen, von denen Benutzer auf ihre zugreifen dürfen WorkSpaces.

Architektur

Bei Windows und Linux WorkSpace ist WorkSpacesjedes einer Virtual Private Cloud (VPC) und einem Verzeichnis zum Speichern und Verwalten von Informationen für Ihr WorkSpaces und Ihre Benutzer zugeordnet. Weitere Informationen finden Sie unter the section called “VPC-Anforderungen”. Verzeichnisse werden über AWS Directory Service verwaltet. Dies bietet folgende Optionen: Simple AD, AD Connector oder AWS Directory Service für Microsoft Active Directory (auch als AWS Managed Microsoft AD bezeichnet). Weitere Informationen finden Sie im Administrationshandbuch zu AWS Directory Service.

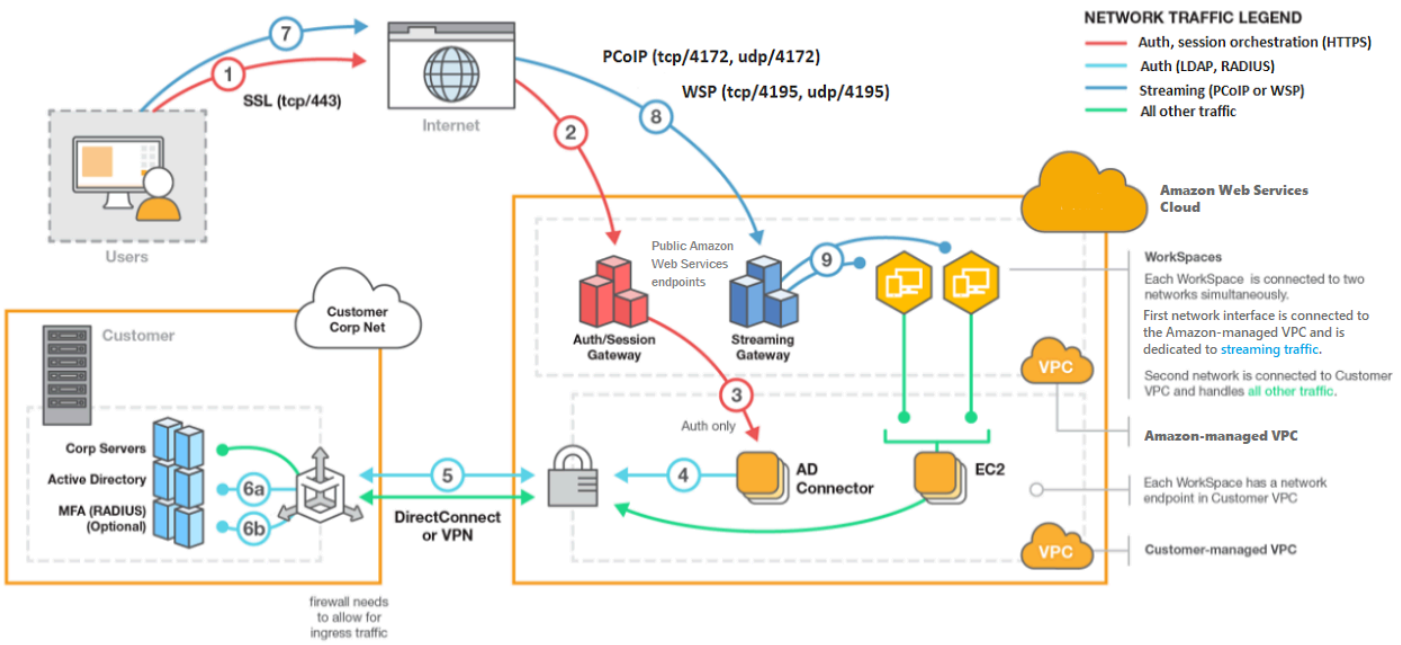
WorkSpaces verwendet Ihr Simple AD-, AD Connector- oder AWS Managed Microsoft AD-Verzeichnis, um Benutzer zu authentifizieren. Benutzer greifen auf ihre zu, WorkSpaces indem sie eine Clientanwendung von einem unterstützten Gerät oder, für Windows WorkSpaces, über einen Webbrowser verwenden, und sie melden sich mit ihren Verzeichnisanmeldeinformationen an. Die Anmeldeinformationen werden an ein Authentifizierungs-Gateway gesendet, das den Datenverkehr an das Verzeichnis für weiterleitet WorkSpace. Nachdem der Benutzer authentifiziert ist, wird der Streaming-Datenverkehr über das Streaming-Gateway gestartet.

Client-Anwendungen verwenden HTTPS über den Port 443 für alle Authentifizierungs- und Sitzungs-Informationen. Clientanwendungen verwenden Port 4172 (PCoIP) und Port 4195 (WSP) für Pixel-Streaming an die WorkSpace und die Ports 4172 und 4195 für Netzwerkzustandsprüfungen. Weitere Informationen finden Sie unter Ports für Clientanwendungen.

WorkSpace Jedem sind zwei Elastic Network-Schnittstellen zugeordnet: eine Netzwerkschnittstelle für Verwaltung und Streaming (eth0) und eine primäre Netzwerkschnittstelle (eth1). Die primäre Netzwerkschnittstelle hat eine IP-Adresse, die von Ihrer VPC bereitgestellt wird, aus denselben Subnetzen, die im Verzeichnis verwendet werden. Dadurch wird sichergestellt, dass der Datenverkehr von Ihrem problemlos das Verzeichnis erreichen WorkSpace kann. Der Zugriff auf Ressourcen in der VPC wird durch die Sicherheitsgruppen kontrolliert, die der primären Netzwerkschnittstelle zugewiesen sind. Weitere Informationen finden Sie unter Netzwerkschnittstellen.

Das folgende Diagramm zeigt die Architektur von WorkSpaces.

Amazon WorkSpaces Architectural Diagram



Zugriff auf Ihr WorkSpace

Sie können eine Verbindung zu Ihrem herstellen WorkSpaces , indem Sie die Client-Anwendung für ein unterstütztes Gerät verwenden, indem Sie einen unterstützten Webbrowser auf einem unterstützten Betriebssystem verwenden.

> **Note**
>
> Sie können keinen Webbrowser verwenden, um eine Verbindung zu Amazon Linux herzustellen WorkSpaces.

Für die folgenden Geräte stehen Client-Anwendungen zur Verfügung:

- Windows-Computer
- macOS-Computer
- Ubuntu Linux 18.04 Computer
- Chromebooks
- iPads

- Android-Geräte
- Fire-Tablets
- Zero-Client-Geräte (Teradici Zero-Client-Geräte werden nur mit PCoIP unterstützt.)

Auf Windows-, macOS- und Linux-PCs können Sie die folgenden Webbrowser verwenden, um eine Verbindung zu Windows und Ubuntu Linux herzustellen WorkSpaces:

- Chrome 53 und höher (nur Windows und macOS)
- Firefox 49 und höher

Weitere Informationen finden Sie unter WorkSpaces Clients im Amazon- WorkSpaces Benutzerhandbuch.

Preisgestaltung

Nachdem Sie sich bei registriert habenAWS, können Sie WorkSpaces kostenlos mit beginnen, indem Sie das WorkSpaces kostenlose Kontingent nutzen. Weitere Informationen finden Sie unter -WorkSpaces Preise.

Mit zahlen Sie nur für das WorkSpaces, was Sie tatsächlich nutzen. Ihnen wird basierend auf dem Paket und der Anzahl der berechnet WorkSpaces , die Sie starten. Die Preise für WorkSpaces beinhalten die Verwendung von Simple AD und AD Connector, aber nicht die Verwendung von AWS Managed Microsoft AD.

WorkSpaces bietet eine monatliche oder stündliche Fakturierung für WorkSpaces. Mit der monatlichen Fakturierung zahlen Sie eine feste Gebühr für die unbegrenzte Nutzung. Dies eignet sich am besten für Benutzer, die ihre WorkSpaces volle Zeit nutzen. Bei der stündlichen Fakturierung zahlen Sie eine geringe feste monatliche Gebühr pro sowie einen niedrigen Stundensatz für jede Stunde WorkSpace, in der der ausgeführt WorkSpace wird. Weitere Informationen finden Sie unter -WorkSpaces Preise.

Weitere Informationen zu unterstützten Regionen finden Sie unter -WorkSpaces Preise.

Erste Schritte

Um eine zu erstellen WorkSpace, probieren Sie eines der folgenden Tutorials aus:

- Erste Schritte mit Quick Setup von WorkSpaces
- Starten eines WorkSpaces über AWS Managed Microsoft AD
- Starten eines WorkSpaces über Simple AD
- Starten eines WorkSpace über AD Connector
- Starten eines WorkSpaces über eine vertrauenswürdige Domain

Sie können sich auch diese Ressourcen ansehen, um mehr über Amazon zu erfahren WorkSpaces:

- Bereitstellen von Desktops in der Cloud
- Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces
- Amazon- WorkSpaces Ressourcen – enthält Whitepaper, Blogbeiträge, Webinare und re:Invent-Sitzungen
- Amazon WorkSpaces FAQs

Erste Schritte mit Quick Setup von WorkSpaces

In diesem Tutorial erfahren Sie, wie Sie mit WorkSpaces und AWS Directory Service einen virtuellen, cloud-basierten Microsoft-Windows-, Amazon-Linux- oder Ubuntu-Linux-Desktop, einen sogenannten WorkSpace, bereitstellen.

In diesem Tutorial wird die Quick-Setup-Option verwendet, um den WorkSpace zu starten. Diese Option ist nur verfügbar, solange Sie noch nie einen WorkSpace gestartet haben. Eine alternative Vorgehensweise finden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

> **Note**
>
> Quick Setup wird nur in den folgenden AWS-Regionen unterstützt:
>
> - USA Ost (Nord-Virginia)
> - USA West (Oregon)
> - Europa (Irland)
> - Asien-Pazifik (Singapur)
> - Asien-Pazifik (Sydney)
> - Asien-Pazifik (Tokio)
>
> Informationen zum Ändern Ihrer Region finden Sie unter Auswählen einer Region.

Aufgaben

Bevor Sie beginnen

Überprüfen Sie zu Beginn, ob die folgenden Anforderungen erfüllt sind:

- Sie müssen über ein AWS-Konto verfügen, um einen WorkSpace erstellen oder verwalten zu können. Benutzer benötigen kein AWS-Konto, um eine Verbindung zu ihren WorkSpaces herstellen und sie verwenden zu können.
- WorkSpaces ist nicht in allen Regionen verfügbar. Überprüfen Sie die unterstützten Regionen und wählen Sie eine Region für Ihre WorkSpaces aus. Weitere Informationen zu den unterstützten Regionen finden Sie unter WorkSpaces – Preise nach AWS-Region.

Machen Sie sich mit den folgenden Inhalten vertraut, bevor Sie fortfahren:

- Wenn Sie einen WorkSpace in Betrieb nehmen, müssen Sie ein WorkSpace-Paket auswählen. Weitere Informationen finden Sie unter Amazon-WorkSpaces-Pakete und Amazon WorkSpaces – Preise.
- Wenn Sie einen WorkSpace starten, müssen Sie auswählen, welches Protokoll (PCoIP oder WorkSpaces Streaming Protocol [WSP]) Sie mit Ihrem Paket verwenden möchten. Weitere Informationen finden Sie unter Protokolle für Amazon WorkSpaces.
- Wenn Sie einen WorkSpace starten, müssen Sie Profilinformationen für den Benutzer angeben, unter anderem einen Benutzernamen und eine E-Mail-Adresse. Die Benutzer vervollständigen das Profil durch Angeben eines Passworts. Informationen zu WorkSpaces und Benutzern sind in einem Verzeichnis gespeichert. Weitere Informationen finden Sie unter Verzeichnisse.

So funktioniert Quick Setup

Quick Setup führt in Ihrem Namen folgende Aufgaben aus:

- Es wird eine IAM-Rolle erstellt, mit der der WorkSpaces-Service Elastic-Network-Schnittstellen erstellen und die WorkSpaces-Verzeichnisse auflisten kann. Diese Rolle hat den Namen `workspaces_DefaultRole`.
- Es wird eine Virtual Private Cloud (VPC) erstellt. Wenn Sie stattdessen eine vorhandene VPC verwenden möchten, stellen Sie sicher, dass sie die unter Konfigurieren einer VPC für WorkSpaces aufgeführten Anforderungen erfüllt, und folgen Sie dann den Schritten in einem der unter Starten eines virtuellen Desktops mit WorkSpaces aufgeführten Tutorials. Wählen Sie das Tutorial aus, das dem Active-Directory-Typ entspricht, den Sie verwenden möchten.

- Es wird ein Simple-AD-Verzeichnis in der VPC eingerichtet und für Amazon WorkDocs aktiviert. Dieses Simple-AD-Verzeichnis wird zum Speichern von Benutzer- und WorkSpace-Informationen verwendet. Das erste AWS-Konto, das von Quick Setup erstellt wird, ist Ihr Administrator-AWS-Konto. † Das Verzeichnis hat auch ein Administratorkonto. Weitere Informationen finden Sie unter Was wird erstellt im AWS Directory Service-Administratorhandbuch.
- Erstellt die angegebenen AWS-Konten und fügt sie dem Verzeichnis hinzu.
- Erstellt WorkSpaces. Jeder WorkSpace erhält eine öffentliche IP-Adresse für den Internetzugang. Der Ausführungsmodus ist AlwaysOn. Weitere Informationen finden Sie unter Verwalten des WorkSpace-Funktionsmodus.
- An die angegebenen Benutzer werden E-Mail-Einladungen versendet. Wenn Ihre Benutzer ihre Einladungs-E-Mails nicht erhalten, finden Sie weitere Informationen unter Senden einer Einladungs-E-Mail.

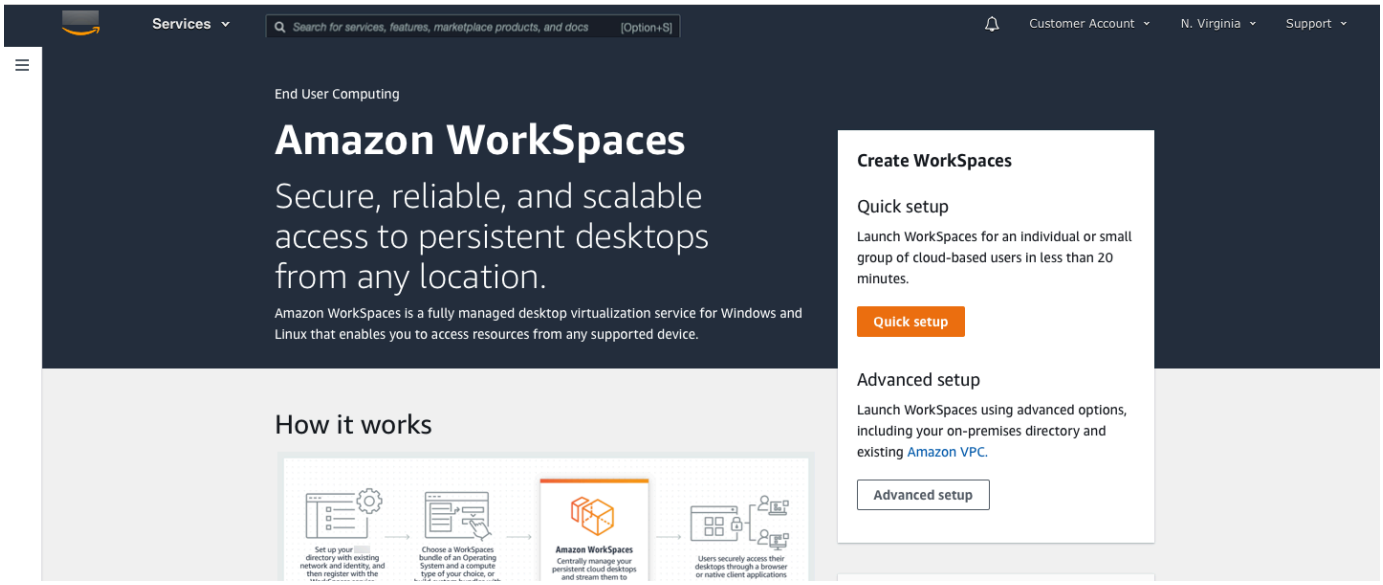
† Das erste AWS-Konto, das von Quick Setup erstellt wird, ist Ihr Administrator-AWS-Konto. Sie können dieses AWS-Konto nicht über die WorkSpaces-Konsole aktualisieren. Geben Sie die Informationen für dieses neue Konto nicht an andere weiter. Erstellen Sie ein neues AWS-Konten für andere Benutzer, um andere Benutzer zur Nutzung von WorkSpaces einzuladen.

Schritt 1: Starten des WorkSpace

Mit Quick Setup können Sie innerhalb weniger Minuten Ihren ersten WorkSpace starten.

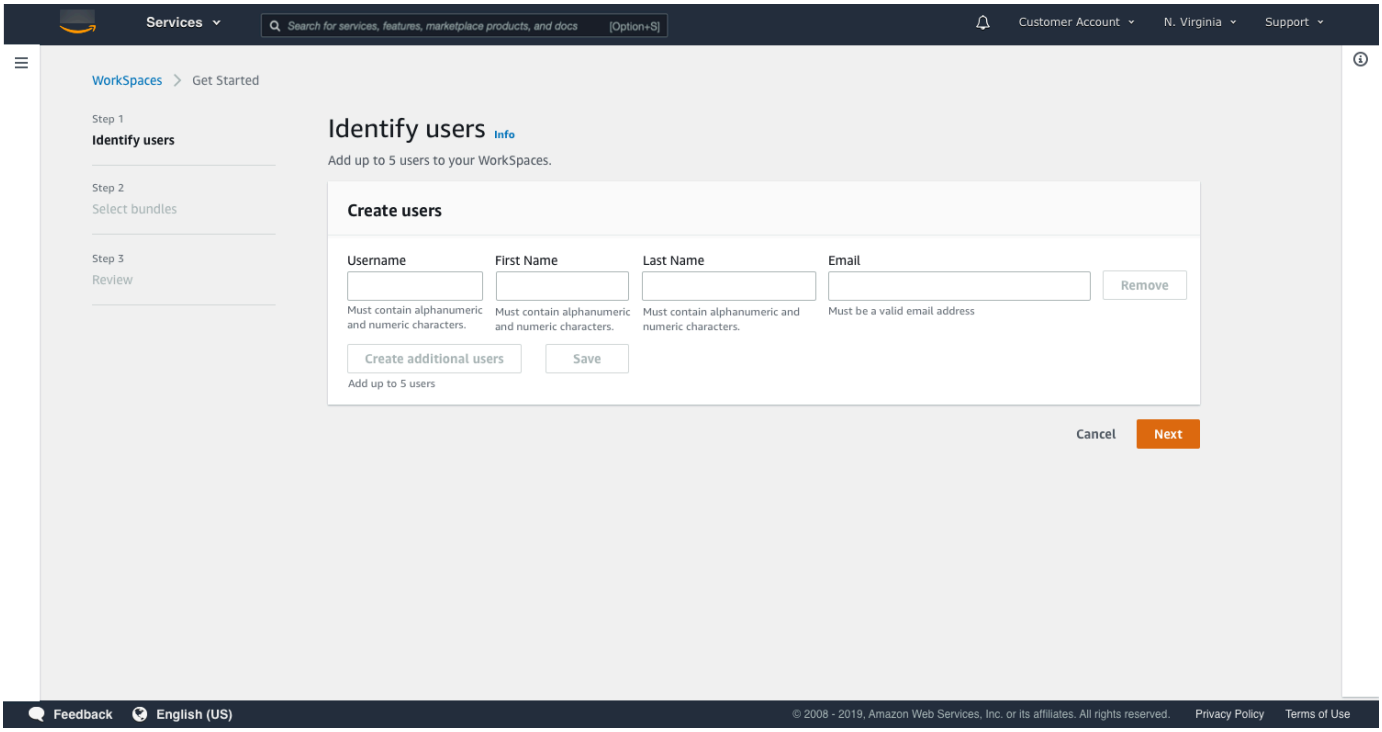
So starten Sie einen WorkSpace

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie Quick setup aus. Wenn diese Schaltfläche nicht angezeigt wird, haben Sie entweder bereits einen WorkSpace in dieser Region gestartet oder Sie verwenden keine der Regionen, die Quick Setup unterstützen. Lesen Sie in diesem Fall Starten eines virtuellen Desktops mit WorkSpaces.

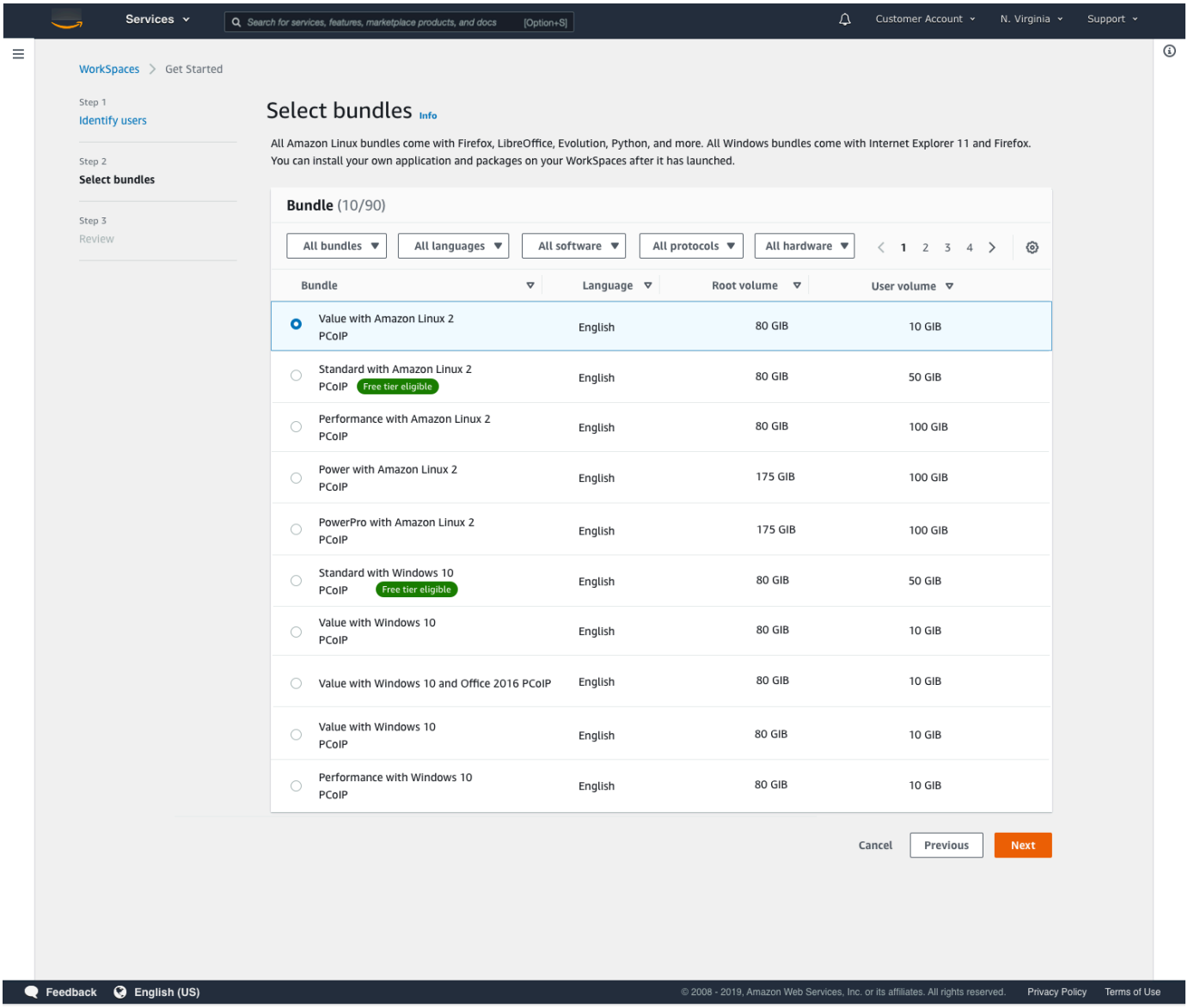


3. Geben Sie unter Benutzer identifizieren den Benutzernamen und den Vornamen ein. Nachname und E-Mail. Wählen Sie anschließend Next (Weiter).

> **Note**
>
> Wenn Sie WorkSpaces zum ersten Mal verwenden, empfehlen wir, zu Testzwecken einen/eine Benutzer:in für Sie selbst zu erstellen.



4. Wählen Sie unter Pakete ein Paket (Hardware und Software) für den/die Benutzer:in mit dem entsprechenden Protokoll (PCoIP oder WSP) aus. Weitere Informationen zu den verschiedenen öffentlichen Pakete, die für Amazon WorkSpaces verfügbar sind, finden Sie unter Amazon WorkSpaces-Pakete.



5. Überprüfen Sie Ihre Informationen Wählen Sie dann WorkSpace erstellen aus.
6. Es dauert ungefähr 20 Minuten, bis Ihr WorkSpace gestartet wird. Gehen Sie zum linken Navigationsbereich und wählen Sie Verzeichnisse aus, um den Fortschritt zu überwachen. Sie werden sehen, dass ein Verzeichnis mit dem Anfangsstatus `REQUESTED` erstellt wird und dann zu `CREATING` wechselt.

   Nachdem das Verzeichnis erstellt wurde und den Status `ACTIVE` hat, können Sie im linken Navigationsbereich WorkSpaces auswählen, um den Fortschritt des WorkSpace-Startvorgangs zu überwachen. Der ursprüngliche Status des WorkSpace ist `PENDING`. Nach dem Start ist der Status `AVAILABLE` und eine Einladung wird an die E-Mail-Adresse gesendet, die Sie für den/die Benutzer:in angegeben haben. Wenn Ihre Benutzer ihre Einladungs-E-Mails nicht erhalten, finden Sie weitere Informationen unter Senden einer Einladungs-E-Mail.

Schritt 2: Verbinden mit dem WorkSpace

Nach dem Erhalt der Einladungs-E-Mail können Sie über einen Client Ihrer Wahl eine Verbindung zum WorkSpace herstellen. Nachdem Sie sich angemeldet haben, zeigt der Client den WorkSpace-Desktop an.

Herstellen einer Verbindung zum WorkSpace.

1. Wenn Sie für den Benutzer noch keine Anmeldeinformationen eingerichtet haben, öffnen Sie den Link in der Einladungs-E-Mail und folgen Sie der Anleitung. Merken Sie sich das von Ihnen festgelegte Passwort, da Sie es für die Verbindung zum WorkSpace benötigen werden.

   > **Note**
   >
   > Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden und es müssen mindestens 8 und höchstens 64 Zeichen enthalten sein. Passwörter müssen mindestens ein Zeichen aus jeder der folgenden Kategorien enthalten: Kleinbuchstaben (a–z), Großbuchstaben (A–Z), Ziffern (0–9) und ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Weitere Informationen zu den Anforderungen für die WorkSpaces-Clients finden Sie im Amazon-WorkSpaces-Benutzerhandbuch. Gehen Sie dann wie folgt vor:

   - Wenn Sie dazu aufgefordert werden, laden Sie eine der Client-Anwendungen herunter oder starten Sie Web Access.
   - Wenn Sie nicht gefragt werden und noch keine Clientanwendung installiert haben, öffnen Sie https://clients.amazonworkspaces.com/ und laden Sie eine der Clientanwendungen herunter oder starten Sie Web Access.

   > **Note**
   >
   > Sie können keinen Webbrowser (Web Access) verwenden, um eine Verbindung mit Amazon-Linux-WorkSpaces herzustellen.

3. Starten Sie den Client, geben Sie den Registrierungscode aus der Einladungs-E-Mail ein und wählen Sie Register aus.
4. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie die Anmeldeinformationen ein und wählen Sie dann Anmelden aus.

5. (Optional) Wenn Sie zur Speicherung Ihrer Anmeldeinformationen aufgefordert werden, wählen Sie Yes aus.

Weitere Informationen zur Verwendung der Client-Anwendungen, z. B. zur Einrichtung mehrerer Monitore oder zur Verwendung von Peripheriegeräten, finden Sie unter WorkSpaces-Clients und Peripheriegeräte-Support im Amazon-WorkSpaces-Benutzerhandbuch.

Schritt 3: Bereinigen (Optional)

Wenn Sie den für dieses Tutorial erstellten WorkSpace nicht mehr benötigen, können Sie ihn löschen. Weitere Informationen finden Sie unter the section called “Löschen eines WorkSpaces”.

> **Note**
>
> Simple AD wird Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem Simple-AD-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.
> Informationen zum Löschen leerer Verzeichnisse finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces. Wenn Sie Ihr Simple-AD-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

Nächste Schritte

Sie können mit der Anpassung des WorkSpace, das Sie gerade erstellt haben fortfahren. Beispielsweise können Sie Software installieren und dann ein benutzerdefiniertes Paket Ihres WorkSpace erstellen. Sie können außerdem verschiedene Verwaltungsaufgaben für Ihre WorkSpaces und Ihr WorkSpaces-Verzeichnis ausführen. Weitere Informationen finden Sie in der folgenden Dokumentation.

- Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket
- Verwalten Ihres WorkSpaces
- Verwalten von Verzeichnissen für WorkSpaces

Führen Sie einen der folgenden Schritte aus, um weitere WorkSpaces zu erstellen:

- Wenn Sie die VPC und das Simple-AD-Verzeichnis, die durch Quick Setup erstellt wurden, weiterhin verwenden möchten, können Sie WorkSpaces für weitere Benutzer hinzufügen, indem Sie die Schritte im Abschnitt Schritt 2: Einen WorkSpace erstellen des Tutorials „Starten eines WorkSpace mit Simple AD“ befolgen.
- Wenn Sie einen anderen Verzeichnistyp oder ein vorhandenes Active Directory verwenden müssen, finden Sie das entsprechende Tutorial im Starten eines virtuellen Desktops mit WorkSpaces.

Weitere Informationen zur Verwendung der WorkSpaces-Clientanwendungen, z. B. zur Einrichtung mehrerer Monitore oder zur Verwendung von Peripheriegeräten, finden Sie unter WorkSpaces-Clients und Peripheriegeräte-Support im Amazon-WorkSpaces-Benutzerhandbuch.

Erste Schritte mit der erweiterten Einrichtung von WorkSpaces

In diesem Tutorial erfahren Sie, wie Sie mit WorkSpaces und AWS Directory Service einen virtuellen, cloud-basierten Microsoft-Windows- oder Amazon-Linux-Desktop, einen sogenannten WorkSpace, bereitstellen.

In diesem Tutorial wird die Option zur erweiterten Einrichtung verwendet, um den WorkSpace zu starten.

> **Note**
>
> Die erweiterte Einrichtung wird in allen Regionen für WorkSpaces unterstützt.

Aufgaben

- Bevor Sie beginnen
- Verwenden der erweiterten Einrichtung zum Starten Ihres WorkSpace

Bevor Sie beginnen

Bevor Sie beginnen, stellen Sie sicher, dass Sie über ein AWS-Konto, das Sie für die Erstellung oder Verwaltung von WorkSpaces verwenden können, verfügen. Benutzer benötigen kein AWS-Konto, um eine Verbindung zu ihren WorkSpaces herstellen und sie verwenden zu können.

Machen Sie sich mit den folgenden Konzepten vertraut, bevor Sie fortfahren:

- Wenn Sie einen WorkSpace in Betrieb nehmen, müssen Sie ein WorkSpace-Paket auswählen. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete.
- Wenn Sie einen WorkSpace starten, müssen Sie auswählen, welches Protokoll (PCoIP oder WorkSpaces Streaming Protocol [WSP]) Sie mit Ihrem Paket verwenden möchten. Weitere Informationen finden Sie unter Protokolle für Amazon WorkSpaces.
- Wenn Sie einen WorkSpace starten, müssen Sie Profilinformationen für den Benutzer angeben, unter anderem einen Benutzernamen und eine E-Mail-Adresse. Die Benutzer vervollständigen das Profil durch Angeben eines Passworts. Informationen zu WorkSpaces und Benutzern sind in einem Verzeichnis gespeichert. Weitere Informationen finden Sie unter Verzeichnisse.

Verwenden der erweiterten Einrichtung zum Starten Ihres WorkSpace

So verwenden Sie die erweiterte Einrichtung zum Starten Ihres WorkSpace:

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie eine der folgenden Verzeichnistypen und klicken Sie dann auf Weiter:

   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector

3. Geben Sie die Verzeichnisinformationen ein.
4. Wählen Sie zwei Subnetze in einer VPC aus zwei verschiedenen Availability Zones aus. Weitere Informationen finden Sie unter Konfigurieren einer VPC mit öffentlichen Subnetzen.
5. Überprüfen Sie die Informationen Ihres Verzeichnisses und wählen Sie Verzeichnis erstellen.

Netzwerk und Zugriff für WorkSpaces

Als WorkSpace-Administrator:in müssen Sie Folgendes über das Netzwerk und den Zugriff in WorkSpaces wissen.

Inhalt

Protokolle für Amazon WorkSpaces

Amazon WorkSpaces unterstützt zwei Protokolle: PCoIP und WorkSpaces Streaming Protocol (WSP). Das von Ihnen gewählte Protokoll hängt von mehreren Faktoren ab, z. B. von der Art der Geräte, WorkSpaces von denen aus Ihre Benutzer auf ihre zugreifen, von welchem Betriebssystem auf Ihrem WorkSpaces, von welchen Netzwerkbedingungen Ihre Benutzer konfrontiert werden und ob Ihre Benutzer bidirektionale Videounterstützung benötigen.

Voraussetzungen

WSP WorkSpaces werden nur mit den folgenden Mindestanforderungen unterstützt.

Agentenanforderungen für den Host-Agent

- Windows-Host-Agent Version 2.0.0.312 oder höher
- Unbutu-Host-Agent Version 2.1.0.501 oder höher
- Amazon-Linux-2-Host-Agent Version 2.0.0.596 oder höher

Clientanforderungen:

- Nativer Windows-Client Version 5.1.0.329 oder höher
- Nativer macOS-Client Version 5.5.0 oder höher
- Web Access

Weitere Informationen darüber, wie Sie Ihre WorkSpace Client-Version und Ihre Host-Agent-Version überprüfen können, finden Sie in den Häufig gestellten Fragen zu .

Wann sollte WSP verwendet werden?

- Wenn Sie aufgrund der Netzwerkbedingungen Ihrer Endbenutzenden eine höhere Verlust-/Latenztoleranz benötigen. Sie haben beispielsweise Benutzer, die WorkSpaces über globale Entfernungen auf ihre zugreifen oder unzuverlässige Netzwerke verwenden.
- Wenn Sie möchten, dass sich Ihre Benutzer mit Smartcards authentifizieren oder Smartcards während der Sitzung verwenden.
- Wenn Sie Funktionen zur Unterstützung von Webcams während der Sitzung benötigen.
- Wenn Sie Web Access mit dem von Windows Server 2019 unterstützten WorkSpaces Paket verwenden müssen.
- Wenn Sie Ubuntu verwenden müssen WorkSpaces.
- Wenn Sie Windows 11 BYOL verwenden müssen WorkSpaces.
- Wenn Sie GPU-basierte Ubuntu-Pakete verwenden müssen (Graphics.g4dn und GraphicsPro.g4dn).
- Wenn Sie möchten, dass sich Ihre Benutzer während der Sitzung mit WebAuthn Authentifikatoren wie YubiKey oder Windows Hello authentifizieren.

Wann sollte PCoIP verwendet werden?

- Wenn Sie die iPad- oder Android-Linux-Clients verwenden möchten.
- Wenn Sie Teradici-Zero-Client-Geräte verwenden.
- Wenn Sie GPU-basierte Pakete verwenden müssen (Graphics.g4dn, GraphicsPro.g4dn, Graphics oder GraphicsPro).
- Wenn Sie ein Linux-Paket für Szenarien ohne Smartcard verwenden müssen.
- Wenn Sie WorkSpaces in der Region China (Ningxia),verwenden müssen.

> **Note**
>
> - Ein Verzeichnis kann eine Mischung aus PCoIP und WSP WorkSpaces enthalten.
> - Ein Benutzer kann sowohl eine PCoIP als auch einen WSP haben, WorkSpace solange sich die beiden in separaten Verzeichnissen WorkSpaces befinden. Derselbe Benutzer darf keine PCoIP und einen WSP WorkSpace im selben Verzeichnis haben. Weitere Informationen zum Erstellen mehrerer WorkSpaces für einen Benutzer finden Sie unter Erstellen mehrerer WorkSpaces für einen/eine Benutzer:in.
> - Sie können eine WorkSpace zwischen den beiden Protokollen migrieren, indem Sie die - WorkSpaces Migrationsfunktion verwenden, die eine Neuerstellung der erfordert WorkSpace. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.
> - Wenn Ihr mit PCoIP-Paketen erstellt WorkSpace wurde, können Sie das Streaming-Protokoll so ändern, dass es zwischen den beiden Protokollen migriert wird, ohne dass eine Neuerstellung erforderlich ist, während das Stamm-Volume erhalten bleibt. Weitere Informationen finden Sie unter Ändern von Protokollen.
> - Für ein optimales Erlebnis mit Videokonferenzen empfehlen wir, nur Power- oder PowerPro Bundles zu verwenden.

Konfigurieren einer VPC für WorkSpaces

WorkSpaces startet Ihre WorkSpaces in einer Virtual Private Cloud (VPC).

Sie können eine VPC mit zwei privaten Subnetzen für Ihr WorkSpaces und einem NAT-Gateway in einem öffentlichen Subnetz erstellen. Alternativ können Sie eine VPC mit zwei öffentlichen Subnetzen

für Ihr erstellen WorkSpaces und jedem eine öffentliche IP-Adresse oder Elastic IP-Adresse zuordnen WorkSpace.

Weitere Informationen zu Überlegungen zum VPC-Design finden Sie unter Bewährte Methoden für VPCs und Netzwerke in Amazon- WorkSpaces Bereitstellungen und Bewährte Methoden für die Bereitstellung – VPC WorkSpaces -Design.

Inhalt

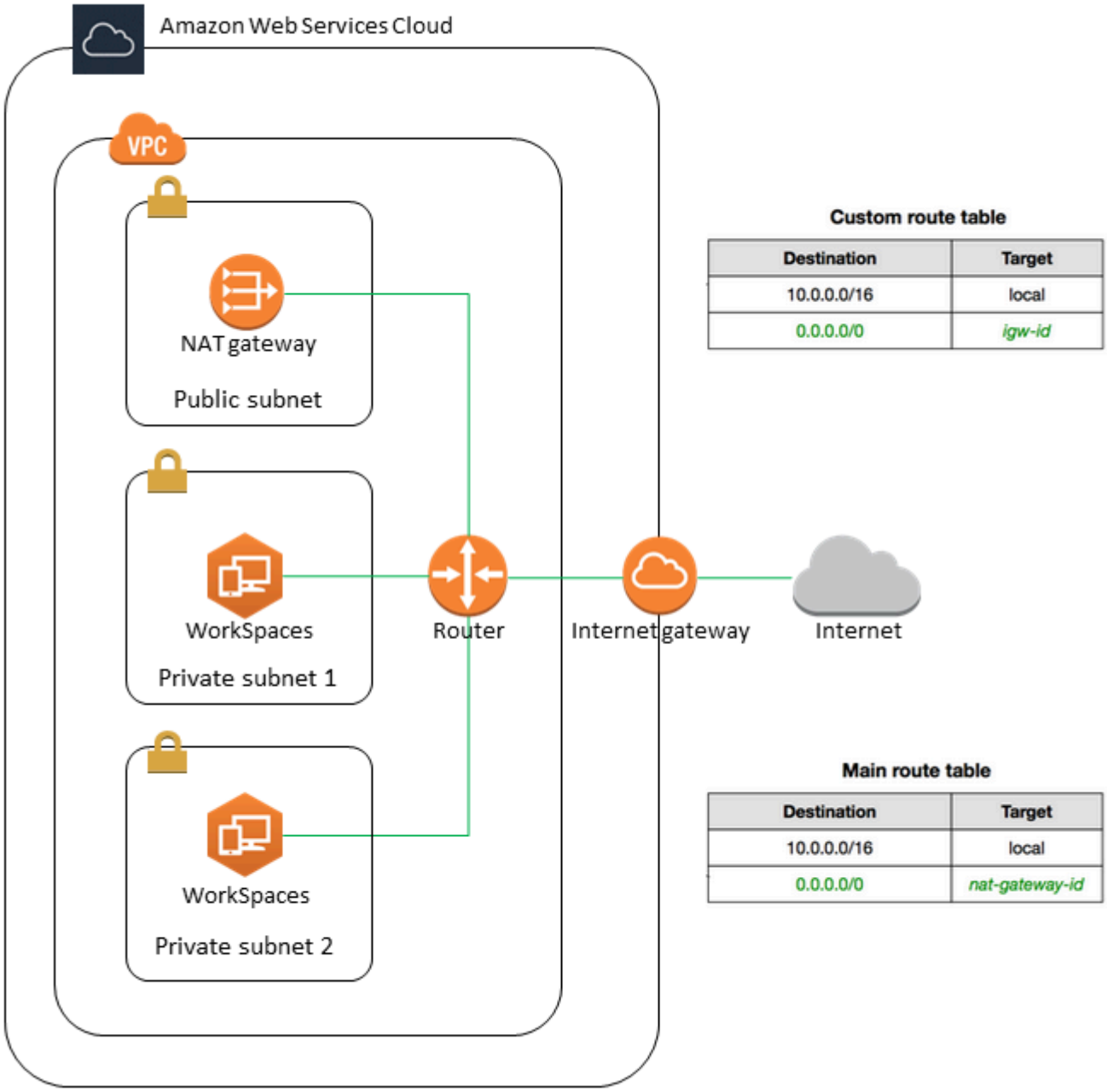
Voraussetzungen

Die Subnetze Ihrer VPC müssen sich in verschiedenen Availability Zones in der Region befinden, in der Sie starten WorkSpaces. Availability Zones sind unabhängige Standorte, die so aufgebaut sind, dass sie von Fehlern in anderen Availability Zones nicht betroffen sind. Indem Instances in separaten Availability Zones gestartet werden, können Sie Ihre Anwendungen vor den Fehlern eines einzelnen Standorts schützen. Jedes Subnetz muss sich vollständig innerhalb einer Availability Zone befinden und darf nicht mehrere Zonen umfassen.

> **Note**
>
> Amazon WorkSpaces ist in einer Teilmenge der Availability Zones in jeder unterstützten Region verfügbar. Informationen dazu, welche Availability Zones Sie für die Subnetze der VPC verwenden können, die Sie für verwenden WorkSpaces, finden Sie unter Availability Zones für Amazon WorkSpaces.

Konfigurieren einer VPC mit privaten Subnetzen und einem NAT-Gateway

Wenn Sie AWS Directory Service verwenden, um ein AWS Managed Microsoft oder Simple AD zu erstellen, empfehlen wir die Konfiguration der VPC mit einem öffentlichen Subnetz und zwei privaten Subnetzen. Konfigurieren Sie Ihr Verzeichnis, um Ihre WorkSpaces in den privaten Subnetzen zu starten. Um Internetzugriff auf WorkSpaces in einem privaten Subnetz zu gewähren, konfigurieren Sie ein NAT-Gateway im öffentlichen Subnetz.



So erstellen Sie eine VPC mit einem öffentlichen Subnetz und zwei privaten Subnetzen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC erstellen aus.
3. Wählen Sie unter Resources to create (Zu erstellende Ressourcen) die Option VPC and more (VPC und mehr) aus.

4. Geben Sie unter Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.
5. Führen Sie zur Konfiguration der Subnetze folgende Schritte aus:
    a. Wählen Sie unter Number of Availability Zones (Anzahl der Availability Zones) je nach Bedarf 1 oder 2 aus.
    b. Erweitern Sie AZs anpassen und wählen Sie Ihre Availability Zones aus. Andernfalls wählt AWS für diese Sie aus. Informationen zum Treffen einer geeigneten Auswahl finden Sie unter Availability Zones für Amazon WorkSpaces.
    c. Stellen Sie unter Number of public subnets (Anzahl der öffentlichen Subnetze) sicher, dass ein öffentliches Subnetz pro Availability Zone vorhanden ist.
    d. Stellen Sie unter Anzahl der privaten Subnetze sicher, dass ein privates Subnetz pro Availability Zone vorhanden ist.
    e. Geben Sie für jedes Subnetz einen CIDR-Block ein. Weitere Informationen finden Sie unter Dimensionierung von Subnetzen im Amazon-VPC-Benutzerhandbuch.
6. Wählen Sie für NAT-Gateways 1 pro AZ aus.
7. Wählen Sie VPC erstellen aus.

IPv6-CIDR-Blöcke

Sie können Ihrer VPC und Ihren Subnetzen IPv6-CIDR-Blöcke zuweisen. Wenn Sie Ihre Subnetze jedoch so konfigurieren, dass den im Subnetz gestarteten Instances automatisch IPv6-Adressen zugewiesen werden, können Sie keine Graphics-Bundles verwenden. (Sie können jedoch Graphics.g4dn-, GraphicsPro.g4dn- und - GraphicsPro Pakete verwenden.) Diese Einschränkung ergibt sich aus einer Hardwareeinschränkung für Instance-Typen der vorherigen Generation, die IPv6 nicht unterstützen.

Um dieses Problem zu umgehen, können Sie die Einstellung für die automatische Zuweisung von IPv6-Adressen in den WorkSpaces Subnetzen vorübergehend deaktivieren, bevor Sie Graphics-Pakete starten, und diese Einstellung dann nach dem Starten von Graphics-Paketen wieder aktivieren (falls erforderlich), sodass alle anderen Pakete die gewünschten IP-Adressen erhalten.

Die Einstellungauto-assign IPv6 addresses (Automatisches Zuweisung von IPv6-Adressen) ist standardmäßig deaktiviert. Wählen Sie im Navigationsbereich Subnetze aus, um diese Einstellung über die Amazon-VPC-Konsole zu überprüfen. Wählen Sie das Subnetz und anschließend Actions

(Aktionen) und Modify auto-assign IP settings (Automatisches Zuweisen von IP-Einstellungen bearbeiten)aus.

Konfigurieren einer VPC mit öffentlichen Subnetzen

Wenn Sie möchten, können Sie eine VPC mit zwei öffentlichen Subnetzen erstellen. Um Internetzugriff auf WorkSpaces in öffentlichen Subnetzen zu gewähren, konfigurieren Sie das Verzeichnis so, dass Elastic IP-Adressen automatisch zugewiesen werden, oder weisen Sie jeder manuell eine Elastic IP-Adresse zu WorkSpace.

Aufgaben

- Schritt 1: Erstellen einer VPC
- Schritt 2: Zuweisen öffentlicher IP-Adressen zu Ihrem WorkSpaces

Schritt 1: Erstellen einer VPC

Erstellen Sie wie folgt eine VPC mit einem öffentlichen Subnetz.

So erstellen Sie die VPC

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC erstellen aus.
3. Wählen Sie unter Resources to create (Zu erstellende Ressourcen) die Option VPC and more (VPC und mehr) aus.
4. Geben Sie unter Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.
5. Führen Sie zur Konfiguration der Subnetze folgende Schritte aus:

    a. Wählen Sie für Anzahl der Availability Zones 2 aus.

    b. Erweitern Sie AZs anpassen und wählen Sie Ihre Availability Zones aus. Andernfalls wählt AWS für diese Sie aus. Informationen zum Treffen einer geeigneten Auswahl finden Sie unter Availability Zones für Amazon WorkSpaces.

    c. Wählen Sie für Number of public subnets (Anzahl der öffentlichen Subnetze) 2 aus.

    d. Wählen Sie für Anzahl der öffentlichen Subnetze (Number of private subnets) 0 aus.

    e. Geben Sie für jedes öffentliche Subnetz einen CIDR-Block ein. Weitere Informationen finden Sie unter Dimensionierung von Subnetzen im Amazon-VPC-Benutzerhandbuch.

6. Wählen Sie VPC erstellen aus.

IPv6-CIDR-Blöcke

Sie können Ihrer VPC und Ihren Subnetzen einen IPv6 CIDR-Block zuweisen. Wenn Sie Ihre Subnetze jedoch so konfigurieren, dass den im Subnetz gestarteten Instances automatisch IPv6-Adressen zugewiesen werden, können Sie keine Graphics-Bundles verwenden. (Sie können jedoch GraphicsPro Pakete verwenden.) Diese Einschränkung ergibt sich aus einer Hardwareeinschränkung für Instance-Typen der vorherigen Generation, die IPv6 nicht unterstützen.

Um dieses Problem zu umgehen, können Sie die Einstellung für die automatische Zuweisung von IPv6-Adressen in den WorkSpaces Subnetzen vorübergehend deaktivieren, bevor Sie Graphics-Pakete starten, und diese Einstellung dann nach dem Starten von Graphics-Paketen wieder aktivieren (falls erforderlich), sodass alle anderen Pakete die gewünschten IP-Adressen erhalten.

Die Einstellungauto-assign IPv6 addresses (Automatisches Zuweisung von IPv6-Adressen) ist standardmäßig deaktiviert. Wählen Sie im Navigationsbereich Subnetze aus, um diese Einstellung über die Amazon-VPC-Konsole zu überprüfen. Wählen Sie das Subnetz und anschließend Actions (Aktionen) und Modify auto-assign IP settings (Automatisches Zuweisen von IP-Einstellungen bearbeiten)aus.

Schritt 2: Zuweisen öffentlicher IP-Adressen zu Ihrem WorkSpaces

Sie können Ihrem WorkSpaces automatisch oder manuell öffentliche IP-Adressen zuweisen. Informationen zur Verwendung der automatischen Zuweisung finden Sie unter the section called “Konfigurieren automatischer öffentlicher IP-Adressen”. Gehen Sie wie folgt vor, um öffentliche IP-Adressen manuell zuzuweisen.

Ein Video-Tutorial zum Zuweisen einer Elastic IP-Adresse zu einem WorkSpacefinden Sie im AWS Knowledge Center-Video Wie verknüpfe ich eine Elastic IP-Adresse mit einem WorkSpace?.

So weisen Sie einem WorkSpace manuell eine öffentliche IP-Adresse zu

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Erweitern Sie die Zeile (wählen Sie das Pfeilsymbol) für die WorkSpace und notieren Sie sich den Wert von WorkSpace IP . Dies ist die primäre private IP-Adresse des WorkSpace.
4. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

5. Wählen Sie im Navigationsbereich Elastic IPs. Wenn Sie keine verfügbare Elastic-IP-Adresse haben, wählen Sie Neue Elastic-IP-Adresse zuweisen und dann Amazon-Pool von IPv4-Adressen oder IPv4-Adressen im Besitz des Kunden und dann Zuordnen aus. Notieren Sie sich die neue IP-Adresse.
6. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
7. Wählen Sie die Netzwerkschnittstelle für Ihr aus WorkSpace. Um die Netzwerkschnittstelle für Ihr zu finden WorkSpace, geben Sie den WorkSpace IP-Wert (den Sie zuvor notiert haben) in das Suchfeld ein und drücken Sie dann die Eingabetaste. Der WorkSpace IP-Wert entspricht der primären privaten IPv4-Adresse für die Netzwerkschnittstelle. Beachten Sie, dass die VPC-ID der Netzwerkschnittstelle mit der ID Ihrer WorkSpaces VPC übereinstimmt.
8. Wählen Sie Actions, Manage IP Addresses aus. Wählen Sie Assign new IP (Neue IP zuweisen) und dann Yes, Update (Ja, aktualisieren) aus. Notieren Sie sich die neue IP-Adresse.
9. Wählen Sie Aktionen, Adresse zuweisen aus.
10. Wählen Sie auf der Seite Associate Elastic IP Address (Elastic IP-Adresse zuordnen) unter Address (Adresse) eine Elastic IP- Adresse aus. Geben Sie für Associate to private IP address (Zu privater IP-Adresse zuordnen) die neue private IP-Adresse an und wählen Sie dann Associate Address (Adresse zuordnen) aus.

Availability Zones für Amazon WorkSpaces

Wenn Sie eine Virtual Private Cloud (VPC) für die Verwendung mit Amazon erstellen WorkSpaces, müssen sich die Subnetze Ihrer VPC in verschiedenen Availability Zones in der Region befinden, in der Sie starten WorkSpaces. Availability Zones sind unabhängige Standorte, die so aufgebaut sind, dass sie von Fehlern in anderen Availability Zones nicht betroffen sind. Indem Instances in separaten Availability Zones gestartet werden, können Sie Ihre Anwendungen vor den Fehlern eines einzelnen Standorts schützen. Jedes Subnetz muss sich vollständig innerhalb einer Availability Zone befinden und darf nicht mehrere Zonen umfassen.

Eine Availability Zone wird durch einen Regionscode gefolgt von einem Buchstaben als Bezeichner angegeben, z. B. `us-east-1a`. Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes AWS-Konto zu. So befindet sich die Availability Zone `us-east-1a` für Ihr AWS-Konto möglicherweise nicht im selben Ort wie `us-east-1a` für ein anderes AWS-Konto.

Um die Availability Zones kontenübergreifend zu koordinieren, müssen Sie die AZ-ID verwenden, die eine eindeutige und konsistente Kennung für eine Availability Zone ist. Beispielsweise ist `use1-az2` eine AZ-ID für die `us-east-1`-Region und hat in jedem AWS-Konto den gleichen Standort.

Mit der Anzeige von AZ-IDs können Sie den Standort von Ressourcen in einem Konto im Verhältnis zu den Ressourcen in einem anderen Konto bestimmen. Wenn Sie beispielsweise ein Subnetz in der Availability Zone mit der AZ-ID `use1-az2` mit einem anderen Konto teilen, steht dieses Subnetz dem Konto in der Availability Zone zur Verfügung, dessen AZ-ID ebenfalls `use1-az2` ist. Die AZ-ID für jede VPC und jedes Subnetz wird in der Amazon VPC-Konsole angezeigt.

Amazon WorkSpaces ist nur in einer Teilmenge der Availability Zones für jede unterstützte Region verfügbar. In der folgenden Tabelle sind alle AZ-IDs aufgeführt, die Sie für jede Region verwenden können. Informationen über die Zuordnung von AZ-IDs zu Availability Zones in Ihrem Konto finden Sie unter AZ-IDs für Ihre Ressourcen im AWS RAM-Benutzerhandbuch.

Name der Region	Regionscode	Unterstützte AZ-IDs
USA Ost (Nord-Virginia)	`us-east-1`	`use1-az2`, `use1-az4`, `use1-az6`
USA West (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`
Asia Pacific (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-az2`, `aps1-az3`
Asia Pacific (Seoul)	`ap-northeast-2`	`apne2-az1` , `apne2-az3`
Asien-Pazifik (Singapur)	`ap-southeast-1`	`apse1-az1` , `apse1-az2`
Asien-Pazifik (Sydney)	`ap-southeast-2`	`apse2-az1` , `apse2-az3`
Asien-Pazifik (Tokio)	`ap-northeast-1`	`apne1-az1` , `apne1-az4`
Canada (Central)	`ca-central-1`	`cac1-az1`, `cac1-az2`
Europe (Frankfurt)	`eu-central-1`	`euc1-az2`, `euc1-az3`
Europa (Irland)	`eu-west-1`	`euw1-az1`, `euw1-az2`, `euw1-az3`

Name der Region	Regionscode	Unterstützte AZ-IDs
Europe (London)	`eu-west-2`	`euw2-az2`, `euw2-az3`
Südamerika (São Paulo)	`sa-east-1`	`sae1-az1`, `sae1-az3`
Afrika (Kapstadt)	`af-south-1`	`afs1-az1`, `afs1-az2`, `afs1-az3`
Israel (Tel Aviv)	`il-central-1`	`ilc1-az1`, `ilc1-az2`, `ilc1-az3`
AWS GovCloud (USA-West)	`us-gov-west-1`	`usgw1-az1` , `usgw1-az2` , `usgw1-az3`
AWS GovCloud (USA-Ost)	`us-gov-east-1`	`usge1-az1` , `usge1-az2` , `usge1-az3`

Weitere Informationen zu Availability Zones und AZ-IDs finden Sie unter Regionen, Availability Zones und lokale Zonen im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

IP-Adresse und Port-Anforderungen für WorkSpaces

Um eine Verbindung zu Ihrem herzustellen WorkSpaces, muss das Netzwerk, mit dem Ihre WorkSpaces Clients verbunden sind, bestimmte Ports für die IP-Adressbereiche der verschiedenen -AWSServices geöffnet haben (in Teilmengen gruppiert). Diese Adressbereiche variieren je nach AWS-Region. Die gleichen Ports müssen auch in jeder Firewall geöffnet sein, die auf dem Client installiert ist. Weitere Informationen über die AWS-IP-Adressbereiche für verschiedene Regionen finden Sie unter AWS-IP-Adressbereiche im Allgemeine Amazon Web Services-Referenz.

Ein Architekturdiagramm finden Sie unter WorkSpaces Architektur . Weitere Architekturdiagramme finden Sie unter Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces.

Ports für Clientanwendungen

Die WorkSpaces Client-Anwendung benötigt ausgehenden Zugriff auf die folgenden Ports:

Port 53 (UDP)

Dieser Port wird für den Zugriff auf DNS-Server verwendet. Er muss für die IP-Adressen Ihrer DNS-Server geöffnet sein, damit der Client öffentliche Domänennamen auflösen kann. Diese Port-Anforderung ist optional, wenn Sie keine DNS-Server für die Domänennamenauflösung verwenden.

Port 443 (TCP)

Dieser Port wird für die Aktualisierung, Registrierung und Authentifizierung der Client-Anwendung verwendet. Die Desktop-Client-Anwendungen unterstützen die Verwendung eines Proxyservers für den Datenverkehr über Port 443 (HTTPS). Öffnen Sie die Client-Anwendung, klicken Sie auf Erweiterte Einstellungen, wählen Sie Proxyserver verwenden aus, geben Sie die Adresse und den Port des Proxyservers ein und klicken Sie dann auf Speichern, um die Verwendung des Proxyservers zu aktivieren.

Dieser Port muss für die folgenden IP-Adressbereiche geöffnet sein:

- Die `AMAZON`-Untergruppe in der Region `GLOBAL`.
- Die `AMAZON` Teilmenge in der Region, in der sich die WorkSpace befindet.
- Die `AMAZON`-Untergruppe in der Region `us-east-1`.
- Die `AMAZON`-Untergruppe in der Region `us-west-2`.
- Die `S3`-Untergruppe in der Region `us-west-2`.

Port 4172 (UDP und TCP)

Dieser Port wird für das Streamen der WorkSpace Desktop- und Zustandsprüfungen für PCoIP WorkSpaces verwendet. Dieser Port muss für das PCoIP Gateway und die Zustandsprüfungsserver in der Region geöffnet sein, in der sich das WorkSpace befindet. Weitere Informationen finden Sie unter Server für die Zustandsprüfung und PCoIP-Gatewayserver.

Für PCoIP WorkSpaces unterstützen die Desktop-Client-Anwendungen weder die Verwendung eines Proxyservers noch die TLS-Entschlüsselung und -Inspektion für Port-4172-Datenverkehr in UDP (für Desktop-Datenverkehr). Sie benötigen eine direkte Verbindung mit dem Port 4172.

Port 4195 (UDP und TCP)

Dieser Port wird für das Streamen der WorkSpace Desktop- und Zustandsprüfungen für WorkSpaces das Streaming Protocol (WSP) verwendet WorkSpaces. Dieser Port muss für die IP-Adressbereiche des WSP-Gateways und die Zustandsprüfungsserver in der Region geöffnet sein, in der sich das WorkSpace befindet. Weitere Informationen finden Sie unter Server für die Zustandsprüfung und WSP-Gatewayserver.

Für WSP unterstützen WorkSpacesdie WorkSpaces Windows-Clientanwendung (Version 5.1 und höher) und die macOS-Clientanwendung (Version 5.4 und höher) die Verwendung von HTTP-Proxyservern für den TCP-Datenverkehr von Port 4195, die Verwendung eines Proxys wird jedoch nicht empfohlen. TLS-Entschlüsselung und -Inspektion werden nicht unterstützt. Weitere Informationen finden Sie unter Konfigurieren von Geräte-Proxy-Servereinstellungen für den Internetzugang für Windows WorkSpaces, Amazon Linux WorkSpaces und Ubuntu WorkSpaces.

> **Note**
>
> - Wenn Ihre Firewall Stateful-Filterung verwendet, werden flüchtige (auch bekannt als dynamische) Ports automatisch geöffnet, um eine Rücksendung zu ermöglichen. Wenn Ihre Firewall mit Stateless-Filterung arbeitet, müssen Sie die flüchtigen Ports ausdrücklich für die zurückgesendete Kommunikation öffnen. Der erforderliche flüchtige Portbereich, den Sie öffnen müssen, hängt von Ihrer Konfiguration ab.
> - Die Proxyserverfunktion wird für UDP-Datenverkehr nicht unterstützt. Wenn Sie einen Proxy-Server verwenden, werden die API-Aufrufe, die die Client-Anwendung an die Amazon WorkSpaces -Services sendet, ebenfalls als Proxy weitergeleitet. Sowohl API-Aufrufe als auch Desktop-Datenverkehr sollten über denselben Proxyserver geleitet werden.

Ports für Internetzugang

WorkSpaces Web Access erfordert ausgehenden Zugriff für die folgenden Ports:

Port 53 (UDP)

Dieser Port wird für den Zugriff auf DNS-Server verwendet. Er muss für die IP-Adressen Ihrer DNS-Server geöffnet sein, damit der Client öffentliche Domänennamen auflösen kann. Diese Port-Anforderung ist optional, wenn Sie keine DNS-Server für die Domänennamenauflösung verwenden.

Port 80 (UDP und TCP)

Dieser Port wird für erstmalige Verbindungen zu `https://clients.amazonworkspaces.com` verwendet. Die Verbindung wird anschließend auf HTTPS umgestellt. Er muss für alle IP-

Adressbereiche in der EC2 Teilmenge in der Region geöffnet sein, in der sich das WorkSpace befindet.

Port 443 (UDP und TCP)

Dieser Port wird für die Registrierung und die Authentifizierung über HTTPS verwendet. Er muss für alle IP-Adressbereiche in der EC2 Teilmenge in der Region geöffnet sein, in der sich das WorkSpace befindet.

Port 4195 (UDP und TCP)

Für WorkSpaces , die für WorkSpaces Streaming Protocol (WSP) konfiguriert sind, wird dieser Port für das Streamen des WorkSpaces Desktop-Datenverkehrs verwendet. Dieser Port muss für die folgenden IP-Adressbereiche des WSP-Gateways geöffnet sein. Weitere Informationen finden Sie unter WSP-Gatewayserver.

Der WSP-Internetzugang unterstützt die Verwendung eines Proxyservers für den TCP-Datenverkehr über Port 4195, wird jedoch nicht empfohlen. Weitere Informationen finden Sie unter Konfigurieren von Geräte-Proxy-Servereinstellungen für den Internetzugang für Windows WorkSpaces, Amazon Linux WorkSpaces und Ubuntu WorkSpaces.

> **Note**
>
> Wenn Ihre Firewall Stateful-Filterung verwendet, werden flüchtige (auch bekannt als dynamische) Ports automatisch geöffnet, um eine Rücksendung zu ermöglichen. Wenn Ihre Firewall mit Stateless-Filterung arbeitet, müssen Sie die flüchtigen Ports ausdrücklich für die zurückgesendete Kommunikation öffnen. Der erforderliche flüchtige Portbereich, den Sie öffnen müssen, hängt von Ihrer Konfiguration ab.

In der Regel wählt der Webbrowser nach dem Zufallsprinzip einen Quellport im großen Bereich aus, der für das Streaming von Datenverkehr verwendet werden soll. WorkSpaces Web Access hat keine Kontrolle über den Port, den der Browser auswählt. Sie müssen sicherstellen, dass zu diesem Port zurückfließender Datenverkehr zulässig ist.

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Damit die WorkSpaces Clientanwendung auf den WorkSpaces Service zugreifen kann, müssen Sie der Zulassungsliste in dem Netzwerk, von dem aus der Client auf den Service zugreifen möchte, die folgenden Domains und IP-Adressen hinzufügen.

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Domain oder IP-Adresse
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	• https://d2td7dqidlhjx7.cloudfront.net/ • In der Region AWS GovCloud (USA-West): https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/WorkSpacesAppCastx64.xml
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domains: • https://skylight-client-ds.us-east-1.amazonaws.com • https://skylight-client-ds.us-west-2.amazonaws.com • https://skylight-client-ds.ap-south-1.amazonaws.com • https://skylight-client-ds.ap-northeast-2.amazonaws.com • https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com • https://skylight-client-ds.ap-northeast-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
	• https://skylight-client-ds.ca-central-1.amazonaws.com • https://skylight-client-ds.eu-central-1.amazonaws.com • https://skylight-client-ds.eu-west-1.amazonaws.com • https://skylight-client-ds.eu-west-2.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • https://skylight-client-ds.af-south-1.amazonaws.com • https://skylight-client-ds.il-central-1.amazonaws.com • In der Region AWS GovCloud (USA-West): https://skylight-client-ds.us-gov-west-1.amazonaws.com • In der Region AWS GovCloud (USA-Ost): https://skylight-client-ds.us-gov-east-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domains: • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com • https://ws-client-service.ap-south-1.amazonaws.com • https://ws-client-service.ap-northeast-2.amazonaws.com • https://ws-client-service.ap-southeast-1.amazonaws.com • https://ws-client-service.ap-southeast-2.amazonaws.com • https://ws-client-service.ap-northeast-1.amazonaws.com • https://ws-client-service.ca-central-1.amazonaws.com • https://ws-client-service.eu-central-1.amazonaws.com • https://ws-client-service.eu-west-1.amazonaws.com • https://ws-client-service.eu-west-2.amazonaws.com • https://ws-client-service.sa-east-1.amazonaws.com • https://ws-client-service.af-south-1.amazonaws.com • https://ws-client-service.il-central-1.amazonaws.com • In der Region AWS GovCloud (USA-West):

Kategorie	Domain oder IP-Adresse
	https://ws-client-service.us-gov-west-1.amazonaws.com • In der Region AWS GovCloud (USA-Ost): https://ws-client-service.us-gov-east-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/*<region>*/*<directory ID>* Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • Legacy — https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> • USA Ost (Nord-Virginia) – https://d2h1yryv1jxiq.cloudfront.net/ • USA West (Oregon) – https://d1fq42e1gi7rtq.cloudfront.net/ • Asien-Pazifik (Mumbai) – https://d1ctsk4u02kky7.cloudfront.net/ • Asien-Pazifik (Seoul) – https://dyoj3cw6iktvg.cloudfront.net • Asien-Pazifik (Singapur) – https://d1525ef92caquk.cloudfront.net/ • Asien-Pazifik (Sydney) – https://dodwxjr2amr8p.cloudfront.net/

Kategorie	Domain oder IP-Adresse
	• Asien-Pazifik (Tokio) – https://d3v7kcib8ir2e1.cloudfront.net/ • Kanada (Zentral) – https://d1ebdk07rro1qy.cloudfront.net/ • Europa (Frankfurt) – https://d39q4y7cndearu.cloudfront.net/ • Europa (Irland) – https://d2127w6wvrc6l3.cloudfront.net/ • Europa (London) – https://df4ahgpxbxqy2.cloudfront.net/ • Südamerika (São Paulo) – https://d2nezqurrjvain.cloudfront.net/ • Afrika (Kapstadt) – https://dr6ry0pwaoy23.cloudfront.net • Israel (Tel Aviv) – https://d2kmf63k5sit88.cloudfront.net CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • USA Ost (Nord-Virginia) – https://d32i4gd7pg4909.cloudfront.net/ • USA West (Oregon) – https://d18af777lco7lp.cloudfront.net/ • Asien-Pazifik (Mumbai) – https://d78hovzzqqtsb.cloudfront.net/ • Asien-Pazifik (Seoul) – https://dtyv4uwoh7ynt.cloudfront.net/

Kategorie	Domain oder IP-Adresse
	• Asien-Pazifik (Singapur) – https://d3qzmd7y07pz0i.cloudfront.net/ • Asien-Pazifik (Sydney) – https://dwcpoxuuza83q.cloudfront.net/ • Asien-Pazifik (Tokio) – https://d2c2t8mxjhq5z1.cloudfront.net/ • Kanada (Zentral) – https://d2wfbsypmqjmog.cloudfront.net/ • Europa (Frankfurt) – https://d1whcm49570jjw.cloudfront.net/ • Europa (Irland) – https://d3pgffbf39h4k4.cloudfront.net/ • Europa (London) – https://d16q6638mh01s7.cloudfront.net/ • Südamerika (São Paulo) – https://d2lh2qc5bdoq4b.cloudfront.net/ • Afrika (Kapstadt) – https://di5ygl2cs0mrh.cloudfront.net/ • Israel (Tel Aviv) – https://d1a3pnge9on3sx.cloudfront.net In der Region AWS GovCloud (USA-West): • Kunden-Verzeichniseinstellungen: https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<Verzeichnis-ID> • Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: https://workspace-client-assets-pdt.s3-us-gov-west-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
	• CSS-Datei zum Gestalten der Anmeldeseiten: https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • JavaScript -Datei für die Anmeldeseiten: Nicht zutreffend In der Region AWS GovCloud (USA-Ost): • Kunden-Verzeichniseinstellungen: https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<Verzeichnis-ID> • Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: https://workspace-client-assets-pdt.s3-us-gov-east-1.amazonaws.com • CSS-Datei zum Gestalten der Anmeldeseiten: https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • JavaScript -Datei für die Anmeldeseiten: Nicht zutreffend
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung

Kategorie	Domain oder IP-Adresse
Smartcard-Authentifizierungsendpunkte vor der Sitzung	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin.amazonaws-us-gov.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist) In den Regionen AWS GovCloud (USA-West) und AWS GovCloud (USA-Ost): https://login.us-gov-home.awsapps.com/directory/<directory id>/ (wobei <directory id> die Domain des Kunden ist)

Kategorie	Domain oder IP-Adresse
WS Broker	Domains: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com • https://ws-broker-service.ap-south-1.amazonaws.com • https://ws-broker-service.ap-northeast-2.amazonaws.com • https://ws-broker-service.ap-southeast-1.amazonaws.com • https://ws-broker-service.ap-southeast-2.amazonaws.com • https://ws-broker-service.ap-northeast-1.amazonaws.com • https://ws-broker-service.ca-central-1.amazonaws.com • https://ws-broker-service.eu-central-1.amazonaws.com • https://ws-broker-service.eu-west-1.amazonaws.com • https://ws-broker-service.eu-west-2.amazonaws.com • https://ws-broker-service.sa-east-1.amazonaws.com • https://ws-broker-service.af-south-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
	• https://ws-broker-service.il-central-1.amazonaws.com • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com • https://ws-broker-service.us-gov-east-1.amazonaws.com • https://ws-broker-service-fips.us-gov-east-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
WorkSpaces API-Endpunkte	Domains: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com • https://workspaces.us-gov-east-1.amazonaws.com • https://workspaces-fips.us-gov-east-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
WorkSpaces Endpunkte für SAML Single Sign-On (SSO)	Domains: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.us-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.af-south-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.il-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.us-gov-west-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-gov-west-1.amazonaws.com/v1/report-heartbeat

Kategorie	Domain oder IP-Adresse
	• https://euc-sso-sm.us-gov-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-gov-east-1.amazonaws.com/v1/report-heartbeat

Domains und IP-Adressen, die der Zulassungsliste für PCoIP hinzugefügt werden sollten

Kategorie	Domain oder IP-Adresse
PCoIP-Sitzungs-Gateway (PSG)	PCoIP-Gatewayserver
Sitzungs-Broker (PCM)	Domains: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
	• https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com • https://skylight-cm.us-gov-east-1.amazonaws.com • https://skylight-cm-fips.us-gov-east-1.amazonaws.com

Kategorie	Domain oder IP-Adresse
Web-Access-TURN-Server für PCoIP	Server: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Web Access ist derzeit in der Region Asien-Pazifik (Mumbai) nicht verfügbar. • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • Web Access ist derzeit in der Region Afrika (Kapstadt) nicht verfügbar • Web Access ist derzeit in der Region Israel (Tel Aviv) nicht verfügbar.

Domains und IP-Adressen, die Ihrer Zulassungsliste für WorkSpaces Streaming Protocol (WSP) hinzugefügt werden sollen

Kategorie	Domain oder IP-Adresse
WSP Session Gateway (WSG)	WSP-Gatewayserver
Web-Access-TURN-Server für WSP	WSP-Gatewayserver

Server für die Zustandsprüfung

Die WorkSpaces Clientanwendungen führen Zustandsprüfungen über die Ports 4172 und 4195 durch. Diese Prüfungen überprüfen, ob TCP- oder UDP-Datenverkehr von den WorkSpaces Servern zu den Client-Anwendungen gestreamt wird. Damit diese Prüfungen erfolgreich durchgeführt werden können, müssen die Firewall-Richtlinien ausgehenden Datenverkehr zu den IP-Adressen der folgenden regionalen Zustandsprüfungsserver zulassen.

Region	Hostname der Systemzustandsprüfung	IP-Adressen
USA Ost (Nord-Virginia)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
USA West (Oregon)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
Asien-Pazifik (Mumbai)	drp-bom.amazonworkspaces.com	13.127.57.82 13.234.250.73
Asien-Pazifik (Seoul)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105

Region	Hostname der Systemzustandsprüfung	IP-Adressen
		52.78.44.253 52.79.54.102
Asien-Pazifik (Singapur)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
Asien-Pazifik (Sydney)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
Asien-Pazifik (Tokio)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
Kanada (Zentral)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
Europa (Frankfurt)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227

Region	Hostname der Systemzustandsprüfung	IP-Adressen
Europa (Irland)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224
Europa (London)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
Südamerika (São Paulo)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
Afrika (Kapstadt)	drp-cpt.amazonworkspaces.com/	13.244.128.155 13.245.205.255 13.245.216.116
Israel (Tel Aviv)	drp-tlv.amazonworkspaces.com/	51.17.52.90 51.17.109.231 51.16.190.43

Region	Hostname der Systemzustandsprüfung	IP-Adressen
AWS GovCloud (USA-West)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88
AWS GovCloud (USA-Ost)	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

PCoIP-Gatewayserver

WorkSpaces verwendet PCoIP, um die Desktop-Sitzung über Port 4172 an Clients zu streamen. Für seine PCoIP-Gateway-Server WorkSpaces verwendet einen kleinen Bereich öffentlicher IPv4-Adressen von Amazon EC2. Auf diese Weise können Sie detailliertere Firewall-Richtlinien für Geräte einstellen, die auf WorkSpaces zugreifen. Beachten Sie, dass die WorkSpaces Clients derzeit keine IPv6-Adressen als Konnektivitätsoption unterstützen.

Region	Öffentliche IP-Adressbereiche
USA Ost (Nord-Virginia)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
USA West (Oregon)	35.80.88.0 – 35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255

Region	Öffentliche IP-Adressbereiche
Asien-Pazifik (Mumbai)	13.126.243.0 – 13.126.243.255
Asien-Pazifik (Seoul)	3.34.37.0 – 3.34.37.255 3.34.38.0 – 3.34.39.255 13.124.247.0 - 13.124.247.255
Asien-Pazifik (Singapur)	18.141.152.0 – 18.141.152.255 18.141.154.0 – 18.141.155.255 52.76.127.0 - 52.76.127.255
Asien-Pazifik (Sydney)	3.25.43.0 – 3.25.43.255 3.25.44.0 – 3.25.45.255 54.153.254.0 - 54.153.254.255
Asien-Pazifik (Tokio)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
Kanada (Zentral)	15.223.100.0 – 15.223.100.255 15.223.102.0 – 15.223.103.255 35.183.255.0 - 35.183.255.255
Europa (Frankfurt)	18.156.52.0 – 18.156.52.255 18.156.54.0 – 18.156.55.255 52.59.127.0 - 52.59.127.255
Europa (Irland)	3.249.28.0 – 3.249.29.255 52.19.124.0 - 52.19.125.255

Region	Öffentliche IP-Adressbereiche
Europa (London)	18.132.21.0 – 18.132.21.255 18.132.22.0 – 18.132.23.255 35.176.32.0 - 35.176.32.255
Südamerika (São Paulo)	18.230.103.0 – 18.230.103.255 18.230.104.0 – 18.230.105.255 54.233.204.0 – 54.233.204.255
Afrika (Kapstadt)	13.246.120.0 – 13.246.123.255
Israel (Tel Aviv)	51.17.28.0-51.17.31.255
AWS GovCloud (USA-West)	52.61.193.0 - 52.61.193.255
AWS GovCloud (USA-Ost)	18.254.140.0 – 18.254.143.255

WSP-Gatewayserver

> **Important**
>
> Ab Juni 2020 WorkSpaces streamt die Desktop-Sitzung für WSP WorkSpaces über Port 4195 statt über Port 4172 an Clients. Wenn Sie WSP verwenden möchten WorkSpaces, stellen Sie sicher, dass Port 4195 für den Datenverkehr geöffnet ist.

WorkSpaces verwendet einen kleinen Bereich öffentlicher IPv4-Adressen von Amazon EC2 für seine WSP-Gateway-Server. Auf diese Weise können Sie detailliertere Firewall-Richtlinien für Geräte einstellen, die auf WorkSpaces zugreifen. Beachten Sie, dass die WorkSpaces Clients derzeit keine IPv6-Adressen als Konnektivitätsoption unterstützen.

Region	Öffentliche IP-Adressbereiche
USA Ost (Nord-Virginia)	• 3.227.4.0/22

Region	Öffentliche IP-Adressbereiche
	• 44.209.84.0/22
USA West (Oregon)	34.223.96.0/22
Asien-Pazifik (Mumbai)	65.1.156.0/22
Asien-Pazifik (Seoul)	3.35.160.0/22
Asien-Pazifik (Singapur)	13.212.132.0/22
Asien-Pazifik (Sydney)	3.25.248.0/22
Asien-Pazifik (Tokio)	3.114.164.0/22
Kanada (Zentral)	3.97.20.0/22
Europa (Frankfurt)	18.192.216.0/22
Europa (Irland)	3.248.176.0/22
Europa (London)	18.134.68.0/22
Südamerika (São Paulo)	15.228.64.0/22
Afrika (Kapstadt)	13.246.108.0/22
Israel (Tel Aviv)	51.17.72.0/22
AWS GovCloud (USA-West)	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud (USA-Ost)	18.254.148.0/22

WSP-Gateway-Domänennamen

In der folgenden Tabelle sind die WSP WorkSpace -Gateway-Domänennamen aufgeführt. Diese Domains müssen erreichbar sein, damit die WorkSpaces Clientanwendung auf den WorkSpace WSP-Service zugreifen kann.

Region	Domain
USA Ost (Nord-Virginia)	*.prod.us-east-1.highlander.aws.a2z.com
USA West (Oregon)	*.prod.us-west-2.highlander.aws.a2z.com
Asien-Pazifik (Mumbai)	*.prod.ap-south-1.highlander.aws.a2z.com
Asien-Pazifik (Seoul)	*.prod.ap-northeast-2.highlander.aws.a2z.com
Asien-Pazifik (Singapur)	*.prod.ap-southeast-1.highlander.aws.a2z.com
Asien-Pazifik (Sydney)	*.prod.ap-southeast-2.highlander.aws.a2z.com
Asien-Pazifik (Tokio)	*.prod.ap-northeast-1.highlander.aws.a2z.com
Kanada (Zentral)	*.prod.ca-central-1.highlander.aws.a2z.com
Europa (Frankfurt)	*.prod.eu-central-1.highlander.aws.a2z.com
Europa (Irland)	*.prod.eu-west-1.highlander.aws.a2z.com
Europa (London)	*.prod.eu-west-2.highlander.aws.a2z.com
Südamerika (São Paulo)	*.prod.sa-east-1.highlander.aws.a2z.com
Afrika (Kapstadt)	*.prod.af-south-1.highlander.aws.a2z.com
Israel (Tel Aviv)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (USA-West)	*.prod.us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (USA-Ost)	*.prod.us-gov-east-1.highlander.aws.a2z.com

Netzwerkschnittstellen

Jede WorkSpace hat die folgenden Netzwerkschnittstellen:

- Die primäre Netzwerkschnittstelle (eth1) bietet Konnektivität zu den Ressourcen in Ihrer VPC und im Internet und wird verwendet, um dem Verzeichnis WorkSpace beizutreten.
- Die Verwaltungsnetzwerkschnittstelle (eth0) ist mit einem sicheren WorkSpaces-Verwaltungsnetzwerk verbunden. Es wird für das WorkSpace interaktive Streaming des Desktops an WorkSpaces Clients verwendet und ermöglicht WorkSpaces die Verwaltung des WorkSpace.

WorkSpaces wählt die IP-Adresse für die Verwaltungsnetzwerkschnittstelle aus verschiedenen Adressbereichen aus, abhängig von der Region, in der die erstellt WorkSpaces werden. Wenn ein Verzeichnis registriert ist, WorkSpaces testet das VPC CIDR und die Routing-Tabellen in Ihrer VPC, um festzustellen, ob diese Adressbereiche einen Konflikt verursachen. Bei einem Konflikt in allen verfügbaren Adressbereichen in der Region wird eine Fehlermeldung angezeigt, und das Verzeichnis wird nicht registriert. Wenn Sie die Routing-Tabellen in Ihrer VPC ändern, nachdem das Verzeichnis registriert wurde, können Sie einen Konflikt verursachen.

Warning

Ändern oder löschen Sie keine der Netzwerkschnittstellen, die an eine angefügt sind WorkSpace. Dies kann dazu führen WorkSpace , dass der nicht mehr erreichbar ist oder den Internetzugang verliert. Wenn Sie beispielsweise die automatische Zuweisung von Elastic IP-Adressen auf Verzeichnisebene aktiviert haben, wird Ihrem WorkSpace beim Start eine Elastic IP-Adresse (aus dem von Amazon bereitgestellten Pool) zugewiesen. Wenn Sie jedoch eine Elastic IP-Adresse, die Sie besitzen WorkSpace, einem zuordnen und diese Elastic IP-Adresse später von der trennen WorkSpace, WorkSpace verliert die ihre öffentliche IP-Adresse und erhält nicht automatisch eine neue aus dem von Amazon bereitgestellten Pool.

Um eine neue öffentliche IP-Adresse aus dem von Amazon bereitgestellten Pool mit dem zu verknüpfen WorkSpace, müssen Sie das neu erstellen WorkSpace. Wenn Sie die nicht neu erstellen möchten WorkSpace, müssen Sie dem eine andere Elastic IP-Adresse zuordnen, die Sie besitzen WorkSpace.

IP-Adressbereiche für Verwaltungsschnittstellen

In der folgenden Tabelle werden die für die einzelnen IP-Adressbereiche für die Verwaltungsnetzwerkschnittstelle aufgeführt.

> **Note**
>
> - Wenn Sie Bring Your Own License (BYOL) Windows verwenden WorkSpaces, gelten die IP-Adressbereiche in der folgenden Tabelle nicht. Stattdessen WorkSpaces verwendet PCoIP BYOL den IP-Adressbereich 54.239.224.0/20 für den Datenverkehr der Verwaltungsschnittstelle in allen AWS Regionen. Für WSP BYOL Windows gelten sowohl die IP-Adressbereiche 54.239.224.0/20 WorkSpacesals auch 10.0.0.0/8 in allen AWS Regionen. (Diese IP-Adressbereiche werden zusätzlich zum CIDR-Block /16 verwendet, den Sie für die Verwaltung des Datenverkehrs für Ihr BYOL auswählen WorkSpaces.)
> - Wenn Sie WSP verwenden, das aus öffentlichen Paketen WorkSpaces erstellt wurde, gilt der IP-Adressbereich 10.0.0.0/8 zusätzlich zu den in der folgenden Tabelle aufgeführten PCoIP-/WSP-Bereichen auch für den Datenverkehr der Verwaltungsschnittstelle in allen AWS Regionen.

Region	IP-Adressbereich
USA Ost (Nord-Virginia)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
USA West (Oregon)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 und 198.19.0.0/16 WSP: 10.0.0.0/8
Asien-Pazifik (Mumbai)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
Asien-Pazifik (Seoul)	PCoIP/WSP: 198.19.0.0/16

Region	IP-Adressbereich
	WSP: 10.0.0.0/8
Asien-Pazifik (Singapur)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Asien-Pazifik (Sydney)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 und 198.19.0.0/16 WSP: 10.0.0.0/8
Asien-Pazifik (Tokio)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Kanada (Zentral)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Frankfurt)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Irland)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 und 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (London)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Südamerika (São Paulo)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Afrika (Kapstadt)	PCoIP/WSP: 172.31.0.0/16 und 198.19.0.0/16 WSP: 10.0.0.0/8

Region	IP-Adressbereich
Israel (Tel Aviv)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
AWS GovCloud (USA-West)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8 und 192.169.0.0/16
AWS GovCloud (USA-Ost)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

Ports für die Verwaltungsschnittstelle

Die folgenden Ports müssen auf der Verwaltungsnetzwerkschnittstelle aller geöffnet sein WorkSpaces:

- Eingehendes TCP an Port 4172. Dieser Port wird zum Aufbau einer Streaming-Verbindung im PCoIP-Protokoll verwendet.
- Eingehendes UDP an Port 4172. Dies wird für das Streaming von Benutzereingaben im PCoIP-Protokoll verwendet.
- Eingehendes TCP an Port 4489. Dies dient dem Zugriff anhand des Webclients.
- Eingehendes TCP an Port 8200. Dies wird für die Verwaltung und Konfiguration des verwendet WorkSpace.
- Eingehendes TCP an den Ports 8201–8250. Diese Ports werden für den Aufbau der Streaming-Verbindung und für das Streaming von Benutzereingaben im WSP-Protokoll verwendet.
- Eingehendes UDP an Port 8220. Dieser Port wird für den Aufbau der Streaming-Verbindung und für das Streaming von Benutzereingaben im WSP-Protokoll verwendet.
- Ausgehender TCP-Datenverkehr auf Ports 8443 und 9997. Dies dient dem Zugriff anhand des Webclients.
- Ausgehender UDP-Datenverkehr auf Ports 3478, 4172 und 4195. Dies dient dem Zugriff anhand des Webclients.
- Ausgehender UDP-Datenverkehr auf Ports 50002 und 55002. Dieser wird für das Streaming verwendet. Wenn Ihre Firewall mit Stateful-Filterung arbeitet, werden die flüchtigen Ports

50002 und 55002 automatisch für die zurückgesendete Kommunikation geöffnet. Wenn Ihre Firewall mit Stateless-Filterung arbeitet, müssen Sie die flüchtigen Ports 49152 – 65535 für die zurückgesendete Kommunikation öffnen.

- Ausgehendes TCP auf Port 80, wie in den IP-Bereichen der Verwaltungsschnittstelle definiert, an die IP-Adresse 169.254.169.254 für den Zugriff auf den EC2-Metadatenservice. Jeder HTTP-Proxy, der Ihrem zugewiesen ist, WorkSpaces muss auch 169.254.169.254 ausschließen.
- Ausgehender TCP-Datenverkehr auf Port 1688 zu den IP-Adressen 169.254.169.250 und 169.254.169.251, um für die Aktivierung von Windows für WorkSpaces, die auf öffentlichen Bundles basieren, Zugriff auf Microsoft KMS zu gewähren. Wenn Sie Bring Your Own License (BYOL) Windows verwenden WorkSpaces, müssen Sie den Zugriff auf Ihre eigenen KMS-Server für die Windows-Aktivierung zulassen.
- Ausgehendes TCP auf Port 1688 an IP-Adresse 54.239.236.220, um den Zugriff auf Microsoft KMS für die Office-Aktivierung für BYOL zu ermöglichen WorkSpaces.

  Wenn Sie Office über eines der WorkSpaces öffentlichen Pakete verwenden, variiert die IP-Adresse für Microsoft KMS für die Office-Aktivierung. Um diese IP-Adresse zu ermitteln, suchen Sie die IP-Adresse für die Verwaltungsschnittstelle des WorkSpaceund ersetzen Sie dann die letzten beiden Oktette durch `64.250`. Wenn die IP-Adresse der Verwaltungsschnittstelle beispielsweise 192.168.3.5 ist, lautet die IP-Adresse für die Office-Aktivierung für Microsoft KMS 192.168.64.250.
- Ausgehender TCP-Datenverkehr an die IP-Adresse 127.0.0.2 für WSP WorkSpaces , wenn der WorkSpace Host für die Verwendung eines Proxy-Servers konfiguriert ist.
- Kommunikation, die von der Loopback-Adresse 127.0.01 ausgeht.

Unter normalen Umständen konfiguriert der WorkSpaces Service diese Ports für Ihr WorkSpaces. Wenn auf einer Sicherheits- oder Firewall-Software installiert ist WorkSpace , die einen dieser Ports blockiert, funktioniert die WorkSpace möglicherweise nicht richtig oder ist möglicherweise nicht erreichbar.

Primäre Schnittstellen-Ports

Unabhängig davon, welche Art von Verzeichnis Sie haben, müssen die folgenden Ports auf der primären Netzwerkschnittstelle aller geöffnet sein WorkSpaces:

- Für die Internetverbindung müssen die folgenden Ports ausgehend zu allen Zielen und von der WorkSpaces VPC aus eingehen. Sie müssen diese manuell zur Sicherheitsgruppe für Ihr hinzufügen, WorkSpaces wenn Sie möchten, dass sie Internetzugang haben.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)

- Um mit den Verzeichniscontrollern zu kommunizieren, müssen die folgenden Ports zwischen Ihrer WorkSpaces VPC und Ihren Verzeichniscontrollern geöffnet sein. Bei einem Simple-AD-Verzeichnis sind diese Ports bei der durch AWS Directory Service erstellten Sicherheitsgruppe richtig konfiguriert. Bei einem AD-Connector-Verzeichnis müssen Sie die Standard-Sicherheitsgruppe für die VPC möglicherweise anpassen, um diese Ports zu öffnen.
  - TCP/UDP 53 – DNS
  - TCP/UDP 88 – Kerberos-Authentifizierung
  - UDP 123 – NTP
  - TCP 135 – RPC
  - UDP 137-138 – Netlogon
  - TCP 139 – Netlogon
  - TCP/UDP 389 – LDAP
  - TCP/UDP 445 – SMB
  - TCP/UDP 636 – LDAPS (LDAP über TLS/SSL)
  - TCP 1024-65535 – Dynamische Ports für RPC

  Wenn Sicherheits- oder Firewall-Software auf einer installiert ist WorkSpace , die einen dieser Ports blockiert, funktioniert die WorkSpace möglicherweise nicht richtig oder ist möglicherweise nicht erreichbar.

IP-Adresse und Port-Anforderungen nach Region

USA Ost (Nord-Virginia)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/

Kategorie	Details
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.us-east-1.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.us-east-1.amazonaws.com

Kategorie	Details
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • USA Ost (Nord-Virginia) – https://d32i4gd7pg4909.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung

Kategorie	Details
Smartcard-Authentifizierungsendpunkte vor der Sitzung	https://smartcard.us-east-1.signin.aws
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domains: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com
WorkSpaces API-Endpunkte	Domains: https://workspaces.us-east-1.amazonaws.com
Sitzungs-Broker (PCM)	Domains: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.us-east-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-iad.amazonworkspaces.com

Kategorie	Details
IP-Adressen für die Zustandsprüfung	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255
IP-Adressbereich der WSP-Gatewayserver	• 3.227.4.0/22 • 44.209.84.0/22
WSP-Gateway-Domänenname	*.prod.us-east-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

USA West (Oregon)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain:

Kategorie	Details
	https://skylight-client-ds.us-west-2.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.us-west-2.amazonaws.com

Kategorie	Details
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • USA West (Oregon) – https://d18af777lco7lp.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung

Kategorie	Details
Smartcard-Authentifizierungsendpunkte vor der Sitzung	https://smartcard.us-west-2.signin.aws
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domains: • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com
WorkSpaces API-Endpunkte	Domains: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
Sitzungs-Broker (PCM)	Domains: • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.us-west-2.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-pdx.amazonworkspaces.com

Kategorie	Details
IP-Adressen für die Zustandsprüfung	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 35.80.88.0 – 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
IP-Adressbereich der WSP-Gatewayserver	34.223.96.0/22
WSP-Gateway-Domänenname	*.prod.us-west-2.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

Asien-Pazifik (Mumbai)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.ap-south-1.amazonaws.com

Kategorie	Details
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.ap-south-1.amazonaws.com

Kategorie	Details
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Asien-Pazifik (Mumbai) – https://d78hovzzqqtsb.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung

Kategorie	Details
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.ap-south-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.ap-south-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.ap-south-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Web Access ist derzeit in der Region Asien-Pazifik (Mumbai) nicht verfügbar
Hostname der Systemzustandsprüfung	drp-bom.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 13.127.57.82 • 13.234.250.73
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	13.126.243.0 – 13.126.243.255
IP-Adressbereich der WSP-Gatewayserver	65.1.156.0/22
WSP-Gateway-Domänenname	*.prod.ap-south-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 192.168.0.0/16 • WSP: 10.0.0.0/8

Asien-Pazifik (Seoul)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Gerätemetriken (für WorkSpaces Client-Anwendungen ab 1.0 und 2.0)	https://device-metrics-us-2.amazon.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.ap-northeast-2.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.ap-northeast-2.amazonaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>

Kategorie	Details
	Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Asien-Pazifik (Seoul) – https://dtyv4uwoh7ynt.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.ap-northeast-2.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.ap-northeast-2.amazonaws.com

Kategorie	Details
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.ap-northeast-2.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.ap-northeast-2.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-icn.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 3.34.37.0 – 3.34.37.255 • 3.34.38.0 – 3.34.39.255 • 13.124.247.0 - 13.124.247.255
IP-Adressbereich der WSP-Gatewayserver	3.35.160.0/22
WSP-Gateway-Domänenname	*.prod.ap-northeast-2.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asien-Pazifik (Singapur)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/

Kategorie	Details
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.ap-southeast-1.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.ap-southeast-1.amazonaws.com

Kategorie	Details
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Asien-Pazifik (Singapur) – https://d3qzmd7y07pz0i.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung

Kategorie	Details
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.ap-southeast-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.ap-southeast-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.ap-southeast-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.ap-southeast-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-sin.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 18.141.152.0 – 18.141.152.255 • 18.141.154.0 – 18.141.155.255 • 52.76.127.0 - 52.76.127.255
IP-Adressbereich der WSP-Gatewayserver	13.212.132.0/22

Kategorie	Details
WSP-Gateway-Domänenname	*.prod.ap-southeast-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnitt stellen	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asien-Pazifik (Sydney)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-An wendungen ab Version 3.0)	Domain: https://skylight-client-ds.ap-southeast-2.ama zonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.ap-southeast-2.amaz onaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenver zeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/ <region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/

Kategorie	Details
	Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Asien-Pazifik (Sydney) – https://dwcpoxuuza83q.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Smartcard-Authentifizierungsendpunkte vor der Sitzung	https://smartcard.ap-southeast-2.signin.aws
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)

Kategorie	Details
WS Broker	Domain: • https://ws-broker-service.ap-southeast-2.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.ap-southeast-2.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.ap-southeast-2.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.ap-southeast-2.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-syd.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 3.24.11.127 • 13.237.232.125
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 3.25.43.0 – 3.25.43.255 • 3.25.44.0 – 3.25.45.255 • 54.153.254.0 - 54.153.254.255
IP-Adressbereich der WSP-Gatewayserver	3.25.248.0/22
WSP-Gateway-Domänenname	*.prod.ap-southeast-2.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 und 198.19.0.0/16 • WSP: 10.0.0.0/8

Asien-Pazifik (Tokio)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.ap-northeast-1.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.ap-northeast-1.amazonaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene:

Kategorie	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Asien-Pazifik (Tokio) – https://d2c2t8mxjhq5z1.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Smartcard-Authentifizierungsendpunkte vor der Sitzung	https://smartcard.ap-northeast-1.signin.aws
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.ap-northeast-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.ap-northeast-1.amazonaws.com

Kategorie	Details
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.ap-northeast-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.ap-northeast-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-nrt.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 18.178.102.247 • 54.64.174.128
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
IP-Adressbereich der WSP-Gatewayserver	3.114.164.0/22
WSP-Gateway-Domänenname	*.prod.ap-northeast-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Kanada (Zentral)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/

Kategorie	Details
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.ca-central-1.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.ca-central-1.amazonaws.com

Kategorie	Details
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Kanada (Zentral) – https://d2wfbsypmqjmog.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung

Kategorie	Details
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.ca-central-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.ca-central-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.ca-central-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.ca-central-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-yul.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 15.223.100.0 – 15.223.100.255 • 15.223.102.0 – 15.223.103.255 • 35.183.255.0 - 35.183.255.255
IP-Adressbereich der WSP-Gatewayserver	3.97.20.0/22

Kategorie	Details
WSP-Gateway-Domänenname	*.prod.ca-central-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnitt stellen	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Frankfurt)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-An wendungen ab Version 3.0)	Domain: https://skylight-client-ds.eu-central-1.amazo naws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.eu-central-1.amazon aws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenver zeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/ <region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/

Kategorie	Details
	Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Europa (Frankfurt) – https://d1whcm49570jjw.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.eu-central-1.amazonaws.com

Kategorie	Details
WorkSpaces API-Endpunkte	Domain: • https://workspaces.eu-central-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.eu-central-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.eu-central-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-fra.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 18.156.52.0 – 18.156.52.255 • 18.156.54.0 – 18.156.55.255 • 52.59.127.0 - 52.59.127.255
IP-Adressbereich der WSP-Gatewayserver	18.192.216.0/22
WSP-Gateway-Domänenname	*.prod.eu-central-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Irland)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.eu-west-1.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.eu-west-1.amazonaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene:

Kategorie	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Europa (Irland) – https://d3pgffbf39h4k4.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Smartcard-Authentifizierungsendpunkte vor der Sitzung	https://smartcard.eu-west-1.signin.aws
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.eu-west-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.eu-west-1.amazonaws.com

Kategorie	Details
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.eu-west-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.eu-west-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-dub.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 3.249.28.0 – 3.249.29.255 • 52.19.124.0 - 52.19.125.255
IP-Adressbereich der WSP-Gatewayserver	3.248.176.0/22
WSP-Gateway-Domänenname	*.prod.eu-west-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 und 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (London)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/

Kategorie	Details
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.eu-west-2.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.eu-west-2.amazonaws.com

Kategorie	Details
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Europa (London) – https://d16q6638mh01s7.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung

Kategorie	Details
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.eu-west-2.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.eu-west-2.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.eu-west-2.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.eu-west-2.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-lhr.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 18.132.21.0 – 18.132.21.255 • 18.132.22.0 – 18.132.23.255 • 35.176.32.0 - 35.176.32.255
IP-Adressbereich der WSP-Gatewayserver	18.134.68.0/22

Kategorie	Details
WSP-Gateway-Domänenname	*.prod.eu-west-2.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnitt stellen	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Südamerika (São Paulo)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-An wendungen ab Version 3.0)	Domain: https://skylight-client-ds.sa-east-1.amazonaw s.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.sa-east-1.amazonaws .com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenver zeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/ <region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/

Kategorie	Details
	Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Südamerika (São Paulo) – https://d2lh2qc5bdoq4b.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.sa-east-1.amazonaws.com

Kategorie	Details
WorkSpaces API-Endpunkte	Domain: • https://workspaces.sa-east-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.sa-east-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.sa-east-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-gru.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 18.230.103.0 – 18.230.103.255 • 18.230.104.0 – 18.230.105.255 • 54.233.204.0 – 54.233.204.255
IP-Adressbereich der WSP-Gatewayserver	15.228.64.0/22
WSP-Gateway-Domänenname	*.prod.sa-east-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Afrika (Kapstadt)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.af-south-1.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://ws-client-service.af-south-1.amazonaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene:

Kategorie	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Afrika (Kapstadt) – https://di5ygl2cs0mrh.cloudfront.net/
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.af-south-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.af-south-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.af-south-1.amazonaws.com

Kategorie	Details
Hostname der Systemzustandsprüfung	drp-cpt.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 13.246.120.0 – 13.246.123.255
IP-Adressbereich der WSP-Gatewayserver	15.228.64.0/22
WSP-Gateway-Domänenname	*.prod.af-south-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnittstellen	• 172.31.0.0/16 und 198.19.0.0/16 • WSP: 10.0.0.0/8

Israel (Tel Aviv)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://d2td7dqidlhjx7.cloudfront.net/
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: https://skylight-client-ds.il-central-1.amazonaws.com
Dynamic Messaging Service (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain:

Kategorie	Details
	https://ws-client-service.il-central-1.amazonaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • CSS-Datei zum Gestalten der Anmeldeseiten: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript -Datei für die Anmeldeseiten: • Israel (Tel Aviv); –
Forrester-Protokollservice	https://fls-na.amazon.com/

Kategorie	Details
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://<directory id>.awsapps.com/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.il-central-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.il-central-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.il-central-1.amazonaws.com
Web-Access-TURN-Server für PCoIP	Server: • turn:*.il-central-1.rdn.amazonaws.com
Hostname der Systemzustandsprüfung	drp-tlv.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 51.17.28.0-51.17.31.255
IP-Adressbereich der WSP-Gatewayserver	51.17.72.0/22

Kategorie	Details
WSP-Gateway-Domänenname	*.prod.il-central-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnitt stellen	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud Region (USA-West)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/WorkSpacesAppCast.xml
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: hhttps://skylight-client-ds.us-gov-west-1.amazonaws.com
Dynamic Messaging Service (für Clientanwendungen ab WorkSpaces Version 3.0)	Domain: https://ws-client-service.us-gov-west-1.amazonaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients:

Kategorie	Details
	• https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<Verzeichnis-ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/<Verzeichnis-ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript -Datei für die Anmeldeseiten: • Nicht zutreffend
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Smartcard-Authentifizierungsendpunkte vor der Sitzung	https://smartcard.signin.amazonaws-us-gov.com
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Benutzer-Anmeldeseiten	https://login.us-gov-home.awsapps.com/directory/<directory id>/ (wobei <directory id> die Domain des Kunden ist)

Kategorie	Details
WS Broker	Domain: • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com
Hostname der Systemzustandsprüfung	drp-pdt.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 52.61.193.0 - 52.61.193.255

Kategorie	Details
IP-Adressbereich der WSP-Gatewayserver	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
WSP-Gateway-Domänenname	*.prod.us-gov-west-1.highlander.aws.a2z.com
IP-Adressbereiche für Verwaltungsschnitt stellen	• 198.19.0.0/16 • WSP: 10.0.0.0/8 und 192.169.0.0/16

AWS GovCloud Region (USA-Ost)

Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Kategorie	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Automatische Aktualisierung des Clients	https://s3.amazonaws.com/workspaces-client-updates/prod/osu/windows/WorkSpacesAppCast.xml
Konnektivitätsprüfung	https://connectivity.amazonworkspaces.com/
Client-Metriken (für WorkSpaces Client-Anwendungen ab Version 3.0)	Domain: hhttps://skylight-client-ds.us-gov-east-1.amazonaws.com
Dynamic Messaging Service (für Clientanwendungen ab WorkSpaces Version 3.0)	Domain: https://ws-client-service.us-gov-east-1.amazonaws.com
Verzeichniseinstellungen	Authentifizierung vom Client zum Kundenverzeichnis, bevor Sie sich bei der anmelden WorkSpace:

Kategorie	Details
	• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Verbindungen von macOS-Clients: • https://d32i4gd7pg4909.cloudfront.net/ Kunden-Verzeichniseinstellungen: • https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<Verzeichnis-ID> Grafiken auf der Anmeldeseite für das Co-Branding auf Kundenverzeichnisebene: • https://s3.amazonaws.com/workspaces-client-assets/prod/osu/<Verzeichnis-ID> CSS-Datei zum Gestalten der Anmeldeseiten: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript -Datei für die Anmeldeseiten: • Nicht zutreffend
Forrester-Protokollservice	https://fls-na.amazon.com/
Zustandsprüfungsserver (DRP)	Server für die Zustandsprüfung
Smartcard-Authentifizierungsendpunkte vor der Sitzung	https://smartcard.signin.amazonaws-us-gov.com
Registrierungsabhängigkeit (für Web Access und Teradici PCoIP Zero Clients)	https://s3.amazonaws.com

Kategorie	Details
Benutzer-Anmeldeseiten	https://login.us-gov-home.awsapps.com/directory/<directory id>/ (wobei <directory id> die Domain des Kunden ist)
WS Broker	Domain: • https://ws-broker-service.us-gov-east-1.amazonaws.com • https://ws-broker-service-fips.us-gov-east-1.amazonaws.com
WorkSpaces API-Endpunkte	Domain: • https://workspaces.us-gov-east-1.amazonaws.com • https://workspaces-fips.us-gov-east-1.amazonaws.com
Sitzungs-Broker (PCM)	Domain: • https://skylight-cm.us-gov-east-1.amazonaws.com • https://skylight-cm-fips.us-gov-east-1.amazonaws.com
Hostname der Systemzustandsprüfung	drp-osu.amazonworkspaces.com
IP-Adressen für die Zustandsprüfung	• 18.253.251.70 • 18.254.0.118
Öffentlicher IP-Adressbereich für PCoIP-Gatewayserver	• 18.254.140.0 – 18.254.143.255
IP-Adressbereich der WSP-Gatewayserver	18.254.148.0/22
WSP-Gateway-Domänenname	*.prod.us-gov-east-1.highlander.aws.a2z.com

Kategorie	Details
IP-Adressbereiche für Verwaltungsschnitt stellen	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Netzwerkanforderungen an Amazon-WorkSpaces-Clients

Ihre WorkSpaces-Benutzer können Verbindungen mit ihren WorkSpaces mithilfe der Clientanwendung für ein unterstütztes Gerät herstellen. Alternativ können sie einen Webbrowser verwenden, um eine Verbindung mit WorkSpaces herzustellen, die diese Art des Zugriffs unterstützen. Eine Liste der WorkSpaces, die den Webbrowserzugriff unterstützen, finden Sie unter „Welche Amazon-WorkSpaces-Pakete unterstützen Webzugriff?“ in Clientzugriff, Webzugriff und Benutzererfahrung.

> **Note**
>
> Sie können keinen Webbrowser verwenden, um eine Verbindung mit Amazon Linux WorkSpaces herzustellen.

> **Important**
>
> Ab dem 1. Oktober 2020 können Kunden den Access-Client von Amazon WorkSpaces Web nicht mehr verwenden, um eine Verbindung mit benutzerdefinierten WorkSpaces für Windows 7 oder mit Bring-Your-Own-License (BYOL)-WorkSpaces für Windows 7 herzustellen.

Um Ihren Benutzern eine gute Erfahrung mit ihren WorkSpaces zu bieten, stellen Sie sicher, dass die Client-Geräte die folgenden Netzwerkanforderungen erfüllen:

- Das Client-Gerät muss über eine Breitband-Internetverbindung verfügen. Wir empfehlen die Planung für mindestens 1 Mbit/s pro gleichzeitigen Benutzer, der ein 480p-Videofenster ansieht. Abhängig von den Anforderungen der Benutzerqualität für die Videoauflösung ist möglicherweise mehr Bandbreite erforderlich.

- Das Netzwerk, mit dem das Client-Gerät verbunden ist und jegliche Firewalls auf dem Client-Gerät müssen bestimmte Ports für die IP-Adressbereiche für verschiedene AWS-Services geöffnet haben. Weitere Informationen finden Sie unter IP-Adresse und Port-Anforderungen für WorkSpaces.
- Für eine optimale Leistung von PCoIP sollte die Round-Trip-Zeit (RTT) zwischen dem Netzwerk des Clients und der Region, in der sich die WorkSpaces befinden, maximal 100 ms betragen. Wenn die Round-Trip-Zeit (RTT) zwischen 100 ms und 200 ms liegt, kann der Benutzer auf den WorkSpace zugreifen, aber die Leistung ist vermindert. Wenn die Round-Trip-Zeit (RTT) zwischen 200 ms und 375 ms liegt, ist die Leistung beeinträchtigt. Wenn die Round-Trip-Zeit (RTT) 375 ms überschreitet, wird die WorkSpaces-Clientverbindung beendet.

  Für die beste Leistung des WorkSpaces Streaming Protocol darf die Round-Trip-Zeit (RTT) vom Netzwerk des Clients zur Region, in der sich die WorkSpaces befinden, maximal 250 ms betragen. Wenn die Round-Trip-Zeit (RTT) zwischen 250 ms und 400 ms liegt, kann der Benutzer auf den WorkSpace zugreifen, aber die Leistung ist vermindert.

  Verwenden Sie die Zustandsprüfung der Verbindung von Amazon WorkSpaces, um die Round-Trip-Zeit zu den verschiedenen AWS-Regionen von Ihrem Standort aus zu überprüfen.
- Wenn Sie Webcams mit WSP verwenden möchten, empfehlen wir eine Upload-Bandbreite von mindestens 1,7 Megabit pro Sekunde.
- Wenn die Benutzer über ein virtuelles privates Netzwerk (VPN) auf ihren WorkSpace zugreifen, muss die Verbindung eine Maximum Transmission Unit (MTU, maximale Übertragungseinheit) von mindestens 1200 Byte unterstützen.

  > **Note**
  >
  > Sie können auf WorkSpaces nicht über ein VPN zugreifen, das mit Ihrer Virtual Private Cloud (VPC) verbunden ist. Um über ein VPN auf WorkSpaces zuzugreifen, ist eine Internetverbindung (über die öffentlichen IP-Adressen des VPN) erforderlich, wie unter IP-Adresse und Port-Anforderungen für WorkSpaces beschrieben.

- Die Clients benötigen HTTPS-Zugriff auf WorkSpaces-Ressourcen, die vom Service und Amazon Simple Storage Service (Amazon S3) gehostet werden. Die Clients unterstützen keine Proxy-Umleitung auf Anwendungsebene. Der HTTPS-Zugriff ist erforderlich, damit Benutzer die Registrierung erfolgreich abschließen und auf ihre WorkSpaces zugreifen können.
- Wenn Sie den Zugriff von PCoIP-Zero-Clientgeräten aus ermöglichen möchten, müssen Sie ein PCoIP-Protokollpaket für WorkSpaces verwenden. Sie müssen auch das Network Time Protocol

(NTP) in Teradici aktivieren. Weitere Informationen finden Sie unter Einrichten von PCoIP-Zero-Clients für WorkSpaces.

- Wenn Sie bei 3.0+ Clients Single Sign-On (SSO) für Amazon WorkDocs verwenden, müssen Sie die Anweisungen unter Single Sign-On im Administratorhandbuch für AWS Directory Service befolgen.

Sie können wie folgt überprüfen, ob ein Client-Gerät die Netzwerkanforderungen erfüllt.

So überprüfen Sie die Netzwerkanforderungen für 3.0+ Clients

1. Öffnen Sie den WorkSpaces-Client. Wenn Sie den Client das erste Mal öffnen, werden Sie aufgefordert, den Registrierungscode einzugeben, den Sie in der Einladungs-E-Mail erhalten haben.
2. Führen Sie je nachdem, welchen Client Sie verwenden, einen der folgenden Schritte aus.

Verwendetes Betriebssystem	Vorgehensweise
Windows- oder Linux-Clients	Wählen Sie in der oberen rechten Ecke der Clientanwendung das Symbol Netzwerk aus .
macOS-Client	Wählen Sie Connections (Verbindungen), Network (Netzwerk).

   Die Client-Anwendung testet die Netzwerkverbindung, Ports und die Umlaufzeit und erstellt einen Bericht mit den Ergebnissen dieser Tests.
3. Schließen Sie das Dialogfeld Network (Netzwerk) um zur Anmeldeseite zurückzukehren.

So überprüfen Sie die Netzwerkanforderungen für 1.0+ und 2.0+ Clients

1. Öffnen Sie den WorkSpaces-Client. Wenn Sie den Client das erste Mal öffnen, werden Sie aufgefordert, den Registrierungscode einzugeben, den Sie in der Einladungs-E-Mail erhalten haben.

2. Klicken Sie auf Network (Netzwerk) in der unteren rechten Ecke der Client-Anwendung. Die Client-Anwendung testet die Netzwerkverbindung, Ports und die Umlaufzeit und erstellt einen Bericht mit den Ergebnissen dieser Tests.
3. Klicken Sie auf Dismiss (Verwerfen), um auf die Anmeldeseite zurückzukehren.

Beschränken des WorkSpaces Zugriffs auf vertrauenswürdige Geräte

Standardmäßig können Benutzer WorkSpaces von jedem unterstützten Gerät, das mit dem Internet verbunden ist, auf ihr zugreifen. Wenn Ihr Unternehmen den Zugriff auf Unternehmensdaten auf vertrauenswürdige Geräte (auch als verwaltete Geräte bezeichnet) einschränkt, können Sie den WorkSpaces Zugriff auf vertrauenswürdige Geräte mit gültigen Zertifikaten einschränken.

Wenn Sie diese Funktion aktivieren, WorkSpaces verwendet die zertifikatbasierte Authentifizierung, um festzustellen, ob ein Gerät vertrauenswürdig ist. Wenn die WorkSpaces Clientanwendung nicht überprüfen kann, ob ein Gerät vertrauenswürdig ist, blockiert sie Versuche, sich anzumelden oder erneut eine Verbindung vom Gerät herzustellen.

Für jedes Verzeichnis, können Sie bis zu zwei Root-Zertifikate importieren. Wenn Sie zwei Stammzertifikate importieren, WorkSpaces stellt sie beide dem Client vor und der Client findet das erste gültige übereinstimmende Zertifikat, das bis zu einem der Stammzertifikate verkettet ist.

Unterstützte Clients

- Android auf Android- oder Android-kompatiblen Chrome-OS-Systemen
- macOS
- Windows

> **Important**
>
> Dieses Feature wird von den folgenden Clients nicht unterstützt:
>
> - WorkSpaces -Clientanwendungen für Linux oder iPad
> - Clients von Drittanbietern, einschließlich, aber nicht beschränkt auf Teradici PCoIP, RDP-Clients und Remote-Desktop-Anwendungen.

Schritt 1: Erstellen der Zertifikate

Diese Funktion erfordert zwei Arten von Zertifikaten: Root-Zertifikate, die durch eine interne Zertifizierungsstelle (CA) erstellt wurden und Client-Zertifikate, die bis zu einem Root-Zertifikat verkettet sind.

Voraussetzungen

- Stammzertifikate müssen Base64-kodierte Zertifikat-Dateien im CRT-, CERT oder PEM-Format sein.
- Stammzertifikate müssen dem folgenden Muster für reguläre Ausdrücke entsprechen, was bedeutet, dass jede kodierte Zeile außer der letzten genau 64 Zeichen lang sein muss: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`.
- Zertifikate müssen einen Common Name beinhalten.
- Gerätezertifikate müssen die folgenden Erweiterungen enthalten: `Key Usage: Digital Signature` und `Enhanced Key Usage: Client Authentication`.
- Alle Zertifikate in der Kette vom Gerätezertifikat bis zur vertrauenswürdigen Stammzertifizierungsstelle müssen auf dem Client-Gerät installiert sein.
- Die maximal unterstützte Länge der Zertifikatskette ist 4.
- WorkSpaces unterstützt derzeit keine Mechanismen zum Gerätewiderruf, z. B. Zertifikatsperrlisten (CRL) oder Online Certificate Status Protocol (OCSP), für Clientzertifikate.
- Verwenden Sie einen starken Verschlüsselungsalgorithmus. Wir empfehlen SHA256 mit RSA, SHA256 mit ECDSA, SHA384 mit ECDSA oder SHA512 mit ECDSA.
- Wenn sich das Gerätezertifikat in der System-Keychain befindet, empfehlen wir für macOS, dass Sie die WorkSpaces Clientanwendung für den Zugriff auf diese Zertifikate autorisieren. Andernfalls müssen Benutzer die Schlüsselketten-Anmeldeinformationen eingeben, wenn sie sich anmelden oder erneut verbinden.

Schritt 2: Bereitstellen von Client-Zertifikaten auf vertrauenswürdigen Geräten

Auf den vertrauenswürdigen Geräten für Ihre Benutzer müssen Sie ein Zertifikatspaket installieren, das alle Zertifikate in der Kette vom Gerätezertifikat bis zur vertrauenswürdigen

Stammzertifizierungsstelle enthält. Sie können Ihre bevorzugte Lösung für die Installation der Zertifikate für die Gruppe von Client-Geräten verwenden, z. B. System-Center-Konfigurationsmanager (SCCM) oder die Verwaltung mobiler Geräte (MDM). Beachten Sie, dass SCCM und MDM optional eine Bewertung des Sicherheitsstatus durchführen können, um festzustellen, ob die Geräte Ihren Unternehmensrichtlinien für den Zugriff auf entsprechen WorkSpaces.

Die WorkSpaces Clientanwendungen suchen wie folgt nach Zertifikaten:

- Android – Gehen Sie zu Einstellungen, wählen Sie Sicherheit und Speicherort, Anmeldeinformationen und anschließend Von SD-Karte installieren aus.
- Android-kompatible Chrome-OS-Systeme – Öffnen Sie die Android-Einstellungen und wählen Sie Sicherheit und Speicherort, Anmeldeinformationen und dann Von SD-Karte installieren aus.
- macOS – Durchsucht die Schlüsselkette nach Client-Zertifikaten.
- Windows – Durchsucht die Benutzer- und Stammzertifikatsspeicher nach Client-Zertifikaten.

Schritt 3: Konfigurieren der Beschränkung

Nachdem Sie die Client-Zertifikate auf den vertrauenswürdigen Geräten bereitgestellt haben, können Sie das Verzeichnis mit eingeschränktem Zugriff aktivieren. Dazu muss die WorkSpaces Clientanwendung das Zertifikat auf einem Gerät validieren, bevor ein Benutzer sich bei einem anmelden kann WorkSpace.

Konfigurieren der Beschränkung

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis aus und klicken Sie anschließend auf Aktionen, Details zur Aktualisierung.
4. Erweitern Sie Zugriffskontrolloptionen.
5. Wählen Sie unter Für jeden Gerätetyp den Gerätetyp aus, welche Geräte auf zugreifen können WorkSpaces.
6. Importieren Sie bis zu zwei Root-Zertifikate. Für jedes Root-Zertifikat, gehen Sie wie folgt vor:
    a. Wählen Sie Importieren aus.
    b. Kopieren Sie Text des Zertifikats in das Formular.

c. Wählen Sie Importieren aus.

7. (Optional) Geben Sie an, ob andere Gerätetypen Zugriff auf haben WorkSpaces.

   a. Scrollen Sie nach unten zum Abschnitt Other Platforms (Andere Plattformen). Standardmäßig sind WorkSpaces Linux-Clients deaktiviert, und Benutzer können WorkSpaces von ihren iOS-Geräten, Android-Geräten, Web Accesss, Chromebooks und PCoIP-Zero-Client-Geräten auf ihre zugreifen.

   b. Wählen Sie die zu aktivierenden Gerätetypen aus und löschen Sie alle anderen.

   c. Um den Zugriff von allen ausgewählten Gerätetypen zu blockieren, wählen Sie Block aus.

8. Wählen Sie Update and Exit aus.

Integrieren von SAML 2.0 in WorkSpaces

Durch die Integration von SAML 2.0 in Ihre WorkSpaces für die Desktop-Sitzungsauthentifizierung können Ihre Benutzer ihre vorhandenen Anmeldeinformationen und Authentifizierungsmethoden aus dem SAML-2.0-Identitätsanbieter (Identity Provider, IdP) über ihren Standard-Webbrowser verwenden. Sie können WorkSpaces über IdP-Funktionen schützen, indem Sie IdP-Funktionen wie Multi-Faktor-Authentifizierung und kontextbezogene Zugriffsrichtlinien zur Authentifizierung von Benutzern in WorkSpaces einsetzen.

Authentifizierungs-Workflow

In den folgenden Abschnitten wird der Authentifizierungsworkflow beschrieben, der von der WorkSpaces-Clientanwendung, WorkSpaces Web Access und einem SAML-2.0-Identitätsanbieter (IdP) initiiert wurde:

- Wenn der Flow vom IdP initiiert wird. Zum Beispiel, wenn Benutzer eine Anwendung im IdP-Portal für Benutzer in einem Webbrowser auswählen.
- Wenn der Flow vom WorkSpaces-Client initiiert wird. Zum Beispiel, wenn Benutzer die Clientanwendung öffnen und sich anmelden.
- Wenn der Flow vom WorkSpaces-Client initiiert wird. Zum Beispiel, wenn Benutzer Web Access in einem Browser öffnen und sich anmelden.

In diesen Beispielen geben Benutzer `user@example.com` ein, um sich beim IdP anzumelden. Der IdP hat eine SAML-2.0-Dienstanbieteranwendung, die für ein WorkSpaces-Verzeichnis konfiguriert

ist. Die Benutzer sind für die WorkSpaces-SAML-2.0-Anwendung autorisiert. Die Benutzer erstellen einen WorkSpace für ihre Namen (`user`) in einem Verzeichnis, das die SAML-2.0-Authentifizierung ermöglicht. Darüber hinaus installieren die Benutzer die WorkSpaces-Clientanwendung auf ihrem Gerät oder verwenden Web Access in einem Webbrowser.

Vom Identitätsanbieter (IdP) initiierter Workflow mit der Clientanwendung

Mit dem vom IdP initiierten Workflow können Benutzer die WorkSpaces-Clientanwendung automatisch auf ihren Geräten registrieren, ohne einen WorkSpaces-Registrierungscode eingeben zu müssen. Die Benutzer melden sich nicht mit dem vom IdP initiierten Workflow bei ihren WorkSpaces an. Die WorkSpaces-Authentifizierung muss von der Clientanwendung ausgehen.

1. Die Benutzer melden sich mit ihrem Webbrowser beim IdP an.
2. Nach der Anmeldung beim IdP wählen die Benutzer die WorkSpaces-Anwendung aus dem IdP-Portal für Benutzer aus.
3. Die Benutzer werden im Browser auf diese Seite umgeleitet. Die WorkSpaces-Clientanwendung wird automatisch geöffnet.

4. Die WorkSpaces-Clientanwendung ist jetzt registriert und die Benutzer können mit der Anmeldung fortfahren, indem sie auf Mit der Anmeldung bei WorkSpaces fortfahren klicken.

Vom Identitätsanbieter (IdP) initiierter Workflow mit Web Access

Mit dem vom IdP initiierten Web-Access-Workflow können Benutzer die WorkSpaces-Clientanwendung automatisch auf ihren Geräten registrieren, ohne einen WorkSpaces-Registrierungscode eingeben zu müssen. Die Benutzer melden sich nicht mit dem vom IdP initiierten

Workflow bei ihren WorkSpaces an. Die WorkSpaces-Authentifizierung muss von Web Access ausgehen.

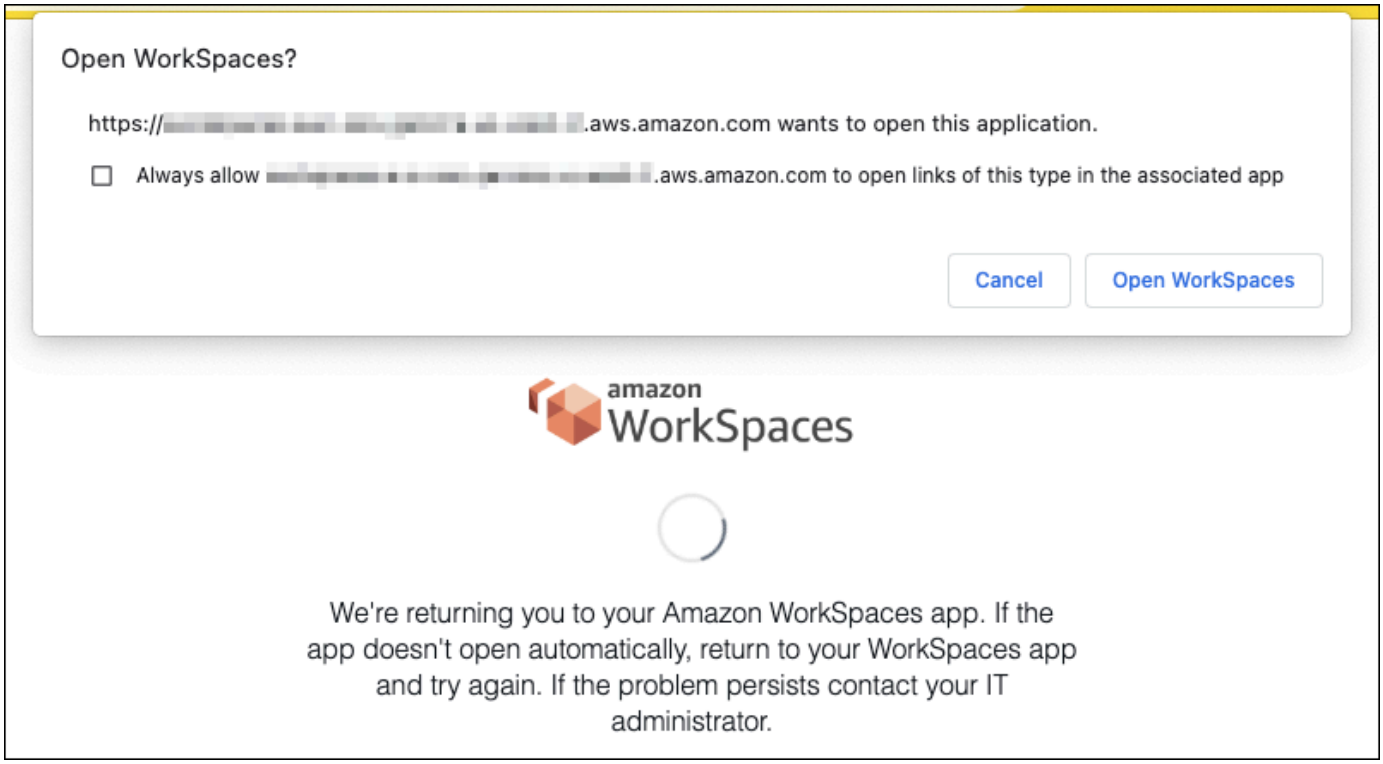
1. Die Benutzer melden sich mit ihrem Webbrowser beim IdP an.
2. Nach der Anmeldung beim IdP wählen die Benutzer die WorkSpaces-Anwendung aus dem IdP-Portal für Benutzer aus.
3. Die Benutzer werden im Browser auf diese Seite umgeleitet. Sie wählen Amazon WorkSpaces im Browser aus, um WorkSpaces zu öffnen.

4. Die WorkSpaces-Clientanwendung ist jetzt registriert und die Benutzer können mit der Anmeldung bei WorkSpaces über Web Access fortfahren.

Vom WorkSpaces-Client initiierter Workflow

Der vom Client initiierte Workflow ermöglicht es Benutzern, sich nach der Anmeldung bei einem IdP bei ihren WorkSpaces anzumelden.

1. Die Benutzer starten die WorkSpaces-Clientanwendung (falls sie nicht bereits ausgeführt wird) und klicken auf Weiter zur Anmeldung bei WorkSpaces.
2. Die Benutzer werden zu ihrem Standard-Webbrowser umgeleitet, um sich beim IdP anzumelden. Wenn die Benutzer in ihrem Browser bereits beim IdP angemeldet sind, müssen sie sich nicht erneut anmelden und überspringen diesen Schritt.
3. Sobald sie beim IdP angemeldet sind, werden die Benutzer zu einem Popup weitergeleitet. Sie folgen den Anweisungen, damit der Webbrowser die Clientanwendung öffnen kann.



4. Die Benutzer werden zur WorkSpaces-Clientanwendung umgeleitet, um die Anmeldung bei ihrem WorkSpace abzuschließen. Die Namen der Benutzer für die WorkSpaces werden automatisch aus der SAML-2.0-Zusicherung des IdP eingetragen. Wenn die Benutzer die zertifikatbasierte Authentifizierung (Certificate-Based Authentication, CBA) verwenden, werden sie automatisch angemeldet.
5. Die Benutzer sind in ihrem WorkSpace angemeldet.

Von WorkSpaces Web Access initiierter Workflow

Der von Web Access initiierte Workflow ermöglicht es Benutzern, sich nach der Anmeldung bei einem IdP bei ihren WorkSpaces anzumelden.

1. Die Benutzer starten den WorkSpaces Web Access und wählen Anmelden aus.
2. Die Benutzer werden in derselben Browser-Registerkarte zum IdP-Portal weitergeleitet. Wenn die Benutzer in ihrem Browser bereits beim IdP angemeldet sind, müssen sie sich nicht erneut anmelden und können diesen Schritt überspringen.
3. Nach der Anmeldung beim IdP werden die Benutzer im Browser zu dieser Seite weitergeleitet. Dann klicken sie auf Bei WorkSpaces anmelden.
4. Die Benutzer werden zur WorkSpaces-Clientanwendung umgeleitet, um die Anmeldung bei ihrem WorkSpace abzuschließen. Die Namen der Benutzer für die WorkSpaces werden

automatisch aus der SAML-2.0-Zusicherung des IdP eingetragen. Wenn die Benutzer die zertifikatbasierte Authentifizierung (Certificate-Based Authentication, CBA) verwenden, werden sie automatisch angemeldet.

5. Die Benutzer sind in ihrem WorkSpace angemeldet.

Einrichten von SAML 2.0

Aktivieren Sie die Registrierung und Anmeldung von WorkSpaces Clientanwendungen WorkSpaces für Ihre Benutzer mithilfe ihrer Anmeldeinformationen und Authentifizierungsmethoden des SAML-2.0-Identitätsanbieters (IdP), indem Sie den Identitätsverbund mit SAML 2.0 einrichten. Verwenden Sie eine IAM-Rolle und eine Relay-State-URL, um Ihren IdP zu konfigurieren und AWS zu aktivieren, um einen Identitätsverbund mit SAML 2.0 einzurichten. Dadurch erhalten Ihre Verbundbenutzer Zugriff auf ein WorkSpaces Verzeichnis. Der Relay-Status ist der WorkSpaces Verzeichnisendpunkt, an den Benutzer weitergeleitet werden, nachdem sie sich erfolgreich bei angemeldet habenAWS.

Inhalt

Voraussetzungen

- Die SAML-2.0-Authentifizierung ist in folgenden Regionen verfügbar:
  - Region USA Ost (Nord-Virginia)
  - Region USA West (Oregon)
  - Region Afrika (Kapstadt)
  - Region Asien-Pazifik (Mumbai)

  - Region Asien-Pazifik (Seoul)
  - Region Asien-Pazifik (Singapur)
  - Region Asien-Pazifik (Sydney)
  - Region Asien-Pazifik (Tokio)
  - Region Kanada (Zentral)
  - Region Europa (Frankfurt)
  - Region Europa (Irland)
  - Region Europa (London)
  - Region Südamerika (São Paulo)
  - Region Israel (Tel Aviv)
  - AWS GovCloud (USA West)
  - AWS GovCloud (USA-Ost)
- Um die SAML-2.0-Authentifizierung mit verwenden zu können WorkSpaces, muss der IdP unerwünschtes, vom IdP initiiertes SSO mit einer Deep-Link-Zielressource oder einer Relay-Status-Endpunkt-URL unterstützen. Beispiele für IdPs sind ADFS, Azure AD, Bol Single Sign-On, Okta PingFederateund PingOne. Weitere Informationen finden Sie in der IdP-Dokumentation.
- Die SAML-2.0-Authentifizierung funktioniert mit , die mit Simple AD WorkSpaces gestartet wurden. Dies wird jedoch nicht empfohlen, da Simple AD nicht in SAML 2.0 integriert ist IdPs.
- Die SAML-2.0-Authentifizierung wird auf den folgenden WorkSpaces Clients unterstützt. Andere Client-Versionen werden für die SAML-2.0-Authentifizierung nicht unterstützt. Öffnen Sie Amazon WorkSpaces Client Downloads, um die neuesten Versionen zu finden:
  - Windows-Client, Version 5.1.0.3029 oder höher
  - macOS-Client, Version 5.x oder höher
  - Web Access

  Andere Clientversionen können keine Verbindung zu herstellen, die für die SAML-2.0-Authentifizierung WorkSpaces aktiviert ist, es sei denn, Fallback ist aktiviert. Weitere Informationen finden Sie unter Aktivieren der SAML-2.0-Authentifizierung im - WorkSpaces Verzeichnis.

step-by-step Anweisungen zur Integration von SAML 2.0 mit WorkSpaces mithilfe von ADFS, Azure AD, Single Sign-On OneLogin, Okta PingFederate und PingOne für Enterprise finden Sie im Handbuch zur Implementierung der Amazon- WorkSpaces SAML-Authentifizierung.

Voraussetzungen

Führen Sie die folgenden Voraussetzungen aus, bevor Sie Ihre SAML-2.0-Identitätsanbieter-(IdP)-Verbindung zu einem WorkSpaces Verzeichnis konfigurieren.

1. Konfigurieren Sie Ihren IdP für die Integration von Benutzeridentitäten aus dem Microsoft Active Directory, das mit dem WorkSpaces Verzeichnis verwendet wird. Für einen Benutzer mit einem müssen WorkSpacedie sAMAccountName- und E-Mail-Attribute für den Active-Directory-Benutzer und die SAML-Anspruchswerte übereinstimmen, damit sich der Benutzer WorkSpaces mit dem IdP bei anmelden kann. Weitere Informationen zur Integration von Active Directory mit Ihrem IdP finden Sie in Ihrer IdP-Dokumentation.
2. Konfigurieren Sie den Identitätsanbieter, um eine Vertrauensbeziehung mit einzurichte AWS.

   - Weitere Informationen zur Konfiguration des AWS-Verbunds finden Sie unter Integrieren von Drittanbieter-SAML-Lösungsanbietern mit AWS. Zu den relevanten Beispielen gehört die IdP-Integration mit AWS-IAM für den Zugriff auf die AWS-Managementkonsole.
   - Nutzen Sie Ihren IdP, um ein Verbundmetadatendokument, in dem Ihre Organisation als IdP beschrieben wird, zu generieren und laden Sie es herunter. Dieses signierte XML-Dokument wird verwendet, um die Vertrauensstellung für die vertrauenden Seiten einzurichten. Speichern Sie diese Datei an einem Standort, auf den Sie später von der IAM-Konsole aus zugreifen können.
3. Erstellen oder registrieren Sie ein Verzeichnis für WorkSpaces mithilfe der - WorkSpaces Managementkonsole. Weitere Informationen finden Sie unter Verwalten von Verzeichnissen für WorkSpaces. Die SAML-2.0-Authentifizierung für WorkSpaces wird für die folgenden Verzeichnistypen unterstützt:

   - AD Connector
   - AWS Managed Microsoft AD
4. Erstellen Sie einen WorkSpace für einen Benutzer, der sich mit einem unterstützten Verzeichnistyp beim IdP anmelden kann. Sie können einen WorkSpace mithilfe der WorkSpaces - WorkSpaces ManagementkonsoleAWS CLI, der oder der API erstellen. Weitere Informationen finden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

Schritt 1: Erstellen eines SAML-Identitätsanbieters in AWS IAM

Erstellen Sie zunächst einen SAML-IdP in AWS IAM. Dieser Identitätsanbieter definiert die IdP-zu-AWS-Vertrauensstellung Ihrer Organisation unter Verwendung des von der IdP-Software in Ihrer

Organisation erstellten Metadaten-Dokuments. Weitere Informationen finden Sie unter Erstellen und Verwalten eines SAML-Identitätsanbieters (Amazon-Web-Services-Managementkonsole). Informationen zum Arbeiten mit SAML IdPs in AWS GovCloud (USA-West) und AWS GovCloud (USA-Ost) finden Sie unter AWS Identity and Access Management.

Schritt 2: Erstellen einer IAM-Rolle für den SAML-2.0-Verbund

Anschließend erstellen Sie eine IAM-Rolle für den SAML-2.0-Verbund. Dieser Schritt stellt eine Vertrauensstellung zwischen IAM und dem IdP Ihrer Organisation her, die Ihren IdP als vertrauenswürdige Entität für den Verbund identifiziert.

So erstellen Sie eine IAM-Rolle für den SAML-IdP

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen und Rolle erstellen aus.
3. Wählen Sie für Role type (Rollentyp) die Option SAML 2.0 federation (SAML 2.0 Verbund).
4. Wählen Sie für SAML-Anbieter den erstellten SAML-Identitätsanbieter aus.

   > **Important**
   >
   > Wählen Sie keine der beiden SAML-2.0-Zugriffsmethoden (Nur programmgesteuerten Zugriff erlauben oder Programmgesteuerten Zugriff und Zugriff über Amazon Web Services Management Console erlauben).

5. Für Attribut wählen Sie SAML:sub_type.
6. Geben Sie für Wert `persistent` ein. Dieser Wert schränkt den Rollenzugriff auf Streaming-Anfragen von SAML-Benutzern ein, die eine SAML-Subjekttypangabe mit dem Wert „persistent“ enthalten. Wenn der SAML:sub_type „persistent“ ist, sendet Ihr IdP denselben eindeutigen Wert für das NameID-Element in allen SAML-Anfragen von einem bestimmten Benutzer. Weitere Informationen über die SAML:sub_type-Angabe finden Sie im Abschnitt Eindeutige Identifizierung von Benutzern im SAML-basierten Verbund unter Verwenden des SAML-basierten Verbunds für API-Zugriff auf AWS.
7. Überprüfen Sie Ihre SAML 2.0-Vertrauensinformationen, um die richtige vertrauenswürdige Entität und Bedingung sicherzustellen, und wählen Sie dann Next: Permissions (Weiter: Berechtigungen).
8. Wählen Sie auf der Seite Attach permissions policies (Berechtigungsrichtlinien hinzufügen) Next: Tags (Weiter: Tags) aus.

9. (Optional) Geben Sie einen Schlüssel und einen Wert für jedes Tag ein, das Sie hinzufügen möchten. Weitere Informationen finden Sie unter Markieren von IAM-Benutzern und -Rollen.
10. Klicken Sie abschließend auf Weiter: Überprüfen. Sie erstellen später eine eingebundene Richtlinie für diese Rolle und betten diese ein.
11. Geben Sie unter Rollenname einen Rollennamen ein, der Ihnen hilft, den Zweck dieser Rolle zu identifizieren. Da verschiedene Entitäten möglicherweise auf die Rolle verweisen, können Sie den Namen der Rolle nach der Erstellung nicht mehr bearbeiten.
12. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung für die neue Rolle ein.
13. Prüfen Sie die Rollendetails und wählen Sie Create Role (Rolle erstellen).
14. Fügen Sie die sts:TagSession permission zur Vertrauensrichtlinie Ihrer neuen IAM-Rolle hinzu. Weitere Informationen finden Sie unter Übergeben von Sitzungs-Tags in AWS STS. Wählen Sie auf der Detailseite für Ihre neue IAM-Rolle die Registerkarte Vertrauensbeziehungen und anschließend Vertrauensbeziehung bearbeiten. Wenn der Richtlinieneditor für Vertrauensstellungen bearbeiten geöffnet wird, fügen Sie die Berechtigung sts:TagSession* wie folgt hinzu:

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

Ersetzen Sie `IDENTITY-PROVIDER` durch den Namen des SAML-IdP, den Sie in Schritt 1 erstellt haben. Wählen Sie Vertrauensrichtlinie aktualisieren aus.

Schritt 3: Einbetten einer eingebundenen Richtlinie für die IAM-Rolle

Anschließend betten Sie eine eingebundene IAM-Richtlinie für die erstellte Rolle ein. Bei der Einbettung einer eingebundenen Richtlinie können die Berechtigungen der Richtlinie nicht versehentlich an die falsche Prinzipal-Entität angefügt werden. Die Inline-Richtlinie bietet Verbundbenutzern Zugriff auf das WorkSpaces Verzeichnis .

> **Important**
>
> IAM-Richtlinien zur Verwaltung des Zugriffs auf AWS basierend auf der Quell-IP werden für die `workspaces:Stream` Aktion nicht unterstützt. Um IP-Zugriffskontrollen für zu verwalten WorkSpaces, verwenden Sie IP-Zugriffskontrollgruppen . Darüber hinaus können Sie bei Verwendung der SAML-2.0-Authentifizierung IP-Zugriffskontrollrichtlinien verwenden, wenn diese über Ihren SAML-2.0-IdP verfügbar sind.

1. Wählen Sie in den Details für die IAM-Rolle, die Sie erstellt haben, die Registerkarte Berechtigungen aus und fügen Sie dann die erforderlichen Berechtigungen zur Berechtigungsrichtlinie der Rolle hinzu. Der Assistent zum Erstellen von Richtlinien wird gestartet.
2. Wählen Sie unter Create policy (Richtlinie erstellen) die Registerkarte JSON.
3. Kopieren Sie die folgende JSON-Richtlinie und fügen Sie sie in das JSON-Fenster ein. Ändern Sie dann die Ressource, indem Sie Ihren AWS-Regionscode, Ihre Konto-ID und Ihre Verzeichnis-ID eingeben. In der folgenden Richtlinie `"Action": "workspaces:Stream"` ist die -Aktion, die Ihren WorkSpaces Benutzern Berechtigungen zum Herstellen einer Verbindung mit ihren Desktop-Sitzungen im - WorkSpaces Verzeichnis erteilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

Ersetzen Sie durch `REGION-CODE` die AWS Region, in der sich Ihr WorkSpaces Verzeichnis befindet. Ersetzen Sie durch `DIRECTORY-ID` die WorkSpaces Verzeichnis-ID, die Sie in der - WorkSpaces Managementkonsole finden. Verwenden Sie für Ressourcen in AWS GovCloud (USA-West) oder AWS GovCloud (USA-Ost) das folgende Format für den ARN: `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`.

4. Klicken Sie abschließend auf Review policy (Richtlinie überprüfen). Die Richtlinienvalidierung meldet mögliche Syntaxfehler.

Schritt 4: Konfigurieren des SAML-2.0-Identitätsanbieters

Abhängig vom SAML-2.0-basierten IdP müssen Sie den IdP gegebenenfalls so aktualisieren, dass er AWS als Serviceanbieter vertraut, indem Sie die Datei `saml-metadata.xml` aus https://signin.aws.amazon.com/static/saml-metadata.xml in den IdP hochladen. Dieser Schritt aktualisiert die Metadaten Ihres IdP. Bei einigen ist IdPsdas Update möglicherweise bereits konfiguriert. In diesem Fall fahren Sie mit dem nächsten Schritt fort.

Wenn diese Aktualisierung in Ihrem IdP noch nicht konfiguriert ist, lesen Sie in der Dokumentation Ihres IdP nach, wie die Metadaten zu aktualisieren sind. Bei einigen Anbietern können Sie die URL eingeben, woraufhin der Identitätsanbieter die Datei für Sie abruft und installiert. Bei anderen Anbietern müssen Sie die Datei über eine URL herunterladen und dann als lokale Datei bereitstellen.

> **Important**
>
> Derzeit können Sie auch Benutzer in Ihrem IdP autorisieren, auf die WorkSpaces Anwendung zuzugreifen, die Sie in Ihrem IdP konfiguriert haben. Benutzer, die berechtigt sind, auf die

WorkSpaces Anwendung für Ihr Verzeichnis zuzugreifen, haben nicht automatisch ein für sie WorkSpace erstellt. Ebenso werden Benutzer, die ein für sie WorkSpace erstellt haben, nicht automatisch für den Zugriff auf die WorkSpaces Anwendung autorisiert. Um mithilfe der SAML-2.0-Authentifizierung erfolgreich eine Verbindung zu einem WorkSpace herzustellen, muss ein Benutzer vom IdP autorisiert sein und muss einen WorkSpace erstellt haben.

Schritt 5: Erstellen von Zusicherungen für die SAML-Authentifizierungsantwort

Konfigurieren Sie als Nächstes die Informationen, die der Identitätsanbieter als SAML-Attribute an AWS als Teil der Authentifizierungsantwort sendet. Abhängig von Ihrem IdP ist dies bereits konfiguriert. Überspringen Sie diesen Schritt und fahren Sie mit Schritt 6: Konfigurieren des Relay-Status Ihres Verbunds fort.

Wenn diese Informationen in Ihrem Identitätsanbieter noch nicht konfiguriert sind, führen Sie die folgenden Schritte aus:

- SAML Subject NameID – Die eindeutige ID für den Benutzer, der sich anmeldet. Der Wert muss mit dem WorkSpaces Benutzernamen übereinstimmen und ist normalerweise das sAMAccountName-Attribut für den Active-Directory-Benutzer.
- SAML-Subjekttyp (mit dem Wert `persistent`) – Durch Verwendung des Werts `persistent` stellen Sie sicher, dass Ihr IdP in allen SAML-Anfragen von einem bestimmten Benutzer dasselbe `NameID`-Element sendet. Stellen Sie sicher, dass Ihre IAM-Richtlinie eine Bedingung enthält, um ausschließlichen SAML-Anfragen mit dem SAML sub_type `persistent` zuzulassen, wie in Erstellen einer IAM-Rolle für den SAML-2.0-Verbund beschrieben.
- **`Attribute`**-Element mit dem **`Name`**-Attribut **`https://aws.amazon.com/SAML/Attributes/Role`** – Dieses Element enthält ein oder mehrere `AttributeValue`-Elemente, die die IAM-Rollen und den SAML IdP auflisten, denen der Benutzer durch Ihren IdP zugeordnet ist. Die Rolle und der IdP werden durch Kommas getrennte Liste von ARN-Paaren angegeben. Ein Beispiel für den erwarteten Wert ist `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`.
- **`Attribute`**-Element mit dem **`Name`**-Attribut **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** – Dieses Element enthält ein `AttributeValue`-Element, das einen Bezeichner für die temporären AWS-Anmeldeinformationen bereitstellt, die für SSO ausgestellt werden. Der Wert des `AttributeValue`-Elements muss zwischen 2 und 64 Zeichen lang sein und darf nur alphanumerische Zeichen, Unterstriche und die folgenden Zeichen enthalten: _ . : / = + - @. Leerzeichen dürfen nicht enthalten sein. Der Wert ist in der Regel eine E-Mail-Adresse oder

ein User Principle Name (UPN). Er sollte kein Wert mit einem Leerzeichen (z. B. der Anzeigename eines Benutzers) sein.

- **`Attribute`**-Element, bei dem das **`Name`**-Attribut **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** ist – Dieses Element enthält ein `AttributeValue`-Element, das die E-Mail-Adresse des/der Benutzer:in angibt. Der Wert muss mit der E-Mail-Adresse des WorkSpaces Benutzers übereinstimmen, wie im WorkSpaces Verzeichnis definiert. Tag-Werte können Kombinationen aus Buchstaben, Zahlen, Leerzeichen sein und die folgenden Zeichen enthalten: _ . : / = + - @ Weitere Informationen finden Sie unter Regeln zum Markieren in IAM und AWS STS im IAM-Benutzerhandbuch.
- **`Attribute`**-Element, bei dem das **`Name`**-Attribut **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** ist (optional) – Dieses Element enthält ein `AttributeValue`-Element, das die Active-Directory-`userPrincipalName` für den Benutzer bereitstellt, der sich anmeldet. Das Format des von Ihnen angegebenen Wertes muss `username@domain.com` sein. Dieser Parameter wird bei der zertifikatbasierten Authentifizierung als alternativer Name des Subjekts im Endbenutzerzertifikat verwendet. Weitere Informationen finden Sie unter „Zertifikatbasierte Authentifizierung“.
- **`Attribute`**-Element, bei dem das **`Name`**-Attribut **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** ist (optional) – Dieses Element enthält ein `AttributeValue`-Element, das die Active-Directory-SID (Security Identifier) für den/die Benutzer:in bereitstellt, der/die sich anmeldet. Dieser Parameter wird bei der zertifikatbasierten Authentifizierung verwendet, um eine sichere Zuordnung zu Active-Directory-Benutzern zu ermöglichen. Weitere Informationen finden Sie unter „Zertifikatbasierte Authentifizierung“.
- **`Attribute`**-Element, bei dem das **`Name`**-Attribut **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** ist (optional) – Dieses Element enthält ein `AttributeValue`-Element, das ein alternatives Benutzernamenformat bereitstellt. Verwenden Sie dieses Attribut, wenn Sie Anwendungsfälle haben, die Benutzernamenformate wie `corp\username`, oder erfordern`corp.example.com\username`, `username@corp.example.com` um sich mit dem WorkSpaces Client anzumelden. Tag-Schlüssel und -Werte können eine beliebige Kombination aus Buchstaben, Zahlen, Leerzeichen sein und die Zeichen _ : / . + = @ - enthalten. Weitere Informationen finden Sie unter Regeln zum Markieren in IAM und AWS STS im IAM-Benutzerhandbuch. Ersetzen Sie\ in der SAML-Assertion durch/, um `corp\username`- oder `corp.example.com\username`-Formate anzugeben.
- -**`Attribute`**Element mit dem -**`Name`**Attribut https://aws.amazon.com/SAML/Attributes/PrincipalTag:Domain (optional) – Dieses Element enthält ein -`AttributeValue`Element, das den vollqualifizierten Active-Directory-DNS-Domainnamen (FQDN) für Benutzer bereitstellt, die sich

anmelden. Dieser Parameter wird bei der zertifikatbasierten Authentifizierung verwendet, wenn die Active-Directory-`userPrincipalName` für die Benutzer ein alternatives Suffix enthält. Der Wert muss in der `domain.com` angegeben werden, einschließlich aller Unterdomains.

- -**`Attribute`**Element mit dem -**`Name`**Attribut https://aws.amazon.com/SAML/Attributes/SessionDuration (optional) – Dieses Element enthält ein -`AttributeValue`Element, das die maximale Zeit angibt, die eine Verbund-Streaming-Sitzung für einen Benutzer aktiv bleiben kann, bevor eine erneute Authentifizierung erforderlich ist. Der Standardwert liegt bei 3600 Sekunden (60 Minuten). Weitere Informationen finden Sie unter SAML `SessionDurationAttribute`.

> **Note**
>
> Auch wenn es sich bei `SessionDuration` um ein optionales Attribut handelt, wird empfohlen, es in die SAML-Antwort aufzunehmen. Wenn Sie dieses Attribut nicht angeben, wird die Sitzungsdauer auf einen Standardwert von 3600 Sekunden (60 Minuten) festgelegt. WorkSpaces Die Desktop-Sitzungen werden nach Ablauf ihrer Sitzungsdauer getrennt.

Weitere Informationen über die Konfiguration dieser Elemente finden Sie unter Konfigurieren von SAML-Zusicherungen für die Authentifizierungsantwort im IAM-Benutzerhandbuch. Weitere Informationen zu spezifischen Konfigurationsanforderungen für Ihren IdP finden Sie in der Dokumentation zu Ihrem IdP.

Schritt 6: Konfigurieren des Relay-Status für den Verbund

Verwenden Sie als Nächstes Ihren IdP, um den Relay-Status Ihres Verbunds so zu konfigurieren, dass er auf die WorkSpaces Verzeichnis-Relay-Status-URL verweist. Nach erfolgreicher Authentifizierung durch wird AWSder Benutzer an den WorkSpaces Verzeichnisendpunkt weitergeleitet, der als Relay-Status in der SAML-Authentifizierungsantwort definiert ist.

Der Relay-Status-URL hat das folgende Format:

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

Erstellen Sie Ihre Relay-Status-URL aus Ihrem WorkSpaces Verzeichnisregistrierungscode und dem Relay-Status-Endpunkt, der der Region zugeordnet ist, in der sich Ihr Verzeichnis befindet. Der Registrierungscode finden Sie in der - WorkSpaces Managementkonsole.

Wenn Sie die regionsübergreifende Umleitung für verwenden WorkSpaces, können Sie optional den Registrierungscode durch den vollqualifizierten Domainnamen (FQDN) ersetzen, der mit Verzeichnissen in Ihren primären und Failover-Regionen verknüpft ist. Weitere Informationen finden Sie unter Regionsübergreifende Umleitung für Amazon WorkSpaces. Wenn Sie die regionsübergreifende Umleitung und die SAML-2.0-Authentifizierung verwenden, müssen sowohl das Primär- als auch das Failover-Verzeichnis für die SAML-2.0-Authentifizierung aktiviert und unabhängig voneinander mit dem IdP konfiguriert werden, wobei der Relay-Status-Endpunkt verwendet wird, der jeder Region zugeordnet ist. Auf diese Weise kann der FQDN korrekt konfiguriert werden, wenn Benutzer ihre WorkSpaces Clientanwendungen vor der Anmeldung registrieren, und ermöglicht Benutzern die Authentifizierung während eines Failover-Ereignisses.

In der folgenden Tabelle sind die Relay-Status-Endpunkte für die Regionen aufgeführt, in denen die WorkSpaces SAML-2.0-Authentifizierung verfügbar ist.

Regionen, in denen die WorkSpaces SAML-2.0-Authentifizierung verfügbar ist

Region	RelayState-Endpunkt
Region USA Ost (Nord-Virginia)	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) Workspaces.euc-sso-fips.us-east-1.aws.amazon.com
Region USA West (Oregon)	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) Workspaces.euc-sso-fips.us-west-2.aws.amazon.com
Region Afrika (Kapstadt)	workspaces.euc-sso.af-south-1.aws.amazon.com
Region Asien-Pazifik (Mumbai)	workspaces.euc-sso.ap-south-1.aws.amazon.com

Region	RelayState-Endpunkt
Region Asien-Pazifik (Seoul)	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
Region Asien-Pazifik (Singapur)	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
Region Asien-Pazifik (Sydney)	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
Region Asien-Pazifik (Tokio)	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
Region Kanada (Zentral)	workspaces.euc-sso.ca-central-1.aws.amazon.com
Region Europa (Frankfurt)	workspaces.euc-sso.eu-central-1.aws.amazon.com
Region Europa (Irland)	workspaces.euc-sso.eu-west-1.aws.amazon.com
Region Europa (London)	workspaces.euc-sso.eu-west-2.aws.amazon.com
Region Südamerika (São Paulo)	workspaces.euc-sso.sa-east-1.aws.amazon.com
Region Israel (Tel Aviv)	workspaces.euc-sso.il-central-1.aws.amazon.com

Region	RelayState-Endpunkt
AWS GovCloud (USA West)	• Workspaces.euc-sso.us-gov-west-1.amazonaws-us-govcom • (FIPS) Workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com **Note** Weitere Informationen zu finden Sie unter Amazon WorkSpaces im AWS GovCloud (US)-Benutzerhandbuch.
AWS GovCloud (USA-Ost)	• Workspaces.euc-sso.us-gov-east-1.amazonaws-us-govcom • (FIPS) Workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** Weitere Informationen zu finden Sie unter Amazon WorkSpaces im AWS GovCloud (US)-Benutzerhandbuch.

Schritt 7: Aktivieren der Integration mit SAML 2.0 in Ihrem WorkSpaces Verzeichnis

Sie können die WorkSpaces Konsole verwenden, um die SAML-2.0-Authentifizierung für das WorkSpaces Verzeichnis zu aktivieren.

So aktivieren Sie die Integration mit SAML 2.0

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie die Verzeichnis-ID für Ihr aus WorkSpaces.

4. Wählen Sie unter Authentifizierung die Option Bearbeiten aus.
5. Wählen Sie SAML-2.0-Identitätsanbieter bearbeiten aus.
6. Aktivieren Sie das Kontrollkästchen SAML-2.0-Authentifizierung aktivieren.
7. Geben Sie für die Benutzerzugriffs-URL und Name des IdP-Deep-Link-Parameters Werte ein, die für Ihren IdP und die Anwendung gelten, die Sie in Schritt 1 konfiguriert haben. Der Standardwert für den IdP-Deep-Link-Parameternamen ist „RelayState“, wenn Sie diesen Parameter weglassen. In der folgenden Tabelle sind URLs und Parameternamen für den Benutzerzugriff aufgeführt, die für verschiedene Identitätsanbieter für Anwendungen eindeutig sind.

   Domains und IP-Adressen, die der Zulassungsliste hinzugefügt werden sollten

Identitätsanbieter	Parameter	URL für den Benutzerzugriff
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Single-Sign-On	`RelayState`	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso`
Okta	`RelayState`	`https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml`
OneLogin	`RelayState`	`https://<sub-domain>.onelogin.com/tr`

Identitätsanbieter	Parameter	URL für den Benutzerzugriff
		`ust/saml2/http-pos t/sso/<app-id>`
PingFederate	`TargetResource`	`https://<host>/idp /startSSO.ping?Par tnerSpId=<sp_id>`
PingOne für Enterprise	`TargetResource`	`https://sso.connec t.pingidentity.com /sso/sp/initsso?sa asid=<app_id>&idpi d=<idp_id>`

Die Benutzerzugriffs-URL wird normalerweise vom Anbieter für unaufgefordertes, vom IdP initiiertes SSO definiert. Ein Benutzer kann diese URL in einen Webbrowser eingeben, um sich direkt mit der SAML-Anwendung zu verbinden. Wählen Sie Testen aus, um die Benutzerzugriffs-URL und die Parameterwerte für Ihren IdP zu testen. Kopieren Sie die Test-URL und fügen Sie sie in ein privates Fenster Ihres aktuellen Browsers oder eines anderen Browsers ein, um die SAML-2.0-Anmeldung zu testen, ohne Ihre aktuelle AWS-Verwaltungskonsolensitzung zu unterbrechen. Wenn der IdP initiierte Flow geöffnet wird, können Sie Ihren WorkSpaces Client registrieren. Weitere Informationen finden Sie unter Vom Identitätsanbieter (IdP) initiierter Flow.

8. Aktivieren oder deaktivieren Sie die Option Anmeldung für Clients zulassen, die SAML 2.0 nicht unterstützen, um die Fallback-Einstellungen zu verwalten. Aktivieren Sie diese Einstellung, um Ihren Benutzern weiterhin Zugriff auf zu gewähren, indem Sie Clienttypen oder Versionen WorkSpaces verwenden, die SAML 2.0 nicht unterstützen, oder wenn Benutzer Zeit benötigen, um auf die neueste Clientversion zu aktualisieren.

   > **Note**
   >
   > Diese Einstellung ermöglicht es Benutzern, SAML 2.0 zu umgehen und sich mithilfe der Verzeichnisauthentifizierung mit älteren Client-Versionen anzumelden.

9. Aktivieren Sie Web Access, um SAML mit dem Webclient zu verwenden. Weitere Informationen finden Sie unter Amazon WorkSpaces Web Access aktivieren und konfigurieren.

> **Note**
>
> PCoIP mit SAML wird bei Web Access nicht unterstützt.

10. Wählen Sie Speichern. Ihr WorkSpaces Verzeichnis ist jetzt mit der SAML-2.0-Integration aktiviert. Sie können die IdP initiierten und von Clientanwendungen initiierten Flows verwenden, um WorkSpaces Clientanwendungen zu registrieren und sich bei anzumelden WorkSpaces.

Zertifikatbasierte Authentifizierung

Sie können die zertifikatbasierte Authentifizierung mit verwenden WorkSpaces , um die Benutzeraufforderung für das Active-Directory-Domain-Passwort zu entfernen. Durch die Verwendung der zertifikatbasierten Authentifizierung mit Ihrer Active Directory-Domain können Sie Folgendes erreichen:

- Sie können den SAML-2.0-Identitätsanbieter zur Authentifizierung der Benutzer und Bereitstellung der SAML-Zusicherungen für die Benutzer in Active Directory verwenden.
- Ermöglichen Sie eine Single-Sign-On-Anmeldung mit weniger Benutzeraufforderungen.
- Aktivieren Sie passwortlose Authentifizierungsabläufe mit Ihrem SAML-2.0-Identitätsanbieter.

Bei der zertifikatbasierten Authentifizierung werden AWS Private CA-Ressourcen in Ihrem AWS-Konto verwendet. AWS Private CA ermöglicht die Erstellung von Hierarchien privater Zertifizierungsstellen (CAs), einschließlich Stamm- und untergeordneter Zertifizierungsstellen. Mit AWS Private CA können Sie Ihre eigene CA-Hierarchie erstellen und damit Zertifikate zur Authentifizierung interner Benutzer ausstellen. Weitere Informationen finden Sie im AWS Private Certificate Authority-Benutzerhandbuch.

Wenn Sie AWS Private CA für die zertifikatbasierte Authentifizierung verwenden, WorkSpaces fordert Zertifikate für Ihre Benutzer während der Sitzungsauthentifizierung automatisch an. Die Benutzer werden mit einer virtuellen Smartcard, die mit den Zertifikaten bereitgestellt wird, bei Active Directory authentifiziert.

Die zertifikatbasierte Authentifizierung wird mit Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP)-Paketen unter Verwendung der neuesten WorkSpaces Web Access-, Windows- und macOS-Clientanwendungen unterstützt. Öffnen Sie Amazon WorkSpaces -Client-Downloads, um die neuesten Versionen zu finden:

- Windows-Client, Version 5.5.0 oder höher
- macOs-Client, Version 5.6.0 oder höher

Weitere Informationen zur Konfiguration der zertifikatbasierten Authentifizierung mit Amazon WorkSpacesfinden Sie unter So konfigurieren Sie die zertifikatbasierte Authentifizierung für Amazon WorkSpaces und Überlegungen zum Design in stark regulierten Umgebungen für die zertifikatbasierte Authentifizierung mit AppStream 2.0 und WorkSpaces .

Voraussetzungen

Führen Sie die folgenden Schritte aus, bevor Sie die zertifikatbasierte Authentifizierung aktivieren.

1. Konfigurieren Sie Ihr WorkSpaces Verzeichnis mit der SAML-2.0-Integration für die Verwendung der zertifikatsbasierten Authentifizierung. Weitere Informationen finden Sie unter WorkSpaces Integration mit SAML 2.0.
2. Konfigurieren Sie das `userPrincipalName` Attribut in Ihrer SAML-Zusicherung. Weitere Informationen finden Sie unter Erstellen von Zusicherungen für die SAML-Authentifizierungsantwort.
3. Konfigurieren Sie das `0bjectSid` Attribut in Ihrer SAML-Zusicherung. Dies ist optional, um eine starke Zuordnung zu den Active-Directory-Benutzern durchzuführen. Die zertifikatbasierte Authentifizierung schlägt fehl, wenn das Attribut nicht mit der Active-Directory-Sicherheitskennung (SID) für den im SAML_Subject `NameID` angegebenen Benutzern übereinstimmt. Weitere Informationen finden Sie unter Erstellen von Zusicherungen für die SAML-Authentifizierungsantwort.
4. Fügen Sie die sts:TagSession-Berechtigung zu Ihrer IAM-Rollenvertrauensrichtlinie hinzu, die mit Ihrer SAML-2.0-Konfiguration verwendet wird, falls sie noch nicht vorhanden ist. Diese Berechtigung ist erforderlich, um die zertifikatbasierte Authentifizierung zu verwenden. Weitere Informationen finden Sie unter Erstellen einer IAM-Rolle für den SAML-2.0-Verbund.
5. Erstellen Sie mit AWS Private CA eine private Zertifizierungsstelle (CA), falls Sie noch keine mit Ihrem Active Directory konfiguriert haben. AWS Private CA ist erforderlich, um die zertifikatbasierte Authentifizierung zu verwenden. Weitere Informationen finden Sie unter Planen Ihrer AWS Private CA-Bereitstellung. Folgen Sie den Anweisungen zur Konfiguration einer Zertifizierungsstelle für die zertifikatbasierte Authentifizierung. Die folgenden AWS Private CA Einstellungen werden im Allgemeinen für die zertifikatbasierte Authentifizierung verwendet:

   a. Optionen für den CA-Typ:

i. CA-Verwendungsmodus für kurzlebige Zertifikate (empfohlen, wenn Sie die CA nur zur Ausstellung von Endbenutzerzertifikaten für die zertifikatbasierte Authentifizierung verwenden)

ii. Einstufige Hierarchie mit einer Stammzertifizierungsstelle (wählen Sie alternativ eine untergeordnete Zertifizierungsstelle aus, wenn Sie eine Integration in eine bestehende Zertifizierungsstellenhierarchie vornehmen möchten)

b. Optionen für den Schlüsselalgorithmus: RSA 2048

c. Optionen für den definierten Namen des Antragstellers: Verwenden Sie eine beliebige Kombination von Optionen, um die Zertifizierungsstelle in Ihrem Active-Directory-Speicher für vertrauenswürdige Stammzertifizierungsstellen zu identifizieren.

d. Optionen zum Widerruf von Zertifikaten: CRL-Verteilung

> **Note**
>
> Für die zertifikatbasierte Authentifizierung ist ein Online-CRL-Verteilungspunkt erforderlich, auf den von Desktops und dem Domain-Controller aus zugegriffen werden kann. Dies erfordert einen nicht authentifizierten Zugriff auf den Amazon S3-Bucket, der für CRL-Einträge von Private CA konfiguriert ist, oder eine CloudFront Verteilung, die Zugriff auf den S3-Bucket hat, wenn der öffentliche Zugriff blockiert wird. Weitere Informationen finden Sie unter Planen einer Zertifikatsperrliste (CRL).

6. Taggen Sie Ihre private Zertifizierungsstelle mit einem Schlüssel, der berechtigt ist, die CA für die Verwendung mit `euc-private-ca` auf EUC-Zertifikaten basierenden Authentifizierung zu kennzeichnen. Für den Schlüssel ist kein Wert erforderlich. Weitere Informationen finden Sie unter Verwalten von Tags für Ihre private CA.
7. Bei der zertifikatbasierten Authentifizierung werden virtuelle Smartcards für die Anmeldung verwendet. Folgen Sie den Richtlinien für die Aktivierung der Smartcard-Anmeldung bei Zertifizierungsstellen von Drittanbietern in Active Directory und führen Sie die folgenden Schritte durch:
   - Konfigurieren Sie Domain-Controller mit einem Domain-Controllerzertifikat zur Authentifizierung von Smartcard-Benutzern. Wenn Sie in Ihrem Active Directory eine Unternehmenszertifizierungsstelle für Active-Directory-Zertifikatsdienste konfiguriert haben, werden Domain-Controller automatisch mit Zertifikaten registriert, um die Smartcard-Anmeldung zu ermöglichen. Wenn Sie nicht über Active-Directory-Zertifikatsdienste verfügen, finden Sie weitere Informationen unter Anforderungen für Domain-Controllerzertifikate von einer Drittanbieter-Zertifizierungsstelle. Sie können ein Domain-Controllerzertifikat mit AWS Private

CA erstellen. Verwenden Sie in diesem Fall keine private Zertifizierungsstelle, die für kurzlebige Zertifikate konfiguriert ist.

> **Note**
>
> Wenn Sie AWS Managed Microsoft AD, können Sie die Zertifikatsdienste in einer EC2-Instance konfigurieren, um die Anforderungen für Domain-Controllerzertifikate zu erfüllen. Beispiele AWS Launch Wizard für Bereitstellungen von , die mit Active Directory Certificate Services AWS Managed Microsoft AD konfiguriert sind. AWS Private CA kann als untergeordnete Zertifizierungsstelle für Active Directory Certificate Services oder als eigenes Stammverzeichnis bei Verwendung von konfiguriert werdenAWS Managed Microsoft AD.
>
> Eine zusätzliche Konfigurationsaufgabe mit AWS Managed Microsoft AD und Active-Directory-Zertifikatsdiensten besteht darin, ausgehende Regeln von der VPC-Sicherheitsgruppe des Controllers zur EC2-Instance zu erstellen, auf der die Zertifikatsdienste ausgeführt werden, sodass die TCP-Ports 135 und 49152-65535 die automatische Registrierung von Zertifikaten ermöglichen. Darüber hinaus muss die ausgeführte EC2-Instance eingehenden Zugriff auf dieselben Ports von Domain-Instances, einschließlich Domain-Controllern, zulassen. Weitere Informationen zum Auffinden der Sicherheitsgruppe für AWS Managed Microsoft AD finden Sie unter Konfigurieren Ihrer VPC-Subnetze und Sicherheitsgruppen.

- Wählen Sie in der AWS Private CA-Konsole oder mithilfe des SDKs oder der CLI Ihre CA aus und exportieren Sie unter dem CA-Zertifikat das private CA-Zertifikat. Weitere Informationen finden Sie unter Exportieren eines privaten Zertifikats.
- Veröffentlichen Sie die CA in Active Directory. Melden Sie sich an einem Domain-Controller oder einem Computer an, der Domain-Mitglied ist. Kopieren Sie das private CA-Zertifikat in einen beliebigen `<path>\<file>` und führen Sie die folgenden Befehle als Domain-Administrator aus. Alternativ können Sie Gruppenrichtlinien und das Microsoft PKI Health Tool (PkIView) verwenden, um die CA zu veröffentlichen. Weitere Informationen finden Sie in den Konfigurationsanweisungen.

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

Stellen Sie sicher, dass die Befehle erfolgreich ausgeführt wurden. Entfernen Sie dann die private Zertifikatsdatei. Abhängig von den Einstellungen für die Active-Directory-Replikation

kann es einige Minuten dauern, bis die Zertifizierungsstelle auf Ihren Domain-Controllern und Desktop-Instances veröffentlicht wird.

> **Note**
>
> - Active Directory muss die CA automatisch an die Trusted Root Certification Authoritys und Enterprise NTAuth-Speicher für WorkSpaces Desktops verteilen, wenn sie der Domain beitreten.
> - Active-Directory-Domain-Controller müssen sich im Kompatibilitätsmodus befinden, damit die strenge Durchsetzung von Zertifikaten die zertifikatsbasierte Authentifizierung unterstützt. Weitere Informationen finden Sie unter KB5014754 – Änderungen der zertifikatsbasierten Authentifizierung auf Windows-Domain-Controllern in der Microsoft Support-Dokumentation. Wenn Sie AWS Managed Microsoft AD verwenden, finden Sie weitere Informationen unter Konfigurieren von Verzeichnissicherheitseinstellungen.

Aktivieren der zertifikatbasierten Authentifizierung

Führen Sie die folgenden Schritte aus, bevor Sie die zertifikatbasierte Authentifizierung aktivieren.

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie die Verzeichnis-ID für Ihr aus WorkSpaces.
4. Klicken Sie unter Authentifizierung auf Bearbeiten.
5. Klicken Sie auf Zertifikatbasierte Authentifizierung bearbeiten.
6. Aktivieren Sie die Option Zertifikatbasierten Authentifizierung aktivieren.
7. Vergewissern Sie sich, dass Ihr privater CA-ARN in der Liste zugeordnet ist. Die private Zertifizierungsstelle sollte sich im selben AWS Konto und in derselben befinden und muss mit einem Schlüssel gekennzeichnet seinAWS-Region, der berechtigt ist euc-private-ca , in der Liste zu erscheinen.
8. Klicken Sie auf Save Changes (Änderungen speichern). Die zertifikatbasierte Authentifizierung ist nun aktiviert.
9. Starten Sie Ihre Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP)-Pakete neu, damit die Änderungen wirksam werden. Weitere Informationen finden Sie unter Neustart einer WorkSpace.

10. Wenn sich Benutzer nach dem Neustart über SAML 2.0 mit einem unterstützten Client authentifizieren, werden sie nicht mehr zur Eingabe des Domain-Passworts aufgefordert.

> **Note**
>
> Wenn die zertifikatbasierte Authentifizierung aktiviert ist, um sich bei anzumelden WorkSpaces, werden Benutzer nicht zur Multi-Faktor-Authentifizierung (MFA) aufgefordert, selbst wenn sie im Verzeichnis aktiviert sind. Wenn Sie die zertifikatbasierte Authentifizierung verwenden, kann MFA über Ihren SAML-2.0-Identitätsanbieter aktiviert werden. Weitere Informationen zur AWS Directory Service-MFA finden Sie unter Multi-Faktor-Authentifizierung (AD Connector) oder Aktivieren der Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD.

Verwalten der zertifikatbasierten Authentifizierung

CA-Zertifikat

In einer typischen Konfiguration hat das private CA-Zertifikat eine Gültigkeitsdauer von 10 Jahren. Weitere Informationen zum Ersetzen einer Zertifizierungsstelle mit einem abgelaufenen Zertifikat oder zur Neuausstellung der Zertifizierungsstelle mit einem neuen Gültigkeitszeitraum finden Sie unter Verwalten des Lebenszyklus einer privaten Zertifizierungsstelle.

Endbenutzerzertifikate

Endbenutzerzertifikate, die von AWS Private CA für die WorkSpaces zertifikatbasierte Authentifizierung ausgestellt wurden, müssen nicht verlängert oder widerrufen werden. Diese Zertifikate sind kurzlebig. WorkSpaces gibt automatisch alle 24 Stunden ein neues Zertifikat aus. Diese Endbenutzerzertifikate haben eine kürzere Gültigkeitsdauer als eine typische AWS Private CA-CRL-Distribution. Daher müssen Endbenutzerzertifikate nicht gesperrt werden und erscheinen auch nicht in einer CRL.

Prüfberichte

Sie können einen Auditbericht erstellen, der die Zertifikate auflistet, die ihre private CA ausgestellt oder widerrufen hat. Weitere Informationen finden Sie unter Verwenden von Prüfberichten mit Ihrer privaten CA.

Protokollieren und Überwachen

Sie können verwendenAWS CloudTrail, um API-Aufrufe an AWS Private CA von aufzuzeichnen WorkSpaces. Weitere Informationen finden Sie unter Verwenden von CloudTrail. Im CloudTrail Ereignisverlauf können Sie - `GetCertificate` und `IssueCertificate`-Ereignisnamen aus der WorkSpaces vom `EcmAssumeRoleSession` Benutzernamen erstellten `acm-pca.amazonaws.com` Ereignisquelle anzeigen. Diese Ereignisse werden für jede auf einem EUC-Zertifikat basierende Authentifizierungsanfrage aufgezeichnet.

Verwenden von Smartcards zur Authentifizierung

Pakete für Windows und Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) ermöglichen die Verwendung von Common Access Card (CAC)- und Personal Identity Verification (PIV)-Smartcards für die Authentifizierung.

Amazon WorkSpaces unterstützt die Verwendung von Smartcards sowohl für die Authentifizierung vor der Sitzung als auch für die Authentifizierung während der Sitzung. Die Authentifizierung vor der Sitzung bezieht sich auf die Smartcard-Authentifizierung, die durchgeführt wird, während sich Benutzer bei ihrem anmelden WorkSpaces. Die Authentifizierung während der Sitzung bezieht sich auf die Authentifizierung, die durchgeführt wird, nachdem Sie sich angemeldet haben.

Beispielsweise können Sie Smartcards für die Authentifizierung während der Sitzung verwenden, während Sie mit Webbrowsern und Anwendungen arbeiten. Sie können Smartcards auch für Aktionen verwenden, für die Administratorberechtigungen erforderlich sind. Wenn der Benutzer beispielsweise über Administratorberechtigungen auf seinem Linux- verfügt WorkSpace, kann er Smartcards verwenden, um sich beim Ausführen von - `sudo` und -`sudo -i`Befehlen zu authentifizieren.

Inhalt

Voraussetzungen

- Für die Authentifizierung vor der Sitzung ist ein Active-Directory-Connector-(AD-Connector)-Verzeichnis erforderlich. AD Connector verwendet die zertifikatbasierte gegenseitige Transport-

Layer-Security-Authentifizierung (mutual TLS), um Benutzer mit hardware- oder softwarebasierten Smartcard-Zertifikaten bei Active Directory zu authentifizieren. Weitere Informationen zum Konfigurieren Ihres AD Connector und Ihres On-Premises-Verzeichnisses finden Sie unter Verzeichniskonfiguration.

- Um eine Smartcard mit einem Windows- oder Linux- zu verwenden WorkSpace, muss der Benutzer den Amazon WorkSpaces -Windows-Client Version 3.1.1 oder höher oder die WorkSpaces macOS-Clientversion 3.1.5 oder höher verwenden. Weitere Informationen zur Verwendung von Smartcards mit den Windows- und macOS-Clients finden Sie unter Smartcard-Unterstützung im Amazon- WorkSpaces Benutzerhandbuch.
- Die Stammzertifizierungsstelle und die Smartcard-Zertifikate müssen bestimmte Anforderungen erfüllen. Weitere Informationen finden Sie unter Aktivieren der mTLS-Authentifizierung in AD Connector für die Verwendung mit Smartcards im AWS Directory Service -Administratorhandbuch und unter Zertifikatanforderungen in der Microsoft-Dokumentation.

  Zusätzlich zu diesen Anforderungen WorkSpaces müssen Benutzerzertifikate, die für die Smartcard-Authentifizierung bei Amazon eingesetzt werden, die folgenden Attribute enthalten:

  - Der AD-Benutzer userPrincipalName (UPN) im Feld subjectAltName (SAN) des Zertifikats. Es wird empfohlen, Smartcard-Zertifikate für den Standard-UPN des/der Benutzer:in auszustellen.
  - Das EKU-Attribut (Extended Key Usage) für die Client-Authentifizierung (1.3.6.1.5.5.7.3.2).
  - Das EKU-Attribut für Smartcard-Anmeldung (1.3.6.1.4.1.311.20.2.2).
- Für die Authentifizierung vor der Sitzung ist das Online Certificate Status Protocol (OCSP) zur Überprüfung des Zertifikats erforderlich. Für die Authentifizierung während der Sitzung wird OCSP empfohlen, ist jedoch nicht erforderlich.

Einschränkungen

- Nur die WorkSpaces Windows-Clientanwendung Version 3.1.1 oder höher und die macOS-Clientanwendung Version 3.1.5 oder höher werden derzeit für die Smartcard-Authentifizierung unterstützt.
- Die WorkSpaces Windows-Clientanwendung 3.1.1 oder höher unterstützt Smartcards nur, wenn der Client auf einer 64-Bit-Version von Windows ausgeführt wird.
- Ubuntu unterstützt derzeit WorkSpaces keine Smartcard-Authentifizierung.
- Derzeit werden nur AD-Connector-Verzeichnisse für die Smartcard-Authentifizierung unterstützt.

- Die Authentifizierung während der Sitzung ist in allen Regionen verfügbar, in denen WSP unterstützt wird. Die Authentifizierung vor der Sitzung ist in folgenden Regionen verfügbar:
  - Region Asien-Pazifik (Sydney)
  - Region Asien-Pazifik (Tokio)
  - Region Europa (Irland)
  - AWS GovCloud Region (USA-Ost)
  - AWS GovCloud Region (USA-West)
  - Region USA Ost (Nord-Virginia)
  - Region USA West (Oregon)
- Für die Authentifizierung während der Sitzung und die Authentifizierung vor der Sitzung unter Linux oder Windows ist derzeit WorkSpacesnur eine Smartcard gleichzeitig zulässig.
- Für die Authentifizierung vor der Sitzung wird die Aktivierung sowohl der Smartcard-Authentifizierung als auch der Anmeldeauthentifizierung im selben Verzeichnis derzeit nicht unterstützt.
- Derzeit werden nur CAC- und PIV-Karten unterstützt. Andere Arten von hardware- oder softwarebasierten Smartcards funktionieren möglicherweise, wurden aber für die Verwendung mit WSP nicht hinreichend getestet.

Verzeichniskonfiguration

Zur Aktivierung der Smartcard-Authentifizierung müssen Sie Ihr AD-Connector-Verzeichnis und Ihr On-Premises-Verzeichnis wie folgt konfigurieren.

Verzeichniskonfiguration für AD Connector

Bevor Sie beginnen, stellen Sie sicher, dass Ihr AD-Connector-Verzeichnis wie unter AD-Connector-Voraussetzungen im AWS Directory Service -Administratorhandbuch beschrieben eingerichtet wurde. Stellen Sie insbesondere sicher, dass Sie die erforderlichen Ports in Ihrer Firewall geöffnet haben.

Zum Abschließen der Konfiguration Ihres AD-Connector-Verzeichnisses folgen Sie den Anweisungen unter Aktivieren der mTLS-Authentifizierung in AD Connector für die Verwendung mit Smartcards im AWS Directory Service -Administratorhandbuch.

> **Note**
>
> Die Smartcard-Authentifizierung setzt voraus, dass Kerberos Constrained Delegation (KCD) ordnungsgemäß funktioniert. KCD erfordert, dass der Benutzernamenteil des AD-Connector-AccountName Servicekontos mit dem sAM desselben Benutzers übereinstimmt. Ein sAM AccountName darf 20 Zeichen nicht überschreiten.

Konfiguration des On-Premises-Verzeichnisses

Neben der Konfiguration Ihres AD-Connector-Verzeichnisses müssen Sie auch sicherstellen, dass für die Zertifikate, die für die Domain-Controller für Ihr On-Premises-Verzeichnis ausgestellt werden, die erweiterte Schlüsselverwendung (Extended Key Usage, EKU) „KDC Authentication“ festgelegt ist. Verwenden Sie dazu die standardmäßige Kerberos-Authentifizierungszertifikatsvorlage für Active Directory Domain Services (AD DS). Verwenden Sie keine Vorlage für ein Domain-Controller-Zertifikat oder eine Zertifikatsvorlage für die Domain-Controller-Authentifizierung, da diese Vorlagen nicht die erforderlichen Einstellungen für die Smartcard-Authentifizierung enthalten.

Smartcards für Windows aktivieren WorkSpaces

Allgemeine Hinweise zur Aktivierung der Smartcard-Authentifizierung unter Windows finden Sie in der Microsoft-Dokumentation unter Richtlinien für die Aktivierung der Smartcard-Anmeldung bei Zertifizierungsstellen von Drittanbietern.

So erkennen Sie den Windows-Sperrbildschirm und trennen die Sitzung

Damit Benutzer Windows entsperren können WorkSpaces , die für die Smartcard-Authentifizierung vor der Sitzung aktiviert sind, wenn der Bildschirm gesperrt ist, können Sie die Windows-Sperrbildschirmerkennung in Benutzersitzungen aktivieren. Wenn der Windows-Sperrbildschirm erkannt wird, wird die WorkSpace Sitzung getrennt, und der Benutzer kann sich mithilfe seiner Smartcard erneut mit dem WorkSpaces Client verbinden.

Sie können mithilfe der Gruppenrichtlinieneinstellungen das Trennen der Sitzung aktivieren, wenn der Windows-Sperrbildschirm für Windows-WorkSpaces erkannt wird. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren des Trennens der Sitzung bei Bildschirmsperre für WSP.

So aktivieren Sie die Authentifizierung während der Sitzung oder vor der Sitzung

Standardmäßig WorkSpaces ist Windows nicht aktiviert, um die Verwendung von Smartcards für die Authentifizierung vor oder während der Sitzung zu unterstützen. Bei Bedarf können Sie die

Authentifizierung während der Sitzung und vor der Sitzung für Windows mithilfe WorkSpaces der Gruppenrichtlinieneinstellungen aktivieren. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der Smartcard-Umleitung für WSP.

Zur Authentifizierung vor der Sitzung müssen Sie nicht nur die Gruppenrichtlinieneinstellungen aktualisieren, sondern auch die Authentifizierung vor der Sitzung über Ihre AD-Connector-Verzeichniseinstellungen aktivieren. Weitere Informationen finden Sie in den Anweisungen unter Aktivieren der mTLS-Authentifizierung in AD Connector für die Verwendung mit Smartcards im AWS Directory Service -Administratorhandbuch.

So ermöglichen Sie die Verwendung von Smartcards in einem Browser

Wenn Ihre Benutzer Chrome als Browser verwenden, ist für die Verwendung von Smartcards keine spezielle Konfiguration erforderlich.

Wenn Ihre Benutzer Firefox als Browser verwenden, können Sie Ihren Benutzern mithilfe von Gruppenrichtlinien die Verwendung von Smartcards in Firefox ermöglichen. Sie können diese Vorlagen für Firefox-Gruppenrichtlinien in verwenden GitHub.

Sie können beispielsweise die 64-Bit-Version von OpenSC für Windows installieren, um PKCS #11 zu unterstützen, und dann die folgende Gruppenrichtlinieneinstellung verwenden, wobei *NAME_OF_DEVICE* der Wert ist, den Sie zur Identifizierung von PKCS #11 verwenden möchten (z. B. `OpenSC`), und *PATH_TO_LIBRARY_FOR_DEVICE* der Pfad zum PKCS-#11-Modul ist. Dieser Pfad sollte auf eine Bibliothek mit der Erweiterung .DLL verweisen (z. B. `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`).

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

> **Tip**
>
> Wenn Sie OpenSC verwenden, können Sie das OpenSC-Modul `pkcs11` auch in Firefox laden, indem Sie das Programm `pkcs11-register.exe` ausführen. Zur Ausführung dieses Programms klicken Sie entweder doppelt auf die Datei unter `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe` oder öffnen Sie ein Befehlszeilenfenster und führen Sie den folgenden Befehl aus:
>
> ```
> "C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
> ```

Gehen Sie wie folgt vor, um zu überprüfen, ob das OpenSC-Modul `pkcs11` in Firefox geladen wurde:

1. Wenn Firefox bereits läuft, schließen Sie es.
2. Öffnen Sie Firefox. Wählen Sie die Menüschaltfläche

   in der oberen rechten Ecke und dann Optionen aus.
3. Wählen Sie auf der Seite about:preferences im linken Navigationsbereich die Option Datenschutz & Sicherheit aus.
4. Wählen Sie unter Zertifikate die Option Sicherheitsgeräte aus.
5. Im Dialogfeld Geräte-Manager sollte im linken Navigationsbereich das OpenSC-Smartcard-Framework (0.21) angezeigt werden und es sollte die folgenden Werte haben, wenn Sie es auswählen:

   Modul: `OpenSC smartcard framework (0.21)`

   Pfad: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

Fehlerbehebung

Informationen zur Problembehandlung bei Smartcards finden Sie in der Microsoft-Dokumentation unter Zertifikat- und Konfigurationsprobleme.

Einige häufig auftretende Probleme, die zu Problemen führen können:

- Falsche Zuordnung der Slots zu den Zertifikaten.
- Es befinden sich mehrere Zertifikate auf der Smartcard, die dem/der Benutzer:in entsprechen können. Zertifikate werden anhand der folgenden Kriterien abgeglichen:
  - Die Stammzertifizierungsstelle für das Zertifikat.
  - Die Felder <KU> und <EKU> des Zertifikats.
  - Der UPN im Zertifikatantragsteller.
- Mehrere Zertifikate, die `<EKU>msScLogin` in der Schlüsselnutzung verwendet.

Im Allgemeinen empfiehlt es sich, nur ein Zertifikat für die Smartcard-Authentifizierung zu verwenden, das dem allerersten Slot der Smartcard zugeordnet ist.

Die Tools zur Verwaltung der Zertifikate und Schlüssel auf der Smartcard (z. B. zum Entfernen oder Neuzuordnen der Zertifikate und Schlüssel) können herstellerspezifisch sein. Weitere Informationen finden Sie in der vom Hersteller Ihrer Smartcards mitgelieferten Dokumentation.

Smartcards für Linux aktivieren WorkSpaces

> **Note**
>
> Linux WorkSpaces auf WSP hat derzeit die folgenden Einschränkungen:
>
> - Zwischenablage-, Audioeingang-, Videoeingang- und Zeitzonenumleitung werden nicht unterstützt.
> - Mehrere Monitore werden nicht unterstützt.
> - Sie müssen die WorkSpaces Windows-Clientanwendung verwenden, um eine Verbindung zu Linux WorkSpaces auf WSP herzustellen.

Um die Verwendung von Smartcards unter Linux zu ermöglichen WorkSpaces, müssen Sie eine Stammzertifizierungsstellenzertifikatdatei im PEM-Format in das WorkSpace Image aufnehmen.

So erhalten Sie Ihr Stammzertifizierungsstellenzertifikat

Sie können Ihr Stammzertifizierungsstellenzertifikat auf verschiedene Arten erhalten:

- Sie können ein Stammzertifizierungsstellenzertifikat verwenden, das von einer externen Zertifizierungsstelle betrieben wird.
- Sie können Ihr eigenes Stammzertifizierungsstellenzertifikat mithilfe der Website für die Webregistrierung exportieren. Dabei handelt es sich entweder um `http://`*`ip_address`*`/certsrv` oder`http://`*`fqdn`*`/certsrv`, wobei *`ip_address`* und *`fqdn`* die IP-Adresse und der vollqualifizierte Domain-Name (FQDN) des Stammzertifizierungsstellenservers sind. Weitere Informationen zur Verwendung der Website für die Webregistrierung finden Sie in der Microsoft-Dokumentation unter So exportieren Sie ein Stammzertifizierungsstellenzertifikat.
- Mit dem folgenden Verfahren können Sie das Stammzertifizierungsstellenzertifikat von einem Stammzertifizierungsserver exportieren, auf dem die Active-Directory-Zertifikatsdienste (AD

CS) ausgeführt werden. Informationen zur Installation von AD CS finden Sie in der Microsoft-Dokumentation unter Installieren der Zertifizierungsstelle.

1. Melden Sie sich mit einem Administratorkonto beim Stammzertifizierungsstellenserver an.
2. Öffnen Sie im Windows-Startmenü ein Befehlszeilenfenster (Start > Windows-System > Eingabeaufforderung).
3. Verwenden Sie den folgenden Befehl, um das Stammzertifizierungsstellenzertifikat in eine neue Datei zu exportieren, wobei der Name der neuen Datei *rootca*.cer lautet:

   ```
   certutil -ca.cert rootca.cer
   ```

   Weitere Informationen zum Ausführen von certutil finden Sie unter certutil in der Microsoft-Dokumentation.
4. Verwenden Sie den folgenden OpenSSL-Befehl, um das exportierte Stammzertifizierungsstellenzertifikat vom DER-Format in das PEM-Format zu konvertieren, wobei *rootca* der Name des Zertifikats ist. Weitere Informationen zu OpenSSL finden Sie unter http://www.openssl.org.

   ```
   openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
   ```

So fügen Sie Ihr Stammzertifizierungsstellenzertifikat zu Linux hinzu WorkSpaces

Zur Unterstützung bei der Aktivierung von Smartcards haben wir das `enable_smartcard`-Skript zu unseren Amazon-Linux-WSP-Paketen hinzugefügt. Dieses Skript führt die folgenden Aktionen aus:

- Importiert Ihr Stammzertifizierungsstellenzertifikat in die Network-Security-Services-(NSS)-Datenbank.
- Installiert das `pam_pkcs11`-Modul für die PAM-Authentifizierung (Pluggable Authentication Module).
- Führt eine Standardkonfiguration durch, die die Aktivierung von `pkinit` während der WorkSpace Bereitstellung beinhaltet.

Im folgenden Verfahren wird erläutert, wie Sie das `enable_smartcard`Skript verwenden, um Ihr Stammzertifizierungsstellenzertifikat zu Linux hinzuzufügen WorkSpaces und Smartcards für Ihr Linux- zu aktivieren WorkSpaces.

1. Erstellen Sie ein neues Linux WorkSpace mit aktiviertem WSP-Protokoll. Stellen Sie beim Starten der WorkSpace in der Amazon- WorkSpaces Konsole auf der Seite Pakete auswählen sicher, dass Sie WSP für das Protokoll auswählen, und wählen Sie dann eines der öffentlichen Pakete von Amazon Linux 2 aus.
2. WorkSpaceFühren Sie in der neuen den folgenden Befehl als Stamm aus, wobei der Pfad zur Stammzertifizierungsstellenzertifikatsdatei im PEM-Format *pem-path* ist.

   ```
   /usr/lib/skylight/enable_smartcard --ca-cert pem-path
   ```

   > **Note**
   >
   > Linux WorkSpaces geht davon aus, dass die Zertifikate auf den Smartcards für den Standardbenutzerprinzipalnamen (User Principal Name, UPN) des Benutzers ausgestellt werden, z. B. *sAMAccountName*@*domain*, wobei ein vollqualifizierter Domänenname (Fully Qualified Domain Name, FQDN) *domain* ist.
   > Weitere Informationen zu alternativen UPN-Suffixen finden Sie unter `run /usr/lib/skylight/enable_smartcard --help`. Die Zuordnung für alternative UPN-Suffixe ist für jeden/jede Benutzer:in eindeutig. Daher muss diese Zuordnung einzeln auf jedem der Benutzer durchgeführt werden WorkSpace.

3. (Optional) Standardmäßig sind alle -Services aktiviert, um die Smartcard-Authentifizierung unter Linux zu verwenden WorkSpaces. Sie müssen `/etc/pam.d/system-auth` bearbeiten, um die Smartcard-Authentifizierung nur auf bestimmte Services zu beschränken. Entfernen Sie den Kommentar der Zeile `auth` für `pam_succeed_if.so` und bearbeiten Sie die Liste der Services nach Bedarf.

   Nachdem die Zeile `auth` kein Kommentar mehr ist, müssen Sie sie der Liste hinzufügen, damit ein Service die Smartcard-Authentifizierung verwenden kann. Damit ein Service nur die Passwortauthentifizierung verwendet, müssen Sie ihn aus der Liste entfernen.
4. Führen Sie alle zusätzlichen Anpassungen an der durch WorkSpace. Möglicherweise möchten Sie beispielsweise eine systemweite Richtlinie hinzufügen, um Benutzern die Verwendung von Smartcards in Firefox zu ermöglichen. (Chrome-Benutzer müssen Smartcards auf ihren Clients selbst aktivieren. Weitere Informationen finden Sie unter Smartcard-Unterstützung im Amazon-WorkSpaces Benutzerhandbuch.)
5. Erstellen Sie ein benutzerdefiniertes WorkSpace Image und ein Paket aus der WorkSpace.
6. Verwenden Sie das neue benutzerdefinierte Paket, um WorkSpaces für Ihre Benutzer zu starten.

So ermöglichen Sie Benutzern die Verwendung von Smartcards in Firefox

Sie können Ihren Benutzern die Verwendung von Smartcards in Firefox ermöglichen, indem Sie Ihrem Linux- WorkSpace Image eine SecurityDevices Richtlinie hinzufügen. Weitere Informationen zum Hinzufügen von systemweiten Richtlinien zu Firefox finden Sie in den Mozilla-Richtlinienvorlagen auf GitHub.

1. Erstellen Sie in der WorkSpace , mit der Sie Ihr WorkSpace Image erstellen, eine neue Datei mit dem Namen `policies.json` in `/usr/lib64/firefox/distribution/`.
2. Fügen Sie in der JSON-Datei die folgende SecurityDevices Richtlinie hinzu, wobei der Wert *`NAME_OF_DEVICE`* ist, den Sie zur Identifizierung des `pkcs` Moduls verwenden möchten. So können Sie beispielsweise einen Wert wie `"OpenSC"` verwenden:

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

Fehlerbehebung

Zur Fehlerbehebung empfehlen wir, das `pkcs11-tools`-Hilfsprogramm hinzuzufügen. Mit dem Hilfsprogramm können Sie die folgenden Aktionen ausführen:

- Auflisten aller Smartcards
- Auflisten der Slots auf jeder Smartcard
- Auflisten der Zertifikate auf jeder Smartcard

Einige häufig auftretende Probleme, die zu Problemen führen können:

- Falsche Zuordnung der Slots zu den Zertifikaten.
- Es befinden sich mehrere Zertifikate auf der Smartcard, die dem/der Benutzer:in entsprechen können. Zertifikate werden anhand der folgenden Kriterien abgeglichen:
  - Die Stammzertifizierungsstelle für das Zertifikat.
  - Die Felder <KU> und <EKU> des Zertifikats.

  - Der UPN im Zertifikatantragsteller.
- Mehrere Zertifikate, die <EKU>msScLogin in der Schlüsselnutzung verwendet.

Im Allgemeinen empfiehlt es sich, nur ein Zertifikat für die Smartcard-Authentifizierung zu verwenden, das dem allerersten Slot der Smartcard zugeordnet ist.

Die Tools zur Verwaltung der Zertifikate und Schlüssel auf der Smartcard (z. B. zum Entfernen oder Neuzuordnen der Zertifikate und Schlüssel) können herstellerspezifisch sein. Zusätzliche Tools, mit deren Hilfe Sie mit Smartcards arbeiten können, sind:

- opensc-explorer
- opensc-tool
- pkcs11_inspect
- pkcs11_listcerts
- pkcs15-tool

So aktivieren Sie die Protokollierung

Zur Behebung von Fehlern in Ihrer pam-krb5- und pam_pkcs11-Konfiguration können Sie die Debug-Protokollierung aktivieren.

1. Bearbeiten Sie in der /etc/pam.d/system-auth-ac-Datei die auth-Aktion und ändern Sie den nodebug-Parameter von pam_pksc11.so zu debug.
2. Ändern Sie in der Datei /etc/pam_pkcs11/pam_pkcs11.conf debug = false; zu debug = true;. Die debug-Option gilt separat für jedes Mapper-Modul, sodass Sie sie möglicherweise sowohl direkt im pam_pkcs11-Abschnitt als auch im entsprechenden Mapper-Abschnitt ändern müssen (standardmäßig ist dies mapper generic).
3. Bearbeiten Sie in der /etc/pam.d/system-auth-ac-Datei die auth-Aktion und fügen Sie den debug- oder debug_sensitive-Parameter zu pam_krb5.so hinzu.

Nachdem Sie die Debug-Protokollierung aktiviert haben, gibt das System pam_pkcs11-Debug-Meldungen direkt im aktiven Terminal aus. Nachrichten von pam_krb5 werden in /var/log/secure protokolliert.

Verwenden Sie den folgenden pklogin_finder-Befehl, um zu überprüfen, welchem Benutzernamen ein Smartcard-Zertifikat zugeordnet ist:

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

Geben Sie bei entsprechender Aufforderung die Smartcard-PIN ein. `pklogin_finder` gibt in `stdout` den Benutzernamen auf dem Smartcard-Zertifikat in der Form *`NETBIOS`*`\`*`username`* aus. Dieser Benutzername sollte mit dem WorkSpace Benutzernamen übereinstimmen.

In Active Directory Domain Services (AD DS) ist der NetBIOS-Domain-Name der Domain-Name vor Windows 2000. Normalerweise (aber nicht immer) ist der NetBIOS-Domain-Name die Unterdomain des DNS-Domain-Namens (Domain Name System). Wenn der DNS-Domain-Name `example.com` lautet, kann die NetBIOS-Domain beispielsweise `EXAMPLE` sein. Wenn der DNS-Domain-Name `corp.example.com` lautet, ist der NetBIOS-Domain normalerweise `CORP`.

Für den Benutzer `mmajor` in der Domain `pklogin_finder` lautet die Ausgabe von `corp.example.com` beispielsweise `CORP\mmajor`.

> **Note**
>
> Wenn Sie die Nachricht `"ERROR:pam_pkcs11.c:504: verify_certificate() failed"` erhalten, weist diese Meldung darauf hin, dass `pam_pkcs11` auf der Smartcard ein Zertifikat gefunden hat, das den Kriterien für den Benutzernamen entspricht, das aber nicht mit einem Stammzertifizierungsstellenzertifikat verknüpft ist, das vom Computer anerkannt wird. In diesem Fall gibt `pam_pkcs11` die Meldung oben aus und es wird dann das nächste Zertifikat versucht. Die Authentifizierung ist nur möglich, wenn ein Zertifikat gefunden wird, das sowohl dem Benutzernamen entspricht als auch mit einem anerkannten Stammzertifizierungsstellenzertifikat verknüpft ist.

Zur Behebung von Fehlern in Ihrer `pam_krb5`-Konfiguration können Sie sie `kinit` manuell im Debug-Modus mit dem folgenden Befehl aufrufen:

```
KRB5_TRACE=/dev/stdout kinit -V
```

Mit diesem Befehl sollte erfolgreich ein Kerberos Ticket Granting Ticket (TGT) abgerufen werden. Falls dies fehlschlägt, versuchen Sie, dem Befehl explizit den richtigen Kerberos-Prinzipalnamen hinzuzufügen. Verwenden Sie beispielsweise für den Benutzer `mmajor` in der Domain `corp.example.com` diesen Befehl:

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

Wenn dieser Befehl erfolgreich ist, liegt das Problem höchstwahrscheinlich in der Zuordnung vom WorkSpace Benutzernamen zum Kerberos-Prinzipalnamen vor. Überprüfen Sie den `[appdefaults]/pam/mappings`-Abschnitt in der Datei `/etc/krb5.conf`.

Wenn dieser Befehl nicht erfolgreich ist, ein passwortbasierter `kinit`-Befehl jedoch erfolgreich ist, überprüfen Sie die entsprechenden Konfigurationen zu `pkinit_` in der Datei `/etc/krb5.conf`. Wenn die Smartcard beispielsweise mehr als ein Zertifikat enthält, müssen Sie möglicherweise Änderungen an `pkinit_cert_match` vornehmen.

Bereitstellen des Internetzugangs von Ihrem aus WorkSpace

Ihr WorkSpaces muss Zugriff auf das Internet haben, damit Sie Updates für das Betriebssystem installieren und Anwendungen bereitstellen können. Sie können eine der folgenden Optionen verwenden, um Ihrem WorkSpaces in einer Virtual Private Cloud (VPC) den Zugriff auf das Internet zu ermöglichen.

Optionen

- Starten Sie Ihre WorkSpaces in privaten Subnetzen und konfigurieren Sie ein NAT-Gateway in einem öffentlichen Subnetz in Ihrer VPC.
- Starten Sie Ihr WorkSpaces in öffentlichen Subnetzen und weisen Sie Ihrem automatisch oder manuell öffentliche IP-Adressen zu WorkSpaces.

Weitere Informationen zu diesen Optionen finden Sie in den entsprechenden Abschnitten unterKonfigurieren einer VPC für WorkSpaces.

Mit einer dieser Optionen müssen Sie sicherstellen, dass die Sicherheitsgruppe für Ihr WorkSpaces ausgehenden Datenverkehr an den Ports 80 (HTTP) und 443 (HTTPS) zu allen Zielen () zulässt`0.0.0.0/0`.

Amazon-Linux-Extras-Bibliothek

Wenn Sie das Amazon Linux-Repository verwenden, WorkSpaces muss Ihr Amazon Linux entweder über Internetzugang verfügen oder Sie müssen VPC-Endpunkte für dieses Repository und das Amazon Linux-Haupt-Repository konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispiel: Gewähren von Zugriff auf Amazon Linux-AMI-Repositorys unter Endpunkte für Amazon S3. Die Amazon Linux-AMI-Repositorys sind Amazon S3-Buckets in den einzelnen Regionen. Wenn Sie Instances in Ihrer VPC Zugriff auf die Repositorys über einen Endpunkt gewähren möchten, erstellen

Sie eine Endpunktrichtlinie, die Zugriff auf diese Buckets gewährt. Die folgende Richtlinie gewährt Zugriff auf die Amazon Linux-Repositorys.

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

Sicherheitsgruppen für Ihr WorkSpaces

Wenn Sie ein Verzeichnis bei registrieren WorkSpaces, werden zwei Sicherheitsgruppen erstellt, eine für Verzeichniscontroller und eine für WorkSpaces im Verzeichnis . Die Sicherheitsgruppe für Verzeichniscontroller hat einen Namen, der aus der Verzeichniskennung gefolgt von _controllers besteht (Beispiel: d-12345678e1_controllers). Die Sicherheitsgruppe für WorkSpaces hat einen Namen, der aus der Verzeichnis-ID gefolgt von _workspacesMembers besteht (z. B. d-123456xy11_workspacesMembers).

> **Warning**
>
> Vermeiden Sie es, die Sicherheitsgruppen _controllers und _workspacesMembers zu ändern, zu löschen oder zu trennen. Seien Sie vorsichtig, wenn Sie diese Sicherheitsgruppen ändern oder löschen, da Sie diese Gruppen nicht neu erstellen und wieder hinzufügen können, nachdem sie geändert oder gelöscht wurden. Weitere Informationen finden Sie unter Amazon-EC2-Sicherheitsgruppen für Linux-Instances oder unter Amazon-EC2-Sicherheitsgruppen für Windows-Instances.

Sie können einem Verzeichnis eine WorkSpaces Standardsicherheitsgruppe hinzufügen. Nachdem Sie eine neue Sicherheitsgruppe mit einem WorkSpaces Verzeichnis verknüpft haben, wird die neue Sicherheitsgruppe für neue WorkSpaces , die Sie starten, oder vorhandene , WorkSpaces die Sie neu erstellen, verwendet. Sie können diese neue Standardsicherheitsgruppe auch zu vorhandenen hinzufügen, WorkSpaces ohne sie neu zu erstellen, wie weiter unten in diesem Thema erläutert.

Wenn Sie einem WorkSpaces Verzeichnis mehrere Sicherheitsgruppen zuordnen, werden die Regeln jeder Sicherheitsgruppe effektiv zu einem einzigen Regelsatz aggregiert. Wir empfehlen, Ihre Sicherheitsgruppenregeln so weit wie möglich zu verdichten.

Weitere Informationen zu Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihre VPC im Amazon-VPC-Benutzerhandbuch.

So fügen Sie eine Sicherheitsgruppe zu einem WorkSpaces Verzeichnis hinzu

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.
4. Erweitern Sie Security Group und wählen Sie eine Sicherheitsgruppe aus.
5. Wählen Sie Update and Exit aus.

Um eine Sicherheitsgruppe zu einem vorhandenen hinzuzufügen, WorkSpace ohne sie neu zu erstellen, weisen Sie die neue Sicherheitsgruppe der Elastic-Network-Schnittstelle (ENI) des zu WorkSpace.

So fügen Sie eine Sicherheitsgruppe zu einem vorhandenen hinzu WorkSpace

1. Suchen Sie die IP-Adresse für jede WorkSpace , die aktualisiert werden muss.
   a. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
   b. Erweitern Sie jede WorkSpace und notieren Sie ihre WorkSpace IP-Adresse.
2. Suchen Sie die ENI für jede WorkSpace und aktualisieren Sie ihre Sicherheitsgruppenzuweisung.
   a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie unter Network & Security (Netzwerk & Sicherheit) die Option Network Interfaces (Netzwerkschnittstellen).

c. Suchen Sie nach der ersten IP-Adresse, die Sie in Schritt 1 aufgezeichnet haben.
d. Wählen Sie die ENI, die mit der IP-Adresse verknüpft ist, klicken Sie auf Actions (Aktionen) und dann auf Change Security Groups (Sicherheitsgruppen ändern).
e. Wählen Sie die neue Sicherheitsgruppe und Save (Speichern) aus.
f. Wiederholen Sie diesen Vorgang nach Bedarf für alle anderen WorkSpaces.

IP-Zugriffskontrollgruppen für WorkSpaces

Mit Amazon WorkSpaces können Sie steuern, von welchen IP-Adressen aus auf Ihre WorkSpaces zugegriffen werden kann. Mit IP-basierten Kontrollgruppen können Sie Gruppen vertrauenswürdiger IP-Adressen definieren und verwalten und Benutzer nur dann Zugriff auf ihre WorkSpaces gewähren, wenn sie mit einem vertrauenswürdigen Netzwerk verbunden sind.

Eine IP-Zugriffskontrollgruppe fungiert als eine virtuelle Firewall, über die Sie bestimmen, von welchen IP-Adressen aus die Benutzer auf ihre WorkSpaces zugreifen dürfen. Fügen Sie Regeln zu Ihrer IP-Zugriffskontrollgruppe hinzu und ordnen die Gruppe dann Ihrem Verzeichnis zu, um die CIDR-Adressbereiche anzugeben. Sie können jede IP-Zugriffskontrollgruppe mit einem oder mehreren Verzeichnissen verknüpfen. Sie können bis zu 100 IP-Zugriffskontrollgruppen pro Region und AWS-Konto erstellen. Allerdings können Sie jedem Verzeichnis nur bis zu 25 IP-Zugriffskontrollgruppen zuweisen.

Jedem Verzeichnis ist eine standardmäßige IP-Zugriffskontrollgruppe zugeordnet. Diese Standardgruppe enthält eine Standardregel, die es Benutzern ermöglicht, von überall aus auf ihre WorkSpaces zuzugreifen. Sie können die Standard-IP-Zugriffskontrollgruppe für Ihr Verzeichnis nicht ändern. Wenn Sie Ihrem Verzeichnis keine IP-Zugriffskontrollgruppe zuordnen, wird die Standardgruppe verwendet. Wenn Sie einem Verzeichnis eine IP-Zugriffskontrollgruppe zuweisen, wird die Verknüpfung mit der standardmäßigen IP-Zugriffskontrollgruppe aufgehoben.

Um die öffentlichen IP-Adressen und IP-Adressbereiche für Ihre vertrauenswürdigen Netzwerke anzugeben, fügen Sie den IP-Zugriffskontrollgruppen Regeln hinzu. Wenn Ihre Benutzer über ein NAT-Gateway oder VPN auf ihre WorkSpaces zugreifen, müssen Sie Regeln erstellen, die den Datenverkehr von den öffentlichen IP-Adressen für das NAT-Gateway oder VPN zulassen.

> **Note**
>
> - IP-Zugriffskontrollgruppen erlauben die Verwendung dynamischer IP-Adressen für NATs nicht. Wenn Sie ein NAT-Gateway verwenden, konfigurieren Sie dieses so, dass anstelle

einer dynamischen IP-Adresse eine statische IP-Adresse verwendet wird. Stellen Sie sicher, dass das NAT-Gateway den gesamten UDP-Datenverkehr während der gesamten WorkSpaces-Sitzung über dieselbe statische IP-Adresse weiterleitet.

- IP-Zugriffskontrollgruppen steuern die IP-Adressen, von denen aus sich Benutzer mit ihren WorkSpaces-Streaming-Sitzungen verbinden können. Die Benutzer können über die öffentlichen APIs von Amazon WorkSpaces weiterhin Funktionen wie Neustart, Neuerstellung und Herunterfahren von jeder beliebigen IP-Adresse ausführen.

Sie können diese Funktion mit Web-Access-, PCoIP-Zero-Clients und den Client-Anwendungen für macOS X, iPad, Windows, Chromebook und Android verwenden.

Erstellen einer IP-Zugriffskontrollgruppe

IP-Zugriffskontrollgruppen erstellen Sie wie folgt. Jede IP-Zugriffskontrollgruppe kann maximal 10 Regeln enthalten.

So erstellen Sie eine IP-Zugriffskontrollgruppe

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich IP Access Controls (IP-Zugriffskontrollen) aus.
3. Klicken Sie auf Create IP Group (IP-Gruppe erstellen).
4. Geben Sie im Dialogfeld Create IP Group (IP-Gruppe erstellen) einen Namen und eine Beschreibung für die Gruppe ein. Klicken Sie dann auf Create (Erstellen).
5. Markieren Sie die Gruppe und wählen Sie Edit (Bearbeiten) aus.
6. Klicken Sie für jede IP-Adresse auf Add Rule (Regel hinzufügen). Geben Sie im Feld Source (Quelle) die IP-Adresse oder den IP-Adressbereich ein. Geben Sie im Feld Description (Beschreibung) eine Beschreibung ein. Wenn Sie mit dem Hinzufügen von Regeln fertig sind, klicken Sie auf Save (Speichern).

Zuordnen einer IP-Zugriffskontrollgruppe zu einem Verzeichnis

Sie können eine IP-Zugriffskontrollgruppe mit einem Verzeichnis verknüpfen, um sicherzustellen, dass nur von vertrauenswürdigen Netzwerken auf WorkSpaces zugegriffen wird.

Wenn Sie eine IP-Zugriffskontrollgruppe zuweisen, die keine Regeln für ein Verzeichnis hat, wird jeglicher Zugriff auf alle WorkSpaces blockiert.

So verknüpfen Sie eine IP-Zugriffskontrollgruppe mit einem Verzeichnis

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.
4. Erweitern Sie IP Access Control Groups (IP-Zugriffskontrollgruppen) und wählen Sie eine oder mehrere IP-Zugriffskontrollgruppen aus.
5. Wählen Sie Update and Exit aus.

Kopieren einer IP-Zugriffskontrollgruppe

Sie können eine vorhandene IP-Zugriffskontrollgruppe als Basis für die Erstellung einer neuen IP-Zugriffskontrollgruppe verwenden.

So erstellen Sie eine IP-Zugriffskontrollgruppe anhand einer vorhandenen

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich IP Access Controls (IP-Zugriffskontrollen) aus.
3. Markieren Sie die Gruppe und wählen Sie Actions (Aktionen) und Copy to New (In neue kopieren) aus.
4. Geben Sie im Dialogfeld Copy IP Group (IP-Gruppe kopieren) einen Namen und eine Beschreibung für die neue Gruppe ein. Klicken Sie dann auf Copy Group (Gruppe kopieren).
5. (Optional) Wenn Sie die Regeln ändern möchten, die Sie aus der ursprünglichen Gruppe kopiert haben, wählen Sie die neue Gruppe aus und klicken Sie auf Edit (Bearbeiten). Sie können nun nach Bedarf Regeln hinzufügen, aktualisieren oder entfernen. Wählen Sie Save (Speichern).

Löschen einer IP-Zugriffskontrollgruppe

Sie können eine Regel für eine IP-Zugriffskontrollgruppe jederzeit löschen. Wenn Sie eine Regel entfernen, die eine Verbindung mit einem WorkSpace zugelassen hat, wird der Benutzer von dem WorkSpace getrennt.

Bevor Sie eine IP-Zugriffskontrollgruppe löschen können, müssen Sie all ihre Verknüpfungen mit Verzeichnissen aufheben.

So löschen Sie eine IP-Zugriffskontrollgruppe

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie für jedes Verzeichnis, das mit der IP-Zugriffskontrollgruppe verknüpft ist, das Verzeichnis aus und klicken Sie auf Actions (Aktionen) Update Details (Details aktualisieren). Erweitern Sie IP Access Control Groups (IP-Zugriffskontrollgruppen), deaktivieren Sie das Kontrollkästchen für die IP-Zugriffskontrollgruppe und klicken Sie auf Update and Exit (Aktualisieren und verlassen).
4. Wählen Sie im Navigationsbereich IP Access Controls (IP-Zugriffskontrollen) aus.
5. Wählen Sie die Gruppe aus und klicken Sie auf Actions (Aktionen), Delete IP Group (IP-Gruppe löschen).

Einrichten von PCoIP-Zero-Clients für WorkSpaces

PCoIP-Zero-Clients sind nur mit WorkSpaces-Paketen kompatibel, die das PCoIP-Protokoll verwenden.

Wenn Ihr Zero-Client-Gerät über die Firmware-Version 6.0.0 oder höher verfügt, können sich Ihre Benutzer direkt mit ihren WorkSpaces verbinden. Wenn Ihre Benutzer über ein Zero-Client-Gerät eine direkte Verbindung zu ihren WorkSpaces herstellen, empfehlen wir, die Multi-Faktor-Authentifizierung (MFA) für Ihr WorkSpaces-Verzeichnis zu verwenden. Weitere Informationen zur Verwendung von MFA mit Ihrem Verzeichnis finden Sie in der folgenden Dokumentation:

- AWS Managed Microsoft AD – Aktivieren der Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD im AWS Directory Service-Administratorhandbuch
- AD Connector – Aktivieren der Multi-Faktor-Authentifizierung für AD Connector im AWS Directory Service-Administratorhandbuch und Multi-Faktor-Authentifizierung (AD Connector).
- Vertrauenswürdige Domains – Aktivieren der Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD im AWS Directory Service-Administratorhandbuch.
- Simple AD – Die Multi-Faktor-Authentifizierung ist für Simple AD nicht verfügbar.

Seit dem 13. April 2021 wird der PCoIP Connection Manager nicht mehr für die Verwendung mit Firmware-Versionen zwischen 4.6.0 und 6.0.0 für Zero-Client-Geräte unterstützt. Wenn Ihre Zero-Client-Firmware nicht Version 6.0.0 oder höher ist, können Sie die neueste Firmware über ein Desktop-Access-Abonnement unter https://www.teradici.com/desktop-access herunterladen.

Important

- Stellen Sie im Teradici PCoIP Administrative Web Interface (AWI) oder der Teradici PCoIP Management Console (MC) sicher, dass Sie Network Time Protocol (NTP) aktivieren. Verwenden Sie **`pool.ntp.org`** für den NTP-Host-DNS-Namen, und legen Sie den NTP-Host-Port auf 123fest. Wenn NTP nicht aktiviert ist, erhalten Ihre PCoIP-Null-Client-Benutzer möglicherweise Zertifikatfehler, z. B. „Das angegebene Zertifikat ist aufgrund des Zeitstempels ungültig.“
- Ab Version 20.10.4 des PCoIP-Agents deaktiviert Amazon WorkSpaces die USB-Umleitung standardmäßig über die Windows-Registrierung. Diese Registrierungseinstellung wirkt sich auf das Verhalten von USB-Peripheriegeräten aus, wenn Ihre Benutzer PCoIP-Zero-Client-Geräte verwenden, um eine Verbindung zu ihren WorkSpaces herzustellen. Weitere Informationen finden Sie unter USB-Drucker und andere USB-Peripheriegeräte funktionieren nicht für PCoIP-Zero-Clients.

Weitere Informationen zum Einrichten und Herstellen einer Verbindung mit einem PCoIP-Zero-Client-Gerät finden Sie unter PCoIP-Zero-Client im Amazon-WorkSpaces-Benutzerhandbuch. Eine Liste der zugelassenen PCoIP-Zero-Client-Geräte finden Sie unter PCoIP-Zero-Clients auf der Teradici-Website.

Einrichten von Android für Chromebooks

Version 2.4.13 ist die endgültige Version der Amazon WorkSpaces Chromebook-Client-Anwendung. Da Google die Unterstützung für Chrome Apps schrittweise aufhebt, werden keine weiteren Aktualisierungen für die WorkSpaces Chromebook-Clientanwendung durchgeführt, und seine Verwendung wird nicht unterstützt.

Für Chromebooks, die die Installation von Android-Anwendungen unterstützen, empfehlen wir stattdessen, die WorkSpaces-Android-Clientanwendung zu verwenden.

Einige Chromebooks, die vor 2019 gestartet wurden, müssen zum Installieren von Android-Apps befähigt werden, bevor Benutzer die Amazon WorkSpaces-Android-Clientanwendung installieren können. Weitere Informationen finden Sie unter Chrome OS-Systeme, die Android-Apps unterstützen.

Informationen zum Remote-Verwalten der Chromebooks Ihrer Benutzer zum Installieren von Android-Apps finden Sie unter Einrichten von Android für Chromebooks.

Amazon WorkSpaces Web Access aktivieren und konfigurieren

Die meisten WorkSpaces Bundles unterstützen Amazon WorkSpaces Web Access. Eine Liste der WorkSpaces unterstützten Webbrowser-Zugriffe finden Sie unter „Welche WorkSpaces Amazon-Bundles unterstützen Web Access?“ in Clientzugriff, Webzugriff und Benutzererfahrung.

Note

- Web Access mit WSP für Windows und Ubuntu WorkSpaces wird in allen Regionen unterstützt, in denen WSP WorkSpaces verfügbar ist. WSP für Amazon Linux WorkSpaces ist nur in AWS GovCloud (US-West) verfügbar.
- Wir empfehlen dringend, Web Access mit WSP WorkSpaces zu verwenden, um die beste Streaming-Qualität und Benutzererfahrung zu erzielen. Bei der Verwendung von Web Access mit WorkSpaces PCoIP gelten die folgenden Einschränkungen:
  - Web Access mit PCoIP wird im asiatisch-pazifischen Raum (Mumbai), Afrika (Kapstadt) und Israel (Tel Aviv) nicht unterstützt AWS GovCloud (US) Regions
  - Web Access mit PCoIP wird nur für Windows unterstützt WorkSpaces, nicht für Amazon Linux. WorkSpaces
  - Web Access ist für einige Windows 10, die WorkSpaces das PCoIP-Protokoll verwenden, nicht verfügbar. Wenn Ihre PCoIP mit Windows Server 2019 betrieben WorkSpaces werden, ist Web Access nicht verfügbar.

Important

Ab dem 1. Oktober 2020 können Kunden den Amazon WorkSpaces Web Access-Client nicht mehr verwenden, um eine Verbindung zu Windows 7 Custom WorkSpaces oder zu Windows 7 Bring Your Own License (BYOL) WorkSpaces herzustellen.

Schritt 1: Aktivieren Sie den Webzugriff auf Ihr WorkSpaces

Sie steuern den Webzugriff WorkSpaces auf Ihre Verzeichnisebene. Führen Sie für jedes Verzeichnis WorkSpaces , auf das Sie Benutzern den Zugriff über den Web Access-Client ermöglichen möchten, die folgenden Schritte aus.

So aktivieren Sie den Webzugriff auf Ihr WorkSpaces

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie in der Spalte Verzeichnis-ID die Verzeichnis-ID des Verzeichnisses aus, für das Sie Web Access aktivieren möchten.
4. Scrollen Sie auf der Seite mit den Verzeichnisdetails nach unten zum Abschnitt Andere Plattformen und wählen Sie Bearbeiten aus.
5. Wählen Sie Web Access.
6. Wählen Sie Speichern.

> **Note**
>
> Nachdem Sie Web Access aktiviert haben, starten Sie Ihren neu, WorkSpace damit die Änderung wirksam wird.

Schritt 2: Konfigurieren des eingehenden und ausgehenden Zugriffs auf Ports für Web Access

Amazon WorkSpaces Web Access erfordert eingehenden und ausgehenden Zugriff für bestimmte Ports. Weitere Informationen finden Sie unter Ports für Internetzugang.

Schritt 3: Konfigurieren von Gruppenrichtlinien- und Sicherheitsrichtlinieneinstellungen, um Benutzern die Anmeldung zu ermöglichen

Amazon WorkSpaces verwendet eine spezielle Konfiguration des Anmeldebildschirms, damit sich Benutzer erfolgreich von ihrem Web Access-Client aus anmelden können.

Damit sich Web Access-Benutzer bei ihnen anmelden können WorkSpaces, müssen Sie eine Gruppenrichtlinieneinstellung und drei Sicherheitsrichtlinieneinstellungen konfigurieren. Wenn diese Einstellungen nicht korrekt konfiguriert sind, kann es bei Benutzern zu langen Anmeldezeiten oder schwarzen Bildschirmen kommen, wenn sie versuchen, sich bei ihren WorkSpaces anzumelden. Gehen Sie folgendermaßen vor, um diese Einstellungen zu konfigurieren.

Sie können Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) verwenden, um Einstellungen für die Verwaltung von Windows WorkSpaces oder Benutzern, die Teil Ihres WorkSpaces Windows-Verzeichnisses sind, anzuwenden. Es wird empfohlen, eine Organisationseinheit für Ihre WorkSpaces Computerobjekte und eine Organisationseinheit für Ihre WorkSpaces Benutzerobjekte zu erstellen.

Weitere Informationen zur Verwendung der Active-Directory-Verwaltungstools für die Arbeit mit GPOs finden Sie unter Installieren der Active-Directory-Verwaltungstools im AWS Directory Service - Administratorhandbuch.

Damit der WorkSpaces Logon Agent zwischen Benutzern wechseln kann

In den meisten Fällen, wenn ein Benutzer versucht, sich bei einem anzumelden WorkSpace, wird das Feld für den Benutzernamen automatisch mit dem Namen dieses Benutzers aufgefüllt. Wenn ein Administrator jedoch eine RDP-Verbindung zu dem WorkSpace hergestellt hat, um Wartungsaufgaben durchzuführen, wird das Feld für den Benutzernamen stattdessen mit dem Namen des Administrators gefüllt.

Um dieses Problem zu vermeiden, deaktivieren Sie die Gruppenrichtlinieneinstellung Einstiegspunkte für die schnelle Benutzerumschaltung ausblenden. Wenn Sie diese Einstellung deaktivieren, kann der WorkSpaces Anmeldeagent die Schaltfläche Benutzer wechseln verwenden, um das Feld für den Benutzernamen mit dem richtigen Namen auszufüllen.

1. Öffnen Sie das Gruppenrichtlinien-Verwaltungstool (gpmc.msc), navigieren Sie zu einem Gruppenrichtlinienobjekt auf der Domänen- oder Domänencontrollerebene des Verzeichnisses, das Sie für Ihr verwenden, und wählen Sie es aus. WorkSpaces (Wenn Sie die administrative WorkSpaces Gruppenrichtlinienvorlage in Ihrer Domäne installiert haben, können Sie das WorkSpaces Gruppenrichtlinienobjekt für Ihre WorkSpaces Computerkonten verwenden.)
2. Klicken Sie im Hauptmenü auf Aktion,Bearbeiten.
3. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, System, und Anmeldung aus.
4. Öffnen Sie die Einstellung Einstiegspunkte für die schnelle Benutzerumschaltung ausblenden.
5. Wählen Sie im Dialogfeld Einstiegspunkte für die schnelle Benutzerumschaltung ausblenden die Option Deaktiviert aus und klicken Sie dann auf OK.

So blenden Sie den zuletzt angemeldeten Benutzernamen aus

Standardmäßig wird anstelle der Schaltfläche Benutzer wechseln die Liste der zuletzt angemeldeten Benutzer angezeigt. Je nach Konfiguration von zeigt die WorkSpace Liste möglicherweise nicht die Kachel Anderer Benutzer an. Wenn diese Situation eintritt und der vorab ausgefüllte Benutzername nicht korrekt ist, kann der WorkSpaces Anmeldeagent das Feld nicht mit dem richtigen Namen füllen.

Um dieses Problem zu vermeiden, aktivieren Sie die Sicherheitsrichtlinieneinstellung Interaktive Anmeldung: Zuletzt angemeldeten Benutzer nicht anzeigenoder Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen (je nachdem, welche Version von Windows Sie verwenden).

1. Öffnen Sie das Gruppenrichtlinien-Verwaltungstool (gpmc.msc), navigieren Sie zu einem Gruppenrichtlinienobjekt auf der Domänen- oder Domänencontrollerebene des Verzeichnisses, das Sie für Ihr verwenden, und wählen Sie es aus. WorkSpaces (Wenn Sie die administrative WorkSpaces Gruppenrichtlinienvorlage in Ihrer Domäne installiert haben, können Sie das WorkSpaces Gruppenrichtlinienobjekt für Ihre WorkSpaces Computerkonten verwenden.)
2. Klicken Sie im Hauptmenü auf Aktion,Bearbeiten.
3. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Windows-Einstellungen, Sicherheitseinstellungen, Lokale Richtlinien und Sicherheitsoptionen aus.
4. Öffnen Sie eine der folgenden Optionen:

   - Für Windows 7 – Interaktive Anmeldung: Zuletzt angemeldet nicht anzeigen
   - Für Windows 10 – Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen
5. Wählen Sie im Dialogfeld Eigenschaften für die Einstellung die Option Aktiviert aus und klicken Sie dann auf OK.

So erzwingen Sie das Drücken von STRG+ALT+ENTF, bevor sich Benutzer anmelden können

Für den WorkSpaces Webzugriff müssen Benutzer STRG+ALT+DEL drücken, bevor sie sich anmelden können. Wenn von Benutzern verlangt wird, vor der Anmeldung STRG+ALT +ENTF zu drücken, wird sichergestellt, dass Benutzer bei der Eingabe ihrer Passwörter einen vertrauenswürdigen Pfad verwenden.

1. Öffnen Sie das Gruppenrichtlinien-Verwaltungstool (gpmc.msc), navigieren Sie zu einem Gruppenrichtlinienobjekt auf der Domänen- oder Domänencontrollerebene des Verzeichnisses, das Sie für Ihr verwenden, und wählen Sie es aus. WorkSpaces (Wenn Sie die administrative WorkSpaces Gruppenrichtlinienvorlage in Ihrer Domäne installiert haben, können Sie das WorkSpaces Gruppenrichtlinienobjekt für Ihre WorkSpaces Computerkonten verwenden.)

2. Klicken Sie im Hauptmenü auf Aktion,Bearbeiten.
3. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Windows-Einstellungen, Sicherheitseinstellungen, Lokale Richtlinien und Sicherheitsoptionen aus.
4. Öffnen Sie die Einstellung Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich.
5. Wählen Sie auf der Registerkarte Lokale Sicherheitseinstellungen die Option Deaktiviert und klicken Sie dann auf OK.

So zeigen Sie die Domänen- und Benutzerinformationen an, wenn die Sitzung gesperrt ist

Der WorkSpaces Logon Agent sucht nach dem Namen und der Domäne des Benutzers. Nachdem diese Einstellung konfiguriert wurde, zeigt der Sperrbildschirm den vollständigen Namen des Benutzers (falls er in Active Directory angegeben ist), den Domänennamen und den Benutzernamen an.

1. Öffnen Sie das Gruppenrichtlinien-Verwaltungstool (gpmc.msc), navigieren Sie zu einem Gruppenrichtlinienobjekt auf der Domänen- oder Domänencontrollerebene des Verzeichnisses, das Sie für Ihr verwenden, und wählen Sie es aus. WorkSpaces (Wenn Sie die administrative WorkSpaces Gruppenrichtlinienvorlage in Ihrer Domäne installiert haben, können Sie das WorkSpaces Gruppenrichtlinienobjekt für Ihre WorkSpaces Computerkonten verwenden.)
2. Klicken Sie im Hauptmenü auf Aktion,Bearbeiten.
3. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Windows-Einstellungen, Sicherheitseinstellungen, Lokale Richtlinien und Sicherheitsoptionen aus.
4. Öffnen Sie die Einstellung Interaktive Anmeldung: Benutzerinformationen anzeigen, wenn Sitzung gesperrt ist.
5. Wählen Sie auf der Registerkarte Lokale Sicherheitseinstellungen die Option Benutzeranzeigename, Domain und Benutzernamen aus und klicken Sie dann auf OK.

So wenden Sie die Änderungen der Gruppenrichtlinien- und Sicherheitsrichtlinieneinstellungen an

Änderungen an den Einstellungen der Gruppenrichtlinien und Sicherheitsrichtlinien werden nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinien- und Sicherheitsrichtlinienänderungen der vorherigen Verfahren anzuwenden:

- Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).

- Geben Sie an einer administrativen Eingabeaufforderung gpupdate /force ein.

Einrichten von Amazon WorkSpaces für die FedRAMP-Autorisierung oder DoD-SRG-Compliance

Sie müssen Amazon WorkSpaces zur Verwendung der FIPS-Endpunktverschlüsselung (Federal Information Processing Standards) auf Verzeichnisebene konfigurieren, um das Federal Risk and Authorization Management Program (FedRAMP) bzw. den Cloud Computing Security Requirements Guide (SRG) des US-Verteidigungsministeriums (Department of Defense, DoD) einzuhalten. Außerdem müssen Sie eine US-AWS-Region festlegen, die über eine FedRAMP-Autorisierung verfügt oder mit dem DoD-SRG konform ist.

Die Stufe der FedRAMP-Autorisierung (Moderate oder High) oder das DoD SRG Impact Level (2, 4 oder 5) hängt von der AWS-Region in den USA ab, in der Amazon WorkSpaces verwendet wird. Informationen zur Stufe der FedRAMP-Autorisierung und zur DoD SRG-Compliance, die für die einzelne Region gelten, finden Sie unter Abgedeckte AWS-Services je Compliance-Programm.

> **Note**
>
> Zusätzlich zur FIPS-Endpunktverschlüsselung können Sie Ihre WorkSpaces verschlüsseln. Weitere Informationen finden Sie unter Verschlüsselte WorkSpaces.

Voraussetzungen

- Sie müssen Ihre WorkSpaces in einer US-AWS-Region, die über eine FedRAMP-Autorisierung verfügt oder mit dem DoD-SRG konform ist, erstellen.
- Das WorkSpaces-Verzeichnis muss den FIPS 140-2 Validated Mode für die Endpunktverschlüsselung verwenden.

> **Note**
>
> Um die Einstellung FIPS 140-2 Validated Mode zu verwenden, muss das WorkSpaces-Verzeichnis entweder neu sein oder alle vorhandenen WorkSpaces im Verzeichnis müssen den FIPS 140-2 Validated Mode für die Endpunktverschlüsselung verwenden. Andernfalls

können Sie diese Einstellung nicht verwenden und die von Ihnen erstellten WorkSpaces erfüllen nicht die FedRAMP- bzw. DoD-Sicherheitsanforderungen.

- Benutzer müssen über eine der folgenden WorkSpaces-Clientanwendung auf ihre WorkSpaces zugreifen:
  - Windows 2.4.3 oder höher
  - macOS 2.4.3 oder höher
  - Linux: 3.0.0 oder höher
  - iOS 2.4.1 oder höher
  - Android 2.4.1 oder höher
  - Fire Tablet 2.4.1 oder höher
  - ChromeOS 2.4.1 oder höher
  - Internetzugang

So verwenden Sie die FIPS-Endpunktverschlüsselung

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Vergewissern Sie sich, dass dem Verzeichnis, in dem Sie FedRAMP-autorisierte und DoD SRG-konforme WorkSpaces erstellen möchten, keine vorhandenen WorkSpaces zugeordnet sind. Wenn dem Verzeichnis WorkSpaces zugeordnet sind und für das Verzeichnis nicht bereits die Verwendung des FIPS 140-2 Validated Mode aktiviert ist, beenden Sie entweder die WorkSpaces oder erstellen Sie ein neues Verzeichnis.
4. Wählen Sie das Verzeichnis aus, das die oben genannten Kriterien erfüllt, und klicken Sie auf Actions (Aktionen) und dann auf Update Details (Details aktualisieren).
5. Klicken Sie auf der Seite Update Directory Details (Aktualisieren von Verzeichnisdetails) auf den Pfeil, um den Abschnitt Access Control Options (Zugriffskontrolloptionen) zu erweitern.
6. Wählen Sie für Endpoint Encryption (Endpunktverschlüsselung), die Option FIPS 140-2 Validated Mode anstelle von TLS Encryption Mode (Standard)aus.
7. Wählen Sie Update and Exit aus.
8. Sie können jetzt aus diesem Verzeichnis FedRAMP-autorisierte und DoD SRG-konforme WorkSpaces erstellen. Um auf diese WorkSpaces zuzugreifen, müssen Benutzer eine der WorkSpaces-Clientanwendungen verwenden, die zuvor im Abschnitt Anforderungen aufgelistet wurden.

Aktivieren von SSH-Verbindungen für Linux WorkSpaces

Wenn Sie oder Ihre Benutzer WorkSpaces über die Befehlszeile eine Verbindung zu Ihrem Amazon Linux herstellen möchten, können Sie SSH-Verbindungen aktivieren. Sie können SSH-Verbindungen zu allen WorkSpaces in einem Verzeichnis oder zu einzelnen WorkSpaces in einem Verzeichnis aktivieren.

Um SSH-Verbindungen zu aktivieren, erstellen Sie eine neue Sicherheitsgruppe oder aktualisieren eine vorhandene Sicherheitsgruppe und fügen eine Regel hinzu, um eingehenden Datenverkehr für diesen Zweck zu erlauben. Sicherheitsgruppen fungieren als Firewall für zugeordnet Instances. Sie steuern den ein- und ausgehenden Datenverkehr auf der Instance-Ebene. Nachdem Sie Ihre Sicherheitsgruppe erstellt oder aktualisiert haben, können Ihre Benutzer und andere PuTTY oder andere Terminals verwenden, um eine Verbindung von ihren Geräten zu Ihrem Amazon Linux herzustellen WorkSpaces. Weitere Informationen finden Sie unter the section called “Sicherheitsgruppen”.

Ein Video-Tutorial finden Sie unter Wie kann ich WorkSpaces über SSH eine Verbindung zu meinem Linux-Amazon herstellen? im - AWS Wissenscenter.

Inhalt

Voraussetzungen für SSH-Verbindungen zu Amazon Linux WorkSpaces

- Aktivieren von eingehendem SSH-Datenverkehr zu einem WorkSpace – Um eine Regel hinzuzufügen, die eingehenden SSH-Datenverkehr zu einer oder mehreren Amazon Linux-zulässt WorkSpaces, stellen Sie sicher, dass Sie über die öffentlichen oder privaten IP-Adressen der Geräte verfügen, die SSH-Verbindungen zu Ihrem benötigen WorkSpaces. Sie können beispielsweise die öffentlichen IP-Adressen von Geräten außerhalb Ihrer Virtual Private Cloud (VPC) oder die private IP-Adresse einer anderen EC2-Instance in derselben VPC wie Ihr angeben WorkSpace.

Wenn Sie eine Verbindung zu einem WorkSpace von Ihrem lokalen Gerät aus herstellen möchten, können Sie die Suchphrase „Was ist meine IP-Adresse“ in einem Internetbrowser verwenden oder den folgenden Service verwenden: Check IP .

- Herstellen einer Verbindung mit einem WorkSpace – Die folgenden Informationen sind erforderlich, um eine SSH-Verbindung von einem Gerät zu einem Amazon Linux- herzustellen WorkSpace.
  - Der NetBIOS-Name der Active Directory-Domain, mit der Sie verbunden sind.
  - Ihr WorkSpace Benutzername.
  - Die öffentliche oder private IP-Adresse des WorkSpace , mit dem Sie eine Verbindung herstellen möchten.

    Privat: Wenn Ihre VPC mit einem Unternehmensnetzwerk verbunden ist und Sie Zugriff auf dieses Netzwerk haben, können Sie die private IP-Adresse des angeben WorkSpace.

    Öffentlich: Wenn Ihr über eine öffentliche IP-Adresse WorkSpace verfügt, können Sie die WorkSpaces Konsole verwenden, um die öffentliche IP-Adresse zu finden, wie im folgenden Verfahren beschrieben.

So finden Sie die IP-Adressen für Amazon Linux, mit dem WorkSpace Sie eine Verbindung herstellen möchten, und Ihren Benutzernamen

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie in der Liste von die aus WorkSpaces, für WorkSpace die Sie SSH-Verbindungen aktivieren möchten.
4. Vergewissern Sie sich in der Spalte Ausführungsmodus, dass der WorkSpace Status Verfügbar lautet.
5. Klicken Sie auf den Pfeil links neben dem WorkSpace Namen, um die Inline-Zusammenfassung anzuzeigen, und notieren Sie sich die folgenden Informationen:

   - Die WorkSpace IP . Dies ist die private IP-Adresse des WorkSpace.

     Die private IP-Adresse ist erforderlich, um die Elastic Network-Schnittstelle zu erhalten, die dem zugeordnet ist WorkSpace. Die Netzwerkschnittstelle ist erforderlich, um Informationen wie die Sicherheitsgruppe oder die öffentliche IP-Adresse abzurufen, die dem zugeordnet ist WorkSpace.

- Der WorkSpace Benutzername . Dies ist der Benutzername, den Sie für die Verbindung mit dem angeben WorkSpace.

6. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
7. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
8. Geben Sie in das Suchfeld die WorkSpace IP ein, die Sie in Schritt 5 notiert haben.
9. Wählen Sie die Netzwerkschnittstelle aus, die der WorkSpace IP zugeordnet ist.
10. Wenn Ihr über eine öffentliche IP-Adresse WorkSpace verfügt, wird diese in der Spalte IPv4 Public IP angezeigt. Notieren Sie sich ggf. diese Adresse.

Um den NetBIOS-Namen der Active Directory-Domain herauszufinden, mit der Sie verbunden sind

1. Öffnen Sie die - AWS Directory Service Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Klicken Sie in der Liste der Verzeichnisse auf den Verzeichnis-ID-Link des Verzeichnisses für die WorkSpace.
3. Notieren Sie im Abschnitt Directory details (Verzeichnisdetails) den Directory NetBIOS name (NetBIOS-Name des Verzeichnisses).

Aktivieren von SSH-Verbindungen zu allen Amazon Linux WorkSpaces in einem Verzeichnis

Gehen Sie wie folgt vor, um SSH-Verbindungen zu allen Amazon Linux WorkSpaces in einem Verzeichnis zu aktivieren.

So erstellen Sie eine Sicherheitsgruppe mit einer Regel, die eingehenden SSH-Datenverkehr zu allen Amazon Linux WorkSpaces in einem Verzeichnis zulässt

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie Sicherheitsgruppen erstellen aus.
4. Geben Sie einen Namen und optional eine Beschreibung für Ihre Sicherheitsgruppe ein.
5. Wählen Sie für VPC die VPC aus, die die enthält WorkSpaces , für die Sie SSH-Verbindungen aktivieren möchten.

6. Wählen Sie auf der Registerkarte Eingehend Add Rule (Regel hinzufügen) und gehen Sie wie folgt vor:

   - Wählen Sie unter Typ die Option SSH aus.
   - Für Protokoll wird TCP automatisch angegeben, wenn Sie die Option SSH wählen.
   - Für Port Range (Portbereich) wird 22 automatisch angegeben, wenn Sie die Option SSH wählen.
   - Geben Sie für Quelle den CIDR-Bereich der öffentlichen IP-Adressen für die Computer an, mit denen Benutzer eine Verbindung zu ihrem herstellen. WorkSpaces Zum Beispiel ein Unternehmensnetzwerk oder ein Heimnetzwerk.
   - Geben Sie unter Description (Beschreibung) (optional) eine Beschreibung für die Regel ein.

7. Wählen Sie Erstellen.

Passwortbasierte Authentifizierung in Amazon Linux 2 WorkSpaces

Amazon Linux 2 WorkSpaces , die vor dem 10. November 2023 veröffentlicht wurden, sind standardmäßig für die SSH-Passwortauthentifizierung aktiviert. Für Amazon Linux 2 WorkSpaces , das nach dem 10. November gestartet wurde. ist die SSH-Passwortauthentifizierung standardmäßig deaktiviert.

So deaktivieren Sie die Passwortauthentifizierung in vorhandenen Amazon Linux 2 WorkSpaces Instances

1. Starten Sie den WorkSpaces Client und melden Sie sich bei Ihrem an WorkSpace.
2. Öffnen Sie das Terminalfenster (Anwendungen > Systemtools > MATE-Terminal).
3. Führen Sie den folgenden Befehl im Terminalfenster aus.

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

So aktivieren Sie die Passwortauthentifizierung in neu erstellten Amazon Linux 2 WorkSpaces Instances

1. Starten Sie den WorkSpaces Client und melden Sie sich bei Ihrem an WorkSpace.
2. Öffnen Sie das Terminalfenster (Anwendungen > Systemtools > MATE-Terminal).
3. Führen Sie den folgenden Befehl im Terminalfenster aus.

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

Im Gegensatz zu Ubuntu behält WorkSpacesAmazon Linux 2 WorkSpaces standardmäßig keine SSH-Passwortauthentifizierungseinstellungen in benutzerdefinierten Images bei. Wenn Sie die standardmäßige SSH-Passwortauthentifizierung in Amazon Linux 2 aktivieren möchten, das aus einem benutzerdefinierten Image WorkSpaces bereitgestellt wird, müssen Sie zusätzlich zur Aktivierung der Passwortauthentifizierung auch die `/etc/cloud/cloud.cfg` Datei ändern, um die Zeile zu entfernen, die `ssh_pwauth` beim Erstellen eines benutzerdefinierten Images enthält. Führen Sie den folgenden Befehl aus, um die `/etc/cloud/cloud.cfg`-Datei zu ändern:

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

Aktivieren von SSH-Verbindungen zu einem bestimmten Amazon Linux WorkSpace

Gehen Sie wie folgt vor WorkSpace, um SSH-Verbindungen zu einer bestimmten Amazon Linux- zu aktivieren.

So fügen Sie eine Regel zu einer vorhandenen Sicherheitsgruppe hinzu, um eingehenden SSH-Datenverkehr zu einem bestimmten Amazon Linux zuzulassen WorkSpace

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich unter Network & Security (Netzwerk und Sicherheit) auf Network Interfaces (Netzwerkschnittstellen).
3. Geben Sie in der Suchleiste die private IP-Adresse des ein WorkSpace , für den Sie SSH-Verbindungen aktivieren möchten.
4. Klicken Sie in der Spalte Security groups (Sicherheitsgruppen) auf den Link für die Sicherheitsgruppe.
5. Klicken Sie auf die Registerkarte Inbound und wählen Sie Edit aus.
6. Wählen Sie Add Rule (Regel hinzufügen) und gehen Sie wie folgt vor:
   - Wählen Sie unter Typ die Option SSH aus.
   - Für Protokoll wird TCP automatisch angegeben, wenn Sie die Option SSH wählen.

- Für Port Range (Portbereich) wird 22 automatisch angegeben, wenn Sie die Option SSH wählen.
- Wählen Sie für Quelle My IP (Meine IP) oder Benutzerdefiniert und geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich in CIDR-Notation an. Wenn zum Beispiel Ihre IPv4-Adresse `203.0.113.25` lautet, geben Sie `203.0.113.25/32` ein, um diese einzelne IPv4-Adresse in CIDR-Notation aufzuführen. Wenn Ihr Unternehmen Adressen aus einem Bereich zuweist, geben Sie den gesamten Bereich an, z. B. `203.0.113.0/24`.
- Geben Sie unter Description (Beschreibung) (optional) eine Beschreibung für die Regel ein.

7. Wählen Sie Speichern.

Herstellen einer Verbindung mit einem Amazon Linux WorkSpace über Linux oder PuTTY

Nachdem Sie Ihre Sicherheitsgruppe erstellt oder aktualisiert und die erforderliche Regel hinzugefügt haben, können Ihre Benutzer und andere Linux oder PuTTY verwenden, um eine Verbindung von ihren Geräten zu Ihrem herzustellen WorkSpaces.

> **Note**
>
> Vor dem Abschließen von einem der folgenden Verfahren stellen Sie sicher, dass Sie Folgendes haben:
>
> - Der NetBIOS-Name der Active Directory-Domain, mit der Sie verbunden sind.
> - Der Benutzername, den Sie verwenden, um eine Verbindung mit dem herzustellen WorkSpace.
> - Die öffentliche oder private IP-Adresse des WorkSpace , mit dem Sie eine Verbindung herstellen möchten.
>
> Anweisungen zum Abrufen dieser Informationen finden Sie unter „Voraussetzungen für SSH-Verbindungen zu Amazon Linux WorkSpaces“ weiter oben in diesem Thema.

Herstellen einer Verbindung mit einem Amazon Linux WorkSpace über Linux

1. Öffnen Sie die Eingabeaufforderung als Administrator und geben Sie den folgenden Befehl ein. Geben Sie für *NetBIOS-Name, Benutzername* und *WorkSpace IP* die entsprechenden Werte ein.

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

   Nachstehend finden Sie ein Beispiel für den SSH-Befehl, bei dem:

   - Der *NetBIOS_NAME* „anycompany“ lautet
   - Der *Benutzername* „janedoe“ lautet
   - Die *WorkSpace IP* ist 203.0.113.25

   ```
   ssh "anycompany\janedoe"@203.0.113.25
   ```

2. Wenn Sie dazu aufgefordert werden, geben Sie dasselbe Passwort ein, das Sie bei der Authentifizierung beim WorkSpaces Client verwenden (Ihr Active-Directory-Passwort).

So stellen Sie eine Verbindung zu einem Amazon Linux WorkSpace mithilfe von PuTTY her

1. Öffnen Sie PuTTY.
2. Führen Sie im Dialogfeld PuTTY Configuration (PuTTY-Konfiguration) die folgenden Schritte aus:

   - Geben Sie unter Host Name (or IP address) (Hostname (oder IP-Adresse)) den folgenden Befehl ein. Ersetzen Sie die Werte durch den NetBIOS-Namen der Active-Directory-Domain, mit der Sie verbunden sind, den Benutzernamen, den Sie für die Verbindung mit dem verwenden WorkSpace, und die IP-Adresse des WorkSpace , mit dem Sie eine Verbindung herstellen möchten.

     ```
     NetBIOS_NAME\Username@WorkSpaceIP
     ```

   - Geben Sie im Feld Port **22** ein.
   - Wählen Sie für Connection type (Verbindungstyp) den Eintrag SSH.

   Ein Beispiel des SSH-Befehls finden Sie unter Schritt 1 im vorherigen Verfahren.

3. Klicken Sie auf Open.
4. Wenn Sie dazu aufgefordert werden, geben Sie dasselbe Passwort ein, das Sie bei der Authentifizierung beim WorkSpaces Client verwenden (Ihr Active-Directory-Passwort).

Erforderliche Konfigurations- und Servicekomponenten für WorkSpaces

Als WorkSpace Administrator müssen Sie Folgendes über die erforderlichen Konfigurations- und Servicekomponenten verstehen.

- the section called “Erforderliche Routing-Tabellen-Konfiguration”
- the section called “Komponenten für Windows”
- the section called “Komponenten für Linux”
- the section called “Komponenten für Ubuntu”

Erforderliche Routing-Tabellen-Konfiguration

Wir empfehlen, die Routing-Tabelle auf Betriebssystemebene für ein nicht zu ändern WorkSpace. Der WorkSpaces Service erfordert die vorkonfigurierten Routen in dieser Tabelle, um den Systemstatus zu überwachen und Systemkomponenten zu aktualisieren. Wenn für Ihre Organisation Änderungen an der Routing-Tabelle erforderlich sind, wenden Sie sich an den AWS-Support oder Ihr AWS-Account-Team, bevor die Änderungen übernommen werden.

Erforderliche Servicekomponenten für Windows

Unter Windows werden WorkSpacesdie Servicekomponenten an den folgenden Speicherorten installiert. Diese Objekte dürfen nicht gelöscht, geändert, blockiert oder isoliert werden. Wenn Sie dies tun, funktioniert die WorkSpace nicht richtig.

Wenn Antivirensoftware auf der installiert ist WorkSpace, stellen Sie sicher, dass sie die an den folgenden Speicherorten installierten Servicekomponenten nicht beeinträchtigt.

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`

- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

32-Bit-PCoIP-Agent

Am 29. März 2021 haben wir den PCoIP-Agent von 32-Bit auf 64-Bit aktualisiert. Für Windows WorkSpaces , die das PCoIP-Protokoll verwenden, bedeutet dies, dass sich der Speicherort der Teradici-Dateien von `C:\Program Files (x86)\Teradici` in geändert hat`C:\Program Files \Teradici`. Da wir PCoIP-Agenten während regulärer Wartungsfenster aktualisiert haben, haben einige Ihrer den 32-Bit-Agenten während der Umstellung WorkSpaces möglicherweise länger verwendet als andere.

Wenn Sie Firewallregeln, Ausnahmen von Antivirensoftware (auf der Client- und Hostseite), Einstellungen für Gruppenrichtlinienobjekte (GPO) oder Einstellungen für Microsoft System Center Configuration Manager (SCCM), Microsoft Endpoint Configuration Manager oder ähnliche Konfigurationsverwaltungstools konfiguriert haben, die auf dem vollständigen Pfad zum 32-Bit-Agent basieren, müssen Sie diesen Einstellungen auch den vollständigen Pfad zum 64-Bit-Agent hinzufügen.

Wenn Sie nach den Pfaden zu 32-Bit-PCoIP-Komponenten filtern, achten Sie darauf, die Pfade zu den 64-Bit-Versionen der Komponenten hinzuzufügen. Da Ihre WorkSpaces möglicherweise nicht alle gleichzeitig aktualisiert werden, ersetzen Sie den 32-Bit-Pfad nicht durch den 64-Bit-Pfad, da andere Ihrer WorkSpaces möglicherweise nicht funktionieren. Wenn Sie beispielsweise für Ihre Ausschlüsse oder Kommunikationsfilter `C:\Program Files (x86)\Teradici\PCoIP Agent \bin\pcoip_server_win32.exe` als Grundlage verwenden, müssen Sie auch `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe` hinzufügen. Wenn Sie für Ihre Ausschlüsse oder Kommunikationsfilter `C:\Program Files (x86)\Teradici\PCoIP Agent \bin\pcoip_agent.exe` als Grundlage verwenden, müssen Sie auch `C:\Program Files \Teradici\PCoIP Agent\bin\pcoip_agent.exe` hinzufügen.

Änderung des PCoIP-Arbiter-Service – Beachten Sie, dass der PCoIP-Arbiter-Service (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) entfernt wird, wenn Ihr aktualisiert WorkSpaces wird, um den 64-Bit-Agent zu verwenden.

PCoIP-Zero-Clients und USB-Geräte – Ab Version 20.10.4 des PCoIP-Agenten WorkSpaces deaktiviert Amazon die USB-Umleitung standardmäßig über die Windows-Registrierung. Diese Registrierungseinstellung wirkt sich auf das Verhalten von USB-Kabeln aus, wenn Ihre Benutzer

PCoIP-Zero-Client-Geräte verwenden, um eine Verbindung zu ihrem herzustellen WorkSpaces. Weitere Informationen finden Sie unter USB-Drucker und andere USB-Peripheriegeräte funktionieren nicht für PCoIP-Zero-Clients.

Erforderliche Servicekomponenten

Auf Amazon Linux werden WorkSpacesdie Servicekomponenten an den folgenden Speicherorten installiert. Diese Objekte dürfen nicht gelöscht, geändert, blockiert oder isoliert werden. Wenn Sie dies tun, funktioniert die WorkSpace nicht richtig.

> **Note**
>
> Das Vornehmen von Änderungen an anderen Dateien als `/etc/pcoip-agent/pcoip-agent.conf` kann dazu führen WorkSpaces , dass Ihr nicht mehr funktioniert und Sie sie möglicherweise neu erstellen müssen. Informationen über das Ändern von `/etc/pcoip-agent/pcoip-agent.conf` finden Sie unter Verwalten von Amazon Linux WorkSpaces.

- `/etc/dhcp/dhclient.conf`
- `/etc/logrotate.d/pcoip-agent`
- `/etc/logrotate.d/pcoip-server`
- `/etc/os-release`
- `/etc/pam.d/pcoip`
- `/etc/pam.d/pcoip-session`
- `/etc/pcoip-agent`
- `/etc/profile.d/system-restart-check.sh`
- `/etc/X11/default-display-manager`
- `/etc/yum/pluginconf.d/halt_os_update_check.conf`
- `/lib/systemd/system/pcoip.service`
- `/lib/systemd/system/pcoip-agent.service`
- `/lib64/security/pam_self.so`
- `/usr/bin/pcoip-fne-view-license`
- `/usr/bin/pcoip-list-licenses`
- `/usr/bin/pcoip-validate-license`

- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp

Erforderliche Servicekomponenten für Ubuntu

Auf Ubuntu werden WorkSpacesdie Servicekomponenten an den folgenden Speicherorten installiert. Diese Objekte dürfen nicht gelöscht, geändert, blockiert oder isoliert werden. Wenn Sie dies tun, funktioniert die WorkSpace nicht richtig.

- /etc/X11/default-display-manager
- /etc/X11/xorg.conf
- /etc/dcv

- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp
- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/share/X11
- /var/lib/skylight
- /var/log/skylight

Verwalten von Verzeichnissen für WorkSpaces

WorkSpaces verwendet ein Verzeichnis zum Speichern und Verwalten von Informationen für Ihre WorkSpaces und Benutzer. Verwenden Sie eine der folgenden Optionen:

- AD Connector – Verwenden Sie Ihr vorhandenes on-premises Microsoft Active Directory. Benutzer können sich mit ihren lokalen Anmeldeinformationen bei ihren WorkSpaces anmelden und von dort aus auf on-premises Ressourcen zugreifen.
- AWS Managed Microsoft AD – Erstellen Sie ein auf AWS gehostetes Microsoft Active Directory.
- Simple AD – Erstellen Sie ein Verzeichnis, das mit Microsoft Active Directory kompatibel ist, das über Samba 4 verfügt und das auf AWS gehostet wird.
- Gegenseitiges Vertrauen – Stellen Sie eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD-Verzeichnis und Ihrer On-Premises-Domain her.

Tutorials, die zeigen, wie Sie diese Verzeichnisse einrichten und WorkSpaces starten, finden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

> **Tip**
>
> Eine ausführliche Erläuterung der Überlegungen zum Design von Verzeichnissen und Virtual Private Clouds (VPC) für verschiedene Bereitstellungsszenarien finden Sie unter Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces.

Nach dem Erstellen eines Verzeichnisses führen Sie den Großteil der Verwaltungsaufgaben für das Verzeichnis über Tools wie beispielsweise die Active-Directory-Verwaltungstools aus. Manche Verwaltungsaufgaben für das Verzeichnis können Sie über die WorkSpaces-Konsole ausführen, andere über die Gruppenrichtlinie. Weitere Informationen zum Verwalten von Benutzern und Gruppen finden Sie unter Verwalten von WorkSpaces-Benutzern und Einrichten der Active-Directory-Verwaltungstools für WorkSpaces.

> **Note**
>
> - Derzeit werden keine freigegebenen Verzeichnisse mit Amazon WorkSpaces unterstützt.
> - Wenn Sie Ihr von AWS verwaltetes Microsoft-AD-Verzeichnis für die Replikation in mehreren Regionen konfigurieren, kann nur das Verzeichnis in der primären Region für

die Verwendung mit Amazon WorkSpaces registriert werden. Versuche, das Verzeichnis in einer replizierten Region für die Verwendung mit Amazon WorkSpaces zu registrieren, schlagen fehl. Die regionsübergreifende Replikation mit von AWS verwaltetem Microsoft AD wird für die Verwendung mit Amazon WorkSpaces innerhalb replizierter Regionen nicht unterstützt.

- Simple AD und AD Connector werden Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem AD-Connector-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.

  Informationen zum Löschen leerer Verzeichnisse finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces. Wenn Sie Ihr Simple-AD- oder AD-Connector-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

Inhalt

Registrieren eines dedizierten Verzeichnisses für WorkSpaces

Damit WorkSpaces ein vorhandenes AWS Directory Service-Verzeichnis verwenden kann, müssen Sie es bei WorkSpaces registrieren. Nach dem Registrieren eines Verzeichnisses können Sie WorkSpaces im Verzeichnis starten.

Voraussetzungen

Ein Verzeichnis muss die folgenden Anforderungen erfüllen, um es für die Verwendung mit WorkSpaces zu registrieren:

- Wenn Sie AWS Managed Microsoft AD oder Simple AD verwenden, kann sich Ihr Verzeichnis in einem dedizierten privaten Subnetz befinden, sofern das Verzeichnis Zugriff auf die VPC hat, in der sich die WorkSpaces befinden.

Weitere Informationen zum Verzeichnis- und VPC-Design finden Sie im Whitepaper Best Practices for Deployment Amazon WorkSpaces.

> **Note**
>
> Simple AD und AD Connector werden Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem AD-Connector-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.
> Informationen zum Löschen leerer Verzeichnisse finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces. Wenn Sie Ihr Simple-AD- oder AD-Connector-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

So registrieren Sie ein Verzeichnis

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis aus.
4. Wählen Sie Actions, Register aus.

> **Note**
>
> - Derzeit werden keine freigegebenen Verzeichnisse mit Amazon WorkSpaces unterstützt.
> - Wenn Ihr von AWS Managed Microsoft AD verwaltetes Verzeichnis für die Replikation in mehreren Regionen konfiguriert ist, kann nur das Verzeichnis in der primären Region für die Verwendung mit Amazon WorkSpaces registriert werden. Versuche, das Verzeichnis in einer replizierten Region für die Verwendung mit Amazon WorkSpaces zu registrieren, schlagen fehl. Die regionsübergreifende Replikation

mit AWS Managed Microsoft AD wird für die Verwendung mit Amazon WorkSpaces innerhalb replizierter Regionen nicht unterstützt.

5. Wählen Sie zwei Subnetze Ihrer VPC aus, die sich nicht in derselben Availability Zone befinden. Diese Subnetze werden verwendet, um Ihre WorkSpaces zu starten. Weitere Informationen finden Sie unter Availability Zones für Amazon WorkSpaces.

> **Note**
>
> Wenn Sie nicht wissen, welche Subnetze Sie auswählen sollen, wählen Sie Keine Präferenz aus.

6. Legen Sie für Enable Self Service Permissions (Self-Service-Berechtigungen aktivieren) den Wert Ja fest, um Ihren Benutzern zu ermöglichen, ihre WorkSpaces neu zu erstellen sowie die Volume-Größe, den Datenverarbeitungstyp und den Ausführungsmodus zu ändern. Die Aktivierung beeinflusst möglicherweise Ihre Kosten für Amazon WorkSpaces. Wählen Sie andernfalls Nein aus.
7. Wählen Sie für Amazon WorkDocs aktivieren die Option Ja aus, um das Verzeichnis zur Verwendung mit Amazon WorkDocs zu registrieren. Wählen Sie andernfalls Nein aus.

> **Note**
>
> Diese Option wird nur angezeigt, wenn in der Region Amazon WorkDocs verfügbar ist und Sie nicht AWS Managed Microsoft AD verwenden. Wenn Sie AWS Managed Microsoft AD verwenden, schließen Sie die Registrierung Ihres Verzeichnisses ab und lesen Sie dann Aktivieren von Amazon WorkDocs für AWS Managed Microsoft AD.

8. Wählen Sie Register aus. Zunächst lautet der Wert für Registered `REGISTERING`. Nach der Registrierung lautet der Wert `Yes`.

Wenn Sie das Verzeichnis nicht mehr mit WorkSpaces verwenden, können Sie die Registrierung aufheben. Beachten Sie, dass Sie ein Verzeichnis abmelden müssen, bevor Sie es löschen können. Wenn Sie ein Verzeichnis abmelden und löschen möchten, müssen Sie zuerst alle Anwendungen und Services finden und entfernen, die für das Verzeichnis registriert sind. Weitere Informationen finden Sie unter Löschen Ihres Verzeichnisses im AWS Directory Service-Administratorhandbuch.

So melden Sie ein Verzeichnis ab

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis aus.
4. Wählen Sie Actions, Deregister aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Deregister aus. Nach Abschluss der Abmeldung lautet der Wert für Registered No.

Aktualisieren der Verzeichnisdetails für Ihr WorkSpaces

Sie können die folgenden Verzeichnisverwaltungsaufgaben mit der WorkSpaces Konsole ausführen.

Aufgaben

- Auswählen einer Organisationseinheit
- Konfigurieren automatischer öffentlicher IP-Adressen
- Kontrollieren des Gerätezugriffs
- Verwalten lokaler Administratorberechtigungen
- Aktualisieren des AD Connector-Kontos (AD Connector)
- Multi-Faktor-Authentifizierung (AD Connector)

Auswählen einer Organisationseinheit

WorkSpace -Computerkonten werden in der Standardorganisationseinheit (OU) für das WorkSpaces Verzeichnis platziert. Zunächst befinden sich die Computerkonten in der Computer-Organisationseinheit Ihres Verzeichnisses bzw. des Verzeichnisses, mit dem Ihr AD Connector verbunden ist. Sie können eine andere Organisationseinheit aus Ihrem Verzeichnis bzw. dem verbundenen Verzeichnis auswählen, oder eine Organisationseinheit in einer separaten Zieldomäne angeben. Beachten Sie, dass Sie pro Verzeichnis nur eine Organisationseinheit auswählen können.

Nachdem Sie eine neue Organisationseinheit ausgewählt haben, werden die Maschinenkonten für alle WorkSpaces erstellten oder neu erstellten Organisationseinheiten in der neu ausgewählten Organisationseinheit platziert.

So wählen Sie eine Organisationseinheit aus

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Ihr Verzeichnis aus.
4. Wählen Sie unter Zieldomäne und Organisationseinheit die Option Bearbeiten aus.
5. Um eine Organisationseinheit zu finden, können Sie unter Ziel und Organisationseinheit mit der Eingabe des Organisationseinheitsnamens ganz oder teilweise beginnen und die Organisationseinheit auswählen, die Sie verwenden möchten.
6. (Optional) Wählen Sie einen OU-getrennten Namen aus, um Ihre ausgewählte OU mit einer benutzerdefinierten OU zu überschreiben.
7. Wählen Sie Speichern.
8. (Optional) Erstellen Sie das vorhandene neu WorkSpaces , um die Organisationseinheit zu aktualisieren. Weitere Informationen finden Sie unter Neuerstellen eines WorkSpace.

Konfigurieren automatischer öffentlicher IP-Adressen

Nachdem Sie die automatische Zuweisung öffentlicher IP-Adressen aktiviert haben, wird jedem , den Sie starten WorkSpace , eine öffentliche IP-Adresse aus dem von Amazon bereitgestellten Pool öffentlicher Adressen zugewiesen. Ein WorkSpace in einem öffentlichen Subnetz kann über das Internet-Gateway auf das Internet zugreifen, wenn er über eine öffentliche IP-Adresse verfügt. WorkSpaces , die bereits vorhanden sind, bevor Sie die automatische Zuweisung aktivieren, erhält keine öffentlichen Adressen, bis Sie sie neu erstellen.

Beachten Sie, dass Sie die automatische Zuweisung öffentlicher Adressen nicht aktivieren müssen, wenn sich Ihr in privaten Subnetzen WorkSpaces befindet und Sie ein NAT-Gateway für die Virtual Private Cloud (VPC) konfiguriert haben oder wenn sich Ihr in öffentlichen Subnetzen WorkSpaces befindet und Sie ihm Elastic IP-Adressen zugewiesen haben. Weitere Informationen finden Sie unter Konfigurieren einer VPC für WorkSpaces.

> **Warning**
>
> Wenn Sie eine Elastic IP-Adresse, die Sie besitzen WorkSpace, einem zuordnen und diese Elastic IP-Adresse später von der trennen WorkSpace, WorkSpace verliert die ihre öffentliche IP-Adresse und erhält nicht automatisch eine neue aus dem von Amazon bereitgestellten Pool. Um eine neue öffentliche IP-Adresse aus dem von Amazon bereitgestellten Pool mit

dem zu verknüpfen WorkSpace, müssen Sie das neu erstellen WorkSpace. Wenn Sie die nicht neu erstellen möchten WorkSpace, müssen Sie dem eine andere Elastic IP-Adresse zuordnen, die Sie besitzen WorkSpace.

So konfigurieren Sie Elastic IP-Adressen

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis für Ihr aus WorkSpaces.
4. Wählen Sie Actions, Update Details aus.
5. Erweitern Sie Access to Internet und wählen Sie Enable oder Disable aus.
6. Wählen Sie Aktualisieren.

Kontrollieren des Gerätezugriffs

Sie können die Gerätetypen angeben, die Zugriff auf haben WorkSpaces. Darüber hinaus können Sie den Zugriff auf WorkSpaces vertrauenswürdige Geräte (auch als verwaltete Geräte bezeichnet) einschränken.

So steuern Sie den Gerätezugriff auf WorkSpaces

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Ihr Verzeichnis aus.
4. Wählen Sie unter Optionen für die Zugriffskontrolle die Option Bearbeiten aus.
5. Geben Sie unter Vertrauenswürdige Geräte an, auf welche Gerätetypen zugegriffen werden kann, WorkSpaces indem Sie entweder Alle zulassen, Vertrauenswürdige Geräte oder Alle verweigern auswählen. Weitere Informationen finden Sie unter Beschränken des WorkSpaces Zugriffs auf vertrauenswürdige Geräte.
6. Wählen Sie Save (Speichern) aus.

Verwalten lokaler Administratorberechtigungen

Sie können angeben, ob Benutzer lokale Administratoren auf ihrem sind WorkSpaces, wodurch sie die Anwendung installieren und Einstellungen auf ihrem ändern können WorkSpaces. Benutzer sind standardmäßig lokale Administratoren. Wenn Sie diese Einstellung ändern, gilt die Änderung für alle neuen , WorkSpaces die Sie erstellen, und alle WorkSpaces , die Sie neu erstellen.

So ändern Sie die lokalen Administratorberechtigungen

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Ihr Verzeichnis aus.
4. Wählen Sie unter Lokale Administratoreinstellungen die Option Bearbeiten aus.
5. Um sicherzustellen, dass Benutzer lokale Administratoren sind, wählen Sie Lokale Administratoreinstellung aktivieren aus.
6. Wählen Sie Speichern.

Aktualisieren des AD Connector-Kontos (AD Connector)

Sie können das AD-Connector-Konto aktualisieren, das zum Lesen von Benutzern und Gruppen und zum Verbinden von WorkSpaces Maschinenkonten mit Ihrem AD-Connector-Verzeichnis verwendet wird.

So aktualisieren Sie das AD Connector-Konto

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Ihr Verzeichnis und dann Details anzeigen aus.
4. Wählen Sie unter AD-Konnektor-Konto die Option Bearbeiten aus.
5. Geben Sie die Anmeldeinformationen für das neue Konto ein.
6. Wählen Sie Speichern.

Multi-Faktor-Authentifizierung (AD Connector)

Sie können für Ihr AD-Connector-Verzeichnis die Multi-Faktor-Authentifizierung aktivieren. Weitere Informationen zur Verwendung der Multi-Faktor-Authentifizierung mit AWS Directory Service

finden Sie unter Multi-Faktor-Authentifizierung für AD Connector aktivieren und AD-Connector-Voraussetzungen.

> **Note**
>
> - Ihr RADIUS-Server kann entweder von AWS oder on-premises gehostet werden.
> - Die Benutzernamen müssen zwischen Active Directory und Ihrem RADIUS-Server übereinstimmen.

So aktivieren Sie die Multi-Factor Authentication

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Ihr Verzeichnis und anschließend Actions, Update Details aus.
4. Erweitern Sie Multi-Factor Authentication und wählen Sie Enable Multi-Factor Authentication aus.
5. Geben Sie unter RADIUS server IP address(es) die IP-Adressen Ihrer RADIUS-Server-Endpunkte getrennt durch Kommas oder die IP-Adresse Ihres RADIUS-Server-Load Balancers ein.
6. Geben Sie unter Port den Port ein, den Ihr RADIUS-Server für die Kommunikation verwendet. Ihr On-Premises-Netzwerk muss eingehenden Datenverkehr über den Standard-RADIUS-Server-Port (UDP 1812) von AD Connector zulassen.
7. Geben Sie unter Shared secret code und Confirm shared secret code den gemeinsamen geheimen Code für Ihren RADIUS-Server ein.
8. Wählen Sie für Protocol das Protokoll für Ihren RADIUS-Server aus.
9. Geben Sie unter Server timeout die Zeit in Sekunden ein, die auf eine Antwort des RADIUS-Servers gewartet wird. Dieser Wert muss zwischen 1 und 50 liegen.
10. Geben Sie unter Max retries die Anzahl der Kommunikationsversuche mit dem RADIUS-Server ein. Dieser Wert muss zwischen 0 und 10 liegen.
11. Wählen Sie Update and Exit aus.

Die Multi-Faktor-Authentifizierung ist verfügbar, wenn für RADIUS status die Option Enabled ausgewählt ist. Während die Multi-Faktor-Authentifizierung eingerichtet wird, können sich Benutzer nicht bei ihrem anmelden WorkSpaces.

Aktualisieren von DNS-Servern für Amazon WorkSpaces

Wenn Sie nach dem Start Ihrer WorkSpaces die DNS-Server-IP-Adressen für Ihr Active Directory aktualisieren müssen, müssen Sie auch Ihre WorkSpaces mit den neuen DNS-Servereinstellungen aktualisieren.

Sie können Ihre WorkSpaces auf eine der folgenden Arten mit den neuen DNS-Einstellungen aktualisieren:

- Aktualisieren Sie die DNS-Einstellungen in den WorkSpaces, bevor Sie die DNS-Einstellungen für Active Directory aktualisieren.
- Erstellen Sie die WorkSpaces neu, nachdem Sie die DNS-Einstellungen für Active Directory aktualisiert haben.

Wir empfehlen, die DNS-Einstellungen in den WorkSpaces zu aktualisieren, bevor Sie die DNS-Einstellungen in Active Directory aktualisieren (wie in Schritt 1 des folgenden Verfahrens erklärt).

Wenn Sie stattdessen die WorkSpaces neu erstellen möchten, aktualisieren Sie eine der DNS-Server-IP-Adressen in Ihrem Active Directory (Schritt 2) und folgen Sie dann dem Verfahren unter Neuerstellen eines WorkSpace, um Ihre WorkSpaces neu zu erstellen. Nachdem Sie Ihre WorkSpaces neu erstellt haben, folgen Sie dem Verfahren in Schritt 3, um Ihre DNS-Serverupdates zu testen. Nachdem Sie diesen Schritt abgeschlossen haben, aktualisieren Sie die IP-Adresse Ihres sekundären DNS-Servers in Active Directory. Erstellen Sie dann Ihre WorkSpaces erneut. Folgen Sie unbedingt dem Verfahren in Schritt 3, um das Update des sekundären DNS-Servers zu testen. Wie im Abschnitt Bewährte Methoden erwähnt, empfehlen wir, die IP-Adressen Ihrer DNS-Server nacheinander zu aktualisieren.

Bewährte Methoden

Wenn Sie Ihre DNS-Servereinstellungen aktualisieren, empfehlen wir die folgenden bewährten Methoden:

- Zur Vermeidung von Verbindungsabbrüchen und nicht verfügbaren Domain-Ressourcen, empfehlen wir dringend, DNS-Serverupdates außerhalb der Spitzenzeiten oder während eines geplanten Wartungszeitraums durchzuführen.
- Starten Sie in den 15 Minuten vor und in den 15 Minuten nach der Änderung Ihrer DNS-Servereinstellungen keine neuen WorkSpaces.

- Wenn Sie Ihre DNS-Servereinstellungen aktualisieren, ändern Sie jeweils eine DNS-Server-IP-Adresse. Stellen Sie sicher, dass das erste Update korrekt ist, bevor Sie die zweite IP-Adresse aktualisieren. Wir empfehlen, das folgende Verfahren (Schritt 1, Schritt 2 und Schritt 3) zweimal durchzuführen, um die IP-Adressen nacheinander zu aktualisieren.

Schritt 1: Aktualisieren der DNS-Servereinstellungen auf den WorkSpaces

Im folgenden Verfahren werden die aktuellen und neuen DNS-Server-IP-Adresswerte wie folgt bezeichnet:

- Aktuelle DNS-IP-Adressen: *OldIP1*, *OldIP2*
- Neue DNS-IP-Adressen: *NewIP1*, *NewIP2*

> **Note**
>
> Wenn Sie dieses Verfahren zum zweiten Mal durchführen, ersetzen Sie *OldIP1* durch *OldIP2* und *NewIP1* durch *NewIP2*.

Aktualisieren der DNS-Servereinstellungen für Windows-WorkSpaces

Wenn Sie über mehrere WorkSpaces verfügen, können Sie das folgende Registrierungsupdate für die WorkSpaces bereitstellen, indem Sie ein Gruppenrichtlinienobjekt (GPO) auf die Active-Directory-Organisationseinheit für Ihre WorkSpaces anwenden. Weitere Informationen zur Arbeit mit GPOs finden Sie unter Verwalte dein Windows WorkSpaces.

Sie können diese Updates entweder mithilfe des Registrierungseditors oder mithilfe von Windows PowerShell vornehmen. Beide Verfahren werden in diesem Abschnitt beschrieben.

So aktualisieren Sie die DNS-Registrierungseinstellungen mit dem Registrierungseditor

1. Öffnen Sie auf dem Windows-WorkSpace das Windows-Suchfeld und geben Sie **`registry editor`** ein, um den Registrierungs-Editor (regedit.exe) zu öffnen.
2. Wählen Sie auf die Frage „Möchten Sie dieser App erlauben, Änderungen an Ihrem Gerät vorzunehmen?“, Ja aus.
3. Navigieren Sie im Registrierungs-Editor zu folgendem Registrierungseintrag:

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\SkyLight

4. Öffnen Sie den DomainJoinDNS-Registrierungsschlüssel. Aktualisieren Sie *OldIP1* mit *NewIP1* und wählen Sie dann OK aus.
5. Schließen Sie den Registrierungs-Editor.
6. Starten Sie den WorkSpace neu oder starten Sie den Service SkylightWorkspaceConfigService neu.

   > **Note**
   >
   > Nachdem Sie den Service SkylightWorkspaceConfigService neu gestartet haben, kann es bis zu 1 Minute dauern, bis der Netzwerkadapter die Änderung wiedergibt.

7. Fahren Sie mit Schritt 2 fort und aktualisieren Sie Ihre DNS-Servereinstellungen in Active Directory, um *OldIP1* durch *NewIP1* zu ersetzen.

So aktualisieren Sie die DNS-Registrierungseinstellungen mit PowerShell

Das folgende Verfahren verwendet PowerShell-Befehle, um Ihre Registrierung zu aktualisieren und den Service SkylightWorkspaceConfigService neu zu starten.

1. Öffnen Sie auf dem Windows-WorkSpace das Windows-Suchfeld und geben Sie **`powershell`** ein. Wählen Sie Als Administrator ausführen aus.
2. Wählen Sie auf die Frage „Möchten Sie dieser App erlauben, Änderungen an Ihrem Gerät vorzunehmen?“, Ja aus.
3. Führen Sie im PowerShell-Fenster den folgenden Befehl aus, um die aktuellen DNS-Server-IP-Adressen abzurufen.

   ```
   Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
   ```

   Die Ausgabe sollte folgendermaßen aussehen.

   ```
   DomainJoinDns : OldIP1,OldIP2
   PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon\SkyLight
   PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon
   PSChildName   : SkyLight
   PSDrive       : HKLM
   ```

```
PSProvider    : Microsoft.PowerShell.Core\Registry
```

4. Führen Sie den folgenden Befehl in einem PowerShell-Fenster aus, um *OldIP1* zu *NewIP1* zu ändern. Stellen Sie sicher, dass Sie *OldIP2* vorerst so lassen.

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
 "NewIP1,OldIP2"
```

5. Führen Sie den folgenden Befehl aus, um den Service SkylightWorkspaceConfigService neu zu starten.

```
restart-service -Name SkyLightWorkspaceConfigService
```

> **Note**
>
> Nachdem Sie den Service SkylightWorkspaceConfigService neu gestartet haben, kann es bis zu 1 Minute dauern, bis der Netzwerkadapter die Änderung wiedergibt.

6. Fahren Sie mit Schritt 2 fort und aktualisieren Sie Ihre DNS-Servereinstellungen in Active Directory, um *OldIP1* durch *NewIP1* zu ersetzen.

Aktualisieren der DNS-Servereinstellungen für Linux-WorkSpaces

Wenn Sie mehr als einen Linux WorkSpace haben, empfehlen wir die Verwendung einer Konfigurationsmanagement-Lösung zur Verteilung und Durchsetzung von Richtlinien. Sie können beispielsweise AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise oder Ansible verwenden.

So aktualisieren Sie die DNS-Servereinstellungen für Linux-WorkSpaces

1. Öffnen Sie in Ihrem Linux-WorkSpace ein Terminalfenster (Anwendungen > Systemprogramme > MATE Terminal).
2. Entpacken Sie die Datei `/etc/dhcp/dhclient.conf` mit folgendem Linux-Befehl. Sie benötigen Root-Benutzerrechte, um diese Datei bearbeiten zu können. Verwenden Sie für Root-Rechte entweder den `sudo -i`-Befehl oder führen Sie wie dargestellt alle Befehle mit `sudo` aus.

```
sudo vi /etc/dhcp/dhclient.conf
```

In der `/etc/dhcp/dhclient.conf`-Datei sehen Sie den folgenden `prepend`-Befehl, wobei *`OldIP1`* und *`OldIP2`* die IP-Adressen Ihrer DNS-Server sind.

```
prepend domain-name-servers OldIP1, OldIP2; # skylight
```

3. Ersetzen Sie *`OldIP1`* durch *`NewIP1`* und lassen Sie *`OldIP2`* vorerst unverändert.
4. Speichern Sie Ihre Änderungen in `/etc/dhcp/dhclient.conf`.
5. Starten Sie den WorkSpace neu.
6. Fahren Sie mit Schritt 2 fort und aktualisieren Sie Ihre DNS-Servereinstellungen in Active Directory, um *`OldIP1`* durch *`NewIP1`* zu ersetzen.

Schritt 2: Aktualisieren der DNS-Servereinstellungen für Active Directory

In diesem Schritt aktualisieren Sie die DNS-Servereinstellungen für Active Directory. Wie im Abschnitt Bewährte Methoden erwähnt, empfehlen wir, die IP-Adressen Ihrer DNS-Server nacheinander zu aktualisieren.

Informationen zum Aktualisieren Ihrer DNS-Servereinstellungen für Active Directory finden Sie in der folgenden Dokumentation im AWS Directory Service-Administratorhandbuch:

- AD Connector: Aktualisieren der DNS-Adresse für AD Connector
- AWS Managed Microsoft AD: Konfigurieren der bedingte DNS-Weiterleitungen für Ihre On-Premises-Domain
- Simple AD: Konfigurieren von DNS

Nachdem Sie Ihre DNS-Servereinstellungen aktualisiert haben, fahren Sie mit Schritt 3 fort.

Schritt 3: Testen der aktualisierten DNS-Servereinstellungen

Gehen Sie nach Abschluss von Schritt 1 und Schritt 2 wie folgt vor, um zu überprüfen, ob Ihre aktualisierten DNS-Servereinstellungen wie erwartet funktionieren.

Im folgenden Verfahren werden die aktuellen und neuen DNS-Server-IP-Adresswerte wie folgt bezeichnet:

- Aktuelle DNS-IP-Adressen: *`OldIP1`*, *`OldIP2`*
- Neue DNS-IP-Adressen: *`NewIP1`*, *`NewIP2`*

> **Note**
>
> Wenn Sie dieses Verfahren zum zweiten Mal durchführen, ersetzen Sie *OldIP1* durch *OldIP2* und *NewIP1* durch *NewIP2*.

Testen der aktualisierten DNS-Servereinstellungen für Windows-WorkSpaces

1. Fahren Sie den *OldIP1*-DNS-Server herunter.
2. Melden Sie sich bei einem Windows-WorkSpace an.
3. Wählen Sie im Windows-Startmenü Windows System und dann Eingabeaufforderung aus.
4. Führen Sie den folgenden Befehl aus, wobei *AD_Name* der Name Ihres Active Directory ist (z. B. `corp.example.com`).

   ```
   nslookup AD_Name
   ```

   Der `nslookup`-Befehl sollte Folgendes zurückgeben. (Wenn Sie dieses Verfahren zum zweiten Mal ausführen, sollten Sie *NewIP2* statt *OldIP2* sehen.)

   ```
   Server:  Full_AD_Name
   Address:  NewIP1

   Name:    AD_Name
   Addresses:  OldIP2
             NewIP1
   ```

5. Wenn die Ausgabe nicht Ihren Erwartungen entspricht oder wenn Sie Fehler erhalten, wiederholen Sie Schritt 1.
6. Warten Sie eine Stunde und vergewissern Sie sich, dass keine Benutzerprobleme gemeldet wurden. Stellen Sie sicher, dass *NewIP1* DNS-Abfragen empfangen und beantwortet werden.
7. Nachdem Sie sich vergewissert haben, dass der erste DNS-Server ordnungsgemäß funktioniert, wiederholen Sie Schritt 1, um den zweiten DNS-Server zu aktualisieren. Ersetzen Sie dieses Mal *OldIP2* durch *NewIP2*. Wiederholen Sie dann Schritt 2 und Schritt 3.

Testen der aktualisierten DNS-Servereinstellungen für Linux-WorkSpaces

1. Fahren Sie den *OldIP1*-DNS-Server herunter.

2. Melden Sie sich bei einem Linux-WorkSpace an.
3. Öffnen Sie in Ihrem Linux-WorkSpace ein Terminalfenster (Anwendungen > Systemprogramme > MATE Terminal).
4. Die in der DHCP-Antwort zurückgegebenen DNS-Server-IP-Adressen werden in die lokale `/etc/resolv.conf`-Datei im WorkSpace geschrieben. Führen Sie die folgenden Befehle aus, um den Inhalt der `/etc/resolv.conf` -Datei anzuzeigen.

```
cat /etc/resolv.conf
```

Die Ausgabe sollte folgendermaßen aussehen. (Wenn Sie dieses Verfahren zum zweiten Mal ausführen, sollten Sie *NewIP2* statt *OldIP2* sehen.)

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

> **Note**
>
> Wenn Sie manuelle Änderungen an der `/etc/resolv.conf`-Datei vornehmen, gehen diese Änderungen verloren, wenn der WorkSpace neu gestartet wird.

5. Wenn die Ausgabe nicht Ihren Erwartungen entspricht oder wenn Sie Fehler erhalten, wiederholen Sie Schritt 1.
6. Die tatsächlichen IP-Adressen des DNS-Servers werden in der `/etc/dhcp/dhclient.conf`-Datei gespeichert. Führen Sie den folgenden Befehl aus, um den Inhalt der Datei anzuzeigen.

```
sudo cat /etc/dhcp/dhclient.conf
```

Die Ausgabe sollte folgendermaßen aussehen. (Wenn Sie dieses Verfahren zum zweiten Mal ausführen, sollten Sie *NewIP2* statt *OldIP2* sehen.)

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your WorkSpace inaccessible until rebuild
```

```
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. Warten Sie eine Stunde und vergewissern Sie sich, dass keine Benutzerprobleme gemeldet wurden. Stellen Sie sicher, dass *NewIP1* DNS-Abfragen empfangen und beantwortet werden.
8. Nachdem Sie sich vergewissert haben, dass der erste DNS-Server ordnungsgemäß funktioniert, wiederholen Sie Schritt 1, um den zweiten DNS-Server zu aktualisieren. Ersetzen Sie dieses Mal *OldIP2* durch *NewIP2*. Wiederholen Sie dann Schritt 2 und Schritt 3.

Löschen des Verzeichnisses für Ihre WorkSpaces

Sie können das Verzeichnis für Ihre WorkSpaces löschen, wenn es von anderen WorkSpaces oder andere Anwendungen wie Amazon WorkDocs, Amazon WorkMail oder Amazon Chime nicht länger verwendet wird. Beachten Sie, dass Sie ein Verzeichnis abmelden müssen, bevor Sie es löschen können.

> **Note**
>
> Simple AD und AD Connector werden Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem AD-Connector-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.
> Wenn Sie Ihr Simple-AD- oder AD-Connector-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

Das passiert, wenn ein Verzeichnis gelöscht wird

Wenn ein Simple-AD- oder AWS Directory Service for Microsoft Active Directory-Verzeichnis gelöscht wird, werden auch alle Verzeichnisdaten und Snapshots gelöscht und können nicht wiederhergestellt werden. Alle Amazon-EC2-Instances, die dem Verzeichnis zugeordnet sind, bleiben erhalten, nachdem das Verzeichnis gelöscht wurde. Sie können sich jedoch nicht mit den Anmeldeinformationen Ihres Verzeichnisses bei diesen Instances anmelden. In dem Fall müssen Sie sich mit einem lokalen AWS-Konto bei den jeweiligen Instances anmelden.

Wenn ein AD-Connector-Verzeichnis gelöscht wird, bleibt Ihr on-premises Verzeichnis intakt. Alle zugeordneten Amazon-EC2-Instances bleiben ebenfalls erhalten und sind weiterhin mit Ihrem on-

premises Verzeichnis verknüpft. Sie können sich nach wie vor mit den Anmeldeinformationen Ihres Verzeichnisses bei diesen Instances anmelden.

So löschen Sie ein Verzeichnis

1. Löschen Sie alle WorkSpaces im Verzeichnis. Weitere Informationen finden Sie unter Löschen eines WorkSpaces.
2. Suchen Sie alle Anwendungen und Dienste, die im Verzeichnis registriert sind, und entfernen Sie sie. Weitere Informationen finden Sie unter Löschen Ihres Verzeichnisses im AWS Directory Service-Administratorhandbuch.
3. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
4. Wählen Sie im Navigationsbereich Verzeichnisse aus.
5. Wählen Sie das Verzeichnis und anschließend Actions, Deregister aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Deregister aus.
7. Wählen Sie erneut das Verzeichnis und anschließend Actions, Delete aus.
8. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

> **Note**
>
> Das Entfernen von Anwendungszuweisungen kann manchmal mehr Zeit in Anspruch nehmen als erwartet. Wenn die folgende Fehlermeldung angezeigt wird, überprüfen Sie, ob Sie alle Anwendungszuweisungen entfernt haben, und warten Sie 30 bis 60 Minuten, bevor Sie erneut versuchen, das Verzeichnis zu löschen:
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (Optional) Nach dem Löschen aller Ressourcen in der Virtual Private Cloud (VPC) für Ihr Verzeichnis, können Sie die VPC löschen und die für das NAT-Gateway verwendete Elastic IP-Adresse freigeben. Weitere Informationen finden Sie unter Löschen der VPC und Arbeiten mit Elastic-IP-Adressen im Amazon-VPC-Benutzerhandbuch.
10. (Optional) Informationen zum Löschen nicht länger benötigter, benutzerdefinierter Bundles und Bilder finden Sie unter Löschen Sie ein benutzerdefiniertes WorkSpaces Bundle oder Image.

Aktivieren von Amazon WorkDocs für AWS Managed Microsoft AD

Wenn Sie AWS Managed Microsoft AD mit Amazon WorkSpaces verwenden, können Sie Amazon WorkDocs für Ihr Verzeichnis entweder über die Amazon-WorkDocs-Konsole oder die AWS Directory Service-Konsole aktivieren.

> **Note**
>
> Amazon WorkDocs ist nicht in allen AWS-Regionen verfügbar, in denen Amazon WorkSpaces verfügbar ist. Weitere Informationen dazu finden Sie unter Amazon WorkDocs – Preise.

So aktivieren Sie WorkDocs über die Amazon-WorkDocs-Konsole

1. Öffnen Sie die Amazon-WorkDocs-Konsole unter https://console.aws.amazon.com/zocalo/.
2. Klicken Sie auf Create a New WorkDocs Site (Eine neue WorkDocs-Website erstellen).
3. Wählen Sie unter Standard Setup (Standard-Einrichtung), die Option Launch (Starten).
4. Wählen Sie das Verzeichnis aus und erstellen Sie den Namen Ihrer Website.
5. Geben Sie den Benutzer an, der die WorkDocs-Website verwaltet. Sie können den Administrator oder einen beliebigen Benutzer verwenden, der im Verzeichnis erstellt wurde.

Weitere Informationen finden Sie unter Erste Schritte mit AWS Managed Microsoft AD im Amazon-WorkDocs-Administratorhandbuch.

So aktivieren Sie WorkDocs über die AWS Directory Service-Konsole

1. Melden Sie sich bei der AWS Directory Service-Konsole unter https://console.aws.amazon.com/directoryservicev2/ an.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihr Verzeichnis aus.
4. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
5. Wenn dem Verzeichnis keine Zugriffs-URL zugewiesen ist, wird im Bereich Application access URL (URL für den Anwendungszugriff) die Schaltfläche Create (Erstellen) angezeigt. Geben Sie

einen Verzeichnisalias ein und wählen Sie Create (Erstellen) aus. Weitere Informationen finden Sie unter Erstellen einer Zugriffs-URL im AWS Directory Service-Administratorhandbuch.

6. Wählen Sie unter Application access URL (URL für den Anwendungszugriff) die Option Enable (Aktivieren) aus, um Single Sign-On für Amazon WorkDocs zu aktiveren. Weitere Informationen finden Sie unter Single Sign-On im AWS Directory Service-Administratorhandbuch.

Einrichten der Active-Directory-Verwaltungstools für WorkSpaces

Zum Ausführen von Aufgaben in Ihrem WorkSpaces-Verzeichnis werden Sie Verzeichnis-Verwaltungstools, wie zum Beispiel die Aktiven Verzeichnis-Verwaltungstools verwenden. Allerdings werden Sie die WorkSpaces-Konsole verwenden, um einige Aufgaben, die mit dem Verzeichnis in Zusammenhang stehen, durchzuführen. Weitere Informationen finden Sie unter Verwalten von Verzeichnissen für WorkSpaces.

Wenn Sie ein Verzeichnis mit AWS Managed Microsoft AD oder Simple AD mit fünf oder mehr WorkSpaces erstellen, empfehlen wir Ihnen, Ihre Administration auf einer EC2-Instance zu zentralisieren. Sie haben zwar die Möglichkeit, die Tools für die Verwaltung von Verzeichnissen auf einem WorkSpace zu installieren, aber eine Amazon-EC2-Instance ist die robustere Lösung.

Aktive Verzeichnis-Administrationstools einrichten

1. Starten Sie eine Amazon EC2-Windows-Instance und fügen Sie sie mit Ihrem WorkSpaces-Verzeichnis hinzu, indem Sie eine der folgenden Optionen verwenden:

   - Wenn Sie noch keine bestehende Amazon-EC2-Windows-Instance haben, können Sie die Instance Ihrer Verzeichnis-Domain hinzufügen, wenn Sie die Instance starten. Weitere Informationen finden Sie unter Nahtloser Beitritt zu einer Windows-EC2-Instance im AWS Directory Service-Administratorhandbuch.
   - Wenn Sie bereits über eine bestehende Amazon-EC2-Windows-Instance verfügen, können Sie diese manuell mit Ihrem Verzeichnis verknüpfen. Weitere Informationen finden Sie unter Nahtloser Beitritt zu einer Windows-Instance im AWS Directory Service-Administratorhandbuch.

2. Installieren Sie in der Amazon-EC2-Windows-Instance die Active-Directory-Verwaltungstools. Weitere Informationen finden Sie unter Installation von Active-Directory-Verwaltungstools im AWS Directory Service-Administrationshandbuch.

> **Note**
>
> Achten Sie bei der Installation der Active-Directory-Verwaltungstools darauf, auch die Gruppenrichtlinienverwaltung auszuwählen, um den Gruppenrichtlinienverwaltungs-Editor (gpmc.msc) zu installieren.

Wenn die Installation der Funktion abgeschlossen ist, sind die Active-Directory-Verwaltungstools im Windows-Startmenü unter Windows-Verwaltungstools verfügbar.

3. Führen sie die Tools als Verzeichnisadministrator wie folgt aus:

   a. Öffnen Sie im Windows-Startmenü die Windows-Verwaltungstools.

   b. Halten Sie die Umschalttaste gedrückt, klicken Sie mit der rechten Maustaste auf die Tool-Verknüpfung und wählen Sie Als anderer Benutzer ausführen aus.

   c. Geben Sie die Anmeldeinformationen für den Administrator ein. Bei Simple AD lautet der Benutzername **`Administrator`**, und bei AWS Managed Microsoft AD ist der Administrator **`Admin`**.

Sie können nun mit Ihrem vertrauten Aktiven Verzeichnis-Tools Aufgaben in der Administratorverwaltung ausführen. Zum Beispiel können Sie die Aktiven Verzeichnis-Benutzer- und Computer-Tools verwenden, um Benutzer hinzuzufügen, zu löschen, einem Benutzer Zugriff zum Administratorverzeichnis zu erlauben, oder ein Benutzerpasswort zurückzusetzen. Beachten Sie, dass Sie in Ihrer Windows-Instance als Benutzer angemeldet sein müssen, der befugt ist, Benutzer im Verzeichnis zu verwalten.

Ein Benutzerkonto zum Verzeichnisadministrator-Konto erweitern

> **Note**
>
> Dieses Verfahren gilt nur für Verzeichnisse, die mit Simple AD erstellt wurden, nicht für AWS Managed AD. Informationen zu Verzeichnissen, die mit AWS Managed AD erstellt wurden, finden Sie unter Verwalten von Benutzern und Gruppen in AWS Managed Microsoft AD im AWS Directory Service-Administratorhandbuch.

1. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer".

2. Navigieren Sie in Ihrer Domain zum Ordner Benutzer und wählen Sie den Benutzer aus, dem Sie Zugriff erlauben möchten.
3. Wählen Sie Aktionen, Eigenschaften aus.
4. Wählen Sie im Dialogfeld ***Benutzername***-Eigenschaften Mitglied von aus.
5. Fügen Sie den Benutzer zu den folgenden Gruppen hinzu und klicken Sie auf OK.

    - Administratoren
    - Domain-Administratoren
    - Enterprise-Administratoren
    - Gruppenrichtlinien-Ersteller/-Besitzer
    - Schema-Administratoren

Hinzufügen oder Entfernen von Benutzern

Sie können neue Benutzer nur während des Startvorgangs eines WorkSpace über die Amazon-WorkSpaces-Konsole erstellen, und Sie können keine Benutzer über die Amazon-WorkSpaces-Konsole löschen. Die meisten Benutzerverwaltungsaufgaben, einschließlich der Verwaltung von Benutzergruppen, müssen über Ihr Verzeichnis ausgeführt werden.

> **Important**
>
> Bevor Sie einen Benutzer entfernen können, müssen Sie den diesem Benutzer zugewiesenen WorkSpace entfernen. Weitere Informationen finden Sie unter Löschen eines WorkSpaces.

Mit welchem Prozess Sie Benutzern und Gruppen verwalten, hängt von dem von Ihnen verwendeten Verzeichnistyp ab.

- Wenn Sie AWS Managed Microsoft AD verwenden, finden Sie weitere Informationen unter Verwalten von Benutzern und Gruppen in AWS Managed Microsoft AD im AWS Directory ServiceAdministrationshandbuch.
- Wenn Sie Simple AD verwenden, finden Sie weitere Informationen unter Verwalten von Benutzern und Gruppen in Simple AD im AWS Directory Service-Administratorhandbuch.
- Wenn Sie Microsoft Active Directory über AD Connector oder eine Vertrauensstellung verwenden, können Sie Benutzer und Gruppen mit Hilfe des Active-Directory-Moduls verwalten.

To reset a user password

Wenn Sie das Passwort eines bestehenden Benutzers zurücksetzen, stellen Sie nicht Benutzer muss bei der nächsten Anmeldung Passwort ändern ein. Andernfalls können die Benutzer keine Verbindung mit ihren WorkSpaces aufbauen. Weisen Sie jedem Benutzer stattdessen ein sicheres temporäres Passwort zu, und bitten Sie die Benutzer, das Passwort bei der nächsten Anmeldung manuell im WorkSpace zu ändern.

> **Note**
>
> Wenn Sie AD Connector verwenden oder wenn sich Ihre Benutzer in der AWS-Region GovCloud (USA-West) befinden, können Ihre Benutzer ihre eigenen Passwörter nicht zurücksetzen. (Die Option Passwort vergessen? auf dem Anmeldebildschirm der WorkSpaces-Clientanwendung ist nicht verfügbar.)

Starten eines virtuellen Desktops mit WorkSpaces

Mit WorkSpaces können Sie die Bereitstellung von virtuellen, cloud-basierten Microsoft-Windows-, Amazon-Linux- oder Ubuntu-Linux-Desktops für Ihre Benutzer durchführen, die als WorkSpaces bezeichnet werden.

Note

Der Computername, der für einen WorkSpace in der Amazon-WorkSpaces-Konsole angezeigt wird, variiert je nachdem, welchen WorkSpace-Typ Sie gestartet haben (Amazon Linux, Ubuntu oder Windows). Der Computername für einen WorkSpace kann eines der folgenden Formate aufweisen:

- Amazon Linux: A-*xxxxxxxxxxxxx*
- Ubuntu: U-*xxxxxxxxxxxxx*
- Windows: IP-C*xxxxxx* oder WSAMZN-*xxxxxxx* oder EC2AMAZ-*xxxxxxx*

Bei Windows-WorkSpaces wird das Computernamenformat durch den Pakettyp bestimmt und im Fall von WorkSpaces, die aus öffentlichen Paketen oder aus benutzerdefinierten Paketen auf der Grundlage von öffentlichen Abbildern erstellt wurden, durch den Zeitpunkt der Erstellung der öffentlichen Abbilder.
Ab dem 22. Juni 2020 haben Windows-WorkSpaces, die aus öffentlichen Paketen gestartet wurden, das Format WSAMZN-*xxxxxxx* für ihre Computernamen anstelle des IP-C*xxxxxx*-Formats.
Bei benutzerdefinierten Paketen, die auf einem öffentlichen Abbild basieren, haben die Computernamen das Format EC2AMAZ-*xxxxxxx*, sofern das öffentliche Abbild vor dem 22. Juni 2020 erstellt wurde. Wenn das öffentliche Abbild am oder nach dem 22. Juni 2020 erstellt wurde, haben die Computernamen das Format WSAMZN-*xxxxxxx*.
Für BYOL-Pakete (Bring-Your-Own-License) wird standardmäßig entweder das Format DESKTOP-*xxxxxxx* oder das Format EC2AMAZ-*xxxxxxx* für die Computernamen verwendet.
Wenn Sie ein benutzerdefiniertes Format für die Computernamen in Ihren benutzerdefinierten oder BYOL-Paketen angegeben haben, überschreibt Ihr benutzerdefiniertes Format diese Standardwerte. Informationen zum Angeben eines benutzerdefinierten Formats finden Sie unter Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket.

Wichtig – Wenn Sie den Computernamen für einen WorkSpace über die Windows-Systemeinstellungen ändern, können Sie nicht mehr auf den WorkSpace zugreifen.

WorkSpaces verwendet ein Verzeichnis zum Speichern und Verwalten von Informationen für Ihre WorkSpaces und Benutzer. Sie können einen der folgenden Schritte ausführen:

- Simple AD-Verzeichnis erstellen.
- Erstellen Sie einen AWS Directory Service für Microsoft Active Directory, auch als AWS Managed Microsoft AD bezeichnet.
- Mithilfe eines Active Directory-Connector mit einem bestehenden Microsoft Active Directory verbinden.
- Eine Vertrauensstellung zwischen dem AWS Managed Microsoft AD-Verzeichnis und der on-premises Domain erstellen.

Note

- Derzeit werden keine freigegebenen Verzeichnisse mit Amazon WorkSpaces unterstützt.
- Wenn Sie Ihr von AWS verwaltetes Microsoft-AD-Verzeichnis für die Replikation in mehreren Regionen konfigurieren, kann nur das Verzeichnis in der primären Region für die Verwendung mit Amazon WorkSpaces registriert werden. Versuche, das Verzeichnis in einer replizierten Region für die Verwendung mit Amazon WorkSpaces zu registrieren, schlagen fehl. Die regionsübergreifende Replikation mit von AWS verwaltetem Microsoft AD wird für die Verwendung mit Amazon WorkSpaces innerhalb replizierter Regionen nicht unterstützt.
- Simple AD und AD Connector werden Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem AD-Connector-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.

  Informationen zum Löschen leerer Verzeichnisse finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces. Wenn Sie Ihr Simple-AD- oder AD-Connector-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

Die folgenden Tutorials zeigen Ihnen, wie Sie einen WorkSpace mit den unterstützten Verzeichnisdienstoptionen starten können.

Tutorials

- Starten eines WorkSpaces über AWS Managed Microsoft AD
- Starten eines WorkSpaces über Simple AD
- Starten eines WorkSpace über AD Connector
- Starten eines WorkSpaces über eine vertrauenswürdige Domain

Starten eines WorkSpaces über AWS Managed Microsoft AD

Amazon WorkSpaces ermöglicht Ihnen die Bereitstellung von virtuellen, cloud-basierten Windows- oder Amazon-Linux-Desktops für Ihre Benutzer, die als WorkSpaces bezeichnet werden.

WorkSpaces verwendet Verzeichnisse zum Speichern und Verwalten von Informationen für Ihre WorkSpaces und Benutzer. Für Ihr Verzeichnis können Sie aus Simple AD, AD Connector oder AWS Directory Service für Microsoft Active Directory, auch als AWS Managed Microsoft AD bezeichnet, auswählen. Zusätzlich können Sie eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD-Verzeichnis und Ihrer lokalen Domain einrichten.

In diesem Tutorial starten Sie einen WorkSpace, der AWS Managed Microsoft AD verwendet. Tutorials, in denen andere Optionen verwendet werden, finden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

Aufgaben

- Bevor Sie beginnen
- Schritt 1: Erstellen eines AWS Managed Microsoft AD-Verzeichnisses
- Schritt 2: Einen WorkSpace erstellen
- Schritt 3: Verbinden mit dem WorkSpace
- Nächste Schritte

Bevor Sie beginnen

- WorkSpaces ist nicht in allen Regionen verfügbar. Überprüfen Sie die unterstützten Regionen und wählen Sie eine Region für Ihre WorkSpaces aus. Weitere Informationen zu den unterstützten Regionen finden Sie unter WorkSpaces – Preise nach AWS-Region.

- Wenn Sie einen WorkSpace in Betrieb nehmen, müssen Sie ein WorkSpace-Paket auswählen. Ein Paket ist eine Kombination aus einem Betriebssystem und Speicher-, Datenverarbeitungs- und Softwareressourcen. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete.
- Wenn Sie mit AWS Directory Service ein Verzeichnis erstellen oder einen WorkSpace starten, müssen Sie eine Virtual Private Cloud erstellen oder auswählen, die mit einem öffentlichen sowie zwei privaten Subnetzen konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren einer VPC für WorkSpaces.

Schritt 1: Erstellen eines AWS Managed Microsoft AD-Verzeichnisses

Erstellen Sie zuerst ein AWS Managed Microsoft AD-Verzeichnis. AWS Directory Service erstellt zwei Verzeichnis-Server, jeweils einen in den privaten Subnetzen in Ihrer VPC. Beachten Sie, dass es anfänglich keine Benutzer in dem Verzeichnis gibt. Im nächsten Schritt fügen Sie beim Starten des WorkSpace einen Benutzer hinzu.

> **Note**
>
> - Derzeit werden keine freigegebenen Verzeichnisse mit Amazon WorkSpaces unterstützt.
> - Wenn Ihr AWS-Managed-Microsoft-AD-Verzeichnis für die Replikation in mehreren Regionen konfiguriert ist, kann nur das Verzeichnis in der primären Region für die Verwendung mit Amazon WorkSpaces registriert werden. Versuche, das Verzeichnis in einer replizierten Region für die Verwendung mit Amazon WorkSpaces zu registrieren, schlagen fehl. Die regionsübergreifende Replikation mit von AWS verwaltetem Microsoft AD wird für die Verwendung mit Amazon WorkSpaces innerhalb replizierter Regionen nicht unterstützt.

So erstellen Sie ein AWS Managed Microsoft AD-Verzeichnis

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Set up Directory, Create Microsoft AD aus.
4. Konfigurieren Sie das Verzeichnis wie folgt:

    a. Geben Sie unter Organization name (Name der Organisation) einen eindeutigen Namen für das Verzeichnis (z. B. mein-demo-verzeichnis) ein. Dieser Name muss mindestens vier

Zeichen lang sein, darf nur alphanumerischen Zeichen sowie Bindestriche (-) enthalten und als Anfangs- oder Endzeichen ein anderes Zeichen als den Bindestrich haben.

b. Geben Sie unter Directory DNS (Verzeichnis-DNS) den vollqualifizierten Namen für das Verzeichnis ein (z. B. workspaces.demo.com).

> **Important**
>
> Wenn Sie den DNS-Server nach dem Start Ihrer WorkSpaces aktualisieren müssen, gehen Sie wie unter Aktualisieren von DNS-Servern für Amazon WorkSpaces beschrieben vor, um sicherzustellen, dass Ihre WorkSpaces ordnungsgemäß aktualisiert werden.

c. Geben Sie unter NetBIOS name (NetBIOS-Name) eine Kurzbezeichnung für das Verzeichnis ein (z. B. workspaces).

d. Geben Sie im Feld Admin password (Admin-Passwort) und Confirm password (Passwort bestätigen) das Passwort für das Verzeichnis-Administrator-Konto ein. Weitere Informationen zu Passwortvoraussetzungen finden Sie unter Erstellen Ihres AWS-Managed-Microsoft-AD-Verzeichnisses im AWS Directory Service-Administratorhandbuch.

e. (Optional) Geben Sie im Feld Description (Beschreibung) eine Beschreibung für das Verzeichnis ein.

f. Wählen Sie unter VPC die erstellte VPC aus.

g. Wählen Sie unter Subnets die zwei privaten Subnetze aus (mit den CIDR-Blöcken `10.0.1.0/24` und `10.0.2.0/24`).

h. Wählen Sie Next Step (Weiter) aus.

5. Wählen Sie Create Microsoft AD aus.
6. Wählen Sie Done (Erledigt) aus. Der ursprüngliche Status des Verzeichnisses ist `Creating`. Nach erfolgreicher Erstellung des Verzeichnisses ist der Status `Active`.

Schritt 2: Einen WorkSpace erstellen

Nachdem Sie jetzt ein AWS Managed Microsoft AD-Verzeichnis erstellt haben, können Sie mit der Erstellung eines WorkSpaces beginnen.

So erstellen Sie einen WorkSpace:

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.

2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie Launch WorkSpaces aus.
4. Wählen Sie auf der Seite Verzeichnis auswählen das erstellte Verzeichnis aus und klicken Sie auf Nächster Schritt. WorkSpaces registriert Ihr Verzeichnis.
5. Fügen Sie dem Verzeichnis auf der Seite Benutzer identifizieren folgendermaßen einen neuen Benutzer hinzu:

   a. Füllen Sie die Felder Username, First Name, Last Name und Email aus. Verwenden Sie eine E-Mail-Adresse, auf die Sie zugreifen können.

   b. Klicken Sie auf Create Users.

   c. Wählen Sie Next Step (Weiter) aus.
6. Wählen Sie auf der Seite Select Bundle ein Bundle aus und klicken Sie anschließend auf Next Step.

> **Note**
>
> Lesen Sie die empfohlenen Verwendungszwecke und Spezifikationen der einzelnen Pakete, um sicherzustellen, dass Sie das Paket auswählen, das für Ihre Benutzer am besten geeignet ist. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete. Weitere Informationen zu Paketspezifikationen, empfohlenen Verwendungsmöglichkeiten und Preisen finden Sie unter Amazon WorkSpaces – Preise.

7. Wählen Sie auf der Seite WorkSpaces Configuration einen Ausführungsmodus aus und klicken Sie anschließend auf Next Step.
8. Klicken Sie auf der Seite Review & Launch WorkSpaces auf Launch WorkSpaces. Der ursprüngliche Status des WorkSpace ist `PENDING`. Nach dem Start ist der Status `AVAILABLE` und eine Einladung wird an die E-Mail-Adresse gesendet, die Sie für den Benutzer angegeben haben.

> **Note**
>
> Einladungs-E-Mails werden nicht gesendet, wenn Benutzer bereits in Active Directory vorhanden sind. Stellen Sie stattdessen sicher, dass Sie den Benutzern manuell eine Einladungs-E-Mail senden. Weitere Informationen finden Sie unter Senden einer Einladungs-E-Mail.

9. (Optional) Wenn Amazon WorkDocs in der Region unterstützt wird, können Sie Amazon WorkDocs für alle Benutzer im Verzeichnis aktivieren. Weitere Informationen finden Sie unter Aktivieren von Amazon WorkDocs für AWS Managed Microsoft AD. Weitere Informationen zur Verwendung von Amazon WorkDocs finden Sie unter Amazon WorkDocs Drive im Administrationshandbuch für Amazon WorkDocs.

Schritt 3: Verbinden mit dem WorkSpace

Nach dem Erhalt der Einladungs-E-Mail können Sie über einen Client Ihrer Wahl eine Verbindung zu Ihrem WorkSpace herstellen. Nachdem Sie sich angemeldet haben, zeigt der Client den WorkSpace-Desktop an.

Herstellen einer Verbindung zum WorkSpace.

1. Öffnen Sie den Link in der Einladungs-E-Mail. Wenn Sie dazu aufgefordert werden, legen Sie ein Passwort fest und aktivieren Sie den Benutzer. Merken Sie sich dieses Passwort, da Sie es für die Anmeldung bei Ihrem WorkSpace benötigen.

   > **Note**
   >
   > Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden und es müssen mindestens 8 und höchstens 64 Zeichen enthalten sein. Passwörter müssen mindestens ein Zeichen aus jeder der folgenden Kategorien enthalten: Kleinbuchstaben (a–z), Großbuchstaben (A–Z), Ziffern (0–9) und ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Weitere Informationen zu den Anforderungen für die WorkSpaces-Clients finden Sie im Amazon-WorkSpaces-Benutzerhandbuch. Gehen Sie dann wie folgt vor:

   - Wenn Sie dazu aufgefordert werden, laden Sie eine der Client-Anwendungen herunter oder starten Sie Web Access.
   - Wenn Sie nicht gefragt werden und noch keine Clientanwendung installiert haben, öffnen Sie https://clients.amazonworkspaces.com/ und laden Sie eine der Clientanwendungen herunter oder starten Sie Web Access.

> **Note**
>
> Sie können keinen Webbrowser (Web Access) verwenden, um eine Verbindung mit Amazon-Linux-WorkSpaces herzustellen.

3. Starten Sie den Client, geben Sie den Registrierungscode aus der Einladungs-E-Mail ein und wählen Sie Register aus.
4. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie die Anmeldeinformationen des/der Benutzer:in ein und wählen Sie dann Anmelden aus.
5. (Optional) Wenn Sie zur Speicherung Ihrer Anmeldeinformationen aufgefordert werden, wählen Sie Yes aus.

Nächste Schritte

Sie können mit der Anpassung des WorkSpace, das Sie gerade erstellt haben fortfahren. Beispielsweise können Sie Software installieren und dann ein benutzerdefiniertes Paket Ihres WorkSpace erstellen. Sie können außerdem verschiedene Verwaltungsaufgaben für Ihre WorkSpaces und Ihr WorkSpaces-Verzeichnis ausführen. Wenn Sie Ihren WorkSpace nicht mehr benötigen, können Sie ihn löschen. Weitere Informationen finden Sie in der folgenden Dokumentation.

- Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket
- Verwalten Ihres WorkSpaces
- Verwalten von Verzeichnissen für WorkSpaces
- Löschen eines WorkSpaces

Weitere Informationen zur Verwendung der WorkSpaces-Clientanwendungen, z. B. zur Einrichtung mehrerer Monitore oder zur Verwendung von Peripheriegeräten, finden Sie unter WorkSpaces-Clients und Peripheriegeräte-Support im Amazon-WorkSpaces-Benutzerhandbuch.

Starten eines WorkSpaces über Simple AD

Amazon WorkSpaces ermöglicht Ihnen die Bereitstellung von virtuellen, cloud-basierten Microsoft-Windows- oder Amazon-Linux-Desktops für Ihre Benutzer, die als WorkSpaces bezeichnet werden.

WorkSpaces verwendet Verzeichnisse zum Speichern und Verwalten von Informationen für Ihre WorkSpaces und Benutzer. Für Ihr Verzeichnis können Sie aus Simple AD, AD Connector oder AWS Directory Service für Microsoft Active Directory, auch als AWS Managed Microsoft AD bezeichnet, auswählen. Zusätzlich können Sie eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD-Verzeichnis und Ihrer lokalen Domain einrichten.

In diesem Tutorial starten Sie einen WorkSpace, der Simple AD verwendet. Tutorials, in denen andere Optionen verwendet werden, finden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

Aufgaben

Bevor Sie beginnen

- Simple AD ist nicht in allen Regionen verfügbar. Überprüfen Sie die unterstützten Regionen und wählen Sie eine Region für Ihr Simple-AD-Verzeichnis aus. Weitere Informationen zu den unterstützten Regionen für Simple AD finden Sie unter Verfügbarkeit von Regionen für AWS Directory Service.
- WorkSpaces ist nicht in allen Regionen verfügbar. Überprüfen Sie die unterstützten Regionen und wählen Sie eine Region für Ihre WorkSpaces aus. Weitere Informationen zu den unterstützten Regionen finden Sie unter WorkSpaces – Preise nach AWS-Region.
- Wenn Sie einen WorkSpace in Betrieb nehmen, müssen Sie ein WorkSpace-Paket auswählen. Ein Paket ist eine Kombination aus einem Betriebssystem und Speicher-, Datenverarbeitungs- und Softwareressourcen. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete.
- Wenn Sie mit AWS Directory Service ein Verzeichnis erstellen oder einen WorkSpace starten, müssen Sie eine Virtual Private Cloud erstellen oder auswählen, die mit einem öffentlichen sowie zwei privaten Subnetzen konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren einer VPC für WorkSpaces.

Schritt 1: Erstellen eines Simple-AD-Verzeichnisses

Erstellen Sie Simple AD-Verzeichnis. AWS Directory Service erstellt zwei Verzeichnis-Server, jeweils einen in den privaten Subnetzen in Ihrer VPC. Beachten Sie, dass es anfänglich keine Benutzer in dem Verzeichnis gibt. Im nächsten Schritt fügen Sie beim Erstellen des WorkSpace einen Benutzer hinzu.

> **Note**
>
> Simple AD wird Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem Simple-AD-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.
> Informationen zum Löschen leerer Verzeichnisse finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces. Wenn Sie Ihr Simple-AD-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

Ein Simple AD-Verzeichnis erstellen

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Verzeichnis einrichten, Simple AD und Weiter aus.
4. Konfigurieren Sie das Verzeichnis wie folgt:

    a. Geben Sie unter Organization name (Name der Organisation) einen eindeutigen Namen für das Verzeichnis (z. B. mein-beispiel-verzeichnis) ein. Dieser Name muss mindestens vier Zeichen lang sein, darf nur alphanumerischen Zeichen sowie Bindestriche (-) enthalten und als Anfangs- oder Endzeichen ein anderes Zeichen als den Bindestrich haben.

    b. Geben Sie unter Verzeichnis-DNS den vollständig qualifizierten Namen für das Verzeichnis ein (z. B. example.com).

    > **Important**
    >
    > Wenn Sie den DNS-Server nach dem Start Ihrer WorkSpaces aktualisieren müssen, gehen Sie wie unter Aktualisieren von DNS-Servern für Amazon WorkSpaces

beschrieben vor, um sicherzustellen, dass Ihre WorkSpaces ordnungsgemäß aktualisiert werden.

c. Geben Sie unter NetBIOS name (NetBIOS-Name) eine Kurzbezeichnung für das Verzeichnis ein (z. B. example).

d. Geben Sie im Feld Admin password (Admin-Passwort) und Confirm password (Passwort bestätigen) das Passwort für das Verzeichnis-Administrator-Konto ein. Weitere Informationen zu Passwortvoraussetzungen finden Sie unter So erstellt man ein Microsoft-AD-Verzeichnis im AWS Directory Service-Administratorhandbuch.

e. (Optional) Geben Sie im Feld Description (Beschreibung) eine Beschreibung für das Verzeichnis ein.

f. Wählen Sie für Verzeichnisgröße die Option Klein aus.

g. Wählen Sie unter VPC die erstellte VPC aus.

h. Wählen Sie unter Subnets die zwei privaten Subnetze aus (mit den CIDR-Blöcken `10.0.1.0/24` und `10.0.2.0/24`).

i. Wählen Sie Next (Weiter).

5. Wählen Sie Verzeichnis erstellen aus.
6. Der ursprüngliche Status des Verzeichnis ist `Requested` und dann `Creating`. Wenn die Verzeichniserstellung abgeschlossen ist (dies kann einige Minuten dauern), lautet der Status `Active`.

Was passiert beim Erstellen eines Verzeichnisses?

WorkSpaces führt in Ihrem Namen folgende Aufgaben aus:

- Es wird eine IAM-Rolle erstellt, mit der der WorkSpaces-Service Elastic-Network-Schnittstellen erstellen und die WorkSpaces-Verzeichnisse auflisten kann. Diese Rolle hat den Namen `workspaces_DefaultRole`.
- In der VPC wird ein Simple AD-Verzeichnis für die Speicherung von Benutzer- und WorkSpace-Informationen eingerichtet. Das Verzeichnis hat ein Administrator-Konto mit dem Benutzernamen des Administrators und dem angegebenen Passwort.
- Es werden zwei Sicherheitsgruppen erstellt: eine für den Verzeichnis-Controller und die andere für die WorkSpaces im Verzeichnis.

Schritt 2: Einen WorkSpace erstellen

Nun sind Sie bereit den WorkSpace zu starten.

Erstellen eines WorkSpace für einen Benutzer

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie Launch WorkSpaces aus.
4. Führen Sie auf der Seite Verzeichnis auswählen die folgenden Schritte aus:
   a. Wählen Sie unter Verzeichnis das Verzeichnis, das Sie erstellt haben, aus.
   b. Wählen Sie für Self-Service-Berechtigungen aktivieren die Option Ja oder Nein aus und geben Sie eine Beschreibung ein.
   c. Für die Option Amazon WorkDocs aktivieren, wählen Sie Ja aus.

      > **Note**
      >
      > Diese Option ist nur verfügbar, wenn Amazon WorkDocs in der ausgewählten Region verfügbar ist.

   d. Wählen Sie Next Step (Weiter) aus. WorkSpaces registriert Ihr Simple-AD-Verzeichnis.
5. Fügen Sie dem Verzeichnis auf der Seite Benutzer identifizieren folgendermaßen einen neuen Benutzer hinzu:
   a. Füllen Sie die Felder Username, First Name, Last Name und Email aus. Verwenden Sie eine E-Mail-Adresse, auf die Sie zugreifen können.
   b. Klicken Sie auf Create Users.
   c. Wählen Sie Next Step (Weiter) aus.
6. Wählen Sie auf der Seite Select Bundle ein Bundle aus und klicken Sie anschließend auf Next Step.

   > **Note**
   >
   > Lesen Sie die empfohlenen Verwendungszwecke und Spezifikationen der einzelnen Pakete, um sicherzustellen, dass Sie das Paket auswählen, das für Ihre Benutzer am besten geeignet ist. Weitere Informationen finden Sie unter Amazon

WorkSpaces-Pakete. Weitere Informationen zu Paketspezifikationen, empfohlenen Verwendungsmöglichkeiten und Preisen finden Sie unter Amazon WorkSpaces – Preise.

7. Wählen Sie auf der Seite WorkSpaces Configuration einen Ausführungsmodus aus und klicken Sie anschließend auf Next Step.
8. Klicken Sie auf der Seite Review & Launch WorkSpaces auf Launch WorkSpaces. Der ursprüngliche Status des WorkSpace ist `PENDING`. Nach dem Start (kann 20 Minuten dauern) ist der Status `AVAILABLE` und eine Einladung wird an die E-Mail-Adresse gesendet, die Sie für die Benutzer angegeben haben.

> **Note**
>
> Einladungs-E-Mails werden nicht gesendet, wenn Benutzer bereits in Active Directory vorhanden sind. Stellen Sie stattdessen sicher, dass Sie den Benutzern manuell eine Einladungs-E-Mail senden. Weitere Informationen finden Sie unter Senden einer Einladungs-E-Mail.

Schritt 3: Verbinden mit dem WorkSpace

Nach dem Erhalt der Einladungs-E-Mail können Sie über einen Client Ihrer Wahl eine Verbindung zu Ihrem WorkSpace herstellen. Nachdem Sie sich angemeldet haben, zeigt der Client den WorkSpace-Desktop an.

Herstellen einer Verbindung zum WorkSpace.

1. Öffnen Sie den Link in der Einladungs-E-Mail. Wenn Sie dazu aufgefordert werden, geben Sie ein Passwort ein und aktivieren Sie den Benutzer. Merken Sie sich dieses Passwort, da Sie es für die Anmeldung bei Ihrem WorkSpace benötigen.

> **Note**
>
> Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden und es müssen mindestens 8 und höchstens 64 Zeichen enthalten sein. Passwörter müssen mindestens ein Zeichen aus jeder der folgenden Kategorien enthalten: Kleinbuchstaben (a–z), Großbuchstaben (A–Z), Ziffern (0–9) und ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Weitere Informationen zu den Anforderungen für die WorkSpaces-Clients finden Sie im Amazon-WorkSpaces-Benutzerhandbuch. Gehen Sie dann wie folgt vor:

   - Wenn Sie dazu aufgefordert werden, laden Sie eine der Client-Anwendungen herunter oder starten Sie Web Access.
   - Wenn Sie nicht gefragt werden und noch keine Clientanwendung installiert haben, öffnen Sie https://clients.amazonworkspaces.com/ und laden Sie eine der Clientanwendungen herunter oder starten Sie Web Access.

   > **Note**
   >
   > Sie können keinen Webbrowser (Web Access) verwenden, um eine Verbindung mit Amazon-Linux-WorkSpaces herzustellen.

3. Starten Sie den Client, geben Sie den Registrierungscode aus der Einladungs-E-Mail ein und wählen Sie Register aus.
4. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie die Anmeldeinformationen des/der Benutzer:in ein und wählen Sie dann Anmelden aus.
5. (Optional) Wenn Sie zur Speicherung Ihrer Anmeldeinformationen aufgefordert werden, wählen Sie Yes aus.

Nächste Schritte

Sie können mit der Anpassung des WorkSpace, das Sie gerade erstellt haben fortfahren. Beispielsweise können Sie Software installieren und dann ein benutzerdefiniertes Paket Ihres WorkSpace erstellen. Sie können außerdem verschiedene Verwaltungsaufgaben für Ihre WorkSpaces und Ihr WorkSpaces-Verzeichnis ausführen. Wenn Sie Ihren WorkSpace nicht mehr benötigen, können Sie ihn löschen. Weitere Informationen finden Sie in der folgenden Dokumentation.

- Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket
- Verwalten Ihres WorkSpaces
- Verwalten von Verzeichnissen für WorkSpaces
- Löschen eines WorkSpaces

Weitere Informationen zur Verwendung der WorkSpaces-Clientanwendungen, z. B. zur Einrichtung mehrerer Monitore oder zur Verwendung von Peripheriegeräten, finden Sie unter WorkSpaces-Clients und Peripheriegeräte-Support im Amazon-WorkSpaces-Benutzerhandbuch.

Starten eines WorkSpace über AD Connector

Amazon WorkSpaces ermöglicht Ihnen die Bereitstellung von virtuellen, cloud-basierten Microsoft-Windows- oder Amazon-Linux-Desktops für Ihre Benutzer, die als WorkSpaces bezeichnet werden.

WorkSpaces verwendet Verzeichnisse zum Speichern und Verwalten von Informationen für Ihre WorkSpaces und Benutzer. Für Ihr Verzeichnis können Sie aus Simple AD, AD Connector oder AWS Directory Service für Microsoft Active Directory, auch als AWS Managed Microsoft AD bezeichnet, auswählen. Zusätzlich können Sie eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD-Verzeichnis und Ihrer on-premises Domain einrichten.

In diesem Tutorial starten Sie einen WorkSpace, der AD Connector verwendet. Tutorials, in denen andere Optionen verwendet werden, finden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

Aufgaben

Bevor Sie beginnen

- WorkSpaces ist nicht in allen Regionen verfügbar. Überprüfen Sie die unterstützten Regionen und wählen Sie eine Region für Ihre WorkSpaces aus. Weitere Informationen zu den unterstützten Regionen finden Sie unter WorkSpaces – Preise nach AWS-Region.
- Wenn Sie einen WorkSpace in Betrieb nehmen, müssen Sie ein WorkSpace-Paket auswählen. Ein Paket ist eine Kombination aus einem Betriebssystem und Speicher-, Datenverarbeitungs- und Softwareressourcen. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete.
- Erstellen Sie eine Virtual Private Cloud mit mindestens zwei privaten Subnetzen. Weitere Informationen finden Sie unter Konfigurieren einer VPC für WorkSpaces. Die VPC mit Ihrem on-

premises Netzwerk über ein VPN (Virtual Private Network) oder AWS Direct Connect verbunden sein. Mehr Informationen finden Sie unter Voraussetzungen für AD Connector im AWS Directory Service-Administratorhandbuch.

- Stellen Sie eine Internetverbindung im WorkSpace her. Weitere Informationen finden Sie unter Bereitstellen des Internetzugangs von Ihrem aus WorkSpace.

Schritt 1: Erstellen eines AD Connectors

> **Note**
>
> AD Connector wird Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem AD-Connector-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.
> Informationen zum Löschen leerer Verzeichnisse finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces. Wenn Sie Ihr AD-Connector-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

So erstellen Sie einen AD Connector

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie Verzeichnis einrichten, AD Connector erstellen aus.
4. Geben Sie unter Organization name (Name der Organisation) einen eindeutigen Namen für das Verzeichnis (z. B. mein-beispiel-verzeichnis) ein. Dieser Name muss mindestens vier Zeichen lang sein, darf nur alphanumerischen Zeichen sowie Bindestriche (-) enthalten und als Anfangs- oder Endzeichen ein anderes Zeichen als den Bindestrich haben.
5. Geben Sie im Feld Connected directory DNS (DNS des verbundenen Verzeichnisses) den vollqualifizierten Namen Ihres on-premises Verzeichnisses ein (z. B. example.com).
6. Geben Sie im Feld Connected directory NetBIOS name (NetBIOS-Name des verbundenen Verzeichnisses) den Kurznamen Ihres lokalen Verzeichnisses ein (z. B. example).
7. Geben Sie im Feld Connector account username (Connector-Konto-Benutzername) den Benutzernamen eines Benutzers in Ihrem lokalen Verzeichnis ein. Der Benutzer muss über die

Berechtigungen zum Lesen von Benutzern und Gruppen, Erstellen von Computerobjekten und Hinzufügen von Computern in der Domain verfügen.

8. Geben Sie im Feld Connector-Konto-Passwort und Passwort bestätigen das Passwort für das On-Premises-Benutzerkonto ein.
9. Geben Sie im Feld DNS Address (DNS-Adresse) die IP-Adresse von mindestens einem DNS-Server in Ihrem lokalen Verzeichnis ein.

> **Important**
>
> Wenn Sie die IP-Adresse Ihres DNS-Servers nach dem Start Ihrer WorkSpaces aktualisieren müssen, gehen Sie wie unter Aktualisieren von DNS-Servern für Amazon WorkSpaces beschrieben vor, um sicherzustellen, dass Ihre WorkSpaces ordnungsgemäß aktualisiert werden.

10. (Optional) Geben Sie im Feld Description (Beschreibung) eine Beschreibung für das Verzeichnis ein.
11. Halten Sie die Größe Klein.
12. Wählen Sie im Feld VPC Ihre VPC aus.
13. Wählen Sie im Feld Subnetze Ihre Subnetze aus. Die DNS-Server, die sie spezifiziert haben, müssen von jedem Subnetz abrufbar sein.
14. Wählen Sie Next Step (Weiter) aus.
15. Wählen Sie AD Connector erstellen aus. Es dauert einige Minuten, bis Ihr Verzeichnis verbunden ist. Der ursprüngliche Status des Verzeichnis ist `Requested` und dann `Creating`. Nach erfolgreicher Erstellung des Verzeichnisses ist der Status `Active`.

Schritt 2: Einen WorkSpace erstellen

Jetzt sind Sie bereit WorkSpaces für einen oder mehrerer Benutzer auf Ihrem lokalen Verzeichnis zu starten.

So starten Sie einen WorkSpace für einen vorhandenen Benutzer

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie Launch WorkSpaces aus.

4. Wählen Sie unter Verzeichnis das Verzeichnis, das Sie erstellt haben, aus.
5. (Optional) Wenn Sie ein WorkSpace zum ersten Mal in diesem Verzeichnis starten und Amazon WorkDocs in dieser Region unterstützt wird, können Sie Amazon WorkDocs für alle Benutzer in diesem Verzeichnis aktivieren oder deaktivieren. Weitere Informationen zur Verwendung von Amazon WorkDocs finden Sie unter Amazon WorkDocs Drive im Administrationshandbuch für Amazon WorkDocs.
6. Wählen Sie Next (Weiter). WorkSpaces registriert Ihren AD Connector.
7. Wählen Sie einen oder mehrere bestehende Benutzer aus Ihrem lokalen Verzeichnis aus. Fügen Sie keine neuen Benutzer zu einem On-Premises-Verzeichnis über die WorkSpaces-Konsole hinzu.

   Um nach auswählbaren Benutzern zu suchen, können Sie den Namen des Benutzers vollständig oder teilweise eingeben und Search (Suchen) wählen oder Sie können Show All Users (Alle Benutzer anzeigen) wählen. Beachten Sie, dass Sie einen Benutzer, der keine E-Mail-Adresse hat, nicht hinzufügen können.

   Nachdem Sie die Benutzer ausgewählt haben, klicken Sie auf Auswahl hinzufügen und anschließend auf Nächster Schritt.
8. Unter Paket auswählen, klicken Sie auf das Standard-WorkSpace-Paket, das für die WorkSpaces verwendet werden soll. Unter WorkSpace-Pakete zuweisen, können Sie bei Bedarf ein anderes Paket für ein bestimmtes WorkSpace auswählen. Wenn Sie fertig sind, klicken Sie auf Nächster Schritt.

   > **Note**
   >
   > Lesen Sie die empfohlenen Verwendungszwecke und Spezifikationen der einzelnen Pakete, um sicherzustellen, dass Sie das Paket auswählen, das für Ihre Benutzer am besten geeignet ist. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete. Weitere Informationen zu Paketspezifikationen, empfohlenen Verwendungsmöglichkeiten und Preisen finden Sie unter Amazon WorkSpaces – Preise.
9. Wählen Sie einen Ausführungsmodus für Ihre WorkSpaces aus und klicken Sie anschließend auf Nächster Schritt. Weitere Informationen finden Sie unter Verwalten des WorkSpace-Funktionsmodus.
10. Wählen Sie Launch WorkSpaces aus. Der ursprüngliche Status des WorkSpace ist `PENDING`. Nach abgeschlossenem Start, ist der Status `AVAILABLE`.

11. Senden Sie eine Einladung an die E-Mail-Adresse jedes Benutzers. (Diese Einladungen werden nicht automatisch gesendet, wenn Sie AD Connector verwenden.) Weitere Informationen finden Sie unter Senden einer Einladungs-E-Mail.

Schritt 3: Verbinden mit dem WorkSpace

Sie können eine Verbindung zu Ihrem WorkSpace mit dem Client Ihrer Wahl aufbauen. Nachdem Sie sich angemeldet haben, zeigt der Client den WorkSpace-Desktop an.

Herstellen einer Verbindung zum WorkSpace.

1. Öffnen Sie den Link in der Einladungs-E-Mail.
2. Weitere Informationen zu den Anforderungen für die WorkSpaces-Clients finden Sie im Amazon-WorkSpaces-Benutzerhandbuch. Gehen Sie dann wie folgt vor:

   - Wenn Sie dazu aufgefordert werden, laden Sie eine der Client-Anwendungen herunter oder starten Sie Web Access.
   - Wenn Sie nicht gefragt werden und noch keine Clientanwendung installiert haben, öffnen Sie https://clients.amazonworkspaces.com/ und laden Sie eine der Clientanwendungen herunter oder starten Sie Web Access.

   > **Note**
   >
   > Sie können keinen Webbrowser (Web Access) verwenden, um eine Verbindung mit Amazon-Linux-WorkSpaces herzustellen.

3. Starten Sie den Client, geben Sie den Registrierungscode aus der Einladungs-E-Mail ein und wählen Sie Register aus.
4. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie die Anmeldeinformationen des/der Benutzer:in ein und wählen Sie dann Anmelden aus.
5. (Optional) Wenn Sie zur Speicherung Ihrer Anmeldeinformationen aufgefordert werden, wählen Sie Yes aus.

> **Note**
>
> Da Sie AD Connector verwenden, können Ihre Benutzer ihre eigenen Kennwörter nicht zurücksetzen. (Die Option Passwort vergessen? auf dem Anmeldebildschirm der WorkSpaces-Clientanwendung ist nicht verfügbar.) Weitere Informationen zum Zurücksetzen von Benutzerpasswörtern finden Sie unter Einrichten der Active-Directory-Verwaltungstools für WorkSpaces.

Nächste Schritte

Sie können mit der Anpassung des WorkSpace, das Sie gerade erstellt haben fortfahren. Beispielsweise können Sie Software installieren und dann ein benutzerdefiniertes Paket Ihres WorkSpace erstellen. Sie können außerdem verschiedene Verwaltungsaufgaben für Ihre WorkSpaces und Ihr WorkSpaces-Verzeichnis ausführen. Wenn Sie Ihren WorkSpace nicht mehr benötigen, können Sie ihn löschen. Weitere Informationen finden Sie in der folgenden Dokumentation.

- Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket
- Verwalten Ihres WorkSpaces
- Verwalten von Verzeichnissen für WorkSpaces
- Löschen eines WorkSpaces

Weitere Informationen zur Verwendung der WorkSpaces-Clientanwendungen, z. B. zur Einrichtung mehrerer Monitore oder zur Verwendung von Peripheriegeräten, finden Sie unter WorkSpaces-Clients und Peripheriegeräte-Support im Amazon-WorkSpaces-Benutzerhandbuch.

Starten eines WorkSpaces über eine vertrauenswürdige Domain

WorkSpaces ermöglicht Ihnen die Bereitstellung von virtuellen, cloud-basierten Microsoft-Windows-, Amazon-Linux- oder Ubuntu-Linux-Desktops für Ihre Benutzer, die als WorkSpaces bezeichnet werden.

WorkSpaces verwendet Verzeichnisse zum Speichern und Verwalten von Informationen für Ihre WorkSpaces und Benutzer. Für Ihr Verzeichnis können Sie aus Simple AD, AD Connector oder AWS Directory Service für Microsoft Active Directory, auch als AWS Managed Microsoft AD bezeichnet,

auswählen. Zusätzlich können Sie eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD-Verzeichnis und Ihrer lokalen Domain einrichten.

In diesem Tutorial starten Sie einen WorkSpace, der eine Vertrauensstellung verwendet. Tutorials, in denen andere Optionen verwendet werden, finden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

Aufgaben

Bevor Sie beginnen

- Das Starten von WorkSpaces mit AWS-Konten in einer separaten, vertrauenswürdigen Domain funktioniert mit AWS Managed Microsoft AD, wenn es mit einer Vertrauensstellung zu Ihrem On-Premises-Verzeichnis konfiguriert ist. WorkSpaces, die Simple AD oder AD Connector verwenden, können WorkSpaces jedoch nicht für Benutzer aus einer vertrauenswürdigen Domain starten.
- WorkSpaces ist nicht in allen Regionen verfügbar. Überprüfen Sie die unterstützten Regionen und wählen Sie eine Region für Ihre WorkSpaces aus. Weitere Informationen zu den unterstützten Regionen finden Sie unter WorkSpaces – Preise nach AWS-Region.
- Wenn Sie einen WorkSpace in Betrieb nehmen, müssen Sie ein WorkSpace-Paket auswählen. Ein Paket ist eine Kombination aus Datenverarbeitungsressourcen, Speicherplatz und Softwareanwendungen. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete.
- Wenn Sie mit AWS Directory Service ein Verzeichnis erstellen oder einen WorkSpace starten, müssen Sie eine Virtual Private Cloud erstellen oder auswählen, die mit einem öffentlichen sowie zwei privaten Subnetzen konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren einer VPC für WorkSpaces.

Schritt 1: Einrichten einer Vertrauensstellung

So richten Sie eine Vertrauenstellung ein

1. Richten Sie AWS Managed Microsoft AD in Ihrer Virtual Private Cloud (VPC) ein. Weitere Informationen finden Sie unter Erstellen Ihres AWS-Managed-Microsoft-AD-Verzeichnisses im AWS Directory Service-Administratorhandbuch.

   > **Note**
   >
   > - Derzeit werden keine freigegebenen Verzeichnisse mit Amazon WorkSpaces unterstützt.
   > - Wenn Ihr AWS-Managed-Microsoft-AD-Verzeichnis für die Replikation in mehreren Regionen konfiguriert ist, kann nur das Verzeichnis in der primären Region für die Verwendung mit Amazon WorkSpaces registriert werden. Versuche, das Verzeichnis in einer replizierten Region für die Verwendung mit Amazon WorkSpaces zu registrieren, schlagen fehl. Die regionsübergreifende Replikation mit von AWS verwaltetem Microsoft AD wird für die Verwendung mit Amazon WorkSpaces innerhalb replizierter Regionen nicht unterstützt.

2. Stellen Sie eine Vertrauensstellung zwischen AWS Managed Microsoft AD und Ihrer lokalen Domain her. Stellen Sie sicher, dass die Vertrauensstellung als 2-Wege-Vertrauensstellung konfiguriert ist. Weitere Informationen finden Sie unter Tutorial: Herstellung einer Vertrauensstellung zwischen Ihrer AWS Managed Microsoft AD und Ihrer On-Premises-Domain im AWS Directory Service-Administratorhandbuch.

Eine unidirektionale oder bidirektionale Vertrauensstellung kann zur Verwaltung und Authentifizierung von WorkSpaces verwendet werden, damit On-Premises-Benutzern und -Gruppen WorkSpaces bereitgestellt werden können. Weitere Informationen finden Sie unter Bereitstellen von Amazon WorkSpaces mithilfe einer einseitigen Vertrauensstellung für eine Ressourcendomain mit AWS Directory Service.

> **Note**
>
> Ubuntu-WorkSpaces verwendet System Security Services Daemon (SSSD) für die Active-Directory-Integration und SSSD unterstützt keine Gesamtstrukturvertrauensstellungen.

Konfigurieren Sie stattdessen externe Vertrauensstellungen. Für Amazon-Linux- und Ubuntu-WorkSpaces werden bidirektionale Vertrauensstellungen empfohlen.

Schritt 2: Einen WorkSpace erstellen

Nach dem Herstellen einer Vertrauensstellung zwischen AWS Managed Microsoft AD und Ihrer on-premises Microsoft Active Directory-Domain können Sie WorkSpaces für Benutzer in der on-premises Domain bereitstellen.

Sie müssen sicherstellen, dass GPO-Einstellungen über die Domains hinweg repliziert werden, bevor Sie sie auf WorkSpaces anwenden können.

So starten Sie WorkSpaces für Benutzer in einer vertrauenswürdigen On-Premises-Domain

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie Launch WorkSpaces aus.
4. Wählen Sie auf der Seite Select a Directory das Verzeichnis aus, das Sie gerade registriert haben, und klicken Sie auf Next Step.
5. Führen Sie auf der Seite Identify Users die folgenden Schritte aus:
   a. Wählen Sie für Select trust from forest die erstellte Vertrauenstellung aus.
   b. Wählen Sie die Benutzer aus der on-premises Domain aus und klicken Sie dann auf Add Selected.
   c. Wählen Sie Next Step (Weiter) aus.
6. Wählen Sie das für die WorkSpaces zu verwendende Bundle aus und klicken Sie auf dann auf Next Step.

> **Note**
>
> Lesen Sie die empfohlenen Verwendungszwecke und Spezifikationen der einzelnen Pakete, um sicherzustellen, dass Sie das Paket auswählen, das für Ihre Benutzer am besten geeignet ist. Weitere Informationen finden Sie unter Amazon WorkSpaces-Pakete. Weitere Informationen zu Paketspezifikationen, empfohlenen Verwendungsmöglichkeiten und Preisen finden Sie unter Amazon WorkSpaces – Preise.

7. Wählen Sie den Ausführungsmodus und anschließend die Verschlüsselungseinstellungen aus. Konfigurieren Sie dann alle Tags. Wenn Sie fertig sind, klicken Sie auf Next Step.
8. Wählen Sie Launch WorkSpaces aus. Bitte beachten Sie, dass es bis zu 20 Minuten dauern kann, bis die WorkSpaces verfügbar sind, und bis zu 40 Minuten, wenn die Verschlüsselung aktiviert ist. Der ursprüngliche Status des WorkSpace ist `PENDING`. Nach abgeschlossenem Start, ist der Status `AVAILABLE`.
9. Senden Sie eine Einladung an die E-Mail-Adresse jedes Benutzers. (Diese Einladungen werden nicht automatisch gesendet, wenn Sie AD Connector verwenden.) Weitere Informationen finden Sie unter Senden einer Einladungs-E-Mail.

Schritt 3: Verbinden mit dem WorkSpace

Nach dem Erhalt der Einladungs-E-Mail können Sie eine Verbindung zum WorkSpace herstellen. Benutzer können ihre Benutzernamen in der Form username, corp\username oder corp.example.com\username eingeben.

Herstellen einer Verbindung zum WorkSpace.

1. Öffnen Sie den Link in der Einladungs-E-Mail. Wenn Sie dazu aufgefordert werden, geben Sie ein Passwort ein und aktivieren Sie den Benutzer. Merken Sie sich dieses Passwort, da Sie es für die Anmeldung bei Ihrem WorkSpace benötigen.

   > **Note**
   >
   > Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden und es müssen mindestens 8 und höchstens 64 Zeichen enthalten sein. Passwörter müssen mindestens ein Zeichen aus jeder der folgenden Kategorien enthalten: Kleinbuchstaben (a–z), Großbuchstaben (A–Z), Ziffern (0–9) und ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/.

2. Weitere Informationen zu den Anforderungen für die WorkSpaces-Clients finden Sie im Amazon-WorkSpaces-Benutzerhandbuch. Gehen Sie dann wie folgt vor:

   - Wenn Sie dazu aufgefordert werden, laden Sie eine der Client-Anwendungen herunter oder starten Sie Web Access.
   - Wenn Sie nicht gefragt werden und noch keine Clientanwendung installiert haben, öffnen Sie https://clients.amazonworkspaces.com/ und laden Sie eine der Clientanwendungen herunter oder starten Sie Web Access.

> **Note**
>
> Sie können keinen Webbrowser (Web Access) verwenden, um eine Verbindung mit Amazon-Linux-WorkSpaces herzustellen.

3. Starten Sie den Client, geben Sie den Registrierungscode aus der Einladungs-E-Mail ein und wählen Sie Register aus.
4. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie die Anmeldeinformationen des/der Benutzer:in ein und wählen Sie dann Anmelden aus.
5. (Optional) Wenn Sie zur Speicherung Ihrer Anmeldeinformationen aufgefordert werden, wählen Sie Yes aus.

Nächste Schritte

Sie können mit der Anpassung des WorkSpace, das Sie gerade erstellt haben fortfahren. Beispielsweise können Sie Software installieren und dann ein benutzerdefiniertes Paket Ihres WorkSpace erstellen. Sie können außerdem verschiedene Verwaltungsaufgaben für Ihre WorkSpaces und Ihr WorkSpaces-Verzeichnis ausführen. Wenn Sie Ihren WorkSpace nicht mehr benötigen, können Sie ihn löschen. Weitere Informationen finden Sie in der folgenden Dokumentation.

- Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket
- Verwalten Ihres WorkSpaces
- Verwalten von Verzeichnissen für WorkSpaces
- Löschen eines WorkSpaces

Weitere Informationen zur Verwendung der WorkSpaces-Clientanwendungen, z. B. zur Einrichtung mehrerer Monitore oder zur Verwendung von Peripheriegeräten, finden Sie unter WorkSpaces-Clients und Peripheriegeräte-Support im Amazon-WorkSpaces-Benutzerhandbuch.

Verwalten von WorkSpace-Benutzern

Jeder WorkSpace wird einem einzelnen Benutzer zugewiesen und kann nicht von mehreren Benutzern gemeinsam genutzt werden. Standardmäßig ist nur ein WorkSpace pro Benutzer pro Verzeichnis zulässig.

Inhalt

Verwalten von WorkSpaces-Benutzern

Als WorkSpaces-Administrator können Sie die folgenden Aufgaben zur Verwaltung von WorkSpaces-Benutzern durchzuführen.

Benutzerinformationen bearbeiten

Sie können mit der WorkSpaces-Konsole die Benutzerinformationen für einen WorkSpace bearbeiten.

> **Note**
>
> Diese Funktion ist nur verfügbar, wenn Sie AWS Managed Microsoft AD oder Simple AD verwenden. Wenn Sie Microsoft Active Directory über AD Connector oder eine Vertrauensstellung verwenden, können Sie Benutzer und Gruppen mit Hilfe des Active-Directory-Moduls verwalten.

So bearbeiten Sie Benutzerinformationen

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.

2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie einen Benutzer und dann Aktionen, Benutzer bearbeiten aus.
4. Aktualisieren Sie die Felder Vorname, Nachname und E-Mail nach Bedarf.
5. Wählen Sie Aktualisieren aus.

Hinzufügen oder Löschen von Benutzern

Sie können Benutzer nur während des Startvorgangs eines WorkSpace über die Amazon-WorkSpaces-Konsole erstellen und Sie können keine Benutzer über die Amazon-WorkSpaces-Konsole löschen. Die meisten Benutzerverwaltungsaufgaben, einschließlich der Verwaltung von Benutzergruppen, müssen über Ihr Verzeichnis ausgeführt werden.

So fügen Sie Benutzer und Gruppen hinzu oder löschen sie

Falls Sie Benutzer und Gruppen hinzufügen, löschen oder anderweitig verwalten möchten, müssen Sie dies über Ihr Verzeichnis tun. Zum Ausführen von Aufgaben in Ihrem WorkSpaces-Verzeichnis werden Sie Verzeichnis-Verwaltungstools, wie zum Beispiel die Aktiven Verzeichnis-Verwaltungstools verwenden. Weitere Informationen finden Sie unter Einrichten der Active-Directory-Verwaltungstools für WorkSpaces.

> **Important**
>
> Bevor Sie einen Benutzer entfernen können, müssen Sie den diesem Benutzer zugewiesenen WorkSpace entfernen. Weitere Informationen finden Sie unter Löschen eines WorkSpaces.

Mit welchem Prozess Sie Benutzern und Gruppen verwalten, hängt von dem von Ihnen verwendeten Verzeichnistyp ab.

- Wenn Sie AWS Managed Microsoft AD verwenden, finden Sie weitere Informationen unter Verwalten von Benutzern und Gruppen in AWS Managed Microsoft AD im AWS Directory ServiceAdministrationshandbuch.
- Wenn Sie Simple AD verwenden, finden Sie weitere Informationen unter Verwalten von Benutzern und Gruppen in Simple AD im AWS Directory Service-Administratorhandbuch.
- Wenn Sie Microsoft Active Directory über AD Connector oder eine Vertrauensstellung verwenden, können Sie Benutzer und Gruppen mit Hilfe des Active-Directory-Moduls verwalten.

Senden einer Einladungs-E-Mail

Gegebenenfalls können Sie eine Einladungs-E-Mail manuell an einen Benutzer senden.

> **Note**
>
> Wenn Sie AD Connector oder eine vertrauenswürdige Domain verwenden, werden Begrüßung-E-Mails nicht automatisch an Ihre Benutzer gesendet, daher müssen Sie sie manuell senden. Einladungs-E-Mails werden auch nicht automatisch gesendet, wenn Benutzer bereits in Active Directory vorhanden sind.

So senden Sie eine Einladung-E-Mail erneut

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Verwenden Sie auf der Seite WorkSpaces das Suchfeld, um nach dem Benutzer zu suchen, an den Sie eine Einladung senden möchten, und wählen Sie dann den entsprechenden WorkSpace aus den Suchergebnissen aus. Sie können jeweils nur einen WorkSpace auswählen.
4. Wählen Sie Aktionen, Benutzer einladen aus.
5. Wählen Sie auf der Seite Benutzer zum WorkSpace einladen die Option Einladung senden aus.

Erstellen mehrerer WorkSpaces für einen/eine Benutzer:in

Standardmäßig können Sie nur einen WorkSpace pro Benutzer pro Verzeichnis erstellen. Bei Bedarf können Sie jedoch je nach Verzeichniseinrichtung mehrere WorkSpaces für einen Benutzer erstellen.

- Wenn Sie nur ein Verzeichnis für Ihre WorkSpaces haben, erstellen Sie mehrere Benutzernamen für den/die Benutzer:in. Eine Benutzerin mit dem Namen Mary Major kann beispielsweise mmajor1, mmajor2 usw. als Benutzernamen haben. Jeder Benutzername ist mit einem anderen WorkSpace im selben Verzeichnis verknüpft, aber die WorkSpaces haben denselben Registrierungscode, sofern die WorkSpaces alle im selben Verzeichnis in derselben AWS-Region erstellt wurden.
- Wenn Sie mehrere Verzeichnisse für Ihre WorkSpaces haben, erstellen Sie die WorkSpaces für den Benutzer in separaten Verzeichnissen. Sie können denselben oder verschiedene Benutzernamen in den Verzeichnissen verwenden. Die WorkSpaces haben unterschiedliche Registrierungscodes.

> **Tip**
>
> Damit Sie alle WorkSpaces, die Sie für einen/eine Benutzer:in erstellt haben, leicht finden können, verwenden Sie für jeden WorkSpace denselben Basisbenutzernamen.
> Wenn Sie beispielsweise eine Benutzerin namens Mary Major mit dem Active-Directory-Benutzernamen mmajor haben, erstellen Sie WorkSpaces für sie mit Benutzernamen wie mmajor, mmajor1, mmajor2, mmajor3 oder anderen Varianten wie mmajor_windows oder mmajor_linux. Solange alle WorkSpaces denselben Basisbenutzernamen (mmajor) haben, können Sie in Ihrer WorkSpaces-Konsole nach dem Benutzernamen sortieren, um alle WorkSpaces für diesen/diese Benutzer:in zu gruppieren.

> **Important**
>
> - Benutzer können sowohl über einen PCoIP- als auch über einen WSP-WorkSpace verfügen, sofern sich die beiden WorkSpaces in separaten Verzeichnissen befinden. Benutzer können keinen PCoIP- und WSP-WorkSpace im selben Verzeichnis haben.
> - Wenn Sie mehrere WorkSpaces für die Verwendung mit der regionsübergreifenden Umleitung einrichten, müssen Sie die WorkSpaces in verschiedenen Verzeichnissen in verschiedenen AWS-Regionen einrichten und in jedem Verzeichnis dieselben Benutzernamen verwenden. Weitere Informationen zu regionsübergreifenden Umleitungen finden Sie unter Regionsübergreifende Umleitung für Amazon WorkSpaces.

Um zwischen WorkSpaces zu wechseln, meldet sich der/die Benutzer:in mit dem Benutzernamen und dem Registrierungscode an, der einem bestimmten WorkSpace zugeordnet ist. Wenn der Benutzer Version 3.0+ der WorkSpaces-Clientanwendungen für Windows, macOS oder Linux verwendet, kann der Benutzer den WorkSpaces verschiedene Namen zuweisen, indem er in der Clientanwendung zu Settings (Einstellungen), Manage Login Information (Anmeldeinformationen verwalten) navigiert.

Anpassen, wie sich Benutzer bei ihrem anmelden WorkSpaces

Passen Sie den Zugriff Ihrer Benutzer auf an, WorkSpaces indem Sie einheitliche Ressourcenkennungen (URIs) verwenden, um eine vereinfachte Anmeldeerfahrung zu bieten, die in bestehende Workflows in Ihrer Organisation integriert werden kann. Sie können

beispielsweise automatisch Anmelde-URIs generieren, die Ihre Benutzer mithilfe ihres WorkSpaces Registrierungscodes registrieren. Das Ergebnis:

- Benutzer können die manuelle Registrierung umgehen.
- Ihre Benutzernamen werden automatisch auf ihrer WorkSpaces Client-Anmeldeseite eingegeben.
- Wenn in Ihrer Organisation die Multi-Faktor-Authentifizierung (MFA) verwendet wird, werden ihre Benutzernamen und MFA-Codes automatisch auf der Client-Anmeldeseite eingetragen.

Der URI-Zugriff funktioniert sowohl mit regionsbasierten Registrierungscodes (z. B. `WSpdx+ABC12D`) als auch mit auf vollqualifizierten Domainnamen (FQDN) basierenden Registrierungscodes (z. B. `desktop.example.com`). Weitere Informationen zum Erstellen und Verwenden von FQDN-basierten Registrierungscodes finden Sie unter Regionsübergreifende Umleitung für Amazon WorkSpaces.

Sie können den URI-Zugriff auf WorkSpaces für Clientanwendungen auf den folgenden unterstützten Geräten konfigurieren:

- Windows-Computer
- macOS-Computer
- Ubuntu Linux 18.04-, 20.04- und 22.04-Computer
- iPads
- Android-Geräte

Um URIs für den Zugriff auf ihre zu verwenden WorkSpaces, müssen Benutzer zuerst die Clientanwendung für ihr Gerät installieren, indem sie https://clients.amazonworkspaces.com/ öffnen und den Anweisungen folgen.

Der URI-Zugriff wird auf den Browsern Firefox und Chrome auf Windows- und macOS-Computern, auf dem Firefox-Browser auf Ubuntu Linux 18.04-, 20.04- und 22.04-Computern und auf den Browsern Internet Explorer und Microsoft Edge auf Windows-Computern unterstützt. Weitere Informationen zu WorkSpaces Clients finden Sie unter WorkSpaces Clients im Amazon- WorkSpaces Benutzerhandbuch.

> **Note**
>
> Auf Android-Geräten funktioniert der URI-Zugriff nur mit dem Firefox-Browser, nicht mit dem Google Chrome-Browser.

Um den URI-Zugriff auf zu konfigurieren WorkSpaces, verwenden Sie eines der in der folgenden Tabelle beschriebenen URI-Formate.

> **Note**
>
> Wenn die Datenkomponente Ihrer URI eines der folgenden reservierten Zeichen enthält, empfehlen wir Ihnen, die Prozentcodierung in der Datenkomponente zu verwenden, um Mehrdeutigkeiten zu vermeiden:
> `@ : / ? & =`
> Wenn Sie beispielsweise Benutzernamen haben, die eines dieser Zeichen enthalten, sollten Sie diese Benutzernamen in Ihrer URI prozentual kodieren. Weitere Informationen finden Sie unter Uniform Resource Identifier (URI): Generic Syntax.

Unterstützte Syntax	Beschreibung
workspaces://	Öffnet die WorkSpaces Clientanwendung. (Hinweis: Die Verwendung von workspaces:// alleine wird in der Linux-Clientanwendung derzeit nicht unterstützt.)
workspaces://@registrationcode	Registriert einen Benutzer mithilfe seines WorkSpace s Registrierungscodes. Zeigt außerdem die Client-An meldeseite an.
workspaces://username@regis trationcode	Registriert einen Benutzer mithilfe seines WorkSpaces Registrierungscodes. Trägt außerdem automatisch den Benutzernamen in das Feld username auf der Client-An meldeseite ein.
workspaces://username@regis trationcode?MFACode=mfa	Registriert einen Benutzer mithilfe seines WorkSpaces Registrierungscodes. Trägt außerdem automatisch den Benutzernamen in das Feld username und den MFA-

Unterstützte Syntax	Beschreibung
	Code (Multi-Faktor-Authentifizierung) in das Feld MFA-Code auf der Client-Anmeldeseite ein.
workspaces://@registrationcode?MFACode=mfa	Registriert einen Benutzer mithilfe seines WorkSpaces Registrierungscodes. Trägt außerdem automatisch den MFA-Code (Multi-Faktor-Authentifizierung) in das Feld MFA code (MFA-Code) auf der Client-Anmeldeseite ein.

> **Note**
>
> Wenn Benutzer einen URI-Link öffnen, wenn sie bereits von einem Windows-Client WorkSpace aus mit einem verbunden sind, wird eine neue WorkSpaces Sitzung geöffnet und ihre ursprüngliche WorkSpaces Sitzung bleibt geöffnet. Wenn Benutzer einen URI-Link öffnen, wenn sie WorkSpace von einem macOS-, iPad- oder Android-Client aus mit einem verbunden sind, wird keine neue Sitzung geöffnet. Nur ihre ursprüngliche WorkSpaces Sitzung bleibt geöffnet.

Aktivieren von Self-Service-WorkSpace-Verwaltungsfunktionen für Ihre Benutzer

In WorkSpaces können Sie Self-Service-WorkSpace-Verwaltungsfunktionen für Ihre Benutzer aktivieren, um ihnen mehr Kontrolle über ihre Erfahrung zu bieten. Dadurch kann auch die Arbeitslast für Ihre IT-Support-Mitarbeiter für WorkSpaces reduziert werden. Wenn Sie Self-Service-Funktionen aktivieren, können Benutzer mindestens eine der folgenden Aufgaben direkt über ihren Windows- oder OS-X-Client für WorkSpaces auszuführen:

- Speichern Sie die Anmeldeinformationen auf ihrem Client. Auf diese Weise können sie erneut eine Verbindung zu ihrem WorkSpace herstellen, ohne ihre Anmeldeinformationen erneut einzugeben.
- Starten Sie ihren WorkSpace neu.
- Vergrößern Sie die Größe der Stamm- und Benutzer-Volumes in ihrem WorkSpace.
- Ändern Sie den Datenverarbeitungstyp (Paket) für ihren WorkSpace.
- Ändern Sie den Funktionsmodus ihres WorkSpace.

- Erstellen Sie ihren WorkSpace neu.

Unterstützte Clients

- Android auf Android- oder Android-kompatiblen Chrome-OS-Systemen
- Linux
- macOS
- Windows

So aktivieren Sie die Self-Service-Verwaltungsfunktionen für Ihre Benutzer

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.
4. Erweitern Sie User Self-Service Permissions (Benutzer-Self-Service-Berechtigungen). Aktivieren oder deaktivieren Sie die folgenden Optionen nach Bedarf, um die WorkSpace-Verwaltungsaufgaben zu bestimmen, die Benutzer über ihren Client ausführen können:

   - Passwort speichern – Die Benutzer können auswählen, ob ihre Anmeldeinformation auf ihrem Client gespeichert werden sollen. Dazu wählen Sie auf der Anmeldeseite die Kontrollkästchen Passwort speichern oder Angemeldet bleiben aus. Die Anmeldeinformationen werden nur im RAM zwischengespeichert. Wenn Benutzer ihre Anmeldeinformationen speichern möchten, können sie eine erneute Verbindung zu ihren WorkSpaces herstellen, ohne ihre Anmeldeinformationen noch einmal einzugeben. Unter Festlegen der maximalen Gültigkeitsdauer eines Kerberos-Tickets finden Sie Informationen dazu, wie lange Benutzer ihre Anmeldeinformationen zwischenspeichern können.
   - WorkSpace vom Client aus neu starten – Die Benutzer können ihren WorkSpace neu starten. Durch einen Neustart werden die Benutzer von ihrem WorkSpace getrennt, WorkSpace wird heruntergefahren und neu gestartet. Benutzerdaten, Betriebssystem und Systemeinstellungen sind davon nicht betroffen.
   - Volumengröße erhöhen – Die Benutzer können die Stamm- und Benutzervolumes in ihrem WorkSpace auf eine bestimmte Größe erweitern, ohne sich an den IT-Support wenden zu müssen. Benutzer können die Größe des Stammvolumes (für Windows das Laufwerk C:; für Linux /) bis zu 175 GB und die Größe des Benutzervolumes (für Windows das Laufwerk D:; für Linux /home) bis zu 100 GB erhöhen. WorkSpace-Stamm- und Benutzervolumes werden

in festgelegten Gruppen bereitgestellt, die nicht geändert werden können. Die verfügbaren Gruppen sind: [Stamm (GB), Benutzer (GB)]: [80, 10], [80, 50], [80, 100], [175 bis 2000, 100 bis 2000]. Weitere Informationen finden Sie unter Ändern eines WorkSpace.

Bei einem neu erstellten WorkSpace müssen Benutzer 6 Stunden warten, bevor sie diese Laufwerke erweitern können. Anschließend können sie dies nur einmal alle 6 Stunden tun. Während ein Volume vergrößert wird, können Benutzer einen Großteil ihrer Aufgaben auf ihrem WorkSpace ausführen. Folgende Aufgaben können sie nicht durchführen: Ändern ihres WorkSpace-Datenverarbeitungstyps, Ändern des WorkSpace-Ausführungsmodus, Neustarten oder neu Erstellen ihres WorkSpace. Wenn der Prozess abgeschlossen ist, muss der WorkSpace neu gestartet werden, damit die Änderungen wirksam werden. Dieser Vorgang kann bis zu einer Stunde dauern.

> **Note**
>
> Wenn Benutzer das Volume auf ihrem WorkSpace erweitern, erhöht dies den Gebührensatz für ihren WorkSpace.

- Datenverarbeitungstyp ändern – Die Benutzer können ihren WorkSpace zwischen Datenverarbeitungstypen (Pakete) wechseln. Bei einem neu erstellten WorkSpace müssen Benutzer 6 Stunden warten, bevor sie zu einem anderen Paket wechseln können. Danach können sie nur einmal alle 6 Stunden zu einem größeren Paket oder einmal alle 30 Tage zu einem kleineren Paket wechseln. Wenn ein WorkSpace-Datenverarbeitungstyp geändert wird, wird die Verbindung der Benutzer zu ihrem WorkSpace getrennt, und sie können den WorkSpace nicht verwenden oder ändern. Der WorkSpace wird während des Änderungsvorgangs des Datenverarbeitungstyps automatisch neu gestartet. Dieser Vorgang kann bis zu einer Stunde dauern.

  > **Note**
  >
  > Wenn Benutzer ihren WorkSpace-Datenverarbeitungstyp ändern, ändert sich der Gebührensatz für ihren WorkSpace.

- Betriebsmodus wechseln – Die Benutzer können ihren WorkSpace zwischen den Betriebsmodi AlwaysOn und AutoStop wechseln. Weitere Informationen finden Sie unter Verwalten des WorkSpace-Funktionsmodus.

> **Note**
>
> Wenn Benutzer den Ausführungsmodus ihres WorkSpace umstellen, ändert sich dadurch der Gebührensatz für ihren WorkSpace.

- WorkSpace vom Client aus neu erstellen – Die Benutzer können das Betriebssystem eines WorkSpace in seinen ursprünglichen Zustand zurückversetzen. Wenn ein WorkSpace neu erstellt wird, wird das Benutzervolume (Laufwerk D:) aus der neuesten Sicherung neu erstellt. Da Sicherungen alle 12 Stunden durchgeführt werden, könnten Benutzerdaten bis zu 12 Stunden alt sein. Bei einem neu erstellten WorkSpace müssen Benutzer 12 Stunden warten, bevor sie WorkSpace neu erstellen können. Wenn ein WorkSpace neu erstellt wird, wird die Verbindung der Benutzer zu ihrem WorkSpace getrennt, und sie können den WorkSpace nicht verwenden oder Änderungen daran vornehmen. Dieser Vorgang kann bis zu einer Stunde dauern.

5. Wählen Sie Update (Aktualisieren) oder Update and Exit (Aktualisieren und beenden).

Aktivieren der Amazon-Connect-Audiooptimierung für Ihre Benutzer

In der WorkSpaces-Managementkonsole können Sie die Audiooptimierung Amazon Connect Contact Control Panel (CCP) für Ihre WorkSpaces-Flotten aktivieren, um die Sicherheit zu erhöhen und Audioqualität in nativer Qualität zu ermöglichen. Nach der Aktivierung der CCP-Audiooptimierung wird das CCP-Audio von den Client-Endpunkten verarbeitet, während WorkSpaces-Benutzer von ihren WorkSpaces aus mit dem CCP interagieren können.

Die Audiooptimierung Amazon Connect Contact Control Panel (CCP) funktioniert mit:

- WorkSpaces-Windows-Client
- Amazon-Linux- und -Windows-WorkSpaces.
- WorkSpaces, die PCoIP oder WSP verwenden

Voraussetzungen

- (müssen mit Amazon Connect eingerichtet sein)
- Sie müssen ein benutzerdefiniertes CCP mit der Amazon-Connect-Streams-API erstellen, indem Sie ein CCP ohne Medien für die Anrufsignalisierung erstellen. Auf diese Weise werden die

Medien auf dem lokalen Desktop mithilfe des Standard-CCP und von Signalisierungs- und Anrufsteuerungen auf der entfernten Verbindung mit dem CCP ohne Medien verarbeitet. Weitere Informationen über die Amazon-Connect-Streams-API finden Sie im GitHub-Repository unter https://github.com/aws/amazon-connect-streams. Das benutzerdefinierte CCP, das Sie erstellen, ist das CCP, das Ihre Amazon-Connect-Agenten in ihren WorkSpaces verwenden werden.

- Auf dem WorkSpaces-Clientendpunkt muss ein Webbrowser installiert sein, der von Amazon Connect unterstützt wird. Eine Liste der unterstützten Browser finden Sie unter Von Amazon Connect unterstützte Browser.

> **Note**
>
> Wenn Ihre Benutzer Browser verwenden, die nicht unterstützt werden, werden sie aufgefordert, einen unterstützten Browser herunterzuladen, wenn sie versuchen, sich beim CCP anzumelden.

Aktivieren der Audiooptimierung von Amazon Connect

So aktivieren Sie die Amazon-Connect-Audiooptimierung für Ihre Benutzer:

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.
4. Erweitern Sie Amazon-Connect-Audiooptimierung.

> **Note**
>
> Wählen Sie vor der Konfiguration mit Amazon Connect Update aus, um alle zuvor in der Managementkonsole vorgenommenen ungespeicherten Änderungen zu speichern.

5. Wählen Sie Amazon Connect konfigurieren aus.
6. Geben Sie einen Namen für das Amazon Connect Contact Control Panel (CCP) ein.

> **Note**
>
> Der Name, den Sie Ihrem CCP geben, wird im Benutzer-Add-In-Menü verwendet. Wählen Sie einen Namen aus, der für Ihre Benutzer von Bedeutung sein wird.

7. Geben Sie die URL des Amazon Connect Contact Control Panels ein, die von Amazon Connect generiert wurde. Weitere Informationen zum Abrufen der URL finden Sie unter Zugriff auf das Contact Control Panel gewähren.
8. Wählen Sie Amazon Connect erstellen aus.

Aktualisieren der Amazon-Connect-Audiooptimierungsdetails des Verzeichnisses

So aktualisieren Sie die Amazon-Connect-Audiooptimierungsdetails des Verzeichnisses:

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.
4. Erweitern Sie Amazon-Connect-Audiooptimierung.

> **Note**
>
> Wählen Sie vor der Konfiguration mit Amazon Connect Update aus, um alle zuvor in der Managementkonsole vorgenommenen ungespeicherten Änderungen zu speichern.

5. Wählen Sie Amazon Connect konfigurieren aus.
6. Wählen Sie Edit (Bearbeiten) aus.
7. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.
8. Aktualisieren Sie den Namen und die URL des Amazon Connect Contact Control Panels.
9. Wählen Sie Save (Speichern).

Löschen der Amazon-Connect-Audiooptimierungsdetails des Verzeichnisses

So löschen Sie die Amazon-Connect-Audiooptimierungsdetails des Verzeichnisses:

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.
4. Erweitern Sie Amazon-Connect-Audiooptimierung.

> **Note**
>
> Wählen Sie vor der Konfiguration mit Amazon Connect Update aus, um alle zuvor in der Managementkonsole vorgenommenen ungespeicherten Änderungen zu speichern.

5. Wählen Sie Amazon Connect konfigurieren aus.
6. Wählen Sie Amazon Connect löschen aus.

Weitere Informationen finden Sie unter Agent-Schulungsleitfaden.

Aktivieren der Uploads von Diagnoseprotokollen

Um WorkSpaces Clientprobleme zu beheben, aktivieren Sie automatische Uploads von Diagnoseprotokollen. Dies wird derzeit für Windows-, macOS-, Linux- und Web-Access-Clients unterstützt.

> **Note**
>
> Die Funktion zum Hochladen von WorkSpaces Client-Diagnoseprotokollen ist derzeit in der Region AWS GovCloud (USA-West) nicht verfügbar.

Hochladen des Diagnoseprotokolls

Mit Uploads von Diagnoseprotokollen können Sie WorkSpaces Client-Protokolldateien direkt in hochladen, um Probleme WorkSpaces zu beheben, ohne die Verwendung des WorkSpaces Clients zu unterbrechen. Wenn Sie das Hochladen von Diagnoseprotokollen für Ihre Benutzer aktivieren

oder Ihre Benutzer dies selbst tun lassen, werden die Protokolldateien WorkSpaces automatisch an gesendet. Sie können das Hochladen von Diagnoseprotokollen vor oder während einer WorkSpaces Streaming-Sitzung aktivieren.

Um Diagnoseprotokolle automatisch von verwalteten Geräten hochzuladen, installieren Sie einen WorkSpaces Client, der Diagnose-Uploads unterstützt. Das Hochladen von Protokollen ist standardmäßig aktiviert. Sie können die Einstellungen mit einer der folgenden Methoden ändern:

Option 1: Verwenden der AWS-Konsole

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie den Verzeichnisnamen aus, für den Sie die Diagnoseprotokollierung aktivieren möchten.
4. Scrollen Sie nach unten zu Self-Service-Berechtigungen.
5. Wählen Sie Bearbeiten aus.
6. Wählen Sie Hochladen des Diagnoseprotokolls aus.
7. Wählen Sie Speichern.

Option 2: Verwenden eines API-Aufrufs

Sie können die Verzeichniseinstellungen bearbeiten, um den WorkSpaces Windows-, macOS- und Linux-Client so zu aktivieren oder zu deaktivieren, dass Diagnoseprotokolle automatisch mithilfe eines API-Aufrufs hochgeladen werden. Wenn diese Option aktiviert ist, werden die Protokolle bei einem Clientproblem WorkSpaces ohne Benutzerinteraktion an gesendet. Weitere Informationen finden Sie in der API WorkSpaces -Referenz zu .

Sie können die Benutzer auch selbst entscheiden lassen, ob sie automatische Uploads der Diagnoseprotokolle nach der Clientinstallation aktivieren möchten. Weitere Informationen finden Sie unter WorkSpaces Windows-Clientanwendung , WorkSpaces macOS-Clientanwendung und WorkSpaces Linux-Clientanwendung .

> **Note**
>
> - Diagnoseprotokolle enthalten keine vertraulichen Informationen. Sie können automatische Uploads von Diagnoseprotokollen auf Verzeichnisebene deaktivieren oder Ihren Benutzern erlauben, diese Funktionen selbst zu deaktivieren.

- Um auf die Funktion zum Hochladen von Diagnoseprotokollen zuzugreifen, müssen Sie die folgenden Versionen der WorkSpaces Clients installieren:
  - 5.4.0 oder höher des Windows-Clients
  - 5.8.0 oder höher des macOS-Clients
  - 2023.1 des Ubuntu-22.04-Clients
  - 2023.1 des Ubuntu-20.04-Clients
  - Sie können auch mit dem Web-Access-Client auf die Funktion zum Hochladen von Diagnoseprotokollen zugreifen

Verwalten Ihres WorkSpaces

Sie können Ihre WorkSpaces über die WorkSpaces Konsole verwalten.

Informationen zur Durchführung von Verzeichnisverwaltungsaufgaben finden Sie unterthe section called “Einrichten der Verzeichnisadministration”.

> **Note**
>
> - Stellen Sie sicher, dass Sie Netzwerkabhängigkeitstreiber wie ENA-, NVMe- und PV-Treiber auf Ihrem aktualisieren WorkSpaces. Sie sollten dies mindestens einmal alle 6 Monate tun. Weitere Informationen finden Sie unter Installieren oder Aktualisieren des Elastic Network Adapter (ENA)-Treibers, AWS-NVMe-Treiber für Windows-Instances und Aktualisieren von PV-Treibern auf Windows-Instances.
> - Stellen Sie sicher, dass Sie die EC2Config, EC2Launch und EC2Launch V2-Agenten regelmäßig auf die neuesten Versionen aktualisieren. Sie sollten dies mindestens einmal alle 6 Monate tun. Weitere Informationen finden Sie unter Aktualisieren von EC2Config und EC2Launch.

Inhalt

- Wiederherstellen eines WorkSpace
- Microsoft 365 Bring-Your-Own-License (BYOL)
- Windows BYOL aktualisieren WorkSpaces
- Migrieren eines WorkSpace
- Löschen eines WorkSpaces

Verwalte dein Windows WorkSpaces

Sie können Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) verwenden, um Einstellungen zur Verwaltung von Windows WorkSpaces oder Benutzern anzuwenden, die Teil Ihres WorkSpaces Windows-Verzeichnisses sind.

> **Note**
>
> Für Linux-Instances gelten Gruppenrichtlinien nicht. Informationen zur Verwaltung von Amazon Linux WorkSpaces finden Sie unterVerwalten von Amazon Linux WorkSpaces.

Wir empfehlen Ihnen, eine Organisationseinheit für Ihre WorkSpaces Computerobjekte und eine Organisationseinheit für Ihre WorkSpaces Benutzerobjekte zu erstellen.

Um die für Amazon spezifischen Gruppenrichtlinieneinstellungen zu verwenden WorkSpaces, müssen Sie die administrative Gruppenrichtlinien-Vorlage für das oder die verwendeten Protokolle installieren, entweder PCoIP oder WorkSpaces Streaming Protocol (WSP).

> **Warning**
>
> Gruppenrichtlinieneinstellungen können sich wie folgt auf die WorkSpace Benutzererfahrung auswirken:
>
> - Durch die Implementierung einer interaktiven Anmeldenachricht zur Anzeige eines Anmeldebanners können Benutzer nicht auf ihre zugreifen. WorkSpaces Die Gruppenrichtlinieneinstellung für interaktive Anmeldenachrichten wird derzeit nicht unterstützt von. WorkSpaces
> - Das Deaktivieren des Wechselspeichers über Gruppenrichtlinieneinstellungen führt zu einem Anmeldefehler, der seinerseits dazu führt, dass Benutzer bei temporären Benutzerprofilen angemeldet sind und keinen Zugriff auf Laufwerk D haben.

- Wenn Benutzer über Gruppenrichtlinieneinstellungen aus der lokalen Gruppe „Remotedesktopbenutzer“ entfernt werden, können sich diese Benutzer nicht über die WorkSpaces Clientanwendungen authentifizieren. Weitere Informationen zu dieser Gruppenrichtlinieneinstellung finden Sie in der Microsoft-Dokumentation unter Anmeldung über Remotedesktopdienste zulassen.
- Wenn Sie die integrierte Benutzergruppe aus der Sicherheitsrichtlinie Lokales Anmelden zulassen entfernen, können Ihre WorkSpaces PCoIP-Benutzer WorkSpaces über die Client-Anwendungen keine Verbindung zu ihren Benutzern herstellen. WorkSpaces Ihr PCoIP erhält WorkSpaces auch keine Updates für die PCoIP-Agentsoftware. PCoIP-Agent-Updates können Sicherheits- und andere Fixes enthalten, oder sie ermöglichen möglicherweise neue Funktionen für Sie. WorkSpaces Weitere Informationen zum Arbeiten mit dieser Sicherheitsrichtlinie finden Sie in der Microsoft-Dokumentation unter Lokales Anmelden zulassen.
- Gruppenrichtlinieneinstellungen können verwendet werden, um den Zugriff auf Laufwerke zu beschränken. Wenn Sie Gruppenrichtlinieneinstellungen so konfigurieren, dass der Zugriff auf Laufwerk C oder Laufwerk D beschränkt wird, können Benutzer nicht auf ihre zugreifen. WorkSpaces Stellen Sie sicher, dass Ihre Benutzer Zugriff auf die Laufwerke C und D haben, um ein Auftreten dieses Problems zu verhindern.
- Für die WorkSpaces Audioeingabe ist ein lokaler Anmeldezugriff innerhalb des erforderlich. WorkSpace Die Audioeingabefunktion ist für Windows standardmäßig aktiviert. WorkSpaces Wenn Sie jedoch über eine Gruppenrichtlinieneinstellung verfügen, die die lokale Anmeldung von Benutzern in ihren Umgebungen einschränkt WorkSpaces, funktioniert die Audioeingabe auf Ihrem Computer nicht. WorkSpaces Wenn Sie diese Gruppenrichtlinieneinstellung entfernen, wird die Audioeingabefunktion nach dem nächsten Neustart von aktiviert. WorkSpace Weitere Informationen zum Arbeiten mit dieser Gruppenrichtlinieneinstellung finden Sie in der Microsoft-Dokumentation unter Lokales Anmelden zulassen.

  Weitere Informationen zum Aktivieren oder Deaktivieren der Audioeingangsumleitung finden Sie unter Aktivieren oder Deaktivieren der Zwischenablageumleitung für PCoIP oder Aktivieren oder Deaktivieren der Eingangsaudioumleitung für WSP.
- Wenn Sie Gruppenrichtlinien verwenden, um den Windows-Energieplan auf „Ausgewogen“ oder „Stromsparmodus“ zu setzen, werden Sie möglicherweise in den Standbymodus versetzt WorkSpaces , wenn die Geräte inaktiv bleiben. Es wird dringend empfohlen, Gruppenrichtlinien zu verwenden, um den Windows-Energiesparplan auf Hohe Leistung

festzulegen. Weitere Informationen finden Sie unter Mein Windows WorkSpace wechselt in den Standbymodus, wenn es inaktiv bleibt.

- Einige Gruppenrichtlinieneinstellungen erzwingen, dass Benutzer sich abmelden, wenn keine Verbindung zu einer Sitzung besteht. Alle Anwendungen, die Benutzer auf ihren geöffnet haben, WorkSpaces sind geschlossen.
- „Zeitlimit für aktive, aber inaktive Remote Desktop Services-Sitzungen festlegen“ wird derzeit auf WSP WorkSpaces nicht unterstützt. Vermeiden Sie die Verwendung während WSP-Sitzungen, da dies zu einer Unterbrechung führt, selbst wenn Aktivität vorhanden ist und die Sitzung nicht im Leerlauf ist.

Weitere Informationen zur Verwendung der Active-Directory-Verwaltungstools zum Arbeiten mit GPOs finden Sie unter Einrichten der Active-Directory-Verwaltungstools für WorkSpaces.

Inhalt

Installieren Sie die administrativen Gruppenrichtlinien-Vorlagendateien für das WorkSpaces Streaming Protocol (WSP)

Um die Gruppenrichtlinieneinstellungen zu verwenden, die für die WorkSpaces Verwendung des WorkSpaces Streaming Protocol (WSP) spezifisch sind, müssen Sie die administrative

Gruppenrichtlinienvorlage `wsp.admx` und die `wsp.adml` Dateien für WSP dem zentralen Speicher des Domänencontrollers für Ihr Verzeichnis hinzufügen. WorkSpaces Weitere Informationen zu `.admx`- und `.adml`-Dateien finden Sie in der Microsoft-Dokumentation unter So erstellen und verwalten Sie den zentralen Speicher für administrative Gruppenrichtlinienvorlagen in Windows.

Das folgende Verfahren erläutert, wie Sie den zentralen Speicher erstellen und ihm die administrativen Vorlagendateien hinzufügen. Führen Sie das folgende Verfahren für eine Verzeichnisverwaltung WorkSpace oder Amazon EC2 EC2-Instance aus, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist.

So installieren Sie die administrativen Gruppenrichtlinien-Vorlagendatei für WSP

1. Erstellen Sie von einem laufenden Windows WorkSpace aus eine Kopie der `wsp.adml` Dateien `wsp.admx` und im `C:\Program Files\Amazon\WSP` Verzeichnis.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, den Windows-Datei-Explorer und geben Sie in der Adressleiste den vollqualifizierten Domainnamen (FQDN) Ihrer Organisation ein, z. B. `\\example.com`
3. Öffnen Sie das Verzeichnis `sysvol`.
4. Öffnen Sie den Ordner mit dem Namen *FQDN*.
5. Öffnen Sie das Verzeichnis `Policies`. Sie sollten sich jetzt in `\\`*FQDN*`\sysvol\`*FQDN*`\Policies` befinden.
6. Wenn er noch nicht vorhanden ist, erstellen Sie einen Ordner mit dem Namen `PolicyDefinitions`.
7. Öffnen Sie das Verzeichnis `PolicyDefinitions`.
8. Kopieren Sie die Datei `wsp.admx` in den Ordner `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions`.
9. Erstellen Sie einen Ordner mit dem Namen `en-US` im Ordner `PolicyDefinitions`.
10. Öffnen Sie das Verzeichnis `en-US`.
11. Kopieren Sie die Datei `wsp.adml` in den Ordner `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions\en-US`.

So überprüfen Sie, ob die administrativen Vorlagendateien korrekt installiert sind

1. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
2. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
3. Erweitern Sie Domains.
4. Erweitern Sie Ihren FQDN (z. B. `example.com`).
5. Erweitern Sie Gruppenrichtlinienobjekte.
6. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Stattdessen müssen Sie das Gruppenrichtlinienobjekt unter dem Domain-Container mit delegierten Rechten erstellen und verknüpfen.
   > Wenn Sie ein Verzeichnis mit erstellen AWS Managed Microsoft AD, AWS Directory Service erstellt eine Organisationseinheit (OU) für *`Ihren Domainnamen`* unter dem Domänenstamm. Der Name dieser Organisationseinheit basiert auf dem NetBIOS-Namen, den Sie eingegeben haben, als Sie Ihr Verzeichnis erstellt haben. Wenn Sie keinen NetBIOS-Namen angegeben haben, wird dieser standardmäßig auf den ersten Teil Ihres Verzeichnis-DNS-Namens gesetzt (im Falle von `corp.example.com` wäre der NetBIOS-Name z. B. `corp`).
   > Wählen Sie statt Standard-Domain-Richtlinie die Organisationseinheit *`yourdomainname`* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie Gruppenrichtlinienobjekt in dieser Domain erstellen und hier verknüpfen aus, um Ihr Gruppenrichtlinienobjekt zu erstellen.
   > Weitere Informationen zur Organisationseinheit *`yourdomainname`* finden Sie unter Was wird erstellt im AWS Directory Service -Administratorhandbuch.

7. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.

8. Sie können dieses WSP-Gruppenrichtlinienobjekt jetzt verwenden, um die Gruppenrichtlinieneinstellungen zu ändern, die für die WorkSpaces Verwendung von WSP spezifisch sind.

Gruppenrichtlinieneinstellungen für das WorkSpaces Streaming Protocol (WSP) verwalten

Verwenden Sie Gruppenrichtlinieneinstellungen, um Ihr Windows zu verwalten WorkSpaces , das WSP verwendet.

Konfigurieren der Druckerunterstützung für WSP

Standardmäßig WorkSpaces aktiviert Basic Remote Printing, das eingeschränkte Druckfunktionen bietet, da es einen generischen Druckertreiber auf der Hostseite verwendet, um kompatibles Drucken zu gewährleisten.

Mit dem erweiterten Remote-Drucken für Windows-Clients (nicht für WSP verfügbar) können Sie bestimmte Funktionen Ihres Druckers verwenden, z. B. doppelseitiges Drucken. Es ist jedoch eine Installation des passenden Druckertreibers auf der Hostseite erforderlich.

Remote-Drucken wird als virtueller Kanal implementiert. Wenn virtuelle Kanäle deaktiviert sind, funktioniert das Remote-Drucken nicht.

Unter Windows WorkSpaces können Sie die Druckerunterstützung mithilfe der Gruppenrichtlinieneinstellungen nach Bedarf konfigurieren.

Konfigurieren des Druckersupports

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).

6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Konfigurieren von Remote-Drucken.
10. Führen Sie im Dialogfeld Configure remote printing (Remote-Drucken konfigurieren) einen der folgenden Schritte aus:
    - Wählen Sie Aktiviert und dann für Druckoptionen die Option Basis aus, um die lokale Druckerumleitung zu aktivieren. Wählen Sie Lokalen Standarddrucker dem Remote-Host zuordnen aus, um den aktuellen Standarddrucker des Client-Computers automatisch zu verwenden
    - Wählen Sie Deaktiviert aus, um das Drucken zu deaktivieren.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Konfigurieren der Zwischenablageumleitung für WSP

WorkSpaces Unterstützt standardmäßig die bidirektionale Umleitung (Kopieren/Einfügen) in die Zwischenablage. Unter Windows WorkSpaces können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren oder die Richtung konfigurieren, in der die Zwischenablageumleitung zulässig ist.

So konfigurieren Sie die Zwischenablageumleitung für Windows WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr Verzeichnis installiert ist. WorkSpaces
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *`yourdomainname`* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *`yourdomainname`* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.
8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Konfigurieren von Zwischenablagen-Umleitung.

10. Wählen Sie im Dialogfeld Zwischenablageumleitung konfigurieren die Option Aktiviert oder Deaktiviert aus.

    Wenn Zwischenablageumleitung konfigurieren aktiviert ist, sind die folgenden Optionen für die Zwischenablageumleitung verfügbar:

    - Wählen Sie Kopieren und Einfügen aus, um eine bidirektionale Umleitung zum Kopieren und Einfügen in die Zwischenablage zu ermöglichen.
    - Wählen Sie Nur kopieren aus, um nur das Kopieren von Daten aus der Server-Zwischenablage in die Client-Zwischenablage zu ermöglichen.
    - Wählen Sie Nur einfügen aus, um nur das Einfügen von Daten aus der Client-Zwischenablage in die Server-Zwischenablage zu ermöglichen.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Bekannte Einschränkung

Wenn Sie Inhalte WorkSpace, die größer als 890 KB sind, aus einer Microsoft Office-Anwendung kopieren, wird die Anwendung möglicherweise langsam oder reagiert für bis zu 5 Sekunden nicht mehr, wenn Sie die Zwischenablageumleitung aktivieren.

Timeout für die Wiederaufnahme der Sitzung für WSP festlegen

Wenn Sie die Netzwerkverbindung verlieren, wird Ihre aktive WorkSpaces Clientsitzung unterbrochen. WorkSpaces Client-Anwendungen für Windows und macOS versuchen, die Sitzung automatisch wieder zu verbinden, wenn die Netzwerkkonnektivität innerhalb einer bestimmten Zeit wiederhergestellt wird. Das standardmäßige Timeout für WorkSpaces die Wiederaufnahme der Sitzung beträgt 20 Minuten (1200 Sekunden). Sie können diesen Wert jedoch ändern, sodass er von den Gruppenrichtlinieneinstellungen Ihrer Domäne gesteuert wird.

So legen Sie den Wert für die automatische Sitzungszeitbeschränkung fest

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.
8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Automatische Wiederverbindung aktivieren/deaktivieren.
10. Wählen Sie im Dialogfeld Automatische Wiederverbindung aktivieren/deaktivieren die Option Aktiviert aus und legen Sie dann das Zeitlimit für die Wiederverbindung (Sekunden) auf das gewünschte Zeitlimit in Sekunden fest.
11. Wählen Sie OK aus.

12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren oder Deaktivieren der Eingangsvideoumleitung für WSP

WorkSpaces Unterstützt standardmäßig das Umleiten von Daten von einer lokalen Kamera. Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

Um die Videoeingangsumleitung für Windows zu aktivieren oder zu deaktivieren WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr Verzeichnis installiert ist. WorkSpaces
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *`yourdomainname`* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit

yourdomainname finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Eingangsvideoumleitung aktivieren/deaktivieren.
10. Wählen Sie im Dialogfeld Eingangsvideoumleitung aktivieren/deaktivieren die Option Aktiviert oder Deaktiviert aus.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren oder Deaktivieren der Eingangsaudioumleitung für WSP

WorkSpaces Unterstützt standardmäßig das Umleiten von Daten von einem lokalen Mikrofon. Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

Um die Audioeingangsumleitung für Windows zu aktivieren oder zu deaktivieren WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr Verzeichnis installiert ist. WorkSpaces
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.

7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Eingangsaudioumleitung aktivieren/deaktivieren.
10. Wählen Sie im Dialogfeld Eingangsaudioumleitung aktivieren/deaktivieren die Option Aktiviert oder Deaktiviert aus.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren oder Deaktivieren der Eingangsaudioumleitung für WSP

Leitet Daten WorkSpaces standardmäßig an einen lokalen Sprecher weiter. Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

Um die Audioausgangsumleitung für Windows zu aktivieren oder zu deaktivieren WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr Verzeichnis installiert ist. WorkSpaces
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN. z. B. `example.com`.
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *`yourdomainname`* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *`yourdomainname`* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.
8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Ausgangsaudioumleitung aktivieren/deaktivieren.
10. Wählen Sie im Dialogfeld Ausgangsaudioumleitung aktivieren/deaktivieren die Option Aktiviert oder Deaktiviert aus.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

- Starten Sie den WorkSpace neu. Wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen > Neustart aus WorkSpaces.
- Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

So deaktivieren Sie die Zeitzonenumleitung für WSP

Standardmäßig ist die Zeit innerhalb eines Workspace so eingestellt, dass sie der Zeitzone des Clients entspricht, der für die Verbindung mit dem verwendet wird WorkSpace. Dieses Verhalten wird durch die Zeitzonenumleitung gesteuert. Vielleicht möchten Sie die Zeitzonenumleitung aus einem der folgenden Gründe deaktivieren. Beispielsweise:

- Ihr Unternehmen möchte, dass alle Mitarbeiter in einer bestimmten Zeitzone arbeiten (auch wenn sich einige Mitarbeiter in anderen Zeitzonen befinden).
- Sie haben Aufgaben in einem geplant WorkSpace , die zu einer bestimmten Zeit in einer bestimmten Zeitzone ausgeführt werden sollen.
- Ihre Benutzer, die viel reisen, möchten aus Konsistenzgründen und persönlichen Vorlieben ihre WorkSpaces Zeitzone beibehalten.

Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

Um die Zeitzonenumleitung für Windows zu deaktivieren WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Zeitzonenumleitung aktivieren/deaktivieren.
10. Wählen Sie im Dialogfeld Zeitzonenumleitung aktivieren/deaktivieren die Option Deaktiviert aus.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.
13. Stellen Sie die Zeitzone für die WorkSpaces auf die gewünschte Zeitzone ein.

Die Zeitzone von WorkSpaces ist jetzt statisch und spiegelt nicht mehr die Zeitzone der Client-Computer wider.

Konfigurieren von WSP-Sicherheitseinstellungen

Bei WSP werden Daten während der Übertragung mit der TLS-1.2-Verschlüsselung verschlüsselt. Standardmäßig sind alle der folgenden Verschlüsselungen zulässig. Client und Server handeln aus, welche Verschlüsselung verwendet werden soll:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256

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

Unter Windows können Sie Gruppenrichtlinieneinstellungen verwenden WorkSpaces, um den TLS-Sicherheitsmodus zu ändern und neue Verschlüsselungssammlungen hinzuzufügen oder bestimmte Verschlüsselungssammlungen zu blockieren. Eine ausführliche Erläuterung dieser Einstellungen und der unterstützten Verschlüsselungs-Suites finden Sie im Dialogfeld Gruppenrichtlinie-Sicherheitseinstellungen konfigurieren.

So konfigurieren Sie WSP-Sicherheitseinstellungen

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr Verzeichnis installiert ist. WorkSpaces
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN. z. B. `example.com`.
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit

yourdomainname finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie Sicherheitseinstellungen konfigurieren.
10. Wählen Sie im Dialogfeld Sicherheitseinstellungen konfigurieren die Option Aktiviert aus. Fügen Sie Verschlüsselungs-Suites hinzu, die Sie zulassen möchten. Entfernen Sie Verschlüsselungs-Suites, die Sie blockieren möchten. Weitere Informationen zu diesen Einstellungen finden Sie in den Beschreibungen im Dialogfeld Sicherheitseinstellungen konfigurieren.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für und nach dem Neustart der WorkSpace Sitzung wirksam. WorkSpace Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
    - Um den neu zu starten WorkSpace, wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces.
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Konfigurieren von Erweiterungen für WSP

Standardmäßig ist die Unterstützung für WorkSpaces Erweiterungen deaktiviert. Bei Bedarf können Sie Ihre Einstellungen WorkSpace für die Verwendung von Erweiterungen auf folgende Weise konfigurieren:

- Server und Client – Aktivieren von Erweiterungen für Server und Clients
- Nur Server – Erweiterungen nur für Server aktivieren
- Nur Client – Erweiterungen nur für Clients aktivieren

Für Windows WorkSpaces können Sie Gruppenrichtlinieneinstellungen verwenden, um die Verwendung von Erweiterungen zu konfigurieren.

So konfigurieren Sie Erweiterungen für WSP

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN. Beispiel: `example.com`
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.
8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Erweiterungen konfigurieren.
10. Wählen Sie im Dialogfeld Erweiterungen konfigurieren die Option Aktiviert aus und legen Sie dann die gewünschte Supportoption fest. Wählen Sie Nur Client, Server und Client oder Nur Server aus.
11. Wählen Sie OK aus.

12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie den neu WorkSpace. Wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und anschließend Aktionen, Neustart aus WorkSpaces.
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren oder Deaktivieren der Smartcard-Umleitung für WSP

Standardmäßig unterstützt Amazon weder WorkSpaces die Verwendung von Smartcards für die Authentifizierung vor der Sitzung noch für die Authentifizierung während der Sitzung. Die Authentifizierung vor der Sitzung bezieht sich auf die Smartcard-Authentifizierung, die durchgeführt wird, während sich Benutzer bei ihrem anmelden. WorkSpaces Die Authentifizierung während der Sitzung bezieht sich auf die Authentifizierung, die durchgeführt wird, nachdem Sie sich angemeldet haben.

Bei Bedarf können Sie die Authentifizierung vor und während der Sitzung für Windows WorkSpaces mithilfe der Gruppenrichtlinieneinstellungen aktivieren. Die Authentifizierung vor der Sitzung muss auch über Ihre AD Connector Connector-Verzeichniseinstellungen mithilfe der EnableClientAuthentication API-Aktion oder des enable-client-authentication AWS CLI Befehls aktiviert werden. Weitere Informationen finden Sie unter Aktivieren der Smartcard-Authentifizierung für AD Connector im AWS Directory Service -Administratorhandbuch.

> **Note**
>
> Um die Verwendung von Smartcards mit Windows zu ermöglichen WorkSpaces, sind zusätzliche Schritte erforderlich. Weitere Informationen finden Sie unter Verwenden von Smartcards zur Authentifizierung.

Um die Smartcard-Umleitung für Windows zu aktivieren oder zu deaktivieren WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.

2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *`yourdomainname`* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *`yourdomainname`* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Smartcard-Umleitung aktivieren/deaktivieren.
10. Wählen Sie im Dialogfeld Smartcard-Umleitung aktivieren/deaktivieren die Option Aktiviert oder Deaktiviert aus.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem Neustart der WorkSpace Sitzung wirksam. Um die Änderung der Gruppenrichtlinie zu übernehmen, starten Sie den neu WorkSpace (wählen Sie in der WorkSpaces WorkSpace Amazon-Konsole die und dann Aktionen, Neustart WorkSpaces).

Aktivieren oder deaktivieren Sie die WebAuthn (FIDO2) -Umleitung für WSP

Standardmäßig WorkSpaces aktiviert Amazon die Verwendung von WebAuthn Authentifikatoren für die Authentifizierung während der Sitzung. Die Authentifizierung während der Sitzung bezieht sich auf die WebAuthn Authentifizierung, die nach der Anmeldung durchgeführt und von den Webanwendungen angefordert wird, die in der Sitzung ausgeführt werden.

Voraussetzungen

WebAuthn Die (FIDO2) -Umleitung für WSP erfordert Folgendes:

- WSP-Hostagent Version 2.0.0.1425 oder höher
- WorkSpaces Kunden:
  - Linux Ubuntu 22.04 2023.3 oder höher
  - Windows 5.19.0 oder höher
  - Mac-Client 5.19.0 oder höher
- Webbrowser, die auf Ihrem Computer installiert sind, auf WorkSpaces dem die Amazon WebAuthn DCV-Umleitungserweiterung ausgeführt wird:
  - Google Chrome 116+
  - Microsoft Edge 116 oder höher

Aktivieren oder Deaktivieren der WebAuthn (FIDO2) -Umleitung für Windows WorkSpaces

Bei Bedarf können Sie die Unterstützung für die sitzungsinterne Authentifizierung mit WebAuthn Authentifikatoren für Windows WorkSpaces mithilfe der Gruppenrichtlinieneinstellungen aktivieren oder deaktivieren. Wenn Sie diese Einstellung aktivieren oder nicht konfigurieren, wird die WebAuthn Umleitung aktiviert und Benutzer können lokale Authentifikatoren innerhalb der Fernsteuerung verwenden. WorkSpace

Wenn die Funktion aktiviert ist, werden alle WebAuthn Anfragen vom Browser in der Sitzung an den lokalen Client umgeleitet. Benutzer können Windows Hello oder lokal angeschlossene Sicherheitsgeräte wie YubiKey oder andere FIDO2-konforme Authentifikatoren verwenden, um den Authentifizierungsprozess abzuschließen.

So aktivieren oder deaktivieren Sie die WebAuthn (FIDO2) -Umleitung für Windows WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr Verzeichnis installiert ist. WorkSpaces
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Umleitung aktivieren/deaktivieren WebAuthn .
10. Wählen Sie im Dialogfeld WebAuthn Umleitung aktivieren/deaktivieren die Option Aktiviert oder Deaktiviert aus.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem Neustart der WorkSpace Sitzung wirksam. Um die Änderungen an den Gruppenrichtlinien zu übernehmen, starten Sie den

neu, WorkSpace indem Sie zur WorkSpaces Amazon-Konsole gehen und die Option auswählen WorkSpace. Wählen Sie dann Aktionen, Neustart WorkSpaces).

Installation der Amazon WebAuthn DCV-Umleitungserweiterung

Benutzer müssen die Amazon DCV WebAuthn Redirection Extension installieren, um sie verwenden zu können, WebAuthn nachdem die Funktion aktiviert wurde. Gehen Sie dazu wie folgt vor:

- Ihre Benutzer werden aufgefordert, die Browsererweiterung in ihrem Browser zu aktivieren.

> **Note**
>
> Dies ist eine einmalige Browseraufforderung. Ihre Benutzer erhalten die Benachrichtigung, wenn Sie die WSP-Agent-Version auf 2.0.0.1425 oder höher aktualisieren. Wenn Ihre Endbenutzer die WebAuthn Umleitung nicht benötigen, können sie die Erweiterung einfach aus dem Browser entfernen. Sie können die Installationsaufforderung für die WebAuthn Umleitungserweiterung auch mithilfe der folgenden GPO-Richtlinie blockieren.

- Mithilfe der folgenden GPO-Richtlinie können Sie die Installation der Umleitungserweiterung für Ihre Benutzer erzwingen. Wenn Sie die GPO-Richtlinie aktivieren, wird die Erweiterung automatisch installiert, wenn Ihre Benutzer die unterstützten Browser mit Internetzugang starten.
- Ihre Benutzer können die Erweiterung manuell mit Microsoft Edge-Add-Ons oder dem Chrome Web Store installieren.

Verwalten und installieren Sie die Browsererweiterung mithilfe von Gruppenrichtlinien

Sie können die Amazon WebAuthn DCV-Umleitungserweiterung mithilfe von Gruppenrichtlinien installieren, entweder zentral von Ihrer Domain aus für Sitzungshosts, die zu einer Active Directory (AD) -Domäne gehören, oder mithilfe des Local Group Policy Editors für jeden Sitzungshost. Dieser Vorgang ändert sich je nachdem, welchen Browser Sie verwenden.

Für Microsoft Edge

1. Laden Sie die administrative Microsoft Edge-Vorlage herunter und installieren Sie sie.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).

4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.
8. Wählen Sie Computerkonfiguration, administrative Vorlagen, Microsoft Edge und Erweiterungen
9. Öffnen Sie Configure Extension Management Settings und setzen Sie die Option auf Aktiviert.
10. Geben Sie unter Einstellungen für die Erweiterungsverwaltung konfigurieren Folgendes ein:

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem WorkSpace Neustart der Sitzung wirksam. Um die Änderungen an den Gruppenrichtlinien zu übernehmen, starten Sie den neu, WorkSpace indem Sie zur WorkSpaces Amazon-Konsole gehen und die Option auswählen WorkSpace. Wählen Sie dann Aktionen, Neustart WorkSpaces).

> **Note**
>
> Sie können die Installation der Erweiterung blockieren, indem Sie die folgende Konfigurationsverwaltungseinstellung anwenden:
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

Für Google Chrome

1. Laden Sie die administrative Vorlage für Google Chrome herunter und installieren Sie sie. Weitere Informationen finden Sie unter Chrome-Browserrichtlinien auf verwalteten PCs festlegen.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).

3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.
8. Wählen Sie Computerkonfiguration, Administrative Vorlagen, Google Chrome und Erweiterungen
9. Öffnen Sie Configure Extension Management Settings und setzen Sie die Option auf Aktiviert.
10. Geben Sie unter Einstellungen für die Erweiterungsverwaltung konfigurieren Folgendes ein:

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

11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem WorkSpace Neustart der Sitzung wirksam. Um die Änderungen an den Gruppenrichtlinien zu übernehmen, starten Sie den neu, WorkSpace indem Sie zur WorkSpaces Amazon-Konsole gehen und die Option auswählen WorkSpace. Wählen Sie dann Aktionen, Neustart WorkSpaces).

> **Note**
>
> Sie können die Installation der Erweiterung blockieren, indem Sie die folgende Konfigurationsverwaltungseinstellung anwenden:
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Aktivieren oder Deaktivieren des Trennens der Sitzung bei Bildschirmsperre für WSP

Bei Bedarf können Sie WorkSpaces Benutzersitzungen trennen, wenn der Windows-Sperrbildschirm erkannt wird. Um die Verbindung vom WorkSpaces Client aus wiederherzustellen, können sich Benutzer mit ihren Kennwörtern oder Smartcards authentifizieren, je nachdem, welcher Authentifizierungstyp für sie aktiviert wurde. WorkSpaces

Diese Gruppenrichtlinieneinstellung ist standardmäßig deaktiviert. Bei Bedarf können Sie mithilfe der Gruppenrichtlinieneinstellungen das Trennen der Sitzung aktivieren, wenn der Windows-Sperrbildschirm für Windows WorkSpaces erkannt wird.

> **Note**
>
> - Diese Gruppenrichtlinieneinstellung gilt sowohl für Sitzungen mit Passwortauthentifizierung als auch für Sitzungen mit Smartcard-Authentifizierung.
> - Um die Verwendung von Smartcards mit Windows zu ermöglichen WorkSpaces, sind zusätzliche Schritte erforderlich. Weitere Informationen finden Sie unter Verwenden von Smartcards zur Authentifizierung.

So aktivieren oder deaktivieren Sie die Sitzungsunterbrechung mit der Bildschirmsperre für Windows WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain

erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Trennen der Sitzung bei Bildschirmsperre aktivieren/deaktivieren.
10. Wählen Sie im Dialogfeld Sitzung trennen bei Bildschirmsperre aktivieren/deaktivieren die Option Aktiviert oder Deaktiviert aus.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren oder deaktivieren Sie den Indirect Display Driver (IDD) für WSP

WorkSpaces Unterstützt standardmäßig die Verwendung des Indirect Display Driver (IDD). Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

So aktivieren oder deaktivieren Sie den Indirect Display Driver (IDD) für Windows WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon Elastic Compute Cloud-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Forest:FQDN).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.

7. Wählen Sie Standard-Domänenrichtlinie aus, öffnen Sie den Kontext, indem Sie mit der rechten Maustaste auf das Menü klicken, und wählen Sie Bearbeiten.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS verwaltetes Microsoft AD-Verzeichnis handelt, können Sie die Standarddomänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die `yourdomainname` Organisationseinheit (OU) oder eine beliebige Organisationseinheit unter diesem Domänennamen aus, öffnen Sie den Kontext, indem Sie mit der rechten Maustaste auf das Menü klicken, und wählen Sie Gruppenrichtlinienobjekt in dieser Domäne erstellen und hier verknüpfen aus. Weitere Informationen zur `yourdomainname` Organisationseinheit finden Sie unter What Gets Created im AWS Directory Service Administration Guide.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Treiber für AWS indirekte Displays aktivieren.
10. Wählen Sie im Dialogfeld „Treiber für AWS indirekte Bildschirme aktivieren“ die Option „Aktiviert“ oder „Deaktiviert“.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem WorkSpace Neustart der Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    a. Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Konsole das WorkSpace und dann Aktionen, Neustart WorkSpaces).

    b. Geben Sie in einer administrativen Eingabeaufforderung `gpupdate /force` ein.

Konfigurieren der Anzeigeeinstellungen für WSP

WorkSpaces ermöglicht es Ihnen, verschiedene Anzeigeeinstellungen zu konfigurieren, darunter die maximale Bildrate, die minimale Bildqualität, die maximale Bildqualität und die YUV-Kodierung. Passen Sie diese Einstellungen an die von Ihnen benötigte Bildqualität, Reaktionsgeschwindigkeit und Farbgenauigkeit an.

Standardmäßig beträgt der Wert für die maximale Bildrate 25. Der Wert für die maximale Bildrate gibt die maximal zulässige Anzahl von Bildern pro Sekunde (FPS) an. Bei 0 ist die Bildrate unbegrenzt.

Standardmäßig ist der Wert für die Mindestbildqualität 30. Die Mindestbildqualität kann für die beste Reaktionsgeschwindigkeit oder die beste Bildqualität optimiert werden. Reduzieren Sie die Mindestqualität, um eine optimale Reaktionsgeschwindigkeit zu erzielen. Erhöhen Sie die Mindestqualität, um die beste Qualität zu erzielen.

- Ideale Werte für die beste Reaktionsgeschwindigkeit liegen zwischen 30 und 90.
- Ideale Werte für die beste Qualität liegen zwischen 60 und 90.

Standardmäßig ist der Wert für die maximale Bildqualität 80. Die maximale Bildqualität hat keinen Einfluss auf die Reaktionsgeschwindigkeit oder Qualität des Bilds, legt jedoch einen Höchstwert fest, um die Netzwerknutzung zu begrenzen.

Standardmäßig ist die Bildkodierung auf YUV420 eingestellt. Wenn Sie YUV444-Kodierung aktivieren auswählen, wird die YUV444-Kodierung für eine hohe Farbgenauigkeit aktiviert.

Unter Windows WorkSpaces können Sie mithilfe von Gruppenrichtlinieneinstellungen die Werte für maximale Bildrate, minimale Bildqualität und maximale Bildqualität konfigurieren.

So konfigurieren Sie die Anzeigeeinstellungen für Windows WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *yourdomainname* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *yourdomainname* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Anzeigeeinstellungen konfigurieren.
10. Wählen Sie im Dialogfeld Anzeigeeinstellungen konfigurieren die Option Aktiviert aus und legen Sie dann die Werte für Maximale Bildrate (FPS), Minimale Bildqualität und Maximale Bildqualität auf die gewünschten Werte fest.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie die WorkSpace WorkSpaces Amazon-Konsole neu, wählen Sie die WorkSpace und dann Aktionen, Neustart WorkSpaces
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren oder deaktivieren Sie VSync für den AWS Virtual Display-Only Driver für WSP

WorkSpaces Unterstützt standardmäßig die Verwendung der VSync-Funktion für den Virtual Display-Only Driver. AWS Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

Um VSync für Windows zu aktivieren oder zu deaktivieren WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis installiert ist.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon Elastic Compute Cloud-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Forest:FQDN).
4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN (z. B. `example.com`).
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domänenrichtlinie aus, öffnen Sie den Kontext, indem Sie mit der rechten Maustaste auf das Menü klicken, und wählen Sie Bearbeiten.

   > **Note**
   >
   > Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS verwaltetes Microsoft AD-Verzeichnis handelt, können Sie die Standarddomänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die `yourdomainname` Organisationseinheit (OU) oder eine beliebige Organisationseinheit unter diesem Domänennamen aus, öffnen Sie den Kontext, indem Sie mit der rechten Maustaste auf das Menü klicken, und wählen Sie Gruppenrichtlinienobjekt in dieser Domäne erstellen und hier verknüpfen aus. Weitere Informationen zur `yourdomainname` Organisationseinheit finden Sie unter Was wird erstellt im AWS Directory Service Administration Guide.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Funktion „VSync aktivieren“ in der Einstellung „Treiber nur AWS virtueller Bildschirm“.
10. Wählen Sie im Dialogfeld „Treiber nur AWS virtueller Bildschirm“ unter „VSync aktivieren“ die Option „Aktiviert“ oder „Deaktiviert“.
11. Wählen Sie OK aus.

12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Gehen Sie wie folgt vor, um die Gruppenrichtlinienänderungen zu übernehmen:

    a. Starten Sie das neu, WorkSpace indem Sie einen der folgenden Schritte ausführen:

        i. Option 1 — Wählen Sie in der WorkSpaces Konsole die aus, die WorkSpace Sie neu starten möchten. Wählen Sie dann Aktionen, Neustart WorkSpaces.

        ii. Option 2 — Geben Sie in einer administrativen Befehlszeile ein`gpupdate /force`.

    b. Stellen Sie erneut eine Verbindung mit WorkSpace dem her, um die Einstellung zu übernehmen.

    c. Starten Sie den Workspace erneut neu.

Konfigurieren der Ausführlichkeit der Protokolle für WSP

Standardmäßig ist die Protokoll-Ausführlichkeitsstufe für WSP WorkSpaces auf Info festgelegt. Sie können die Protokollstufen auf Ausführlichkeitsstufen festlegen, die von der geringsten bis zur ausführlichsten Beschreibung reichen, wie hier beschrieben:

- Fehler: am wenigsten ausführlich
- Warnung
- Info: Standard
- Debug: am ausführlichsten

Unter Windows können Sie die Gruppenrichtlinieneinstellungen verwenden WorkSpaces, um die Ausführlichkeitsstufen der Protokolle zu konfigurieren.

So konfigurieren Sie die Ausführlichkeitsstufen der Protokolle für Windows WorkSpaces

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für WSP im zentralen Speicher des Domänencontrollers für Ihr Verzeichnis installiert ist. WorkSpaces
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
3. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).

4. Erweitern Sie Domains.
5. Erweitern Sie Ihren FQDN. z. B. `example.com`.
6. Erweitern Sie Gruppenrichtlinienobjekte.
7. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Wählen Sie stattdessen die OU *`yourdomainname`* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus. Weitere Informationen zur Organisationseinheit *`yourdomainname`* finden Sie unter Was wird erstellt im AWS Directory Service - Administratorhandbuch.

8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Computerkonfiguration, Richtlinien, Administrative Vorlagen, Amazon und WSP aus.
9. Öffnen Sie die Einstellung Protokollausführlichkeitsstufe konfigurieren.
10. Wählen Sie im Dialogfeld Protokollausführlichkeitsstufe konfigurieren die Option Aktiviert aus und legen Sie dann die Protokollausführlichkeitsstufe auf Debug, Fehler, Info oder Warnung fest.
11. Wählen Sie OK aus.
12. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie den neu WorkSpace. Wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und anschließend Aktionen, Neustart aus WorkSpaces.
    - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Installieren der administrativen Gruppenrichtlinienvorlage für PCoIP

Um die für Amazon spezifischen Gruppenrichtlinieneinstellungen WorkSpaces bei der Verwendung des PCoIP-Protokolls zu verwenden, müssen Sie die administrative Gruppenrichtlinienvorlage

hinzufügen, die für die Version des PCoIP-Agenten (entweder 32-Bit oder 64-Bit) geeignet ist, die für Sie verwendet wird. WorkSpaces

> **Note**
>
> Wenn Sie eine Mischung aus 32-Bit- und 64-Bit-Agenten verwenden, können Sie die administrativen Gruppenrichtlinienvorlagen für 32-Bit-Agenten verwenden. Ihre Gruppenrichtlinieneinstellungen werden dann sowohl auf 32-Bit- als auch auf 64-Bit-Agenten angewendet. WorkSpaces Wenn Sie alle den WorkSpaces 64-Bit-Agenten verwenden, können Sie zur Verwendung der administrativen Vorlage für 64-Bit-Agenten wechseln.

Um festzustellen, ob Sie den 32-Bit-Agent oder den 64-Bit-Agenten WorkSpaces haben

1. Melden Sie sich bei einem an und öffnen Sie dann den Task-Manager WorkSpace, indem Sie Ansicht, Senden, Strg + Alt + Löschen wählen oder mit der rechten Maustaste auf die Taskleiste klicken und Task-Manager wählen.
2. Gehen Sie im Task-Manager zur Registerkarte Details, klicken Sie mit der rechten Maustaste auf die Spaltenüberschriften und wählen Sie Spalten auswählen aus.
3. Wählen Sie im Dialogfeld Spalten auswählen die Option Plattform und anschließend OK aus.
4. Suchen Sie auf der Registerkarte Details nach dem Wert in der Spalte Plattform und überprüfen Sie dann, ob es sich bei dem PCoIP-Agent um eine 32-Bit- oder 64-Bit-Version handelt. (Möglicherweise sehen Sie eine Mischung aus 32-Bit- und WorkSpaces 64-Bit-Komponenten. Das ist normal.)

Installieren der administrativen Gruppenrichtlinienvorlage für PCoIP (32-Bit)

Um die Gruppenrichtlinieneinstellungen zu verwenden, die für die WorkSpaces Verwendung des PCoIP-Protokolls mit dem 32-Bit-PCoIP-Agent spezifisch sind, müssen Sie die administrative Gruppenrichtlinienvorlage für PCoIP installieren. Führen Sie das folgende Verfahren für eine Verzeichnisverwaltung WorkSpace oder Amazon EC2 EC2-Instance aus, die mit Ihrem Verzeichnis verknüpft ist.

Weitere Informationen zum Arbeiten mit ADM-Dateien finden Sie in der Microsoft-Dokumentation unter Empfehlungen für die Verwaltung administrativer Gruppenrichtlinienvorlagendateien (.adm).

Installieren der administrativen Gruppenrichtlinienvorlage für PCoIP

1. Erstellen Sie von einem laufenden Windows WorkSpace aus eine Kopie der `pcoip.adm` Datei im `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` Verzeichnis.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu der Organisationseinheit in Ihrer Domain, die Ihre WorkSpaces Computerkonten enthält.
3. Öffnen Sie das Kontextmenü (rechte Maustaste) für die Organisationseinheit des Computer-Kontos und klicken Sie auf Ein Gruppenrichtlinienobjekt in dieser Domain erstellen und verknüpfen.
4. Geben Sie im Dialogfeld Neues Gruppenrichtlinienobjekt einen aussagekräftigen Namen für das Gruppenrichtlinienobjekt ein, z. B. WorkSpaces Maschinenrichtlinien, und lassen Sie Source Starter GPO auf (none) eingestellt. Wählen Sie OK aus.
5. Öffnen Sie das Kontextmenü (rechte Maustaste) für das neue GPO und wählen Sie Edit (Bearbeiten).
6. Klicken Sie im Gruppenrichtlinien-Editor auf Computerkonfiguration, Richtlinien und Administrative Vorlagen. Klicken Sie im Hauptmenü auf Aktion, Vorlagen hinzufügen/entfernen.
7. Klicken Sie im Dialogfeld Vorlagen hinzufügen/entfernen auf Hinzufügen, wählen Sie die `pcoip.adm` vorher kopierte Datei aus und klicken Sie dann auf Öffnen, Schließen.
8. Schließen Sie den Gruppenrichtlinien-Verwaltungseditor. Sie können dieses Gruppenrichtlinienobjekt jetzt verwenden, um die Gruppenrichtlinieneinstellungen zu ändern, die spezifisch für sind. WorkSpaces

So überprüfen Sie, ob die administrative Vorlagendatei korrekt installiert ist

1. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zum WorkSpaces GPO für Ihre WorkSpaces Computerkonten und wählen Sie es aus. Klicken Sie im Hauptmenü auf Aktion,Bearbeiten.
2. Klicken Sie im Gruppenrichtlinienverwaltungseditor auf Computerkonfiguration, Richtlinien, Administrative Vorlagen, Klassische administrative Vorlagen und PCoIP Sitzungsvariablen.
3. Sie können jetzt dieses Gruppenrichtlinienobjekt für PCoIP-Sitzungsvariablen verwenden, um die für Amazon spezifischen Gruppenrichtlinieneinstellungen zu ändern, WorkSpaces wenn Sie PCoIP verwenden.

> **Note**
>
> Wählen Sie Überschreibbare Administrationsstandwerte aus, um den Benutzern zu ermöglichen, Ihre Einstellung außer Kraft zu setzen. Andernfalls wählen Sie Nicht überschreibbare Administrationsstandardwerte aus.

Installieren der administrativen Gruppenrichtlinienvorlage für PCoIP (64-Bit)

Um die Gruppenrichtlinieneinstellungen zu verwenden, die für die WorkSpaces Verwendung des PCoIP-Protokolls spezifisch sind, müssen Sie die administrative Gruppenrichtlinienvorlage `PCoIP.admx` und die `PCoIP.adml` Dateien für PCoIP zum zentralen Speicher des Domänencontrollers für Ihr Verzeichnis hinzufügen. WorkSpaces Weitere Informationen zu `.admx`- und `.adml`-Dateien finden Sie in der Microsoft-Dokumentation unter So erstellen und verwalten Sie den zentralen Speicher für administrative Gruppenrichtlinienvorlagen in Windows.

Das folgende Verfahren erläutert, wie Sie den zentralen Speicher erstellen und ihm die administrativen Vorlagendateien hinzufügen. Führen Sie das folgende Verfahren für eine Verzeichnisverwaltung WorkSpace oder Amazon EC2 EC2-Instance aus, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist.

Installieren der administrativen Gruppenrichtlinienvorlagendatei für PCoIP

1. Erstellen Sie von einem laufenden Windows WorkSpace aus eine Kopie der `PCoIP.adml` Dateien `PCoIP.admx` und im `C:\Program Files\Teradici\PCoIP Agent \configuration\policyDefinitions` Verzeichnis. Die `PCoIP.adml`-Datei befindet sich im Unterordner `en-US` dieses Verzeichnisses.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, den Windows-Datei-Explorer und geben Sie in der Adressleiste den vollqualifizierten Domainnamen (FQDN) Ihrer Organisation ein, z. B. `\ \example.com`
3. Öffnen Sie das Verzeichnis `sysvol`.
4. Öffnen Sie den Ordner mit dem Namen *FQDN*.
5. Öffnen Sie das Verzeichnis `Policies`. Sie sollten sich jetzt in `\\`*FQDN*`\sysvol \`*FQDN*`\Policies` befinden.

6. Wenn er noch nicht vorhanden ist, erstellen Sie einen Ordner mit dem Namen `PolicyDefinitions`.
7. Öffnen Sie das Verzeichnis `PolicyDefinitions`.
8. Kopieren Sie die Datei `PCoIP.admx` in den Ordner `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions`.
9. Erstellen Sie einen Ordner mit dem Namen `en-US` im Ordner `PolicyDefinitions`.
10. Öffnen Sie das Verzeichnis `en-US`.
11. Kopieren Sie die Datei `PCoIP.adml` in den Ordner `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`.

So überprüfen Sie, ob die administrativen Vorlagendateien korrekt installiert sind

1. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
2. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
3. Erweitern Sie Domains.
4. Erweitern Sie Ihren FQDN (z. B. `example.com`).
5. Erweitern Sie Gruppenrichtlinienobjekte.
6. Wählen Sie Standard-Domain-Richtlinie aus, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie Bearbeiten aus.

> **Note**
>
> Wenn es sich bei der Domäne, hinter der das WorkSpaces steht, um ein AWS Managed Microsoft AD Verzeichnis handelt, können Sie die Standard-Domänenrichtlinie nicht verwenden, um Ihr GPO zu erstellen. Stattdessen müssen Sie das Gruppenrichtlinienobjekt unter dem Domain-Container mit delegierten Rechten erstellen und verknüpfen.
> Wenn Sie ein Verzeichnis mit erstellen AWS Managed Microsoft AD, AWS Directory Service erstellt eine Organisationseinheit (OU) für *`Ihren Domainnamen`* unter dem Domänenstamm. Der Name dieser Organisationseinheit basiert auf dem NetBIOS-Namen, den Sie eingegeben haben, als Sie Ihr Verzeichnis erstellt haben. Wenn Sie keinen NetBIOS-Namen angegeben haben, wird dieser standardmäßig auf den ersten

Teil Ihres Verzeichnis-DNS-Namens gesetzt (im Falle von `corp.example.com` wäre der NetBIOS-Name z. B. `corp`).
Wählen Sie statt Standard-Domain-Richtlinie die Organisationseinheit *`yourdomainname`* (oder eine beliebige Organisationseinheit unter dieser) aus, öffnen Sie das Kontextmenü (klicken Sie mit der rechten Maustaste) und wählen Sie Gruppenrichtlinienobjekt in dieser Domain erstellen und hier verknüpfen aus, um Ihr Gruppenrichtlinienobjekt zu erstellen.
Weitere Informationen zur Organisationseinheit *`yourdomainname`* finden Sie unter Was wird erstellt im AWS Directory Service -Administratorhandbuch.

7. Klicken Sie im Gruppenrichtlinien-Verwaltungseditor auf Computerkonfiguration, Richtlinien, Administrative Vorlagen und PCoIP Sitzungsvariablen.
8. Sie können jetzt dieses Gruppenrichtlinienobjekt für PCoIP-Sitzungsvariablen verwenden, um die Gruppenrichtlinieneinstellungen zu ändern, die für die Verwendung von PCoIP spezifisch sind. WorkSpaces

> **Note**
>
> Wählen Sie Überschreibbare Administrationsstandwerte aus, um den Benutzern zu ermöglichen, Ihre Einstellung außer Kraft zu setzen. Andernfalls wählen Sie Nicht überschreibbare Administrationsstandardwerte aus.

Gruppenrichtlinieneinstellungen für PCoIP verwalten

Verwenden Sie Gruppenrichtlinieneinstellungen, um Ihr Windows zu verwalten WorkSpaces , das PCoIP verwendet.

Konfigurieren der Druckerunterstützung für PCoIP

Standardmäßig WorkSpaces aktiviert Basic Remote Printing, das eingeschränkte Druckmöglichkeiten bietet, da es einen generischen Druckertreiber auf der Hostseite verwendet, um kompatibles Drucken zu gewährleisten.

Mit Advanced Remote-Drucken für Windows-Clients können Sie bestimmte Funktionen Ihres Druckers verwenden, z. B. doppelseitiges Drucken. Es ist jedoch eine Installation des passenden Druckertreibers auf der Hostseite erforderlich.

Remote-Drucken wird als virtueller Kanal implementiert. Wenn virtuelle Kanäle deaktiviert sind, funktioniert das Remote-Drucken nicht.

Unter Windows WorkSpaces können Sie die Druckerunterstützung mithilfe der Gruppenrichtlinieneinstellungen nach Bedarf konfigurieren.

Konfigurieren des Druckersupports

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung Konfigurieren von Remote-Drucken.
4. Führen Sie im Dialogfeld Configure remote printing (Remote-Drucken konfigurieren) einen der folgenden Schritte aus:
   - Um Advanced Remote-Drucken zu aktivieren, wählen Sie Enabled (Aktiviert) und dann unter Options (Optionen), Configure remote printing (Remote-Drucken konfigurieren) die Option Basic and Advanced printing for Windows clients (Basic- und Advanced-Drucken für Windows-Clients) aus. Um den aktuellen Standarddrucker des Client-Computers automatisch zu verwenden, wählen Sie Automatically set default printer (Standarddrucker automatisch festlegen) aus.
   - Um das Drucken zu deaktivieren, wählen Sie Enabled (Aktiviert) und dann unter Options (Optionen), Configure remote printing (Remote-Drucken konfigurieren) die Option Printing disabled (Drucken deaktiviert) aus.
5. Wählen Sie OK aus.
6. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Standardmäßig ist die automatische Umleitung eines lokalen Druckers deaktiviert. Sie können diese Funktion mithilfe der Gruppenrichtlinieneinstellungen aktivieren, sodass Ihr lokaler Drucker jedes Mal, wenn Sie eine Verbindung zu Ihrem herstellen, als Standarddrucker festgelegt wird WorkSpace.

> **Note**
>
> Die lokale Druckerumleitung ist für Amazon Linux WorkSpaces nicht verfügbar.

So aktivieren Sie die automatische Umleitung eines lokalen Druckers

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinien-Vorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinien-Vorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung Konfigurieren von Remote-Drucken.
4. Wählen Sie Aktiviert aus und wählen Sie dann unter Optionen, Remotedruck konfigurieren eine der folgenden Optionen aus:
   - Grundlegendes und erweitertes Drucken für Windows-Clients
   - Grundlegendes Drucken
5. Wählen Sie Automatisch als Standarddrucker festlegen und anschließend OK aus.
6. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

So aktivieren oder deaktivieren Sie die Zwischenablageumleitung für PCoIP

WorkSpaces Unterstützt standardmäßig die Zwischenablage-Umleitung. Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

So aktivieren oder deaktivieren Sie die Zwischenablageumleitung

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung Konfigurieren von Zwischenablagen-Umleitung.
4. Wählen Sie im Dialogfeld Configure clipboard redirection (Konfigurieren von Zwischenablagen-Umleitung) den Wert Aktiviert aus und wählen Sie dann eine der folgenden Einstellungen aus, um die Richtung festzulegen, in welche die Zwischenablagen-Umleitung zulässig ist. Wählen Sie OK, wenn Sie damit fertig sind.

   - Deaktiviert in beide Richtungen
   - Nur Agent für Client aktiviert (WorkSpace für lokalen Computer)
   - Nur Client-zu-Agent aktiviert (lokaler Computer für WorkSpace)
   - Aktiviert in beide Richtungen
5. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem WorkSpace Neustart der Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Bekannte Einschränkung

Wenn Sie Inhalte WorkSpace, die größer als 890 KB sind, aus einer Microsoft Office-Anwendung kopieren, wird die Anwendung möglicherweise langsam oder reagiert für bis zu 5 Sekunden nicht mehr, wenn Sie die Zwischenablageumleitung aktivieren.

Timeout für die Wiederaufnahme der Sitzung für PCoIP festlegen

Wenn Sie die Netzwerkverbindung verlieren, wird Ihre aktive WorkSpaces Clientsitzung unterbrochen. WorkSpaces Client-Anwendungen für Windows und macOS versuchen, die Sitzung

automatisch wieder zu verbinden, wenn die Netzwerkkonnektivität innerhalb einer bestimmten Zeit wiederhergestellt wird. Das standardmäßige Timeout für die Wiederaufnahme der Sitzung beträgt 20 Minuten. Sie können diesen Wert jedoch so ändern WorkSpaces , dass er von den Gruppenrichtlinieneinstellungen Ihrer Domäne gesteuert wird.

So legen Sie den Wert für die automatische Sitzungszeitbeschränkung fest

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung Konfigurieren von automatischer Wiederverbindungs-Richtlinie .
4. Klicken Sie im Dialogfeld Automatische Sitzungs-Neuverbindungs-Richtlinie auf Aktivieren, legen Sie die OptionKonfigurieren der automatischen Sitzungs-Neuverbindungs-Richtlinie auf das gewünschte Timeout in Minuten fest und klicken Sie auf OK.
5. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren oder Deaktivieren der Zwischenablageumleitung für PCoIP

Standardmäßig WorkSpaces unterstützt Amazon die Umleitung von Daten von einem lokalen Mikrofon. Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

> **Note**
>
> Wenn Sie über eine Gruppenrichtlinieneinstellung verfügen, die die lokale Anmeldung von Benutzern in ihren Geräten einschränkt WorkSpaces, funktioniert die Audioeingabe auf Ihrem Computer nicht. WorkSpaces Wenn Sie diese Gruppenrichtlinieneinstellung entfernen,

wird die Audioeingabefunktion nach dem nächsten Neustart von aktiviert. WorkSpace Weitere Informationen zum Arbeiten mit dieser Gruppenrichtlinieneinstellung finden Sie in der Microsoft-Dokumentation unter Lokales Anmelden zulassen.

So aktivieren oder deaktivieren Sie die Zwischenablageumleitung

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung Audioeingabe in der PCoIP-Sitzung aktivieren/deaktivieren.
4. Wählen Sie im Dialogfeld Audioeingabe in der PCoIP-Sitzung aktivieren/deaktivieren die Option Aktiviert oder Deaktiviert aus.
5. Wählen Sie OK aus.
6. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

So deaktivieren Sie die Zeitzonenumleitung für PCoIP

Standardmäßig ist die Zeit innerhalb eines Workspace so eingestellt, dass sie der Zeitzone des Clients entspricht, der für die Verbindung mit dem verwendet wird WorkSpace. Dieses Verhalten wird durch die Zeitzonenumleitung gesteuert. Vielleicht möchten Sie die Zeitzonenumleitung aus einem der folgenden Gründe deaktivieren:

- Ihr Unternehmen möchte, dass alle Mitarbeiter in einer bestimmten Zeitzone arbeiten (auch wenn sich einige Mitarbeiter in anderen Zeitzonen befinden).

- Sie haben Aufgaben in einem geplant WorkSpace , die zu einer bestimmten Zeit in einer bestimmten Zeitzone ausgeführt werden sollen.
- Ihre Benutzer, die viel reisen, möchten aus Konsistenzgründen und persönlichen Vorlieben ihre WorkSpaces Zeitzone beibehalten.

Falls für Windows erforderlich WorkSpaces, können Sie diese Funktion mithilfe der Gruppenrichtlinieneinstellungen deaktivieren.

So deaktivieren Sie die Zeitzonenumleitung

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung Zeitzonenumleitung konfigurieren.
4. Wählen Sie im Dialogfeld Zeitzonenumleitung konfigurieren die Option Deaktiviert aus.
5. Wählen Sie OK aus.
6. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.
7. Stellen Sie die Zeitzone für die WorkSpaces auf die gewünschte Zeitzone ein.

Die Zeitzone von WorkSpaces ist jetzt statisch und spiegelt nicht mehr die Zeitzone der Client-Computer wider.

Konfigurieren von PCoIP-Sicherheitseinstellungen

Bei PCoIP werden Daten während der Übertragung mit der TLS-1.2-Verschlüsselung und SigV4-Anforderungssignatur verschlüsselt. Das PCoIP-Protokoll verwendet verschlüsselten UDP-

Datenverkehr mit AES-Verschlüsselung für Streaming-Pixel. Die Streaming-Verbindung, die Port 4172 (TCP und UDP) verwendet, ist mit AES-128- und AES-256-Verschlüsselungen verschlüsselt, die Standardverschlüsselung ist jedoch 128-Bit. Sie können diese Standardeinstellung mithilfe der Gruppenrichtlinieneinstellung PCoIP-Sicherheitseinstellungen konfigurieren auf 256-Bit ändern.

Sie können diese Gruppenrichtlinieneinstellung auch verwenden, um den TLS-Sicherheitsmodus zu ändern und bestimmte Verschlüsselungs-Suites zu blockieren. Eine ausführliche Erläuterung dieser Einstellungen und der unterstützten Verschlüsselungs-Suites finden Sie im Dialogfeld Gruppenrichtlinie für PCoIP-Sicherheitseinstellungen konfigurieren.

So konfigurieren Sie PCoIP-Sicherheitseinstellungen

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung PCoIP-Sicherheitseinstellungen konfigurieren.
4. Wählen Sie im Dialogfeld PCoIP-Sicherheitseinstellungen konfigurieren die Option Aktiviert aus. Wechseln Sie zur Option PCoIP-Datenverschlüsselungen und wählen Sie nur AES-256-GCM aus, um die Standardverschlüsselung für Streaming-Datenverkehr auf 256-Bit festzulegen.
5. (Optional) Passen Sie die Einstellung für den TLS-Sicherheitsmodus an und listen Sie dann alle Verschlüsselungs-Suites auf, die Sie blockieren möchten. Weitere Informationen zu diesen Einstellungen finden Sie in den Beschreibungen im Dialogfeld PCoIP-Sicherheitseinstellungen konfigurieren.
6. Wählen Sie OK aus.
7. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Aktivieren Sie die USB-Umleitung für U2F YubiKey

> **Note**
>
> Amazon unterstützt WorkSpaces derzeit die USB-Umleitung nur für YubiKey U2F. Andere Arten von USB-Geräten werden möglicherweise umgeleitet, aber sie werden nicht unterstützt und funktionieren möglicherweise nicht richtig.

Um die USB-Umleitung für U2F zu aktivieren YubiKey

1. Stellen Sie sicher, dass Sie die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die neueste administrative WorkSpaces Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen.
3. Öffnen Sie die Einstellung USB in der PCoIP-Sitzung aktivieren/deaktivieren.
4. Wählen Sie Aktiviert und anschließend OK aus.
5. Öffnen Sie die Einstellung PCoIP-USB-Geräte für zulässige und unzulässige Geräte konfigurieren.
6. Wählen Sie Aktiviert aus und konfigurieren Sie unter USB-Autorisierungstabelle eingeben (maximal zehn Regeln) die Regeln für die Zulassungsliste Ihres USB-Geräts.

   - Autorisierungsregeln – 110500407. Dieser Wert ist eine Kombination aus einer Vendor-ID (VID) und einer Produkt-ID (PID). Das Format für eine VID/PID-Kombination ist 1xxxxyyyy, wobei xxxx die VID im Hexadezimalformat und yyyy die PID im Hexadezimalformat ist. In diesem Beispiel ist 1050 die VID und 0407 die PID. Weitere YubiKey USB-Werte finden Sie unter YubiKey USB-ID-Werte.
7. Konfigurieren Sie unter USB-Autorisierungstabelle eingeben (maximal zehn Regeln) die Regeln für die Zulassungsliste Ihres USB-Geräts.

   - Geben Sie für Nicht-autorisiert-Regel eine leere Zeichenfolge ein. Das bedeutet, dass nur USB-Geräte in der Autorisierungsliste zulässig sind.

   > **Note**

Sie können maximal 10 USB-Autorisierungsregeln und maximal 10 USB-Nicht-autorisiert-Regeln definieren. Verwenden Sie den senkrechten Strich (|), um mehrere Regeln voneinander zu trennen. Ausführliche Informationen zu den Regeln für die Autorisierung und Nicht-Autorisierung finden Sie unter Teradici PCoIP Standard Agent für Windows.

8. Wählen Sie OK aus.
9. Die Änderung der Gruppenrichtlinieneinstellungen wird nach dem nächsten Gruppenrichtlinien-Update für die Sitzung WorkSpace und nach dem WorkSpace Neustart der Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie in einer administrativen Eingabeaufforderung **`gpupdate /force`** ein.

Sobald die Einstellung wirksam wird, können alle unterstützten USB-Geräte umgeleitet werden, WorkSpaces sofern in den Einstellungen für USB-Geräteregeln keine Einschränkungen konfiguriert wurden.

Festlegen der maximalen Gültigkeitsdauer eines Kerberos-Tickets

Wenn Sie die Funktion „Angemeldet bleiben“ in Windows nicht deaktiviert haben WorkSpaces, können Ihre WorkSpace Benutzer in ihrer WorkSpaces Client-Anwendung das Kontrollkästchen „Angemeldet bleiben“ oder „Angemeldet bleiben“ verwenden, um ihre Anmeldeinformationen zu speichern. Mit dieser Funktion können Benutzer problemlos eine Verbindung zu ihren herstellen, WorkSpaces während die Client-Anwendung weiterhin ausgeführt wird. Ihre Anmeldeinformationen sind für die gesamte maximale Gültigkeitsdauer des Kerberos-Tickets sicher gespeichert.

Wenn Sie ein AD Connector Connector-Verzeichnis WorkSpace verwenden, können Sie die maximale Gültigkeitsdauer der Kerberos-Tickets für Ihre WorkSpaces Benutzer mithilfe von Gruppenrichtlinien ändern, indem Sie die Schritte unter Maximale Gültigkeitsdauer für ein Benutzerticket in der Microsoft Windows-Dokumentation befolgen.

Informationen zum Aktivieren oder Deaktivieren der Funktion Passwort speichern finden Sie unter Aktivieren von Self-Service-WorkSpace-Verwaltungsfunktionen für Ihre Benutzer.

Konfigurieren der Proxyservereinstellungen des Geräts für den Internetzugang

Standardmäßig verwenden die WorkSpaces Client-Anwendungen den Proxyserver, der in den Betriebssystemeinstellungen des Geräts für HTTPS-Verkehr (Port 443) angegeben ist. Die WorkSpaces Amazon-Client-Anwendungen verwenden den HTTPS-Port für Updates, Registrierung und Authentifizierung.

> **Note**
>
> Proxyserver, die eine Authentifizierung mit Anmeldeinformationen erfordern, werden nicht unterstützt.

Sie können die Geräteproxyservereinstellungen für Ihr Windows WorkSpaces mithilfe von Gruppenrichtlinien konfigurieren, indem Sie die Schritte unter Geräteproxy- und Internetverbindungseinstellungen konfigurieren in der Microsoft-Dokumentation befolgen.

Weitere Informationen zur Konfiguration der Proxyeinstellungen in der WorkSpaces Windows-Client-Anwendung finden Sie unter Proxy-Server im WorkSpaces Amazon-Benutzerhandbuch.

Weitere Informationen zur Konfiguration der Proxyeinstellungen in der WorkSpaces macOS-Client-Anwendung finden Sie unter Proxy-Server im WorkSpaces Amazon-Benutzerhandbuch.

Weitere Informationen zur Konfiguration der Proxyeinstellungen in der WorkSpaces Web Access-Client-Anwendung finden Sie unter Proxy-Server im WorkSpaces Amazon-Benutzerhandbuch.

Proxy für Desktop-Datenverkehr

Für PCoIP WorkSpaces unterstützen die Desktop-Client-Anwendungen weder die Verwendung eines Proxyservers noch die TLS-Entschlüsselung und Überprüfung von Port 4172-Verkehr in UDP (für Desktop-Verkehr). Sie benötigen eine direkte Verbindung mit dem Port 4172.

Für WSP WorkSpaces unterstützen die WorkSpaces Windows-Client-Anwendung (Version 5.1 und höher) und die macOS-Client-Anwendung (Version 5.4 und höher) die Verwendung von HTTP-Proxyservern für den TCP-Verkehr nach Port 4195. TLS-Entschlüsselung und -Inspektion werden nicht unterstützt.

WSP unterstützt nicht die Verwendung von Proxys für Desktop-Datenverkehr über UDP. Nur WorkSpaces Windows- und macOS-Desktop-Client-Anwendungen und WSP-Webzugriff unterstützen die Verwendung von Proxy für TCP-Verkehr.

> **Note**
>
> Wenn Sie sich für die Verwendung eines Proxyservers entscheiden, werden die API-Aufrufe, die die Client-Anwendung an die WorkSpaces Dienste sendet, ebenfalls per Proxy weitergeleitet. Sowohl API-Aufrufe als auch Desktop-Datenverkehr sollten über denselben Proxyserver geleitet werden.

Empfehlung zur Verwendung von Proxyservern

Wir empfehlen nicht, einen Proxyserver für Ihren WorkSpaces Desktop-Verkehr zu verwenden.

Der WorkSpaces Amazon-Desktop-Verkehr ist bereits verschlüsselt, sodass Proxys die Sicherheit nicht verbessern. Ein Proxy stellt einen zusätzlichen Hop im Netzwerkpfad dar, der die Streaming-Qualität durch Latenz beeinträchtigen könnte. Proxys könnten auch den Durchsatz verringern, wenn ein Proxy nicht die richtige Größe hat, um Desktop-Streaming-Datenverkehr zu verarbeiten. Darüber hinaus sind die meisten Proxys nicht für die Unterstützung von Verbindungen mit langer Laufzeit WebSocket (TCP) konzipiert und können die Streaming-Qualität und -Stabilität beeinträchtigen.

Wenn Sie einen Proxy verwenden müssen, platzieren Sie Ihren Proxyserver bitte so nah wie möglich am WorkSpace Client, vorzugsweise im selben Netzwerk, um eine zusätzliche Netzwerklatenz zu vermeiden, die sich negativ auf die Streaming-Qualität und Reaktionsfähigkeit auswirken könnte.

Amazon WorkSpaces für die Unterstützung des Zoom Meeting Media Plug-ins aktivieren

Benutzer mit Administratorrechten für Active Directory können mithilfe eines Gruppenrichtlinienobjekts (GPO) einen Registrierungsschlüssel generieren. Auf diese Weise kann der Benutzer den Registrierungsschlüssel mithilfe eines erzwungenen Updates an alle Windows WorkSpaces innerhalb Ihrer Domain senden. Alternativ können Kunden mit Administratorrechten die Registrierungsschlüssel auch einzeln auf ihrem WorkSpaces Host installieren.

Voraussetzungen für die Nutzung von Zoom für WorkSpaces

Unterstützte WorkSpaces Client-Version: Windows: 5.4.0.xxxx oder höher.

Erstellen Sie den Registrierungsschlüssel auf einem Windows-Host WorkSpaces

Gehen Sie wie folgt vor, um einen Registrierungsschlüssel auf einem WorkSpaces Windows-Host zu erstellen. Der Registrierungsschlüssel ist erforderlich, um Zoom unter Windows zu verwenden WorkSpaces.

1. Öffnen Sie den Windows-Registrierungseditor als Administrator.
2. Wechseln Sie zu `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. Wenn der Extension-Schlüssel nicht existiert, klicken Sie mit der rechten Maustaste, wählen Sie Neu > Schlüssel aus und nennen Sie ihn Extension.
4. Klicken Sie mit der rechten Maustaste auf den neuen Extension-Schlüssel, wählen Sie Neu > DWORD aus und nennen Sie ihn enable. Der Name muss in Kleinbuchstaben geschrieben sein.
5. Klicken Sie auf das neue DWORD-Element und ändern Sie den Wert auf 1.
6. Starten Sie den Computer neu, um den Vorgang abzuschließen.
7. Laden Sie auf Ihrem WorkSpaces Host den neuesten Zoom VDI-Client herunter und installieren Sie ihn. Laden Sie auf Ihrem WorkSpaces Client (5.4 oder höher) das neueste Zoom VDI-Client-Plugin für Amazon WorkSpaces herunter und installieren Sie es. Weitere Informationen finden Sie unter VDI-Versionen und -Downloads auf der Zoom-Support-Website.

Starten Sie Zoom, um Ihren Videoanruf zu starten.

Fehlerbehebung

Führen Sie die folgenden Aktionen aus, um Probleme mit Zoom unter Windows WorkSpaces zu beheben.

- Vergewissern Sie sich, dass die Aktivierung des Registrierungsschlüssels korrekt durchgeführt wurde.
- Wechseln Sie zu `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`. `wse_core_dll` sollte angezeigt werden.
- Stellen Sie sicher, dass die Versionen auf dem Host und den Clients korrekt und identisch sind.

Wenn Sie weiterhin Schwierigkeiten haben, wenden Sie sich AWS Support über das AWS Support Center an uns.

Sie können die folgenden Beispiele verwenden, um ein GPO als Administrator Ihres Verzeichnisses anzuwenden.

WSE.adml:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native GPO
 template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
```

```
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

Verwalten von Amazon Linux WorkSpaces

Wie bei Windows WorkSpaces sind auch Amazon Linux WorkSpacesdomänenverbunden, sodass Sie Active-Directory-Benutzer und -Gruppen verwenden können, um:

- Verwalten von Amazon Linux WorkSpaces
- Gewähren von Zugriff auf diejenigen WorkSpaces für Benutzer

Da Linux-Instances nicht der Gruppenrichtlinie entsprechen, empfehlen wir, dass Sie eine Konfigurationsverwaltungslösung verwenden, um Richtlinien zu verteilen und durchzusetzen. Sie können beispielsweise AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise oder Ansible verwenden.

> **Note**
>
> Die lokale Druckerumleitung ist für Amazon Linux nicht verfügbar WorkSpaces.

Control WorkSpaces Streaming Protocol (WSP)-Verhalten unter Amazon Linux WorkSpaces

Das Verhalten des PCoIP-Agents wird durch Konfigurationseinstellungen in der `wsp.conf`-Datei gesteuert, die sich im Verzeichnis `/etc/wsp/` befindet. Verwenden Sie eine Konfigurationsmanagement-Lösung, die Amazon-Linux unterstützt, um Gruppenrichtlinien bereitzustellen und Änderungen durchzusetzen. Alle Änderungen werden wirksam, sobald der Agent gestartet wird.

> **Note**
>
> - Wenn Sie falsche oder nicht unterstützte Änderungen an der `wsp.conf` Datei vornehmen, werden Richtlinienänderungen möglicherweise nicht auf die neu hergestellten Verbindungen in Ihrem angewendet WorkSpace.
> - Amazon-Linux WorkSpaces -on-WSP-Pakete haben derzeit die folgenden Einschränkungen:
>   - Derzeit nur in den AWS GovCloud (USA-West) und AWS GovCloud (USA-Ost) verfügbar.
>   - Videoeingang wird nicht unterstützt.
>   - Das Trennen der Sitzung bei der Bildschirmsperre wird nicht unterstützt.

In den folgenden Abschnitten wird die Aktivierung oder Deaktivierung bestimmter Funktionen beschrieben.

Konfigurieren der Zwischenablageumleitung für WSP Amazon Linux WorkSpaces

Standardmäßig WorkSpaces unterstützt die Zwischenablageumleitung. Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu konfigurieren. Diese Einstellung wird wirksam, wenn Sie die trennen und erneut verbinden WorkSpace.

So konfigurieren Sie die Zwischenablageumleitung für WSP Amazon Linux WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. ```
   clipboard = X
   ```

   Mögliche Werte für *X*:

   `enabled` – Die Zwischenablageumleitung ist in beide Richtungen aktiviert (Standard).

   `disabled` – Die Zwischenablageumleitung ist in beide Richtungen deaktiviert.

   `paste-only` – Die Zwischenablageumleitung ist aktiviert, ermöglicht Ihnen jedoch nur, Inhalte vom lokalen Client-Gerät zu kopieren und auf dem Remote-Host-Desktop einzufügen.

   `copy-only` – Die Zwischenablageumleitung ist aktiviert, ermöglicht Ihnen jedoch nur, Inhalte vom Remote-Host-Desktop zu kopieren und auf dem lokalen Client-Gerät einzufügen.

Aktivieren oder Deaktivieren der Audioeingangsumleitung für WSP Amazon Linux WorkSpaces

Standardmäßig WorkSpaces unterstützt die Audioeingangsumleitung. Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu deaktivieren. Diese Einstellung wird wirksam, wenn Sie die Verbindung zum trennen und erneut eine Verbindung zum herstellen WorkSpace.
   ```

So aktivieren oder deaktivieren Sie die Audioeingangsumleitung für WSP Amazon Linux WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der Datei hinzu.

   ```
   audio-in = X
   ```

   Mögliche Werte für *X*:

   `enabled` – Die Audioeingangsumleitung ist aktiviert (Standard).

   `disabled` – Die Audioeingangsumleitung ist deaktiviert.

Aktivieren oder Deaktivieren der Zeitzonenumleitung für WSP Amazon Linux WorkSpaces

Standardmäßig ist die Zeit innerhalb eines Workspace so eingestellt, dass sie die Zeitzone des Clients widerspiegelt, der für die Verbindung mit dem verwendet wird WorkSpace. Dieses Verhalten wird durch die Zeitzonenumleitung gesteuert. Vielleicht möchten Sie die Zeitzonenumleitung aus einem der folgenden Gründe deaktivieren:

- Ihr Unternehmen möchte, dass alle Mitarbeiter in einer bestimmten Zeitzone arbeiten (auch wenn sich einige Mitarbeiter in anderen Zeitzonen befinden).
- Sie haben Aufgaben in einer geplant WorkSpace , die zu einem bestimmten Zeitpunkt in einer bestimmten Zeitzone ausgeführt werden sollen.
- Ihre Benutzer, die viel verreisen, möchten ihre aus Konsistenzgründen und persönlichen Präferenzen WorkSpaces in einer Zeitzone aufbewahren.

Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu konfigurieren. Diese Einstellung wird wirksam, nachdem Sie die Verbindung zum getrennt und erneut hergestellt haben WorkSpace.

So aktivieren oder deaktivieren Sie die Zeitzonenumleitung für WSP Amazon Linux WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der Datei hinzu.

   ```
   timezone_redirect= X
   ```

   Mögliche Werte für *X*:

   enabled – Die Zeitzonenumleitung ist aktiviert (Standard).

   disabled – Die Zeitzonenumleitung ist deaktiviert.

Steuern des Verhaltens von PCoIP-Agenten auf Amazon Linux WorkSpaces

Das Verhalten des PCoIP Agents wird durch Konfigurationseinstellungen in der Datei `pcoip-agent.conf` gesteuert, die sich im Verzeichnis `/etc/pcoip-agent/` befindet. Verwenden Sie eine Konfigurationsmanagement-Lösung, die Amazon-Linux unterstützt, um Gruppenrichtlinien bereitzustellen und Änderungen durchzusetzen. Alle Änderungen werden wirksam, sobald der Agent gestartet wird. Beim Neustart des Agenten werden alle offenen Verbindungen beendet und der Fenstermanager wird neu gestartet. Um Änderungen anzuwenden, empfehlen wir einen Neustart der WorkSpace.

> **Note**
>
> Wenn Sie falsche oder nicht unterstützte Änderungen an der `pcoip-agent.conf` Datei vornehmen, können Sie dazu führen, dass Ihre WorkSpace nicht mehr funktioniert. Wenn Ihr WorkSpace nicht mehr funktioniert, müssen Sie möglicherweise entweder WorkSpace über SSH eine Verbindung zu Ihrem herstellen, um die Änderungen rückgängig zu machen, oder Sie müssen möglicherweise neu erstellen WorkSpace.

In den folgenden Abschnitten wird die Aktivierung oder Deaktivierung bestimmter Funktionen beschrieben. Eine vollständige Liste der verfügbaren Einstellungen finden Sie, `man pcoip-agent.conf` wenn Sie vom Terminal auf jeder Amazon Linux- ausführen WorkSpace.

Konfigurieren der Zwischenablageumleitung für PCoIP Amazon Linux WorkSpaces

Standardmäßig WorkSpaces unterstützt die Zwischenablageumleitung. Bei Bedarf können Sie diese Funktion mit der PCoIP-Agentenkonfiguration deaktivieren. Diese Einstellung wird wirksam, wenn Sie den neu starten WorkSpace.

So konfigurieren Sie die Zwischenablageumleitung für PCoIP Amazon Linux WorkSpaces

1. Öffnen Sie die `pcoip-agent.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der Datei hinzu.

   ```
   pcoip.server_clipboard_state = X
   ```

   Mögliche Werte für *X*:

   0 – Die Zwischenablageumleitung ist in beide Richtungen deaktiviert.

   1 – Die Zwischenablageumleitung ist in beide Richtungen aktiviert.

   2 – Die Zwischenablageumleitung ist nur vom Client zum Agent aktiviert (Sie können nur vom lokalen Client-Gerät zum Remote-Host-Desktop kopieren und einfügen).

   3 – Die Zwischenablageumleitung ist nur vom Agent zum Client aktiviert (Sie können nur vom Remote-Host-Desktop zum lokalen Client-Gerät kopieren und einfügen).

> **Note**
>
> Die Zwischenablageumleitung wird als virtueller Kanal implementiert. Wenn virtuelle Kanäle deaktiviert sind, funktioniert die Umleitung der Zwischenablage nicht. Informationen zur

Aktivierung virtueller Kanäle finden Sie unter Virtuelle PCoIP-Kanäle in der Teradici-Dokumentation.

Aktivieren oder Deaktivieren der Audioeingangsumleitung für PCoIP Amazon Linux WorkSpaces

Standardmäßig WorkSpaces unterstützt die Audioeingangsumleitung. Bei Bedarf können Sie diese Funktion mit der PCoIP-Agentenkonfiguration deaktivieren. Diese Einstellung wird wirksam, wenn Sie den neu starten WorkSpace.

So aktivieren oder deaktivieren Sie die Audioeingangsumleitung für PCoIP Amazon Linux WorkSpaces

1. Öffnen Sie die `pcoip-agent.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der Datei hinzu.

   ```
   pcoip.enable_audio = X
   ```

   Mögliche Werte für *X*:

   0 – Die Audioeingangsumleitung ist deaktiviert.

   1 – Die Audioeingangsumleitung ist aktiviert.

Aktivieren oder Deaktivieren der Zeitzonenumleitung für PCoIP Amazon Linux WorkSpaces

Standardmäßig ist die Zeit innerhalb eines Workspace so eingestellt, dass sie die Zeitzone des Clients widerspiegelt, der für die Verbindung mit dem verwendet wird WorkSpace. Dieses Verhalten wird durch die Zeitzonenumleitung gesteuert. Vielleicht möchten Sie die Zeitzonenumleitung aus einem der folgenden Gründe deaktivieren:

- Ihr Unternehmen möchte, dass alle Mitarbeiter in einer bestimmten Zeitzone arbeiten (auch wenn sich einige Mitarbeiter in anderen Zeitzonen befinden).
- Sie haben Aufgaben in einer geplant WorkSpace , die zu einem bestimmten Zeitpunkt in einer bestimmten Zeitzone ausgeführt werden sollen.
- Ihre Benutzer, die viel verreisen, möchten ihre aus Konsistenzgründen und persönlichen Präferenzen WorkSpaces in einer Zeitzone aufbewahren.

Bei Bedarf für Linux können WorkSpacesSie diese Funktion mit der PCoIP-Agent-Konfiguration deaktivieren. Diese Einstellung wird wirksam, wenn Sie den neu starten WorkSpace.

So aktivieren oder deaktivieren Sie die Zeitzonenumleitung für PCoIP Amazon Linux WorkSpaces

1. Öffnen Sie die `pcoip-agent.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der Datei hinzu.

   ```
   pcoip.enable_timezone_redirect= X
   ```

   Mögliche Werte für *X*:

   0 – Die Zeitzonenumleitung ist deaktiviert.

   1 – Die Zeitzonenumleitung ist aktiviert

Gewähren von SSH-Zugriff für Amazon Linux- WorkSpaces Administratoren

Standardmäßig können nur zugewiesene Benutzer und Konten in der Domain-Admins-Gruppe WorkSpaces über SSH eine Verbindung zu Amazon Linux herstellen.

Wir empfehlen Ihnen, eine dedizierte Administratorgruppe für Ihre Amazon- WorkSpacesLinux-Administratoren in Active Directory zu erstellen.

So aktivieren Sie den sudo-Zugriff für Mitglieder der Active-Directory-Gruppe „Linux_WorkSpaces_Admins“

1. Bearbeiten Sie die Datei `sudoers` mit `visudo`, wie im folgenden Beispiel gezeigt.

```
[example\username@workspace-id ~]$ sudo visudo
```

2. Fügen Sie die folgende Zeile zu.

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Nachdem Sie die dedizierte Administratorgruppe erstellt haben, führen Sie die folgenden Schritte aus, um die Anmeldung für die Mitglieder der Gruppe zu ermöglichen.

So aktivieren Sie die Anmeldung für Mitglieder der Linux_WorkSpaces_Admins Active Directory-Gruppe

1. Bearbeiten Sie `/etc/security/access.conf` mit erhöhten Rechten.

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Fügen Sie die folgende Zeile zu.

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

Weitere Informationen zum Aktivieren von SSH-Verbindungen finden Sie unter Aktivieren von SSH-Verbindungen für Linux WorkSpaces.

Überschreiben der Standard-Shell für Amazon Linux WorkSpaces

Um die Standard-Shell für Linux zu überschreiben WorkSpaces, empfehlen wir Ihnen, die -`~/.bashrc`Datei des Benutzers zu bearbeiten. Wenn Sie beispielsweise `Z shell` anstelle von `Bash`-Shell verwenden möchten, fügen Sie die folgenden Zeilen zu `/home/`*`username`*`/.bashrc` hinzu.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Nachdem Sie diese Änderung vorgenommen haben, müssen Sie entweder die neu starten WorkSpace oder sich von der abmelden WorkSpace (nicht nur trennen) und sich dann wieder anmelden, damit die Änderung wirksam wird.

Schützen von benutzerdefinierten Repositorys vor unbefugtem Zugriff

Wir empfehlen die Verwendung der in Amazon Virtual Private Cloud (Amazon VPC) integrierten Sicherheitsfunktionen anstelle von Passwörtern, um den Zugriff auf Ihre benutzerdefinierten Repositorys zu steuern. Verwenden Sie beispielsweise Netzwerk-Zugriffskontrolllisten (ACLs) und Sicherheitsgruppen. Weitere Informationen finden Sie unter Sicherheit im Amazon-VPC-Benutzerhandbuch.

Wenn Sie Passwörter zum Schutz Ihrer Repositorys verwenden müssen, stellen Sie sicher, dass Sie Ihre `yum`-Repository-Definitionsdateien erstellen, wie in Repository-Definitionsdateien in der Fedora-Dokumentation gezeigt.

Verwenden des Amazon-Linux-Extras-Library-Repositorys

Mit Amazon Linux können Sie die Extras-Bibliothek verwenden, um Anwendungs- und Software-Updates auf Ihren Instances zu installieren. Informationen zur Verwendung der Extras Library finden Sie unter Extras Library (Amazon Linux) im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

> **Note**
>
> Wenn Sie das Amazon-Linux-Repository verwenden, WorkSpaces muss Ihr Amazon Linux über Internetzugang verfügen, oder Sie müssen Virtual Private Cloud (VPC)-Endpunkte für dieses Repository und das Haupt-Amazon-Linux-Repository konfigurieren. Weitere Informationen finden Sie unter Bereitstellen des Internetzugangs von Ihrem aus WorkSpace.

Verwenden von Smartcards für die Authentifizierung unter Linux WorkSpaces

Pakete des Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) ermöglichen die Verwendung von Common Access Card (CAC)- und Personal Identity Verification (PIV)- Smartcards

für die Authentifizierung. Weitere Informationen finden Sie unter Verwenden von Smartcards zur Authentifizierung.

Konfigurieren der Proxyservereinstellungen des Geräts für den Internetzugang

Standardmäßig verwenden die WorkSpaces Clientanwendungen den Proxyserver, der in den Betriebssystemeinstellungen des Geräts für HTTPS-Datenverkehr (Port 443) angegeben ist. Die Amazon- WorkSpaces Clientanwendungen verwenden den HTTPS-Port für Updates, Registrierung und Authentifizierung.

> **Note**
>
> Proxyserver, die eine Authentifizierung mit Anmeldeinformationen erfordern, werden nicht unterstützt.

Sie können die Einstellungen des Geräte-Proxy-Servers für Linux WorkSpaces über die Gruppenrichtlinie konfigurieren, indem Sie die Schritte unter Geräte-Proxy und Internetkonnektivitätseinstellungen konfigurieren in der Microsoft-Dokumentation befolgen.

Weitere Informationen zum Konfigurieren der Proxy-Einstellungen in der WorkSpaces Windows-Clientanwendung finden Sie unter Proxy Server im Amazon- WorkSpaces Benutzerhandbuch.

Weitere Informationen zum Konfigurieren der Proxy-Einstellungen in der WorkSpaces macOS-Clientanwendung finden Sie unter Proxy Server im Amazon- WorkSpaces Benutzerhandbuch.

Weitere Informationen zum Konfigurieren der Proxy-Einstellungen in der WorkSpaces Web-Access-Client-Anwendung finden Sie unter Proxy-Server im Amazon- WorkSpaces Benutzerhandbuch.

Proxy für Desktop-Datenverkehr

Für PCoIP WorkSpaces unterstützen die Desktop-Client-Anwendungen weder die Verwendung eines Proxyservers noch die TLS-Entschlüsselung und -Inspektion für Port-4172-Datenverkehr in UDP (für Desktop-Datenverkehr). Sie benötigen eine direkte Verbindung mit dem Port 4172.

Für WSP unterstützen WorkSpacesdie WorkSpaces Windows-Clientanwendung (Version 5.1 und höher) und die macOS-Clientanwendung (Version 5.4 und höher) die Verwendung von HTTP-Proxyservern für den TCP-Datenverkehr von Port 4195. TLS-Entschlüsselung und -Inspektion werden nicht unterstützt.

WSP unterstützt nicht die Verwendung von Proxys für Desktop-Datenverkehr über UDP. Nur WorkSpaces Windows- und macOS-Desktop-Client-Anwendungen und WSP-Webzugriff unterstützen die Verwendung von Proxy für TCP-Datenverkehr.

> **Note**
>
> Wenn Sie einen Proxy-Server verwenden, werden die API-Aufrufe, die die Client-Anwendung an die WorkSpaces Services sendet, ebenfalls als Proxy weitergeleitet. Sowohl API-Aufrufe als auch Desktop-Datenverkehr sollten über denselben Proxyserver geleitet werden.

Empfehlung zur Verwendung von Proxyservern

Wir empfehlen nicht, einen Proxy-Server mit Ihrem WorkSpaces Desktop-Datenverkehr zu verwenden.

Der Amazon WorkSpaces -Desktop-Datenverkehr ist bereits verschlüsselt, sodass Proxys die Sicherheit nicht verbessern. Ein Proxy stellt einen zusätzlichen Hop im Netzwerkpfad dar, der die Streaming-Qualität durch Latenz beeinträchtigen könnte. Proxys könnten auch den Durchsatz verringern, wenn ein Proxy nicht die richtige Größe hat, um Desktop-Streaming-Datenverkehr zu verarbeiten. Darüber hinaus sind die meisten Proxys nicht für die Unterstützung von lang andauernden WebSocket (TCP) Verbindungen konzipiert und können sich auf die Streaming-Qualität und -Stabilität auswirken.

Wenn Sie einen Proxy verwenden müssen, platzieren Sie Ihren Proxy-Server so nah wie möglich am WorkSpace Client, vorzugsweise im selben Netzwerk, um eine zusätzliche Netzwerklatenz zu vermeiden, die sich negativ auf die Streaming-Qualität und Reaktionsfähigkeit auswirken könnte.

Verwalten Ihrer Ubuntu WorkSpaces

Wie bei Windows und Amazon Linux WorkSpaces sind WorkSpacesauch Ubuntu domainverbunden, sodass Sie Active-Directory-Benutzer und -Gruppen verwenden können, um:

- Verwalten Ihres Ubuntu WorkSpaces
- Gewähren von Zugriff auf diejenigen WorkSpaces für Benutzer

Sie können Ubuntu WorkSpaces mit Gruppenrichtlinien verwalten, indem Sie ADsys verwenden. Weitere Informationen zur Active-Directory-Integration finden Sie unter FAQ zur Ubuntu-Active-

Directory-Integration. Sie können außerdem andere Konfigurations- und Verwaltungslösungen wie Landscape und Ansible verwenden.

Control WorkSpaces Streaming Protocol (WSP)-Verhalten auf Ubuntu WorkSpaces

Das Verhalten des PCoIP-Agents wird durch Konfigurationseinstellungen in der `wsp.conf`-Datei gesteuert, die sich im Verzeichnis `/etc/wsp/` befindet. Verwenden Sie eine Konfigurationsmanagement-Lösung, die Ubuntu unterstützt, um Gruppenrichtlinien bereitzustellen und Änderungen durchzusetzen. Alle Änderungen werden wirksam, sobald der Agent gestartet wird.

> **Note**
>
> Wenn Sie falsche oder nicht unterstützte Änderungen an den `wsp.conf` Richtlinien vornehmen, werden möglicherweise nicht auf die neu hergestellten Verbindungen zu Ihrem angewendet WorkSpace.

In den folgenden Abschnitten wird die Aktivierung oder Deaktivierung bestimmter Funktionen beschrieben.

Aktivieren oder Deaktivieren der Zwischenablageumleitung für Ubuntu WorkSpaces

Standardmäßig WorkSpaces unterstützt die Zwischenablageumleitung. Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu deaktivieren.

So aktivieren oder deaktivieren Sie die Zwischenablageumleitung für Ubuntu WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der `[policies]`-Gruppe hinzu.

   ```
   clipboard = X
   ```

   Mögliche Werte für *X*:

enabled – Die Zwischenablageumleitung ist in beide Richtungen aktiviert (Standard).

disabled – Die Zwischenablageumleitung ist in beide Richtungen deaktiviert.

paste-only – Die Zwischenablageumleitung ist aktiviert und ermöglicht Ihnen nur, Inhalte vom lokalen Client-Gerät zu kopieren und auf dem Remote-Host-Desktop einzufügen.

copy-only – Die Zwischenablageumleitung ist aktiviert und ermöglicht Ihnen nur, Inhalte vom Remote-Host-Desktop zu kopieren und auf dem lokalen Client-Gerät einzufügen.

Aktivieren oder Deaktivieren der Audioeingangsumleitung für Ubuntu WorkSpaces

Standardmäßig WorkSpaces unterstützt die Audioeingangsumleitung. Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu deaktivieren.

So aktivieren oder deaktivieren Sie die Audioeingangsumleitung für Ubuntu WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der `[policies]`-Gruppe hinzu.

   ```
   audio-in = X
   ```

   Mögliche Werte für *X*:

   enabled – Die Audioeingangsumleitung ist aktiviert (Standard).

   disabled – Die Audioeingangsumleitung ist deaktiviert.

Aktivieren oder Deaktivieren der Videoeingangsumleitung für Ubuntu WorkSpaces

Standardmäßig WorkSpaces unterstützt die Videoeingangsumleitung. Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu deaktivieren.

So aktivieren oder deaktivieren Sie die Videoeingangsumleitung für Ubuntu WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der `[policies]`-Gruppe hinzu.

   ```
   video-in = X
   ```

   Mögliche Werte für *X*:

   enabled – Die Eingangsvideoumleitung ist aktiviert (Standard).

   disabled – Die Eingangsvideoumleitung ist deaktiviert.

Aktivieren oder Deaktivieren der Zeitzonenumleitung für Ubuntu WorkSpaces

Standardmäßig ist die Zeit innerhalb eines Workspace so eingestellt, dass sie die Zeitzone des Clients widerspiegelt, der für die Verbindung mit dem verwendet wird WorkSpace. Dieses Verhalten wird durch die Zeitzonenumleitung gesteuert. Vielleicht möchten Sie die Zeitzonenumleitung aus einem der folgenden Gründe deaktivieren:

- Ihr Unternehmen möchte, dass alle Mitarbeiter in einer bestimmten Zeitzone arbeiten (auch wenn sich einige Mitarbeiter in anderen Zeitzonen befinden).
- Sie haben Aufgaben in einer geplant WorkSpace , die zu einem bestimmten Zeitpunkt in einer bestimmten Zeitzone ausgeführt werden sollen.
- Ihre Benutzer sind sehr viel unterwegs und möchten ihre aus Gründen der Konsistenz und persönlichen Präferenzen WorkSpaces in einer Zeitzone behalten.

Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu konfigurieren.

So aktivieren oder deaktivieren Sie die Zeitzonenumleitung für Ubuntu WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Fügen Sie die folgende Zeile am Ende der `[policies]`-Gruppe hinzu.

```
timezone-redirection = X
```

Mögliche Werte für *X*:

enabled – Die Zeitzonenumleitung ist aktiviert (Standard).

disabled – Die Zeitzonenumleitung ist deaktiviert.

Aktivieren oder Deaktivieren der Druckerumleitung für Ubuntu WorkSpaces

Standardmäßig WorkSpaces unterstützt die Druckerumleitung. Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu deaktivieren.

So aktivieren oder deaktivieren Sie die Druckerumleitung für Ubuntu WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Fügen Sie die folgende Zeile am Ende der `[policies]`-Gruppe hinzu.

```
remote-printing = X
```

Mögliche Werte für *X*:

enabled – Die Druckerumleitung ist aktiviert (Standard).

disabled – Die Druckerumleitung ist deaktiviert

Aktivieren oder Deaktivieren des Trennens der Sitzung bei Bildschirmsperre für WSP

Aktivieren Sie die Trennungssitzung auf der Bildschirmsperre, damit Ihre Benutzer ihre WorkSpaces Sitzung beenden können, wenn der Windows-Sperrbildschirm erkannt wird. Um die Verbindung vom WorkSpaces Client aus wiederherzustellen, können Benutzer ihre Passwörter oder ihre Smartcards verwenden, um sich zu authentifizieren, je nachdem, welche Art der Authentifizierung für ihr aktiviert wurde WorkSpaces.

Standardmäßig unterstützt WorkSpaces das Trennen der Sitzung bei der Bildschirmsperre nicht. Verwenden Sie die WSP-Konfigurationsdatei, um diese Funktion bei Bedarf zu aktivieren.

So aktivieren oder deaktivieren Sie die Trennungssitzung auf der Bildschirmsperre für Windows WorkSpaces

1. Öffnen Sie die `wsp.conf`-Datei in einem Editor mit erhöhten Rechten, indem Sie den folgenden Befehl verwenden.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Fügen Sie die folgende Zeile am Ende der `[policies]`-Gruppe hinzu.

   ```
   disconnect-on-lock = X
   ```

   Mögliche Werte für *X*:

   enabled – Das Trennen der Verbindung bei Bildschirmsperre ist aktiviert.

   disabled – Das Trennen der Verbindung bei Bildschirmsperre ist deaktiviert.

Gewähren von SSH-Zugriff für Ubuntu- WorkSpaces Administratoren

Standardmäßig können nur zugewiesene Benutzer und Konten in der Domain-Admins-Gruppe WorkSpaces über SSH eine Verbindung zu Ubuntu herstellen. Damit andere Benutzer und Konten WorkSpaces über SSH eine Verbindung zu Ubuntu herstellen können, empfehlen wir Ihnen, eine dedizierte Administratorgruppe für Ihre Ubuntu- WorkSpaces Administratoren in Active Directory zu erstellen.

So aktivieren Sie den sudo-Zugriff für Mitglieder der Active-Directory-Gruppe **`Linux_WorkSpaces_Admins`**

1. Bearbeiten Sie die Datei `sudoers` mit `visudo`, wie im folgenden Beispiel gezeigt.

```
[username@workspace-id ~]$ sudo visudo
```

2. Fügen Sie die folgende Zeile zu.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Nachdem Sie die dedizierte Administratorgruppe erstellt haben, führen Sie die folgenden Schritte aus, um die Anmeldung für die Mitglieder der Gruppe zu ermöglichen.

So aktivieren Sie die Anmeldung für Mitglieder der Active-Directory-Gruppe **`Linux_WorkSpaces_Admins`**

1. Bearbeiten Sie /`etc/security/access.conf` mit erhöhten Rechten.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Fügen Sie die folgende Zeile zu.

```
+:(Linux_WorkSpaces_Admins):ALL
```

Mit Ubuntu müssen WorkSpaces Sie keinen Domänennamen hinzufügen, wenn Sie den Benutzernamen für die SSH-Verbindung angeben. Standardmäßig ist die Passwortauthentifizierung deaktiviert. Um eine Verbindung über SSH herzustellen, müssen Sie entweder Ihren öffentlichen SSH-Schlüssel zu `$HOME/.ssh/authorized_keys` auf Ihrem Ubuntu- hinzufügen oder bearbeiten WorkSpace, `/etc/ssh/sshd_config` um PasswordAuthentication auf festzulegen`yes`. Weitere

Informationen zum Aktivieren von SSH-Verbindungen finden Sie unter Aktivieren von SSH-Verbindungen für Ihr Linux- WorkSpaces.

Überschreiben der Standard-Shell für Ubuntu WorkSpaces

Um die Standard-Shell für Ubuntu zu überschreiben WorkSpaces, empfehlen wir Ihnen, die -`~/.bashrc`Datei des Benutzers zu bearbeiten. Wenn Sie beispielsweise `Z shell` anstelle von `Bash`-Shell verwenden möchten, fügen Sie die folgenden Zeilen zu `/home/username/.bashrc` hinzu.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Nachdem Sie diese Änderung vorgenommen haben, müssen Sie entweder die neu starten WorkSpace oder sich von der abmelden WorkSpace (nicht nur trennen) und sich dann wieder anmelden, damit die Änderung wirksam wird.

Konfigurieren der Proxyservereinstellungen des Geräts für den Internetzugang

Standardmäßig verwenden die WorkSpaces Clientanwendungen den Proxyserver, der in den Betriebssystemeinstellungen des Geräts für HTTPS-Datenverkehr (Port 443) angegeben ist. Die Amazon- WorkSpaces Clientanwendungen verwenden den HTTPS-Port für Updates, Registrierung und Authentifizierung.

> **Note**
>
> Proxyserver, die eine Authentifizierung mit Anmeldeinformationen erfordern, werden nicht unterstützt.

Sie können die Einstellungen des Geräte-Proxy-Servers für Ihr Ubuntu WorkSpaces über die Gruppenrichtlinie konfigurieren, indem Sie die Schritte unter Geräte-Proxy und Internetkonnektivitätseinstellungen konfigurieren in der Microsoft-Dokumentation befolgen.

Weitere Informationen zum Konfigurieren der Proxy-Einstellungen in der WorkSpaces Windows-Clientanwendung finden Sie unter Proxy Server im Amazon- WorkSpaces Benutzerhandbuch.

Weitere Informationen zum Konfigurieren der Proxy-Einstellungen in der WorkSpaces macOS-Clientanwendung finden Sie unter Proxy Server im Amazon- WorkSpaces Benutzerhandbuch.

Weitere Informationen zum Konfigurieren der Proxy-Einstellungen in der WorkSpaces Web-Access-Client-Anwendung finden Sie unter Proxy-Server im Amazon- WorkSpaces Benutzerhandbuch.

Proxy für Desktop-Datenverkehr

Für PCoIP WorkSpaces unterstützen die Desktop-Client-Anwendungen weder die Verwendung eines Proxyservers noch die TLS-Entschlüsselung und -Inspektion für Port-4172-Datenverkehr in UDP (für Desktop-Datenverkehr). Sie benötigen eine direkte Verbindung mit dem Port 4172.

Für WSP unterstützen WorkSpacesdie WorkSpaces Windows-Clientanwendung (Version 5.1 und höher) und die macOS-Clientanwendung (Version 5.4 und höher) die Verwendung von HTTP-Proxyservern für den TCP-Datenverkehr von Port 4195. TLS-Entschlüsselung und -Inspektion werden nicht unterstützt.

WSP unterstützt nicht die Verwendung von Proxys für Desktop-Datenverkehr über UDP. Nur WorkSpaces Windows- und macOS-Desktop-Client-Anwendungen und WSP-Webzugriff unterstützen die Verwendung von Proxy für TCP-Datenverkehr.

> **Note**
>
> Wenn Sie einen Proxy-Server verwenden möchten, werden die API-Aufrufe, die die Client-Anwendung an die WorkSpaces Services sendet, ebenfalls als Proxy weitergeleitet. Sowohl API-Aufrufe als auch Desktop-Datenverkehr sollten über denselben Proxyserver geleitet werden.

Empfehlung zur Verwendung von Proxyservern

Wir empfehlen nicht, einen Proxy-Server mit Ihrem WorkSpaces Desktop-Datenverkehr zu verwenden.

Der Amazon WorkSpaces -Desktop-Datenverkehr ist bereits verschlüsselt, sodass Proxys die Sicherheit nicht verbessern. Ein Proxy stellt einen zusätzlichen Hop im Netzwerkpfad dar, der die Streaming-Qualität durch Latenz beeinträchtigen könnte. Proxys könnten auch den Durchsatz verringern, wenn ein Proxy nicht die richtige Größe hat, um Desktop-Streaming-Datenverkehr zu verarbeiten. Darüber hinaus sind die meisten Proxys nicht für die Unterstützung von lang andauernden WebSocket (TCP) Verbindungen konzipiert und können sich auf die Streaming-Qualität und -Stabilität auswirken.

Wenn Sie einen Proxy verwenden müssen, platzieren Sie Ihren Proxy-Server so nah wie möglich am WorkSpace Client, vorzugsweise im selben Netzwerk, um eine zusätzliche Netzwerklatenz zu vermeiden, die sich negativ auf die Streaming-Qualität und Reaktionsfähigkeit auswirken könnte.

Optimieren Sie Amazon WorkSpaces für die Kommunikation in Echtzeit

Amazon WorkSpaces bietet eine Vielzahl von Techniken, um die Bereitstellung von Unified Communication (UC) -Anwendungen wie Microsoft Teams, Zoom, Webex und anderen zu erleichtern. In modernen Anwendungslandschaften bestehen die meisten UC-Anwendungen aus einer Vielzahl von Funktionen, darunter 1:1-Chatrooms, Gruppenchatkanäle für die Zusammenarbeit, nahtlose Speicherung und Austausch von Dateien, Live-Events, Webinare, Übertragungen, interaktive Bildschirmübertragung und Steuerung, Whiteboarding und Offline-Audio-/Video-Messaging-Funktionen. Die meisten dieser Funktionen sind problemlos WorkSpaces als Standardfunktionen verfügbar, ohne dass zusätzliche Feinabstimmungen oder Verbesserungen erforderlich sind. Es sei jedoch darauf hingewiesen, dass Kommunikationselemente in Echtzeit, insbesondere one-on-one Telefongespräche und Gruppentreffen, eine Ausnahme von dieser Regel darstellen. Die erfolgreiche Integration solcher Funktionen erfordert häufig eine gezielte Ausrichtung und Planung während des WorkSpaces Implementierungsprozesses.

Bei der Planung Ihrer Implementierung von Echtzeit-Kommunikationsfunktionen von UC-Anwendungen auf Amazon WorkSpaces stehen Ihnen drei verschiedene Konfigurationsmodi für Echtzeitkommunikation (RTC) zur Auswahl. Die Auswahl hängt von der spezifischen Anwendung oder den Anwendungen ab, die Sie Ihren Benutzern zur Verfügung stellen möchten, und von den Client-Geräten, die Sie verwenden möchten.

Dieses Dokument konzentriert sich auf die Optimierung der Benutzererfahrung für die gängigsten UC-Anwendungen bei Amazon WorkSpaces. WorkSpaces Core-spezifische Optimierungen finden Sie in der partnerspezifischen Dokumentation.

Themen

Überblick über die Modi zur Medienoptimierung

Im Folgenden sind die verfügbaren Optionen zur Medienoptimierung aufgeführt.

Option 1: Medienoptimierte Echtzeitkommunikation (Media Optimized RTC)

In diesem Modus werden UC- und VoIP-Anwendungen von Drittanbietern auf der Fernbedienung ausgeführt WorkSpace, während ihr Media Framework für die direkte Kommunikation auf den unterstützten Client ausgelagert wird. Die folgenden UC-Anwendungen verwenden diesen Ansatz bei Amazon WorkSpaces:

- Zoom-Besprechungen
- Cisco-Webex-Besprechungen

Damit der Media Optimized RTC-Modus funktioniert, sollte der Anbieter der UC-Anwendung die Integration WorkSpaces mithilfe eines der verfügbaren Software Development Kits (SDK) wie dem DCV Extension SDK entwickeln. Für diesen Modus müssen die UC-Komponenten auf dem Client-Gerät installiert sein.

Weitere Informationen zur Konfiguration dieses Modus finden Sie unter Konfigurieren von Media Optimized RTC.

Option 2: Optimierte Echtzeitkommunikation während der Sitzung (In-Session Optimized RTC)

In diesem Modus läuft die unveränderte UC-Anwendung auf dem und leitet den WorkSpace Audio- und Videoverkehr über das WorkSpaces Streaming-Protokoll an das Client-Gerät weiter. Lokales Audio vom Mikrofon und Videostream von einer Webcam werden dorthin umgeleitet WorkSpace, wo sie von der UC-Anwendung konsumiert werden. Dieser Modus bietet umfassende Anwendungskompatibilität und stellt die UC-Anwendung effizient von der Ferne WorkSpace auf eine Vielzahl von Client-Plattformen bereit. Sie müssen die UC-Anwendungskomponenten nicht auf dem Client-Gerät bereitstellen.

Weitere Informationen zur Konfiguration dieses Modus finden Sie unter Konfigurieren von In-session Optimized RTC.

Option 3: Direkte Kommunikation in Echtzeit (Direct RTC)

In diesem Modus WorkSpace übernimmt die innerhalb des ausgeführte Anwendung die Kontrolle über den physischen oder virtuellen Telefonapparat, der sich auf dem Schreibtisch oder dem Client-Betriebssystem des Benutzers befindet. Dies führt dazu, dass der Audiodatenverkehr direkt vom physischen Telefon an der Workstation der Benutzer oder dem virtuellen Telefon, das auf dem Client-Gerät betrieben wird, zum Remote-Call-Peer übertragen wird. Zu den wichtigsten Beispielen für Anwendungen, die in diesem Modus funktionieren, gehören:

- Amazon Connect Connect-Optimierung für Amazon WorkSpaces
- Genesys-Cloud-WebRTC-Medienhelfer
- SIP-Gateway für Microsoft Teams
- Microsoft Teams-Tischtelefone und Teams-Displays
- Teilnahme an Audiokonferenzen über die Einwahlfunktionen oder die „Mein Telefon wählen“-Funktion der UC-Anwendung.

Weitere Informationen zur Konfiguration dieses Modus finden Sie unter Konfigurieren von Direct RTC.

Welcher RTC-Optimierungsmodus sollte verwendet werden?

Verschiedene RTC-Optimierungsmodi können gleichzeitig verwendet oder so eingerichtet werden, dass sie sich gegenseitig als Fallback ergänzen. Erwägen Sie beispielsweise, Media Optimized RTC für Cisco-Webex-Meetings zu aktivieren. Diese Konfiguration stellt sicher, dass Benutzer beim Zugriff WorkSpace über einen Desktop-Client eine optimierte Kommunikation erhalten. In Szenarien, in denen von einem gemeinsam genutzten Internetkiosk auf Webex zugegriffen wird, dem UC-Optimierungskomponenten fehlen, wechselt Webex jedoch nahtlos in den Modus In-Session Optimized RTC, um die Funktionalität aufrechtzuerhalten. Wenn Benutzer mit mehreren UC-Anwendungen arbeiten, können die RTC-Konfigurationsmodi je nach ihren individuellen Anforderungen variieren.

In der folgenden Tabelle sind die allgemeinen Funktionen von UC-Anwendungen aufgeführt. Sie definiert, welcher RTC-Konfigurationsmodus das beste Ergebnis liefert.

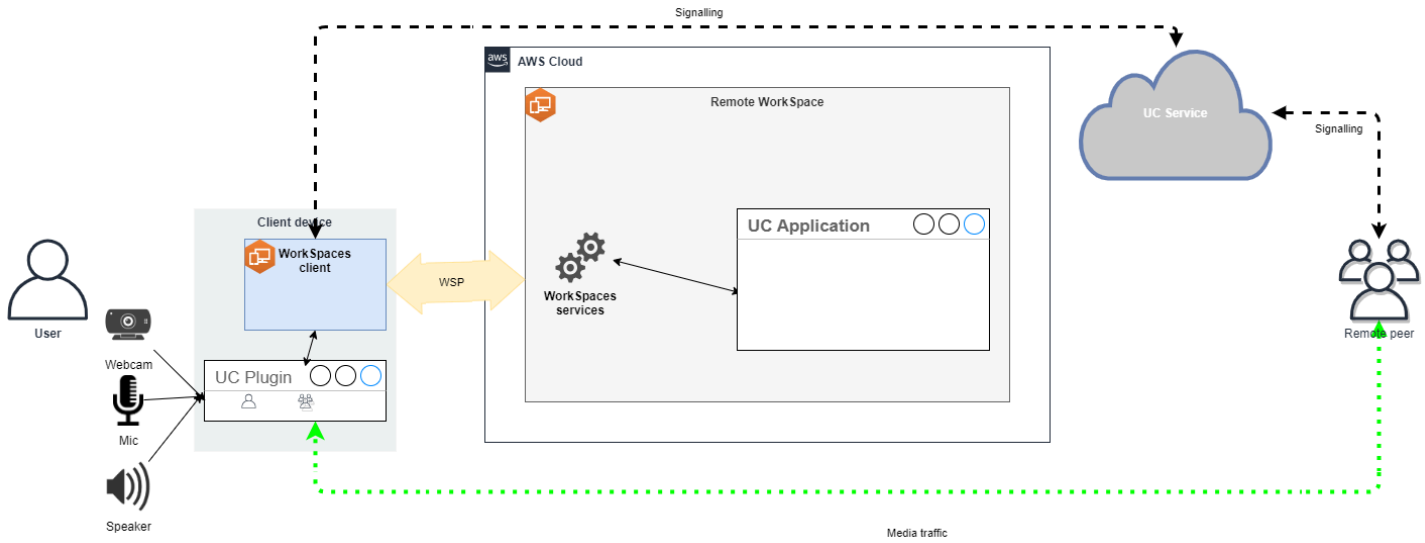
Funktion	Direct RTC	Media Optimized RTC	In-session Optimized RTC
1:1-Chat	Erfordert keine RTC-Konfiguration		
Gruppen-Chatrooms	Erfordert keine RTC-Konfiguration		
Gruppen-Audiokonferenzen	Am besten	Am besten	Gut
Gruppen-Videokonferenzen	Gut	Am besten	Gut
1:1-Audioanrufe	Am besten	Am besten	Gut
1:1-Videoanrufe	Gut	Am besten	Gut
Whiteboarding	Erfordert keine RTC-Konfiguration		
Audio-/Videoclips/ Nachrichten	Nicht zutreffend	Gut	Am besten
Gemeinsame Nutzung von Dateien	Nicht zutreffend	Hängt von der UC-Anwendung ab	Am besten
Bildschirmübertragung und Steuerung	Nicht zutreffend	Hängt von der UC-Anwendung ab	Am besten
Webinare/Broadcast-Events	Nicht zutreffend	Gut	Am besten

Anleitung zur RTC-Optimierung

Konfigurieren von Media Optimized RTC

Der Modus Media Optimized RTC wird durch die Verwendung der von Amazon bereitgestellten SDKs durch den Anbieter der UC-Anwendung ermöglicht. Die Architektur erfordert, dass der UC-Anbieter ein UC-spezifisches Plugin oder eine UC-spezifische Erweiterung entwickelt und auf dem Client bereitstellt.

Das SDK, das öffentlich verfügbare Optionen wie das DCV Extension SDK und benutzerdefinierte private Versionen umfasst, richtet einen Steuerkanal zwischen dem UC-Anwendungsmodul, das innerhalb des verwendet wird, WorkSpace und einem Plug-in auf der Clientseite ein. In der Regel weist dieser Steuerkanal die Clienterweiterung an, einen Anruf einzuleiten oder einem Anruf beizutreten. Sobald der Anruf über die clientseitige Erweiterung hergestellt wurde, erfasst das UC-Plugin den Audiostream vom Mikrofon und den Videostream von der Webcam, die dann direkt an die UC-Cloud oder einen Call-Peer übertragen werden. Der eingehende Audiostream wird lokal abgespielt und der Videostream wird in der Benutzeroberfläche des Remote-Clients eingeblendet. Der Steuerkanal ist dafür verantwortlich, den Status des Anrufs zu kommunizieren.



Amazon unterstützt WorkSpaces derzeit die folgenden Anwendungen mit dem Media Optimized RTC-Modus:

- Zoom-Besprechungen (für PCoIP und WSP) WorkSpaces
- Cisco Webex-Meetings (nur für WSP) WorkSpaces

Wenn Sie eine Anwendung verwenden, die nicht auf der Liste steht, ist es ratsam, den Anwendungsanbieter zu kontaktieren und Support für WorkSpaces Media Optimized RTC anzufordern. Um diesen Prozess zu beschleunigen, bitten Sie sie, sich an @amazon .com zu wendenaws-av-offloading.

Der RTC-Modus für Medienoptimierung verbessert zwar die Anrufleistung und minimiert die WorkSpace Ressourcenauslastung, weist jedoch einige Einschränkungen auf:

- Die UC-Client-Erweiterung muss auf dem Client-Gerät installiert sein.

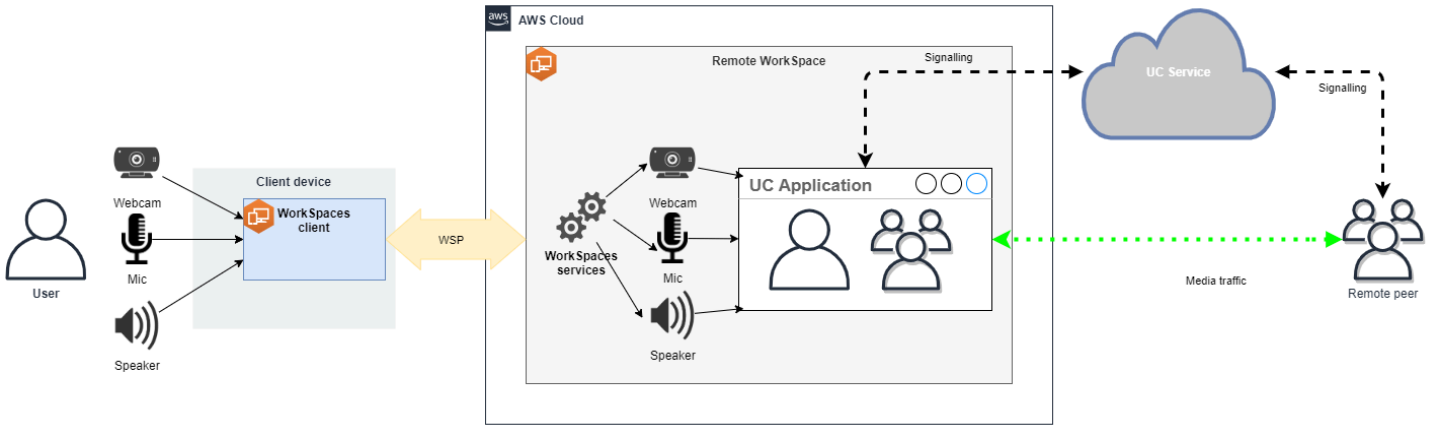
- Die UC-Client-Erweiterung erfordert eine unabhängige Verwaltung und unabhängige Updates.
- UC-Client-Erweiterungen sind auf bestimmten Client-Plattformen, wie z. B. mobilen Plattformen oder Webclients, möglicherweise nicht verfügbar.
- Einige Funktionen von UC-Anwendungen könnten in diesem Modus eingeschränkt sein. Beispielsweise kann das Verhalten bei der Bildschirmübertragung unterschiedlich sein.
- Die Verwendung von clientseitigen Erweiterungen ist möglicherweise nicht für Szenarien wie Bring Your Own Device (BYOD) oder gemeinsam genutzte Kioske geeignet.

Wenn sich der medienoptimierte RTC-Modus für Ihre Umgebung als ungeeignet erweist oder bestimmte Benutzer die Client-Erweiterung nicht installieren können, wird empfohlen, den Modus In-session Optimized RTC als Ausweichoption zu konfigurieren.

Konfigurieren von In-session Optimized RTC

Im RTC-Modus „Während der Sitzung optimiert“ arbeitet die UC-Anwendung WorkSpace ohne Änderungen und bietet so ein lokales Benutzererlebnis. Die von der Anwendung generierten Audio- und Videostreams werden vom WorkSpaces Streaming Protocol (WSP) erfasst und an die Clientseite übertragen. Auf dem Client werden die Mikrofon- (sowohl auf WSP als auch auf PCoIP WorkSpaces) und die Webcam-Signale (nur auf WSP WorkSpaces) erfasst, zurück zur UC-Anwendung umgeleitet und nahtlos an die WorkSpace UC-Anwendung weitergeleitet.

Insbesondere gewährleistet diese Option eine hervorragende Kompatibilität, auch mit älteren Anwendungen, und bietet unabhängig von der Herkunft der Anwendung eine einheitliche Benutzererfahrung. Der Modus In-session optimization funktioniert auch mit dem Webclient.



WorkSpaces Das Streaming Protocol (WSP) wurde sorgfältig optimiert, um die Leistung des Remote RTC-Modus zu verbessern. Die Optimierungsmaßnahmen umfassen:

- Nutzung eines adaptiven UDP-basierten QUIC-Transports, der eine effiziente Datenübertragung gewährleistet.
- Einrichtung eines Audiopfads mit niedriger Latenz, der eine schnelle Audioeingabe und -ausgabe ermöglicht.
- Implementierung sprachoptimierter Audiocodecs zur Aufrechterhaltung der Audioqualität bei gleichzeitiger Reduzierung der CPU- und Netzwerkauslastung.
- Webcam-Umleitung, die die Integration von Webcam-Funktionen ermöglicht.
- Konfiguration der Webcam-Auflösung zur Leistungsoptimierung.
- Integration von adaptiven Anzeige-Codecs für ein optimales Gleichgewichtig zwischen Geschwindigkeit und visueller Qualität.
- Korrektur von Audio-Jitter, die eine reibungslose Audioübertragung garantiert.

Diese Optimierungen tragen zusammen zu einer robusten und flüssigen Erfahrung im Modus Remote RTC bei.

Größenempfehlungen

Um den Remote RTC-Modus effektiv zu unterstützen, ist es wichtig, die richtige Größe von Amazon WorkSpaces sicherzustellen. Die Fernbedienung WorkSpace muss die Systemanforderungen der jeweiligen Unified Communication (UC) -Anwendung erfüllen oder übertreffen. In der folgenden Tabelle sind die unterstützten und empfohlenen WorkSpaces Mindestkonfigurationen für gängige UC-Anwendungen aufgeführt, die für Video- und Audioanrufe verwendet werden:

			Videoanrufe		Audioanrufe		
Anwendung	CPU-Anforderungen für die RTC-App	RAM-Anforderungen für die RTC-App	Minimal unterstützt WorkSpace	Empfohlen WorkSpace	Minimal unterstützt WorkSpace	Empfohlen WorkSpace	Referenz
Microsoft-Teams	2 Kerne erforderlich, 4 Kerne empfohlen	4,0 GB RAM	Power (4 vCPU, 16 GB Speicher)	PowerPro (8 vCPU, 32 GB Speicher)	Performance (2 vCPU, 8 GB Speicher)	Power (4 vCPU, 16 GB Speicher)	Hardwareanforderungen für Microsoft Teams

			Videoanrufe		Audioanrufe		
Anwendung	CPU-Anforderungen für die RTC-App	RAM-Anforderungen für die RTC-App	Minimal unterstützt WorkSpace	Empfohlen WorkSpace	Minimal unterstützt WorkSpace	Empfohlen WorkSpace	Referenz
Zoom	2 Kerne erforderlich, 4 Kerne empfohlen	4,0 GB RAM	Power (4 vCPU, 16 GB Speicher)	PowerPro (8 vCPU, 32 GB Speicher)	Performance (2 vCPU, 8 GB Speicher)	Power (4 vCPU, 16 GB Speicher)	Zoom-Systemanforderungen: Windows, macOS, Linux
Webex	2 Kerne erforderlich	4,0 GB RAM	Power (4 vCPU, 16 GB Speicher)	PowerPro (8 vCPU, 32 GB Speicher)	Performance (2 vCPU, 8 GB Speicher)	Power (4 vCPU, 16 GB Speicher)	Systemanforderungen für Webex-Dienste

Beachten Sie, dass Videokonferenzen einen erheblichen Ressourcenverbrauch für die Videokodierung und -dekodierung darstellen. In Szenarien mit physischen Maschinen werden diese Aufgaben auf die GPU ausgelagert. Ohne GPU WorkSpaces werden diese Aufgaben parallel zur Remote-Protokollcodierung auf der CPU ausgeführt. Daher wird Benutzern, die regelmäßig Videostreaming oder Videoanrufe tätigen, dringend empfohlen, sich für die PowerPro Konfiguration zu entscheiden.

Die gemeinsame Nutzung von Bildschirmen verbraucht ebenfalls erhebliche Ressourcen, wobei der Ressourcenverbrauch mit höheren Auflösungen zunimmt. Daher ist die Bildschirmübertragung bei Geräten ohne GPU WorkSpaces häufig auf eine niedrigere Bildrate beschränkt.

Nutzen Sie den UDP-basierten QUIC-Transport mit dem WorkSpaces Streaming Protocol (WSP)

Der UDP-Transport eignet sich besonders gut für die Übertragung von RTC-Anwendungen. Stellen Sie zur Maximierung der Effizienz sicher, dass Ihr Netzwerk so eingerichtet ist, dass es den QUIC-

Transport für WSP nutzt. Beachten Sie, dass UDP-basierter Transport nur für native Clients verfügbar ist.

Konfigurieren Sie die UC-Anwendung für WorkSpaces

Für erweiterte Videoverarbeitungsfunktionen wie Hintergrundunschärfe, virtuelle Hintergründe, Reaktionen oder die Ausrichtung von Live-Events WorkSpace ist die Entscheidung für eine GPU-fähige Grafikkarte unerlässlich, um eine optimale Leistung zu erzielen.

Die meisten UC-Anwendungen bieten Anleitungen zur Deaktivierung der fortschrittlichen Videoverarbeitung, um die CPU-Auslastung ohne GPU zu reduzieren. WorkSpaces

Weitere Informationen finden Sie in folgenden verwandten Ressourcen.

- Microsoft Teams: Teams für Virtualized Desktop Infrastructure
- Zoom-Besprechungen: Verwaltung der Benutzererfahrung für inkompatible VDI-Plug-ins
- Webex: Bereitstellungsleitfaden für Webex App for Virtual Desktop Infrastructure (VDI) – Webex App für VDI verwalten und Fehler beheben [Webex App]
- Google Meet: Verwenden von VDI

Aktivieren der bidirektionale Audio- und Webcam-Umleitung

Amazon WorkSpaces unterstützt standardmäßig Audioeingang, Audioausgang und Kameraumleitung über Videoeingang. Wenn diese Funktionen jedoch aus bestimmten Gründen deaktiviert wurden, können Sie den bereitgestellten Anweisungen folgen, um die Umleitung wieder zu aktivieren. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der Videoeingangsumleitung für WSP im WorkSpacesAmazon-Administratorhandbuch. Die Benutzer müssen nach dem Herstellen der Verbindung die Kamera auswählen, die sie in der Sitzung verwenden möchten. Weitere Informationen finden Benutzer im WorkSpaces Amazon-Benutzerhandbuch unter Webcams und andere Videogeräte.

Beschränken der maximale Webcam-Auflösung

Benutzern, die Power oder PowerPro WorkSpaces Videokonferenzen nutzen, wird dringend empfohlen, die maximale Auflösung umgeleiteter Webcams einzuschränken. Im Fall von PowerPro beträgt die empfohlene maximale Auflösung 640 Pixel in der Breite und 480 Pixel in der Höhe. Im Fall von PowerPro beträgt die empfohlene maximale Auflösung 320 Pixel in der Breite und 240 Pixel in der Höhe.

Führen Sie die folgenden Schritte aus, um die maximale Webcam-Auflösung zu konfigurieren.

1. Öffnen Sie den Windows Registrierungs-Editor.
2. Navigieren Sie zu folgendem Registrierungspfad:

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. Erstellen Sie einen Zeichenfolgenwert mit dem Namen `max-resolution` und legen Sie ihn auf die gewünschte Auflösung im `(X,Y)` Format fest, wobei `X` die horizontale Pixelanzahl (Breite) und `Y` die vertikale Pixelanzahl (Höhe) darstellt. Legen Sie beispielsweise `(640,480)` fest, um eine Auflösung mit einer Breite von 640 Pixeln und einer Höhe von 480 Pixeln zu verwenden.

Aktivieren der sprachoptimierten Audiokonfiguration

Standardmäßig WorkSpaces sind sie so eingestellt, dass sie 7.1-Hi-Fidelity-Audio vom Client WorkSpaces übertragen und so eine hervorragende Musikwiedergabequalität gewährleisten. Wenn Ihr primärer Anwendungsfall jedoch Audio- oder Videokonferenzen umfasst, können Sie durch Ändern des Audiocodec-Profils auf eine sprachoptimierte Einstellung CPU- und Netzwerkressourcen einsparen.

Führen Sie die folgenden Schritte aus, um das Audioprofil auf sprachoptimiert einzustellen.

1. Öffnen Sie den Windows Registrierungs-Editor.
2. Navigieren Sie zu folgendem Registrierungspfad:

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

3. Erstellen Sie einen Zeichenfolgewert mit dem Namen `default-profile` und legen Sie ihn auf `voice` fest.

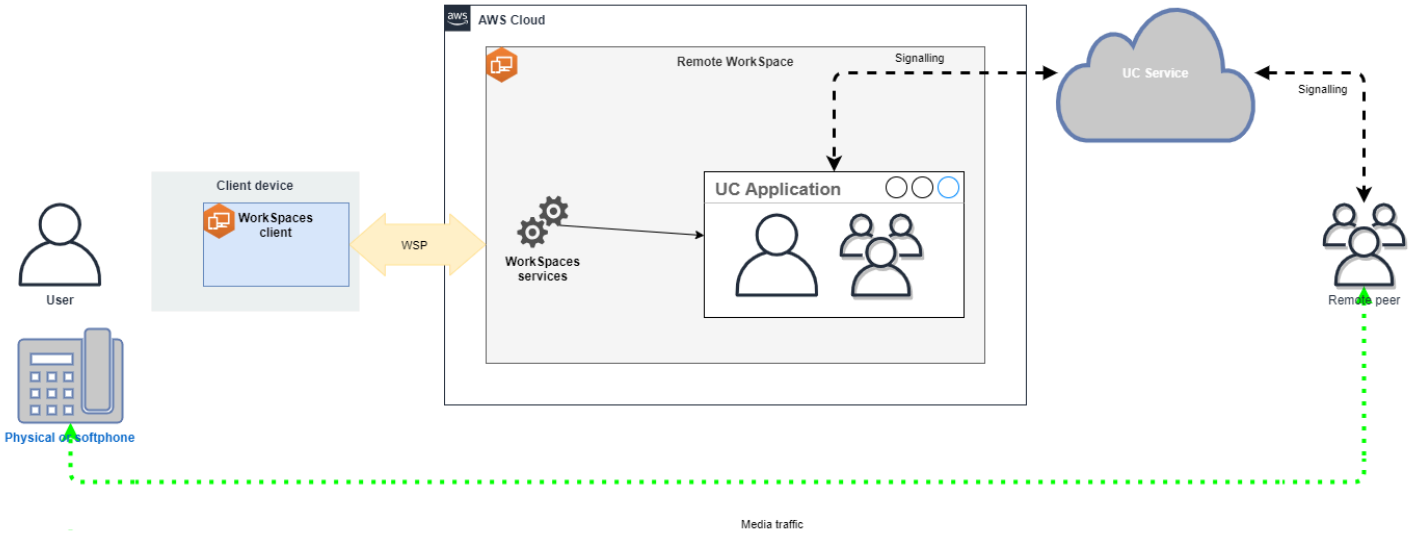
Verwenden hochwertiger Headsets für Audio- und Videoanrufe

Zur Verbesserung der Audioerfahrung und Vermeidung von Echos ist es wichtig, hochwertige Headsets zu verwenden. Die Verwendung von Desktop-Lautsprechern kann zu Echoproblemen am Remote-Ende des Anrufs führen.

Konfigurieren von Direct RTC

Die Konfiguration des Direct RTC-Modus hängt von der jeweiligen Unified Communication (UC) - Anwendung ab und erfordert keine Änderungen an der Konfiguration. WorkSpaces Die folgende

Liste bietet eine nicht vollständige Zusammenstellung von Optimierungen für verschiedene UC-Anwendungen.



- Microsoft-Teams:
  - Planen für SIP-Gateway
  - Audiokonferenzen in Microsoft 365
  - Planen Ihrer Teams-Sprachlösung
- Zoom-Besprechungen:
  - Aktivieren oder Deaktivieren von gebührenpflichtigen Einwahlnummern
  - Verwenden der Festnetzanrufsteuerung
  - Begleitmodus für Tischtelefone
- Webex:
  - Webex App | Telefonieren mit Ihrem Tischtelefon
  - Webex App | Unterstützte Anrufoptionen
- BlueJeans:
  - Von einem Tischtelefon aus in ein Meeting einwählen
- Genesys:
  - Genesys-Cloud-WebRTC-Medienhelfer
- Amazon Connect:
  - Amazon Connect Connect-Optimierung für Amazon WorkSpaces
- Google Meet:

- Verwenden eines Telefons für Audio in einer Videokonferenz

Verwalten des WorkSpace-Funktionsmodus

Der Funktionsmodus eines WorkSpace bestimmt die sofortige Verfügbarkeit und wie Sie dafür bezahlen (monatlich oder stündlich). Beim Erstellen des WorkSpaces können Sie zwischen den folgenden Funktionsmodi wählen:

- AlwaysOn – Verwenden, wenn Sie einen monatlichen Festbetrag für die unbegrenzte Nutzung Ihrer WorkSpaces zahlen. Dieser Modus eignet sich am besten für Benutzer, die ihren WorkSpace in Vollzeit als primären Desktop verwenden.
- AutoStop – Verwenden, wenn Sie WorkSpaces pro Stunde bezahlen. Bei diesem Modus werden Ihre WorkSpaces nach einer festgelegten getrennten Zeit beendet und der Zustand von Apps und Daten wird gespeichert.

Weitere Informationen dazu finden Sie unter WorkSpaces – Preise.

AutoStop-WorkSpaces

Wählen Sie den WorkSpace in der Amazon-WorkSpaces-Konsole aus, wählen Sie Aktionen, Eigenschaften des Funktionsmodus ändern und legen Sie dann AutoStop-Zeit (Stunden) fest, um die automatische Stoppzeit festzulegen. Standardmäßig ist AutoStop Time (Stunden) auf 1 Stunde eingestellt, was bedeutet, dass der WorkSpace automatisch eine Stunde, nachdem der WorkSpace getrennt wurde, stoppt.

Nachdem die Verbindung zu einem WorkSpace getrennt wurde und die AutoStop-Zeit abgelaufen ist, kann es einige zusätzliche Minuten dauern, bis der WorkSpace automatisch beendet wird. Die Abrechnung wird jedoch beendet, sobald der AutoStop-Zeitraum abgelaufen ist, und Ihnen wird diese zusätzliche Zeit nicht in Rechnung gestellt.

Wenn möglich wird der Zustand des Desktops im Stamm-Volume des WorkSpace gespeichert. Der WorkSpace wird fortgesetzt, wenn sich ein Benutzer anmeldet, und alle offenen Dokumente und laufenden Programme werden in dem Zustand angezeigt, in dem sie zuletzt gespeichert wurden.

AutoStop Graphics.g4dn-, GraphicsPro.g4dn-, Graphics- und GraphicsPro-WorkSpaces behalten den Status von Daten und Programmen beim Beenden nicht bei. Für diese Autostop-WorkSpaces empfehlen wir, Ihre Arbeit jedes Mal zu speichern, wenn Sie sie nicht mehr verwenden.

Bei Bring-Your-Own-License (BYOL)-AutoStop-WorkSpaces könnte eine große Anzahl gleichzeitiger Anmeldungen den Zeitrahmen bis zur Verfügbarkeit von WorkSpaces deutlich erhöhen. Wenn Sie erwarten, dass sich viele Benutzer gleichzeitig bei Ihren BYOL-AutoStop-WorkSpaces anmelden, lassen Sie sich von Ihrem/Ihrer Kundenbetreuer:in beraten.

> **Important**
>
> AutoStop-WorkSpaces stoppen nur automatisch, wenn die WorkSpaces getrennt werden.

Ein WorkSpace wird nur unter den folgenden Umständen getrennt:

- Wenn der/die Benutzer:in manuell die Verbindung zum WorkSpace trennt oder die Amazon-WorkSpaces-Client-Anwendung beendet.
- Wenn das Client-Gerät heruntergefahren ist.
- Wenn länger als 20 Minuten keine Verbindung zwischen dem Client-Gerät und dem WorkSpace besteht.

Es hat sich bewährt, dass AutoStop-WorkSpace-Benutzer die Verbindung zu ihren WorkSpaces manuell trennen, wenn sie sie für den aktuellen Tag nicht mehr verwenden wollen. Wählen Sie im Amazon WorkSpaces-Menü der WorkSpaces-Clientanwendungen für Linux, macOS oder Windows die Option WorkSpace trennen oder Amazon WorkSpaces beenden aus, um die Verbindung manuell zu trennen. Wählen Sie für Android oder iPad im Seitenleistenmenü die Option Trennen aus.

AutoStop-WorkSpaces werden in folgenden Fällen möglicherweise nicht automatisch beendet:

- Wenn das Client-Gerät nur gesperrt, im Ruhemodus oder anderweitig inaktiv ist (z. B. wenn der Laptopdeckel geschlossen ist), anstatt heruntergefahren zu werden, wird die WorkSpaces-Anwendung möglicherweise immer noch im Hintergrund ausgeführt. Solange die WorkSpaces-Anwendung noch läuft, wird der WorkSpace möglicherweise nicht getrennt, sodass der WorkSpace möglicherweise nicht automatisch beendet wird.
- WorkSpaces kann Verbindungsabbrüche nur erkennen, wenn Benutzer WorkSpaces-Clients verwenden. Wenn Benutzer Drittanbieter-Clients verwenden, ist WorkSpaces möglicherweise nicht in der Lage, Inaktivität zu erkennen. Daher stoppt der WorkSpace möglicherweise nicht automatisch und das die Abrechnung wird möglicherweise nicht ausgesetzt.

Ändern des Funktionsmodus

Sie können jederzeit zwischen den verschiedenen Funktionsmodi umschalten.

So ändern Sie den Funktionsmodus eines WorkSpaces

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie den WorkSpace aus, den Sie ändern möchten. Wählen Sie dann Aktionen, Eigenschaften des Funktionsmodus ändern aus.
4. Wählen Sie den neuen Funktionsmodus AlwaysOn oder AutoStop und dann Speichern aus.

So ändern Sie den Funktionsmodus eines WorkSpaces mit der AWS CLI

Verwenden Sie den Befehl modify-workspace-properties.

Anhalten und Starten eines AutoStop-WorkSpace

Wenn Ihre AutoStop-WorkSpaces getrennt sind, werden Sie nach einer festgelegten Inaktivitätsspanne automatisch beendet und die stündliche Abrechnung wird ausgesetzt. Zur weiteren Kostenoptimierung können Sie die Stundengebühren für AutoStop-WorkSpaces manuell aussetzen. Der WorkSpace wird beendet und alle Apps und Daten werden für die nächste Anmeldung eines Benutzers beim WorkSpace gespeichert.

Wenn ein Benutzer erneut eine Verbindung zu einem beendeten WorkSpace herstellt, wird dieser in der Regel in weniger als 90 Sekunden dort fortgesetzt, wo er beendet wurde.

Sie können AutoStop-WorkSpaces, die verfügbar sind oder einen Fehlerzustand aufweisen, neu starten.

So beenden Sie einen AutoStop-WorkSpace

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie den WorkSpace aus, der angehalten werden soll. Wählen Sie dann Aktionen, WorkSpaces anhalten aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie WorkSpace stoppen aus.

So starten Sie einen AutoStop-WorkSpace

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie die WorkSpaces aus, die gestartet werden sollen. Wählen Sie dann Aktionen, WorkSpaces starten aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie WorkSpace starten aus.

Um die mit AutoStop-WorkSpaces verbundenen festen Infrastrukturkosten zu entfernen, entfernen Sie den WorkSpace aus Ihrem Konto. Weitere Informationen finden Sie unter Löschen eines WorkSpaces.

So funktioniert das Anhalten und Starten eines AutoStop-WorkSpace über die AWS CLI

Verwenden Sie die Befehle stop-WorkSpaces und start-WorkSpaces.

Verwalten von Anwendungen

Nachdem Sie eine gestartet haben WorkSpace, können Sie die Liste aller Anwendungspakete, die Ihrem zugeordnet sind, WorkSpace in der - WorkSpaces Konsole anzeigen.

So zeigen Sie die Liste aller Anwendungspakete an, die Ihrem zugeordnet sind WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im linken Navigationsbereich WorkSpaces.
3. Wählen Sie und WorkSpace dann Details anzeigen aus.
4. Suchen Sie unter Anwendungen die Liste der Anwendungen, die diesem zugeordnet sind WorkSpace, zusammen mit ihrem Installationsstatus.

Sie können die Anwendungspakete auf Ihrem WorkSpace wie folgt aktualisieren:

- Installieren von Anwendungspaketen auf Ihrem WorkSpace
- Deinstallieren von Anwendungspaketen von Ihrem WorkSpace
- Installieren von Anwendungspaketen und Deinstallieren eines anderen Satzes von Anwendungspaketen auf Ihrem WorkSpace

> **Note**
>
> - Um Anwendungspakete zu aktualisieren, WorkSpace muss die den Status `AVAILABLE` oder haben`STOPPED`.
> - Anwendungen verwalten ist nur für Windows verfügbar WorkSpaces.
> - Das Verwalten von Anwendungen ist nur für Anwendungspakete verfügbar, die über AWS abonniert wurden.

Unterstützte Pakete für die Anwendungsverwaltung

Mit der Anwendungsverwaltung können Sie die folgenden Anwendungen auf Ihrem installieren und deinstallieren WorkSpaces. Das Microsoft-Office-2016-Paket und Microsoft Office 2019 können Sie nur deinstallieren.

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021

Die folgende Tabelle zeigt die Liste der unterstützten und nicht unterstützten Kombinationen von Anwendungen und Betriebssystemen:

	Microsoft Office Professional Plus 2016 (32-Bit)	Microsoft Office Professional Plus 2019 (64-Bit)	Microsoft LTSC Office Professional Plus / Standard 2021 (64-Bit)	Microsoft Project Professional / Standard 2021 (64-Bit)	Microsoft LTSC Visio Professional / Standard 2021 (64-Bit)
Windows Server 2016	Deinstallieren von	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2019	Nicht unterstützt	Deinstallieren von	Installieren/deinstallieren	Installieren/deinstallieren	Installieren/deinstallieren
Windows Server 2022	Nicht unterstützt	Deinstallieren von	Installieren/deinstallieren	Installieren/deinstallieren	Installieren/deinstallieren
Windows 10	Deinstallieren von	Deinstallieren von	Installieren/deinstallieren	Installieren/deinstallieren	Installieren/deinstallieren
Windows 11	Deinstallieren von	Deinstallieren von	Installieren/deinstallieren	Installieren/deinstallieren	Installieren/deinstallieren

Important

- Diese Anwendungen müssen dieselben Editionen nutzen. Sie können beispielsweise Standard-Anwendungen nicht mit Professional-Anwendungen kombinieren.
- Diese Anwendungen müssen dieselben Versionen nutzen. Sie können beispielsweise 2019-Anwendungen nicht mit 2021-Anwendungen kombinieren.
- Microsoft Office/Visio/Project 2021 Standard/Pro Professionalal werden für Werte, Grafiken und GraphicsPro WorkSpaces Pakete nicht unterstützt.

- Wenn Sie Plus-Anwendungspaket für Microsoft Office 2016 von Ihrem deinstallieren WorkSpaces, verlieren Sie den Zugriff auf alle Trend Micro-Lösungen, die im Rahmen dieses Amazon- WorkSpaces Pakets enthalten waren. Wenn Sie Trend Micro-Lösungen weiterhin mit Ihrem Amazon verwenden möchten WorkSpaces, können Sie sie separat auf dem AWS Marketplace kaufen.
- Sie müssen Ihre eigenen Tools und Installationsprogramme verwenden, um Microsoft-365-Apps zu installieren/deinstallieren. Der Workflow zur Verwaltung von Anwendungen kann Microsoft-365-Apps nicht installieren/deinstallieren.
- Sie können kein benutzerdefiniertes Image von WorkSpaces mit Anwendungen erstellen, die über Anwendungen verwalten installiert wurden, aber Sie können ein benutzerdefiniertes Image von erstellen, WorkSpaces aus dem Sie Anwendungspakete mithilfe von Anwendungen verwalten deinstallieren.
- Die DNS-Auflösung muss aktiviert sein, um die Anwendungsverwaltung verwenden zu können.
- Für Opt-in-Regionen wie Afrika (Kapstadt) muss die WorkSpaces Internetverbindung auf Verzeichnisebene aktiviert sein.

So aktualisieren Sie Anwendungspakete auf einem WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie die WorkSpace und dann Aktionen, Anwendungen verwalten aus.
4. Unter Aktuelle Anwendungen wird eine Liste der Anwendungspakete angezeigt, die bereits darauf WorkSpace installiert sind, und unter Anwendungen auswählen finden Sie eine Liste der Anwendungspakete, die auf diesem installiert werden können WorkSpace.
5. So installieren Sie Anwendungspakete auf diesem WorkSpace:

   a. Wählen Sie ein Anwendungspaket aus, das Sie auf diesem installieren möchten WorkSpace, und wählen Sie Zuordnen aus.

   b. Wiederholen Sie den vorherigen Schritt, um andere Anwendungspakete zu installieren.

   c. Während der Installation der Anwendungspakete werden diese unter Aktuelle Anwendungen mit dem `Pending install deployment`-Status angezeigt.
6. So deinstallieren Sie Anwendungspakete aus diesem WorkSpace:

a. Wählen Sie unter Anwendungen auswählen ein Anwendungspaket aus, das Sie deinstallieren möchten, und klicken Sie auf Zuordnung aufheben.

b. Wiederholen Sie den vorherigen Schritt, um andere Anwendungspakete zu deinstallieren.

c. Während der Deinstallation der Anwendungspakete werden diese unter Aktuelle Anwendungen mit dem `Pending uninstall deployment`-Status angezeigt.

7. Gehen Sie wie folgt vor, um die Installation oder den Installationsstatus der Pakete zurückzusetzen.

   - Wenn Sie den `Pending uninstall deployment`-Status der Pakete wiederherstellen möchten, wählen Sie die Anwendung aus, die Sie wiederherstellen möchten und wählen Sie dann Zuordnen aus.
   - Wenn Sie den `Pending install deployment`-Status der Pakete zurücksetzen möchten, wählen Sie die Anwendung aus, die Sie zurücksetzen möchten und wählen Sie dann Zuordnung trennen aus.

8. Wenn sich die Anwendungspakete, die Sie installieren oder deinstallieren möchten, im Status „Ausstehend“ befinden, wählen Sie Anwendungen bereitstellen aus.

   > **Important**
   >
   > Nachdem Sie Anwendungen bereitstellen ausgewählt haben, wird die Endbenutzersitzung beendet und WorkSpaces ist nicht zugänglich, während die Anwendungen installiert oder deinstalliert werden.

9. Geben Sie Bestätigen ein, um Ihre Aktionen zu bestätigen. Wählen Sie Erzwingen aus, um Anwendungspakete zu installieren oder zu deinstallieren, die sich im Status Fehler befinden.

10. So überwachen Sie den Fortschritt Ihrer Anwendungspakete:

    a. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.

    b. Wählen Sie im Navigationsbereich aus WorkSpaces. Sie können den Status unter Status sehen, einschließlich der folgenden Informationen.

       - AKTUALISIERUNG – Das Update des Anwendungspakets ist noch nicht abgeschlossen.
       - VERFÜGBAR/ABGEBROCHEN – Das Update des Anwendungspakets ist abgeschlossen und der WorkSpace befindet sich wieder in seinem ursprünglichen Zustand.

c. Um den Installations- oder Deinstallationsstatus Ihrer Anwendungspakete zu überwachen, wählen Sie die WorkSpace und dann Details anzeigen aus. Unter Anwendungen können Sie den Status unter Status sehen, einschließlich `Pending install`, `Pending uninstall` und `Installed`.

> **Note**
>
> Wenn Ihre Benutzer feststellen, dass ihre neu installierten Anwendungspakete über Managed Applications nicht lizenzaktiviert sind, können Sie einen manuellen WorkSpace Neustart durchführen. Ihre Benutzer können nach einem Neustart mit der Nutzung dieser Anwendungen beginnen. Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den AWS-Support.

Verwalten von WorkSpaces geänderten mithilfe von Anwendungen verwalten

Nach der Installation oder Deinstallation von Anwendungspaketen auf Ihrem können sich WorkSpacesdie folgenden Aktionen auf bestehende Konfigurationen auswirken.

- Wiederherstellen eines WorkSpace – Beim Wiederherstellen eines werden sowohl das Stamm-Volume als auch das Benutzer-Volume WorkSpace neu erstellt, basierend auf den neuesten Snapshots dieser Volumes, die erstellt wurden, als der fehlerfrei WorkSpace war. Vollständige WorkSpace Snapshots werden alle 12 Stunden erstellt. Weitere Informationen finden Sie unter Wiederherstellen eines WorkSpace. Stellen Sie sicher, dass Sie mindestens 12 Stunden warten, bevor Sie Ihre wiederherstellen WorkSpaces , die mit Anwendungen verwalten geändert wurden. Das Wiederherstellen Ihres WorkSpaces vor dem nächsten vollständigen Snapshot, der mithilfe von Anwendungen verwalten geändert wurde, führt zu Folgendem:
  - Die Anwendungspakete, die WorkSpaces mithilfe des Workflows zum Verwalten von Anwendungen auf Ihrem installiert wurden, werden aus Ihrem entfernt WorkSpaces , aber die Lizenz wird weiterhin aktiviert und Ihrem WorkSpaces werden diese Anwendungen in Rechnung gestellt. Um diese Anwendungspakete wieder in Ihrem zu erhalten, müssen WorkSpaces Sie den Workflow Anwendung verwalten erneut ausführen, die Anwendung deinstallieren, um neu zu beginnen, und dann erneut installieren.
  - Die Anwendungspakete, die WorkSpaces mithilfe des Workflows zum Verwalten von Anwendungen aus Ihrem entfernt wurden, befinden sich wieder in Ihrem WorkSpaces.

Diese Anwendungspakete funktionieren jedoch nicht richtig, da die Lizenzaktivierung fehlt. Um diese Anwendungspakete zu entfernen, führen Sie eine manuelle Deinstallation dieser Anwendungspakete von Ihrem aus WorkSpaces.

- Neuerstellung eines WorkSpace – Beim Neuaufbau eines wird das Stamm-Volume WorkSpace neu erstellt. Weitere Informationen finden Sie unter Neuerstellung eines WorkSpace. Das Neuaufbauen Ihrer WorkSpaces , die mithilfe von Anwendungen verwalten geändert wurden, führt zu Folgendem:
  - Die Anwendungspakete, die auf Ihrem WorkSpaces mit dem Workflow Anwendungen verwalten installiert wurden, werden aus Ihrem entfernt und deaktiviert WorkSpaces. Um diese Anwendungen wieder in Ihr zu integrieren, müssen WorkSpaces Sie den Workflow zum Verwalten von Anwendungen erneut ausführen.
  - Die Anwendungspakete, die WorkSpaces über den Workflow zum Verwalten von Anwendungen aus Ihrem entfernt wurden, werden auf Ihrem installiert und aktiviert WorkSpaces. Um diese Anwendungspakete aus Ihrem zu entfernen WorkSpaces, müssen Sie den Workflow zum Verwalten von Anwendungen erneut ausführen.
- Migrieren eines WorkSpace – Der Migrationsprozess erstellt das neu, WorkSpace indem er ein neues Stamm-Volume aus dem Ziel-Bundle-Image und das Benutzer-Volume aus dem letzten verfügbaren Snapshot des ursprünglichen verwendet WorkSpace. Ein neuer WorkSpace mit einer neuen WorkSpace ID wird erstellt. Weitere Informationen finden Sie unter Migrieren eines WorkSpace s, WorkSpaces das mit Anwendungen verwalten geändert wurde, führt zu Folgendem:
  - Das gesamte Anwendungspaket aus der Quelle WorkSpaces wird entfernt und deaktiviert. Das neue Ziel WorkSpaces erbt Anwendungen vom WorkSpaces Zielpaket. WorkSpaces Quellanwendungspakete werden für den ganzen Monat in Rechnung gestellt, Anwendungspakete im Zielpaket haben jedoch eine anteilige Rechnung.

Ändern eines WorkSpace

Nachdem Sie eine gestartet haben WorkSpace, können Sie ihre Konfiguration auf drei Arten ändern:

- Sie können die Größe des Stammdatenträgers (für Windows Laufwerk „C, für Linux „/“) und dessen Benutzervolume (für Windows Laufwerk „D“, für Linux „/home“) ändern.
- Sie können den Rechentyp ändern, um ein neues Bundle auszuwählen.
- Sie können das Streaming-Protokoll mithilfe der AWS CLI oder Amazon WorkSpaces API ändern, wenn Ihr mit PCoIP-Paketen erstellt WorkSpace wurde.

Um den aktuellen Änderungsstatus eines anzuzeigen WorkSpace, wählen Sie den Pfeil aus, um weitere Details zu diesem anzuzeigen WorkSpace. Die möglichen Werte für State (Status) sind Modifying Compute (Ändern des Servers), Modifying Storage (Ändern des Speichers) und None (Keiner).

Wenn Sie eine ändern möchten WorkSpace, muss sie den Status `AVAILABLE` oder haben`STOPPED`. Sie können nicht gleichzeitig die Volume-Größe und den Datenverarbeitungstyp ändern.

Wenn Sie die Volume-Größe oder den Datenverarbeitungstyp eines ändern WorkSpace , ändert sich der Abrechnungssatz für das WorkSpace.

Informationen dazu, wie Benutzer ihre Volumes und Datenverarbeitungstypen selbst ändern können, finden Sie unter Aktivieren von Self-Service-WorkSpace-Verwaltungsfunktionen für Ihre Benutzer.

Ändern der Volume-Größe

Sie können die Größe der Root- und Benutzer-Volumes für eine auf WorkSpacejeweils 2000 GB erhöhen. WorkSpace Root und Benutzer-Volumes befinden sich in Satzgruppen, die nicht geändert werden können. Die verfügbaren Gruppen sind:

[Root (GB), Benutzer (GB)]
[80, 10]
[80, 50]
[80, 100]
[175 bis 2000, 100 bis 2000]

Sie können die Stamm- und Benutzervolumes erweitern, unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind. Eine solche Erweiterung ist bei beiden Volumes in einem 6-stündigen Zeitraum einmal möglich. Sie können die Größe der Stamm- und Benutzervolumes jedoch nicht gleichzeitig erhöhen. Weitere Informationen finden Sie unter Einschränkungen für das Erhöhen von Volumes.

> **Note**
>
> Wenn Sie ein Volume für ein erweitern WorkSpace, erweitert die Partition des Volumes WorkSpaces automatisch innerhalb von Windows oder Linux. Wenn der Vorgang abgeschlossen ist, müssen Sie den neu starten, damit WorkSpace die Änderungen wirksam werden.

Um sicherzustellen, dass Ihre Daten beibehalten werden, können Sie die Größe der Root- oder Benutzer-Volumes nicht verringern, nachdem Sie eine gestartet haben WorkSpace. Stellen Sie stattdessen sicher, dass Sie die Mindestgrößen für diese Volumes angeben, wenn Sie eine starten WorkSpace. Sie können einen Wert, Standard, Leistung, Leistung oder PowerPro WorkSpace mit mindestens 80 GB für das Stamm-Volume und 10 GB für das Benutzer-Volume starten. Sie können eine Graphics.g4dn, GraphicsPro.g4dn, Graphics oder GraphicsPro WorkSpace mit mindestens 100 GB für das Stamm-Volume und 100 GB für das Benutzer-Volume starten.

Während eine Erhöhung der WorkSpace Festplattengröße ausgeführt wird, können Benutzer die meisten Aufgaben auf ihrem ausführen WorkSpace. Sie können jedoch ihren WorkSpace Datenverarbeitungstyp nicht ändern, den WorkSpace Ausführungsmodus wechseln, ihren neu erstellen WorkSpaceoder ihren neu starten (neu starten WorkSpace).

> **Note**
>
> Wenn Sie möchten, dass Ihre Benutzer ihre verwenden können, WorkSpaces während die Erhöhung der Festplattengröße im Gange ist, stellen Sie sicher, dass die den Status `AVAILABLE` anstelle von WorkSpaces haben, `STOPPED` bevor Sie die Größe der Volumes der ändern WorkSpaces. Wenn die WorkSpaces sind`STOPPED`, können sie nicht gestartet werden, während die Erhöhung der Festplattengröße im Gange ist.

In den meisten Fällen kann der Vorgang zur Erhöhung der Festplattengröße bis zu zwei Stunden dauern. Wenn Sie jedoch die Volume-Größen für eine große Anzahl von ändern WorkSpaces, kann der Vorgang erheblich länger dauern. Wenn Sie eine große Anzahl von ändern WorkSpaces müssen, empfehlen wir Ihnen, sich an zu wenden, um Unterstützung AWS Support zu erhalten.

Einschränkungen beim Erhöhen von Volumes

- Sie können nur die Größe von SSD-Volumes ändern.

- Wenn Sie eine starten WorkSpace, müssen Sie 6 Stunden warten, bevor Sie die Größe ihrer Volumes ändern können.
- Sie können die Größe der Stamm- und Benutzervolumes nicht gleichzeitig erhöhen. Um das Stammvolume zu erhöhen, müssen Sie zuerst das Benutzervolume auf 100 GB ändern. Nachdem diese Änderung vorgenommen wurde, können Sie das Stammvolume auf einen beliebigen Wert zwischen 175 und 2000 GB aktualisieren. Nachdem das Stammvolume auf einen beliebigen Wert zwischen 175 und 2000 GB geändert wurde, können Sie das Benutzervolume anschließend auf einen beliebigen Wert zwischen 100 und 2000 GB aktualisieren.

> **Note**
>
> Wenn Sie beide Volumes erhöhen möchten, müssen Sie 20-30 Minuten warten, bis der erste Vorgang abgeschlossen ist, bevor Sie den zweiten Vorgang starten können.

- Wenn WorkSpace es sich bei nicht um ein Graphics.g4dn-, GraphicsPro.g4dn-, Graphics- oder handelt GraphicsPro WorkSpace, darf das Root-Volume nicht weniger als 175 GB groß sein, wenn das Benutzer-Volume 100 GB groß ist. Graphics.g4dn, GraphicsPro.g4dn, Graphics und GraphicsPro WorkSpaces können die Root- und Benutzer-Volumes auf mindestens 100 GB festlegen.
- Wenn das Benutzervolume 50 GB beträgt, können Sie das Stammvolume nur auf 80 GB aktualisieren. Wenn das Stammvolume 80 GB beträgt, kann das Benutzervolume nur 10, 50 oder 100 GB betragen.

So ändern Sie das Stamm-Volume eines WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie die WorkSpace und dann Aktionen, Stamm-Volume ändern aus.
4. Wählen Sie unter Stammvolume-Größen eine Volume-Größe aus oder wählen Sie Benutzerdefiniert aus, um eine benutzerdefinierte Volume-Größe einzugeben.
5. Wählen Sie Änderungen speichern aus.
6. Wenn die Erhöhung der Festplattengröße abgeschlossen ist, müssen Sie den neu starten WorkSpace, damit die Änderungen wirksam werden. Um Datenverlust zu vermeiden, stellen Sie sicher, dass der Benutzer alle geöffneten Dateien speichert, bevor Sie den neu starten WorkSpace.

So ändern Sie das Benutzer-Volume eines WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie die WorkSpace und dann Aktionen, Benutzervolume ändern aus.
4. Wählen Sie unter Benutzervolume-Größen eine Volume-Größe aus oder wählen Sie Benutzerdefiniert aus, um eine benutzerdefinierte Volume-Größe einzugeben.
5. Wählen Sie Änderungen speichern aus.
6. Wenn die Erhöhung der Festplattengröße abgeschlossen ist, müssen Sie den neu starten WorkSpace, damit die Änderungen wirksam werden. Um Datenverlust zu vermeiden, stellen Sie sicher, dass der Benutzer alle geöffneten Dateien speichert, bevor Sie den neu starten WorkSpace.

So ändern Sie die Volume-Größen eines WorkSpace

Verwenden Sie den modify-workspace-properties Befehl mit der `UserVolumeSizeGib` Eigenschaft `RootVolumeSizeGib` oder .

Ändern von Datenverarbeitungstypen

Sie können zwischen WorkSpace den PowerPro Datenverarbeitungstypen Standard, Leistung, Leistung und wechseln. Weitere Informationen zu diesen Datenverarbeitungstypen finden Sie unter Amazon WorkSpaces-Pakete.

> **Note**
>
> - Sie können den Datenverarbeitungstyp von Graphics.g4dn in GraphicsPro.g4dn oder von GraphicsPro.g4dn in Graphics.g4dn ändern. Sie können den Datenverarbeitungstyp von Graphics.g4dn und GraphicsPro.g4dn nicht in einen anderen Wert ändern.
> - Das Graphics-Paket wird nach dem 30. November 2023 nicht mehr unterstützt. Wir empfehlen, Ihr WorkSpaces zu Graphics.g4dn-Paket zu migrieren. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.
> - Sie können den Datenverarbeitungstyp von Graphics und nicht GraphicsPro auf einen anderen Wert ändern.

Wenn Sie eine Datenverarbeitungsänderung anfordern, startet die WorkSpace mit dem neuen Datenverarbeitungstyp WorkSpaces neu. WorkSpaces behält das Betriebssystem, Anwendungen, Daten und Speichereinstellungen für bei WorkSpace.

Sie können alle 6 Stunden einen größeren Datenverarbeitungstyp oder alle 30 Tage einen kleineren Datenverarbeitungstyp anfordern. Bei einem neu gestarteten müssen Sie 6 Stunden warten WorkSpace, bevor Sie einen größeren Datenverarbeitungstyp anfordern.

Wenn eine Änderung des WorkSpace Datenverarbeitungstyps ausgeführt wird, werden Benutzer von ihrem getrennt WorkSpaceund können den nicht verwenden oder ändern WorkSpace. Die WorkSpace wird während des Prozesses zur Änderung des Datenverarbeitungstyps automatisch neu gestartet.

> **Important**
>
> Um Datenverlust zu vermeiden, stellen Sie sicher, dass Benutzer alle geöffneten Dokumente und andere Anwendungsdateien speichern, bevor Sie den WorkSpace Datenverarbeitungstyp ändern.

Der Prozess zur Änderung des Datenverarbeitungstyps kann bis zu einer Stunde dauern.

So ändern Sie den Datenverarbeitungstyp eines WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie die WorkSpace und dann Aktionen, Datenverarbeitungstyp ändern aus.
4. Wählen Sie unter Datenverarbeitungstyp einen Datenverarbeitungstyp aus.
5. Wählen Sie Änderungen speichern aus.

So ändern Sie den Datenverarbeitungstyp eines WorkSpace

Verwenden Sie den -modify-workspace-propertiesBefehl mit der -`ComputeTypeName`Eigenschaft.

Modifizieren von Protokollen

Wenn Ihr mit PCoIP-Paketen erstellt WorkSpace wird, können Sie sein Streaming-Protokoll mithilfe der AWS CLI oder der Amazon WorkSpaces -API ändern. Auf diese Weise können Sie das Protokoll mit Ihrem vorhandenen migrieren, WorkSpace ohne die WorkSpace Migrationsfunktion

zu verwenden. Auf diese Weise können Sie auch das WorkSpaces Streaming Protocol (WSP) verwenden und Ihr Stamm-Volume verwalten, ohne während des Migrationsprozesses eine bestehende PCoIP WorkSpaces neu zu erstellen.

- Sie können Ihr Protokoll nur ändern, wenn Ihr mit PCoIP-Paketen erstellt WorkSpace wurde.
- Bevor Sie das Protokoll in WSP ändern, stellen Sie sicher, dass Ihr die folgenden Anforderungen für einen WSP WorkSpace erfüllt WorkSpace.
  - Ihr WorkSpaces Client unterstützt WSP
  - Die Region, in der Ihr bereitgestellt WorkSpace wird, unterstützt WSP
  - Die IP-Adresse und die erforderlichen Ports für WSP sind offen. Weitere Informationen finden Sie unter IP-Adresse und Port-Anforderungen für WorkSpaces.
  - Stellen Sie sicher, dass Ihr aktuelles Paket mit WSP verfügbar ist.
  - Für ein optimales Erlebnis mit Videokonferenzen empfehlen wir, nur Power- oder PowerPro Bundles zu verwenden.

> **Note**
>
> - Wir empfehlen dringend, mit Ihrer Nicht-Produktion zu testen, WorkSpaces bevor Sie mit dem Ändern des Protokolls beginnen.
> - Wenn Sie das Protokoll von PCoIP zu WSP und dann wieder zu PCoIP ändern, können Sie WorkSpaces über Web Access keine Verbindung zu herstellen.

So ändern Sie das Protokoll eines WorkSpace

1. [Optional] Starten Sie Ihre neu WorkSpace und warten Sie, bis sie sich im `AVAILABLE` Status befindet, bevor Sie das Protokoll ändern.
2. [Optional] Verwenden Sie den `describe-workspaces` Befehl , um die WorkSpace Eigenschaften aufzulisten. Vergewissern Sie sich, dass er im `AVAILABLE`-Status ist und dass der aktuelle `Protocol` korrekt ist.
3. Verwenden Sie den `modify-workspace-properties`-Befehl und ändern Sie die `Protocols`-Eigenschaft von `PCOIP` zu `WSP` oder umgekehrt.

```
aws workspaces modify-workspace-properties
--workspace-id <value>
```

```
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> Die `Protocols`-Eigenschaft berücksichtigt Groß- und Kleinschreibung. Stellen Sie sicher, dass Sie `PCOIP` oder `WSP` verwenden.

4. Nachdem Sie den Befehl ausgeführt haben, kann es bis zu 20 Minuten dauern WorkSpace , bis neu gestartet und die erforderlichen Konfigurationen abgeschlossen werden.
5. Verwenden Sie den `describe-workspaces` Befehl erneut, um die WorkSpace Eigenschaften aufzulisten und zu überprüfen, ob sie sich in einem -`AVAILABLE`Status befinden und die aktuelle `Protocols` Eigenschaft in das richtige Protokoll geändert wurde.

> **Note**
>
> - Durch das Ändern des WorkSpaceProtokolls von wird die Bundle-Beschreibung in der Konsole nicht aktualisiert. Die Beschreibung des Startpakets wird sich nicht ändern.
> - Wenn die nach 20 Minuten in einem -`UNHEALTHY`Status WorkSpace bleibt, starten Sie die WorkSpace in der -Konsole neu.

6. Sie können jetzt eine Verbindung zu Ihrem herstellen WorkSpace.

Anpassen des WorkSpace Brandings

Mit Amazon WorkSpaces können Sie eine vertraute WorkSpaces Erfahrung für Ihre Benutzer erstellen, indem Sie APIs verwenden, um das Erscheinungsbild der Anmeldeseite Ihres mit Ihrem eigenen Branding-Logo, IT-Supportinformationen, Link zum WorkSpacevergessenen Passwort und Anmeldenachricht anzupassen. Ihr Branding wird Ihren Benutzern auf ihrer WorkSpace Anmeldeseite angezeigt, nicht dem Standard- WorkSpaces Branding.

Folgende Clients werden unterstützt:

- Windows
- Linux
- Android
- MacOS

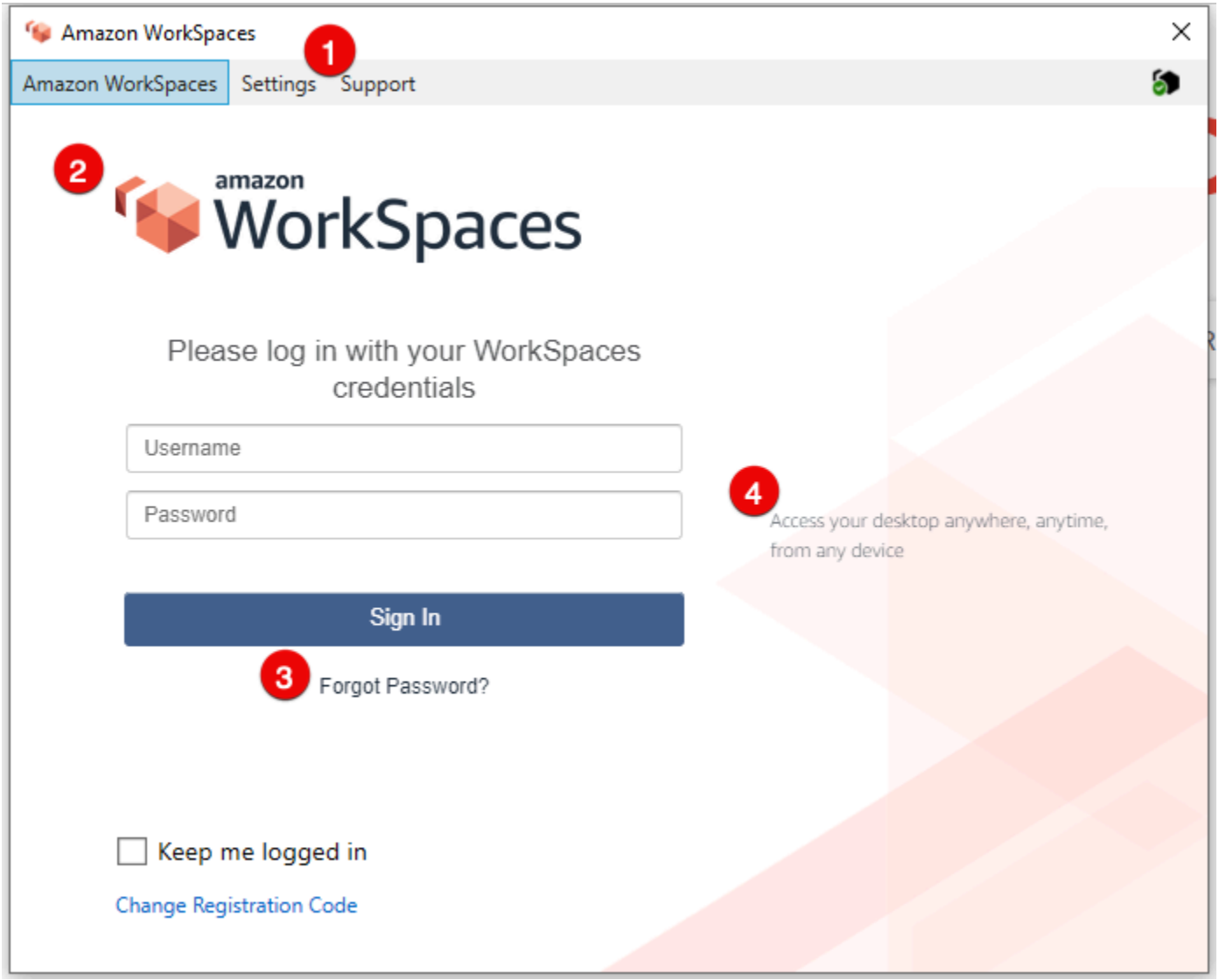
- iOS
- Web Access

> **Note**
>
> Um Branding-Elemente mithilfe der ClientBranding APIs in der zu ändernAWS GovCloud (US) Region, verwenden Sie eine WorkSpaces Client-Version 5.10.0.

Importieren eines benutzerdefinierten Brandings

Verwenden Sie die Aktion `ImportClientBranding`, die die folgenden Elemente umfasst, um Ihre Client-Branding-Anpassung zu importieren. Weitere Informationen finden Sie in der ImportClientBranding -API-Referenz.

> **Important**
>
> Die Branding-Attribute von Client sind öffentlich zugänglich. Stellen Sie sicher, dass Sie keine sensiblen Informationen verwenden.



1. Support link
2. Logo
3. Link für „Passwort vergessen“
4. Anmeldenachricht

Benutzerdefinierte Branding-Elemente

Branding-Element	Beschreibung	Anforderungen und Empfehlungen
Support link	Ermöglicht Ihnen die Angabe eines Support-E-Mail-Links,	• Pro Plattformtyp schließen sich die Parameter

Branding-Element	Beschreibung	Anforderungen und Empfehlungen
	mit dem Benutzer sich an wenden können, um Hilfe bei ihrem zu erhalten WorkSpaces. Sie können das `SupportEmail` -Attribut verwenden oder mithilfe des `SupportLink` -Attributs einen Link zu Ihrer Support-Seite bereitstellen.	`SupportEmail` und `SupportLink` gegenseitig aus. Sie können einen einzelnen Parameter für jeden Plattformtyp angeben, aber nicht beides. • Die Standard-E-Mail ist `workspaces-feedback@amazon.com` . • Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 200 Zeichen.

Logo	Ermöglicht es Ihnen, das Logo Ihrer Organisation mithilfe des Logo-Attributs anzupassen.	• Das einzige zulässige Bildformat ist ein binäres Datenobjekt, das aus einer `.png`-Datei konvertiert wird.
		• Empfohlene Auflösungen:
		  • Android: 978 x 190
		  • Desktop: 319 x 55
		  • iOS@2x: 110 x 200
		  • iOS@3x: 1650 x 300

Link für „Passwort vergessen“	Ermöglicht das Hinzufügen einer Webadresse mit dem ForgotPasswordLink Attribut , zu dem Benutzer gehen können, wenn sie ihr Passwort für ihr vergessen WorkSpace.	Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Höchstlänge = 200 Zeichen.

Branding-Element	Beschreibung	Anforderungen und Empfehlungen
Anmeldenachricht	Ermöglicht es Ihnen, eine Nachricht mithilfe des `LoginMessage` -Attributs auf dem Anmeldebildschirm anzupassen.	• Längenbeschränkungen: Minimale Länge von 0. Maximale Länge von 2000 Zeichen für die Integration mit HTML-Tags und unterschiedlicher Schriftgröße. Für Standardfälle ohne HTML-Tags wird empfohlen, die Anmeldenachricht unter 600 Zeichen zu halten. • Unterstützte SSML-Tags: `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

Im Folgenden finden Sie Beispielcodeausschnitte für die Verwendung von ImportClientBranding.

AWS-CLI Version 2

> **Warning**
>
> Beim Import von benutzerdefiniertem Branding werden die Attribute, die Sie innerhalb dieser Plattform angeben, mit Ihren benutzerdefinierten Daten überschrieben. Außerdem werden die Attribute, die Sie nicht angeben, durch Standardwerte für benutzerdefinierte Branding-Attribute überschrieben. Sie müssen die Daten für jedes Attribut angeben, das Sie nicht überschreiben möchten.

```
aws workspaces import-client-branding \
```

```
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

Die Import-JSON-Datei sollte wie folgt aussehen:

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

Der folgende Java-Beispielcodeausschnitt konvertiert das Logobild in eine base64-kodierte Zeichenfolge:

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

Der folgende Python-Beispielcodeausschnitt konvertiert das Logobild in eine base64-kodierte Zeichenfolge:

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> Beim Import von benutzerdefiniertem Branding werden die Attribute, die Sie innerhalb dieser Plattform angeben, mit Ihren benutzerdefinierten Daten überschrieben. Außerdem werden die Attribute, die Sie nicht angeben, durch Standardwerte für benutzerdefinierte Branding-Attribute überschrieben. Sie müssen die Daten für jedes Attribut angeben, das Sie nicht überschreiben möchten.

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> Beim Import von benutzerdefiniertem Branding werden die Attribute, die Sie innerhalb dieser Plattform angeben, mit Ihren benutzerdefinierten Daten überschrieben. Außerdem werden die Attribute, die Sie nicht angeben, durch Standardwerte für benutzerdefinierte Branding-Attribute überschrieben. Sie müssen die Daten für jedes Attribut angeben, das Sie nicht überschreiben möchten.

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"
```

```
# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

Um eine Vorschau der Anmeldeseite anzuzeigen, starten Sie die WorkSpaces Anwendung oder die Web-Anmeldeseite.

> **Note**
>
> Es kann bis zu 1 Minute dauern, bis Änderungen angezeigt werden.

Beschreiben des benutzerdefinierten Brandings

Verwenden Sie die Aktion `DescribeCustomBranding`, um die Details der Anpassung des Client-Brandings anzuzeigen, die Sie derzeit verwenden. Im Folgenden finden Sie das Beispielskript für die Verwendung von DescribeClientBranding. Weitere Informationen finden Sie in der DescribeClientBranding -API-Referenz.

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

Löschen des benutzerdefinierten Brandings

Verwenden Sie die Aktion `DeleteCustomBranding`, um Ihre Client-Branding-Anpassung zu löschen. Im Folgenden finden Sie das Beispielskript für die Verwendung von DeleteClientBranding. Weitere Informationen finden Sie in der DeleteClientBranding -API-Referenz.

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> Es kann bis zu 1 Minute dauern, bis Änderungen angezeigt werden.

Markieren von WorkSpaces-Ressourcen

Sie können die Ressourcen für Ihre WorkSpaces organisieren und verwalten, indem Sie jeder Ressource Ihre eigenen Metadaten in Form von Tags zuweisen. Sie geben für jedes Tag einen Schlüssel und einen Wert an. Ein Schlüssel kann einer allgemeinen Kategorie angehören, wie zum Beispiel "Projekt", "Eigentümer" oder "Umgebung", die über bestimmte zugehörige Werte verfügen. Die Verwendung von Tags ist ein einfacher, aber effizienter Weg, um AWS-Ressourcen zu verwalten und Daten, einschließlich Fakturierungsdaten, zu organisieren.

Wenn Sie einer vorhandenen Ressource Tags hinzufügen, werden diese Tags erst am ersten Tag des Folgemonats in Ihrem Kostenzuordnungsbericht angezeigt. Wenn Sie einem vorhandenen WorkSpace beispielsweise am 15. Juli Tags hinzufügen, erscheinen die Tags erst am 1. August in Ihrem Kostenzuordnungsbericht. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS BillingLeitfaden.

> **Note**
>
> Zur Anzeige Ihrer WorkSpaces-Tags im Cost Explorer müssen Sie die Tags aktivieren, die Sie auf Ihre WorkSpaces-Ressourcen angewendet haben. Folgen Sie dazu den Anweisungen unter Aktivieren von benutzerdefinierten Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch.
> Obwohl Tags 24 Stunden nach der Aktivierung angezeigt werden, kann es 4 bis 5 Tage dauern, bis die mit diesen Tags verknüpften Werte im Cost Explorer angezeigt werden. Damit Kostendaten im Cost Explorer angezeigt und bereitgestellt werden können, müssen für WorkSpaces-Ressourcen, die mit Tags versehen wurden, während dieser Zeit Gebühren anfallen. Der Cost Explorer zeigt nur Kostendaten ab dem Zeitpunkt an, an dem die Tags aktiviert wurden, und darüber hinaus. Derzeit sind keine Verlaufsdaten verfügbar.

Ressourcen, die mit Tags versehen werden können

- Sie können die folgenden Ressourcen bei ihrer Erstellung von Markierungen hinzufügen: WorkSpaces, importierte Abbilder und IP-Zugriffskontrollgruppen.

- Sie können Tags zu vorhandenen Ressourcen der folgenden Typen hinzufügen: WorkSpaces, registrierte Verzeichnisse, benutzerdefinierte Pakete, Abbilder und IP-Zugriffskontrollgruppen.

Tag (Markierung)-Einschränkungen

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 127 Unicode-Zeichen
- Maximale Wertlänge: 255 Unicode-Zeichen
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen.
- Verwenden Sie in Tag-Namen oder -Werten nicht die Präfixe `aws:` oder `aws:workspaces:`, das sie für die AWS-Verwendung reserviert ist. Tag-Namen oder Werte mit diesen Präfixen können nicht bearbeitet oder gelöscht werden.

So aktualisieren Sie die Tags für eine bestehende Ressource mithilfe der Konsole (Verzeichnisse, WorkSpaces oder IP-Zugriffskontrollgruppen)

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich einen der folgenden Ressourcentypen aus: Verzeichnisse, WorkSpaces oder IP-Zugriffskontrollen.
3. Wählen Sie die Ressource aus, um ihre Detailseite zu öffnen.
4. Führen Sie eine oder mehrere der folgenden Aktionen aus:
   - Um ein Tag zu aktualisieren, bearbeiten Sie die Werte für Key und Value.
   - Um ein Tag hinzuzufügen, wählen Sie Add Tag aus und bearbeiten anschließend die Werte für Key und Value.
   - Um ein Tag zu löschen, wählen Sie das Symbol "Löschen" (x) neben dem Tag.
5. Wenn Sie mit dem Aktualisieren der Tags fertig sind, wählen Sie Save aus.

So aktualisieren Sie die Tags für eine vorhandene Ressource mithilfe der Konsole (Abbilder oder Pakete)

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.

2. Wählen Sie im Navigationsbereich einen der folgenden Ressourcentypen aus: Pakete oder Images.
3. Wählen Sie die Ressource aus, um ihre Detailseite zu öffnen.
4. Wählen Sie unter Tags die Option Manage tags (Tags verwalten) aus.
5. Führen Sie eine oder mehrere der folgenden Aktionen aus:
   - Um ein Tag zu aktualisieren, bearbeiten Sie die Werte für Key und Value.
   - Um ein Tag hinzuzufügen, wählen Sie Tag hinzufügen aus und bearbeiten anschließend die Werte für Schlüssel und Wert.
   - Um ein Tag zu löschen, wählen Sie Entfernen neben dem Tag.
6. Wenn Sie die Aktualisierung der Tags abgeschlossen haben, wählen Sie Änderungen speichern.

So aktualisieren Sie die Tags für eine vorhandene Ressource mithilfe der AWS CLI

Verwenden Sie die Befehle create-tags und delete-tags.

Warten von WorkSpace

Wir empfehlen Ihnen, Ihre WorkSpaces regelmäßig zu warten. WorkSpaces plant Standard-Wartungsfenster für Ihre WorkSpaces. Innerhalb des Wartungsfensters installiert der WorkSpace wichtige Updates von Amazon WorkSpaces und führt nötigenfalls einen Neustart durch. Falls verfügbar, werden Betriebssystemupdates auch vom Betriebssystemaktualisierungsserver installiert, für den der WorkSpace konfiguriert ist. Während der Wartung sind die WorkSpaces unter Umständen nicht verfügbar.

Standardmäßig sind Ihre Windows-WorkSpaces so konfiguriert, dass sie Updates von Windows Update empfangen. Informationen zum Konfigurieren eigener Mechanismen für automatische Updates für Windows finden Sie in der Dokumentation zu Windows Server Update Services (WSUS) und Configuration Manager.

Anforderung

Ihre WorkSpaces müssen Zugriff auf das Internet haben, damit Sie Updates für das Betriebssystem installieren und Anwendungen bereitstellen können. Weitere Informationen finden Sie unter the section called “Internetzugang”.

Wartungsfenster für AlwaysOn-WorkSpaces

Für AlwaysOn-WorkSpaces wird das Wartungsfenster durch die Betriebssystem-Einstellungen bestimmt. Der Standardwert ist ein 4-Stunden-Zeitraum von 00:00 Uhr bis 04:00 Uhr an jedem Sonntagmorgen in der Zeitzone des WorkSpace. Standardmäßig wird die Zeitzone eines AlwaysOn-WorkSpace in die Zeitzone der AWS-Region für den WorkSpace gelegt. Wenn Sie jedoch bei aktivierter Zeitzonen-Umleitung eine Verbindung von einer anderen Region herstellen und die Verbindung dann trennen, wird die Zeitzone des WorkSpace auf die Zeitzone der Region aktualisiert, aus der Sie sich verbunden haben.

Sie können die Zeitzonenumleitung für Windows-WorkSpaces mithilfe von Gruppenrichtlinien deaktivieren. Sie können die Zeitzonenumleitung für Linux-WorkSpaces deaktivieren, indem Sie die PCoIP-Agent-conf verwenden.

Für Windows-WorkSpaces können Sie das Wartungsfenster mittels einer Gruppenrichtlinie konfigurieren. Weitere Informationen finden Sie unter Configure Group Policy Settings for Automatic Updates. Das Wartungsfenster für Linux-WorkSpaces kann nicht von Ihnen konfiguriert werden.

Wartungsfenster für AutoStop-WorkSpaces

AutoStop-WorkSpaces werden automatisch einmal pro Monat gestartet, um wichtige Updates zu installieren. Ab dem dritten Montag des Monats und für bis zu zwei Wochen ist das Wartungsfenster in der Zeitzone der AWS-Region für den WorkSpace jeden Tag von 00:00 bis 05:00 geöffnet. Der WorkSpace kann an jedem beliebigen Tag im Wartungsfenster gewartet werden. Während dieses Zeitfensters werden nur WorkSpaces verwaltet, die älter als 7 Tage sind.

Während des Zeitraums, in dem der WorkSpace gewartet wird, wird der Status des WorkSpace auf `MAINTENANCE` eingestellt.

Obwohl Sie die Zeitzone, die zum Verwalten von AutoStop-WorkSpaces verwendet wird, nicht ändern können, können Sie das Wartungsfenster für Ihre AutoStop-WorkSpaces wie folgt deaktivieren. Wenn Sie den Wartungsmodus deaktivieren, werden Ihre WorkSpaces nicht neu gestartet und gehen nicht in den Zustand `MAINTENANCE` über.

So deaktivieren Sie den Wartungsmodus

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Actions, Update Details aus.

4. Erweitern Sie Maintenance Mode.
5. Um automatische Updates zu aktivieren, wählen Sie Enabled aus. Wenn Sie es vorziehen, Updates manuell zu verwalten, wählen Sie Disabled (Deaktiviert) aus.
6. Wählen Sie Update and Exit aus.

Manuelle Wartung

Wenn Sie möchten, können Sie Ihre WorkSpaces nach einem eigenen Zeitplan warten. Wenn Sie Wartungsaufgaben ausführen, empfehlen wir, dass Sie den Status des WorkSpace zu Wartung ändern. Wenn Sie fertig sind, können Sie den Status des WorkSpace wieder zu Verfügbar ändern.

Wenn sich ein WorkSpace im Status Wartung befindet, treten die folgenden Verhaltensweisen auf:

- Der WorkSpace reagiert nicht auf Anforderungen, neu zu starten, zu stoppen, zu starten oder neu zu erstellen.
- Benutzer können sich nicht beim WorkSpace anmelden.
- Ein AutoStop-WorkSpace wird nicht in den Ruhezustand versetzt.

So ändern Sie den Status des WorkSpace mithilfe der Konsole

> **Note**
>
> Zum Ändern des Status eines WorkSpace muss der WorkSpace den Status Verfügbar haben. Die Einstellung Status ändern ist nicht verfügbar, wenn sich ein WorkSpace nicht im Status Verfügbar befindet.

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie den WorkSpace und anschließend Aktionen, Status ändern aus.
4. Wählen Sie unter Status ändern die Option Verfügbar oder Wartung aus.
5. Wählen Sie Save (Speichern).

So ändern Sie den Status des WorkSpace mithilfe der AWS CLI

Verwenden Sie den Befehl modify-workspace-state.

Verschlüsselte WorkSpaces

WorkSpaces ist mit AWS Key Management Service (AWS KMS) integriert. Dadurch können Sie Speichervolumes von WorkSpaces mit AWS KMS-Schlüsseln verschlüsseln. Wenn Sie einen WorkSpace starten, können Sie das Stamm-Volume (unter Microsoft Windows Laufwerk „C“, unter Linux „/“) und das Benutzer-Volume (unter Windows Laufwerk „D“, unter Linux „/home“) verschlüsseln. Auf diese Weise wird sichergestellt, dass Daten im Ruhezustand, Festplatten-Ein-/Ausgaben und Snapshots von Volumes verschlüsselt werden.

> **Note**
>
> Zusätzlich zur Verschlüsselung Ihrer WorkSpaces können Sie in bestimmten AWS-US-Regionen auch die FIPS-Endpunktverschlüsselung verwenden. Weitere Informationen finden Sie unter Einrichten von Amazon WorkSpaces für die FedRAMP-Autorisierung oder DoD-SRG-Compliance.

Inhalt

Voraussetzungen

Sie benötigen einen AWS KMS-Schlüssel, bevor Sie die Verschlüsselung beginnen können. Dieser KMS-Schlüssel kann entweder der von AWS verwaltete KMS-Schlüssel für Amazon WorkSpaces (aws/workspaces) oder ein symmetrischer, vom Kunden verwalteter KMS-Schlüssel sein.

- Von AWS verwaltete KMS-Schlüssel – Wenn Sie einen nicht verschlüsselten WorkSpace erstmals über die WorkSpaces-Konsole in einer Region starten, erstellt Amazon WorkSpaces automatisch einen von AWS verwalteten CMK-Schlüssel (aws/workspaces) in Ihrem Konto. Sie können diesen von AWS verwalteten Schlüssel zum Verschlüsseln der Benutzer- und Stammvolumes

Ihres WorkSpace auswählen. Details hierzu finden Sie unter Übersicht über die WorkSpaces-Verschlüsselung mit AWS KMS.

Sie können diesen von AWS verwalteten KMS-Schlüssel, einschließlich seiner Richtlinien und Berechtigungserteilungen, anzeigen und seine Verwendung in AWS CloudTrail-Protokollen nachverfolgen, aber Sie können diesen KMS-Schlüssel nicht verwenden oder verwalten. Amazon WorkSpaces erstellt und verwaltet diesen KMS-Schlüssel. Dieser KMS-Schlüssel kann nur von Amazon WorkSpaces und nur zum Verschlüsseln von WorkSpaces-Ressourcen in Ihrem Konto verwendet werden.

Von AWS verwaltete Schlüssel, einschließlich des von Amazon WorkSpaces unterstützten Schlüssels, werden alle drei Jahre rotiert. Details dazu finden Sie unter Rotieren von AWS KMS-Schlüsseln im Entwicklerhandbuch für .

- Vom Kunden verwalteter KMS-Schlüssel – Alternativ können Sie einen symmetrischen, vom Kunden verwalteten KMS-Schlüssel auswählen, den Sie mit AWS KMS erstellt haben. Sie können diesen KMS-Schlüssel anzeigen, verwenden und verwalten, einschließlich Festlegen seiner Richtlinien. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service-Entwicklerhandbuch. Weitere Informationen zum Erstellen von KMS-Schlüsseln mit der AWS KMS-API finden Sie unter Arbeiten mit Schlüsseln im AWS Key Management Service-Entwicklerhandbuch.

  Vom Kunden verwaltete KMS-Schlüssel werden nicht automatisch rotiert, es sei denn, Sie entscheiden sich dafür, die automatische Schlüsselrotation zu aktivieren. Details dazu finden Sie unter Rotieren von AWS KMS-Schlüsseln im Entwicklerhandbuch für AWS Key Management Service.

> **Important**
>
> Wenn Sie KMS-Schlüssel manuell rotieren, müssen Sie sowohl den ursprünglichen KMS-Schlüssel als auch den neuen KMS-Schlüssel aktiviert lassen, damit AWS KMS die WorkSpaces, die der ursprüngliche KMS-Schlüssel verschlüsselt hat, entschlüsseln kann. Wenn Sie den ursprünglichen KMS-Schlüssel nicht aktiviert lassen möchten, müssen Sie Ihre WorkSpaces neu erstellen und sie mit dem neuen KMS-Schlüssel verschlüsseln.

Folgende Anforderungen müssen erfüllt sein, damit Sie einen AWS KMS-Schlüssel für die Verschlüsselung Ihrer WorkSpaces verwenden können:

- Der KMS-Schlüssel muss symmetrisch sein. Amazon WorkSpaces unterstützt keine asymmetrischen KMS-Schlüssel. Informationen zum Unterscheiden zwischen symmetrischen und asymmetrischen KMS-Schlüsseln finden Sie unter Identifizieren symmetrischer und asymmetrischer KMS-Schlüssel im AWS Key Management Service-Entwicklerhandbuch.
- Der KMS-Schlüssel muss aktiviert sein. Informationen darüber, ob ein KMS-Schlüssel aktiviert ist, finden Sie unter Anzeigen von KMS-Schlüsseldetails im AWS Key Management Service-Entwicklerhandbuch.
- Dem KMS-Schlüssel müssen die richtigen Berechtigungen und Richtlinien zugeordnet sein. Weitere Informationen finden Sie unter Teil 2: Erteilen von zusätzlichen Berechtigung für WorkSpaces-Administratoren mit einer IAM-Richtlinie.

Einschränkungen

- Sie können einen vorhandenen WorkSpace nicht verschlüsseln. Sie müssen einen WorkSpace verschlüsseln, wenn Sie ihn starten.
- Das Erstellen eines benutzerdefinierten Abbilds von einem verschlüsselten WorkSpace wird nicht unterstützt.
- Das Deaktivieren der Verschlüsselung für einen verschlüsselten WorkSpace wird derzeit nicht unterstützt.
- Bei WorkSpaces, die mit aktivierter Stamm-Volume-Verschlüsselung gestartet werden, kann die Bereitstellung bis zu einer Stunde dauern.
- Stellen Sie zunächst sicher, dass der AWS KMS-Schlüssel aktiviert ist, um einen verschlüsselten WorkSpace neu zu starten oder neu zu erstellen. Andernfalls kann der WorkSpace nicht mehr benutzt werden. Informationen darüber, ob ein KMS-Schlüssel aktiviert ist, finden Sie unter Anzeigen von KMS-Schlüsseldetails im AWS Key Management Service-Entwicklerhandbuch.

Übersicht über die WorkSpaces-Verschlüsselung mit AWS KMS

Wenn Sie WorkSpaces mit verschlüsselten Volumes erstellen, verwendet WorkSpaces Amazon Elastic Block Store (Amazon EBS), um diese Volumes zu erstellen und verwalten. Amazon EBS verschlüsselt Ihr Volume mit einem Datenschlüssel mithilfe des branchenüblichen AES-256-Algorithmus. Sowohl Amazon EBS als auch Amazon WorkSpaces verwenden Ihren KMS-Schlüssel, um mit den verschlüsselten Volumes zu arbeiten. Weitere Informationen zur EBS-Verschlüsselung von Volumes finden Sie unter Amazon-EBS-Verschlüsselung im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

Wenn Sie WorkSpaces mit verschlüsselten Volumes starten, wird der End-to-End-Prozess folgendermaßen durchgeführt:

1. Sie geben den KMS-Schlüssel für die Verschlüsselung, den/die WorkSpace-Benutzer:in und das WorkSpace-Verzeichnis an. Diese Aktion erstellt eine Erteilung, mit der WorkSpaces Ihren KMS-Schlüssel nur für diesen WorkSpace, also nur für den dem/der angegebenen Benutzer:in und Verzeichnis zugeordneten WorkSpace, verwenden darf.
2. WorkSpaces erstellt ein verschlüsseltes EBS-Volume für den WorkSpace und legt den zu verwendenden KMS-Schlüssel sowie den/die Benutzer:in und das Verzeichnis des Volumes fest. Diese Aktion erstellt eine Erteilung, mit der Amazon EBS Ihren KMS-Schlüssel nur für diesen WorkSpace und dieses Volume, also nur für den dem/der angegebenen Benutzer:in und Verzeichnis zugeordneten WorkSpace und nur für das angegebene Volume, verwenden darf.
3. Amazon EBS fordert einen Volume-Datenschlüssel an, der mit Ihrem KMS-Schlüssel verschlüsselt ist, und gibt die Active-Directory-SID (Security Identifier) des WorkSpace-Benutzers, die AWS Directory Service-Verzeichnis-ID und die Volume-ID als Verschlüsselungskontext an.
4. AWS KMS erstellt einen neuen Datenschlüssel, verschlüsselt diesen mit Ihrem KMS-Schlüssel und sendet den verschlüsselten Datenschlüssel an Amazon EBS.
5. WorkSpaces nutzt Amazon EBS, um das verschlüsselte Volume an Ihren WorkSpace anzufügen. Amazon EBS sendet den verschlüsselten Datenschlüssel an AWS KMS mit einer `Decrypt`-Anforderung und gibt die SID des WorkSpace-Benutzers, seine Verzeichnis-ID und die Volume-ID an, die als Verschlüsselungskontext verwendet wird.
6. AWS KMS verwendet Ihren KMS-Schlüssel, um den Datenschlüssel zu entschlüsseln, und sendet den Klartext-Datenschlüssel an Amazon EBS.
7. Amazon EBS verwendet den Klartext-Datenschlüssel, um alle eingehenden und ausgehenden Daten vom verschlüsselten Volume zu verschlüsseln. Amazon EBS speichert den Klartext-Datenschlüssel so lange, wie das Volume dem WorkSpace angefügt ist.
8. Amazon EBS speichert den verschlüsselten Datenschlüssel (eingegangen in Step 4) mit den Volume-Metadaten für die künftige Nutzung und für den Fall, dass Sie den WorkSpace neu starten oder wiederherstellen müssen.
9. Wenn Sie mit der AWS Management Console einen WorkSpace entfernen (oder die Aktion `TerminateWorkspaces` der WorkSpaces-API verwenden), heben WorkSpaces und Amazon EBS die Erteilungen auf, die ihnen die Nutzung Ihres KMS-Schlüssels für diesen WorkSpace erlaubt hat.

WorkSpaces-Verschlüsselungskontext

WorkSpaces verwendet Ihren KMS-Schlüssel direkt für kryptografische Operationen (z. B. `Encrypt`, `Decrypt`, `GenerateDataKey` usw.), was bedeutet, dass WorkSpaces keine Anforderungen an AWS KMS sendet, die einen Verschlüsselungskontext enthalten. Wenn Amazon EBS jedoch einen verschlüsselten Datenschlüssel für die verschlüsselten Volumes Ihres WorkSpace (Step 3 in der Übersicht über die WorkSpaces-Verschlüsselung mit AWS KMS) und eine Klartext-Kopie dieses Datenschlüssels (Step 5) anfordert, enthält die Anforderung Verschlüsselungskontext.

Der Verschlüsselungskontext enthält zusätzliche authentifizierte Daten (AAD), anhand derer AWS KMS die Datenintegrität sicherstellt. Der Verschlüsselungskontext wird zudem in Ihre AWS CloudTrail-Protokolldateien geschrieben, sodass Sie herausfinden können, warum ein bestimmter KMS-Schlüssel verwendet wurde. Amazon EBS verwendet Folgendes für den Verschlüsselungskontext:

- Die Sicherheits-ID (SID) des/der Active-Directory-Benutzer:in, der/die dem WorkSpace zugeordnet ist.
- Die Verzeichnis-ID des AWS Directory Service-Verzeichnisses, das dem WorkSpace zugeordnet ist.
- Die Amazon-EBS-Volume-ID des verschlüsselten Volumes.

Das folgende Beispiel zeigt eine JSON-Darstellung des von Amazon EBS verwendeten Verschlüsselungskontextes:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

Erteilen der Berechtigung, einen KMS-Schlüssel in Ihrem Namen zu verwenden für WorkSpaces

Sie können Ihre WorkSpace-Daten mit dem von AWS verwalteten KMS-Schlüssel für (aws/workspaces) oder einem kundenverwalteten KMS-Schlüssel schützen. Wenn Sie einen kundenverwalteten KMS-Schlüssel verwenden, müssen Sie WorkSpaces die Berechtigung zur Verwendung des KMS-Schlüssels im Namen der WorkSpaces-Administratoren in Ihrem Konto

erteilen. Der von AWS verwaltete KMS-Schlüssel für WorkSpaces verfügt standardmäßig über die erforderlichen Berechtigungen.

Gehen Sie wie folgt vor, um Ihren kundenverwalteten KMS-Schlüssel für die Verwendung mit WorkSpaces vorzubereiten.

1. Fügen Sie die WorkSpaces-Administratoren zu der Liste der Schlüsselbenutzer in der Schlüsselrichtlinie des KMS-Schlüssels hinzu
2. Erteilen Sie den WorkSpaces-Administratoren mit einer IAM-Richtlinie zusätzliche Berechtigungen

WorkSpaces-Administratoren benötigen ebenfalls die Berechtigung, WorkSpaces zu verwenden. Weitere Informationen zu diesen Berechtigungen finden Sie unter Identitäts- und Zugriffsverwaltung für WorkSpaces.

Teil 1: Hinzufügen von WorkSpaces-Administratoren zu den Benutzern eines CMK

Sie können den WorkSpaces-Administratoren die erforderlichen Berechtigungen über die AWS Management Console oder die AWS KMS-API erteilen.

Hinzufügen von WorkSpaces-Administratoren als Schlüsselbenutzer für einen KMS-Schlüssel (Konsole)

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Key Management Service (AWS KMS)-Konsole unter https://console.aws.amazon.com/kms.
2. Wenn Sie die AWS-Region ändern möchten, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.
4. Wählen Sie die Schlüssel-ID oder den Alias Ihres bevorzugten kundenverwalteten KMS-Schlüssels aus.
5. Wählen Sie die Registerkarte Key policy (Schlüsselrichtlinie). Unter Key users (Schlüsselbenutzer), wählen Sie Add (Hinzufügen) aus.
6. Wählen Sie in der Liste der IAM-Benutzer und -Rollen die Benutzer und Rollen aus, die Ihren WorkSpaces-Administratoren entsprechen, und wählen Sie dann Anfügen.

Hinzufügen von WorkSpaces-Administratoren als Schlüsselbenutzer für einen KMS-Schlüssel (API)

1. Rufen Sie mithilfe der Operation GetKeyPolicy die bestehende Schlüsselrichtlinie ab und speichern Sie das Richtliniendokument anschließend in einer Datei.
2. Öffnen Sie die Richtlinien in Ihrem bevorzugten Texteditor. Fügen Sie die IAM-Benutzer und -Rollen für Ihre WorkSpaces-Administratoren zu den Richtlinienanweisungen hinzu, die Schlüsselbenutzern Berechtigungen erteilen. Speichern Sie dann die Datei.
3. Verwenden Sie PutKeyPolicy-Operation, um die Schlüsselrichtlinie auf den KMS-Schlüssel anzuwenden.

Teil 2: Erteilen von zusätzlichen Berechtigung für WorkSpaces-Administratoren mit einer IAM-Richtlinie

Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung auswählen, müssen Sie IAM-Richtlinien festlegen, die es Amazon WorkSpaces ermöglichen, den KMS-Schlüssel im Namen eines IAM-Benutzers in Ihrem Konto zu verwenden, der verschlüsselte WorkSpaces startet. Dieser Benutzer benötigt auch die Berechtigung zur Verwendung von Amazon WorkSpaces. Weitere Informationen zum Erstellen von IAM-Benutzerrichtlinien finden Sie unter Verwalten von IAM-Richtlinien im IAM-Benutzerhandbuch und unter Identitäts- und Zugriffsverwaltung für WorkSpaces.

Die WorkSpaces-Verschlüsselung erfordert eingeschränkten Zugriff auf den KMS-Schlüssel. Nachfolgend finden Sie eine Schlüsselmusterrichtlinie, die Sie verwenden können. Diese Richtlinie trennt die Prinzipale, die den AWS KMS-Schlüssel verwalten können, von denjenigen, die ihn verwenden können. Bevor Sie diese Beispiel-Schlüsselrichtlinie verwenden, ersetzen Sie die Beispiel-Konto-ID und den IAM-Benutzernamen durch tatsächliche Werte aus Ihrem Konto.

Die erste Anweisung entspricht der standardmäßigen AWS KMS-Schlüsselrichtlinie. Sie erteilt Ihrem Konto die Berechtigung, IAM-Richtlinien zu verwenden, um den Zugriff auf den KMS-Schlüssel zu steuern. Die zweite und dritte Anweisung definieren, welche AWS-Prinzipale den Schlüssel verwalten beziehungsweise verwenden können. Die vierte Anweisung ermöglicht es AWS-Services, die in AWS KMS integriert sind, den Schlüssel für den angegebenen Prinzipal zu verwenden. Diese Anweisung ermöglicht es AWS-Services, Zuwendungen zu erstellen und zu verwalten. Die Anweisung verwendet ein Bedingungselement, das die Berechtigungserteilungen für den KMS-Schlüssel auf diejenigen beschränkt, die von AWS-Services im Auftrag von Benutzern in Ihrem Konto vorgenommen werden.

> **Note**
>
> Wenn die WorkSpaces-Administratoren die AWS Management Console verwenden, um WorkSpaces mit verschlüsselten Volumes zu erstellen, die Berechtigung, Aliasnamen und Schlüssel auflisten (die Berechtigungen `"kms:ListAliases"` und `"kms:ListKeys"`). Wenn Ihre WorkSpaces-Administratoren nur die Amazon-WorkSpaces-API (nicht die Konsole) verwenden, können Sie die Berechtigungen `"kms:ListAliases"` und `"kms:ListKeys"` weglassen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
```

```
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

Die IAM-Richtlinie für Benutzer oder Rollen zum Verschlüsseln eines WorkSpace muss Nutzungsberechtigungen für die von Benutzern verwalteten KMS-Schlüssel sowie Zugriff auf WorkSpaces umfassen. Sie können den IAM-Benutzern oder der IAM-Rolle die folgende Beispielrichtlinie zuweisen, um Benutzern oder einer Rolle WorkSpaces-Berechtigungen zu erteilen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Die folgende IAM-Richtlinie wird von Benutzern für die Verwendung von AWS KMS benötigt. Sie gibt den Benutzern schreibgeschützten Zugriff auf den KMS-Schlüssel zusammen mit der Möglichkeit, Berechtigungserteilungen zu erstellen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Wenn Sie den KMS-Schlüssel in Ihrer Richtlinie angeben möchten, verwenden Sie eine IAM-Richtlinie, die der folgenden ähnelt. Ersetzen Sie den ARN des Beispiel-KMS-Schlüssels durch einen gültigen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

Verschlüsseln eines WorkSpace

So verschlüsseln Sie einen WorkSpace

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie Launch WorkSpaces aus und führen Sie die ersten drei Schritte aus.
3. Gehen Sie für WorkSpaces Configuration wie folgt vor:
   a. Wählen Sie die zu verschlüsselnden Volumes aus: Root Volume, User Volume oder beide Volumes.
   b. Wählen Sie für Verschlüsselungsschlüssel einen AWS KMS-Schlüssel aus (entweder den von Amazon WorkSpaces erstellten, von AWS verwalteten KMS-Schlüssel oder einen von Ihnen erstellten KMS-Schlüssel). Der KMS-Schlüssel, den Sie auswählen, muss symmetrisch sein. Amazon WorkSpaces unterstützt keine asymmetrischen KMS-Schlüssel.
   c. Wählen Sie Next Step (Weiter) aus.
4. Wählen Sie Launch WorkSpaces aus.

Anzeigen verschlüsselter WorkSpaces

Wählen Sie in der Navigationsleiste auf der linken Seite WorkSpaces aus, um zu prüfen, welche WorkSpaces und Volumes von der WorkSpaces-Konsole verschlüsselt wurden. In der Spalte Volume Encryption sehen Sie, ob die Verschlüsselung für die einzelnen WorkSpaces aktiviert oder deaktiviert ist. Erweitern Sie den WorkSpace-Eintrag, sodass das Feld Encrypted Volumes angezeigt wird und Sie sehen können, welche Volumes verschlüsselt wurden.

Neustart einer WorkSpace

Gelegentlich müssen Sie einen WorkSpace manuell neu starten (neu starten). Durch den Neustart eines wird die Verbindung des Benutzers WorkSpace getrennt und anschließend wird das heruntergefahren und neu gestartet WorkSpace. Um Datenverlust zu vermeiden, stellen Sie sicher, dass der Benutzer alle geöffneten Dokumente und andere Anwendungsdateien speichert, bevor Sie

den neu starten WorkSpace. Benutzerdaten, Betriebssystem und Systemeinstellungen sind davon nicht betroffen.

> **Warning**
>
> Um eine verschlüsselte neu zu starten WorkSpace, stellen Sie zunächst sicher, dass der AWS KMS Schlüssel aktiviert ist. Andernfalls WorkSpace wird die unbrauchbar. Informationen darüber, ob ein KMS-Schlüssel aktiviert ist, finden Sie unter Anzeigen von KMS-Schlüsseldetails im AWS Key Management Service-Entwicklerhandbuch.

So starten Sie einen neu WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie die aus, die neu gestartet werden WorkSpaces soll, und wählen Sie Aktionen , Neustart WorkSpaces.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Neustart aus WorkSpaces.

So starten Sie eine WorkSpace mithilfe der neu AWS CLI

Verwenden Sie den Befehl reboot-workspaces.

So führen Sie einen Massen-Neustart durch WorkSpaces

Verwenden Sie die amazon-workspaces-admin-module.

Neuerstellen eines WorkSpace

Bei der Neuerstellung eines WorkSpace werden das Stammvolume, das Benutzervolume und die primäre Elastic-Network-Schnittstelle des neuesten Abbilds des Pakets, von dem aus der WorkSpace gestartet wurde, neu erstellt. Beim Neuerstellen eines WorkSpace werden mehr Daten gelöscht als beim Wiederherstellen eines WorkSpace. Sie benötigen jedoch nur einen Snapshot des Benutzervolumes. Weitere Informationen zum Wiederherstellen eines WorkSpace finden Sie unter Wiederherstellen eines WorkSpace.

Beim Neuerstellen eines WorkSpace geschieht Folgendes:

- Das Stammvolume (für Microsoft Windows Laufwerk C; für Linux,/) wird mit dem neuesten Abbild des Pakets aktualisiert, aus dem der WorkSpace erstellt wurde. Alle installierten Anwendungen oder Systemeinstellungen, die nach der Erstellung des WorkSpace geändert wurden, gehen verloren.
- Das Benutzer-Volume (für Microsoft Windows: Laufwerk D; für Linux: /home) wird aus dem letzten Snapshot neu erstellt. Die aktuellen Inhalte des Benutzer-Volumes werden überschrieben.

  Automatische Snapshots, die beim Neuerstellen eines WorkSpace verwendet werden, werden alle 12 Stunden geplant. Diese Snapshots des Benutzervolumes werden unabhängig vom Status des WorkSpace erstellt. Wenn Sie Aktionen, WorkSpace neu erstellen/wiederherstellen auswählen, werden Datum und Uhrzeit des letzten Snapshots angezeigt.
- Die primäre Elastic Network-Schnittstelle wird neu erstellt. Der WorkSpace erhält eine neue private IP-Adresse.

> **Important**
>
> Nach dem 14. Januar 2020 können WorkSpaces, die aus einem öffentlichen Windows 7-Paket erstellt wurden, nicht mehr neu erstellt werden. Sie sollten Ihre Windows 7-WorkSpaces zu Windows 10 migrieren. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.

Sie können einen WorkSpace nur dann neu erstellen, wenn die folgenden Bedingungen erfüllt sind:

- Der WorkSpace muss den Status`AVAILABLE`, `ERROR`, `UNHEALTHY`, `STOPPED` oder `REBOOTING` haben. Sie müssen den API-Vorgang RebuildWorkspaces oder den AWS CLI-Befehl rebuild-workspaces verwenden, um einen WorkSpace im `REBOOTING`-Status neu zu erstellen.
- Ein Snapshot des Benutzervolumes muss vorhanden sein.

So erstellen Sie einen WorkSpace neu

> **Warning**
>
> Stellen Sie zunächst sicher, dass der AWS KMS-Schlüssel aktiviert ist, um einen verschlüsselten WorkSpace neu zu erstellen. Andernfalls kann der WorkSpace nicht mehr

benutzt werden. Informationen darüber, ob ein KMS-Schlüssel aktiviert ist, finden Sie unter Anzeigen von KMS-Schlüsseldetails im AWS Key Management Service-Entwicklerhandbuch.

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie den WorkSpace aus, der neu erstellt werden soll. Wählen Sie dann Aktionen und dann WorkSpaces neu erstellen/wiederherstellen aus.
4. Wählen Sie unter Snapshot den Zeitstempel des Snapshots aus.
5. Wählen Sie Rebuild (Neu erstellen).

So erstellen Sie einen WorkSpace über die AWS CLI neu

Verwenden Sie den Befehl rebuild-workspaces.

Fehlerbehebung

Wenn Sie einen WorkSpace neu erstellen, nachdem Sie das Benutzernamenattribut sAMAccountName des Benutzers in Active Directory geändert haben, wird möglicherweise die folgende Fehlermeldung angezeigt:

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

Kehren Sie entweder zum ursprünglichen Benutzernamenattribut zurück und initiieren Sie dann die Neuerstellung oder erstellen Sie einen neuen WorkSpace für diesen Benutzer, um dieses Problem zu umgehen.

Wiederherstellen eines WorkSpace

Wiederherstellen eines WorkSpace erstellt sowohl das Stammvolume als auch das Benutzervolume basierend auf den neuesten Snapshots dieser Volumes neu, die generiert wurden, als der WorkSpace fehlerfrei war. Beim Wiederherstellen eines WorkSpace werden weniger Daten gelöscht als beim Neuerstellen eines WorkSpace. Sie benötigen jedoch Snapshots sowohl des Stammvolumes als auch des Benutzervolumes, während für die Neuerstellung eines WorkSpace nur ein Snapshot des Benutzervolumes erforderlich ist. Informationen zum Neuerstellen eines WorkSpace finden Sie unter Neuerstellen eines WorkSpace.

Beim Wiederherstellen eines WorkSpace geschieht Folgendes:

- Das Stammvolume (für Microsoft Windows, Laufwerk C; für Linux,/) wird auf den neuesten Snapshot zurückgesetzt. Alle installierten Anwendungen oder Systemeinstellungen, die nach der Erstellung des letzten Snapshots geändert wurden, gehen verloren.
- Das Benutzer-Volume (für Microsoft Windows: Laufwerk D; für Linux: /home) wird aus dem letzten Snapshot neu erstellt. Die aktuellen Inhalte des Benutzer-Volumes werden überschrieben.

Wenn Snapshots erstellt werden

Snapshots des Stamm- und Benutzervolumes werden auf der folgenden Grundlage erstellt. Wenn Sie Aktionen, WorkSpace neu erstellen/wiederherstellen auswählen, werden Datum und Uhrzeit des letzten Snapshots angezeigt.

- Nachdem ein WorkSpace zum ersten Mal erstellt wurde – In der Regel werden die ersten Snapshots der Stamm- und Benutzervolumes kurz nach der Erstellung eines WorkSpace erstellt (oft innerhalb von 30 Minuten). In einigen AWS-Regionen kann es mehrere Stunden dauern, bis die ersten Snapshots nach der Erstellung eines WorkSpace erstellt werden.

  Wenn ein WorkSpace vor der Erstellung der ersten Snapshots fehlerhaft wird, kann der WorkSpace nicht wiederhergestellt werden. In diesem Fall können Sie versuchen, den WorkSpace neu zu erstellen, oder sich an den AWS-Support wenden, um Unterstützung zu erhalten.
- Während der normalen Nutzung – Automatische Snapshots, die beim Wiederherstellen eines WorkSpace verwendet werden, werden alle 12 Stunden geplant. Wenn der WorkSpace fehlerfrei ist, werden etwa zur gleichen Zeit Snapshots des Stamm-Volumes und des Benutzer-Volumes erstellt. Wenn der WorkSpace fehlerhaft ist, werden Snapshots nur für das Benutzervolume erstellt.
- Nachdem ein WorkSpace wiederhergestellt wurde – Wenn Sie einen WorkSpace wiederherstellen, werden kurz nach Abschluss der Wiederherstellung (oft innerhalb von 30 Minuten) neue Snapshots erstellt. In einigen AWS-Regionen kann es mehrere Stunden dauern, bis diese Snapshots nach der Wiederherstellung eines WorkSpace erstellt werden.

  Wenn ein WorkSpace wiederhergestellt wurde und der WorkSpace nicht mehr richtig funktioniert, bevor neue Snapshots erstellt werden können, kann der WorkSpace nicht erneut wiederhergestellt werden. In diesem Fall können Sie versuchen, den WorkSpace neu zu erstellen, oder sich an den AWS-Support wenden, um Unterstützung zu erhalten.

Sie können einen WorkSpace nur dann wiederherstellen, wenn die folgenden Bedingungen erfüllt sind:

- Der WorkSpace muss den Status `AVAILABLE`, `ERROR`, `UNHEALTHY` oder `STOPPED` haben.
- Es müssen Snapshots der Stamm- und Benutzervolumes vorhanden sein.

So stellen Sie einen WorkSpace wieder her

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie den WorkSpace aus, der wiederhergestellt werden soll. Wählen Sie dann Aktionen und dann WorkSpaces neu erstellen/wiederherstellen aus.
4. Wählen Sie unter Snapshot den Zeitstempel des Snapshots aus.
5. Wählen Sie Restore (Wiederherstellen) aus.

So stellen Sie einen WorkSpace über die AWS CLI wieder her

Verwenden Sie den Befehl restore-workspace.

Microsoft 365 Bring-Your-Own-License (BYOL)

Amazon WorkSpaces ermöglicht es Ihnen, Ihre eigenen Microsoft 365-Lizenzen mitzubringen, wenn sie die Lizenzanforderungen von Microsoft erfüllen. Mit diesen Lizenzen können Sie Microsoft 365 Apps for Enterprise Software auf installieren und aktivieren WorkSpaces , die von den folgenden Betriebssystemen unterstützt werden:

- Windows 10 (Bring-Your-Own-License)
- Windows 11 (Bring-Your-Own-License)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Um Microsoft 365 Apps for Enterprise auf verwenden zu können WorkSpaces, müssen Sie ein Abonnement für Microsoft 365 E3/E5, Microsoft 365 A3/A5 oder Microsoft 365 Business Premium haben.

Auf Ihrem Amazon können WorkSpaces Sie Ihre Microsoft 365-Lizenzen verwenden, um Microsoft 365 Apps for Enterprise zu installieren und zu aktivieren, einschließlich der folgenden:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

Weitere Informationen finden Sie in der vollständigen Liste zu Microsoft 365 Apps for Enterprise.

Sie können auch Microsoft-Anwendungen installieren, die nicht in Microsoft 365 enthalten sind, z. B. Microsoft Project, Microsoft Visio und Microsoft Power Automate auf , WorkSpaces aber Sie müssen Ihre eigenen zusätzlichen Lizenzen mitbringen.

Sie können Microsoft 365 und andere Microsoft-Anwendungen auf primären und Failover-Anwendungen installieren WorkSpaces und verwenden, WorkSpaces indem Sie Multi-Region Resilience verwenden.

Inhalt

Erstellen WorkSpaces mit Microsoft 365 Apps for Enterprise

Um WorkSpaces mit Microsoft 365 Apps for Enterprise zu erstellen, müssen Sie ein benutzerdefiniertes Image mit den installierten Anwendungen erstellen und es zum Erstellen eines benutzerdefinierten Pakets verwenden. Sie können das Paket verwenden, um neue zu starten WorkSpaces , auf denen die Anwendungen installiert sind. WorkSpaces stellt keine öffentlichen Pakete mit Microsoft 365 Apps for Enterprise bereit.

So erstellen Sie WorkSpaces mit Microsoft 365 Apps for Enterprise:

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Starten Sie eine WorkSpace , die Sie als Image für andere Microsoft-Anwendungen verwenden möchten WorkSpaces. Dort installieren Sie Ihre Microsoft-Anwendungen. Weitere Informationen

zum Starten eines WorkSpacefinden Sie unter Starten eines virtuellen Desktops mit WorkSpaces.

3. Starten Sie die Client-Anwendung unter https://clients.amazonworkspaces.com/, geben Sie den Registrierungscode aus Ihrer Einladungs-E-Mail ein und wählen Sie Registrieren aus.
4. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie die Anmeldeinformationen des/der Benutzer:in ein und wählen Sie dann Anmelden aus.
5. Installieren und konfigurieren Sie Microsoft 365 Apps for Enterprise.
6. Erstellen Sie ein benutzerdefiniertes Image aus und WorkSpaceverwenden Sie es, um ein benutzerdefiniertes Paket zu erstellen. Weitere Informationen zum Erstellen von benutzerdefinierten Images und Paketen finden Sie unter Erstellen eines benutzerdefinierten WorkSpaces Images und Pakets.
7. Starten Sie WorkSpaces mit dem benutzerdefinierten Paket, das Sie erstellt haben. Auf diesen WorkSpaces ist Microsoft 365 Apps for Enterprise installiert.

Migrieren Sie Ihr vorhandenes WorkSpaces zur Verwendung von Microsoft 365 Apps for Enterprise

Wenn Ihr WorkSpaces über keine Microsoft Office-Lizenz verfügtAWS, können Sie Microsoft 365 Apps for Enterprise auf Ihrem installieren und konfigurieren WorkSpaces.

Wenn Ihr WorkSpaces über eine Microsoft- Office-Lizenz verfügtAWS, müssen Sie zuerst Ihre Microsoft- Office-Lizenz abmelden, bevor Sie Microsoft 365 Apps for Enterprise installieren.

Important

Durch die Deinstallation von Microsoft Office-Anwendungen von Ihrem WorkSpaces werden die Lizenzen nicht abgemeldet. Um zu vermeiden, dass Ihnen Microsoft Office-Lizenzen in Rechnung gestellt werden, heben Sie die Registrierung Ihres WorkSpaces von Microsoft Office-Anwendungen über auf, AWS indem Sie einen der folgenden Schritte ausführen:

- Anwendungen verwalten (empfohlen) – Sie können Microsoft Office 2016 und 2019 von Ihrem deinstallieren WorkSpaces. Weitere Informationen finden Sie unter Anwendungen verwalten. Nach der Deinstallation können Sie Microsoft 365 Apps for Enterprise auf Ihrem installieren WorkSpaces.
- Migrieren eines WorkSpace – Sie können einen WorkSpace von einem Paket zu einem anderen migrieren, während die Daten auf dem Benutzer-Volume beibehalten werden.

- Migrieren Sie Ihr WorkSpaces zu einem Paket mit einem Image, das kein Microsoft Office-Abonnement hat. Nach Abschluss der Migration können Sie Microsoft 365 Apps for Enterprise auf Ihrem installieren WorkSpaces.
- Oder erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket, auf dem bereits Microsoft 365 Apps for Enterprise installiert ist, und migrieren Sie dann Ihr WorkSpaces zu diesem neuen benutzerdefinierten Paket. Nach Abschluss der Migration können Ihre WorkSpaces Benutzer Microsoft 365 Apps for Enterprise verwenden.
- Weitere Informationen zur Migration von WorkSpacesfinden Sie unter Migrieren eines WorkSpace.

Aktualisieren Sie Ihre Microsoft 365 Apps for Enterprise auf WorkSpaces

Standardmäßig sind Ihre , die auf dem Microsoft Windows-Betriebssystem WorkSpaces ausgeführt werden, so konfiguriert, dass sie Updates von Windows Update erhalten. Updates für Microsoft 365 Apps for Enterprise sind jedoch nicht mit Windows Update verfügbar. Richten Sie Updates so ein, dass sie automatisch über das Office-CDN ausgeführt werden, oder verwenden Sie Windows Server Update Services (WSUS) in Verbindung mit Microsoft Configuration Manager, um Microsoft 365 Apps for Enterprise zu aktualisieren. Weitere Informationen finden Sie unter Verwalten von Updates für Microsoft 365 Apps mit Microsoft Configuration Manager. Um die Häufigkeit von Microsoft 365-Anwendungsaktualisierungen festzulegen, geben Sie einen Aktualisierungskanal an und setzen Sie ihn auf Aktuelles oder monatliches Unternehmen, um die Microsoft 365 WorkSpaces-Lizenzierungsrichtlinie zu erfüllen.

Windows BYOL aktualisieren WorkSpaces

Auf Ihrer Windows Bring Your Own License (BYOL) WorkSpaces können Sie mithilfe des direkten Upgrade-Prozesses auf eine neuere Version von Windows aktualisieren. Folgen Sie dazu den Anweisungen in diesem Thema.

Das direkte Upgrade gilt nur für Windows 10 und 11 BYOL. WorkSpaces

Important

Führen Sie Sysprep nicht auf einem aktualisierten Gerät aus. WorkSpace Andernfalls kann ein Fehler auftreten, der verhindert, dass Sysprep abgeschlossen wird. Wenn Sie Sysprep

ausführen möchten, tun Sie dies nur auf einem Computer, der noch nicht WorkSpace aktualisiert wurde.

> **Note**
>
> Sie können diesen Vorgang verwenden, um Windows 10 und 11 auf eine neuere Version WorkSpaces zu aktualisieren. Dieser Vorgang kann jedoch nicht verwendet werden, um Windows 10 auf Windows 11 WorkSpaces zu aktualisieren.

Inhalt

Voraussetzungen

- Wenn Sie Windows 10- und 11-Upgrades mithilfe von Gruppenrichtlinien oder System Center Configuration Manager (SCCM) verzögert oder angehalten haben, aktivieren Sie Betriebssystemaktualisierungen für Windows 10 und 11. WorkSpaces
- Falls es sich um ein WorkSpace handelt AutoStop WorkSpace, ändern Sie es AlwaysOn WorkSpace vor dem direkten Upgrade-Vorgang in ein, damit es nicht automatisch beendet wird, während Updates installiert werden. Weitere Informationen finden Sie unter Ändern des Funktionsmodus. Wenn Sie es vorziehen, die WorkSpace Einstellung beizubehalten AutoStop, ändern Sie die AutoStop Zeit auf drei Stunden oder mehr, während das Upgrade stattfindet.
- Das direkte Upgrade erstellt das Benutzerprofil neu, indem eine Kopie eines speziellen Profils mit dem Namen „Standard-Benutzer“ (`C:\Users\Default`) erstellt wird. Verwenden Sie dieses Standardbenutzerprofil nicht, um Anpassungen vorzunehmen. Wir empfehlen stattdessen Anpassungen am Benutzerprofil über Gruppenrichtlinienobjekte (Group Policy Objects, GPOs).

Anpassungen, die über Gruppenrichtlinienobjekte vorgenommen werden, können leicht geändert oder zurückgesetzt werden und sind weniger fehleranfällig.

- Beim In-Place-Upgradeprozess kann nur ein Benutzerprofil gesichert und neu erstellt werden. Wenn Sie mehrere Benutzerprofile auf Laufwerk D haben, löschen Sie alle Profile mit Ausnahme des Profils, das Sie benötigen.

Überlegungen

Beim direkten Upgrade werden zwei Registrierungsskripts (`enable-inplace-upgrade.ps1`und`update-pvdrivers.ps1`) verwendet, um die erforderlichen Änderungen an Ihrem vorzunehmen WorkSpaces , damit der Windows Update-Prozess ausgeführt werden kann. Diese Änderungen beinhalten das Erstellen eines (temporären) Benutzerprofils auf Laufwerk „C“ anstelle von Laufwerk „D“. Wenn auf Laufwerk „D“ bereits ein Benutzerprofil vorhanden ist, verbleiben die Daten in diesem ursprünglichen Benutzerprofil auf Laufwerk „D“.

Standardmäßig WorkSpaces erstellt das Benutzerprofil in`D:\Users\%USERNAME%`. Das Skript `enable-inplace-upgrade.ps1` konfiguriert Windows so, dass ein neues Benutzerprofil in `C:\Users\%USERNAME%` erstellt wird, und leitet die Benutzer-Shell-Ordner zu `D:\Users\%USERNAME%` um. Dieses neue Benutzerprofil wird erstellt, wenn sich ein Benutzer zum ersten Mal anmeldet.

Nach dem direkten Upgrade haben Sie die Möglichkeit, Ihre Benutzerprofile auf Laufwerk „C“ zu belassen, damit Ihre Benutzer ihre Computer zukünftig anhand des Windows Update-Prozesses aktualisieren können. Beachten Sie jedoch, dass WorkSpaces Profile, die auf Laufwerk C gespeichert sind, nicht neu erstellt oder migriert werden können, ohne dass alle Daten im Benutzerprofil verloren gehen, es sei denn, Sie sichern und stellen diese Daten selbst wieder her. Wenn Sie sich dafür entscheiden, die Profile auf Laufwerk C zu belassen, können Sie den UserShellFoldersRedirectionRegistrierungsschlüssel verwenden, um die Benutzer-Shell-Ordner auf Laufwerk D umzuleiten, wie später in diesem Thema erklärt wird.

Um sicherzustellen, dass Sie Ihre Dateien neu erstellen oder migrieren können WorkSpaces und um mögliche Probleme mit der Umleitung von User-Shell-Ordnern zu vermeiden, empfehlen wir Ihnen, Ihre Benutzerprofile nach dem direkten Upgrade auf Laufwerk D wiederherzustellen. Dazu können Sie den Registrierungsschlüssel PostUpgradeRestoreProfileOnD verwenden, wie später in diesem Thema erklärt wird.

Bekannte Beschränkungen

- Die Änderung des Speicherorts des Benutzerprofils von Laufwerk D auf Laufwerk C findet bei WorkSpace Neuerstellungen oder Migrationen nicht statt. Wenn Sie ein direktes Upgrade auf einem Windows 10- oder 11-BYOL durchführen WorkSpace und es dann neu erstellen oder migrieren, WorkSpace wird das Benutzerprofil auf dem neuen Laufwerk D gespeichert.

  > **Warning**
  >
  > Wenn Sie das Benutzerprofil nach dem direkten Upgrade auf Laufwerk „C“ belassen, gehen die auf Laufwerk „C“ gespeicherten Benutzerprofildaten bei einer Neuerstellung oder bei Migrationen verloren, es sei denn, Sie sichern die Benutzerprofildaten vor dem Neuerstellen oder Migrieren manuell und stellen die sie nach dem Neuerstellungs- oder Migrationsprozess manuell wieder her.

- Wenn Ihr Standard-BYOL-Paket ein Image enthält, das auf einer früheren Version von Windows 10 und 11 basiert, müssen Sie das direkte Upgrade erneut durchführen, nachdem WorkSpace es neu erstellt oder migriert wurde.

Zusammenfassung der Registrierungsschlüsseleinstellungen

Sie müssen eine Reihe von Registrierungsschlüsseln festlegen, um den direkten Upgrade-Prozess zu aktivieren und anzugeben, welches Benutzerprofil nach dem Upgrade vorhanden sein soll.

Registrierungspfad: HKL M:\Software\Amazon\WorkSpacesConfig\ .ps1 enable-inplace-upgrade

Registrierungsschlüssel	Typ	Werte
Aktiviert	DWORD	0 – (Standard) Deaktiviert In-Place-Upgrade 1 – Ermöglicht ein In-Place-Upgrade
PostUpgradeRestoreProfileOnD	DWORD	0 – (Standard) Versucht nicht, den Benutzerprofilpfad nach dem In-Place-Upgrade wiederherzustellen

Registrierungsschlüssel	Typ	Werte
		1 — Stellt den Benutzerprofilpfad (ProfileImagePath) nach dem direkten Upgrade wieder her
UserShellFoldersRedirection	DWORD	0 – Aktiviert nicht die Umleitung von Benutzer-Shell-Ordnern 1 – (Standard) Aktiviert die Umleitung von Benutzer-Shell-Ordnern zu `D:\Users\%USERNAME%` , nachdem das Benutzerprofil auf `C:\Users\%USERNAME%` neu generiert wurde.
NoReboot	DWORD	0 – (Standard) Ermöglicht Ihnen zu steuern, wann ein Neustart erfolgt, nachdem die Registrierung für das Benutzerprofil geändert wurde 1 — Lässt nicht zu, dass das Skript neu gestartet wird, WorkSpace nachdem die Registrierung für das Benutzerprofil geändert wurde

Registrierungspfad: HKL M:\Software\Amazon\WorkSpacesConfig\ update-pvdrivers.ps1

Registrierungsschlüssel	Typ	Werte
Aktiviert	DWORD	0 — (Standard) Deaktiviert das PV-Treiber-Update AWS

Registrierungsschlüssel	Typ	Werte
		1 — Aktiviert die Aktualisierung von AWS PV-Treibern

Durchführen eines direkten Upgrades

Um direkte Windows-Upgrades auf Ihrem BYOL zu aktivieren WorkSpaces, müssen Sie bestimmte Registrierungsschlüssel festlegen, wie im folgenden Verfahren beschrieben. Sie müssen auch bestimmte Registrierungsschlüssel festlegen, um das Laufwerk (C oder D) anzugeben, auf dem sich die Benutzerprofile befinden sollen, nachdem die direkten Upgrades abgeschlossen wurden.

Sie können diese Registrierungsänderungen manuell vornehmen. Wenn Sie mehrere WorkSpaces zu aktualisieren haben, können Sie Gruppenrichtlinien oder SCCM verwenden, um ein Skript zu pushen. PowerShell Ein PowerShell Beispielskript finden Sie unterAktualisieren Sie Ihre WorkSpace Registrierung mithilfe eines Skripts PowerShell .

So führen Sie ein direktes Upgrade von Windows 10 und 11 durch

1. Notieren Sie sich, welche Version von Windows derzeit auf den Windows 10 und 11 BYOL ausgeführt wird WorkSpaces , die Sie aktualisieren, und starten Sie sie dann neu.
2. Aktualisieren Sie die folgenden Systemregistrierungsschlüssel von Windows, um den Wert für Aktiviert von 0 bis 1 zu ändern. Diese Registrierungsänderungen ermöglichen direkte Upgrades für. WorkSpace

   - HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade
   - HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ update-pvdrivers.ps1 WorkSpacesConfig

> **Note**
>
> Wenn diese Schlüssel nicht existieren, starten Sie den neu. WorkSpace Die Schlüssel sollten hinzugefügt werden, wenn das System neu gestartet wird.

(Optional) Wenn Sie einen verwalteten Workflow wie SCCM-Tasksequenzen verwenden, um das Upgrade durchzuführen, legen Sie den folgenden Schlüsselwert auf 1 fest, um zu verhindern, dass der Computer neu gestartet wird.

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. Entscheiden Sie, auf welchem Laufwerk sich Benutzerprofile nach dem In-Place-Upgrade befinden sollen (weitere Informationen finden Sie unter Überlegungen), und legen Sie die Registrierungsschlüssel wie folgt fest:

   - Einstellungen, wenn sich das Benutzerprofil nach dem Upgrade auf Laufwerk „C“ befinden soll:

     HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     Schlüsselname PostUpgradeRestoreProfileOn: D

     Schlüsselwert: 0

     Schlüsselname: UserShellFoldersRedirection

     Schlüsselwert: 1

   - Einstellungen, wenn sich das Benutzerprofil nach dem Upgrade auf Laufwerk „D“ befinden soll:

     HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     Schlüsselname PostUpgradeRestoreProfileOn: D

     Schlüsselwert: 1

     Schlüsselname: UserShellFoldersRedirection

     Schlüsselwert: 0

4. Nachdem Sie die Änderungen in der Registrierung gespeichert haben, starten Sie das System WorkSpace erneut, damit die Änderungen übernommen werden.

> **Note**
>
> - Nach dem Neustart wird durch die Anmeldung bei ein neues Benutzerprofil WorkSpace erstellt. Ihnen werden möglicherweise Platzhaltersymbole im Start-Menü angezeigt. Dieses Verhalten wird automatisch behoben, sobald das direkte Upgrade abgeschlossen ist.
> - Warten Sie 10 Minuten, um sicherzustellen, dass der entsperrt WorkSpace ist.

(Optional) Vergewissern Sie sich, dass der folgende Schlüsselwert auf 1 gesetzt ist, wodurch die Sperre WorkSpace für die Aktualisierung aufgehoben wird:

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ Gelöscht WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. Durchführen des direkten Upgrades. Sie können alle Methoden verwenden, die Sie möchten, wie z. B. SCCM, ISO oder Windows Update (WU). Abhängig von Ihrer ursprünglichen Windows 10- und 11-Version und der Anzahl der installierten Apps kann dieser Vorgang zwischen 40 und 120 Minuten dauern.

> **Note**
>
> Der In-Place-Upgrade-Vorgang kann mindestens eine Stunde dauern. Der WorkSpace Instanzstatus kann wie `UNHEALTHY` während des Upgrades angezeigt werden.

6. Nachdem der Aktualisierungsvorgang abgeschlossen ist, vergewissern Sie sich, dass die Windows-Version aktualisiert wurde.

> **Note**
>
> Wenn das direkte Upgrade fehlschlägt, führt Windows automatisch ein Rollback durch, um die Windows 10- und 11-Versionen zu verwenden, die vor dem Start des Upgrades installiert waren. Weitere Informationen zur Fehlerbehebung finden Sie in der Microsoft-Dokumentation.

(Optional) Zur Bestätigung, dass die Aktualisierungs-Skripts erfolgreich ausgeführt wurden, stellen Sie sicher, dass der folgende Schlüsselwert auf 1 festgelegt ist:

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. Wenn Sie den Betriebsmodus von geändert haben, indem Sie ihn auf AlwaysOn oder WorkSpace indem Sie den AutoStop Zeitraum so geändert haben, dass der direkte Upgrade-Vorgang ohne Unterbrechung ausgeführt werden kann, setzen Sie den Laufmodus wieder auf Ihre ursprünglichen Einstellungen zurück. Weitere Informationen finden Sie unter Ändern des Funktionsmodus.

Wenn Sie den PostUpgradeRestoreProfileOnD-Registrierungsschlüssel nicht auf 1 festgelegt haben, wird das Benutzerprofil von Windows neu generiert und `C:\Users\%USERNAME%` nach dem direkten Upgrade hinzugefügt, sodass Sie die oben genannten Schritte bei future direkten Upgrades von Windows 10 und 11 nicht erneut ausführen müssen. Standardmäßig leitet das Skript `enable-inplace-upgrade.ps1` die folgenden Shell-Ordner zu Laufwerk „D“ um:

- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates`

Wenn Sie die Shell-Ordner an andere Speicherorte auf Ihrem umleiten WorkSpaces, führen Sie WorkSpaces nach den direkten Upgrades die erforderlichen Operationen auf den Ordnern durch.

Fehlerbehebung

Wenn Probleme bei der Aktualisierung auftreten, überprüfen Sie die folgenden Elemente zur Fehlerbehebung:

- Windows-Protokolle, die sich standardmäßig an den folgenden Speicherorten befinden:

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`
- Windows-Ereignisanzeige

  Windows-Protokolle > Anwendung > Quelle: Amazon WorkSpaces

> **Tip**
>
> Wenn Sie während des direkten Upgrade-Vorgangs feststellen, dass einige Symbolverknüpfungen auf dem Desktop nicht mehr funktionieren, liegt das daran, dass alle Benutzerprofile von Laufwerk D auf Laufwerk C WorkSpaces verschoben werden, um das Upgrade vorzubereiten. Nachdem das Upgrade abgeschlossen wurde, funktionieren die Verknüpfungen wie erwartet.

Aktualisieren Sie Ihre WorkSpace Registrierung mithilfe eines Skripts PowerShell

Sie können das folgende PowerShell Beispielskript verwenden, um die Registrierung auf Ihrem WorkSpaces zu aktualisieren, um direkte Upgrades zu ermöglichen. Folgen Sie den AnweisungenDurchführen eines direkten Upgrades, aber verwenden Sie dieses Skript, um die Registrierung auf jedem WorkSpace Server zu aktualisieren.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
```

```
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

Migrieren eines WorkSpace

> **Note**
>
> Wenn Sie Microsoft Office-Versionslizenzen über Ihr abmelden oder AWS deinstallieren möchten WorkSpace, empfehlen wir die Verwendung von Anwendungen verwalten.

Sie können eine WorkSpace von einem Paket zu einem anderen migrieren und gleichzeitig die Daten auf dem Benutzer-Volume beibehalten. Hier sind Beispielszenarien:

- Sie können WorkSpaces von der Windows-7-Desktop-Umgebung zur Windows-10-Desktop-Umgebung migrieren.
- Sie können WorkSpaces vom PCoIP-Protokoll zum WorkSpaces Streaming Protocol (WSP) migrieren.
- Sie können WorkSpaces vom 32-Bit- WorkSpaces Paket von Microsoft Office unter Windows Server 2016 zu den 64-Bit- WorkSpaces Paketen von Microsoft Office unter Windows Server 2019 und Windows Server 2022 migrieren.
- Sie können WorkSpaces von einem öffentlichen oder benutzerdefinierten Paket zu einem anderen migrieren. Sie können beispielsweise von GPU-fähigen Paketen (Graphics.g4dn. GraphicsProg4dn, Graphics und GraphicsPro) zu nicht GPU-fähigen Paketen sowie in die andere Richtung migrieren.
- Sie können WorkSpaces von Windows 10 BYOL auf Windows 11 BYOL migrieren, aber die Migration von Windows 11 zu Windows 10 wird nicht unterstützt.
- Value-Pakete werden unter Windows 11 nicht unterstützt. Um Ihr Paket mit Windows 7 oder 10 Werten WorkSpaces zu Windows 11 zu migrieren, müssen Sie zuerst Ihren Wert WorkSpaces auf ein größeres Paketangebot umstellen.
- Bevor Sie WorkSpaces von Windows 7 zu Windows 11 migrieren, müssen Sie es zu Windows 10 migrieren. Melden Sie sich WorkSpace mindestens einmal bei Windows 10 an, bevor Sie es zu Windows 11 migrieren. Die direkte Migration von Windows 7 WorkSpaces zu Windows 11 wird nicht unterstützt.
- Sie können Windows WorkSpaces , die Microsoft Office verwendenAWS, zu einem benutzerdefinierten WorkSpaces Paket mit Microsoft 365-Anwendungen migrieren. Nach der Migration WorkSpaces werden Ihre von Microsoft Office abgemeldet.

- Sie können Windows WorkSpaces , die Microsoft Office verwendenAWS, zu einem WorkSpaces Paket ohne Office 2016/2019-Abonnement migrieren. Nach der Migration WorkSpaces werden Ihre von Microsoft Office abgemeldet.

Weitere Informationen zu Amazon- WorkSpaces Paketen finden Sie unter WorkSpace -Pakete und -Images.

Der Migrationsprozess erstellt das neu, WorkSpace indem ein neues Stamm-Volume aus dem Ziel-Bundle-Image und das Benutzer-Volume aus dem letzten verfügbaren Snapshot des ursprünglichen verwendet werden WorkSpace. Zur besseren Kompatibilität wird während der Migration ein neues Benutzerprofil generiert. Das alte Benutzerprofil wird umbenannt, und dann werden bestimmte Dateien im alten Benutzerprofil in das neue Benutzerprofil verschoben. (Details dazu, was verschoben wird, finden Sie unter Was passiert bei der Migration?.)

Der Migrationsprozess dauert bis zu einer Stunde pro WorkSpace. Wenn Sie den Migrationsprozess initiieren, WorkSpace wird ein neuer erstellt. Wenn ein Fehler auftritt, der eine erfolgreiche Migration verhindert, WorkSpace wird das Original wiederhergestellt und in seinen ursprünglichen Zustand zurückversetzt, und das neue WorkSpace wird beendet.

Inhalt

Migrationseinschränkungen

- Sie können nicht zu einem öffentlichen oder benutzerdefinierten Windows 7-Desktopumgebungsbundle migrieren. Sie können auch nicht zu Verwendung der eigenen Lizenz (Bring-Your-Own-License, BYOL) Windows 7-Bundles migrieren.
- Sie können BYOL WorkSpaces nur zu anderen BYOL-Paketen migrieren. Um ein BYOL WorkSpace von PCoIP zu WSP zu migrieren, müssen Sie zunächst ein BYOL-Paket mit dem

WSP-Protokoll erstellen. Anschließend können Sie Ihr PCoIP BYOL WorkSpaces zu diesem WSP BYOL-Paket migrieren.

- Sie können ein , das aus öffentlichen oder benutzerdefinierten Paketen WorkSpace erstellt wurde, nicht zu einem BYOL-Paket migrieren.
- Graphics.g4dn, GraphicsPro.g4dn, Graphics und GraphicsPro Bundles sind derzeit nur für das PCoIP-Protokoll verfügbar, sodass Graphics.g4dn, GraphicsPro.g4dn, Graphics und noch nicht zu WSP migriert werden GraphicsPro WorkSpaces können.
- Die Migration von Linux WorkSpaces wird derzeit nicht unterstützt.
- In AWS Regionen, die mehr als eine Sprache unterstützen, können Sie zwischen Sprachpaketen migrieren WorkSpaces.
- Die Quell- und Zielbundles müssen unterschiedlich sein. (In Regionen, die mehr als eine Sprache unterstützen, können Sie jedoch zu demselben Windows 10-Paket migrieren, solange die Sprachen unterschiedlich sind.) Wenn Sie Ihre WorkSpace mit demselben Paket aktualisieren möchten, erstellen Sie stattdessen die neu WorkSpace.
- Sie können nicht WorkSpaces zwischen Regionen migrieren.
- Wenn die Migration nicht erfolgreich abgeschlossen werden kann, wird in einigen Fällen möglicherweise keine Fehlermeldung angezeigt. Möglicherweise wurde der Migrationsprozess nicht gestartet. Wenn das WorkSpace Paket eine Stunde nach dem Versuch der Migration gleich bleibt, ist die Migration nicht erfolgreich. Wenden Sie sich an das AWS Support-Center, um Hilfe zu erhalten.

Migrationszenarien

Die folgende Tabelle zeigt, welche Migrationsszenarien verfügbar sind:

Quell-Betriebssystem	Zielbetriebssystem	Verfügbar?
Öffentliches oder benutzerdefiniertes Bundle Windows 7	Öffentliches oder benutzerdefiniertes Bundle Windows 10	Ja
Benutzerdefiniertes Bundle Windows 7	Öffentliches Bundle Windows 7	Nein
Benutzerdefiniertes Bundle Windows 7	Benutzerdefiniertes Bundle Windows 7	Nein

Quell-Betriebssystem	Zielbetriebssystem	Verfügbar?
Öffentliches Bundle Windows 7	Benutzerdefiniertes Bundle Windows 7	Nein
Öffentliches oder benutzerdefiniertes Bundle Windows 10	Öffentliches oder benutzerdefiniertes Bundle Windows 7	Nein
Öffentliches oder benutzerdefiniertes Bundle Windows 10	Benutzerdefiniertes Bundle Windows 10	Ja
Windows 7 BYOL-Bundle	Windows 7 BYOL-Bundle	Nein
Windows 7 BYOL-Bundle	BYOL-Bundle für Windows 10	Ja
BYOL-Bundle für Windows 10	Windows 7 BYOL-Bundle	Nein
BYOL-Bundle für Windows 10	BYOL-Bundle für Windows 10	Ja
Öffentliches Windows-10-Paket mit Windows Server 2016	Öffentliches Windows-10-Paket mit Windows Server 2019 	Ja
Öffentliches Windows-10-Paket mit Windows Server 2019 	Öffentliches Windows-10-Paket mit Windows Server 2016	Ja
BYOL-Bundle für Windows 10	BYOL-Bundle für Windows 11	Ja
BYOL-Bundle für Windows 11	BYOL-Bundle für Windows 10	Nein

Quell-Betriebssystem	Zielbetriebssystem	Verfügbar?
Benutzerdefiniertes Windows-10-Paket mit Windows Server 2016	Öffentliches Windows-10-Paket mit Windows Server 2019	Ja
Benutzerdefiniertes Windows-10-Paket mit Windows Server 2016	Öffentliches Windows-10-Paket mit Windows Server 2022	Ja
Benutzerdefiniertes Windows-10-Paket mit Windows Server 2019	Öffentliches Windows-10-Paket mit Windows Server 2022	Ja

Note

Web Access ist für den öffentlichen Windows-10-Paket-PCoIP-Branch mit Windows Server 2019 nicht verfügbar.

Important

Das öffentliche Windows-10-Plus-Paket mit Windows Server 2016 beinhaltet Microsoft Office 2016 und Trend Micro Worry-Free Business Security Services. Das öffentliche Windows-10-Plus-Paket mit Windows Server 2019 beinhaltet nur Microsoft Office 2019. Trend Micro Worry-Free Business Security Services ist nicht enthalten.

Was passiert bei der Migration?

Während der Migration bleiben die Daten auf dem Benutzervolume (Laufwerk D) erhalten, aber alle Daten auf dem Stammvolume (Laufwerk C) gehen verloren. Dies bedeutet, dass keine der installierten Anwendungen, Einstellungen und Änderungen an der Registrierung beibehalten werden. Der alte Benutzerprofilordner wird mit dem `.NotMigrated`-Suffix umbenannt, und ein neues Benutzerprofil wird erstellt.

Beim Migrationsprozess wird Laufwerk D basierend auf dem letzten Snapshot des ursprünglichen Benutzervolumes neu erstellt. Beim ersten Start des neuen verschiebt WorkSpaceder Migrationsprozess den ursprünglichen `D:\Users\%USERNAME%` Ordner in einen Ordner mit dem Namen `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Ein neuer `D:\Users\%USERNAME%\`-Ordner wird vom neuen Betriebssystem generiert.

Nachdem das neue Benutzerprofil erstellt wurde, werden die Dateien in den folgenden Benutzer-Shell-Ordnern aus dem alten `.NotMigrated`-Profil in das neue Profil verschoben:

- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`

Important

Der Migrationsprozess versucht, die Dateien aus dem alten Benutzerprofil in das neue Profil zu verschieben. Alle Dateien, die während der Migration nicht verschoben wurden, verbleiben im `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`-Ordner. Wenn die Migration erfolgreich ist, können Sie sehen, welche Dateien zu `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs` verschoben wurden. Sie können alle Dateien, die nicht automatisch verschoben wurden, manuell verschieben.
In den öffentlichen Paketen ist die lokale Suchindizierung standardmäßig deaktiviert. Wenn Sie diese aktivieren, wird standardmäßig in `C:\Users` und nicht in `D:\Users` gesucht. Sie müssen dies daher anpassen. Wenn Sie die lokale Suchindizierung speziell auf `D:\Users\`*`username`* und nicht `D:\Users` festgelegt haben, funktioniert die lokale Suchindizierung nach der Migration möglicherweise nicht für Benutzerdateien, die sich im Ordner `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` befinden.

Alle Tags, die dem Original zugewiesen sind, WorkSpace werden während der Migration übertragen, und der Ausführungsmodus des WorkSpace bleibt erhalten. Das neue WorkSpace erhält jedoch eine neue WorkSpace ID, einen neuen Computernamen und eine neue IP-Adresse.

Bewährte Methoden

Bevor Sie eine migrieren WorkSpace, gehen Sie wie folgt vor:

- Sichern Sie alle wichtigen Daten auf Laufwerk C an einem anderen Speicherort. Alle Daten auf Laufwerk C werden während der Migration gelöscht.
- Stellen Sie sicher, dass die WorkSpace migrierte mindestens 12 Stunden alt ist, um sicherzustellen, dass ein Snapshot des Benutzer-Volumes erstellt wurde. Auf der Seite Migrieren WorkSpaces in der Amazon- WorkSpaces Konsole können Sie den Zeitpunkt des letzten Snapshots sehen. Alle Daten, die nach dem letzten Snapshot erstellt wurden, gehen während der Migration verloren.
- Um potenziellen Datenverlust zu vermeiden, stellen Sie sicher, dass sich Ihre Benutzer von ihrem WorkSpaces abmelden und sich erst wieder anmelden, nachdem der Migrationsprozess abgeschlossen ist. Beachten Sie, dass nicht migriert werden WorkSpaces kann, wenn sie sich im -`ADMIN_MAINTENANCE`Modus befinden.
- Stellen Sie sicher, dass die , die WorkSpaces Sie migrieren möchten`AVAILABLE`, den Status `STOPPED`, oder haben`ERROR`.
- Stellen Sie sicher, dass Sie über genügend IP-Adressen für die verfügen, die WorkSpaces Sie migrieren. Während der Migration werden dem neue IP-Adressen zugewiesen WorkSpaces.
- Wenn Sie Skripts verwenden, um zu migrieren WorkSpaces, migrieren Sie sie in Batches von nicht mehr als 25 WorkSpaces gleichzeitig.

Fehlerbehebung

- Wenn Ihre Benutzer nach der Migration fehlende Dateien melden, überprüfen Sie, ob ihre Benutzerprofildateien während des Migrationsvorgangs nicht verschoben wurden. Sie können sehen, welche Dateien in `C:\Program Files\Amazon\WorkspacesConfig\Logs \MigrationLogs` verschoben wurden. Die Dateien, die nicht verschoben wurden, befinden sich im `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`-Ordner. Sie können alle Dateien, die nicht automatisch verschoben wurden, manuell verschieben.
- Wenn Sie die -API für die Migration verwenden WorkSpaces und die Migration nicht erfolgreich ist, wird die von der API zurückgegebene Ziel- WorkSpace ID nicht verwendet und der WorkSpace hat immer noch die ursprüngliche WorkSpace ID.

- Wenn eine Migration nicht erfolgreich abgeschlossen wurde, überprüfen Sie Active Directory, ob sie entsprechend bereinigt wurde. Möglicherweise müssen Sie manuell entfernen WorkSpaces , die Sie nicht mehr benötigen.

Auswirkungen auf die Abrechnung

Während des Monats, in dem die Migration stattfindet, werden Ihnen anteilige Beträge sowohl für das neue als auch für das ursprüngliche berechnet WorkSpaces. Wenn Sie beispielsweise am 10. Mai WorkSpace A zu WorkSpace B migrieren, wird Ihnen vom 1. Mai bis zum 10. Mai WorkSpace A in Rechnung gestellt, und Ihnen wird vom 11. Mai bis zum 30. Mai WorkSpace B in Rechnung gestellt.

> **Note**
>
> Wenn Sie eine WorkSpace zu einem anderen Bundle-Typ migrieren (z. B. von Performance zu Power oder Value zu Standard), kann die Größe des Stamm-Volumes (Laufwerk C) und des Benutzer-Volumes (Laufwerk D) während des Migrationsprozesses zunehmen. Falls erforderlich, erhöht sich das Root-Volume und entspricht der Standardgröße des Root-Volumes für das neue Bundle. Wenn Sie jedoch bereits eine andere Größe (höher oder niedriger) für das Benutzervolume als die Standardgröße für das ursprüngliche Bundle angegeben haben, wird dieselbe Größe des Benutzervolumes während des Migrationsprozesses beibehalten. Andernfalls verwendet der Migrationsprozess die größere Größe des WorkSpace Quellbenutzer-Volumes und die Standardgröße des Benutzer-Volumes für das neue Paket.

Migrieren eines WorkSpace

Sie können WorkSpaces über die Amazon- WorkSpaces Konsole, die AWS CLI oder die Amazon WorkSpaces-API migrieren.

So migrieren Sie eine WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie Ihre WorkSpace und Aktionen, Migrieren aus WorkSpaces.
4. Wählen Sie unter Pakete das Paket aus, zu dem Sie Ihre migrieren möchten WorkSpace .

> **Note**
>
> Um ein BYOL WorkSpace von PCoIP zu WSP zu migrieren, müssen Sie zunächst ein BYOL-Paket mit dem WSP-Protokoll erstellen. Anschließend können Sie Ihr PCoIP BYOL WorkSpaces zu diesem WSP BYOL-Paket migrieren.

5. Wählen Sie Migrieren aus WorkSpaces.

   Ein neuer WorkSpace mit dem Status wird in der Amazon WorkSpaces-Konsole `PENDING` angezeigt. Wenn die Migration abgeschlossen ist, WorkSpace wird das Original beendet und der Status des neuen WorkSpace wird auf gesetzt`AVAILABLE`.

6. (Optional) Informationen zum Löschen benutzerdefinierter Bundles und Abbilder, die Sie nicht mehr benötigen, finden Sie unter Löschen Sie ein benutzerdefiniertes WorkSpaces Bundle oder Image.

Verwenden Sie den Befehl migrate-workspaceAWS CLI, um WorkSpaces durch die zu migrieren. Informationen zur Migration WorkSpaces über die Amazon WorkSpaces -API finden Sie unter MigrateWorkSpace in der Amazon WorkSpaces -API-Referenz .

Löschen eines WorkSpaces

Wenn Sie einen WorkSpace nicht mehr benötigen, können Sie ihn löschen. Sie können auch verwandte Ressourcen löschen.

> **Warning**
>
> Das Löschen eines WorkSpace ist ein dauerhafter Vorgang und kann nicht rückgängig gemacht werden. Die Daten des WorkSpace-Benutzers bleiben nicht erhalten und werden vernichtet. Wenn Sie Hilfe bei der Sicherung von Benutzerdaten benötigen, wenden Sie sich an den AWS-Support.

> **Note**
>
> Simple AD und AD Connector werden Ihnen kostenlos zur Verwendung mit WorkSpaces zur Verfügung gestellt. Wenn an 30 aufeinanderfolgenden Tagen keine WorkSpaces mit Ihrem

AD-Connector-Verzeichnis verwendet werden, wird dieses Verzeichnis automatisch für die Verwendung mit Amazon WorkSpaces abgemeldet. Das Verzeichnis wird Ihnen gemäß den AWS Directory Service-Preisbedingungen in Rechnung gestellt.
Informationen zum Löschen leerer Verzeichnisse finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces. Wenn Sie Ihr Simple-AD- oder AD-Connector-Verzeichnis löschen, können Sie jederzeit ein neues erstellen, wenn Sie WorkSpaces wieder verwenden möchten.

So löschen Sie einen WorkSpace

Sie können einen WorkSpace löschen, der sich in einem beliebigen Status (mit Ausnahme von Ausgesetzt) befindet.

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich WorkSpaces aus.
3. Wählen Sie den WorkSpace und Löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie WorkSpace löschen. Das Löschen eines WorkSpace dauert ungefähr 5 Minuten. Während des Löschvorgangs wird der Status des WorkSpace auf Beenden gesetzt. Wenn der Löschvorgang abgeschlossen ist, verschwindet der WorkSpace aus der Konsole.
5. (Optional) Informationen zum Löschen nicht länger benötigter, benutzerdefinierter Bundles und Bilder finden Sie unter Löschen Sie ein benutzerdefiniertes WorkSpaces Bundle oder Image.
6. (Optional) Nach dem Löschen aller WorkSpaces in einem Verzeichnis können Sie das Verzeichnis löschen. Weitere Informationen finden Sie unter Löschen des Verzeichnisses für Ihre WorkSpaces.
7. (Optional) Nach dem Löschen aller Ressourcen in der Virtual Private Cloud (VPC) für Ihr Verzeichnis, können Sie die VPC löschen und die für das NAT-Gateway verwendete Elastic IP-Adresse freigeben. Weitere Informationen finden Sie unter Löschen der VPC und Arbeiten mit Elastic-IP-Adressen im Amazon-VPC-Benutzerhandbuch.

So löschen Sie einen WorkSpace über die AWS CLI

Verwenden Sie den Befehl terminate-workspaces.

WorkSpace -Pakete und -Images

Ein WorkSpace Paket ist eine Kombination aus Betriebssystem und Speicher-, Datenverarbeitungs- und Softwareressourcen. Wenn Sie eine starten WorkSpace, wählen Sie das Paket aus, das Ihren Anforderungen entspricht. Die für verfügbaren Standardpakete WorkSpaces werden als öffentliche Pakete bezeichnet. Weitere Informationen zu den verschiedenen öffentlichen Paketen, die für verfügbar sind WorkSpaces, finden Sie unter Amazon WorkSpaces-Pakete.

Wenn Sie ein Windows oder Linux gestartet WorkSpace und angepasst haben, können Sie ein benutzerdefiniertes Image aus diesem erstellen WorkSpace.

Ein benutzerdefiniertes Image enthält nur das Betriebssystem, die Software und die Einstellungen für die WorkSpace. Ein benutzerdefiniertes Paket ist eine Kombination aus diesem benutzerdefinierten Image und der Hardware, von der aus ein gestartet werden WorkSpace kann.

Nachdem Sie ein benutzerdefiniertes Image erstellt haben, können Sie ein benutzerdefiniertes Paket erstellen, das das benutzerdefinierte WorkSpace Image und die zugrunde liegende Datenverarbeitungs- und Speicherkonfiguration kombiniert, die Sie auswählen. Sie können dieses benutzerdefinierte Paket dann angeben, wenn Sie neu starten, WorkSpaces um sicherzustellen, dass die neuen dieselbe konsistente Konfiguration WorkSpaces haben (Hardware und Software).

Wenn Sie Softwareupdates durchführen oder zusätzliche Software auf Ihrem installieren müssen WorkSpaces, können Sie Ihr benutzerdefiniertes Paket aktualisieren und es zum Neuaufbau Ihres verwenden WorkSpaces.

WorkSpaces unterstützt mehrere verschiedene Betriebssysteme (OS), Streaming-Protokolle und Pakete. Die folgende Tabelle enthält Informationen zu den Lizenzen, Streaming-Protokollen und Paketen, die von jedem Betriebssystem unterstützt werden.

Betriebssystem	Lizenzen	Streaming-Protokolle	Unterstützte Pakete	Lebenszyklusrichtlinie/ Ausmusterungsdatum
Windows Server 2016	Enthalten	WSP, PCoIP	Wert, Standard, Leistung, Leistung, PowerPro, Grafik (veraltet), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	12. Januar 2027
Windows Server 2019	Enthalten	WSP, PCoIP	Wert, Standard, Leistung, Leistung, PowerPro, Grafik (veraltet), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	9. Januar 2029
Windows Server 2022	Enthalten	WSP, PCoIP	Standard, Leistung, Leistung, PowerPro, Grafik (veraltet), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	14. Oktober 2031
Windows 10	Bring Your Own License (BYOL)	WSP, PCoIP	Wert, Standard, Leistung, Leistung, PowerPro, Grafik (veraltet), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	In - Unterstützung
Windows 11	Bring Your Own License (BYOL)	WSP	Standard, Leistung, Leistung, PowerPro	In - Unterstützung
Amazon Linux 2	Enthalten	WSP, PCoIP	Wert, Standard, Leistung, Leistung, PowerPro	30. Juni 2025

Betriebssystem	Lizenzen	Streaming-Protokolle	Unterstützte Pakete	Lebenszyklusrichtlinie/ Ausmusterungsdatum
Ubuntu 22.04 LTS	Enthalten	WSP	Wert, Standard, Leistung, Leistung, PowerProGrafik.g4dn, GraphicsPro.g4dn	Juni 2032

> **Note**
>
> - Es ist nicht garantiert, dass Betriebssystemversionen funktionieren, die vom Anbieter nicht mehr unterstützt werden, und werden von nicht unterstütztAWS.
> - Für die WorkSpaces Ausführung auf einem Windows-Betriebssystem unterstützt Graphics-Bundles nur das PCoIP-Streaming-Protokoll.

Inhalt

Paketoptionen

Bevor Sie ein Paket auswählen, stellen Sie sicher, dass das Paket, das Sie auswählen möchten, mit dem Protokoll, dem Betriebssystem, dem Netzwerk und dem Computertyp Ihrer WorkSpaces kompatibel ist. Weitere Informationen zu Protokollen finden Sie unter Protokolle für Amazon

WorkSpaces. Weitere Informationen zu Netzwerken finden Sie unter Netzwerkanforderungen für Amazon-WorkSpaces-WorkSpaces-Clients.

> **Note**
>
> - Wir empfehlen, eine maximale Netzwerklatenz von 250 ms für PCoIP-WorkSpaces nicht zu überschreiten. Wie empfehlen, die Netzwerklatenz unter 100 ms zu halten, um die beste Erfahrung für Benutzer mit PCoIP-WorkSpaces zu erzielen. Wenn die Round-Trip-Zeit (RTT) 375 ms überschreitet, wird die WorkSpaces-Client-Verbindung heruntergefahren. Für eine optimale Erfahrung der Benutzer mit dem WorkSpaces Streaming Protocol (WSP) empfehlen wir, die RTT unter 250 ms zu halten. Wenn die RTT zwischen 250 ms und 400 ms liegt, können die Benutzer auf die WorkSpaces zugreifen, die Leistung wird jedoch erheblich sinken.
> - Wir empfehlen, die Leistung der Pakete, die Sie auswählen möchten, in einer Testumgebung zu prüfen, indem Sie Anwendungen ausführen und verwenden, die die täglichen Aufgaben Ihrer Benutzer abbilden.

> **Important**
>
> - Das Graphics-Paket wird nach dem 30. November 2023 nicht mehr unterstützt. Wir empfehlen, mithilfe des Graphics-Pakets zum Graphics.g4dn-Paket für WorkSpaces zu wechseln.
> - Die Graphics- und GraphicsPro-Pakete sind derzeit in der Region Asien-Pazifik (Mumbai) nicht verfügbar.

Im Folgenden sind die Pakete aufgeführt, die WorkSpaces anbietet. Weitere Informationen zu den verschiedenen Paketen in WorkSpaces finden Sie unter Amazon-WorkSpaces-Pakete.

Value-Paket

Dieses Paket eignet sich ideal für:

- Grundlegende Textbearbeitung und Dateneingabe
- Surfen im Internet mit geringer Nutzung
- Instant-Messaging

Dieses Paket wird nicht für Textverarbeitung, Audio- und Videokonferenzen, Bildschirmübertragung, Softwareentwicklungstools, Business-Intelligence-Anwendungen und Grafikanwendungen empfohlen.

Standard-Paket

Dieses Paket eignet sich ideal für:

- Grundlegende Textbearbeitung und Dateneingabe
- Surfen im Internet
- Instant-Messaging
- E-Mail

Dieses Paket wird nicht für Textverarbeitung, Audio- und Videokonferenzen, Bildschirmübertragung, Softwareentwicklungstools, Business-Intelligence-Anwendungen und Grafikanwendungen empfohlen.

Performance-Paket

Dieses Paket eignet sich ideal für:

- Surfen im Internet
- Textverarbeitung
- Instant-Messaging
- E-Mail
- Tabellenkalkulation
- Audioverarbeitung
- Courseware

Dieses Paket wird nicht für Audio- und Videokonferenzen, Bildschirmübertragung, Softwareentwicklungstools, Business-Intelligence-Anwendungen und Grafikanwendungen empfohlen.

Power-Paket

Dieses Paket eignet sich ideal für:

- Surfen im Internet
- Textverarbeitung
- E-Mail

- Instant-Messaging
- Tabellenkalkulation
- Audioverarbeitung
- Softwareentwicklung (Integrierte Entwicklungsumgebung, IDE)
- Datenverarbeitung auf niedriger bis mittlerer Ebene
- Audio- und Videokonferenzen

Dieses Paket wird nicht für Bildschirmübertragung, Softwareentwicklungstools, Business-Intelligence-Anwendungen und Grafikanwendungen empfohlen.

PowerPro-Paket

Dieses Paket eignet sich ideal für:

- Surfen im Internet
- Textverarbeitung
- E-Mail
- Instant-Messaging
- Tabellenkalkulation
- Audioverarbeitung
- Softwareentwicklung (Integrierte Entwicklungsumgebung, IDE)
- Data-Warehousing
- Business-Intelligence-Anwendungen
- Audio- und Videokonferenzen

Dieses Paket wird nicht für das Training von Machine-Learning-Modellen und für Grafikanwendungen empfohlen.

GraphicsPro-Paket

Dieses Paket bietet eine grundlegende Grafikleistung und ein hohes Maß an CPU-Leistung und Arbeitsspeicher für Ihre WorkSpaces. Es eignet sich ideal für:

- Surfen im Internet
- Textverarbeitung

- E-Mail
- Instant-Messaging
- Tabellenkalkulation
- Audiokonferenzen
- Softwareentwicklung (Integrierte Entwicklungsumgebung, IDE)
- Data-Warehousing
- Business-Intelligence-Anwendungen
- Grafikdesign
- Bildverarbeitung

Dieses Paket wird nicht für Audio- und Videokonferenzen, 3D-Rendering und fotorealistisches Design empfohlen.

Graphics.g4dn-Paket

Dieses Paket bietet eine grundlegende Grafikleistung und ein hohes Maß an CPU-Leistung und Arbeitsspeicher für Ihre WorkSpaces.

- Surfen im Internet
- Textverarbeitung
- E-Mail
- Tabellenkalkulation
- Instant-Messaging
- Audiokonferenzen
- Softwareentwicklung (Integrierte Entwicklungsumgebung, IDE)
- Datenverarbeitung auf niedriger bis mittlerer Ebene
- Data-Warehousing
- Business-Intelligence-Anwendungen
- Grafikdesign
- CAD/CAM (Computer-Aided Design/Computer-Aided Manufacturing)

Dieses Paket wird nicht für Audio- und Videokonferenzen, 3D-Rendering, fotorealistisches Design und das Training von Machine-Learning-Modellen empfohlen.

GraphicsPro.g4dn

Graphics.g4dn-Paket

Dieses Paket bietet eine hohe Grafikleistung, CPU-Leistung und Arbeitsspeicher für Ihre WorkSpaces und eignet sich für:

- Surfen im Internet
- Textverarbeitung
- E-Mail
- Tabellenkalkulation
- Instant-Messaging
- Audiokonferenzen
- Softwareentwicklung (Integrierte Entwicklungsumgebung, IDE)
- Datenverarbeitung auf niedriger bis mittlerer Ebene
- Data-Warehousing
- Business-Intelligence-Anwendungen
- Grafikdesign
- CAD/CAM (Computer-Aided Design/Computer-Aided Manufacturing)
- Videotranskodierung
- 3D-Rendering
- Fotorealistisches Design
- Game-Streaming
- ML-Modelltraining (Machine Learning) und ML-Inferenz

Dieses Paket wird nicht für Audio- und Videokonferenzen empfohlen.

Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket

Wenn Sie ein Windows- oder Linux-Betriebssystem gestartet WorkSpace und es angepasst haben, können Sie ein benutzerdefiniertes Image und daraus benutzerdefinierte Bundles erstellen. WorkSpace

Ein benutzerdefiniertes Image enthält nur das Betriebssystem, die Software und die WorkSpace Einstellungen für. Ein benutzerdefiniertes Paket ist eine Kombination aus diesem benutzerdefinierten Image und der Hardware, von der aus ein gestartet werden WorkSpace kann.

> **Note**
>
> Stellen Sie sicher, dass Sie nach dem Löschen eines Bundles mindestens 2 Stunden warten, bevor Sie ein neues Bundle mit demselben Namen erstellen.

Nachdem Sie ein benutzerdefiniertes Abbild erstellt haben, können Sie ein benutzerdefiniertes Bundle erstellen, das das benutzerdefinierte Abbild mit der zugrunde liegenden Rechen- und Speicherkonfiguration kombiniert, die Sie auswählen. Sie können dieses benutzerdefinierte Paket dann angeben, wenn Sie ein neues Paket starten, WorkSpaces um sicherzustellen, dass das neue Paket dieselbe konsistente Konfiguration (Hardware und Software) WorkSpaces hat.

Sie können anhand desselben benutzerdefinierten Image verschiedene benutzerdefinierte Bundles erstellen, indem Sie für jedes Bundle verschiedene Rechen- und Speicheroptionen auswählen.

> **Important**
>
> - Wenn Sie vorhaben, ein Abbild von einem Windows 10-System aus zu erstellen WorkSpace, beachten Sie, dass die Imageerstellung auf Windows 10-Systemen nicht unterstützt wird, die von einer Version von Windows 10 auf eine neuere Version von Windows 10 aktualisiert wurden (ein Windows-Funktions-/Versionsupgrade). Kumulative Windows-Updates oder Sicherheitsupdates werden jedoch vom Prozess der Image-Erstellung unterstützt. WorkSpaces
> - Nach dem 14. Januar 2020 können keine Abbilder aus öffentlichen Windows 7-Bundles mehr erstellt werden. Möglicherweise möchten Sie eine Migration von Windows 7 WorkSpaces auf Windows 10 in Betracht ziehen. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.
> - Das Graphics-Paket wird nach dem 30. November 2023 nicht mehr unterstützt. Wir empfehlen, Ihr Paket auf Graphics.G4DN WorkSpaces zu migrieren. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.
> - Grafiken und GraphicsPro Bundles sind derzeit in der Region Asien-Pazifik (Mumbai) nicht verfügbar.

- Speichervolumen für benutzerdefinierte Pakete dürfen nicht kleiner sein als Speichervolumen für Bilder.

Benutzerdefinierte Bundles kosten genauso viel wie die öffentlichen Bundles, aus denen sie erstellt werden. Weitere Informationen zur Preisgestaltung finden Sie unter WorkSpaces Amazon-Preise.

Inhalt

Anforderungen zum Erstellen von benutzerdefinierten Windows-Abbildern

> **Note**
>
> Windows definiert 1 GB derzeit als 1.073.741.824 Byte. Kunden müssen sicherstellen, dass sie mehr als 12.884.901.888 Byte (oder 12 GiB) auf Laufwerk C frei haben und das Benutzerprofil weniger als 10.737.418.240 Byte (oder 10 GiB) groß ist, um ein Image von a zu erstellen. WorkSpace

- Der Status von muss verfügbar sein und sein Änderungsstatus muss „Keine“ lauten WorkSpace .
- Alle Anwendungen und Benutzerprofile auf WorkSpaces Images müssen mit Microsoft Sysprep kompatibel sein.
- Alle Anwendungen, die im Abbild enthalten sein sollen, müssen auf dem Laufwerk C installiert sein.
- Für Windows 7 WorkSpaces muss die Gesamtgröße (Dateien und Daten) weniger als 10 GB betragen.

- Für Windows 7 WorkSpaces muss das C Laufwerk über mindestens 12 GB verfügbaren Speicherplatz verfügen.
- Alle Anwendungsdienste, die auf dem ausgeführt werden, WorkSpace müssen ein lokales Systemkonto anstelle von Domänenbenutzeranmeldeinformationen verwenden. Beispielsweise können Sie die Microsoft SQL Server Express-Installation nicht mit den 'Anmeldeinformationen' des Domänenbenutzers ausführen.
- Das WorkSpace darf nicht verschlüsselt sein. Die Erstellung von Bildern aus einer verschlüsselten WorkSpace Datei wird derzeit nicht unterstützt.
- Die folgenden Komponenten sind in einem Abbild erforderlich. Ohne diese Komponenten funktioniert WorkSpaces das, was Sie vom Image aus starten, nicht richtig. Weitere Informationen finden Sie unter the section called “Erforderliche Konfiguration”.
  - Windows PowerShell Version 3.0 oder höher
  - Remote Desktop Services
  - AWS PV-Treiber
  - Windows Remote Management (WinRM)
  - Teradici PCoIP-Agenten und Treiber
  - STXHD-Agenten und Treiber
  - AWS und WorkSpaces Zertifikate
  - Skylight-Agent

Anforderungen zum Erstellen von benutzerdefinierten Linux-Abbildern

- Der Status von WorkSpace muss „Verfügbar“ sein und sein Änderungsstatus muss „Keine“ lauten.
- Alle Anwendungen, die im Abbild enthalten sein sollen, müssen außerhalb des Benutzervolumes (des Verzeichnisses `/home`) installiert werden.
- Das Stamm-Volume ("/") sollte zu weniger als 97 % belegt sein.
- Der WorkSpace darf nicht verschlüsselt sein. Die Erstellung von Bildern aus einer verschlüsselten WorkSpace Datei wird derzeit nicht unterstützt.
- Die folgenden Komponenten sind in einem Abbild erforderlich. Ohne diese Komponenten funktioniert WorkSpaces das, was Sie vom Image aus starten, nicht richtig:
  - Cloud-init
  - Teradici PCoIP- oder WSP-Agenten und Treiber
  - Skylight-Agent

Bewährte Methoden

Bevor Sie ein Bild aus einem erstellen WorkSpace, gehen Sie wie folgt vor:

- Verwenden Sie eine separate VPC, die nicht mit Ihrer Produktionsumgebung verbunden ist.
- Stellen Sie das WorkSpace in einem privaten Subnetz bereit und verwenden Sie eine NAT-Instanz für ausgehenden Datenverkehr.
- Verwenden Sie ein kleines Simple AD-Verzeichnis.
- Verwenden Sie die kleinste Volume-Größe für die Quelle und passen Sie dann die Volume-Größe nach Bedarf an WorkSpace, wenn Sie das benutzerdefinierte Bundle erstellen.
- Installieren Sie alle Betriebssystemupdates (außer Windows-Funktions-/Versionsupdates) und alle Anwendungsupdates auf dem. WorkSpace Weitere Informationen finden Sie unter Wichtiger Hinweis am Anfang dieses Themas.
- Löschen Sie zwischengespeicherte Daten aus dem WorkSpace , die nicht im Paket enthalten sein sollten (z. B. den Browserverlauf, zwischengespeicherte Dateien und Browser-Cookies).
- Löschen Sie die Konfigurationseinstellungen aus den WorkSpace , die nicht im Paket enthalten sein sollten (z. B. E-Mail-Profile).
- Wechseln Sie mit DHCP zu dynamischen IP-Adresseinstellungen.
- Vergewissern Sie sich, dass Sie Ihr Kontingent für WorkSpace Bilder, die in einer Region zulässig sind, nicht überschritten haben. Standardmäßig sind dir 40 WorkSpace Bilder pro Region erlaubt. Wenn Sie dieses Kontingent erreicht haben, schlagen neue Versuche, ein Abbild zu erstellen, fehl. Verwenden Sie das Formular „WorkSpaces Limits“, um eine Erhöhung des Kontingents zu beantragen.
- Stellen Sie sicher, dass Sie nicht versuchen, ein Bild aus einer verschlüsselten Datei zu erstellen WorkSpace. Die Erstellung von Bildern aus einer verschlüsselten WorkSpace Datei wird derzeit nicht unterstützt.
- Wenn Sie Antivirensoftware auf dem ausführen WorkSpace, deaktivieren Sie diese, während Sie versuchen, ein Image zu erstellen.
- Wenn Sie auf Ihrem eine Firewall aktiviert haben WorkSpace, stellen Sie sicher, dass sie keine erforderlichen Ports blockiert. Weitere Informationen finden Sie unter IP-Adresse und Port-Anforderungen für WorkSpaces.
- Für Windows sollten WorkSpaces Sie vor der Image-Erstellung keine Gruppenrichtlinienobjekte (GPOs) konfigurieren.

- Passen Sie unter Windows WorkSpaces das Standardbenutzerprofil (`C:\Users\Default`) nicht an, bevor Sie ein Image erstellen. Wir empfehlen, Anpassungen am Benutzerprofil über Gruppenrichtlinienobjekte vorzunehmen und diese nach der Erstellung des Bildes anzuwenden. Gruppenrichtlinienobjekte können leicht geändert oder zurückgesetzt werden und sind daher weniger fehleranfällig als Anpassungen am Standardbenutzerprofil.
- Informationen zu Linux WorkSpaces finden Sie auch im Whitepaper „Bewährte Methoden zur Vorbereitung Ihrer Amazon WorkSpaces for Linux-Images“.
- Wenn Sie Smartcards unter Linux WorkSpaces mit aktiviertem WorkSpaces Streaming Protocol (WSP) verwenden möchten, finden Verwenden von Smartcards zur Authentifizierung Sie hier die Anpassungen, die Sie an Ihrem Linux vornehmen müssen, WorkSpace bevor Sie Ihr Image erstellen.
- Stellen Sie sicher, dass Sie Treiber für Netzwerkabhängigkeiten wie ENA-, NVMe- und PV-Treiber auf Ihrem aktualisieren. WorkSpaces Sie sollten dies mindestens einmal alle 6 Monate tun. Weitere Informationen finden Sie unter Installieren oder Aktualisieren des Elastic Network Adapter (ENA) -Treibers AWS-NVMe-Treiber für Windows-Instances und Aktualisieren von PV-Treibern auf Windows-Instances.
- Stellen Sie sicher, dass Sie die Agenten EC2Config, EC2Launch und EC2Launch V2 regelmäßig auf die neuesten Versionen aktualisieren. Sie sollten dies mindestens einmal alle 6 Monate tun. Weitere Informationen finden Sie unter Update EC2Config und EC2Launch.

(Optional) Schritt 1: Angeben eines benutzerdefinierten Computernamensformats für Ihr Abbild

Für Images, die über Ihre benutzerdefinierte Version oder Bring Your Own License (BYOL) WorkSpaces gestartet wurden, können Sie ein benutzerdefiniertes Präfix für das Computernamenformat angeben, anstatt das standardmäßige Computernamenformat zu verwenden. Folgen Sie dem für Ihren Abbildtyp entsprechenden Verfahren, um ein benutzerdefiniertes Präfix anzugeben.

So geben Sie ein benutzerdefiniertes Computernamenformat für benutzerdefinierte Abbilder an

1. Öffnen Sie WorkSpace das Bild, mit dem Sie Ihr benutzerdefiniertes Bild erstellen, `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` in Notepad oder einem anderen Texteditor. Weitere Informationen zum Arbeiten mit der `Unattend.xml`-Datei finden Sie in der Microsoft-Dokumentation unter Antwortdateien (unattend.xml).

> **Note**
>
> Um über den Windows-Datei-Explorer auf Ihrem auf das Laufwerk C: zuzugreifen WorkSpace, geben Sie **`C:\`** in die Adressleiste ein.

2. Vergewissern Sie sich, dass im `<settings pass="specialize">`-Abschnitt `<ComputerName>` mit einem Sternchen (`*`) festgelegt ist. Wenn `<ComputerName>` auf einen anderen Wert festgelegt ist, werden Ihre Einstellungen für den benutzerdefinierten Computernamen ignoriert. Weitere Informationen zu dieser `<ComputerName>` Einstellung finden Sie ComputerNamein der Microsoft-Dokumentation.
3. Legen Sie `<RegisteredOrganization>` und `<RegisteredOwner>` im `<settings pass="specialize">`-Abschnitt auf Ihre bevorzugten Werte fest.

   Bei Sysprep werden die Werte, die Sie für `<RegisteredOwner>` und `<RegisteredOrganization>` angeben und die miteinander verknüpft sind, sowie die ersten 7 Zeichen der kombinierten Zeichenfolge verwendet, um den Computernamen zu erstellen. *Wenn Sie beispielsweise für <RegisteredOrganization> und* ***Amazon.com EC2*** *für angeben<RegisteredOwner>, beginnen die Computernamen für das aus Ihrem benutzerdefinierten Paket WorkSpaces erstellte Paket mit EC2AMAZ-xxxxxxx.*

   > **Note**
   >
   > Die `<RegisteredOwner>`- und `<RegisteredOrganization>`-Werte im Abschnitt `<settings pass="oobeSystem">` werden von Sysprep ignoriert.

4. Speichern Sie Ihre Änderungen in der `Unattend.xml`-Datei.

So geben Sie ein benutzerdefiniertes Computernamenformat für BYOL-Abbilder an

1. Wenn Sie Windows 10 verwenden, öffnen Sie `C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml` in Notepad oder einem anderen Texteditor. Wenn Sie Windows 11 verwenden, öffnen Sie `C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml`.
2. Heben Sie die Auskommentierung von `<ComputerName>*</ComputerName>` im Abschnitt `<settings pass="specialize">` auf und vergewissern Sie sich, dass `<ComputerName>`

mit einem Sternchen (*) festgelegt ist. Wenn <ComputerName> auf einen anderen Wert festgelegt ist, werden Ihre Einstellungen für den benutzerdefinierten Computernamen ignoriert. Weitere Informationen zu dieser <ComputerName> Einstellung finden Sie ComputerNamein der Microsoft-Dokumentation.

3. Legen Sie <RegisteredOrganization> und <RegisteredOwner> im <settings pass="specialize">-Abschnitt auf Ihre bevorzugten Werte fest.

   Bei Sysprep werden die Werte, die Sie für <RegisteredOwner> und <RegisteredOrganization> angeben und die miteinander verknüpft sind, sowie die ersten 7 Zeichen der kombinierten Zeichenfolge verwendet, um den Computernamen zu erstellen. *Wenn Sie beispielsweise für <RegisteredOrganization> und* ***Amazon.com EC2*** *für angeben<RegisteredOwner>, beginnen die Computernamen für das aus Ihrem benutzerdefinierten Paket WorkSpaces erstellte Paket mit EC2AMAZ-xxxxxxx.*

   > **Note**
   >
   > Die <RegisteredOwner>- und <RegisteredOrganization>-Werte im Abschnitt <settings pass="oobeSystem"> werden von Sysprep ignoriert.

4. Wenn Sie Windows 10 verwenden, speichern Sie Ihre Änderungen in der Sysprep2008.xml-Datei. Wenn Sie Windows 11 verwenden, speichern Sie Ihre Änderungen in OOBE_unattend.xml.

Schritt 2: Ausführen von Image Checker

> **Note**
>
> Der Image Checker ist nur für Windows verfügbar. WorkSpaces Wenn Sie ein Image von einem Linux-Computer aus erstellen WorkSpace, fahren Sie mit Schritt 3: Erstellen eines benutzerdefinierten Abbilds und eines benutzerdefinierten Pakets fort.

Um zu überprüfen, ob Ihr Windows die Anforderungen für die Image-Erstellung WorkSpace erfüllt, empfehlen wir, den Image Checker auszuführen. Der Image Checker führt eine Reihe von Tests an dem Gerät durch WorkSpace , das Sie zum Erstellen Ihres Abbilds verwenden möchten, und bietet Anleitungen zur Lösung aller gefundenen Probleme.

> **Important**
>
> - Der WorkSpace muss alle vom Image Checker ausgeführten Tests bestehen, bevor Sie ihn für die Image-Erstellung verwenden können.
> - Bevor Sie den Image Checker ausführen, stellen Sie sicher, dass die neuesten Windows-Sicherheitsupdates und kumulativen Updates auf Ihrem installiert sind. WorkSpace

Führen Sie zum Abrufen von Image Checker einen der folgenden Schritte aus:

- Starten Sie Ihr neu. WorkSpace Image Checker wird während des Neustarts automatisch heruntergeladen und unter `C:\Program Files\Amazon\ImageChecker.exe` installiert.
- Laden Sie den Amazon WorkSpaces Image Checker von https://tools.amazonworkspaces.com/ImageChecker .zip https://tools.amazonworkspaces.awsapps.cn/ ImageChecker .zip Sie die Datei. `ImageChecker.exe` Kopieren Sie diese Datei nach `C:\Program Files\Amazon\`.

So führen Sie Image Checker aus

1. Öffnen Sie die `C:\Program Files\Amazon\ImageChecker.exe` Datei.
2. Wählen Sie im Dialogfeld Amazon WorkSpaces Image Checker die Option Ausführen aus.
3. Nach dem Abschluss des jeweiligen Tests können Sie dessen Status anzeigen.

   Wählen Sie für jeden Test mit dem Status FEHLGESCHLAGEN die Option Info, um Informationen anzuzeigen, wie Sie das Problem beheben, das den Fehler verursacht hat. Weitere Informationen zum Beheben dieser Probleme finden Sie unter Tipps zur Lösung von Problemen, die vom Image Checker erkannt wurden.

   Wenn bei einem Test der Status WARNUNG angezeigt wird, klicken Sie auf die Schaltfläche Fix All Warnings (Alle Warnungen beheben).

   Das Werkzeug generiert eine Ausgabeprotokolldatei in demselben Verzeichnis, in dem sich Image Checker befindet. Standardmäßig befindet sich diese Datei im Pfad `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

> **Tip**
>
> Löschen Sie diese Protokolldatei nicht. Wenn ein Problem auftritt, kann diese Protokolldatei bei der Fehlerbehebung hilfreich sein.

4. Beheben Sie gegebenenfalls alle Probleme, die zu Testfehlern und Warnungen führen, und wiederholen Sie den Vorgang, den Image Checker auszuführen, bis alle Tests WorkSpace bestanden sind. Alle Fehler und Warnungen müssen behoben werden, bevor Sie ein Abbild erstellen können.
5. Nachdem Sie WorkSpace alle Tests bestanden haben, wird die Meldung Überprüfung erfolgreich abgeschlossen angezeigt. Sie können nun ein benutzerdefiniertes Bundle erstellen.

Tipps zur Lösung von Problemen, die vom Image Checker erkannt wurden

Lesen Sie zusätzlich zu den folgenden Tipps zur Behebung von Problemen, die von Image Checker erkannt werden, auch unbedingt die Image Checker-Protokolldatei unter `C:\Program Files \Amazon\ImageChecker_yyyyMMddhhmmss.log`.

PowerShell Version 3.0 oder höher muss installiert sein

Installieren Sie die neueste Version von Microsoft Windows PowerShell.

> **Important**
>
> Die PowerShell Ausführungsrichtlinie für a WorkSpace muss so eingestellt sein, dass sie RemoteSignedSkripts zulässt. Führen Sie den ExecutionPolicy PowerShell Befehl Get- aus, um die Ausführungsrichtlinie zu überprüfen. Wenn die Ausführungsrichtlinie nicht auf Uneingeschränkt oder festgelegt ist RemoteSigned, führen Sie den ExecutionPolicy RemoteSigned Befehl Set- ExecutionPolicy — aus, um den Wert der Ausführungsrichtlinie zu ändern. Die RemoteSignedEinstellung ermöglicht die Ausführung von Skripten auf Amazon WorkSpaces, was zur Erstellung eines Images erforderlich ist.

Nur die C- und D-Laufwerke können vorhanden sein

Auf einem, das für das Imaging verwendet wird, können nur WorkSpace die `D` Laufwerke `C` und vorhanden sein. Entfernen Sie alle anderen Laufwerke, einschließlich virtueller Laufwerke.

Es können keine ausstehenden Neustarts aufgrund von Windows-Updates erkannt werden

- Der Prozess „Image erstellen“ kann erst ausgeführt werden, wenn Windows neu gestartet wurde, um die Installation von Sicherheits- oder kumulativen Updates abzuschließen. Starten Sie Windows neu, um diese Updates anzuwenden, und stellen Sie sicher, dass keine anderen ausstehenden Windows-Sicherheits- oder kumulativen Updates installiert werden müssen.
- Die Abbilderstellung wird auf Windows 10-Systemen mit Upgrade von einer Version von Windows 10 auf eine neuere Version von Windows 10 (eine Windows-Funktions-/Versionsaktualisierung) nicht unterstützt. Kumulative Windows-Updates oder Sicherheitsupdates werden jedoch von der WorkSpaces Image-Erstellung unterstützt.

Die Sysprep-Datei muss vorhanden sein und darf nicht leer sein

Wenn Probleme mit der Sysprep-Datei auftreten, wenden Sie sich an das AWS Support -Center, um Ihre EC2Config oder EC2Launch zu reparieren.

Die Benutzerprofilgröße muss weniger als 10 GB betragen.

Für Windows 7 WorkSpaces muss das Benutzerprofil (`D:\Users\`*`username`*) insgesamt weniger als 10 GB groß sein. Entfernen Sie Dateien nach Bedarf, um die Größe des Benutzerprofils zu reduzieren.

Laufwerk „C“ muss genügend freien Speicherplatz haben

Für Windows 7 WorkSpaces benötigen Sie mindestens 12 GB freien Speicherplatz auf dem LaufwerkC. Entfernen Sie Dateien nach Bedarf, um auf Laufwerk `C` Speicherplatz freizugeben. Ignorieren Sie unter Windows 10 WorkSpaces, wenn Sie eine `FAILED` Nachricht erhalten und der Festplattenspeicher mehr als 2 GB beträgt.

Unter einem Domänenkonto dürfen derzeit keine Services ausgeführt werden

Um den Prozess „Image erstellen“ auszuführen, dürfen keine Dienste auf dem WorkSpace unter einem Domänenkonto ausgeführt werden. Alle Services müssen unter einem lokalen Konto ausgeführt werden.

So führen Sie Services unter einem lokalen Konto aus

1. Öffnen Sie `C:\Program Files\Amazon\ImageChecker_`*`yyyyMMddhhmmss`*`.log` und suchen Sie die Liste der Dienste, die unter einem Domänenkonto ausgeführt werden.

2. Geben Sie im Windows-Suchfeld **`services.msc`** ein, um den Windows-Dienst-Manager zu öffnen.
3. Suchen Sie unter Anmelden als nach den Diensten, die unter Domänenkonten ausgeführt werden. (Durch Dienste, die als lokales System, lokaler Dienst oder Netzwerkdienst ausgeführt werden, wird die Erstellung von Abbildern nicht beeinträchtigt.)
4. Wählen Sie einen Dienst aus, der unter einem Domänenkonto ausgeführt wird, und wählen Sie dann Aktion, Eigenschaften.
5. Öffnen Sie die Registerkarte Anmelden. Wählen Sie unter Anmelden als die Option Lokales Systemkonto aus.
6. Wählen Sie OK aus.

Der WorkSpace muss für die Verwendung von DHCP konfiguriert sein

Sie müssen alle Netzwerkadapter auf dem so konfigurieren WorkSpace , dass sie DHCP anstelle von statischen IP-Adressen verwenden.

So stellen Sie alle Netzwerkadapter auf die Verwendung von DHCP ein

1. Geben Sie im Windows-Suchfeld **`control panel`** ein, um die Systemsteuerung zu öffnen.
2. Wählen Sie Netzwerk und Internet.
3. Wählen Sie Netzwerk- und Freigabecenter.
4. Wählen Sie Adaptereinstellungen ändern und wählen Sie einen Adapter aus.
5. Wählen Sie Einstellungen dieser Verbindung ändern.
6. Wählen Sie auf der Registerkarte Netzwerk die Option Internetprotokoll Version 4 (TCP/IPv4) aus und wählen Sie dann Eigenschaften.
7. Wählen Sie im Dialogfeld Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) die Option IP-Adresse automatisch beziehen aus.
8. Wählen Sie OK aus.
9. Wiederholen Sie diesen Vorgang für alle Netzwerkadapter auf dem WorkSpace.

Remotedesktopdienste müssen aktiviert sein

Für den Prozess „Image erstellen“ müssen Remotedesktopdienste aktiviert sein.

So aktivieren Sie Remotedesktopdienste

1. Geben Sie im Windows-Suchfeld **`services.msc`** ein, um den Windows-Dienst-Manager zu öffnen.
2. Suchen Sie in der Spalte Name nach Remotedesktopdiensten.
3. Wählen Sie Remotedesktopdienste aus, und wählen Sie dann Aktion, Eigenschaften.
4. Wählen Sie auf der Registerkarte Allgemein für Starttyp die Option Manuell oder Automatisch aus.
5. Wählen Sie OK aus.

Ein Benutzerprofil muss vorhanden sein

Das WorkSpace , das Sie zum Erstellen von Bildern verwenden, muss über ein Benutzerprofil (`D:\Users\`*`username`*) verfügen. Wenn dieser Test fehlschlägt, bitten Sie das AWS Support -Center um Hilfe.

Der Pfad der Umgebungsvariablen muss ordnungsgemäß konfiguriert sein

Im Pfad der Umgebungsvariablen für den lokalen Computer fehlen Einträge für System32 und Windows PowerShell. Diese Einträge sind erforderlich, damit „Image erstellen“ ausgeführt werden kann.

So konfigurieren Sie den Pfad der Umgebungsvariablen

1. Geben Sie im Windows-Suchfeld **`environment variables`** ein und wählen Sie Systemumgebungsvariablen bearbeiten.
2. Öffnen Sie im Dialogfeld Systemeigenschaften die Registerkarte Erweitert und wählen Sie Umgebungsvariablen.
3. Wählen Sie im Dialogfeld Umgebungsvariablen unter Systemvariablen den Eintrag Pfad aus und wählen Sie dann Bearbeiten.
4. Wählen Sie Neu und fügen Sie den folgenden Pfad hinzu:

   ```
   C:\Windows\System32
   ```
5. Wählen Sie erneut Neu und fügen Sie den folgenden Pfad hinzu:

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. Wählen Sie OK aus.

7. Starten Sie den WorkSpace neu.

> **Tip**
>
> Die Reihenfolge, in der Elemente im Pfad der Umgebungsvariablen angezeigt werden, ist wichtig. Um die richtige Reihenfolge zu ermitteln, sollten Sie den Pfad Ihrer Umgebungsvariablen WorkSpace mit dem Pfad einer neu erstellten WorkSpace oder einer neuen Windows-Instanz vergleichen.

Windows Modules Installer muss aktiviert sein

Für den Prozess „Image erstellen“ muss der Windows Modules Installer-Dienst aktiviert sein.

So aktivieren Sie den Windows Modules Installer-Dienst

1. Geben Sie im Windows-Suchfeld **`services.msc`** ein, um den Windows-Dienst-Manager zu öffnen.
2. Suchen Sie in der Spalte Name nach Windows Modules Installer.
3. Wählen Sie Windows Modules Installer, aus, und wählen Sie dann Aktion, Eigenschaften.
4. Wählen Sie auf der Registerkarte Allgemein für Starttyp die Option Manuell oder Automatisch aus.
5. Wählen Sie OK aus.

Amazon SSM Agent muss deaktiviert sein

Für den Prozess „Image erstellen“ muss der Amazon SSM Agent-Dienst deaktiviert sein.

So deaktivieren Sie den Amazon SSM Agent-Dienst

1. Geben Sie im Windows-Suchfeld **`services.msc`** ein, um den Windows-Dienst-Manager zu öffnen.
2. Suchen Sie in der Spalte Name nach Amazon SSM Agent.
3. Wählen Sie Amazon SSM Agent und dann Aktion, Eigenschaften.
4. Wählen Sie auf der Registerkarte Allgemein für Starttyp die Option Deaktiviert aus.
5. Wählen Sie OK aus.

SSL3 und TLS Version 1.2 müssen aktiviert sein

Informationen zum Konfigurieren von SSL/TLS für Windows finden Sie unter How to Enable TLS 1.2 in der Microsoft Windows-Dokumentation.

Es kann nur ein Benutzerprofil auf dem existieren WorkSpace

Für das, das Sie zum Erstellen von Bildern verwenden WorkSpace , kann es nur ein WorkSpaces Benutzerprofil (`D:\Users\`*`username`*) geben. Löschen Sie alle Benutzerprofile, die nicht dem vorgesehenen Benutzer von gehören WorkSpace.

Damit die Image-Erstellung funktioniert, WorkSpace können Sie nur drei Benutzerprofile darauf haben:

- Das Benutzerprofil des vorgesehenen Benutzers von WorkSpace (`D:\Users\`*`username`*)
- Das Standardbenutzerprofil (auch als Standardprofil bezeichnet)
- Das Administrator-Benutzerprofil

Wenn weitere Benutzerprofile vorhanden sind, können Sie sie über die erweiterten Systemeigenschaften in der Windows-Systemsteuerung löschen.

So löschen Sie ein Benutzerprofil

1. Führen Sie einen der folgenden Schritte aus, um auf die erweiterten Systemeigenschaften zuzugreifen:
   - Drücken Sie die Windows-Taste+Pause Unterbr und wählen Sie dann Erweiterte Systemeinstellungen im linken Bereich des Dialogfelds Systemsteuerung > System und Sicherheit > System aus.
   - Geben Sie in das Windows-Suchfeld **`control panel`** ein. Wählen Sie in der Systemsteuerung System und Sicherheit aus. Wählen Sie dann „System“ und danach Erweiterte Systemeinstellungen im linken Bereich der Systemsteuerung > System und Sicherheit > System aus.
2. Wählen Sie im Dialogfeld Systemeigenschaften auf der Registerkarte Erweitert unter Benutzerprofile die Option Einstellungen aus.
3. Wenn ein anderes Profil als das Administratorprofil, das Standardprofil und das Profil des vorgesehenen WorkSpaces Benutzers aufgeführt ist, wählen Sie dieses zusätzliche Profil aus und klicken Sie auf Löschen.

4. Wenn Sie gefragt werden, ob Sie das Profil löschen möchten, wählen Sie Ja.
5. Falls erforderlich, wiederholen Sie die Schritte 3 und 4, um alle anderen Profile zu entfernen, die nicht zu dem gehören WorkSpace.
6. Wählen Sie zweimal OK und schließen Sie die Systemsteuerung.
7. Starten Sie den neu WorkSpace.

Keine AppX-Pakete können sich in einem bereitgestellten Zustand befinden

Ein oder mehrere AppX-Pakete befinden sich in einem bereitgestellten Zustand. Dies kann zu einem Sysprep-Fehler während der Abbilderstellung führen.

So entfernen Sie alle bereitgestellten AppX-Pakete

1. Geben Sie in das Windows-Suchfeld **`powershell`** ein. Wählen Sie Als Administrator ausführen aus.
2. Wählen Sie auf die Frage „Möchten Sie dieser App erlauben, Änderungen an Ihrem Gerät vorzunehmen?“, Ja aus.
3. Geben Sie im PowerShell Windows-Fenster die folgenden Befehle ein, um alle bereitgestellten AppX-Pakete aufzulisten, und drücken Sie nach jedem einzelnen die Eingabetaste.

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. Geben Sie den folgenden Befehl ein, um alle bereitgestellten AppX-Pakete zu entfernen, und drücken Sie die Eingabetaste.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Führen Sie Image Checker erneut aus. Wenn dieser Test weiterhin fehlschlägt, geben Sie die folgenden Befehle ein, um alle AppX-Pakete zu entfernen, und drücken Sie nach jedem einzelnen die Eingabetaste.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows darf nicht von einer früheren Version aktualisiert worden sein

Die Abbilderstellung wird auf Windows-Systemen mit Upgrade von einer Version von Windows 10 auf eine neuere Version von Windows 10 (eine Windows-Funktions-/Versionsaktualisierung) nicht unterstützt.

Verwenden Sie zum Erstellen von Images ein, für WorkSpace das noch kein Windows-Funktions-/Versionsupgrade durchgeführt wurde.

Die WindowsRearm-Anzahl darf nicht „0“ sein

Mit der Rearm-Funktion können Sie den Aktivierungszeitraum für die Testversion von Windows verlängern. Der Prozess „Image erstellen“ erfordert, dass die Rearm-Anzahl ein anderer Wert als „0“ ist.

So überprüfen Sie die Windows-Rearm-Anzahl

1. Wählen Sie im Windows-Startmenü Windows System und dann Eingabeaufforderung aus.
2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie anschließend die Eingabetaste.

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

Informationen zum Zurücksetzen der Rearm-Anzahl auf einen anderen Wert als „0“ finden Sie unter Sysprep (Generalize) a Windows installation in der Microsoft Windows-Dokumentation.

Weitere Tipps zur Problembehandlung

Wenn Sie WorkSpace alle vom Image Checker ausgeführten Tests bestanden haben, Sie aber trotzdem kein Image aus dem erstellen können WorkSpace, überprüfen Sie, ob die folgenden Probleme vorliegen:

- Stellen Sie sicher, dass WorkSpace das keinem Benutzer innerhalb einer Domain-Gäste-Gruppe zugewiesen ist. Führen Sie den folgenden PowerShell Befehl aus, um zu überprüfen, ob Domänenkonten vorhanden sind.

  ```
  Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
  $env:USERDOMAIN*" }
  ```

- WorkSpaces Nur für Windows 7: Wenn Probleme auftreten, während das Benutzerprofil während der Image-Erstellung kopiert wird, überprüfen Sie, ob die folgenden Probleme vorliegen:
  - Lange Profilpfade können Fehler beim Erstellen von Abbildern verursachen. Stellen Sie sicher, dass die Pfade aller Ordner innerhalb des Benutzerprofils 261 Zeichen nicht überschreiten.
  - Stellen Sie sicher, dass Sie dem System und allen Anwendungspaketen vollständige Berechtigungen für den Profilordner erteilen.
  - Wenn Dateien im Benutzerprofil während der Abbilderstellung durch einen Prozess gesperrt werden oder in Gebrauch sind, schlägt das Kopieren des Profils möglicherweise fehl.
- Einige Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) beschränken den Zugriff auf den Fingerabdruck des RDP-Zertifikats, wenn dieser während der Windows-Instance-Konfiguration vom EC2config-Dienst oder den EC2Launch-Skripten angefordert wird. Bevor Sie versuchen, ein Image zu erstellen, verschieben Sie es in eine neue Organisationseinheit (OU) mit blockierter Vererbung und ohne angewendete GPOs. WorkSpace
- Stellen Sie sicher, dass der Windows-Remoteverwaltungsdienst (WinRM) so konfiguriert ist, dass er automatisch gestartet wird. Gehen Sie wie folgt vor:
  1. Geben Sie im Windows-Suchfeld **`services.msc`** ein, um den Windows-Dienst-Manager zu öffnen.
  2. Suchen Sie in der Spalte Name die Windows-Remoteverwaltung (WS-Verwaltung).
  3. Wählen Sie Windows-Remoteverwaltung (WS-Verwaltung) aus, und wählen Sie dann Aktion, Eigenschaften.
  4. Wählen Sie auf der Registerkarte Allgemein für Starttyp die Option Automatisch aus.
  5. Wählen Sie OK aus.

Schritt 3: Erstellen eines benutzerdefinierten Abbilds und eines benutzerdefinierten Pakets

Nachdem Sie Ihr WorkSpace Image validiert haben, können Sie mit der Erstellung Ihres benutzerdefinierten Images und Ihres benutzerdefinierten Bundles fortfahren.

So erstellen Sie ein benutzerdefiniertes Bild und ein benutzerdefiniertes Bundle

1. Wenn Sie immer noch mit dem verbunden sind WorkSpace, trennen Sie die Verbindung, indem Sie in der WorkSpaces Client-Anwendung Amazon WorkSpaces und Disconnect auswählen.
2. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
3. Wählen Sie im Navigationsbereich aus WorkSpaces.
4. Wählen Sie das aus WorkSpace , um die zugehörige Detailseite zu öffnen, und wählen Sie Image erstellen. Wenn der Status von „Gestoppt“ WorkSpace lautet, müssen Sie ihn zuerst starten (wählen Sie „Aktionen“, „Start“ WorkSpaces), bevor Sie „Aktionen“, „Image erstellen“ wählen können.

   > **Note**
   >
   > Verwenden Sie die CreateWorkspaceImage API-Aktion, um ein Image programmgesteuert zu erstellen. Weitere Informationen finden Sie CreateWorkspaceImagein der Amazon WorkSpaces API-Referenz.

5. Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, Ihren Computer neu zu starten (neu zu starten), WorkSpace bevor Sie fortfahren. Wenn Sie Ihre Amazon-Software neu starten, wird Ihre WorkSpaces Amazon-Software auf die neueste Version WorkSpace aktualisiert.

   Starten Sie Ihren neu, WorkSpace indem Sie die Nachricht schließen und den Anweisungen unter folgen. Neustart einer WorkSpace Wenn Sie fertig sind, wiederholen Sie Step 4 dieses Vorgangs, aber wählen Sie dieses Mal Weiter, wenn die Neustartmeldung angezeigt wird. Um ein Image zu erstellen, WorkSpace muss der Status von „Verfügbar“ und der Änderungsstatus „Keine“ lauten.
6. Geben Sie einen Namen und eine Beschreibung zur Identifizierung des Image ein und klicken Sie dann auf Create Image (Image erstellen). Während der Erstellung des Images lautet der Status von „Gesperrt WorkSpace “ und „ WorkSpace ist nicht verfügbar“.
7. Wählen Sie im Navigationsbereich Abbilder aus. Das Image ist fertig, wenn sich der Status des Images auf Verfügbar WorkSpace ändert (dies kann bis zu 45 Minuten dauern).

8. Wählen Sie das Abbild und anschließend Aktionen, Paket erstellen aus.

> **Note**
>
> Verwenden Sie die API-Aktion CreateWorkspaceBundle, um ein Paket programmgesteuert zu erstellen. Weitere Informationen finden Sie CreateWorkspaceBundlein der Amazon WorkSpaces API-Referenz.

9. Geben Sie einen Namen und eine Beschreibung für das Paket ein und gehen Sie dann wie folgt vor:

   - Wählen Sie unter Bundle-Hardwaretyp die Hardware aus, die beim Start WorkSpaces aus diesem benutzerdefinierten Paket verwendet werden soll.
   - Wählen Sie unter Speichereinstellungen eine der Standardkombinationen für die Größe des Stammvolumes und des Benutzervolumes aus oder wählen Sie Benutzerdefiniert aus und geben Sie dann Werte (bis zu 2000 GB) für Größe des Stammvolumes und Größe des Benutzervolumes ein.

     Für das Stammvolume (unter Microsoft Windows Laufwerk C, unter Linux „/“) und das Benutzervolume (unter Windows Laufwerk D, unter Linux „/home“) sind folgende Größenkombinationen verfügbar:

     - Stamm: 80 GB, Benutzer: 10 GB, 50 GB, oder 100 GB
     - Stamm: 175 GB, Benutzer: 100 GB
     - Nur für Graphics.g4dn, GraphicsPro .g4dn, Graphics und GraphicsPro WorkSpaces nur: Root: 100 GB, Benutzer: 100 GB

     Alternativ können Sie das Stamm- und Benutzer-Volume auch auf jeweils 2000 GB erweitern.

> **Note**
>
> Um sicherzustellen, dass Ihre Daten erhalten bleiben, können Sie die Größe der Stamm- oder Benutzervolumes nicht verringern, nachdem Sie a gestartet haben. WorkSpace Stellen Sie stattdessen sicher, dass Sie beim Starten von a die Mindestgrößen für diese Volumes angeben WorkSpace. Sie können ein Value-, Standard-, Performance-, Power- oder Volume PowerPro WorkSpace mit mindestens 80 GB für das Root-Volume und 10 GB für das Benutzer-Volume starten. Sie können

ein Graphics.g4dn, GraphicsPro .g4dn, Graphics oder GraphicsPro WorkSpace mit mindestens 100 GB für das Root-Volume und 100 GB für das Benutzervolume starten.

10. Klicken Sie auf Paket erstellen.
11. Wählen Sie Pakete aus und vergewissern Sie sich, dass das Paket aufgeführt ist, um zu überprüfen, ob Ihr Paket erstellt wurde.

Was ist WorkSpaces in benutzerdefinierten Windows-Images enthalten

Wenn Sie ein Abbild unter Windows 7, Windows 10 oder Windows 11 erstellen WorkSpace, ist der gesamte Inhalt des `C` Laufwerks enthalten.

Bei Windows 10 oder 11 WorkSpaces `D:\Users\`*`username`* ist das Benutzerprofil in nicht im benutzerdefinierten Abbild enthalten.

Für Windows 7 WorkSpaces ist der gesamte Inhalt des Benutzerprofils `D:\Users\`*`username`* enthalten, mit Ausnahme der folgenden:

- Kontakte
- Downloads
- Musik
- Bilder
- Gespeicherte Spiele
- Videos
- Podcasts
- Virtuelle Maschinen
- .virtualbox
- Nachverfolgung
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\

- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Was ist in WorkSpace benutzerdefinierten Linux-Images enthalten

Wenn Sie ein Image von einem Amazon Linux aus erstellen WorkSpace, wird der gesamte Inhalt des Benutzervolumes (/home) entfernt. Der Inhalt des Stammvolumes („/“) wird eingeschlossen, die folgenden anwendbaren Ordner und Schlüssel werden dabei jedoch entfernt:

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud

- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/ domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /Pos1
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/.yaml zz-workspaces-domain
- /etc/netplan/ yy-workspaces-base .yaml
- /var/lib/ AccountsService /users

Die folgenden Schlüssel werden beim Erstellen des benutzerdefinierten Abbilds permanent gelöscht:

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

Aktualisieren eines benutzerdefinierten WorkSpaces-Pakets

Sie können ein vorhandenes benutzerdefiniertes WorkSpaces-Bundle aktualisieren, indem Sie einen auf dem Bundle basierenden WorkSpace abändern und dazu ein Abbild des WorkSpace erstellen

und das Bundle mit dem neuen Abbild aktualisieren. Sie können neue WorkSpaces dann mit dem aktualisierten Bundle starten.

> **Important**
>
> Vorhandene WorkSpaces werden nicht automatisch aktualisiert, wenn Sie das Bundle aktualisieren, auf dem sie basieren. Um vorhandene WorkSpaces zu aktualisieren, die auf einem aktualisierten Bundle basieren, müssen Sie die WorkSpaces entweder umgestalten oder löschen und neu erstellen.

So aktualisieren Sie ein Paket mithilfe der Konsole

1. Stellen Sie eine Verbindung zu einem WorkSpace her, der auf dem Bundle basiert, und nehmen Sie die gewünschten Änderungen vor. Beispielsweise können Sie die neuesten Betriebssystem- und Anwendungs-Patches und zusätzliche Anwendungen installieren.

   Alternativ können Sie einen neuen WorkSpace mit demselben grundlegenden Softwarepaket (Plus oder Standard) wie dem des Abbilds, das zur Erstellung des Bundle verwendet wurde, erstellen und Änderungen durchführen.
2. Wenn Sie immer noch mit dem WorkSpace verbunden sind, trennen Sie die Verbindung, indem Sie in der WorkSpaces-Client-Anwendung Amazon WorkSpaces und Trennen auswählen.
3. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
4. Wählen Sie im Navigationsbereich WorkSpaces aus.
5. Wählen Sie den WorkSpace und anschließend Aktionen, Abbild erstellen aus. Wenn der Status des WorkSpace `STOPPED` ist, müssen Sie ihn zuerst starten (wählen Sie Aktionen, WorkSpaces starten aus), bevor Sie Aktionen, Abbild erstellen auswählen können.
6. Geben Sie einen Namen und eine Beschreibung für das Image ein und wählen Sie anschließend Create Image (Image erstellen) aus. Der WorkSpace ist nicht verfügbar, während das Abbild erstellt wird. Ausführliche Informationen zur Abbilderstellung finden Sie unter Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket.
7. Wählen Sie im Navigationsbereich Pakete aus.
8. Wählen Sie das Paket aus, um die zugehörige Detailseite zu öffnen und wählen Sie dann unter Quellabbild die Option Bearbeiten aus.
9. Wählen Sie auf der Seite Quellabbild aktualisieren das Abbild aus, das Sie erstellt haben und wählen Sie Paket aktualisieren aus.

10. Aktualisieren Sie wie erforderlich alle vorhandenen WorkSpaces, die auf dem Bundle basieren, indem Sie die WorkSpaces umgestalten oder löschen und neu erstellen. Weitere Informationen finden Sie unter Neuerstellen eines WorkSpace.

So aktualisieren Sie ein Paket programmgesteuert

Verwenden Sie die UpdateWorkspaceBundle-API-Aktion, um ein Paket programmgesteuert zu erstellen. Weitere Informationen finden Sie unter UpdateWorkspaceBundle in der Amazon-WorkSpaces-API-Referenz.

Kopieren eines benutzerdefinierten WorkSpaces-Abbilds

Sie können ein benutzerdefiniertes WorkSpace-Abbild innerhalb oder zwischen AWS-Regionen kopieren. Durch das Kopieren eines Abbilds wird ein identisches Abbild mit einem eindeutigen Bezeichner erstellt.

Sie können ein Bring-Your-Own-License (BYOL)-Abbild in eine andere Region kopieren, solange die Zielregion für BYOL aktiviert ist. Stellen Sie sicher, dass BYOL für alle beteiligten Konten und Regionen aktiviert ist.

> **Note**
>
> In der Region China (Ningxia) können Sie nur Abbilder innerhalb derselben Region kopieren. Wenden Sie sich an den AWS-Support, um Abbilder in und aus anderen AWS-Regionen zu kopieren.
> Wenden Sie sich an den AWS-Support, um Abbilder in andere Regionen zu kopieren.
> Weitere Informationen zu Opt-in-Regionen finden Sie unter Verfügbare Regionen.

Sie können auch ein Abbild kopieren, das von einem anderen AWS-Konto für Sie freigegeben wurde. Weitere Informationen über freigegebene Abbilder finden Sie unter Freigeben oder Aufheben der Freigabe eines benutzerdefinierten WorkSpaces-Abbildes.

Für das Kopieren eines Abbilds innerhalb von oder zwischen Regionen fallen keine zusätzlichen Gebühren an. Es gilt jedoch das Kontingent für die Anzahl von Abbildern in der Zielregion. Weitere Informationen über Amazon-WorkSpaces-Kontingente finden Sie unter Amazon- WorkSpaces Kontingente.

IAM-Berechtigungen zum Kopieren eines Abbilds

Wenn Sie einen IAM-Benutzer zum Kopieren eines Abbilds verwenden, muss der Benutzer die Berechtigung `workspaces:DescribeWorkspaceImages` und `workspaces:CopyWorkspaceImage` haben.

Die folgende Beispielrichtlinie erlaubt Benutzern das Kopieren des angegebenen Abbilds in das angegebene Konto in der angegebenen Region.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

Wenn Sie eine IAM-Richtlinie zum Kopieren von geteilten Abbildern für Konten erstellen, denen die Abbilder nicht gehören, können Sie im ARN keine Konto-ID angeben. Stattdessen müssen Sie * für die Konto-ID verwenden, wie in der folgenden Beispielrichtlinie gezeigt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
```

```
    ]
}
```

Sie können im ARN nur dann eine Konto-ID angeben, wenn dieses Konto Besitzer der zu kopierenden Abbilder ist.

Weitere Informationen zur Arbeit mit IAM finden Sie unter Identitäts- und Zugriffsverwaltung für WorkSpaces.

Massenkopieren von Abbilder

Sie können Abbilder nacheinander über die Konsole kopieren. Verwenden Sie zum Massenkopieren von Abbildern den API-Vorgang CopyWorkspaceImage oder den Befehl copy-workspace-image in der AWS Command Line Interface (AWS CLI). Weitere Informationen finden Sie unter CopyWorkspaceImage in der Amazon-WorkSpaces API-Referenz oder unter copy-workspace-image in der AWS CLI-Befehlsreferenz.

Important

Bevor Sie ein freigegebenes Abbild kopieren, stellen Sie sicher, dass es vom richtigen AWS-Konto aus freigegeben wurde. Verwenden Sie die API-Operationen DescribeWorkSpaceImages und DescribeWorkSpaceImagePermissions oder die Befehle describe-workspace-images und describe-workspace-image-permissions in der AWS CLI, um festzustellen, ob ein Abbild geteilt wurde, und um die AWS-Konto-ID zu sehen, der ein Abbild gehört,

Kopieren eines Abbilds mit der Konsole

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Abbilder aus.
3. Wählen Sie das Abbild und anschließend Aktionen und Abbild kopieren aus.
4. Wählen Sie unter Ziel auswählen die AWS-Region aus, in die Sie das Abbild kopieren möchten.
5. Geben Sie unter Name der Kopie den neuen Namen für das kopierte Abbild und unter Beschreibung eine Beschreibung für das kopierte Abbild ein.
6. (Optional) Geben Sie unter Tags Tags für das kopierte Abbild ein. Weitere Informationen finden Sie unter Markieren von WorkSpaces-Ressourcen.

7. Klicken Sie auf Abbild kopieren.

Freigeben oder Aufheben der Freigabe eines benutzerdefinierten WorkSpaces-Abbildes

Sie können benutzerdefinierte WorkSpaces-Abbilder innerhalb derselben AWS-Region für AWS-Konten freigeben. Nachdem ein Abbild freigegeben wurde, kann es nach Bedarf über das Empfängerkonto in andere AWS-Regionen kopiert werden. Weitere Informationen über das Kopieren von Abbildern finden Sie unter Kopieren eines benutzerdefinierten WorkSpaces-Abbilds.

> **Note**
>
> In der Region China (Ningxia) können Sie nur Abbilder innerhalb derselben Region kopieren. Wenden Sie sich an den AWS-Support, um Abbilder in und aus anderen AWS-Regionen zu kopieren.

Für die Freigabe von Abbildern fallen keine zusätzlichen Gebühren an. Es gilt jedoch das Kontingent für die Anzahl von Abbildern in der AWS-Region. Ein geteiltes Abbild wird erst dann auf das Kontingent des Empfängerkontos angerechnet, wenn der Empfänger das Abbild kopiert hat. Weitere Informationen über Amazon-WorkSpaces-Kontingente finden Sie unter Amazon- WorkSpaces Kontingente.

Wenn Sie ein freigegebenen Abbild löschen möchten, müssen Sie die Freigabe des Abbilds beenden, bevor Sie es löschen können.

Freigeben von Bring-Your-Own-License (BYOL)-Abbildern

Sie können Bring-Your-Own-License (BYOL)-Abbilder nur für AWS-Konten freigeben, für die BYOL aktiviert ist. Das AWS-Konto, für das Sie BYOL-Abbilder freigeben möchten, muss ebenfalls Ihrer Organisation bzw. deren Zahlerkonto angehören.

> **Note**
>
> Die Freigabe von BYOL-Abbildern für mehrere AWS-Konten wird in den Regionen AWS GovCloud (USA-West) und AWS GovCloud (USA-Ost) nicht unterstützt. Kontaktieren Sie den

AWS-Support, um BYOL-Abbilder für Konten in den Regionen AWS GovCloud (USA-West) und AWS GovCloud (USA-Ost) freizugeben.

Für Sie freigegebene Abbilder

Wenn Abbilder für Sie freigegeben werden, können Sie diese kopieren. Sie können dann Ihre Kopien der freigegebenen Abbilder verwenden, um Pakete zum Starten neuer WorkSpaces zu erstellen.

Important

Bevor Sie ein freigegebenes Abbild kopieren, stellen Sie sicher, dass es vom richtigen AWS-Konto aus freigegeben wurde. Verwenden Sie die API-Operationen DescribeWorkSpaceImages und DescribeWorkspaceImagePermissions oder die Befehle describe-workspace-images und describe-workspace-image-permissions in der AWS-Befehlszeilenschnittstelle (CLI), um programmgesteuert festzustellen, ob ein Abbild freigegeben wurde.

Das angezeigte Erstellungsdatum für ein Abbild, das für Sie freigegeben wurde, ist das Datum, an dem das Abbild ursprünglich erstellt wurde, nicht das Datum, an dem das Abbild für Sie freigegeben wurde.

Wenn ein Abbild mit Ihnen geteilt wurde, können Sie dieses Abbild nicht weiter mit anderen Konten teilen.

So geben Sie ein Abbild frei

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Abbilder aus.
3. Wählen Sie das Abbild aus, um ihre Detailseite zu öffnen.
4. Wählen Sie auf der Abbilddetailseite im Abschnitt Gemeinsame Konten die Option Konto hinzufügen aus.
5. Geben Sie auf der Seite Konto hinzufügen unter Konto zum Teilen hinzufügen die Konto-ID des Kontos ein, mit dem Sie das Abbild teilen möchten.

> **Important**
>
> Bevor Sie ein Abbild freigeben, überprüfen Sie, ob Sie die richtige AWS-Konto-ID verwenden.

6. Wählen Sie Abbild freigeben aus.

> **Note**
>
> Das Empfängerkonto muss das Abbild zuerst kopieren, um das geteilte Abbild verwenden zu können. Im Empfängerkonto können diese Kopien dann verwendet werden, um Pakete zum Starten neuer WorkSpaces zu erstellen.

So beenden Sie die Freigabe eines Abbilds

1. Öffnen Sie die WorkSpaces-Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Abbilder aus.
3. Wählen Sie das Abbild aus, um ihre Detailseite zu öffnen.
4. Wählen Sie auf der Abbilddetailseite im Abschnitt Gemeinsame Konten das AWS-Konto aus, mit dem Sie das Teilen beenden möchten, und wählen Sie dann Freigabe aufheben aus.
5. Wenn Sie gefragt werden, ob Sie das Teilen des Abbilds rückgängig machen möchten, wählen Sie Freigabe aufheben aus.

> **Note**
>
> Wenn Sie das Abbild löschen möchten, nachdem es nicht freigegeben ist, müssen Sie zuerst die Freigabe für alle Konten aufheben, mit denen es geteilt wurde.

Wenn Sie die Freigabe eines Abbildes aufheben, können über das Empfängerkonto keine Kopien des Abbildes mehr erstellt werden. Alle Kopien freigegebener Abbilder, die sich bereits im Empfängerkonto befinden, verbleiben jedoch in diesem Konto, und neue WorkSpaces können über diese Kopien gestartet werden.

So geben Sie Abbilder programmgesteuert frei oder heben die Freigabe auf

Verwenden Sie den API-Vorgang UpdateWorkspaceImagePermission oder den Befehl update-workspace-image-permission AWS Command Line Interface (AWS CLI), um Abbilder programmgesteuert freizugeben oder deren Freigabe aufzuheben. Verwenden Sie den API-Vorgang DescribeWorkspaceImagePermissions oder den CLI-Befehl describe-workspace-image-permissions, um festzustellen, ob ein Abbild geteilt wurde.

Löschen Sie ein benutzerdefiniertes WorkSpaces Bundle oder Image

Sie können nicht verwendete Pakete bei Bedarf löschen.

Löschen eines Pakets

Um ein Bundle zu löschen, müssen Sie zuerst alle Pakete löschen WorkSpaces , die auf dem Bundle basieren.

So löschen Sie ein Paket mithilfe der Konsole

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Pakete aus.
3. Wählen Sie das zu löschende Paket und dann Löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

So löschen Sie ein Paket programmgesteuert

Verwenden Sie die DeleteWorkspaceBundle-API-Aktion, um ein Paket programmgesteuert zu löschen. Weitere Informationen finden Sie DeleteWorkspaceBundlein der Amazon WorkSpaces API-Referenz.

> **Note**
>
> Stellen Sie sicher, dass Sie nach dem Löschen eines Bundles mindestens 2 Stunden warten, bevor Sie ein neues Bundle mit demselben Namen erstellen.

Ein Image löschen

Nachdem Sie ein benutzerdefiniertes Bundle gelöscht haben, können Sie das Abbild löschen, das Sie zum Erstellen oder Aktualisieren dieses Bundles verwendet haben.

Zum Löschen eines Abbilds müssen Sie zuerst entweder alle Pakete löschen, die dem Abbild zugeordnet sind, oder Sie müssen diese Pakete aktualisieren, um ein anderes Quellabbild zu verwenden. Sie müssen die Freigabe des Abbilds auch rückgängig machen, wenn es mit anderen Konten geteilt wurde. Das Abbild darf ebenfalls nicht im Zustand Ausstehenden oder Validierung sein.

So löschen Sie ein Abbild mit der Konsole

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Abbilder aus.
3. Wählen Sie das zu löschende Abbild und dann die Optionen Löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

So löschen Sie ein Abbild programmgesteuert

Verwenden Sie die DeleteWorkspaceImage-API-Aktion, um ein Abbild programmgesteuert zu löschen. Weitere Informationen finden Sie DeleteWorkspaceImagein der Amazon WorkSpaces API-Referenz.

Bring Your Own Windows Desktop-Lizenzen

Wenn Ihre Lizenzvereinbarung mit Microsoft dies zulässt, können Sie Ihren Windows 10- oder 11-Desktop auf Ihrem Computer installieren und bereitstellen WorkSpaces. Dafür müssen Sie Bring-Your-Own-License (BYOL) aktivieren und eine Windows-10- oder Windows-11-Lizenz bereitstellen, die die folgenden Voraussetzungen erfüllt. Weitere Informationen zur Verwendung von Microsoft-Software finden Sie unter Amazon Web Services und Microsoft. AWS

Um die Lizenzbedingungen von Microsoft einzuhalten, führen Sie AWS Ihr BYOL WorkSpaces auf Hardware aus, die für Sie in der AWS Cloud vorgesehen ist. Indem Sie Ihre eigenen Lizenzen verwenden, bieten Sie ein für alle Ihre Benutzer einheitliches Erlebnis. Weitere Informationen finden Sie unter WorkSpaces Preisgestaltung.

> **Important**
>
> Die Imageerstellung wird auf Windows 10- oder 11-Systemen nicht unterstützt, die von einer Version von Windows 10 oder 11 auf eine neuere Version von Windows 10 oder 11 aktualisiert wurden (ein Windows-Funktions-/Versionsupgrade). Kumulative Windows-Updates oder Sicherheitsupdates werden jedoch von der Image-Erstellung unterstützt. WorkSpaces

Inhalt

Voraussetzungen

Bevor Sie beginnen, prüfen Sie Folgendes:

- Ihre Lizenzvereinbarung von Microsoft Windows sieht vor, dass Windows in einer virtuell gehosteten Umgebung ausgeführt werden darf.
- Wenn Sie Pakete verwenden, die nicht GPU-fähig sind (andere Bundles als Graphics.G4DN, GraphicsPro .g4dn, Graphics und), stellen Sie sicher, dass Sie mindestens 100 pro Region verwenden. GraphicsPro WorkSpaces Diese 100 AlwaysOn AutoStop WorkSpaces können WorkSpaces eine beliebige Mischung aus und sein. Die Verwendung von mindestens 100

WorkSpaces pro Region ist eine Voraussetzung für den Betrieb Ihrer eigenen WorkSpaces dedizierten Hardware. Der Betrieb Ihrer WorkSpaces eigenen Hardware ist erforderlich, um die Microsoft-Lizenzanforderungen zu erfüllen. Die dedizierte Hardware wird AWS nebenbei bereitgestellt, sodass Ihre VPC weiterhin die Standard-Tenancy nutzen kann.

Wenn Sie GPU-fähige Bundles (Graphics.G4DN, GraphicsPro .g4dn, Graphics und GraphicsPro) verwenden möchten, stellen Sie sicher, dass Sie in einer Region mindestens 4 oder 20 GPU-fähige Pakete pro Monat auf dedizierter Hardware ausführen. AlwaysOn AutoStop WorkSpaces

> **Note**
>
> - Graphics.g4dn, .g4dn, Graphics und Bundles können derzeit nur für das PCoIP-Protokoll erstellt werden. GraphicsPro GraphicsPro
> - Das Graphics-Paket wird nach dem 30. November 2023 nicht mehr unterstützt. Wir empfehlen, Ihr Paket auf WorkSpaces Graphics.G4DN zu migrieren. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.
> - Grafiken und GraphicsPro Bundles sind derzeit in der Region Asien-Pazifik (Mumbai) nicht verfügbar.
> - Graphics.g4dn, GraphicsPro .g4dn, Graphics und GraphicsPro Bundles sind derzeit in der Region Afrika (Kapstadt) nicht verfügbar.
> - Um Ihr System WorkSpaces in der Region Afrika (Kapstadt) ausführen zu können, müssen Sie mindestens 400 WorkSpaces Exemplare in der Region Afrika (Kapstadt) ausführen.
> - Windows-11-Pakete können nur für das WSP-Protokoll erstellt werden.
> - Die Graphics.g4dn- und GraphicsPro .g4dn-Pakete sind derzeit nicht für Windows 11 verfügbar.
> - Grafiken und Bundles werden für Windows 11 nicht unterstützt. GraphicsPro
> - Value-Pakete sind für Windows 11 nicht verfügbar. Weitere Informationen zur Migration Ihres vorhandenen Value-Bundles WorkSpaces finden Sie unter. Migrieren eines WorkSpace
> - Für ein optimales Videokonferenzerlebnis empfehlen wir die Verwendung von Power oder Bundles PowerPro

- WorkSpaces kann eine Verwaltungsschnittstelle im IP-Adressbereich /16 verwenden. Die Verwaltungsschnittstelle ist mit einem sicheren WorkSpaces Verwaltungsnetzwerk verbunden,

das für interaktives Streaming verwendet wird. Dies ermöglicht WorkSpaces die Verwaltung Ihrer WorkSpaces. Weitere Informationen finden Sie unter Netzwerkschnittstellen. Dazu müssen Sie eine a /16-Netzmaske aus mindestens einem der folgenden IP-Adressbereiche reservieren:

- 10.0.0.0/8
- 100.64.0.0/10
- 172.16.0.0/12
- 192.168.0.0/16
- 198.18.0.0/15

> **Note**
>
> - Mit der Einführung des WorkSpaces Dienstes ändern sich die verfügbaren IP-Adressbereiche der Verwaltungsschnittstelle häufig. Führen Sie den Befehl list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI) aus, um festzustellen, welche Bereiche derzeit verfügbar sind.
> - Zusätzlich zu dem von Ihnen ausgewählten CIDR-Block /16 wird der IP-Adressbereich 54.239.224.0/20 für den Verwaltungsschnittstellenverkehr in allen Regionen verwendet. AWS

- Stellen Sie sicher, dass Sie die erforderlichen Verwaltungsschnittstellenports für Microsoft Windows und die Microsoft Office KMS-Aktivierung für BYOL WorkSpaces geöffnet haben. Weitere Informationen finden Sie unter Ports für die Verwaltungsschnittstelle.
- Sie haben eine virtuelle Maschine (VM), die eine unterstützte 64-Bit-Version von Windows ausführt. Eine Liste der unterstützten Versionen finden Sie im nächsten Abschnitt in diesem Thema, Für BYOL unterstützte Windows-Versionen. Die VM muss zudem die folgenden Anforderungen erfüllen:
  - Ihr Windows-Betriebssystem muss für Ihre Schlüsselverwaltungs-Server aktiviert sein.
  - Auf Ihrem Windows-Betriebssystem muss Englisch (USA) als primäre Sprache eingestellt sein.
  - Keine Software außerhalb des Lieferumfangs von Windows kann auf der VM installiert werden. Sie können zusätzliche Software installieren, z. B. eine Antiviren-Lösung, wenn Sie später ein benutzerdefiniertes Abbild erstellen.
  - Passen Sie das Standardbenutzerprofil (`C:\Users\Default`) nicht an und nehmen Sie keine anderen Anpassungen vor dem Erstellen eines Abbilds vor. Alle Anpassungen sollten nach der Erstellung des Abbildes vorgenommen werden. Es wird empfohlen, Anpassungen am Benutzerprofil über Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) durchzuführen

und diese nach der Erstellung des Abbilds anzuwenden. Dies liegt daran, dass Anpassungen, die über Gruppenrichtlinienobjekte vorgenommen werden, leicht geändert oder zurückgesetzt werden können und weniger fehleranfällig sind als Anpassungen am Standardbenutzerprofil.

- Sie müssen ein WorkSpaces_BYOL-Konto mit lokalem Administratorzugriff erstellen, bevor Sie das Bild teilen können. Das Passwort für dieses Konto ist möglicherweise später erforderlich, also notieren Sie es.
- Die VM muss sich auf einem einzelnen Volume mit einer maximalen Größe von 70 GB und mindestens 10 GB verfügbarem Speicherplatz befinden. Wenn Sie außerdem planen, Microsoft Office für Ihr BYOL-Abbild zu abonnieren, muss sich die VM auf einem einzigen Volume mit einer maximalen Größe von 70 GB und mindestens 20 GB freiem Speicherplatz befinden. Der Datenträger, auf dem sich das Root-Volume befindet, darf 70 GB nicht überschreiten.
- Auf Ihrer VM muss Windows PowerShell Version 4 oder höher ausgeführt werden.

- Stellen Sie sicher, dass Sie die neuesten Microsoft-Windows-Patches installiert haben, bevor Sie das BYOL-Checker-Skript in Schritt 3: Führen Sie das BYOL PowerShell Checker-Skript auf einer Windows-VM aus ausführen.

> **Note**
>
> - Bei BYOL AutoStop WorkSpaces kann eine große Anzahl gleichzeitiger Anmeldungen dazu führen, dass die Verfügbarkeit erheblich länger WorkSpaces dauert. Wenn Sie erwarten, dass sich viele Benutzer gleichzeitig AutoStop WorkSpaces bei Ihrem BYOL anmelden, lassen Sie sich bitte von Ihrem Kundenbetreuer beraten.
> - Verschlüsselte AMIs werden beim Importvorgang nicht unterstützt. Stellen Sie sicher, dass Sie bei der Instance, die zur Erstellung des EC2-AMI verwendet wird, die EBS-Verschlüsselung deaktivieren. Die Verschlüsselung kann aktiviert werden, nachdem die endgültige Version WorkSpaces bereitgestellt wurde.

Für BYOL unterstützte Windows-Versionen

Ihre VM muss eine der folgenden Windows-Versionen ausführen:

- Windows 10 Version 21H2 (Update Dezember 2021)
- Windows 10 Version 22H2 (Update November 2022)
- Windows 10 Enterprise LTSC 2019 (1809)

- Windows 10 LTSC für Unternehmen 2021 (21H2)
- Windows 11 Version 23H2 (Version Oktober 2023)
- Windows 11 Version 22H2 (Version Oktober 2022)

Alle unterstützten Betriebssystemversionen unterstützen alle Compute-Typen, die in der AWS Region verfügbar sind, in der Sie sie verwenden WorkSpaces. Für Versionen von Windows, die von Microsoft nicht mehr unterstützt werden, kann nicht garantiert werden, dass sie funktionieren, und sie werden auch nicht vom AWS Support unterstützt.

> **Note**
>
> Windows 10 N und Windows 11 N werden derzeit nicht für BYOL unterstützt.

Hinzufügen von Microsoft Office zum BYOL-Abbild

Wenn Sie Office über abonnieren AWS, fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter WorkSpaces Preisgestaltung.

> **Important**
>
> - Wenn Microsoft Office bereits auf der VM installiert ist, mit der Sie Ihr BYOL-Image erstellen, müssen Sie es von der VM deinstallieren, wenn Sie Office abonnieren möchten. AWS
> - Wenn Sie Office über abonnieren möchten AWS, stellen Sie sicher, dass Ihre VM über mindestens 20 GB freien Festplattenspeicher verfügt.
> - Während des Abbild-Imports können Sie Office 2016 oder 2019 abonnieren, Office 2021 jedoch nicht. Informationen zu Office 2021 und anderen Anwendungen wie Microsoft Visio 2021 und Microsoft Project 2021 finden Sie unter Anwendungen verwalten.
> - Um Ihre eigenen Microsoft 365-Lizenzen sowohl für browserbasierte als auch für Desktop-Anwendungen auf Amazon zu verwenden WorkSpaces, installieren Sie Microsoft 365-Anwendungen auf Ihrem BYOL-Image, nachdem der BYOL-Image-Aufnahmeprozess abgeschlossen ist.

> **Note**
>
> Graphics.g4dn- und GraphicsPro .g4dn-BYOL-Images unterstützen nur Office 2019 und nicht Office 2016.

Wenn Sie Office abonnieren, dauert die Erfassung von BYOL-Abbild-Dateien mindestens 3 Stunden.

Einzelheiten zum Abonnieren von Office während des BYOL-Erfassungsprozesses finden Sie unter Schritt 6: Erstellen Sie mit der Konsole ein BYOL-Image WorkSpaces .

Office-Spracheinstellungen

Wir wählen die für Ihr Office-Abonnement verwendete Sprache basierend auf der AWS Region aus, in der Sie Ihre BYOL-Bildaufnahme durchführen. Wenn Sie beispielsweise Ihre BYOL-Abbild-Erfassung in der Region Asien-Pazifik (Tokio) durchführen, ist die Sprache in Ihrem Office-Abonnement Japanisch.

Standardmäßig installieren wir eine Reihe häufig verwendeter Office-Sprachpakete auf Ihrem. WorkSpaces Wenn das gewünschte Sprachpaket nicht installiert ist, können Sie zusätzliche Sprachpakete bei Microsoft herunterladen. Weitere Informationen finden Sie unter Language Accessory Pack for Office in der Microsoft-Dokumentation.

Sie haben mehrere Möglichkeiten, um die Sprache für Office zu ändern:

Option 1: Erlauben Sie einzelnen Benutzern, ihre Office-Spracheinstellungen anzupassen.

Einzelne Benutzer können die Office-Spracheinstellungen auf ihren anpassen WorkSpaces. Weitere Informationen finden Sie unter Hinzufügen einer Bearbeitungs- oder Autorensprache oder Festlegen von Sprachvoreinstellungen in Office in der Microsoft-Dokumentation.

Option 2: Verwenden Sie administrative GPO-Vorlagen (.admx/.adml), um die Office-Standardspracheinstellungen für alle Ihre Benutzer durchzusetzen WorkSpaces

Sie können GPO-Einstellungen (Group Policy Object) verwenden, um die Office-Standardspracheinstellungen für Ihre Benutzer durchzusetzen. WorkSpaces

> **Note**
>
> Ihre WorkSpaces Benutzer werden nicht in der Lage sein, die über GPO erzwungenen Spracheinstellungen zu überschreiben.

Weitere Informationen zur Verwendung von GPOs zum Festlegen der Sprache für Office finden Sie unter Anpassen der Spracheinrichtung und der Einstellungen für Office in der Microsoft-Dokumentation. Office 2016 und Office 2019 verwenden dieselben GPO-Einstellungen (mit Office 2016 gekennzeichnet).

Sie müssen die Active-Directory-Verwaltungstools installieren, um mit GPOs arbeiten zu können. Weitere Informationen zur Verwendung der Active-Directory-Verwaltungstools zum Arbeiten mit GPOs finden Sie unter Einrichten der Active-Directory-Verwaltungstools für WorkSpaces.

Bevor Sie die Richtlinieneinstellungen für Office 2016 oder Office 2019 konfigurieren können, müssen Sie die administrativen Vorlagendateien (.admx/.adml) für Office aus dem Microsoft Download Center herunterladen. Nachdem Sie die administrativen Vorlagendateien heruntergeladen haben, müssen Sie die `office16.adml` Dateien `office16.admx` und dem zentralen Speicher des Domänencontrollers für Ihr WorkSpaces Verzeichnis hinzufügen. (Die `office16.admx`- und `office16.adml`-Dateien gelten sowohl für Office 2016 als auch für Office 2019.) Weitere Informationen zum Arbeiten mit `.admx`- und `.adml`-Dateien finden Sie in der Microsoft-Dokumentation unter So erstellen und verwalten Sie den zentralen Speicher für administrative Gruppenrichtlinienvorlagen in Windows.

Das folgende Verfahren erläutert, wie Sie den zentralen Speicher erstellen und ihm die administrativen Vorlagendateien hinzufügen. Führen Sie das folgende Verfahren auf einer Verzeichnisverwaltungs WorkSpace - oder Amazon EC2 EC2-Instance durch, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist.

So installieren Sie die Dateien für die administrative Gruppenrichtlinienvorlage für Office

1. Laden Sie die administrativen Vorlagendateien (.admx/.adml) für Office aus dem Microsoft Download Center herunter.
2. Öffnen Sie in einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, den Windows-Datei-Explorer und geben Sie in der Adressleiste den vollqualifizierten Domainnamen (FQDN) Ihrer Organisation ein, z. B. `\\example.com`
3. Öffnen Sie das Verzeichnis `SYSVOL`.
4. Öffnen Sie den Ordner mit dem Namen *FQDN*.
5. Öffnen Sie das Verzeichnis `Policies`. Sie sollten sich jetzt in `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies` befinden.

6. Wenn er noch nicht vorhanden ist, erstellen Sie einen Ordner mit dem Namen `PolicyDefinitions`.
7. Öffnen Sie das Verzeichnis `PolicyDefinitions`.
8. Kopieren Sie die Datei `office16.admx` in den Ordner `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions`.
9. Erstellen Sie einen Ordner mit dem Namen `en-US` im Ordner `PolicyDefinitions`.
10. Öffnen Sie das Verzeichnis `en-US`.
11. Kopieren Sie die Datei `office16.adml` in den Ordner `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`.

So konfigurieren Sie die GPO-Spracheinstellungen für Office

1. Öffnen Sie in Ihrer Verzeichnisverwaltung WorkSpace oder Amazon EC2 EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verknüpft ist, das Group Policy Management Tool (gpmc.msc).
2. Erweitern Sie die Gesamtstruktur (Gesamtstruktur: ***FQDN***).
3. Erweitern Sie Domains.
4. Erweitern Sie Ihren FQDN (z. B. `example.com`).
5. Wählen Sie Ihren FQDN aus, öffnen Sie das Kontextmenü (Rechtsklick) oder öffnen Sie das Aktionsmenü und wählen Sie GPO in dieser Domain erstellen und hier verknüpfen aus.
6. Geben Sie Ihrem GPO einen Namen (z. B. **`Office`**).
7. Wählen Sie Ihr GPO aus, öffnen Sie das Kontextmenü (Rechtsklick) oder öffnen Sie das Aktionsmenü und wählen Sie Bearbeiten aus.
8. Wählen Sie im Gruppenrichtlinienverwaltungs-Editor Benutzerkonfiguration, Richtlinien, Richtliniendefinitionen für administrative Vorlagen (ADMX-Dateien), die vom lokalen Computer abgerufen wurden, Microsoft Office 2016 und Spracheinstellungen aus.

> **Note**
>
> Office 2016 und Office 2019 verwenden dieselben GPO-Einstellungen (mit Office 2016 gekennzeichnet). Wenn Richtliniendefinitionen für administrative Vorlagen (ADMX-Dateien), die vom lokalen Computer abgerufen wurden unter Benutzerkonfiguration, Richtlinien nicht angezeigt werden, sind die `office16.admx`- und `office16.adml`-Dateien nicht korrekt auf dem Computer installiert.

9. Geben Sie unter Spracheinstellungen die Sprache an, die für die folgenden Einstellungen verwendet werden soll. Stellen Sie sicher, dass jede Einstellung auf Aktiviert festgelegt ist und wählen Sie dann unter Optionen die gewünschte Sprache aus. Wählen Sie OK aus, um die Einstellung zu speichern.

    - Anzeigesprache > Hilfe anzeigen in
    - Anzeigesprache > Menüs und Dialogfelder anzeigen in
    - Bearbeitungssprachen > Primäre Bearbeitungssprache
10. Schließen Sie das Gruppenrichtlinien-Verwaltungstool, wenn Sie fertig sind.
11. Änderungen an den Gruppenrichtlinieneinstellungen werden nach dem nächsten Gruppenrichtlinien-Update für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:

    - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces Amazon-Konsole die WorkSpace und dann Aktionen, Neustart WorkSpaces).
    - Geben Sie an einer administrativen Eingabeaufforderung gpupdate /force ein.

Option 3: Aktualisieren Sie die Einstellungen der Office-Sprachregistrierung auf Ihrem WorkSpaces

Aktualisieren Sie die folgenden Registrierungseinstellungen, um die Office-Spracheinstellungen über die Registrierung festzulegen:

- HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Office\ 16.0\ Common\\ UILanguage LanguageResources
- HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Office\ 16.0\ Allgemein\\ LanguageResources HelpLanguage

Fügen Sie für diese Einstellungen einen DWORD-Schlüsselwert mit der entsprechenden Office-Gebietsschema-ID (LCID) hinzu. Die LCID für Englisch (USA) lautet beispielsweise 1033. Da es sich bei LCIDs um Dezimalwerte handelt, müssen Sie die Option Basis für den DWORD-Wert auf Dezimal festlegen. Eine Liste der Office-LCIDs finden Sie in der Microsoft-Dokumentation unter Sprachkennungen und OptionState ID-Werte in Office 2016.

Sie können diese Registrierungseinstellungen WorkSpaces über GPO-Einstellungen oder ein Anmeldeskript auf Ihre anwenden.

Weitere Informationen zum Arbeiten mit Spracheinstellungen für Office finden Sie unter Anpassen der Spracheinrichtung und der Einstellungen für Office in der Microsoft-Dokumentation.

Fügen Sie Office zu Ihrem bestehenden BYOL hinzu WorkSpaces

Sie können Ihrem bestehenden BYOL auch ein Abonnement für Office hinzufügen, WorkSpaces indem Sie wie folgt vorgehen.

- Anwendungen verwalten (empfohlen) — Sie können Microsoft Office, Microsoft Visio oder Microsoft Project 2021 auf Ihrem vorhandenen WorkSpaces installieren und konfigurieren. Weitere Informationen finden Sie unter Anwendungen verwalten.
- Migrieren a WorkSpace — Nachdem Sie ein BYOL-Paket mit installiertem Office erstellt haben, können Sie die WorkSpaces Migrationsfunktion verwenden, um Ihr vorhandenes BYOL-Bundle auf das BYOL-Bundle WorkSpaces zu migrieren, das Office abonniert hat. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.

> **Note**
>
> Die Option Anwendungen verwalten ist verfügbar, um Microsoft Office 2021 und andere Anwendungen wie Microsoft Visio 2021 und Microsoft Project 2021 auf Ihrem WorkSpaces zu installieren. Um Microsoft Office 2016 oder 2019 auf Ihrem zu installieren WorkSpaces, verwenden SieMigrieren eines WorkSpace.

Migrieren zwischen Versionen von Microsoft Office

Für die Migration von einer Microsoft-Office-Version zu einer anderen haben Sie die folgenden Optionen:

- Anwendungen verwalten (empfohlen) — Sie können die ursprüngliche Office-Version deinstallieren und Office 2021 und andere Anwendungen wie Microsoft Visio 2021 und Microsoft Project 2021 auf Ihren vorhandenen WorkSpaces installieren. Verwenden Sie den Workflow „Anwendungen verwalten“, um beispielsweise Microsoft Office 2019 zu deinstallieren und Microsoft Office 2021 zu installieren. Weitere Informationen finden Sie unter Anwendungen verwalten.
- Migration a WorkSpace — Um von Microsoft Office 2016 auf 2019 oder von Microsoft Office 2019 auf 2016 zu migrieren, müssen Sie ein BYOL-Paket erstellen, das die Version von Office abonniert hat, zu der Sie migrieren möchten. Verwenden Sie dann die WorkSpaces Migrationsfunktion, um

Ihre vorhandenen BYOL-Konten WorkSpaces , die Office abonniert haben, auf das BYOL-Paket zu migrieren, das die Version von Office abonniert hat, zu der Sie migrieren möchten. Erstellen Sie beispielsweise ein BYOL-Paket, das Office 2019 abonniert hat, um von Office 2016 auf 2019 zu migrieren. Verwenden Sie dann die WorkSpaces Migrationsfunktion, um Ihre vorhandenen BYOL-Konten, die Office 2016 abonniert haben, auf WorkSpaces das BYOL-Paket zu migrieren, das Office 2019 abonniert hat. Weitere Informationen finden Sie unter Migrieren von a. WorkSpace

Sie können diese Optionen verwenden, um Ihre WorkSpaces Microsoft Office-Abonnements zu Microsoft 365-Anwendungen AWS zu migrieren. Die Verwaltung von Anwendungen beschränkt sich jedoch auf die Deinstallation von Microsoft Office von Ihrem WorkSpace. Sie müssen Ihre eigenen Tools und Installationsprogramme mitbringen, um Microsoft 365-Anwendungen auf Ihrem WorkSpaces zu installieren.

> **Note**
>
> Mithilfe von Anwendungen verwalten können Sie Microsoft Office, Microsoft Visio oder MicrosoftProject 2021 auf Ihrem WorkSpaces installieren oder deinstallieren. Für Microsoft Office 2016- oder 2019-Versionen können Sie sie nur aus Ihren entfernen WorkSpaces. Um Microsoft Office 2016 oder 2019 auf Ihrem zu installieren WorkSpaces, migrieren Sie ein WorkSpace.

Weitere Informationen über den Migrationsprozess finden Sie unter Migrieren eines WorkSpace.

Aufheben des Office-Abonnements

Zum Aufheben des Office-Abonnements haben Sie die folgenden Optionen.

- Anwendungen verwalten (empfohlen) — Sie können Microsoft Office und andere Anwendungen wie Microsoft Visio und Microsoft Project von Ihrem WorkSpaces deinstallieren. Weitere Informationen finden Sie unter Anwendungen verwalten.
- Migrieren Sie ein WorkSpace — Sie können ein BYOL-Paket erstellen, das Office nicht abonniert hat. Verwenden Sie dann die WorkSpaces Migrationsfunktion, um Ihr vorhandenes BYOL-Paket auf das BYOL-Paket WorkSpaces zu migrieren, das Office nicht abonniert hat. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.

Office-Updates

Wenn Sie Office über abonniert haben AWS, sind Office-Updates als Teil Ihrer regulären Windows-Updates enthalten. Wir empfehlen Ihnen, Ihre BYOL-Basis-Abbilder regelmäßig zu aktualisieren, um alle Sicherheitspatches und Updates zu erhalten.

Schritt 1: Überprüfen Sie mithilfe der Amazon-Konsole, ob Ihr Konto für BYOL berechtigt ist WorkSpaces

Bevor Sie Ihr Konto für BYOL aktivieren können, müssen Sie einen Überprüfungsprozess durchlaufen, um zu bestätigen, dass Sie für BYOL berechtigt sind. Solange Sie diesen Vorgang nicht durchgeführt haben, ist die Option BYOL aktivieren in Ihrer WorkSpaces Amazon-Konsole nicht verfügbar.

> **Note**
>
> Der Überprüfungsprozess dauert mindestens einen Werktag und kann länger dauern, wenn Sie zwei oder mehr BYOL-fähige AWS Konten miteinander verknüpfen möchten, sodass sie dieselbe zugrunde liegende Hardware verwenden.

Um die Eignung Ihres Kontos für BYOL mithilfe der Amazon-Konsole zu überprüfen WorkSpaces

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Kontoeinstellungen und dann unter Bring Your Own License (BYOL) die Option BYOL-Einstellungen anzeigen WorkSpaces aus. Wenn Ihr Konto derzeit nicht für BYOL geeignet ist, erhalten Sie in einer Nachricht Anleitungen für die nächsten Schritte. Wenden Sie sich zunächst an Ihren AWS Kundenbetreuer oder Vertriebsmitarbeiter oder wenden Sie sich an das AWS Support Center. Ihr/Ihre Ansprechpartner:in wird überprüfen, ob Sie für BYOL berechtigt sind.

   Ihr/Ihre Ansprechpartner:in benötigt bestimmte Informationen von Ihnen, um festzustellen, ob Sie für BYOL berechtigt sind. Beispielsweise könnten Sie aufgefordert werden, die folgenden Fragen zu beantworten.

   - Haben Sie die zuvor aufgeführten BYOL-Anforderungen geprüft und akzeptiert?
   - In welchen AWS Regionen muss Ihr Konto für BYOL aktiviert sein?
   - Wie viele BYOL planen WorkSpaces Sie pro AWS Region einzusetzen?
   - Wie sieht Ihr Ramp-Up-Plan aus?

- Kaufen WorkSpaces Sie bei einem Wiederverkäufer?
- Welche Pakettypen benötigen Sie für BYOL?
- Hat Ihre Organisation weitere AWS Konten für BYOL in derselben Region aktiviert? Falls ja, möchten Sie diese Konten verknüpfen, sodass sie dieselbe zugrunde liegende Hardware verwenden?

  Wenn die Konten verknüpft sind, wird die Gesamtzahl der auf diesen Konten WorkSpaces bereitgestellten Konten zusammengefasst, um festzustellen, ob Sie für BYOL in Frage kommen. Beachten Sie, dass das Verknüpfen der Konten zusätzliche Zeit in Anspruch nimmt. Wenn Sie die Konten verknüpfen möchten, müssen Sie Ihrem Kontakt die Nummern der Konten mitteilen.

3. Nachdem Ihre Eignung für BYOL bestätigt wurde, können Sie mit dem nächsten Schritt fortfahren, in dem Sie BYOL für Ihr Konto in der Amazon-Konsole aktivieren. WorkSpaces

Schritt 2: Aktivieren Sie BYOL für Ihr BYOL-Konto mithilfe der Amazon-Konsole WorkSpaces

Um BYOL für Ihr Konto zu aktivieren, müssen Sie eine Verwaltungsnetzwerkschnittstelle angeben. Diese Schnittstelle ist mit einem sicheren WorkSpaces Amazon-Verwaltungsnetzwerk verbunden. Es wird für das interaktive Streaming des WorkSpace Desktops an WorkSpaces Amazon-Clients verwendet und ermöglicht Amazon WorkSpaces die Verwaltung der WorkSpace.

> **Note**
>
> Die Schritte in diesem Verfahren zur Aktivierung von BYOL für Ihr Konto müssen pro Region nur einmal ausgeführt werden.

So aktivieren Sie BYOL für Ihr Konto mithilfe der Amazon-Konsole WorkSpaces

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Kontoeinstellungen und dann unter Bring Your Own License (BYOL) die Option BYOL-Einstellungen anzeigen WorkSpaces aus.
3. Wählen Sie auf der Seite mit den Kontoeinstellungen unter Bring-Your-Own-License (BYOL) die Option BYOL aktivieren aus.

Wenn die Option BYOL aktivieren nicht angezeigt wird, bedeutet dies, dass Ihr Konto derzeit nicht für BYOL berechtigt ist. Weitere Informationen finden Sie unter Schritt 1: Überprüfen Sie mithilfe der Amazon-Konsole, ob Ihr Konto für BYOL berechtigt ist WorkSpaces .

4. Wählen Sie unter Bring-Your-Own-License (BYOL) (Verwendung der eigenen Lizenz) im Bereich Management network interface IP address range (IP-Adressbereich der Verwaltungsnetzwerkschnittstelle) einen IP-Adressbereich und dann Display available CIDR blocks (Verfügbare CIDR-Blöcke anzeigen).

   Amazon WorkSpaces sucht nach verfügbaren IP-Adressbereichen innerhalb des von Ihnen angegebenen Bereichs und zeigt diese als IPv4-Blöcke für Classless Inter-Domain Routing (CIDR) an. Wenn Sie einen bestimmten IP-Adressbereich benötigen, können Sie die Suche bearbeiten.

   > **Important**
   >
   > Ein einmal festgelegter IP-Adressbereich kann nicht mehr geändert werden. Stellen Sie sicher, dass Sie einen IP-Adressbereich angeben, der in keinem Konflikt mit den von Ihrem internen Netzwerk genutzten Bereichen steht. Wenn Sie Fragen dazu haben, welchen Bereich Sie angeben müssen, wenden Sie sich an Ihren AWS Kundenbetreuer oder Vertriebsmitarbeiter oder wenden Sie sich an das AWS Support Center, bevor Sie fortfahren.

5. Wählen Sie den gewünschten CIDR-Block aus der Liste der Ergebnisse aus und wählen Sie dann Enable BYOL (BYOL aktivieren).

   Dieser Vorgang kann mehrere Stunden in Anspruch nehmen. Fahren Sie während WorkSpaces der Aktivierung Ihres Kontos für BYOL mit dem nächsten Schritt fort.

Schritt 3: Führen Sie das BYOL PowerShell Checker-Skript auf einer Windows-VM aus

Nach dem Aktivieren von BYOL für Ihr Konto müssen Sie überprüfen, ob Ihre VM die Anforderungen für BYOL erfüllt. Gehen Sie dazu wie folgt vor, um das WorkSpaces BYOL Checker-Skript herunterzuladen und auszuführen. PowerShell Das Skript führt eine Reihe von Tests auf der VM durch, die Sie zum Erstellen Ihres Abbilds verwenden möchten.

> **Important**
>
> Die VM muss alle Tests bestehen, bevor Sie sie für BYOL nutzen können.

So laden Sie das BYOL Checker-Skript herunter

Bevor Sie das BYOL Checker-Skript herunterladen und ausführen, stellen Sie sicher, dass die neuesten Windows-Sicherheitsupdates auf Ihrer VM installiert sind. Während dieses Skript ausgeführt wird, wird der Windows Update-Service deaktiviert.

1. Laden Sie die ZIP-Datei des BYOL-Checker-Skripts von https://tools.amazonworkspaces.com/BYOLChecker.zip in Ihren Ordner `Downloads` herunter.
2. Erstellen Sie in Ihrem `Downloads`-Ordner einen `BYOL`-Ordner.
3. Extrahieren Sie die Dateien aus `BYOLChecker.zip` und kopieren Sie sie in den Ordner `Downloads\BYOL`.
4. Löschen Sie den Ordner `Downloads\BYOLChecker.zip`, sodass nur die extrahierten Dateien übrig bleiben.

Führen Sie die folgenden Schritte durch, um das BYOL Checker-Skript auszuführen.

So führen Sie das BYOL Checker-Skript aus

1. Öffnen Sie Windows auf dem Windows-Desktop. PowerShell Wählen Sie die Windows-Schaltfläche Start, klicken Sie mit der rechten Maustaste auf Windows PowerShell und wählen Sie Als Administrator ausführen aus. Wenn Sie von der Benutzerkontensteuerung aufgefordert werden, auszuwählen, ob Sie Änderungen PowerShell an Ihrem Gerät vornehmen möchten, wählen Sie Ja.
2. Wechseln Sie in der PowerShell Befehlszeile in das Verzeichnis, in dem sich das BYOL Checker-Skript befindet. Beispiel: Wenn sich das Skript im `Downloads\BYOL`-Verzeichnis befindet, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

   ```
   cd C:\Users\username\Downloads\BYOL
   ```

3. Geben Sie den folgenden Befehl ein, um die PowerShell Ausführungsrichtlinie auf dem Computer zu aktualisieren. Dies ermöglicht die Ausführung des BYOL Checker-Skripts:

   ```
   Set-ExecutionPolicy AllSigned
   ```

4. Wenn Sie aufgefordert werden, zu bestätigen, ob die PowerShell Ausführungsrichtlinie geändert werden soll, geben Sie A „Ja für Alle“ ein.
5. Geben Sie den folgenden Befehl ein, um das BYOL Checker-Skript auszuführen:

   ```
   .\BYOLChecker.ps1
   ```
6. Wenn eine Sicherheitsbenachrichtigung angezeigt wird, drücken Sie die Taste R, um es einmal auszuführen.
7. Wählen Sie im Dialogfeld „WorkSpaces Imagevalidierung“ die Option Tests starten aus.
8. Nach dem Abschluss des jeweiligen Tests können Sie dessen Status anzeigen. Wählen Sie für jeden Test mit dem Status FEHLGESCHLAGEN die Option Info, um Informationen anzuzeigen, wie Sie das Problem beheben, das den Fehler verursacht hat. Wenn bei einem Test der Status WARNUNG angezeigt wird, klicken Sie auf die Schaltfläche Fix All Warnings (Alle Warnungen beheben).
9. Beheben Sie ggf. sämtliche Probleme, die Fehler und Warnungen bei Tests verursachen, und wiederholen Sie Step 7 und Step 8, bis die VM alle Tests besteht. Alle Fehler und Warnungen müssen behoben werden, bevor Sie die VM exportieren.
10. Der BYOL-Skript-Checker generiert zwei Protokolldateien, `BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` und `ImageInfo.text`. Diese Dateien befinden sich im Verzeichnis mit den BYOL Checker-Skriptdateien.

    > **Tip**
    >
    > Löschen Sie diese Dateien nicht. Wenn ein Problem auftritt, können sie möglicherweise bei der Fehlerbehebung hilfreich sein.

11. Sobald Ihre VM alle Tests erfolgreich bestanden hat, erhalten Sie die NachrichtValidation Successful (Überprüfung erfolgreich). Überprüfen Sie die Gebietsschemaeinstellungen der VM, die im Tool angezeigt werden. Folgen Sie diesen Anweisungen in der Microsoft-Dokumentation, um die Gebietsschemaeinstellungen zu aktualisieren, und führen Sie das BYOL Checker-Skript erneut aus.
12. Fahren Sie die VM herunter und erstellen Sie einen Snapshot davon.
13. Starten Sie die VM erneut. Wählen Sie Run Sysprep (Sysprep ausführen). Wenn Sysprep erfolgreich ist, kann Ihre VM, die Sie im Anschluss an Step 12 exportiert haben, in Amazon Elastic Compute Cloud (Amazon EC2) importiert werden. Andernfalls überprüfen Sie die Sysprep-Protokolle, führen Sie einen Rollback auf den in Step 12 aufgenommenen Snapshot

aus, beheben Sie die gemeldeten Probleme, erstellen Sie einen neuen Snapshot und führen Sie das BYOL-Checker-Skript erneut aus.

Der häufigste Grund für das Fehlschlagen von Sysprep besteht darin, dass die Modern AppX-Pakete nicht für alle Benutzer deinstalliert sind. Verwenden Sie das Remove-AppxPackage PowerShell Cmdlet, um die AppX-Pakete zu entfernen.

14. Nachdem Sie Ihr Image erfolgreich erstellt haben, können Sie das _BYOL-Konto entfernen. WorkSpaces

Liste der Fehlermeldungen und Fehlerkorrekturen

Für den BYOL-Import ist Powershell 4.0 oder höher erforderlich. Die installierte Version von PowerShell wird nicht unterstützt.

PowerShell Version 4.0 oder höher muss installiert sein. Weitere Informationen finden Sie unter Microsoft Windows PowerShell.

Der BYOL-Import unterstützt keine Systeme, auf denen aktives Microsoft Office installiert ist.

Microsoft Office muss vor dem Import deinstalliert werden. Weitere Informationen finden Sie unter Deinstallieren von Office von einem PC.

Für den BYOL-Import ist ein System ohne PCoIP-Agent erforderlich.

Deinstallieren Sie den PCoIP-Agent. Informationen zur Deinstallation des PCoIP-Agents finden Sie unter Deinstallieren des Teradici-PCoIP Software-Clients für Mac

Für den BYOL-Import müssen Windows-Updates deaktiviert sein.

Deaktivieren Sie Windows-Updates, indem Sie die folgenden Schritte ausführen:

1. Drücken Sie die Windows-Taste + R. Geben Sie `services.msc` ein und drücken Sie dann die Eingabetaste.
2. Klicken Sie mit der rechten Maustaste auf Windows Update und wählen Sie dann Eigenschaften aus.
3. Stellen Sie auf der Registerkarte Allgemein den Starttyp auf Deaktiviert ein.
4. Wählen Sie Beenden aus.

5. Wählen Sie Übernehmen und anschließend OK aus.
6. Starten Sie Ihren Computer neu.

Für den BYOL-Import muss Automount aktiviert sein.

Sie müssen Automount aktivieren. Öffnen Sie PowerShell als Administrator und führen Sie den folgenden Befehl aus.

```
C:\> diskpart
DISKPART> automount enable
```

Automatisches Mounten neuer Volumes aktiviert.

Für den BYOL-Import muss das WorkSpaces _BYOL-Konto aktiviert sein

WorkSpacesDas _BYOL-Konto muss aktiviert sein. Weitere Informationen finden Sie unter Aktivieren von BYOL für Ihr Konto für BYOL mithilfe der WorkSpaces Amazon-Konsole.

Für den BYOL-Import muss die Netzwerkschnittstelle DHCP verwenden, um automatisch eine IP-Adresse zu erhalten. Die Netzwerkschnittstelle verwendet derzeit eine statische IP-Adresse.

Die Netzwerkschnittstelle muss geändert werden, um DHCP zu verwenden. Weitere Informationen finden Sie unter Ändern der TCP/IP-Einstellungen.

Der BYOL-Import benötigt mehr als 20 GB Speicherplatz auf der lokalen Festplatte.

Die lokale Festplatte muss über ausreichend Speicherplatz verfügen. Sie müssen 20 GB oder mehr freigeben.

Für den BYOL-Import sind Systeme mit einem lokalen Laufwerk erforderlich. Es gibt zusätzliche lokale Laufwerke, Wechsellaufwerke oder Netzlaufwerke.

Auf einem, das für den Import eines Images verwendet wird, können nur WorkSpace die Laufwerke C und D vorhanden sein. Entfernen Sie alle anderen Laufwerke, einschließlich virtueller Laufwerke.

Für den BYOL-Import ist Windows 10 oder Windows 11 erforderlich.

Verwenden Sie Windows 10 oder Windows 11.

Für den BYOL-Import sind Systeme erforderlich, die keiner AD-Domain angehören.

Das System muss aus der AD-Domain austreten. Weitere Informationen finden Sie unter Häufig gestellte Fragen zur Azure-Active-Directory-Geräteverwaltung.

Für den BYOL-Import sind Systeme erforderlich, die keiner Azure-Domain angehören.

Das System muss aus der Azure-Domain austreten. Weitere Informationen finden Sie unter Häufig gestellte Fragen zur Azure-Active-Directory-Geräteverwaltung.

Für den BYOL-Import muss die öffentliche Windows-Firewall deaktiviert sein.

Das öffentliche Firewall-Profil muss deaktiviert sein. Weitere Informationen finden Sie unter Microsoft Defender Firewall ein- oder ausschalten.

Für den BYOL-Import ist ein System ohne VMware-Tools erforderlich.

Die VMware-Tools müssen deinstalliert werden. Weitere Informationen finden Sie unter Deinstallieren und manuelles Installieren von VMware-Tools in VMware Fusion (1014522).

Für den BYOL-Import muss die lokale Festplatte weniger als 80 GB groß sein.

Die Festplatte muss kleiner als 80 GB sein. Reduzieren Sie die Festplattengröße.

Für den BYOL-Import sind weniger als 2 Partitionen auf dem lokalen Laufwerk erforderlich. Darüber hinaus müssen alle Windows-10-Partitionen MBR-Partitionen sein und alle Windows-11-Partitionen müssen GPT-Partitionen sein.

Die Volumen müssen für Windows 10 als MBR und für Windows 11 als GPT partitioniert sein. Weitere Informationen finden Sie unter Verwalten von Festplatten.

Der BYOL-Import setzt voraus, dass alle ausstehenden Updates, die Neustarts erfordern, abgeschlossen sind.

Installieren Sie alle Updates und starten Sie das Betriebssystem neu.

Für den BYOL-Import AutoLogon ist diese Option deaktiviert.

Um die AutoLogon Registrierung zu deaktivieren:

1. Drücken Sie die Windows-Taste + R und geben Sie `Regedit.exe` in der Befehlszeile ein.

2. Scrollen Sie nach unten bis `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`.
3. Fügen Sie einen Wert für `DontDisplayLastUserName` hinzu.
4. Geben Sie als Typ `REG_SZ` ein.
5. Geben Sie für Wert `0` ein.

> **Note**
>
> - Der Wert `DontDisplayLastUserName` bestimmt, ob im Anmeldedialogfeld der Benutzername des/der letzten Benutzer:in angezeigt wird, der/die sich zuletzt am PC angemeldet hat.
> - Der Wert ist standardmäßig nicht vorhanden. Falls er existiert, müssen Sie ihn auf setzen, `0` sonst `DefaultUser` wird der Wert von gelöscht und AutoLogon schlägt fehl.

Für den BYOL-Import muss **`RealTimeIsUniversal`** aktiviert sein.

RealTimeUniversal Der Registrierungsschlüssel muss aktiviert sein. Weitere Informationen finden Sie unter Konfigurieren der Zeiteinstellungen für Windows Server 2008 und höher.

Für den BYOL-Import ist ein System mit einer bootfähigen Partition erforderlich.

Es darf maximal eine bootfähige Partition vorhanden sein.

So entfernen Sie zusätzliche Partitionen

1. Drücken Sie die Tasten Windows-Logo + R, um das Ausführen-Dialogfeld zu öffnen. Geben Sie `msconfig` ein und drücken Sie die Eingabetaste auf der Tastatur, um das Systemkonfigurationsfenster zu öffnen.
2. Wählen Sie im Fenster die Registerkarte Start aus und überprüfen Sie, ob das Betriebssystem, das Sie verwenden möchten, auf Aktuelles Betriebssystem; Standard-Betriebssystem festgelegt ist. Wenn es nicht festgelegt ist, wählen Sie im Fenster das gewünschte Betriebssystem aus und wählen Sie im selben Fenster die Option Als Standard festlegen aus.
3. Wählen Sie die Partition aus und wählen Sie dann Löschen, Anwenden, OK aus, um eine andere Partition zu löschen.

Wenn der Fehler weiterhin auftritt, starten Sie Ihren Computer von der Installations- oder Reparatur-CD aus und gehen Sie wie folgt vor.

1. Überspringen Sie den ersten Bildschirm mit den Sprachen und wählen Sie dann auf dem Hauptinstallationsbildschirm die Option Computer reparieren aus.
2. Wählen Sie auf dem Bildschirm Option auswählen die Option Problembehandlung aus.
3. Wählen Sie auf dem Bildschirm Erweiterte Optionen die Option Eingabeaufforderungen aus.
4. Geben Sie in der Befehlszeile `bootrec.exe /fixmbr` ein und drücken Sie dann die Eingabetaste.

Für den BYOL-Import ist ein 64-Bit-System erforderlich.

Es muss ein 64-Bit-Betriebssystemabbild verwendet werden. Weitere Informationen finden Sie unter Für BYOL unterstützte Windows-Versionen.

Für den BYOL-Import ist ein System erforderlich, das nicht erneut aktiviert wurde.

Die Abbild-Rearm-Anzahl darf nicht „0“ sein. Mit der Rearm-Funktion können Sie den Aktivierungszeitraum für die Testversion von Windows verlängern. Der Prozess „Image erstellen“ erfordert, dass die Rearm-Anzahl ein anderer Wert als „0“ ist.

So überprüfen Sie die Windows-Rearm-Anzahl

1. Wählen Sie im Windows-Startmenü Windows System und dann Eingabeaufforderung aus.
2. Geben Sie in der Befehlszeile `cscript C:\Windows\System32\slmgr.vbs /dlv` ein und drücken Sie dann die Eingabetaste.
3. Um die Anzahl der Wiederholungen auf einen anderen Wert als 0 zurückzusetzen. Weitere Informationen finden Sie unter Sysprep (Generalisieren) einer Windows-Installation.

Für den BYOL-Import ist ein System erforderlich, für das kein In-Place-Upgrade durchgeführt wurde. Für dieses System wurde ein In-Place-Upgrade durchgeführt.

Windows darf nicht von einer früheren Version aktualisiert worden sein.

Für den BYOL-Import darf kein Antivirenprogramm auf dem System installiert sein.

Sie müssen Ihre Antivirensoftware deinstallieren. Führen Sie BYOLChecker aus, um Informationen zur zu deinstallierenden Antivirensoftware zu erhalten.

Für den BYOL-Import müssen Windows-10-Systeme über einen Legacy-Startmodus verfügen.

Für Windows 10 BootMode muss das Legacy-BIOS verwendet werden. Weitere Informationen finden Sie unter Startmodi.

Schritt 4: Exportieren der VM aus Ihrer Virtualisierungsumgebung

Zum Erstellen eines Abbilds für BYOL müssen Sie zunächst die VM aus Ihrer Virtualisierungsumgebung exportieren. Die VM muss sich auf einem einzelnen Volume mit einer maximalen Größe von 70 GB und mindestens 10 GB verfügbarem Speicherplatz befinden. Weitere Informationen finden Sie in der Dokumentation für Ihre Virtualisierungsumgebung und unter Exportieren Ihrer VM aus der Virtualisierungsumgebung im Benutzerhandbuch für VM Import/Export.

Schritt 5: Importieren der VM als Abbild in Amazon EC2

Überprüfen Sie nach dem Export Ihrer VM die Voraussetzungen für das Importieren von Windows-Betriebssystemen von einer VM. Ergreifen Sie ggf. die notwenigen Maßnahmen. Weitere Informationen finden Sie unter Voraussetzungen für VM Import/Export.

> **Note**
>
> Das Importieren einer VM mit einem verschlüsselten Datenträger wird nicht unterstützt. Wenn Sie sich für die Standardverschlüsselung für Volumes in Amazon Elastic Block Store (Amazon EBS) entschieden haben, müssen Sie diese Option deaktivieren, bevor Sie Ihre VM importieren.

Importieren Sie Ihre VM als Amazon Machine Image (AMI) in Amazon EC2. Verwenden Sie eine der folgenden Methoden:

- Verwenden Sie den Befehl import-image mit der AWS CLI. Weitere Informationen finden Sie unter import-image in der AWS CLI -Befehlsreferenz.
- Verwenden Sie die API-Operation ImportImage. Weitere Informationen finden Sie ImportImagein der Amazon EC2 API-Referenz.

Weitere Informationen finden Sie unter Importieren einer VM als Abbild im Benutzerhandbuch für VM Import/Export.

Schritt 6: Erstellen Sie mit der Konsole ein BYOL-Image WorkSpaces

Gehen Sie wie folgt vor, um ein WorkSpaces BYOL-Image zu erstellen.

> **Note**
>
> Um dieses Verfahren durchzuführen, stellen Sie sicher, dass Sie über AWS Identity and Access Management (IAM-) Berechtigungen verfügen für:
>
> - Rufen Sie an. WorkSpaces **`ImportWorkspaceImage`**
> - Amazon EC2 **`DescribeImages`** im Amazon EC2-Abbild aufrufen, das Sie verwenden möchten, um das BYOL-Abbild zu erstellen.
> - Amazon EC2 **`ModifyImageAttribute`** im Amazon EC2-Abbild aufrufen, das Sie verwenden möchten, um das BYOL-Abbild zu erstellen. Stellen Sie sicher, dass die Startberechtigungen für das Amazon-EC2-Abbild nicht eingeschränkt sind. Das Abbild muss während des gesamten BYOL-Abbild-Erstellungsprozesses zugreifbar sein.
>
> Ein Beispiel für eine IAM-Richtlinie speziell für BYOL finden Sie WorkSpaces unter. Identitäts- und Zugriffsverwaltung für WorkSpaces Weitere Informationen zum Arbeiten mit IAM-Berechtigungen finden Sie unter Ändern von Berechtigungen für einen IAM-Benutzer im IAM-Benutzerhandbuch.
> Wenn Sie aus Ihrem Bild ein Graphics.g4dn-, GraphicsPro .g4dn-, Graphics- oder GraphicsPro Bundle erstellen möchten, wenden Sie sich an das AWS Support Center, damit Ihr Konto zur Zulassungsliste hinzugefügt wird. Sobald Ihr Konto auf der Zulassungsliste steht, können Sie den AWS CLI import-workspace-image Befehl verwenden, um die Dateien Graphics.g4dn, .g4dn, Graphics oder Image aufzunehmen. GraphicsPro GraphicsPro Weitere Informationen finden Sie in der Befehlsreferenz. import-workspace-imageAWS CLI

So erstellen Sie ein Abbild aus der Windows-VM

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Abbilder aus.
3. Wählen Sie BYOL-Abbild erstellen aus.
4. Gehen Sie auf der Seite BYOL-Abbild erstellen wie folgt vor:

- Wählen Sie als AMI-ID den Link EC2-Konsole und dann das Amazon-EC2-Abbild aus, das Sie wie im vorherigen Abschnitt (Schritt 5: Importieren der VM als Abbild in Amazon EC2) beschrieben importiert haben. Der Name des Abbilds muss mit `ami-` beginnen, gefolgt von der Kennung für das AMI (z. B. `ami-1234567e`).
- Geben Sie für Name des BYOL-Abbilds einen eindeutigen Namen für das Abbild ein.
- Geben Sie unter Abbildbeschreibung eine Beschreibung zur schnellen Erkennung des Abbilds ein.
- Wählen Sie unter Instance-Typ den entsprechenden Bundle-Typ (entweder Regular, Graphics.G4DN, Graphics oder GraphicsPro), je nachdem, welches Protokoll Sie für Ihr Image verwenden möchten, entweder PCoIP oder Streaming Protocol (WSP). WorkSpaces Wenn Sie ein .g4dn-Bundle erstellen möchten, wählen Sie Graphics.G4DN. GraphicsPro Wählen Sie für nicht GPU-fähige Bundles (andere Bundles als Graphics.G4DN, .g4dn, Graphics oder) die Option Regular. GraphicsPro GraphicsPro

  > **Note**
  >
  > Graphics.g4dn, GraphicsPro .g4dn, Grafiken und GraphicsPro Bilder können derzeit nur für das PCoIP-Protokoll erstellt werden.

- (Optional) Wählen Sie unter Ausgewählte Anwendungen aus, welche Version von Microsoft Office Sie abonnieren möchten. Weitere Informationen finden Sie unter Hinzufügen von Microsoft Office zum BYOL-Abbild.
- (Optional) Wählen Sie unter Tags die Option Neuen Tag hinzufügen aus, um diesem Abbild Tags zuzuordnen. Weitere Informationen finden Sie unter Markieren von WorkSpaces-Ressourcen.

5. Wählen Sie BYOL-Abbild erstellen aus.

   Während Ihr Abbild erstellt wird, lautet der Abbildstatus auf der Abbilder-Seite der Konsole Ausstehen. Der BYOL-Erfassungsvorgang dauert mindestens 90 Minuten. Wenn Sie Office ebenfalls abonniert haben, müssen Sie damit rechnen, dass der Vorgang mindestens 3 Stunden dauert.

   Bei fehlgeschlagener Bildvalidierung zeigt die Konsole einen Fehlercode an. Ist die Abbilderstellung abgeschlossen, ändert sich der Status in Verfügbar.

Schritt 7: Erstellen eines benutzerdefinierten Pakets aus dem BYOL-Abbild

Nach dem Erstellen Ihres BYOL-Abbilds können Sie das Abbild zum Erstellen eines benutzerdefinierten Pakets verwenden. Weitere Informationen finden Sie unter Erstellen Sie ein benutzerdefiniertes WorkSpaces Image und ein Paket.

Schritt 8: Registrieren Sie ein dediziertes Verzeichnis für WorkSpaces

Um BYOL-Bilder für verwenden zu können WorkSpaces, müssen Sie zu diesem Zweck ein Verzeichnis registrieren.

Um ein Verzeichnis zu registrieren für WorkSpaces

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie das Verzeichnis und anschließend Aktionen, Registrieren.
4. Wählen Sie im Dialogfeld Verzeichnis registrieren unter Dedicated Enable Dedicated WorkSpaces die Option Ja aus.
5. Wählen Sie Register aus.

Wenn Sie bereits ein AWS Managed Microsoft AD Verzeichnis oder ein AD Connector Connector-Verzeichnis registriert haben WorkSpaces , das nicht auf dedizierter Hardware läuft, können Sie zu diesem Zweck ein neues AWS Managed Microsoft AD Verzeichnis oder AD Connector Connector-Verzeichnis einrichten. Sie können das Verzeichnis auch deregistrieren und es dann erneut als Verzeichnis für dediziert registrieren. WorkSpaces Führen Sie dazu die folgenden Schritte aus.

> **Note**
>
> Sie können dieses Verfahren nur ausführen, wenn dem Verzeichnis keine zugeordnet WorkSpaces sind.

Um die Registrierung eines Verzeichnisses aufzuheben und es erneut als dediziertes Verzeichnis zu registrieren WorkSpaces

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/workspaces/. WorkSpaces
2. Bestehende beenden WorkSpaces.

3. Wählen Sie im Navigationsbereich Verzeichnisse aus.
4. Wählen Sie das Verzeichnis und anschließend Actions, Deregister aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Deregister aus.
6. Wählen Sie das Verzeichnis erneut und anschließend Aktionen, Registrieren aus.
7. Wählen Sie im Dialogfeld Verzeichnis registrieren für Dedicated Enable Dedicated WorkSpaces die Option Ja aus.
8. Wählen Sie Register aus.

Schritt 9: Starten Sie Ihr BYOL WorkSpaces

Nachdem Sie ein Verzeichnis für Dedicated registriert haben WorkSpaces, können Sie Ihr BYOL WorkSpaces in diesem Verzeichnis starten. Informationen zum Starten finden Sie WorkSpaces unterStarten eines virtuellen Desktops mit WorkSpaces.

Überwachen Ihres WorkSpaces

Sie können die folgenden Funktionen verwenden, um Ihre zu überwachen WorkSpaces.

CloudWatch -Metriken

Amazon WorkSpaces veröffentlicht Datenpunkte in Amazon CloudWatch über Ihr WorkSpaces. CloudWatch ermöglicht es Ihnen, Statistiken zu diesen Datenpunkten als geordneten Satz von Zeitreihendaten abzurufen, die als Metriken bezeichnet werden. Sie können diese Metriken verwenden, um zu überprüfen, ob Ihre erwartungsgemäß WorkSpaces funktionieren. Weitere Informationen finden Sie unter Überwachen Sie Ihre WorkSpaces mithilfe von CloudWatch Metriken.

CloudWatch Ereignisse

Amazon WorkSpaces kann Ereignisse an Amazon CloudWatch Events senden, wenn sich Benutzer bei Ihrem anmelden WorkSpace. Auf diese Weise können Sie reagieren, wenn das Ereignis eintritt. Weitere Informationen finden Sie unter Überwachen Sie Ihre WorkSpaces Nutzung von Amazon EventBridge.

CloudTrail -Protokolle

AWS CloudTrail liefert Aufzeichnungen der Aktionen eines Benutzers, einer Rolle oder eines AWS-Services in WorkSpaces. Anhand der von CloudTrailgesammelten Informationen können Sie die an gestellte Anfrage WorkSpaces, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen. Weitere Informationen finden Sie unter Protokollieren WorkSpaces von API-Aufrufen mit CloudTrail. AWS CloudTrail protokolliert erfolgreiche und erfolglose Anmeldeereignisse für Smartcard-Benutzer. Weitere Informationen finden Sie unter AWS-Anmeldeereignisse für Smartcard-Benutzer.

CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor bietet Einblicke in die Auswirkungen von Internetproblemen auf die Leistung und Verfügbarkeit zwischen Ihren auf gehosteten Anwendungen AWS und Ihren Endbenutzern. Sie können CloudWatch Internet Monitor auch verwenden, um:

- Erstellen Sie Monitore für ein oder mehrere WorkSpace Verzeichnisse.
- Überwachen der Internetleistung
- Erhalten Sie Alarme für Probleme zwischen dem Stadtnetz Ihrer Endbenutzer, einschließlich Standort und ASN, bei der es sich in der Regel um den Internetdienstanbieter (ISP) und seine WorkSpace Regionen handelt.

Internet Monitor berechnet anhand der Verbindungsdaten, die von AWS aus seiner globalen Netzwerkpräsenz erfasst werden, eine Baseline für Leistung und Verfügbarkeit für den Internetdatenverkehr. Internet Monitor kann derzeit keine Internetleistung für einzelne Endbenutzende bereitstellen. Auf Stadt- und Internetdienstanbieterebene ist dies jedoch möglich.

Überwachen Ihres WorkSpaces Zustands mithilfe des CloudWatch automatischen Dashboards

Sie können WorkSpaces mithilfe des CloudWatch automatischen Dashboards überwachen, das Rohdaten sammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit vorliegen. Die Metriken werden 15 Monate lang aufbewahrt, um auf historische Informationen zuzugreifen und die Leistung Ihrer Webanwendung oder Ihres Services zu überwachen. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im Amazon-CloudWatch Benutzerhandbuch.

Das CloudWatch Dashboard wird automatisch erstellt, wenn Sie Ihr -AWSKonto zum Konfigurieren Ihres verwenden WorkSpaces. Mit dem Dashboard können Sie Ihre WorkSpaces Metriken, z. B. ihren Zustand und ihre Leistung, über -Regionen hinweg überwachen. Sie können das Dashboard auch für die folgenden Zwecke verwenden:

- Identifizieren Sie fehlerhafte WorkSpace Instances.
- Identifizieren Sie Ausführungsmodi, Protokolle und Betriebssysteme mit fehlerhaften WorkSpace Instances.
- Zeigen Sie die kritische Ressourcenauslastung im Laufe der Zeit an.
- Identifizieren Sie Anomalien, die bei der Fehlerbehebung helfen.

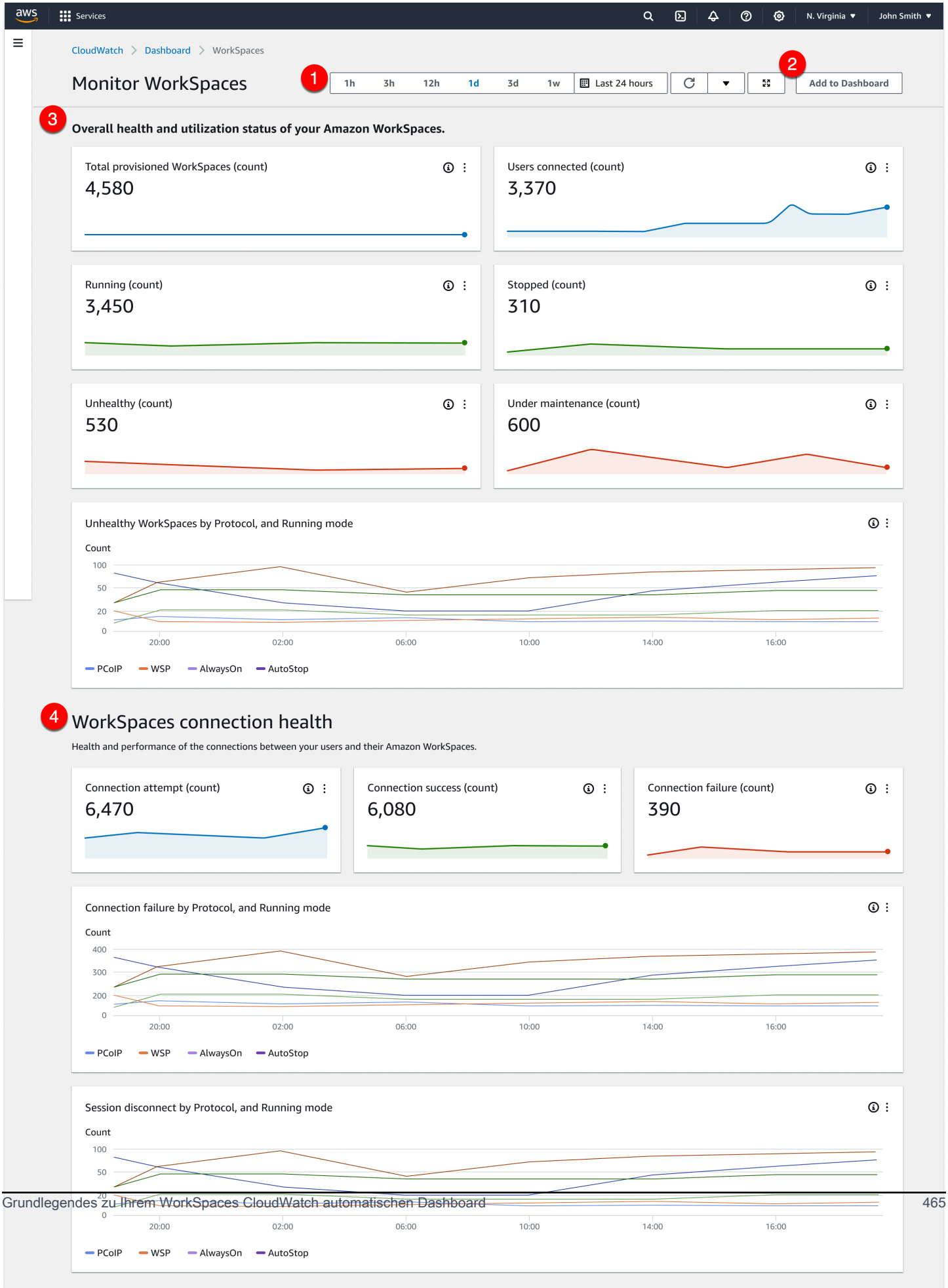
WorkSpaces CloudWatch automatische Dashboards sind in allen AWS kommerziellen Regionen verfügbar.

So verwenden Sie das WorkSpaces CloudWatch automatische Dashboard

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Dashboards aus.
3. Wählen Sie die Registerkarte Automatische Dashboards aus.
4. Wählen Sie WorkSpaces.

Grundlegendes zu Ihrem WorkSpaces CloudWatch automatischen Dashboard

Das CloudWatch automatische Dashboard ermöglicht Ihnen, Einblicke in die Leistung Ihrer - WorkSpaces Ressourcen zu erhalten und Leistungsprobleme zu identifizieren.


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

Das Dashboard besteht aus den folgenden Funktionen:

1. Zeigen Sie historische Daten mithilfe von Zeit- und Datumsbereichskontrollen an.
2. Fügen Sie den CloudWatch benutzerdefinierten Dashboards eine benutzerdefinierte Dashboard-Ansicht hinzu.
3. Überwachen Sie den Gesamtzustand und den Auslastungsstatus Ihrer WorkSpaces wie folgt:
    a. Zeigen Sie die Gesamtzahl der bereitgestellten WorkSpaces, die Anzahl der verbundenen Benutzer, die Anzahl der fehlerhaften und WorkSpace fehlerfreien Instances an.
    b. Zeigen Sie fehlerhafte WorkSpaces und ihre verschiedenen Variablen an, z. B. Protokoll und Datenverarbeitungsmodus.
    c. Bewegen Sie den Mauszeiger über das Liniendiagramm, um die Anzahl der fehlerfreien oder WorkSpace fehlerhaften Instances für ein bestimmtes Protokoll und den Ausführungsmodus über einen bestimmten Zeitraum anzuzeigen.
    d. Wählen Sie das Ellipsenmenü und dann In Metriken anzeigen aus, um die Metriken in einem Zeitskalierungsdiagramm anzuzeigen.
4. Zeigen Sie Ihre Verbindungsmetriken und ihre verschiedenen Variablen an, z. B. die Anzahl der Verbindungsversuche, erfolgreiche Verbindungen und fehlgeschlagene Verbindungen in Ihrer WorkSpaces Umgebung zu einem bestimmten Zeitpunkt.
5. Zeigen Sie InSession Latenzen an, die sich auf die Benutzererfahrung auswirken, z. B. Round Trip Time (RTT), um den Verbindungsstatus und den Paketverlust zur Überwachung des Netzwerkzustands zu ermitteln.
6. Zeigen Sie die Host-Leistung und die Ressourcenauslastung an, um potenzielle Leistungsprobleme zu identifizieren und zu beheben.

Überwachen Sie Ihre WorkSpaces mithilfe von CloudWatch Metriken

WorkSpaces und Amazon CloudWatch sind integriert, sodass Sie Leistungsmetriken sammeln und analysieren können. Sie können diese Metriken über die CloudWatch Konsole, die CloudWatch Befehlszeilenschnittstelle oder programmgesteuert über die CloudWatch -API überwachen. Mit können Sie CloudWatch auch Alarme festlegen, wenn Sie einen bestimmten Schwellenwert für eine Metrik erreichen.

Weitere Informationen zur Verwendung von - CloudWatch und -Alarmen finden Sie im Amazon CloudWatch -Benutzerhandbuch.

Voraussetzungen

Um CloudWatch Metriken zu erhalten, aktivieren Sie den Zugriff auf Port 443 für die `AMAZON` Teilmenge in der `us-east-1` Region. Weitere Informationen finden Sie unter IP-Adresse und Port-Anforderungen für WorkSpaces.

Inhalt

WorkSpaces -Metriken

Der `AWS/WorkSpaces`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten

`Available` [1]	Die Anzahl der WorkSpaces , die einen fehlerfreien Status zurückgegeben haben.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

`Unhealthy` [1]	Die Anzahl der WorkSpaces , die einen fehlerhaften Status zurückgegeben haben.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
		`ComputeType` `BundleId`		

`ConnectionAttempt` [2]	Die Anzahl der Verbindungsversuche.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

`ConnectionSuccess` [2]	Die Anzahl der erfolgreichen Verbindungen.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

`ConnectionFailure` [2]	Die Anzahl der fehlgeschlagenen Verbindungen.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
SessionLaunchTime [2,6]	Die Zeit, die zum Initiieren einer WorkSpaces Sitzung benötigt wird.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Sekunde (Zeit)
InSessionLatency [2,6]	Die Round-Trip-Zeit zwischen dem WorkSpaces Client und der WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Millisekunde (Zeit)
SessionDisconnect [2,6]	Die Anzahl der beendeten Verbindungen, einschließlich vom Benutzer initiierter und fehlgeschlagener Verbindungen.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten

`UserConnected` [3]	Die Anzahl der WorkSpaces , für die ein Benutzer verbunden ist.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

`Stopped`	Die Anzahl der WorkSpaces , die gestoppt werden.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

`Maintenance` [4]	Die Anzahl der WorkSpaces , die gewartet werden.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
TrustedDeviceValidationAttempt [5,6]	Die Anzahl der Versuche zur Überprüfung der Signatur der Geräteauthentifizierung.	DirectoryId	Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl
TrustedDeviceValidationSuccess [5,6]	Die Anzahl der erfolgreichen Versuche zur Überprüfung der Signatur der Geräteauthentifizierung.	DirectoryId	Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl
TrustedDeviceValidationFailure [5,6]	Die Anzahl der fehlgeschlagen Versuche zur Überprüfung der Signatur der Geräteauthentifizierung.	DirectoryId	Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl
TrustedDeviceCertificateDaysBeforeExpiration [6]	Verbleibende Tage, bis das dem Verzeichnis zugeordnete Stammzertifikat abgelaufen ist.	CertificateId	Durchschnitt, Summe, Maximum, Minimum, Datenstichproben	Anzahl

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten

`CPUUsage`	Der Prozentsatz der verwendeten CPU-Ressource.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Maximum, Minimum	Prozentsatz

`MemoryUsage`	Der Prozentsatz des verwendeten Maschinenspeichers.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Maximum, Minimum	Prozentsatz

`RootVolumeDiskUsage`	Der Prozentsatz des verwendeten Root-Datenträger-Volumes.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Durchschnitt, Maximum, Minimum	Prozentsatz

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
UserVolumeDiskUsage	Der Prozentsatz des verwendeten Benutzerdatenträger-Volumes.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Durchschnitt, Maximum, Minimum	Prozentsatz
UDPPacketLossRate [7]	Der Prozentsatz der Pakete, die zwischen dem Client und dem Gateway verworfen wurden.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Durchschnitt, Maximum, Minimum, Datenbeispiele	Prozentsatz
UpTime	Die Zeit seit dem letzten Neustart eines WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Durchschnitt, Maximum, Minimum, Datenbeispiele	Sekunden

[1] WorkSpaces Sendet regelmäßig Statusanforderungen an einen WorkSpace. Ein WorkSpace wird markiert, `Available` wenn er auf diese Anfragen antwortet und `Unhealthy` wenn er nicht auf diese

Anfragen reagiert. Diese Metriken stehen pro WorkSpace Granularität zur Verfügung und werden auch für alle WorkSpaces in einer Organisation aggregiert.

[2] WorkSpaces zeichnet Metriken zu Verbindungen auf, die mit jedem hergestellt wurden WorkSpace. Diese Metriken werden ausgegeben, nachdem sich ein Benutzer erfolgreich über den WorkSpaces Client authentifiziert hat und der Client dann eine Sitzung initiiert. Die Metriken sind pro Granularität WorkSpace verfügbar und werden auch für alle WorkSpaces in einem Verzeichnis aggregiert.

[3] WorkSpaces Sendet regelmäßig Verbindungsstatusanfragen an einen WorkSpace. Benutzer werden als verbunden gemeldet, wenn sie ihre Sitzungen aktiv nutzen. Diese Metrik ist pro WorkSpace Granularität verfügbar und wird auch für alle WorkSpaces in einer Organisation aggregiert.

[4] Diese Metrik gilt für WorkSpaces , die mit einem AutoStop Ausführungsmodus konfiguriert sind. Wenn Sie die Wartung für Ihr aktiviert haben WorkSpaces, erfasst diese Metrik die Anzahl der WorkSpaces , die derzeit gewartet werden. Diese Metrik ist pro WorkSpace Granularität verfügbar, die beschreibt, wann eine in Betrieb WorkSpace genommen wurde und wann sie entfernt wurde.

[5] Wenn die Funktion für vertrauenswürdige Geräte für das Verzeichnis aktiviert ist, WorkSpaces verwendet Amazon die zertifikatbasierte Authentifizierung, um festzustellen, ob ein Gerät vertrauenswürdig ist. Wenn Benutzer versuchen, auf ihr zuzugreifen WorkSpaces, werden diese Metriken ausgegeben, um eine erfolgreiche oder fehlgeschlagene vertrauenswürdige Geräteauthentifizierung anzuzeigen. Diese Metriken sind auf Verzeichnisebene granular und nur für die Amazon WorkSpaces -Windows- und macOS-Clientanwendungen verfügbar.

[6] In WorkSpaces Web Access nicht verfügbar.

[7] Diese Metrik misst den durchschnittlichen Paketverlust.

- Auf PCoIP : Misst den durchschnittlichen Paketverlust am Gateway vom Client.
- Auf WSP: Misst den durchschnittlichen Paketverlust vom Client zum Gateway.

Dimensionen für WorkSpaces Metriken

Verwenden Sie die nachstehenden Dimensionen, um die Metrikdaten zu filtern.

Dimension	Beschreibung
`DirectoryId`	Filtert die Metrikdaten nach im WorkSpaces angegebenen Verzeichnis. Das Format der Verzeichnis-ID ist `d-XXXXXXXXXX` .
`WorkspaceId`	Filtert die Metrikdaten nach dem angegebenen WorkSpace. Das Format der WorkSpace ID ist `ws-XXXXXXXXXX` .
`CertificateId`	Filtert die Metrikdaten nach dem angegeben en Stammzertifikat, das dem Verzeichnis zugeordnet ist. Das Format der Zertifikat-ID ist `wsc-XXXXXXXXX` .
`RunningMode`	Filtert die Metrikdaten nach WorkSpaces ihrem Ausführungsmodus. Die Form des Ausführun gsmodus ist AutoStop oder AlwaysOn.
`BundleId`	Filtert die Metrikdaten nach dem WorkSpace s Protokoll. Das Format des Pakets ist `wsb-XXXXXXXXXX` .
`ComputeType`	Filtert die Metrikdaten WorkSpaces nach dem Datenverarbeitungstyp.

Beispiel für die Überwachung

Das folgende Beispiel zeigt, wie Sie die verwenden können, AWS CLI um auf einen CloudWatch Alarm zu reagieren und festzustellen, bei welchen WorkSpaces in einem Verzeichnis Verbindungsfehler aufgetreten sind.

So reagieren Sie auf einen CloudWatch Alarm

1. Bestimmen Sie, auf welches Verzeichnis sich der Alarm bezieht, indem Sie den Befehl describe-alarms verwenden.

```
aws cloudwatch describe-alarms --state-value "ALARM"
```

```
{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. Rufen Sie die Liste der WorkSpaces im angegebenen Verzeichnis mit dem Befehl describe-workspaces ab.

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. Rufen Sie die CloudWatch Metriken für jeden WorkSpace im Verzeichnis mit dem get-metric-statistics Befehl ab.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Überwachen Sie Ihre WorkSpaces Nutzung von Amazon EventBridge

Sie können Ereignisse von Amazon verwenden, WorkSpaces um erfolgreiche Anmeldungen bei Ihrem WorkSpaces anzusehen, zu suchen, herunterzuladen, zu archivieren, zu analysieren und auf erfolgreiche Anmeldungen zu reagieren. Sie können Ereignisse beispielsweise für folgende Zwecke verwenden:

- Speichern oder archivieren WorkSpaces Sie Anmeldeereignisse als Protokolle zur future Verwendung, analysieren Sie die Protokolle, um nach Mustern zu suchen, und ergreifen Sie auf der Grundlage dieser Muster Maßnahmen.

- Ermitteln Sie anhand der WAN-IP-Adresse, von wo aus Benutzer angemeldet sind, und verwenden Sie dann Richtlinien, um Benutzern nur Zugriff auf Dateien oder Daten zu gewähren WorkSpaces , die den Zugriffskriterien für den Ereignistyp entsprechen`WorkSpaces Access`.
- Analysieren Sie Anmeldedaten und führen Sie automatisierte Aktionen durch mit AWS Lambda.
- Verwenden Sie Richtlinien-Steuerelemente, um den Zugriff auf Dateien und Anwendungen von nicht autorisierten IP-Adressen zu blockieren.
- Finden Sie heraus, mit welcher WorkSpaces Client-Version eine Verbindung hergestellt wurde WorkSpaces.

Amazon WorkSpaces sendet diese Ereignisse nach bestem Wissen und Gewissen. Ereignisse werden nahezu EventBridge in Echtzeit zugestellt. Mit EventBridge können Sie Regeln erstellen, die als Reaktion auf ein Ereignis programmgesteuerte Aktionen auslösen. Sie können beispielsweise eine Regel konfigurieren, die ein SNS-Thema aufruft, um eine E-Mail-Benachrichtigung zu senden, oder eine Lambda-Funktion aufruft, um eine Aktion auszuführen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

WorkSpaces Auf Ereignisse zugreifen

WorkSpaces Clientanwendungen senden `WorkSpaces Access` Ereignisse, wenn sich ein Benutzer erfolgreich bei a anmeldet WorkSpace. Alle WorkSpaces Clients senden diese Ereignisse.

Für Ereignisse, die WorkSpaces mithilfe des WorkSpaces Streaming Protocol (WSP) ausgelöst werden, ist die Version 4.0.1 oder höher der WorkSpaces Client-Anwendung erforderlich.

Ereignisse werden als JSON-Objekte dargestellt. Im Folgenden finden Sie Beispieldaten für ein `WorkSpaces Access`-Ereignis.

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
```

```
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```


Ereignisspezifische Felder

`clientIpAddress`

Die WAN-IP-Adresse der Clientanwendung. Für PCoIP-Zero-Clients ist dies die IP-Adresse des Teradici auth-Clients.

`actionType`

Dieser Wert ist immer `successfulLogin`.

`workspacesClientProductName`

Bei den Werden muss die Groß- und Kleinschreibung beachtet werden.

- `WorkSpaces Desktop client` – Windows-, macOS- und Linux-Clients
- `Amazon WorkSpaces Mobile client` – iOS-Client
- `WorkSpaces Mobile Client` – Android-Clients
- `WorkSpaces Chrome Client` – Chromebook-Client
- `WorkSpacesWebClient` – Web-Access-Client
- `AmazonWorkSpacesThinClient`— Amazon WorkSpaces Thin Client-Gerät
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` – Zero-Client

`loginTime`

Der Zeitpunkt, zu dem sich der Benutzer bei der angemeldet hat WorkSpace.

`clientPlatform`

- `Android`
- `Chrome`

- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

Die Kennung des Verzeichnisses für die WorkSpace. Sie müssen der Verzeichnis-ID `domain/` voranstellen. z. B. `"domain/d-123456789"`.

`clientVersion`

Die Client-Version, mit der die Verbindung hergestellt wurde WorkSpaces.

`workspaceId`

Die Kennung des WorkSpace.

Erstellen Sie eine Regel zur Behandlung von WorkSpaces Ereignissen

Gehen Sie wie folgt vor, um eine Regel für die Behandlung der WorkSpaces Ereignisse zu erstellen.

Voraussetzung

Erstellen Sie ein Amazon-Simple-Notification-Service-Thema, um E-Mail-Benachrichtigungen zu erhalten.

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie Thema erstellen aus.
4. Wählen Sie unter Type (Typ) die Option Standard aus.
5. Geben Sie unter Name einen Namen für Ihr Thema ein.
6. Wählen Sie Thema erstellen aus.
7. Wählen Sie Create subscription (Abonnement erstellen) aus.
8. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.

9. Geben Sie unter Endpoint (Endpunkt) die E-Mail-Adresse ein, an die die Benachrichtigungen gesendet werden sollen.
10. Wählen Sie Create subscription (Abonnement erstellen) aus.
11. Sie erhalten eine E-Mail-Nachricht mit der folgenden Betreffzeile: AWS Notification - Subscription Confirmation. Befolgen Sie die Anweisungen, um Ihr Abonnement zu bestätigen.

Um eine Regel zur Behandlung von WorkSpaces Ereignissen zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Geben Sie unter Name einen Namen für Ihre Regel ein.
4. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
5. Wählen Sie Weiter aus.
6. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:
   a. Wählen Sie für Ereignisquelle die Option AWS-Services aus.
   b. Wählen Sie für AWS-Service WorkSpaces aus.
   c. Wählen Sie als Ereignistyp die Option WorkSpacesAccess aus.
   d. Standardmäßig senden wir Benachrichtigungen für jedes Ereignis. Wenn Sie möchten, können Sie ein Ereignismuster erstellen, das Ereignisse für bestimmte Clients oder WorkSpaces filtert.
7. Wählen Sie Weiter aus.
8. Geben Sie ein Ziel wie folgt an:
   a. Für Target types (Zieltypen), wählen Sie AWS-Service aus.
   b. Für Select a target (Wählen Sie ein Ziel aus), wählen Sie SNS-Thema aus.
   c. Wählen Sie für Benachrichtigungs-ARN den ARN für das SNS-Thema aus, das Sie für Benachrichtigungen erstellt haben.
9. Wählen Sie Weiter aus.
10. (Optional) Fügen Sie Ihrer Regel Tags hinzu.
11. Wählen Sie Weiter aus.
12. Wählen Sie Regel erstellen aus.

AWS-Anmeldeereignisse für Smartcard-Benutzer

AWS CloudTrail protokolliert erfolgreiche und erfolglose Anmeldeereignisse für Smartcard-Benutzer. Dazu gehören Anmeldeereignisse, die jedes Mal erfasst werden, wenn ein Benutzer aufgefordert wird, eine Anmeldeinformation oder bestimmte Faktoren zu lösen, sowie der Status dieser speziellen Anforderung zur Überprüfung der Anmeldeinformationen. Die Benutzer werden erst angemeldet, nachdem Sie alle erforderlichen Anmeldeinformationen bereitstellt haben, was dazu führt, dass ein `UserAuthentication`-Ereignis protokolliert wird.

In der folgenden Tabelle sind die Namen der CloudTrail-Anmeldeereignisse und ihre Zwecke aufgeführt.

Event name (Ereignis name)	Zweck des Ereignisses
`CredentialChallenge`	Benachrichtigt, dass der Benutzer bei der AWS-Anmeldung aufgefordert wurde, eine bestimmte Anmeldeinformation anzugeben, und gibt den `CredentialType` an, der erforderlich ist (z. B. SMARTCARD).
`CredentialVerification`	Benachrichtigt, dass der Benutzer versucht hat, eine bestimmte `CredentialChallenge` -Anfrage zu lösen, und gibt an, ob die Anmeldeinformationen erfolgreich waren oder nicht.
`UserAuthentication`	Benachrichtigt, dass alle Authentifizierungsanforderungen, mit denen der Benutzer konfrontiert wurde, erfolgreich erfüllt wurden und dass der Benutzer erfolgreich angemeldet wurde. Wenn Benutzer die erforderlichen Anmeldeinformationen nicht erfolgreich abschließen können, wird kein `UserAuthentication` -Ereignis protokolliert.

In der folgenden Tabelle werden zusätzliche nützliche Ereignisdatenfelder erfasst, die in bestimmten CloudTrail-Anmeldeereignissen enthalten sind.

Event name (Ereignis name)	Zweck des Ereignisses	Anwendbarkeit des Anmeldeereignisses	Beispielwerte
`AuthWorkflowID`	Korreliert alle Ereignisse, die während einer gesamten Anmeldesequenz ausgelöst wurden. Bei jeder Benutzeranmeldung können bei der AWS-Anmeldung mehrere Ereignisse ausgelöst werden.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	Benachrichtigt, dass der Benutzer versucht hat, eine bestimmte `CredentialChallenge` -Anfrage zu lösen, und gibt an, ob die Anmeldeinformationen erfolgreich waren oder nicht.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType“: „SMARTCARD“ (mögliche Werte heute: SMARTCARD)
`LoginTo`	Benachrichtigt, dass alle Authentifizierungsanforderungen, mit denen der Benutzer konfrontiert wurde, erfolgreich erfüllt wurden und dass der Benutzer erfolgreich angemeldet wurde. Wenn Benutzer die erforderlichen Anmeldeinformationen nicht erfolgreich abschließen können, wird kein `UserAuthe`	`UserAuthentication`	„LoginTo“: „https://skylight.local“

Event name (Ereignis name)	Zweck des Ereignisses	Anwendbarkeit des Anmeldeereignisses	Beispielwerte
	`ntication` -Ereignis protokolliert.		

Beispielereignisse für AWS-Anmeldeszenarien

Die folgenden Beispiele stellen die erwartete Reihenfolge von CloudTrail-Ereignissen für verschiedene Anmeldeszenarien dar.

Inhalt

Erfolgreiche Anmeldung bei der Authentifizierung mit Smartcard

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine erfolgreiche Smartcard-Anmeldung.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```


Erfolgreich CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
```

```
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
}
```

Erfolgreich UserAuthentication

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
```

```
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

Erfolgreiche Anmeldung bei der Authentifizierung nur mit Smartcard

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine fehlgeschlagene Smartcard-Anmeldung.

CredentialChallenge

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
```

```
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```


Fehlgeschlagen CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
```

```
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

Geschäftskontinuität für Amazon WorkSpaces

Amazon WorkSpaces baut auf der AWS globalen -Infrastruktur auf, die in AWS Regionen und Availability Zones organisiert ist. Diese Regionen und Availability Zones bieten Stabilität sowohl in Bezug auf die physische Isolierung als auch auf die Datenredundanz. Weitere Informationen finden Sie unter Ausfallsicherheit in Amazon WorkSpaces.

Amazon bietet WorkSpaces auch eine regionsübergreifende Umleitung, eine Funktion, die mit Ihren DNS-Routing-Richtlinien (Domain Name System) funktioniert, um Ihre WorkSpaces Benutzer auf eine Alternative umzuleiten, WorkSpaces wenn ihre primären nicht verfügbar WorkSpaces sind. Durch die Verwendung von DNS-Failover-Routing-Richtlinien können Sie Ihre Benutzer beispielsweise mit WorkSpaces in der von Ihnen angegebenen Failover-Region verbinden, wenn sie nicht auf ihre WorkSpaces in der primären Region zugreifen können.

Sie können die regionsübergreifende Umleitung verwenden, um eine regionale Stabilität und hohe Verfügbarkeit zu erreichen. Sie können sie auch für andere Zwecke verwenden, z. B. für die Verteilung des Datenverkehrs oder für die Bereitstellung von Alternativen WorkSpaces während der Wartungszeiträume. Wenn Sie Amazon Route 53 für Ihre DNS-Konfiguration verwenden, können Sie Zustandsprüfungen nutzen, die Amazon- CloudWatch Alarme überwachen.

Amazon WorkSpaces Multi-Region Resilience bietet eine automatisierte, redundante virtuelle Desktop-Infrastruktur in einer sekundären WorkSpace Region und optimiert den Prozess der Umleitung von Benutzern in die sekundäre Region, wenn die primäre Region aufgrund von Ausfällen nicht erreichbar ist.

Sie können WorkSpaces Multi-Region Resilience mit regionsübergreifender Umleitung verwenden, um redundante virtuelle Desktop-Infrastruktur in einer sekundären WorkSpace Region bereitzustellen und eine regionsübergreifende Failover-Strategie zur Vorbereitung auf störende Ereignisse zu entwerfen. Sie können diese Lösung auch für andere Zwecke verwenden, z. B. für die Verteilung des Datenverkehrs oder für die Bereitstellung einer Alternative WorkSpaces während der Wartungszeiträume. Wenn Sie Route 53 für Ihre DNS-Konfiguration verwenden, können Sie Zustandsprüfungen nutzen, die CloudWatch Alarme überwachen.

Inhalt

Regionsübergreifende Umleitung für Amazon WorkSpaces

Mit der Funktion zur WorkSpacesregionsübergreifenden Umleitung in Amazon können Sie einen vollqualifizierten Domainnamen (FQDN) als Registrierungscode für Ihr verwenden WorkSpaces. Die regionsübergreifende Umleitung funktioniert mit Ihren DNS-Routing-Richtlinien (Domain Name System), um Ihre WorkSpaces Benutzer auf eine Alternative umzuleiten WorkSpaces , wenn ihre primären nicht verfügbar WorkSpaces sind. Mithilfe von DNS-Failover-Routing-Richtlinien können Sie beispielsweise Ihre Benutzer mit WorkSpaces in der von Ihnen angegebenen Failover-AWSRegion verbinden, wenn sie nicht auf ihre WorkSpaces in der primären Region zugreifen können.

Sie können die regionsübergreifende Umleitung zusammen mit Ihren DNS-Failover-Routingrichtlinien verwenden, um regionale Stabilität und hohe Verfügbarkeit zu erreichen. Sie können diese Funktion auch für andere Zwecke verwenden, z. B. für die Verteilung des Datenverkehrs oder für die Bereitstellung von Alternativen WorkSpaces während der Wartungszeiträume. Wenn Sie Amazon Route 53 für Ihre DNS-Konfiguration verwenden, können Sie Zustandsprüfungen nutzen, die Amazon- CloudWatch Alarme überwachen.

Um diese Funktion verwenden zu können, müssen Sie WorkSpaces für Ihre Benutzer in zwei (oder mehr) AWS Regionen einrichten. Sie müssen ebenfalls spezielle, FQDN-basierte Registrierungscodes erstellen, auch Verbindungsaliase genannt. Diese Verbindungsaliase ersetzen regionsspezifische Registrierungscodes für Ihre WorkSpaces Benutzer. (Die regionsspezifischen Registrierungscodes bleiben gültig. Damit die regionsübergreifende Umleitung funktioniert, müssen Ihre Benutzer jedoch stattdessen den FQDN als ihren Registrierungscode verwenden.)

Geben Sie zur Erstellung eines Verbindungsalias eine Verbindungszeichenfolge an, bei der es sich um einen FQDN handelt, z. B. `www.example.com` oder `desktop.example.com`. Sie müssen ihn bei einem Domain-Registrar registrieren und den DNS-Service für Ihre Domain konfigurieren, um diese Domain für die regionsübergreifende Umleitung zu verwenden.

Nachdem Sie Ihre Verbindungsaliase erstellt haben, verknüpfen Sie sie mit Ihren WorkSpaces Verzeichnissen in verschiedenen Regionen, um Zuordnungspaare zu erstellen. Jedes Zuordnungspaar verfügt über eine primäre Region und eine oder mehrere Failover-Regionen. Wenn in der primären Region ein Ausfall auftritt, leiten Ihre DNS-Failover-Routing-Richtlinien Ihre WorkSpaces Benutzer an die weiter WorkSpaces , die Sie für sie in der Failover-Region eingerichtet haben.

Definieren Sie bei der Konfiguration Ihrer DNS-Failover-Routing-Richtlinien die Regionspriorität (entweder primär oder sekundär), um Ihre primären Regionen und Ihre Failover-Regionen festzulegen.

Inhalt

Voraussetzungen

- Sie müssen Besitzer der Domain sein, die Sie als FQDN in Ihren Verbindungsaliasnamen verwenden möchten. Sie müssen sie außerdem registrieren. Wenn Sie noch keinen anderen Domain-Registrar verwenden, können Sie Amazon Route 53 verwenden, um Ihre Domain zu registrieren. Weitere Informationen finden Sie unter Registrieren von Domain-Namen mithilfe von Amazon Route 53 im Entwicklerhandbuch für Amazon Route 53.

> **Important**
>
> Sie müssen über alle erforderlichen Rechte verfügen, um jeden Domainnamen zu verwenden, den Sie in Verbindung mit Amazon verwenden WorkSpaces. Sie erklären sich damit einverstanden, dass der Domainname keine gesetzlichen Rechte Dritter verletzt oder anderweitig gegen geltendes Recht verstößt.

Die Gesamtlänge Ihres Domainnamens darf 255 Zeichen nicht überschreiten. Weitere Informationen zu Domainnamen finden Sie unter DNS-Domainnamenformat im Amazon-Route 53-Entwicklerhandbuch.

Die regionsübergreifende Umleitung funktioniert sowohl mit öffentlichen Domainnamen als auch mit Domainnamen in privaten DNS-Zonen. Wenn Sie eine private DNS-Zone verwenden, müssen Sie eine VPN-Verbindung (Virtual Private Network) zur Virtual Private Cloud (VPC) bereitstellen, die Ihre enthält WorkSpaces. Wenn Ihre WorkSpaces Benutzer versuchen, einen privaten FQDN aus dem öffentlichen Internet zu verwenden, geben die WorkSpaces Client-Anwendungen die folgende Fehlermeldung zurück:

```
"We're unable to register the WorkSpace because of a DNS server issue.
Contact your administrator for help."
```

- Sie müssen Ihren DNS-Service einrichten und die erforderlichen DNS-Routing-Richtlinien konfigurieren. Die regionsübergreifende Umleitung funktioniert in Verbindung mit Ihren DNS-Routing-Richtlinien, um Ihre WorkSpaces Benutzer nach Bedarf umzuleiten.
- Erstellen Sie in jeder primären und Failover-Region, in der Sie eine regionsübergreifende Umleitung einrichten möchten, WorkSpaces für Ihre Benutzer. Stellen Sie sicher, dass Sie in jedem WorkSpaces Verzeichnis in jeder Region dieselben Benutzernamen verwenden. Um Ihre Active-Directory-Benutzerdaten synchron zu halten, empfehlen wir, AD Connector zu verwenden, um in jeder Region, in der Sie WorkSpaces für Ihre Benutzer eingerichtet haben, auf dasselbe Active Directory zu verweisen. Weitere Informationen zum Erstellen von WorkSpacesfinden Sie unter Starten von WorkSpaces.

> **Important**
>
> Wenn Sie Ihr Verzeichnis in AWS Managed Microsoft AD für die Replikation in mehreren Regionen konfigurieren, kann nur das Verzeichnis in der primären Region für die Verwendung mit Amazon registriert werden WorkSpaces. Versuche, das Verzeichnis in einer replizierten Region für die Verwendung mit Amazon zu registrieren WorkSpaces , schlagen fehl. Die Multi-Region-Replikation mit AWS Managed Microsoft AD wird für die Verwendung mit Amazon WorkSpaces in replizierten Regionen nicht unterstützt.

Wenn Sie mit der Einrichtung der regionsübergreifenden Umleitung fertig sind, müssen Sie sicherstellen, dass Ihre WorkSpaces Benutzer den FQDN-basierten Registrierungscode anstelle

des regionsbasierten Registrierungscodes (z. B. `WSpdx+ABC12D`) für ihre primäre Region verwenden. Dazu müssen Sie ihnen eine E-Mail mit der FQDN-Verbindungszeichenfolge senden, indem Sie das Verfahren unter Schritt 5: Senden der Verbindungszeichenfolge an Ihre WorkSpaces Benutzer verwenden.

> **Note**
>
> Wenn Sie Ihre Benutzer in der WorkSpaces Konsole erstellen, anstatt sie in Active Directory zu erstellen, sendet WorkSpaces automatisch eine Einladungs-E-Mail mit einem regionsbasierten Registrierungscode an Ihre Benutzer, wenn Sie ein neues starten WorkSpace. Das bedeutet, dass Ihre Benutzer bei der Einrichtung WorkSpaces für Ihre Benutzer in der Failover-Region auch automatisch E-Mails für diese Failover- erhalten WorkSpaces. Sie müssen Ihre Benutzer anweisen, E-Mails mit regionalen Registrierungscodes zu ignorieren.

Einschränkungen

- Die regionsübergreifende Umleitung überprüft nicht automatisch, ob Verbindungen zur primären Region fehlgeschlagen sind, und WorkSpaces führt dann ein Failover Ihrer zu einer anderen Region durch. Anders ausgedrückt: Ein automatisches Failover findet nicht statt.

  Sie müssen einen anderen Mechanismus in Verbindung mit der regionsübergreifenden Umleitung verwenden, um ein automatisches Failover-Szenario zu implementieren. Sie können beispielsweise eine Amazon Route 53 Failover DNS-Routing-Richtlinie in Kombination mit einer Route 53-Zustandsprüfung verwenden, die einen CloudWatch Alarm in der primären Region überwacht. Wenn der CloudWatch Alarm in der primären Region ausgelöst wird, leitet Ihre DNS-Failover-Routing-Richtlinie Ihre WorkSpaces Benutzer an die weiter WorkSpaces , die Sie für sie in der Failover-Region eingerichtet haben.
- Wenn Sie die regionsübergreifende Umleitung verwenden, werden Benutzerdaten zwischen WorkSpaces in verschiedenen Regionen nicht beibehalten. Um sicherzustellen, dass Benutzer aus verschiedenen Regionen auf ihre Dateien zugreifen können, empfehlen wir Ihnen, Amazon WorkDocs für Ihre WorkSpaces Benutzer einzurichten, sofern Amazon in Ihren primären Regionen und Failover-Regionen unterstützt WorkDocs wird. Weitere Informationen zu Amazon WorkDocsfinden Sie unter Amazon WorkDocs Drive im Amazon- WorkDocs Administratorhandbuch. Weitere Informationen zum Aktivieren von Amazon WorkDocs für Ihre WorkSpace Benutzer finden Sie unter Registrieren eines dedizierten Verzeichnisses

für WorkSpaces und Aktivieren von Amazon WorkDocs für AWS Managed Microsoft AD. Informationen darüber, wie WorkSpaces Benutzer Amazon WorkDocs auf ihren einrichten können WorkSpaces, finden Sie unter Integrieren mit WorkDocs im Amazon- WorkSpaces Benutzerhandbuch.

- Die regionsübergreifende Umleitung wird nur auf Version 3.0.9 oder höher der Linux-, macOS- und Windows- WorkSpaces Clientanwendungen unterstützt. Sie können die regionsübergreifende Umleitung auch mit Web Access verwenden.
- Die regionsübergreifende Umleitung ist in allen AWS Regionen verfügbar, in denen Amazon verfügbar WorkSpaces ist, mit Ausnahme der Regionen AWS GovCloud (US) Regionen und China (Ningxia).

Schritt 1: Erstellen von Verbindungsaliasen

Erstellen Sie mit demselben AWS-Konto Verbindungsaliase in jeder primären und Failover-Region, in der Sie die regionsübergreifende Umleitung einrichten möchten.

So stellen Sie einen Verbindungsalias her

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie in der oberen rechten Ecke der Konsole die primäre AWS Region für Ihre aus WorkSpaces.
3. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
4. Wählen Sie unter Regionsübergreifende Umleitung die Option Verbindungsalias erstellen aus.
5. Geben Sie als Verbindungszeichenfolge einen vollqualifizierten Domain-Namen ein, (z. B. `www.example.com` oder `desktop.example.com`). Eine Verbindungszeichenfolge darf maximal 255 Zeichen lang sein. Sie darf nur Buchstaben (A–Z und a–z), Ziffern (0–9) und die folgenden Zeichen enthalten: .-

> **Important**
>
> Nachdem Sie eine Verbindungszeichenfolge erstellt haben, ist diese immer mit Ihrem AWS-Konto verknüpft. Eine Verbindungszeichenfolge kann nicht mit einem anderen Konto erneut erstellt werden, selbst wenn Sie alle Instances aus dem ursprünglichen Konto gelöscht haben. Die Verbindungszeichenfolge ist global für Ihr Konto reserviert.

6. (Optional) Geben Sie unter Tags alle Tags an, die Sie Ihrem Verbindungsalias zuordnen möchten.
7. Wählen Sie Verbindung erstellen aus.
8. Wiederholen Sie diese Schritte, aber stellen Sie sicherStep 2, dass Sie in die Failover-Region für Ihr auswählen WorkSpaces. Wenn Sie über mehr als eine Failover-Region verfügen, wiederholen Sie diese Schritte für jede Failover-Region. Achten Sie darauf, in allen Failover-Regionen dasselbe AWS-Konto für die Erstellung des Verbindungsalias zu verwenden.

(Optional) Schritt 2: Teilen eines Verbindungsalias mit einem anderen Konto

Sie können einen Verbindungsalias für ein anderes AWS-Konto in derselben AWS-Region freigeben. Bei Freigabe eines Verbindungsalias für ein anderes Konto kann dieses Konto nur dann den Alias einem seiner Verzeichnisse zuordnen oder eine Zuordnung aufheben, wenn es sich in derselben Region befindet. Nur das Konto, das den Verbindungsalias besitzt, kann den Alias löschen.

> **Note**
>
> Ein Verbindungsalias kann nur einem Verzeichnis pro AWS-Region zugeordnet werden. Wenn Sie einen Verbindungsalias für ein anderes AWS-Konto freigeben, kann der Alias nur von einem Konto (Ihrem Konto oder dem freigegebenen Konto) einem Verzeichnis in dieser Region zugeordnet werden.

So teilen Sie einen Verbindungsalias mit einem anderen AWS-Konto

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie oben rechts in der Konsole die AWS-Region aus, in der Sie den Verbindungsalias für ein anderes AWS-Konto teilen möchten.
3. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
4. Wählen Sie unter Regionsübergreifende Umleitungszuordnungen die Verbindungszeichenfolge aus und wählen Sie dann Aktionen, Verbindungsalias freigeben/Freigabe aufheben aus.

   Sie können einen Alias auch auf der Detailseite des Verbindungsalias teilen. Wählen Sie dazu unter Freigegebenes Konto die Option Verbindungsalias freigeben aus.

5. Geben Sie auf der Seite Verbindungsalias freigeben/Freigabe aufheben unter Für ein Konto freigeben die AWS-Konto-ID ein, mit der Sie Ihren Verbindungsalias in dieser Region teilen möchten. AWS
6. Wählen Sie Freigeben.

Schritt 3: Verknüpfen von Verbindungsaliasen mit Verzeichnissen in jeder Region

Wenn Sie denselben Verbindungsalias einem WorkSpaces Verzeichnis in zwei oder mehr Regionen zuordnen, wird ein Zuordnungspaar zwischen den Verzeichnissen erstellt. Jedes Zuordnungspaar verfügt über eine primäre Region und eine oder mehrere Failover-Regionen.

Wenn Ihre primäre Region beispielsweise die Region USA West (Oregon) ist, können Sie Ihr WorkSpaces Verzeichnis in der Region USA West (Oregon) mit einem WorkSpaces Verzeichnis in der Region USA Ost (Nord-Virginia) verbinden. Wenn in der primären Region ein Ausfall auftritt, funktioniert die regionsübergreifende Umleitung in Verbindung mit Ihren DNS-Failover-Routing-Richtlinien und allen Zustandsprüfungen, die Sie in der Region USA West (Oregon) eingerichtet haben, um Ihre Benutzer an die umzuleiten, die WorkSpaces Sie für sie in der Region USA Ost (Nord-Virginia) eingerichtet haben. Weitere Informationen zu regionsübergreifenden Umleitungen finden Sie unter Was passiert bei der regionsübergreifenden Umleitung?.

> **Note**
>
> Wenn sich Ihre WorkSpaces Benutzer in einer erheblichen Entfernung von der Failover-Region befinden (z. B. Tausende von Kilometern entfernt), reagiert ihre WorkSpaces Erfahrung möglicherweise weniger als gewöhnlich. Um die Round-Trip-Zeit (RTT) zu den verschiedenen -AWSRegionen von Ihrem Standort aus zu überprüfen, verwenden Sie die Zustandsprüfung von Amazon WorkSpaces Connection .

So ordnen Sie einem Verzeichnis einen Verbindungsalias zu

Sie können nur einem Verzeichnis pro AWS-Region einen Verbindungsalias zuordnen. Wenn Sie einen Verbindungsalias für ein anderes AWS-Konto freigegeben haben, kann der Alias nur über ein Konto (Ihr Konto oder das freigegebene Konto) einem Verzeichnis in dieser Region zugeordnet werden.

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.

2. Wählen Sie in der oberen rechten Ecke der Konsole die primäre AWS Region für Ihre aus WorkSpaces.
3. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
4. Wählen Sie unter Regionsübergreifende Umleitungszuordnungen die Verbindungszeichenfolge aus und wählen Sie dann Aktionen, Zuordnen/trennen aus.

   Sie können die Zuordnung eines Verbindungsalias zu einem Verzeichnis auch auf der Detailseite eines Verbindungsalias durchführen. Wählen Sie dazu unter Zugeordnetes Verzeichnis die Option Verzeichnis zuordnen aus.
5. Wählen Sie auf der Seite Zuordnen/trennen unter Einem Verzeichnis zuordnen das Verzeichnis aus, dem Sie Ihren Verbindungsalias in dieser AWS-Region zuordnen möchten.

   > **Note**
   >
   > Wenn Sie Ihr Verzeichnis in AWS Managed Microsoft AD für die Replikation in mehreren Regionen konfigurieren, kann nur das Verzeichnis in der primären Region mit Amazon verwendet werden WorkSpaces. Versuche, das Verzeichnis in einer replizierten Region mit Amazon zu verwenden WorkSpaces , schlagen fehl. Die Multi-Region-Replikation mit AWS Managed Microsoft AD wird für die Verwendung mit Amazon WorkSpaces in replizierten Regionen nicht unterstützt.
6. Wählen Sie Associate aus.
7. Wiederholen Sie diese Schritte, aber stellen Sie sicherStep 2, dass Sie in die Failover-Region für Ihr auswählen WorkSpaces. Wenn Sie über mehr als eine Failover-Region verfügen, wiederholen Sie diese Schritte für jede Failover-Region. Stellen Sie sicher, dass Sie in jeder Failover-Region denselben Verbindungsalias einem Verzeichnis zuordnen.

Schritt 4: Konfigurieren Ihres DNS-Service und Einrichten von DNS-Routing-Richtlinien

Nachdem Sie Ihre Verbindungsaliase und Ihre Verbindungsalias-Zuordnungspaare erstellt haben, können Sie den DNS-Service für die Domain konfigurieren, die Sie in Ihren Verbindungszeichenfolgen verwendet haben. Zu diesem Zweck können Sie einen beliebigen DNS-Service-Anbieter verwenden. Wenn Sie noch keinen bevorzugten DNS-Service-Anbieter haben, können Sie Amazon Route 53 verwenden. Weitere Informationen finden Sie unter Konfigurieren von Amazon Route 53 als DNS-Service im Entwicklerhandbuch für Amazon Route 53.

Nachdem Sie den DNS-Service für Ihre Domain konfiguriert haben, müssen Sie die DNS-Routing-Richtlinien einrichten, die Sie für die regionsübergreifende Umleitung verwenden möchten. Sie können beispielsweise Amazon Route 53-Zustandsprüfungen verwenden, um festzustellen, ob Ihre Benutzer eine Verbindung zu ihren WorkSpaces in einer bestimmten Region herstellen können. Wenn Ihre Benutzer keine Verbindung herstellen können, können Sie eine DNS-Failover-Richtlinie verwenden, um Ihren DNS-Datenverkehr von einer Region in eine andere weiterzuleiten.

Informationen zu DNS-Routing-Richtlinien finden Sie unter Auswahl einer Routing-Richtlinie im Amazon-Route-53-Entwicklerhandbuch. Weitere Informationen zu Amazon-Route 53-Zustandsprüfungen finden Sie unter So überprüft Amazon Route 53 den Zustand Ihrer Ressourcen im Amazon-Route-53-Entwicklerhandbuch.

Wenn Sie Ihre DNS-Routing-Richtlinien einrichten, benötigen Sie die Verbindungskennung für die Zuordnung zwischen dem Verbindungsalias und dem WorkSpaces Verzeichnis in der primären Region. Sie benötigen auch die Verbindungskennung für die Zuordnung zwischen dem Verbindungsalias und dem WorkSpaces Verzeichnis in Ihrer Failover-Region oder Ihren Regionen.

> **Note**
>
> Die Verbindungs-ID ist nicht identisch mit der Alias-ID der Verbindung. Die Alias-ID der Verbindung beginnt mit `wsca-`.

So finden Sie die Verbindungs-ID für eine Verbindung mit einem Verbindungsalias

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie in der oberen rechten Ecke der Konsole die primäre AWS Region für Ihre aus WorkSpaces.
3. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
4. Wählen Sie unter Regionsübergreifende Umleitungszuordnungen den Text der Verbindungszeichenfolge (den FQDN) aus, um die Seite mit den Verbindungsaliasdetails anzuzeigen.
5. Notieren Sie sich auf der Detailseite für Ihren Verbindungsalias unter Zugeordnetes Verzeichnis den Wert, der für Verbindungs-ID angezeigt wird.
6. Wiederholen Sie diese Schritte, aber stellen Sie sicherStep 2, dass Sie in die Failover-Region für Ihr auswählen WorkSpaces. Wenn Sie über mehr als eine Failover-Region verfügen, wiederholen Sie die Schritte zur Suche der Verbindungs-ID für jede Failover-Region.

Beispiel: So richten Sie eine DNS-Failover-Routing-Richtlinie mithilfe von Route 53 ein

Im folgenden Beispiel wird eine öffentlich gehostete Zone für Ihre Domain eingerichtet. Sie können jedoch eine öffentlich oder privat gehostete Zone einrichten. Weitere Informationen über private gehostete Zonen finden Sie unter Arbeiten mit gehosteten Zonen im Amazon-Route-53-Entwicklerhandbuch.

In diesem Beispiel wird auch eine Failover-Routing-Richtlinie verwendet. Sie können andere Routing-Richtlinientypen für Ihre regionsübergreifende Umleitungsstrategie verwenden. Informationen zu DNS-Routing-Richtlinien finden Sie unter Auswahl einer Routing-Richtlinie im Amazon-Route-53-Entwicklerhandbuch.

Wenn Sie eine Failover-Routing-Richtlinie in Route 53 einrichten, ist eine Zustandsprüfung für die primäre Region erforderlich. Weitere Informationen zum Erstellen einer Zustandsprüfung in Route 53 finden Sie unter Erstellen von Amazon-Route-53-Zustandsprüfungen und Konfigurieren von DNS-Failover und Erstellen, Aktualisieren und Löschen von Zustandsprüfungen im Amazon-Route-53-Entwicklerhandbuch.

Wenn Sie einen Amazon- CloudWatch Alarm mit Ihrer Route 53-Zustandsprüfung verwenden möchten, müssen Sie auch einen CloudWatch Alarm einrichten, um die Ressourcen in Ihrer primären Region zu überwachen. Weitere Informationen zu CloudWatchfinden Sie unter Was ist Amazon CloudWatch? im Amazon- CloudWatch Benutzerhandbuch. Weitere Informationen darüber, wie Route 53 CloudWatch Alarme in seinen Zustandsprüfungen verwendet, finden Sie unter Wie Route 53 den Status von Zustandsprüfungen bestimmt, die CloudWatch Alarme überwachen, und Überwachen eines CloudWatch Alarms im Amazon-Route-53-Entwicklerhandbuch.

Sie müssen zunächst eine gehostete Zone für Ihre Domain erstellen, um eine DNS-Failover-Routing-Richtlinie in Route 53 einzurichten.

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Gehostete Zonen aus und wählen Sie dann Gehostete Zone erstellen aus.
3. Geben Sie auf der Seite Gehostete Zone erstellen unter Domainname Ihren Domainnamen (z. B.`example.com`) ein.
4. Wählen Sie unter Typ die Option Öffentliche gehostete Zone aus.
5. Wählen Sie Erstellte gehostete Zone.

Erstellen Sie dann eine Zustandsprüfung für Ihre primäre Region.

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Zustandsprüfungen und dann Zustandsprüfung erstellen aus.
3. Geben Sie auf der Seite Zustandsprüfung konfigurieren einen Namen für Ihre Zustandsprüfung ein.
4. Wählen Sie für Was überwacht werden soll entweder Endpunkt , Status anderer Zustandsprüfungen (berechnete Zustandsprüfung) oder CloudWatch Alarmzustand aus.
5. Abhängig davon, was Sie im vorherigen Schritt ausgewählt haben, konfigurieren Sie Ihre Zustandsprüfung und wählen Sie dann Weiter aus.
6. Wählen Sie auf der Seite Benachrichtigen, wenn die Zustandsprüfung fehlschlägt, für Alarm erstellen die Option Ja oder Nein aus.
7. Wählen Sie Zustandsprüfung erstellen aus.

Nachdem Sie Ihre Zustandsprüfung erstellt haben, können Sie die DNS-Failover-Datensätze erstellen.

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie auf der Seite Gehostete Zonen Ihren Domainnamen aus.
4. Wählen Sie auf der Detailseite für Ihren Domainnamen die Option Datensatz erstellen aus.
5. Wählen Sie auf der Seite Routing-Richtlinie auswählen die Option Failover und dann Weiter aus.
6. Geben Sie auf der Seite Datensätze konfigurieren unter Basiskonfiguration für Datensatzname Ihren Subdomain-Name ein. Wenn Ihr FQDN `desktop.example.com` lautet, geben Sie beispielsweise **`desktop`** ein.

   > **Note**
   >
   > Wenn Sie die Root-Domain verwenden möchten, lassen Sie das Feld Datensatzname leer. Wir empfehlen jedoch, eine Subdomäne wie `desktop` oder zu verwenden, es sei denn`workspaces`, Sie haben die Domäne ausschließlich für die Verwendung mit Ihrem eingerichtet WorkSpaces.

7. Wählen Sie als Datensatztyp die Option TXT – Wird zur Verifizierung von E-Mail-Absendern und für anwendungsspezifische Werte verwendet aus.
8. Belassen Sie die TTL-Sekunden-Einstellungen auf der Standardeinstellung.

9. Wählen Sie unter Zu ***your_domain_name*** hinzuzufügende Failover-Datensätze die Option Failover-Datensatz definieren aus.

Jetzt müssen Sie die Failover-Datensätze für Ihre primären Regionen und Ihre Failover-Regionen einrichten.

Beispiel: So richten Sie den Failover-Datensatz für Ihre primäre Region ein

1. Wählen Sie im Dialogfeld Failover-Datensatz definieren für Wert/Traffic weiterleiten an IP-Adresse oder einen anderen Wert, je nach Datensatztyp aus.
2. Es wird ein Feld geöffnet, in das Sie Ihre Beispieltexteinträge eingeben können. Geben Sie die Verbindungs-ID für die Verbindungsaliaszuordnung für Ihre primäre Region ein.
3. Wählen Sie für Failover-Datensatztyp die Option Primär.
4. Wählen Sie für Zustandsprüfung eine Zustandsprüfung aus, die Sie für Ihre primäre Region erstellt haben.
5. Geben Sie unter Datensatz-ID eine Beschreibung ein, um diesen Datensatz zu identifizieren.
6. Wählen Sie Failover-Datensatz definieren aus. Ihr neuer Failover-Datensatz wird unter Zu ***your_domain_name*** hinzuzufügende Failover-Datensätze angezeigt.

Beispiel: So richten Sie den Failover-Datensatz für Ihre Failover-Region ein

1. Wählen Sie unter Zu ***your_domain_name*** hinzuzufügende Failover-Datensätze die Option Failover-Datensatz definieren aus.
2. Wählen Sie im Dialogfeld Failover-Datensatz definieren für Wert/Traffic weiterleiten an IP-Adresse oder einen anderen Wert, je nach Datensatztyp aus.
3. Es wird ein Feld geöffnet, in das Sie Ihre Beispieltexteinträge eingeben können. Geben Sie die Verbindungs-ID für die Verbindungsaliaszuordnung für Ihre Failover-Region ein.
4. Wählen Sie für Failover-Datensatztyp die Option Sekundär aus.
5. (Optional) Geben Sie für Zustandsprüfung eine Zustandsprüfung ein, die Sie für Ihre Failover-Region erstellt haben.
6. Geben Sie unter Datensatz-ID eine Beschreibung ein, um diesen Datensatz zu identifizieren.
7. Wählen Sie Failover-Datensatz definieren aus. Ihr neuer Failover-Datensatz wird unter Zu ***your_domain_name*** hinzuzufügende Failover-Datensätze angezeigt.

Wenn die Zustandsprüfung, die Sie für Ihre primäre Region eingerichtet haben, fehlschlägt, leitet Ihre DNS-Failover-Routing-Richtlinie Ihre WorkSpaces Benutzer an Ihre Failover-Region weiter. Route 53 überwacht weiterhin die Zustandsprüfung für Ihre primäre Region. Wenn die Zustandsprüfung für Ihre primäre Region nicht mehr fehlschlägt, leitet Route 53 Ihre WorkSpaces Benutzer automatisch zurück zu ihrem WorkSpaces in der primären Region.

Weitere Informationen zum Erstellen von DNS-Datensätzen finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole im Amazon-Route-53-Entwicklerhandbuch. Weitere Informationen über die Konfiguration von DNS-TXT-Datensätzen finden Sie unter TXT-Datensatztyp im Amazon-Route-53-Entwicklerhandbuch.

Schritt 5: Senden der Verbindungszeichenfolge an Ihre WorkSpaces Benutzer

Um sicherzustellen, dass der Ihrer Benutzer bei einem Ausfall nach Bedarf umgeleitet WorkSpaces wird, müssen Sie die Verbindungszeichenfolge (FQDN) an Ihre Benutzer senden. Wenn Sie Ihren WorkSpaces Benutzern bereits regionsbasierte Registrierungscodes (z. B. `WSpdx+ABC12D`) ausgestellt haben, bleiben diese Codes gültig. Damit die regionsübergreifende Umleitung jedoch funktioniert, müssen Ihre WorkSpaces Benutzer die Verbindungszeichenfolge als Registrierungscode verwenden, wenn sie ihre WorkSpaces in der WorkSpaces Clientanwendung registrieren.

> **Important**
>
> Wenn Sie Ihre Benutzer in der WorkSpaces Konsole erstellen, anstatt sie in Active Directory zu erstellen, WorkSpaces sendet automatisch eine Einladungs-E-Mail mit einem regionsbasierten Registrierungscode (z. B. `WSpdx+ABC12D`), wenn Sie ein neues starten WorkSpace. Auch wenn Sie bereits eine regionsübergreifende Umleitung eingerichtet haben, WorkSpaces enthält die Einladungs-E-Mail, die automatisch für neue gesendet wird, diesen regionsbasierten Registrierungscode anstelle Ihrer Verbindungszeichenfolge.
> Um sicherzustellen, dass Ihre WorkSpaces Benutzer die Verbindungszeichenfolge anstelle des regionsbasierten Registrierungscodes verwenden, müssen Sie ihnen mithilfe des folgenden Verfahrens eine weitere E-Mail mit der Verbindungszeichenfolge senden.

So senden Sie die Verbindungszeichenfolge an Ihre WorkSpaces Benutzer

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.

2. Wählen Sie in der oberen rechten Ecke der Konsole die primäre AWS Region für Ihre aus WorkSpaces.
3. Wählen Sie im Navigationsbereich aus WorkSpaces.
4. Verwenden Sie auf der WorkSpaces Seite das Suchfeld, um nach einem Benutzer zu suchen, an den Sie eine Einladung senden möchten, und wählen Sie dann das entsprechende WorkSpace aus den Suchergebnissen aus. Sie können WorkSpace jeweils nur einen auswählen.
5. Wählen Sie Actions (Aktionen), Invite User (Benutzer einladen).
6. Auf der Seite Benutzer zu ihren einladen WorkSpaces sehen Sie eine E-Mail-Vorlage, die Sie an Ihre Benutzer senden können.
7. (Optional) Wenn Ihrem WorkSpaces Verzeichnis mehr als ein Verbindungsalias zugeordnet ist, wählen Sie die Verbindungszeichenfolge aus, die Ihre Benutzer verwenden sollen, aus der Liste Verbindungsaliaszeichenfolge aus. Die E-Mail-Vorlage wird aktualisiert und zeigt nun die von Ihnen gewählte Zeichenfolge an.
8. Kopieren Sie den E-Mail-Vorlagentext und fügen Sie ihn in Ihrer eigenen E-Mail-Anwendung in eine E-Mail an die Benutzer ein. In Ihrer E-Mail-Anwendung können Sie den Text nach Bedarf ändern. Wenn die Einladungs-E-Mail fertig ist, senden Sie sie an die Benutzer.

Diagramm der regionsübergreifenden Umleitungsarchitektur

Das folgende Diagramm beschreibt den Bereitstellungsprozess der regionsübergreifenden Umleitung.

> **Note**
>
> Die regionsübergreifende Umleitung erleichtert nur regionsübergreifendes Failover und Fallback. Es erleichtert nicht das Erstellen und Verwalten WorkSpaces in der sekundären Region und erlaubt keine regionsübergreifende Datenreplikation. WorkSpaces sowohl in der primären als auch in der sekundären Region sollten separat verwaltet werden.

Initiieren einer regionsübergreifenden Umleitung

Im Falle eines Ausfalls können Sie die DNS-Datensätze entweder manuell aktualisieren oder automatisierte Routing-Richtlinien basierend auf Zustandsprüfungen verwenden, die die Failover-

Region bestimmen. Wir empfehlen, die Notfallwiederherstellungsmechanismen zu befolgen, die unter Erstellen von Notfallwiederherstellungsmechanismen mit Amazon Route 53 beschrieben sind.

Was passiert bei der regionsübergreifenden Umleitung?

Während des Regions-Failovers werden Ihre WorkSpaces Benutzer von ihrem WorkSpaces in der primären Region getrennt. Beim Versuch, die Verbindung wiederherzustellen, erhalten sie die folgende Fehlermeldung:

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

Ihre Benutzer werden dann aufgefordert, sich erneut anzumelden. Wenn sie den FQDN als Registrierungscode verwenden, leiten Ihre DNS-Failover-Routing-Richtlinien sie an die weiter, WorkSpaces die Sie für sie in der Failover-Region eingerichtet haben.

> **Note**
>
> In einigen Fällen können Benutzer möglicherweise keine erneute Verbindung herstellen, wenn sie sich erneut anmelden. Wenn dieses Verhalten auftritt, müssen sie die WorkSpaces Client-Anwendung schließen und neu starten und dann erneut versuchen, sich anzumelden.

Trennen der Zuordnung eines Verbindungsalias zu einem Verzeichnis

Nur das Konto, dem ein Verzeichnis gehört, kann die Zuordnung eines Verbindungsalias zu dem Verzeichnis aufheben.

Wenn Sie einen Verbindungsalias für ein anderes Konto verwendet haben und dieses Konto den Verbindungsalias einem seiner Verzeichnisse zugeordnet hat, müssen Sie über dieses Konto die Zuordnung des Verbindungsalias zum Verzeichnis aufheben.

So trennen Sie die Zuordnung eines Verbindungsalias zu einem Verzeichnis

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie oben rechts in der Konsole die AWS-Region aus, die den Verbindungsalias enthält, dessen Zuordnung Sie aufheben möchten.
3. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).

4. Wählen Sie unter Regionsübergreifende Umleitungszuordnungen die Verbindungszeichenfolge aus und wählen Sie dann Aktionen, Zuordnen/trennen aus.

   Sie können einen Verbindungsalias auch über die Seite mit den Verbindungsaliasdetails trennen. Wählen Sie dazu unter Zugeordnetes Verzeichnis die Option Zuordnung aufheben aus.
5. Wählen Sie auf der Seite Zuordnen/Zuordnung aufheben die Option Zuordnung aufheben aus.
6. Wählen Sie in dem Dialogfeld, in dem Sie aufgefordert werden, die Trennung zu bestätigen, die Option Zuordnung aufheben aus.

Freigeben eines Verbindungsalias rückgängig machen

Nur der Besitzer eines Verbindungsalias kann die gemeinsame Nutzung des Alias rückgängig machen. Wenn Sie die gemeinsame Nutzung eines Verbindungsalias mit einem Konto aufheben, kann dieses Konto den Verbindungsalias nicht mehr einem Verzeichnis zuordnen.

So machen Sie das Freigeben eines Verbindungsalias rückgängig

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie oben rechts in der Konsole die AWS-Region aus, die den Verbindungsalias enthält, dessen Freigabe Sie aufheben möchten.
3. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
4. Wählen Sie unter Regionsübergreifende Umleitungszuordnungen die Verbindungszeichenfolge aus und wählen Sie dann Aktionen, Verbindungsalias freigeben/Freigabe aufheben aus.

   Sie können die Freigabe eines Verbindungsalias auch über die Seite mit den Verbindungsaliasdetails aufheben. Wählen Sie dazu unter Freigegebenes Konto die Option Freigabe aufheben aus.
5. Wählen Sie auf der Seite Verbindungsalias freigeben/Freigabe aufheben die Option Freigabe aufheben aus.
6. Wählen Sie in dem Dialogfeld, in dem Sie aufgefordert werden, das Aufheben der Freigabe des Verbindungsalias zu bestätigen, die Option Freigabe aufheben aus.

Löschen eines Verbindungsalias

Sie können einen Verbindungsalias nur löschen, wenn er Ihrem Konto gehört und wenn er keinem Verzeichnis zugeordnet ist.

Wenn Sie einen Verbindungsalias für ein anderes Konto verwendet haben und dieses Konto den Verbindungsalias einem seiner Verzeichnisse zugeordnet hat, müssen Sie über dieses Konto die Zuordnung des Verbindungsalias zum Verzeichnis aufheben, bevor Sie den Alias löschen können.

Important

Nachdem Sie eine Verbindungszeichenfolge erstellt haben, ist diese immer Ihrem AWS-Konto zugeordnet. Eine Verbindungszeichenfolge kann nicht mit einem anderen Konto erneut erstellt werden, selbst wenn Sie alle Instances aus dem ursprünglichen Konto gelöscht haben. Die Verbindungszeichenfolge ist global für Ihr Konto reserviert.

Warning

Wenn Sie keinen FQDN mehr als Registrierungscode für Ihre WorkSpaces Benutzer verwenden, müssen Sie bestimmte Maßnahmen ergreifen, um potenzielle Sicherheitsprobleme zu vermeiden. Weitere Informationen finden Sie unter Sicherheitsüberlegungen beim Beenden der Verwendung der regionsübergreifenden Umleitung.

So löschen Sie einen Verbindungsalias

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie oben rechts in der Konsole die AWS-Region aus, die den Verbindungsalias enthält, den Sie löschen möchten.
3. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
4. Wählen Sie unter Regionsübergreifende Umleitungszuordnungen die Verbindungszeichenfolge aus und wählen Sie dann Löschen aus.

   Sie können das Löschen eines Verbindungsalias auch über die Seite mit den Verbindungsaliasdetails durchführen. Wählen Sie oben rechts auf der Seite Löschen aus.

   Note

   Wenn die Schaltfläche Löschen deaktiviert ist, stellen Sie sicher, dass Sie der Besitzer des Alias sind und dass der Alias keinem Verzeichnis zugeordnet ist.

5. Wählen Sie im Löschdialogfeld die Option Löschen aus, um das Löschen zu bestätigen.

IAM-Berechtigungen für das Zuordnen und Trennen eines Verbindungsalias

Wenn Sie einen IAM-Benutzer verwenden, um Verbindungsaliase zuzuordnen oder zu trennen, muss der Benutzer über Berechtigungen für `workspaces:AssociateConnectionAlias` und `workspaces:DisassociateConnectionAlias` verfügen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

Important

Wenn Sie eine IAM-Richtlinie zum Zuordnen oder Trennen von eines Verbindungsalias für Konten erstellen, denen die Verbindungsaliase nicht gehören, können Sie im ARN keine Konto-ID angeben. Stattdessen müssen Sie * für die Konto-ID verwenden, wie in der folgenden Beispielrichtlinie gezeigt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
```

```
            "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
        ]
      }
    ]
}
```

Sie können im ARN nur dann eine Konto-ID angeben, wenn dieses Konto den Verbindungsalias besitzt, der zugeordnet oder getrennt werden soll.

Weitere Informationen zur Arbeit mit IAM finden Sie unter Identitäts- und Zugriffsverwaltung für WorkSpaces.

Sicherheitsüberlegungen beim Beenden der Verwendung der regionsübergreifenden Umleitung

Wenn Sie keinen FQDN mehr als Registrierungscode für Ihre WorkSpaces Benutzer verwenden, müssen Sie die folgenden Maßnahmen treffen, um potenzielle Sicherheitsprobleme zu vermeiden:

- Stellen Sie sicher, dass Sie Ihren WorkSpaces Benutzern den regionsspezifischen Registrierungscode (z. B. `WSpdx+ABC12D`) für ihr WorkSpaces Verzeichnis ausstellen, und weisen Sie sie an, den FQDN nicht mehr als ihren Registrierungscode zu verwenden.
- Wenn Sie diese Domain immer noch besitzen, aktualisieren Sie unbedingt Ihren DNS-TXT-Datensatz, um diese Domain zu entfernen, sodass sie nicht bei einem Phishing-Angriff ausgenutzt werden kann. Wenn Sie diese Domain aus Ihrem DNS-TXT-Datensatz entfernen und Ihre WorkSpaces Benutzer versuchen, den FQDN als ihren Registrierungscode zu verwenden, schlagen ihre Verbindungsversuche primär fehl.
- Wenn Sie diese Domain nicht mehr besitzen, müssen Ihre WorkSpaces Benutzer ihren regionsspezifischen Registrierungscode verwenden. Wenn sie weiterhin versuchen, den FQDN als ihren Registrierungscode zu verwenden, könnten ihre Verbindungsversuche möglicherweise auf eine schädliche Website umgeleitet werden.

Multiregionale Ausfallsicherheit für Amazon WorkSpaces

Mit Amazon WorkSpaces Multi-Region Resilience (MRR) können Sie Benutzer zu einer sekundären Region umleiten, wenn Ihre primäre WorkSpaces Region aufgrund störender Ereignisse nicht erreichbar ist, ohne dass Ihre Benutzer bei der Protokollierung in ihrer Standby-Instance die

Registrierungscodes wechseln müssen WorkSpaces. Standby WorkSpaces ist ein Feature von Amazon WorkSpaces Multi-Region Resilience, das die Erstellung und Verwaltung der Standby-Bereitstellung optimiert. Nachdem Sie ein Benutzerverzeichnis in Ihrer sekundären Region eingerichtet haben, wählen Sie die WorkSpace in Ihrer primären Region aus, WorkSpace für die Sie eine Standby-Instance erstellen möchten. Das System spiegelt die primären WorkSpace Bundle-Images automatisch in die sekundäre Region. Anschließend wird automatisch eine neue Standby-Instance WorkSpace in Ihrer sekundären Region bereitgestellt.

Amazon WorkSpaces Multi-Region Resilience basiert auf einer regionsübergreifenden Umleitung, die DNS-Zustandsprüfungen und Failover-Funktionen nutzt. Damit können Sie einen vollqualifizierten Domainnamen (FQDN) als WorkSpaces Registrierungscode verwenden. Wenn sich Ihre Benutzer bei anmelden WorkSpaces, können Sie sie basierend auf Ihren DNS-Richtlinien (Domain Name System) für den FQDN zwischen unterstützten WorkSpaces Regionen umleiten. Wenn Sie Amazon Route 53 verwenden, empfehlen wir, Zustandsprüfungen zu verwenden, die Amazon- CloudWatch Alarme überwachen, wenn Sie eine regionsübergreifende Umleitungsstrategie für entwickeln WorkSpaces. Weitere Informationen finden Sie unter Erstellen von Amazon-Route-53-Zustandsprüfungen und Konfigurieren von DNS-Failover im Amazon-Route-53-Entwicklerhandbuch.

Die Datenreplikation ist ein Add-On-Feature von Standby WorkSpaces , das Daten unidirektional von der primären Region in die sekundäre Region repliziert. Nach der Aktivierung der Datenreplikation werden alle 12 Stunden EBS-Snapshots der System- und Benutzer-Volumes erstellt. Multiregionale Ausfallsicherheit sucht regelmäßig nach neuen Snapshots. Wenn die Snapshots gefunden werden, wird eine Kopie in die sekundäre Region initiiert. Wenn Kopien in der sekundären Region ankommen, werden sie verwendet, um die sekundäre zu aktualisieren WorkSpace.

Inhalt

Voraussetzungen

- Sie müssen WorkSpaces für Ihre Benutzer in der primären Region erstellen, bevor Sie Standby- erstellen WorkSpaces. Weitere Informationen zum Erstellen von finden Sie WorkSpacesunter Starten eines virtuellen Desktops mit WorkSpaces.
- Um die Datenreplikation auf Standby- zu aktivieren WorkSpaces, sollten Sie entweder ein selbstverwaltetes Active Directory oder ein AWS Managed Microsoft AD für die Replikation in Ihre Standby-Regionen konfiguriert haben. Weitere Informationen finden Sie unter Erstellen Ihres Verzeichnisses in AWS Managed Microsoft AD und Hinzufügen einer replizierten Region.
- Stellen Sie sicher, dass Sie Netzwerkabhängigkeitstreiber wie ENA-, NVMe- und PV-Treiber auf Ihrem primären aktualisieren WorkSpaces. Sie sollten dies mindestens einmal alle 6 Monate tun. Weitere Informationen finden Sie unter Installieren oder Aktualisieren von Elastic Network Adapter (ENA)-Treibern, AWS-NVMe-Treiber für Windows-Instances und Upgrade von PV-Treibern auf Windows-Instances.
- Stellen Sie sicher, dass Sie die EC2Config, EC2Launch und EC2Launch V2-Agenten regelmäßig auf die neuesten Versionen aktualisieren. Sie sollten dies mindestens einmal alle 6 Monate tun. Weitere Informationen finden Sie unter Aktualisieren von EC2Config und EC2Launch.
- Um eine ordnungsgemäße Datenreplikation sicherzustellen, stellen Sie sicher, dass die Active Directories in den primären und sekundären Regionen für FQDN, OU und Benutzer-SID synchronisiert sind.
- Das Standardkontingent (Limit) für Standby WorkSpaces ist 0. Sie müssen eine Erhöhung des Servicekontingents beantragen, bevor Sie eine Standby- erstellen WorkSpace. Weitere Informationen finden Sie unter Amazon- WorkSpaces Kontingente.
- Stellen Sie sicher, dass Sie vom Kunden verwaltete Schlüssel verwenden, um sowohl Ihren primären als auch Ihren Standby- zu verschlüsseln WorkSpaces. Sie können entweder einzelregionale Schlüssel oder multiregionale Schlüssel verwenden, um Ihre primären und Standby- zu verschlüsseln WorkSpaces.

Einschränkungen

- Standby kopiert WorkSpaces nur das Bundle-Image Ihrer primären , kopiert WorkSpaces jedoch nicht das System-Volume (Laufwerk C) oder das Benutzer-Volume (Laufwerk D) von Ihrer primären WorkSpaces. Um das System-Volume (Laufwerk C) oder das Benutzer-Volume (Laufwerk D) von Ihrem primären WorkSpaces zu Ihrem Standby- zu kopieren WorkSpaces, müssen Sie die Datenreplikation aktivieren.

- Sie können eine Standby- nicht direkt ändern, neu erstellen, wiederherstellen oder migrieren WorkSpace.
- Der Failover für die regionsübergreifende Umleitung wird durch Ihre DNS-Einstellungen gesteuert. Sie müssen einen anderen Mechanismus in Verbindung mit der regionsübergreifenden Umleitung verwenden, um ein automatisches Failover-Szenario zu implementieren. Sie können beispielsweise eine Amazon Route 53 Failover DNS-Routing-Richtlinie in Kombination mit einer Route 53-Zustandsprüfung verwenden, die einen CloudWatch Alarm in der primären Region überwacht. Wenn der CloudWatch Alarm in der primären Region aufgerufen wird, leitet Ihre DNS-Failover-Routing-Richtlinie Ihre WorkSpaces Benutzer an die weiter WorkSpaces , die Sie für sie in der Failover-Region eingerichtet haben.
- Die Datenreplikation ist nur eine Möglichkeit, Daten von der primären Region in die sekundäre Region zu kopieren. Während des Standby- WorkSpaces Failovers können Sie zwischen 12 und 24 Stunden auf die Daten und die Anwendung zugreifen. Sichern Sie nach einem Ausfall manuell alle Daten, die Sie auf dem sekundären erstellt haben, WorkSpace und melden Sie sich ab. Wir empfehlen, Ihre Arbeit auf externen Laufwerken zu speichern, z. B. auf Ihrem Netzwerklaufwerk, damit Sie von der primären aus auf Ihre Daten zugreifen können WorkSpace.
- Die Datenreplikation unterstützt AWS Simple AD nicht.
- Wenn Sie die Datenreplikation auf Standby- aktivieren WorkSpaces, werden alle 12 Stunden EBS-Snapshots des primären WorkSpaces (sowohl Root- als auch System-Volumes) erstellt. Der anfängliche Snapshot für ein bestimmtes Daten-Volume ist voll und nachfolgende Snapshots sind inkrementell. Daher WorkSpace dauert die erste Replikation für eine bestimmte länger als die nachfolgenden. Snapshots werden nach einem Zeitplan initiiert, der intern für ist, WorkSpaces und Sie können das Timing nicht steuern.
- Wenn der primäre WorkSpace und der Standby- WorkSpace Join mit derselben Domain verbunden werden, empfehlen wir, dass Sie WorkSpace zu einem bestimmten Zeitpunkt nur eine Verbindung zum primären WorkSpace oder Standby-Cluster herstellen, um zu vermeiden, dass die Verbindung mit dem Domain-Controller unterbrochen wird.
- Wenn Sie Ihr AWS Managed Microsoft AD für die Multi-Region-Replikation konfigurieren, kann nur das Verzeichnis in der primären Region für die Verwendung mit registriert werden WorkSpaces. Wenn Sie versuchen, das Verzeichnis in einer replizierten Region für die Verwendung mit zu registrieren WorkSpaces, schlägt es fehl. Die Multi-Region-Replikation mit AWS Managed Microsoft AD wird nicht für die Verwendung mit WorkSpaces innerhalb replizierter Regionen unterstützt.
- Wenn Sie Ihre regionsübergreifende Umleitung bereits eingerichtet und sowohl WorkSpaces in Ihrer primären als auch in Ihrer sekundären Region ohne Verwendung von Standby erstellt

haben WorkSpaces, können Sie die vorhandene WorkSpace in der sekundären Region nicht WorkSpace direkt in eine Standby-Region konvertieren. Stattdessen müssen Sie die WorkSpace in Ihrer sekundären Region herunterfahren, die WorkSpace in Ihrer primären Region auswählen, WorkSpace für die Sie eine Standby-Instance erstellen möchten, und Standby verwenden, WorkSpaces um die Standby-Instance zu erstellen WorkSpace.

- Sichern Sie nach einem Ausfall manuell alle Daten, die Sie auf dem sekundären erstellt haben, WorkSpace und melden Sie sich ab. Wir empfehlen, Ihre Arbeit auf externen Laufwerken zu speichern, z. B. auf Ihrem Netzwerklaufwerk, damit Sie von der primären aus auf Ihre Daten zugreifen können WorkSpace.
- WorkSpaces Multiregionale Ausfallsicherheit ist derzeit in den folgenden Regionen verfügbar:
  - Region USA Ost (Nord-Virginia)
  - Region USA West (Oregon)
  - Region Europa (Frankfurt)
  - Europe (Ireland) Region
- WorkSpaces Multiregionale Ausfallsicherheit wird nur von Version 3.0.9 oder höher der Linux-, macOS- und Windows WorkSpaces -Clientanwendungen unterstützt. Sie können Multi-Region Resilience auch mit Web Access verwenden.
- WorkSpaces Multi-Region Resilience unterstützt Windows und Bring Your Own License (BYOL WorkSpaces). Es unterstützt keine Amazon Linux-, Ubuntu- WorkSpacesoder GPU-fähigen WorkSpaces (z. B. Graphics, GraphicsPro, Graphics.g4dn oder GraphicsPro.g4dn).
- Warten Sie nach Abschluss des Failovers oder Failovers 15 bis 30 Minuten, bevor Sie eine Verbindung zu Ihrem herstellen WorkSpace.

Konfigurieren Ihrer Multi-Region Resilience Standby WorkSpace

So konfigurieren Sie Ihre Multi-Region Resilience Standby WorkSpace

1. Richten Sie Benutzerverzeichnisse sowohl in Ihrer primären als auch in Ihrer sekundären Region ein. Stellen Sie sicher, dass Sie in jedem WorkSpaces Verzeichnis in jeder Region dieselben Benutzernamen verwenden.

   Um Ihre Active-Directory-Benutzerdaten synchron zu halten, empfehlen wir, AD Connector zu verwenden, um in jeder Region, in der Sie WorkSpaces für Ihre Benutzer eingerichtet haben, auf dasselbe Active Directory zu verweisen. Weitere Informationen zum Erstellen eines Verzeichnisses finden Sie unter Registrieren eines Verzeichnisses bei WorkSpaces.

> **Important**
>
> Wenn Sie Ihr AWS Managed Microsoft AD Verzeichnis für die Replikation in mehreren Regionen konfigurieren, kann nur das Verzeichnis in der primären Region für die Verwendung mit registriert werden WorkSpaces. Versuche, das Verzeichnis in einer replizierten Region für die Verwendung mit zu registrieren WorkSpaces , schlagen fehl. Die Multi-Region-Replikation mit AWS Managed Microsoft AD wird nicht für die Verwendung mit WorkSpaces innerhalb replizierter Regionen unterstützt.

2. Erstellen Sie WorkSpaces für Ihre Benutzer in der primären Region. Weitere Informationen zum Erstellen von WorkSpacesfinden Sie unter Starten von WorkSpaces.
3. Erstellen Sie eine Standby-Instance WorkSpace in der sekundären Region. Weitere Informationen zum Erstellen eines Standby- WorkSpacefinden Sie unter Erstellen eines Standby- WorkSpace.
4. Erstellen Sie Verbindungszeichenfolgen (FQDN) und verknüpfen Sie sie mit Benutzerverzeichnissen in primären und sekundären Regionen.

   Sie müssen die regionsübergreifende Umleitung in Ihrem Konto aktivieren, da Standby auf der regionsübergreifenden Umleitung WorkSpaces basiert. Folgen Sie Schritt 1 bis 3 der Anweisungen für die regionsübergreifende Umleitung für Amazon WorkSpaces.
5. Konfigurieren Sie den DNS-Service und richten Sie DNS-Routing-Richtlinien ein.

   Sie müssen Ihren DNS-Service einrichten und die erforderlichen DNS-Routing-Richtlinien konfigurieren. Die regionsübergreifende Umleitung funktioniert in Verbindung mit Ihren DNS-Routing-Richtlinien, um Ihre WorkSpaces Benutzer nach Bedarf umzuleiten.
6. Wenn Sie mit der Einrichtung der regionsübergreifenden Umleitung fertig sind, müssen Sie Ihren Benutzern eine E-Mail mit einer FQDN-Verbindungszeichenfolge senden. Weitere Informationen finden Sie unter Schritt 5: Senden der Verbindungszeichenfolge an Ihre WorkSpaces Benutzer. Stellen Sie sicher, dass Ihre WorkSpaces Benutzer den FQDN-basierten Registrierungscode anstelle des regionsbasierten Registrierungscodes (z. B. WSpdx +ABC12D) für ihre primäre Region verwenden.

> **Important**
>
> - Wenn Sie Ihre Benutzer in der WorkSpaces Konsole erstellen, anstatt sie in Active Directory zu erstellen, sendet WorkSpaces automatisch eine Einladungs-E-Mail mit

einem regionsbasierten Registrierungscode an Ihre Benutzer, wenn Sie ein neues starten WorkSpace. Das bedeutet, dass Ihre Benutzer bei der Einrichtung WorkSpaces für Ihre Benutzer in der sekundären Region auch automatisch E-Mails für diese sekundären erhalten WorkSpaces. Sie müssen Ihre Benutzer anweisen, E-Mails mit regionalen Registrierungscodes zu ignorieren.

- Die regionsspezifischen Registrierungscodes bleiben gültig. Damit die regionsübergreifende Umleitung funktioniert, müssen Ihre Benutzer jedoch stattdessen den FQDN als Registrierungscode verwenden.

Erstellen einer Standby-Instance WorkSpace

Bevor Sie eine Standby- erstellen WorkSpace, stellen Sie sicher, dass Sie die Voraussetzungen erfüllt haben, einschließlich der Erstellung eines Benutzerverzeichnisses sowohl in der primären als auch in der sekundären Region, der Bereitstellung WorkSpaces für Ihre Benutzer in Ihrer primären Region, der Konfiguration der regionsübergreifenden Umleitung in Ihrem Konto und der Anforderung einer Erhöhung des Standby- WorkSpaces Limits über das Servicekontingent.

So erstellen Sie eine Standby-Instance WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie in der oberen rechten Ecke der Konsole die primäre AWS Region für Ihre aus WorkSpaces.
3. Wählen Sie im Navigationsbereich aus WorkSpaces.
4. Wählen Sie eine aus, WorkSpace für die WorkSpace Sie eine Standby-Instance erstellen möchten.
5. Wählen Sie Aktionen und dann Standby erstellen aus WorkSpace.
6. Wählen Sie die sekundäre Region aus, in der Sie Ihre Standby- erstellen, WorkSpaceund wählen Sie dann Weiter aus.
7. Wählen Sie das Benutzerverzeichnis in Ihrer sekundären Region aus und wählen Sie dann Weiter aus.
8. (Optional) Fügen Sie Verschlüsselungsschlüssel hinzu, aktivieren Sie die Datenverschlüsselung und verwalten Sie Tags.

   - Um einen Verschlüsselungsschlüssel hinzuzufügen, geben Sie ihn unter Eingabeverschlüsselungsschlüssel ein.

- Um die Datenreplikation zu aktivieren, wählen Sie Datenreplikation aktivieren aus. Aktivieren Sie dann das Kontrollkästchen, um zu bestätigen, dass Sie zusätzliche monatliche Gebühren autorisieren.
- Um ein neues Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen aus.

Wählen Sie anschließend Weiter.

> **Note**
>
> - Wenn das Original verschlüsselt WorkSpace ist, ist dieses Feld vorausgefüllt. Sie können es jedoch durch Ihren eigenen Verschlüsselungsschlüssel ersetzen.
> - Die Aktualisierung des Datenreplikationsstatus dauert einige Minuten.
> - Nachdem die Standby-Version erfolgreich mit den Snapshots aus der primären aktualisiert WorkSpace wurde WorkSpace, finden Sie die Zeitstempel der Sna-Pshots unter Wiederherstellungs-Snapshot.

9. Überprüfen Sie die Einstellungen Ihrer Standby-Instance WorkSpaces und wählen Sie dann Erstellen aus.

> **Note**
>
> - Um Informationen zu Ihrem Standby- anzuzeigen WorkSpaces, gehen Sie zur primären WorkSpace Detailseite.
> - Die Standby-Version kopiert WorkSpace nur das Bundle-Image Ihrer primären , kopiert WorkSpace jedoch nicht das System-Volume (Laufwerk C) oder das Benutzer-Volume (Laufwerk D) von Ihrer primären WorkSpaces. Standardmäßig ist die Datenreplikation deaktiviert. Um das System-Volume (Laufwerk C) oder das Benutzer-Volume (Laufwerk D) von Ihrem primären WorkSpaces zu Ihrem Standby- zu kopieren WorkSpaces, müssen Sie die Datenreplikation aktivieren.

Verwalten einer Standby-Instance WorkSpace

Sie können eine Standby- nicht direkt ändern, neu erstellen, wiederherstellen oder migrieren WorkSpace.

So aktivieren Sie die Datenreplikation für Ihre Standby-Instance WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Gehen Sie zu Ihrer primären Region und wählen Sie die primäre WorkSpace ID aus.
3. Scrollen Sie nach unten zum WorkSpace Abschnitt Standby und wählen Sie Standby bearbeiten aus WorkSpace.
4. Wählen Sie Datenreplikation aktivieren aus. Aktivieren Sie dann das Kontrollkästchen, um zu bestätigen, dass Sie zusätzliche monatliche Gebühren autorisieren. Wählen Sie dann Save (Speichern) aus.

> **Note**
>
> - Standby WorkSpaces kann nicht in den Ruhezustand versetzt werden. Wenn Sie die Standby- anhalten WorkSpace, werden Ihre nicht gespeicherten Arbeiten nicht beibehalten. Wir empfehlen Benutzern, ihre Arbeit immer zu speichern, bevor sie ihre Standby- beenden WorkSpaces.
> - Um die Datenreplikation auf Standby- zu aktivieren WorkSpaces, sollten Sie entweder ein selbstverwaltetes Active Directory oder ein AWS Managed Microsoft AD für die Replikation in Ihre Standby-Regionen konfiguriert haben. Um Ihre Verzeichnisse einzurichten, führen Sie die Schritte 1 bis 3 im Walkthrough-Abschnitt von Entwicklung für Geschäftskontinuität mit Amazon WorkSpaces und AWS Directory Services oder unter Verwenden von Multi-Region AWS Managed Active Directory mit Amazon WorkSpaces aus. Die Multi-Region-Replikation wird nur für die Enterprise Edition von AWS Managed Microsoft AD unterstützt.
> - Die Aktualisierung des Datenreplikationsstatus dauert einige Minuten.
> - Nachdem die Standby-Version erfolgreich mit den Snapshots aus der primären aktualisiert WorkSpace wurde WorkSpace, finden Sie die Zeitstempel der Snapshots unter Wiederherstellungs-Snapshot.

Löschen einer Standby-Instance WorkSpace

Sie können eine Standby-Instance WorkSpace auf die gleiche Weise beenden, wie Sie eine reguläre beenden WorkSpace.

So löschen Sie eine Standby-Instance WorkSpace

1. Öffnen Sie die - WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.
2. Wählen Sie in der oberen rechten Ecke der Konsole die primäre AWS Region für Ihr aus WorkSpaces.
3. Wählen Sie im Navigationsbereich aus WorkSpaces.
4. Wählen Sie den Standby-Modus WorkSpace und dann Löschen aus. Das Löschen eines Standby- dauert etwa 5 Minuten WorkSpace. Während des Löschens WorkSpace wird der Status der Standby-Instance auf Beenden gesetzt. Wenn das Löschen abgeschlossen ist, WorkSpace verschwindet die Standby-Version aus der Konsole.

> **Note**
>
> Das Löschen einer Standby-Instance WorkSpace ist eine permanente Aktion und kann nicht rückgängig gemacht werden. Die Daten des Standby- WorkSpace Benutzers bleiben nicht erhalten und werden zerstört. Wenn Sie Hilfe bei der Sicherung von Benutzerdaten benötigen, wenden Sie sich an den AWS-Support.

Einseitige Datenreplikation für Standby WorkSpaces

Durch die Aktivierung der Datenreplikation in Multi-Region Resilience können Sie Daten aus einer primären Region in eine sekundäre Region replizieren. Während des stabilen Zustands erfasst Multi-Region Resilience WorkSpaces alle 12 Stunden Snapshots des Systems (C-Laufwerk) und der Daten (D-Laufwerk) des primären Clusters. Diese Snapshots werden in die sekundäre -Region übertragen und zum Aktualisieren des Standby- verwendet WorkSpaces. Standardmäßig ist die Datenreplikation für Standby- deaktiviert WorkSpaces.

Nachdem die Datenreplikation für die Standby- aktiviert wurde WorkSpaces, ist der erste Snapshot für ein bestimmtes Datenvolume abgeschlossen, während nachfolgende Snapshots inkrementell sind. Infolgedessen WorkSpace dauert die erste Replikation für eine bestimmte länger als die nachfolgenden. Snapshots werden in vordefinierten Intervallen innerhalb von ausgelöst WorkSpaces und das Timing kann nicht von Benutzern gesteuert werden.

Wenn Benutzer während des Failovers in die sekundäre Region umgeleitet werden, können sie WorkSpaces mit Daten und Anwendungen, die zwischen 12 und 24 Stunden alt sind, auf ihre

Standby-Instance zugreifen. Während Benutzer Standby verwenden WorkSpaces, zwingt Multi-Region Resilience sie nicht, sich von ihrer Standby- WorkSpaces Instance abzumelden oder die Standby-Instance WorkSpaces mit den Snapshots aus der primären Region zu aktualisieren.

Nach einem Ausfall sollten Benutzer alle Daten, die sie auf ihrem sekundären erstellt haben, manuell sichern, WorkSpaces bevor sie sich von ihrem Standby- abmelden WorkSpaces. Wenn sie sich erneut anmelden, werden sie zur primären Region und zu ihrem primären weitergeleitet WorkSpaces.

Sicherheit in Amazon WorkSpaces

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für WorkSpaces gelten, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

In dieser Dokumentation wird erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von WorkSpaces zum Tragen kommt. Es zeigt Ihnen, wie Sie WorkSpaces konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS-Services nutzen können, die Ihnen helfen, Ihre WorkSpaces-Ressourcen zu überwachen und zu schützen.

Inhalt

Datenschutz in Amazon WorkSpaces

Das Modell der AWS geteilten gilt für den Datenschutz in Amazon WorkSpaces. https://aws.amazon.com/compliance/shared-responsibility-model/ Wie in diesem Modell beschrieben, ist AWS für den Schutz der globalen Infrastruktur verantwortlich, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit WorkSpaces oder anderen AWS-Services über die Konsole, APIAWS CLI, oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen

Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Weitere Informationen zu WorkSpaces und zur FIPS-Endpunktverschlüsselung finden Sie unter Einrichten von Amazon WorkSpaces für die FedRAMP-Autorisierung oder DoD-SRG-Compliance.

Verschlüsselung im Ruhezustand

Sie können die Speicher-Volumes für Ihr WorkSpaces mit dem AWS KMS Schlüssel von verschlüsselnAWS Key Management Service. Weitere Informationen finden Sie unter Verschlüsselte WorkSpaces.

Wenn Sie WorkSpaces mit verschlüsselten Volumes erstellen, WorkSpaces verwendet Amazon Elastic Block Store (Amazon EBS), um diese Volumes zu erstellen und zu verwalten. EBS verschlüsselt Ihre Volumes mit einem Datenschlüssel mithilfe des in der Branche üblichen AES-256-Algorithmus. Weitere Informationen finden Sie unter Amazon-EC2-Verschlüsselung im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

Verschlüsselung während der Übertragung

Bei PCoIP werden Daten während der Übertragung mit der TLS-1.2-Verschlüsselung und SigV4-Anforderungssignatur verschlüsselt. Das PCoIP-Protokoll verwendet verschlüsselten UDP-Datenverkehr mit AES-Verschlüsselung für Streaming-Pixel. Die Streaming-Verbindung, die Port 4172 (TCP und UDP) verwendet, wird mit AES-128- und AES-256-Verschlüsselungen verschlüsselt, aber die Standardverschlüsselung ist 128-Bit. Sie können diesen Standardwert auf 256 Bit ändern, indem Sie entweder die Gruppenrichtlinieneinstellung PCoIP-Sicherheitseinstellungen für Windows konfigurieren WorkSpacesoder die PCoIP-Sicherheitseinstellungen in der `pcoip-agent.conf` Datei für Amazon Linux ändern WorkSpaces.

Weitere Informationen zur Gruppenrichtlinienverwaltung für Amazon finden Sie WorkSpacesunter Konfigurieren von PCoIP-Sicherheitseinstellungen in Verwalte dein Windows WorkSpaces. Weitere Informationen zum Ändern der `pcoip-agent.conf`-Datei finden Sie unter Steuern des Verhaltens von PCoIP-Agenten auf Amazon Linux WorkSpaces und PCoIP-Sicherheitseinstellungen in der Teradici-Dokumentation.

Für das WorkSpaces Streaming Protocol (WSP) werden Streaming- und Kontrolldaten während der Übertragung mit DTLS 1.2-Verschlüsselung für UDP-Datenverkehr und TLS 1.2-Verschlüsselung für TCP-Datenverkehr mit AES-256-Verschlüsselungen verschlüsselt.

Identitäts- und Zugriffsverwaltung für WorkSpaces

Standardmäßig haben IAM-Benutzer keine Berechtigungen für WorkSpaces-Ressourcen und -Vorgänge. Um IAM-Benutzern die Verwaltung von WorkSpaces-Ressourcen zu ermöglichen, erstellen Sie eine IAM-Richtlinie, die diesen ausdrücklich Berechtigungen erteilt. Anschließend fügen Sie die Richtlinie den IAM-Benutzern oder -Gruppen an, die diese Berechtigungen benötigen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Weitere allgemeine Informationen zu IAM-Richtlinien finden Sie unter Berechtigungen und Richtlinien im IAM-Benutzerhandbuch.

WorkSpaces erstellt auch eine IAM-Rolle (`workspaces_DefaultRole`), die dem WorkSpaces-Service den Zugriff auf die erforderlichen Ressourcen ermöglicht.

Weitere Informationen über IAM finden Sie unter Identity and Access Management (IAM) und im IAM-Benutzerhandbuch. Sie finden die WorkSpaces-spezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces im IAM-Benutzerhandbuch.

Ein Tool, mit dem Sie IAM-Richtlinien erstellen können, finden Sie im AWS Policy Generator. Sie können außerdem den IAM-Richtliniensimulator verwenden, um zu testen, ob eine Richtlinie eine bestimmte Anforderung an AWS zulässt oder verweigert.

> **Note**
>
> Amazon WorkSpaces unterstützt nicht die Bereitstellung von IAM-Anmeldeinformationen in einem WorkSpace (wie z. B. bei einem Instance-Profil).

Inhalt

Beispielrichtlinien

Die folgenden Beispiele veranschaulichen Richtlinienanweisungen, mit denen Sie die Berechtigungen, die IAM-Benutzer für Amazon WorkSpaces haben, kontrollieren können.

Example 1: Alle WorkSpaces-Aufgaben ausführen

Mit der folgenden Richtlinienanweisung werden IAM-Benutzer zum Ausführen aller WorkSpaces-Aufgaben berechtigt, einschließlich Erstellen und Verwalten von Verzeichnissen. Es erteilt auch die Berechtigung zum Ausführen der Schnellinstallationsprozedur.

Obwohl Amazon WorkSpaces die Elemente `Action` und AWS Management Console bei der Verwendung der API und der Befehlszeilentools vollständig unterstützt, müssen die IAM-Benutzer über Berechtigungen für die folgenden Aktionen und Ressourcen verfügen, um Amazon WorkSpaces von `Resource` aus verwenden zu können:

- Aktionen: „`workspaces:*`" und `"ds:*"`
- Ressourcen: `"Resource": "*"`

Die folgende Beispielrichtlinie zeigt, wie Sie IAM-Benutzern die Verwendung von Amazon WorkSpaces aus AWS Management Console ermöglichen.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Example 2: Führen Sie WorkSpace-spezifische Aufgaben durch

Die folgende Richtlinie erteilt IAM-Benutzern die Berechtigung zum Ausführen von WorkSpace-Aufgaben wie das Starten und Entfernen von WorkSpaces. In der Richtlinienanweisung gewährt die Aktion `ds:*` umfassende Berechtigungen, d. h. vollständige Kontrolle über alle Verzeichnisdienstobjekte des Kontos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Fügen Sie die `workdocs`-Operationen wie im folgenden Beispiel dargestellt hinzu, um Benutzern auch die Möglichkeit zu gewähren, Amazon WorkDocs für Benutzer innerhalb von WorkSpaces zu aktivieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

Damit der Benutzer den Launch WorkSpaces-Assistenten verwenden kann, fügen Sie die im folgenden Beispiel dargestellten kms-Operationen hinzu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3: Ausführen aller WorkSpaces-Aufgaben für BYOL-WorkSpaces

Die folgende Richtlinienanweisung gewährt einem IAM-Benutzer die Erlaubnis, alle WorkSpaces-Aufgaben auszuführen, einschließlich der Amazon-EC2-Aufgaben, die für die Erstellung von Bring-Your-Own-License (BYOL)-WorkSpaces erforderlich sind.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
```

```
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Angeben von WorkSpaces-Ressourcen in einer IAM-Richtlinie

Verwenden Sie den Amazon-Ressourcenname (ARN) der Ressource, um eine WorkSpaces-Ressource im `Resource`-Element der Richtlinie festzulegen. Sie kontrollieren den Zugriff auf Ihre WorkSpaces-Ressourcen, indem Sie die Berechtigungen zur Verwendung von im `Action`-Element Ihrer IAM-Richtlinienanweisung festgelegten API-Aktionen entweder erteilen oder verweigern. WorkSpaces definiert ARNs für WorkSpaces, Pakete, IP-Gruppen und Verzeichnisse.

WorkSpace-ARN

Ein WorkSpace-ARN besitzt die im folgenden Beispiel gezeigte Syntax.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

region

Die Region, in der sich der WorkSpace befindet (z. B. `us-east-1`).

account_id

Die ID des AWS-Kontos ohne Bindestriche (z. B. `123456789012`)

workspace_identifier

Die ID für den WorkSpace (z. B. `ws-a1bcd2efg`).

Das `Resource`-Element einer Richtlinie, das einen bestimmten WorkSpace identifiziert, weist das folgende Format auf.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

Sie können den Platzhalter * verwenden, um alle WorkSpaces anzugeben, die zu einem bestimmten Konto in einer bestimmten Region gehören.

Abbild-ARN

Ein WorkSpace-Abbild-ARN besitzt die im folgenden Beispiel gezeigte Syntax.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

region

Die Region, in der sich das WorkSpace-Abbild befindet (z. B. `us-east-1`).

account_id

Die ID des AWS-Kontos ohne Bindestriche (z. B. `123456789012`)

bundle_identifier

Die ID für das WorkSpace-Abbild (z. B. `wsi-a1bcd2efg`).

Das `Resource`-Element einer Richtlinienanweisung, das ein spezifisches Paket identifiziert, weist das folgende Format auf.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

Sie können den Platzhalter * verwenden, um alle WorkSpaces-Abbilder anzugeben, die zu einem bestimmten Konto in einer bestimmten Region gehören.

Bundle-ARN

Ein Bundle-ARN besitzt die im folgenden Beispiel gezeigte Syntax.

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

region

Die Region, in der sich der WorkSpace befindet (z. B. `us-east-1`).

account_id

Die ID des AWS-Kontos ohne Bindestriche (z. B. `123456789012`)

bundle_identifier

Die ID für das WorkSpace-Paket (z. B. `wsb-a1bcd2efg`).

Das `Resource`-Element einer Richtlinie, das ein spezifisches Bundle identifiziert, weist das folgende Format auf.

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

Sie können den Platzhalter * verwenden, um alle Pakete anzugeben, die zu einem bestimmten Konto in einer bestimmten Region gehören.

ARN der IP-Gruppe

Ein IP-Gruppen-ARN besitzt die im folgenden Beispiel gezeigte Syntax.

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

region

Die Region, in der sich der WorkSpace befindet (z. B. `us-east-1`).

account_id

Die ID des AWS-Kontos ohne Bindestriche (z. B. `123456789012`)

ipgroup_identifier

Die ID der IP-Gruppe (z. B. `wsipg-a1bcd2efg`).

Das `Resource`-Element einer Richtlinie, das eine bestimmte IP-Gruppe identifiziert, weist das folgende Format auf.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

Sie können den Platzhalter * verwenden, um alle IP-Gruppen anzugeben, die zu einem bestimmten Konto in einer bestimmten Region gehören.

Verzeichnis-ARN

Ein Verzeichnis ARN besitzt die im folgenden Beispiel gezeigte Syntax.

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

region

Die Region, in der sich der WorkSpace befindet (z. B. `us-east-1`).

account_id

Die ID des AWS-Kontos ohne Bindestriche (z. B. `123456789012`)

directory_identifier

Die ID des Verzeichnisses (z. B. `d-12345a67b8`).

Das `Resource`-Element einer Richtlinie, das eine bestimmte Richtlinienanweisung identifiziert, weist das folgende Format auf.

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

Sie können den Platzhalter * verwenden, um alle Verzeichnisse anzugeben, die zu einem bestimmten Konto in einer bestimmten Region gehören.

Verbindungsalias-ARN

Ein Verbindungsalias-ARN besitzt die im folgenden Beispiel gezeigte Syntax.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

region

Die Region, in der sich der Verbindungsalias befindet (z. B. `us-east-1`).

account_id

Die ID des AWS-Kontos ohne Bindestriche (z. B. `123456789012`)

connectionalias_identifier

Die ID des Verbindungsalias (z. B. `wsca-12345a67b8`).

Das `Resource`-Element einer Richtlinienanweisung, das einen bestimmten Verbindungsalias angibt, weist das folgende Format auf.

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

Sie können den Platzhalter * verwenden, um alle Verbindungsaliase anzugeben, die zu einem bestimmten Konto in einer bestimmten Region gehören.

API-Aktionen ohne Unterstützung für Berechtigungen auf Ressourcenebene

Mit den folgenden API-Aktionen können Sie keinen Ressourcen-ARN angeben:

- `AssociateIpGroups`
- `CreateIpGroup`
- `CreateTags`
- `DeleteTags`
- `DeleteWorkspaceImage`
- `DescribeAccount`
- `DescribeAccountModifications`
- `DescribeIpGroups`
- `DescribeTags`
- `DescribeWorkspaceDirectories`
- `DescribeWorkspaceImages`
- `DescribeWorkspaces`
- `DescribeWorkspacesConnectionStatus`
- `DisassociateIpGroups`
- `ImportWorkspaceImage`
- `ListAvailableManagementCidrRanges`
- `ModifyAccount`

Bei API-Aktionen, die Berechtigungen auf Ressourcenebene nicht unterstützen, müssen Sie die Ressourcenanweisung wie im folgenden Beispiel dargestellt angeben.

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

API-Aktionen, die Einschränkungen auf Kontoebene für gemeinsam genutzte Ressourcen nicht unterstützen

Für die folgenden API-Aktionen können Sie im Ressourcen-ARN keine Konto-ID angeben, wenn die Ressource nicht dem Konto gehört:

- `AssociateConnectionAlias`
- `CopyWorkspaceImage`
- `DisassociateConnectionAlias`

Für diese API-Aktionen können Sie nur dann eine Konto-ID im Ressourcen-ARN angeben, wenn dieses Konto die Ressourcen besitzt, die verwendet werden sollen. Wenn das Konto nicht Besitzer der Ressourcen ist, müssen Sie, wie im folgenden Beispiel veranschaulicht, für das Konto den Wert * angeben.

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

Erstellen der Rolle workspaces_DefaultRole

Bevor Sie ein Verzeichnis mithilfe der API registrieren können, müssen Sie überprüfen, ob eine Rolle mit dem Namen `workspaces_DefaultRole` existiert. Diese Rolle wird durch das Quick Setup, oder wenn Sie einen WorkSpace mit der AWS Management Console starten, erstellt und gewährt Amazon WorkSpaces die Berechtigung, in Ihrem Namen auf bestimmte AWS-Ressourcen zuzugreifen. Wenn diese Rolle nicht existiert, können Sie sie auf folgende Weise erstellen.

So erstellen Sie die Rolle workspaces_DefaultRole

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich auf der linken Seite Roles (Rollen).
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie unter Typ der vertrauenswürdigen Entität auswählen die Option Weiteres AWS-Konto aus.
5. Geben Sie für Account ID (Konto-ID) Ihre Konto-ID ohne Bindestriche oder Leerzeichen ein.
6. Geben Sie unter Options (Optionen) keine Multi-Faktor-Authentifizierung (MFA) an.
7. Wählen Sie Next: Permissions (Weiter: Berechtigungen) aus.

8. Wählen Sie auf der Seite Berechtigungsrichtlinien anhängen die verwalteten AWS-Richtlinien AmazonWorkSpacesServiceAccess und AmazonWorkSpacesesSelfServiceAccess aus.
9. Es wird empfohlen, unter Berechtigungsgrenze festlegen keine Berechtigungsgrenze zu verwenden, da Konflikte mit den Richtlinien auftreten können, die der Rolle workspaces_DefaultRole zugeordnet sind. Solche Konflikte könnten bestimmte erforderliche Berechtigungen für die Rolle blockieren.
10. Wählen Sie Next: Markierungen (Weiter: Markierungen).
11. Fügen Sie auf der Seite Add tags (optional) (Tags hinzufügen (optional)) Tags hinzu, sofern erforderlich.
12. Wählen Sie Weiter: Prüfen aus.
13. Geben Sie auf der Seite Review (Überprüfen) für Role name (Rollenname) **`workspaces_DefaultRole`** ein.
14. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung ein.
15. Wählen Sie Create Role aus.
16. Wählen Sie auf der Seite Summary (Zusammenfassung) für die Rolle workspaces_DefaultRole die Registerkarte Trust relationships (Vertrauensstellungen).
17. Wählen Sie auf der Registerkarte Trust relationships (Vertrauensstellungen) die Option Edit trust relationship (Vertrauensstellung bearbeiten).
18. Ersetzen Sie auf der Seite Edit Trust Relationship (Vertrauensstellung bearbeiten) die vorhandene Richtlinienanweisung durch die folgende Anweisung.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. Wählen Sie Update Trust Policy (Trust Policy aktualisieren).

Erstellen der Servicerolle AmazonWorkSpacesPCAAccess

Bevor sich Benutzer mit zertifikatbasierter Authentifizierung anmelden können, müssen Sie überprüfen, ob eine Rolle mit dem Namen `AmazonWorkSpacesPCAAccess` existiert. Diese Rolle wird erstellt, wenn Sie die zertifikatbasierte Authentifizierung für ein Verzeichnis mithilfe von AWS Management Console aktivieren. Sie gewährt Amazon WorkSpaces die Berechtigung, in Ihrem Namen auf AWS Private CA-Ressourcen zuzugreifen. Wenn diese Rolle nicht existiert, weil Sie die Konsole nicht zur Verwaltung der zertifikatbasierten Authentifizierung verwenden, können Sie sie mit dem folgenden Verfahren erstellen.

So erstellen Sie die Servicerolle AmazonWorkSpacesPCAAccess mit der AWS CLI

1. Erstellen Sie eine JSON-Datei namens `AmazonWorkSpacesPCAAccess.json` mit dem folgenden Text.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Passen Sie den `AmazonWorkSpacesPCAAccess.json`-Pfad nach Bedarf an und führen Sie die folgenden AWS CLI-Befehle aus, um die Servicerolle zu erstellen und die verwaltete AmazonWorkspacesPCAAccess-Richtlinie anzuhängen.

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

Von AWS verwaltete Richtlinien für WorkSpaces

Wenn Sie Benutzern, Gruppen und Rollen Berechtigungen hinzufügen wollen, ist es einfacher, von AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu erstellen. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Sie können von AWS verwaltete Richtlinien verwenden, um schnell loszulegen. Diese Richtlinien decken häufige Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu verwalteten AWS-Richtlinien finden Sie unter Verwaltete AWS-Richtlinien im IAM-Leitfaden.

AWS-Services pflegen und Aktualisieren von verwalteten AWS-Richtlinien. Die Berechtigungen in von AWS verwalteten Richtlinien können nicht geändert werden. Services fügen einer von AWS verwalteten Richtlinie möglicherweise gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Services entfernen keine Berechtigungen aus einer von AWS verwalteten Richtlinie, sodass Richtlinien-Aktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

Darüber hinaus unterstützt AWS verwaltete Richtlinien für Auftragsfunktionen, die mehrere Services umfassen. Die von AWS verwaltete Richtlinie `ReadOnlyAccess` bietet beispielsweise schreibgeschützten Zugriff auf alle AWS-Services und -Ressourcen. Wenn ein Service ein neues Feature startet, fügt AWS schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS-Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Von AWS verwaltete Richtlinie: AmazonWorkSpacesAdmin

Diese Richtlinie ermöglicht administrative Aktivitäten für Amazon WorkSpaces. Sie stellt die folgenden Berechtigungen bereit:

- `workspaces` – Ermöglicht den Zugriff auf administrative Aktionen für WorkSpaces-Ressourcen.
- `kms` – Ermöglicht den Zugriff auf das Auflisten und Beschreiben von KMS-Schlüsseln sowie das Auflisten von Aliasnamen.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

Von AWS verwaltete Richtlinie: AmazonWorkspacesPCAAccess

Diese verwaltete Richtlinie ermöglicht den Zugriff auf die Ressourcen der AWS Certificate Manager Private Certificate Authority (Private CA) in Ihrem AWS-Konto für die zertifikatbasierte Authentifizierung. Sie ist in der Rolle AmazonWorkSpacesPCAAccess enthalten und bietet die folgenden Berechtigungen:

- `acm-pca` – Ermöglicht den Zugriff auf AWS Private CA zur Verwaltung der zertifikatbasierten Authentifizierung.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

Von AWS verwaltete Richtlinie: AmazonWorkSpacesSelfServiceAccess

Diese Richtlinie bietet Zugriff auf den Amazon-WorkSpaces-Service, um WorkSpaces-Self-Service-Aktionen durchzuführen, die von Benutzern initiiert wurden. Sie ist in der Rolle `workspaces_DefaultRole` enthalten und bietet die folgenden Berechtigungen:

- `workspaces` - Ermöglicht Self-Service-WorkSpace-Verwaltungsfunktionen für Benutzer.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Von AWS verwaltete Richtlinie: AmazonWorkSpacesServiceAccess

Diese Richtlinie gewährt Kundenkonten Zugriff auf den Amazon-WorkSpaces-Service, um einen WorkSpace zu starten. Sie ist in der Rolle `workspaces_DefaultRole` enthalten und bietet die folgenden Berechtigungen:

- `ec2` – Ermöglicht den Zugriff auf die Verwaltung von Amazon-EC2-Ressourcen, die einem WorkSpace zugeordnet sind, wie z. B. Netzwerkschnittstellen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

WorkSpaces-Updates für von AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für von AWS verwaltete Richtlinien für WorkSpaces, seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat.

Änderung	Beschreibung	Datum
the section called “AmazonWorkSpacesAdmin” – Aktualisierte Richtlinie	WorkSpaces hat die `workspaces:RestoreWorkspace` -Aktion zur von Amazon verwalteten Richtlinie WorkSpacesAdmin hinzugefügt und Administratoren Zugriff	25. Juni 2023

Änderung	Beschreibung	Datum
	auf die Wiederherstellung von WorkSpaces gewährt.	
the section called “AmazonWorkspacesPCAAccess” – Neue Richtlinie hinzugefügt.	WorkSpaces hat eine neue, verwaltete Richtlinie hinzugefügt, um die `acm-pca`-Berechtigung zur Verwaltung von AWS Private CA zur Verwaltung der zertifikatbasierten Authentifizierung zu erteilen.	18. November 2022
WorkSpaces hat mit der Änderungsverfolgung begonnen	WorkSpaces hat mit der Verfolgung von Änderungen für seine verwalteten WorkSpace-Richtlinien begonnen.	1. März 2021

Compliance-Validierung für Amazon WorkSpaces

Externe Prüfer bewerten im Rahmen verschiedener AWS-Compliance-Programme die Sicherheit und Compliance von Amazon WorkSpaces. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS-Services im Bereich bestimmter Compliance-Programme finden Sie unter AWS-Services im Bereich nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Weitere Informationen zu WorkSpaces und FedRAMP finden Sie unter Einrichten von Amazon WorkSpaces für die FedRAMP-Autorisierung oder DoD-SRG-Compliance.

Ihre Compliance-Verantwortung bei der Verwendung von WorkSpaces ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Schnellstartanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von sicherheits- und konformitätsorientierten Basisumgebungen auf AWS angegeben.
- Erstellen einer Architektur für HIPAA-Sicherheit und -Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS Compliance Ressourcen – Diese Sammlung von Arbeitsbüchern und Leitfäden könnte auf Ihre Branche und Ihren Standort zutreffen.
- Evaluating Resources with Rules in the AWS Config Developer Guide – AWS Config; assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Ausfallsicherheit in Amazon WorkSpaces

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und -Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Amazon WorkSpaces bietet außerdem eine regionsübergreifende Umleitung – eine Funktion, die mit Ihren DNS-Failover-Routing-Richtlinien (Domain Name System) arbeitet, die Ihre WorkSpaces-Benutzer zu alternativen WorkSpaces in einer anderen AWS-Region umleiten, wenn ihre primären WorkSpaces nicht verfügbar sind. Weitere Informationen finden Sie unter Regionsübergreifende Umleitung für Amazon WorkSpaces.

Sicherheit der Infrastruktur in Amazon WorkSpaces

Als verwalteter Service ist Amazon WorkSpaces durch die globale Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf WorkSpaces zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Netzwerkisolierung

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk in Ihrem eigenen logisch isolierten Bereich in der AWS Cloud. Sie können Ihre WorkSpaces in einem privaten Subnetz in Ihrer VPC bereitstellen. Weitere Informationen finden Sie unter Konfigurieren einer VPC für WorkSpaces.

Um Datenverkehr nur aus bestimmten Adressbereichen (z. B. aus Ihrem Unternehmensnetzwerk) zuzulassen, aktualisieren Sie die Sicherheitsgruppe für Ihre VPC oder verwenden Sie eine IP-Zugriffssteuerungsgruppe.

Sie können den WorkSpace-Zugriff auf vertrauenswürdige Geräte mit gültigen Zertifikaten einschränken. Weitere Informationen finden Sie unter Beschränken des WorkSpaces Zugriffs auf vertrauenswürdige Geräte.

Isolierung auf physischen Hosts

Unterschiedliche WorkSpaces auf demselben physischen Host werden über den Hypervisor voneinander isoliert. Es ist, als ob sie sich auf separaten physischen Hosts befinden. Wenn ein

WorkSpace gelöscht wird, wird der ihm zugewiesene Arbeitsspeicher vom Hypervisor gestrichen (auf Null gesetzt), bevor er einem neuen WorkSpace zugewiesen wird.

Autorisierung von Unternehmensbenutzern

Mit WorkSpaces werden Verzeichnisse über AWS Directory Service verwaltet. Sie können ein eigenständiges, verwaltetes Verzeichnis für Benutzer erstellen. Es ist auch eine Integration in Ihrer vorhandenen Active Directory-Umgebung möglich, sodass Ihre Benutzer ihre aktuellen Anmeldeinformationen verwenden können, um nahtlosen Zugriff auf Unternehmensressourcen zu erhalten. Weitere Informationen finden Sie unter Verwalten von Verzeichnissen für WorkSpaces.

Um den Zugriff auf Ihre WorkSpaces weiter zu steuern, verwenden Sie die Multi-Faktor-Authentifizierung. Weitere Informationen finden Sie unter So aktivieren Sie die Multi-Factor Authentication für AWS-Services.

Durchführen von Amazon-WorkSpaces-API-Anforderungen über einen VPC-Schnittstellenendpunkt

Sie können über einen Schnittstellenendpunkt in Ihrer Virtual Private Cloud (VPC) eine direkte Verbindung mit Amazon-WorkSpaces-API-Endpunkten herstellen, anstatt sich über das Internet zu verbinden. Wenn Sie einen VPC-Schnittstellenendpunkt verwenden, findet die Kommunikation zwischen Ihrer VPC und dem Amazon-WorkSpaces-API-Endpunkt vollständig und sicher innerhalb des AWS-Netzwerks statt.

> **Note**
>
> Diese Funktion kann nur zum Verbinden mit WorkSpaces-API-Endpunkten verwendet werden. Um mithilfe der WorkSpaces-Clients eine Verbindung mit WorkSpaces herzustellen, ist eine Internetverbindung erforderlich, wie unter IP-Adresse und Port-Anforderungen für WorkSpaces beschrieben.

Die Amazon-WorkSpaces-API-Endpunkte unterstützen Amazon-Virtual-Private-Cloud-Schnittstellenendpunkte (Amazon VPC), die von AWS PrivateLink bereitgestellt werden. Jeder VPC-Endpunkt wird durch eine oder mehrere Netzwerkschnittstellen (auch als Elastic Network-Schnittstellen oder ENIs bezeichnet) mit privaten IP-Adressen in Ihren VPC-Subnetzen dargestellt.

Der VPC-Schnittstellenendpunkt verbindet Ihre VPC ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung direkt mit dem Amazon-WorkSpaces-

API-Endpunkt. Die Instances in Ihrer VPC benötigen für die Kommunikation mit dem Amazon-WorkSpaces-API-Endpunkt keine öffentlichen IP-Adressen.

Sie können einen Schnittstellenendpunkt erstellen, um entweder über die Befehle AWS Management Console oder AWS Command Line Interface (AWS CLI) eine Verbindung mit Amazon WorkSpaces herzustellen. Anweisungen finden Sie unter Erstellen eines Schnittstellenendpunkts.

Nachdem Sie einen VPC-Endpunkt erstellt haben, können Sie die folgenden CLI-Beispielbefehle mit dem Parameter `endpoint-url` zur Angabe von Schnittstellenendpunkten für die Amazon-WorkSpaces-API verwenden:

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

Wenn Sie private DNS-Hostnamen für Ihren VPC-Endpunkt aktivieren, müssen Sie die Endpunkt-URL nicht angeben. Der Amazon-WorkSpaces-API-DNS-Hostname, den die CLI und das Amazon-WorkSpaces-SDK standardmäßig verwenden (https://api.workspaces.*Region*.amazonaws.com), wird in Ihren VPC-Endpunkt aufgelöst.

Der Amazon-WorkSpaces-API-Endpunkt unterstützt VPC-Endpunkte in allen AWS-Regionen, in denen sowohl Amazon VPC als auch Amazon WorkSpaces verfügbar sind. Amazon-WorkSpaces unterstützt Aufrufe aller öffentlichen APIs innerhalb Ihrer VPC.

Weitere Informationen zu AWS PrivateLink finden Sie in der AWS PrivateLink-Dokumentation. Informationen zum Preis von VPC-Endpunkten finden Sie unter VPC-Preisgestaltung. Unter Amazon VPC erfahren Sie mehr über die VPC und Endpunkte.

Eine Liste der Amazon-WorkSpaces-API-Endpunkte nach Region finden Sie unter WorkSpaces-API-Endpunkte.

> **Note**
>
> Amazon-WorkSpaces-API-Endpunkte mit AWS PrivateLink werden für FIPS (Federal Information Processing Standard)-Amazon-WorkSpaces-API-Endpunkte nicht unterstützt.

Erstellen einer VPC-Endpunktrichtlinie für Amazon WorkSpaces.

Sie können eine Richtlinie für Amazon-VPC-Endpunkte für Amazon WorkSpaces erstellen, in der Sie Folgendes angeben:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC User Guide.

> **Note**
>
> VPC-Endpunktrichtlinien werden nicht für Federal-Information-Processing-Standard-(FIPS)-Amazon-WorkSpaces-Endpunkte unterstützt.

Das folgende Beispiel für eine VPC-Endpunktrichtlinie legt fest, dass alle Benutzer, die Zugriff auf den VPC-Schnittstellenendpunkt haben, auch den von Amazon WorkSpaces gehosteten Endpunkt mit dem Namen `ws-f9abcdefg` aufrufen können.

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
```

```
}
```

In diesem Beispiel werden die folgenden Aktionen verweigert:

- Aufrufen anderer von Amazon WorkSpaces gehosteter Endpunkte als `ws-f9abcdefg`.
- Ausführen einer Aktion für eine beliebige Ressource außer der angegebenen (WorkSpace-ID: `ws-f9abcdefg`).

> **Note**
>
> In diesem Beispiel können Benutzer weiterhin andere Amazon-WorkSpaces-API-Aktionen von außerhalb der VPC durchführen. Informieren Sie sich unter Identitäts- und Zugriffsverwaltung für WorkSpaces über die Verwendung identitätsbasierter Richtlinien zum Steuern des Zugriffs auf Amazon-WorkSpaces-API-Endpunkte, um API-Aufrufe auf solche innerhalb der VPC zu beschränken.

Verbinden Ihres privaten Netzwerks mit Ihrer VPC

Sie müssen für die Verbindung entweder eine Instance innerhalb Ihrer VPC verwenden oder Ihr privates Netzwerk mit Ihrer VPC verbinden, um sich über Ihre VPC mit der Amazon-WorkSpaces-API verbinden zu können. Dies erreichen Sie mithilfe von AWS Virtual Private Network (AWS VPN) oder AWS Direct Connect. Weitere Informationen finden Sie unter VPN-Verbindungen im Benutzerhandbuch für Amazon Virtual Private Cloud. Informationen zu AWS Direct Connect finden Sie unter Erstellen einer Verbindung im AWS Direct Connect-Benutzerhandbuch.

Aktualisierungsverwaltung in WorkSpaces

Wir empfehlen Ihnen, das Betriebssystem und die Anwendungen auf Ihrem regelmäßig zu patchen, zu aktualisieren und zu sichern WorkSpaces. Sie können Ihre so konfigurieren WorkSpaces , dass sie von WorkSpaces während eines regulären Wartungsfensters aktualisiert werden, oder Sie können sie selbst aktualisieren. Weitere Informationen finden Sie unter Warten von WorkSpace.

Für Anwendungen in Ihrem können Sie alle bereitgestellten automatischen WorkSpacesAktualisierungsservices verwenden oder die Empfehlungen für die Installation von Updates befolgen, die vom Anwendungsanbieter bereitgestellt werden.

Probleme WorkSpaces beheben

Die folgenden Informationen können Ihnen bei der Behebung von Problemen mit Ihrem helfen WorkSpaces.

Aktivieren der erweiterten Protokollierung

Um Probleme zu beheben, die bei Ihren Benutzern auftreten könnten, können Sie die erweiterte Protokollierung auf jedem WorkSpaces Amazon-Client aktivieren.

Die erweiterte Protokollierung erstellt Protokolldateien mit Diagnoseinformationen und Details auf Debugging-Ebene, einschließlich Verbose-Leistungsdaten. Für die Clients ab Version 1.0 und 2.0 werden diese erweiterten Logging-Dateien automatisch in eine Datenbank in hochgeladen. AWS

> **Note**
>
> Wenden Sie sich an, um eine AWS Übersicht über die erweiterten Protokolldateien zu erhalten und technischen Support bei Problemen mit Ihren WorkSpaces Kunden zu erhalten. AWS Support Weitere Informationen finden Sie unter AWS Support -Center.

So aktivieren Sie die erweiterte Protokollierung für Web Access

So aktivieren Sie die erweiterte Protokollierung für Web Access

1. Öffnen Sie Ihren Amazon WorkSpaces Web Access-Client.
2. Wählen Sie oben auf der WorkSpaces Anmeldeseite die Option Diagnoseprotokollierung aus.
3. Vergewissern Sie sich, dass im Pop-up-Dialogfeld die Option Diagnoseprotokollierung aktiviert ist.
4. Wählen Sie unter Protokollebene die Option Erweiterte Protokollierung aus.

So greifen Sie in Google Chrome, Microsoft Edge und Firefox auf Protokolldateien zu

1. Öffnen Sie das Kontextmenü (Rechtsklick) des Browsers oder drücken Sie STRG + UMSCHALT + I (oder für Mac BEFEHL + OPTION + I) auf Ihrer Tastatur, um den Entwicklertools-Bereich zu öffnen.

2. Wählen Sie im Entwicklertools-Bereich die Registerkarte Konsole aus, um nach den Protokolldateien zu suchen.

So greifen Sie in Safari auf Protokolldateien zu

1. Wählen Sie Safari, Einstellungen aus.
2. Wählen Sie auf der Registerkarte Erweitert die Option Einstellungen aus.
3. Wählen Sie Entwickeln-Menü in der Menüleiste anzeigen aus.
4. Wählen Sie in der Menüleiste auf der Registerkarte Entwickeln die Option Entwickeln > Web Inspector einblenden aus.
5. Wählen Sie im Web-Inspector-Bereich von Safari die Registerkarte Konsole aus, um nach den Protokolldateien zu suchen.

So aktivieren Sie die erweiterte Protokollierung für 4.0+ Clients

Die Windows-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

So aktivieren Sie die erweiterte Protokollierung für Windows-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.
2. Öffnen Sie die Eingabeaufforderungs-App.
3. Starten Sie den WorkSpaces Client mit der `-l3` Flagge.

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> Wenn WorkSpaces es für einen Benutzer und nicht für alle Benutzer installiert ist, verwenden Sie die folgenden Befehle:
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> ```

```
workspaces.exe -l3
```

Die macOS-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

So aktivieren Sie die erweiterte Protokollierung für macOS-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.
2. Öffnen Sie das Terminal.
3. Führen Sie den folgenden Befehl aus.

```
open -a workspaces --args -l3
```

So aktivieren Sie die erweiterte Protokollierung für Android-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.
2. Öffnen Sie das Android-Client-Menü.
3. Wählen Sie Support aus.
4. Wählen Sie Protokollierungseinstellungen aus.
5. Wählen Sie Erweiterte Protokollierung aktivieren aus.

Gehen Sie wie folgt vor, um Protokolle für Android-Clients abzurufen, nachdem Sie die erweiterte Protokollierung aktiviert haben:

- Wählen Sie Protokoll extrahieren aus, um komprimierte Protokolle lokal zu speichern.

Die Linux-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

So aktivieren Sie die erweiterte Protokollierung für Linux-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.
2. Öffnen Sie das Terminal.

3. Führen Sie den folgenden Befehl aus.

```
/opt/workspacesclient/workspacesclient -l3
```

So aktivieren Sie die erweiterte Protokollierung für 3.0 Clients

Die Windows-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

So aktivieren Sie die erweiterte Protokollierung für Windows-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.
2. Öffnen Sie die Eingabeaufforderungs-App.
3. Starten Sie den WorkSpaces Client mit der `-l3` Flagge.

```
c:

cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> Wenn WorkSpaces es für einen Benutzer und nicht für alle Benutzer installiert ist, verwenden Sie die folgenden Befehle:
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> workspaces.exe -l3
> ```

Die macOS-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

So aktivieren Sie die erweiterte Protokollierung für macOS-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.

2. Öffnen Sie das Terminal.
3. Führen Sie den folgenden Befehl aus.

```
open -a workspaces --args -l3
```

So aktivieren Sie die erweiterte Protokollierung für Android-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.
2. Öffnen Sie das Android-Client-Menü.
3. Wählen Sie Support aus.
4. Wählen Sie Protokollierungseinstellungen aus.
5. Wählen Sie Erweiterte Protokollierung aktivieren aus.

Gehen Sie wie folgt vor, um Protokolle für Android-Clients abzurufen, nachdem Sie die erweiterte Protokollierung aktiviert haben:

- Wählen Sie Protokoll extrahieren aus, um komprimierte Protokolle lokal zu speichern.

Die Linux-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

So aktivieren Sie die erweiterte Protokollierung für Linux-Clients

1. Schließen Sie den WorkSpaces Amazon-Client.
2. Öffnen Sie das Terminal.
3. Führen Sie den folgenden Befehl aus.

```
/opt/workspacesclient/workspacesclient -l3
```

So aktivieren Sie die erweiterte Protokollierung für 1.0+ und 2.0+ Clients

1. Öffnen Sie den WorkSpaces Client.
2. Wählen Sie das Zahnradsymbol in der oberen rechten Ecke der Client-Anwendung aus.
3. Wählen Sie Advanced settings (Erweiterte Einstellungen) aus.

4. Aktivieren Sie das Kontrollkästchen Enable Advanced Logging (Erweiterte Protokollierung aktivieren).
5. Wählen Sie Speichern.

Die Windows-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

Die macOS-Clientprotokolle werden am folgenden Speicherort gespeichert:

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

Beheben von spezifischen Problemen

Die folgenden Informationen können Ihnen bei der Behebung bestimmter Probleme mit Ihrem helfen WorkSpaces.

Problembereiche

- Ich kann kein Amazon Linux erstellen WorkSpace , da der Benutzername ungültige Zeichen enthält
- Ich habe die Shell für mein Amazon Linux geändert WorkSpace und kann jetzt keine PCoIP-Sitzung bereitstellen
- Mein Amazon Linux WorkSpaces startet nicht
- Der Start WorkSpaces in meinem verbundenen Verzeichnis schlägt häufig fehl
- Das Starten WorkSpaces schlägt mit einem internen Fehler fehl
- Wenn ich versuche, ein Verzeichnis zu registrieren, schlägt die Registrierung fehl und das Verzeichnis erhält den Status FEHLER
- Meine Benutzer können mit einem interaktiven Anmeldebanner keine Verbindung zu WorkSpace einem Windows herstellen
- Meine Benutzer können keine Verbindung zu einem Windows-Computer herstellen WorkSpace
- Meine Benutzer haben Probleme, wenn sie versuchen, sich WorkSpaces über WorkSpaces Web Access anzumelden
- Der WorkSpaces Amazon-Client zeigt für eine Weile einen grauen Bildschirm mit der Aufschrift „Wird geladen...“ an, bevor er zum Anmeldebildschirm zurückkehrt. Es wird keine andere Fehlermeldung angezeigt.

- Meine Benutzer erhalten die Meldung "WorkSpace Status: Ungesund. Wir konnten Sie nicht mit Ihrem WorkSpace verbinden. Please try again in a few minutes."
- Meine Benutzer erhalten die Meldung „Dieses Gerät ist nicht berechtigt, auf das WorkSpace zuzugreifen. Please contact your administrator for assistance." (Dieses Gerät ist nicht berechtigt, auf den WorkSpace zuzugreifen. Wenden Sie sich an Ihren Administrator, um Unterstützung zu erhalten.)
- Meine Benutzer erhalten die Meldung „Kein Netzwerk. Netzwerkverbindung verloren. Überprüfen Sie Ihre Netzwerkverbindung oder kontaktieren Sie Ihren Administrator.“ wenn Sie versuchen, eine Verbindung zu einem WSP herzustellen WorkSpace
- Der WorkSpaces Client gibt meinen Benutzern einen Netzwerkfehler, aber sie können andere netzwerkfähige Apps auf ihren Geräten verwenden
- Meinen WorkSpace Benutzern wird die folgende Fehlermeldung angezeigt: „Das Gerät kann keine Verbindung zum Registrierungsservice herstellen. Check your network settings.“
- Meine PCoIP-Null-Client-Benutzer erhalten die Fehlermeldung „Das angegebene Zertifikat ist aufgrund des Zeitstempels ungültig“.
- USB-Drucker und andere USB-Peripheriegeräte funktionieren nicht für PCoIP-Zero-Clients
- Meine Benutzer haben die Aktualisierung ihrer Windows- oder macOS-Clientanwendungen übersprungen und werden nicht aufgefordert, die neueste Version zu installieren.
- Meine Benutzer können die Android-Clientanwendung nicht auf ihren Chromebooks installieren
- Meine Benutzer erhalten keine Einladungs-E-Mails oder E-Mails zum Zurücksetzen des Passworts.
- Meine Benutzer sehen die Option „Passwort vergessen?“ auf dem Client-Anmeldebildschirm.
- Ich erhalte die Meldung „Der Systemadministrator hat Richtlinien festgelegt, um diese Installation zu verhindern“, wenn ich versuche, Anwendungen unter Windows zu installieren WorkSpace
- Nein, WorkSpaces in meinem Verzeichnis kann ich eine Verbindung zum Internet herstellen
- Mein WorkSpace hat seinen Internetzugang verloren
- Ich erhalte die Fehlermeldung „DNS unavailable“, wenn ich eine Verbindung zu meinem on-premises Verzeichnis herstellen möchte
- Ich erhalte die Fehlermeldung „Connectivity issues detected“, wenn ich eine Verbindung zu meinem on-premises Verzeichnis herstellen möchte
- Ich erhalte die Fehlermeldung „SRV record“, wenn ich eine Verbindung zu meinem on-premises Verzeichnis herstellen möchte
- Mein Windows WorkSpace wechselt in den Standbymodus, wenn es inaktiv bleibt
- Einer von mir WorkSpaces hat einen Zustand von UNHEALTHY

- Mein stürzt WorkSpace unerwartet ab oder wird neu gestartet
- Derselbe Benutzername hat mehrere WorkSpace, aber der Benutzer kann sich nur mit einem der WorkSpaces
- Ich habe Probleme, Docker mit Amazon zu verwenden WorkSpaces
- Ich erhalte ThrottlingException bei einigen meiner API-Aufrufe Fehler
- Meine Verbindung WorkSpace wird immer wieder unterbrochen, wenn ich sie im Hintergrund laufen lasse
- SAML-2.0-Verbund funktioniert nicht. Meine Benutzer sind nicht berechtigt, ihren WorkSpaces Desktop zu streamen.
- Meine Benutzer werden alle 60 Minuten von ihrer WorkSpaces Sitzung getrennt.
- Meine Benutzer erhalten einen Umleitungs-URI-Fehler, wenn sie einen Verbund mithilfe des vom SAML 2.0-Identitätsanbieter (IdP) initiierten Flow herstellen, oder es wird jedes Mal, wenn meine Benutzer versuchen, sich nach dem Verbund mit dem IdP vom WorkSpaces Client aus anzumelden, eine zusätzliche Instanz der Client-Anwendung gestartet.
- Meine Benutzer erhalten die Meldung „Etwas ist schief gelaufen: Beim Starten Ihrer Datei ist ein Fehler aufgetreten WorkSpace“, wenn sie versuchen, sich nach dem Verbund mit dem IdP bei der WorkSpaces Client-Anwendung anzumelden.
- Meine Benutzer erhalten die Meldung „Tags können nicht validiert werden“, wenn sie versuchen, sich nach dem Verbund mit dem IdP bei der WorkSpaces Client-Anwendung anzumelden.
- Meine Benutzer erhalten die Meldung „Der Client und der Server können nicht kommunizieren, da sie keinen gemeinsamen Algorithmus haben“.
- Mein Mikrofon oder meine Webcam funktionieren unter Windows nicht. WorkSpaces
- Meine Benutzer können sich nicht mit zertifikatsbasierter Authentifizierung anmelden und werden entweder auf dem WorkSpaces Client- oder auf dem Windows-Anmeldebildschirm zur Eingabe des Kennworts aufgefordert, wenn sie eine Verbindung zu ihrer Desktopsitzung herstellen.
- Ich versuche, etwas zu tun, für das Windows-Installationsmedien erforderlich sind, die aber WorkSpaces nicht bereitgestellt werden.
- Ich möchte WorkSpaces mit einem vorhandenen AWS verwalteten Verzeichnis starten, das in einer nicht unterstützten WorkSpaces Region erstellt wurde.
- Ich möchte Firefox auf Amazon Linux 2 aktualisieren.
- Mein Benutzer kann sein Passwort mithilfe des WorkSpaces Clients zurücksetzen und ignoriert dabei die Einstellung Fine Grained Password Policy (FFGP), die für konfiguriert ist. AWS Managed Microsoft AD

Ich kann kein Amazon Linux erstellen WorkSpace , da der Benutzername ungültige Zeichen enthält

Für Amazon Linux WorkSpaces sind die Benutzernamen:

- Kann maximal 20 Zeichen enthalten
- Kann Buchstaben, Leerzeichen und Zahlen enthalten, die in UTF-8 darstellbar sind
- Kann folgende Sonderzeichen enthalten: _ .-#
- Kann nicht mit einem Bindestrich (-) als erstes Zeichen des Benutzernamens beginnen

> **Note**
>
> Diese Einschränkungen gelten nicht für Windows WorkSpaces. Windows WorkSpaces unterstützt die Symbole @ und - für alle Zeichen im Benutzernamen.

Ich habe die Shell für mein Amazon Linux geändert WorkSpace und kann jetzt keine PCoIP-Sitzung bereitstellen

Informationen zum Überschreiben der Standard-Shell für Linux finden Sie WorkSpaces unter. Überschreiben der Standard-Shell für Amazon Linux WorkSpaces

Mein Amazon Linux WorkSpaces startet nicht

Ab dem 20. Juli 2020 WorkSpaces wird Amazon Linux neue Lizenzzertifikate verwenden. Diese neuen Zertifikate sind nur mit den Versionen 2.14.1.1, 2.14.7, 2.14.9 und 20.10.6 oder höher des PCoIP-Agents kompatibel.

Wenn Sie eine nicht unterstützte Version des PCoIP-Agents verwenden, müssen Sie sie auf die neueste Version (20.10.6) aktualisieren. Diese enthält die neuesten Korrekturen und Leistungsverbesserungen, die mit den neuen Zertifikaten kompatibel sind. Wenn Sie diese Upgrades nicht bis zum 20. Juli durchführen, schlägt die Sitzungsbereitstellung für Ihr Linux WorkSpaces fehl und Ihre Endbenutzer können keine Verbindung zu ihren WorkSpaces herstellen.

So führen Sie ein Upgrade Ihres PCoIP-Agents auf die neueste Version durch

1. Öffnen Sie die WorkSpaces Konsole unter https://console.aws.amazon.com/workspaces/.

2. Wählen Sie im Navigationsbereich aus WorkSpaces.
3. Wählen Sie Ihr Linux aus und starten Sie es neu WorkSpace, indem Sie Aktionen, Neustart wählen WorkSpaces. Wenn der WorkSpace Status lautet`STOPPED`, müssen Sie Aktionen, Start WorkSpaces zuerst wählen und warten, bis der Status angezeigt wird, `AVAILABLE` bevor Sie es neu starten können.
4. Nachdem Ihr WorkSpace Computer neu gestartet wurde und sein Status lautet`AVAILABLE`, empfehlen wir Ihnen, den Status des WorkSpace zu ändern, `ADMIN_MAINTENANCE` während Sie dieses Upgrade durchführen. Wenn Sie fertig sind, ändern Sie den Status von zu. WorkSpace `AVAILABLE` Weitere Informationen zum `ADMIN_MAINTENANCE`-Modus finden Sie unter Manuelle Wartung.

   Gehen Sie wie folgt vor`ADMIN_MAINTENANCE`, WorkSpace um den Status eines Ziels zu ändern:

   a. Wählen Sie die aus WorkSpace und wählen Sie Aktionen, Ändern WorkSpace.
   b. Wählen Sie Modify State (Status ändern).
   c. Wählen Sie für Beabsichtigter Status ADMIN_MAINTENANCE aus.
   d. Wählen Sie Ändern aus.
5. Stellen Sie WorkSpace über SSH eine Connect zu Ihrem Linux her. Weitere Informationen finden Sie unter Aktivieren von SSH-Verbindungen für Linux WorkSpaces.
6. Führen Sie den folgenden Befehl aus, um den PCoIP-Agent zu aktualisieren:

   ```
   sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
   ```
7. Führen Sie den folgenden Befehl aus, um die Agentenversion zu überprüfen und zu bestätigen, dass das Update erfolgreich war:

   ```
   rpm -q pcoip-agent-standard
   ```

   Der Befehl sollte zu folgendem Ergebnis führen:

   ```
   pcoip-agent-standard-20.10.6-1.el7.x86_64
   ```
8. Trennen Sie die Verbindung zum WorkSpace und starten Sie es erneut.
9. Wenn Sie den Status auf `ADMIN_MAINTENANCE` In gesetzt habenStep 4, wiederholen WorkSpace Sie den Vorgang Step 4 und setzen Sie den gewünschten Status auf`AVAILABLE`.

Wenn Ihr Linux nach dem Upgrade des PCoIP-Agenten WorkSpace immer noch nicht startet, wenden AWS Sie sich an den Support.

Der Start WorkSpaces in meinem verbundenen Verzeichnis schlägt häufig fehl

Stellen Sie sicher, dass die zwei DNS-Server oder Domain-Controller in Ihrem on-premises Verzeichnis über die einzelnen Subnetze zugänglich sind, die Sie angegeben haben, als Sie sich mit Ihrem Verzeichnis verbunden haben. Sie können dies überprüfen, indem Sie in den einzelnen Subnetzen eine Amazon-EC2-Instance starten und mit dieser über die IP-Adressen der beiden DNS-Server Ihrem Verzeichnis beitreten.

Das Starten WorkSpaces schlägt mit einem internen Fehler fehl

Überprüfen Sie, ob Ihre Subnetze so konfiguriert sind, dass sie automatisch IPv6-Adressen an Instances zuweisen, die im Subnetz gestartet wurden. Zur Überprüfung dieser Einstellung öffnen Sie die Amazon-VPC-Konsole und wählen Ihr Subnetz und anschließend Subnetzaktionen, Automatisch zugewiesene IP-Einstellungen ändern aus. Wenn diese Einstellung aktiviert ist, können Sie nicht WorkSpaces mit den Leistungs- oder Grafikpaketen starten. Deaktivieren Sie stattdessen diese Einstellung und geben Sie die IPv6-Adressen manuell ein, wenn Sie Ihre Instances starten.

Wenn ich versuche, ein Verzeichnis zu registrieren, schlägt die Registrierung fehl und das Verzeichnis erhält den Status FEHLER

Dieses Problem kann auftreten, wenn Sie versuchen, ein AWS verwaltetes Microsoft AD-Verzeichnis zu registrieren, das für die Replikation in mehreren Regionen konfiguriert wurde. Das Verzeichnis in der primären Region kann zwar erfolgreich für die Verwendung bei Amazon registriert werden, der Versuch WorkSpaces, das Verzeichnis in einer replizierten Region zu registrieren, schlägt jedoch fehl. Die regionsübergreifende Replikation mit AWS Managed Microsoft AD wird für die Verwendung mit Amazon WorkSpaces in replizierten Regionen nicht unterstützt.

Meine Benutzer können mit einem interaktiven Anmeldebanner keine Verbindung zu WorkSpace einem Windows herstellen

Wenn eine interaktive Anmeldenachricht implementiert wurde, um ein Anmeldebanner anzuzeigen, verhindert dies, dass Benutzer auf ihr Windows zugreifen können. WorkSpaces Die Gruppenrichtlinieneinstellung für interaktive Anmeldenachrichten wird derzeit nicht unterstützt von. WorkSpaces Verschieben Sie WorkSpaces die in eine Organisationseinheit (OU), in der die

Interactive logon: Message text for users attempting to log on Gruppenrichtlinie nicht angewendet wird.

Meine Benutzer können keine Verbindung zu einem Windows-Computer herstellen WorkSpace

Meine Benutzer erhalten die folgende Fehlermeldung, wenn sie versuchen, eine Verbindung zu ihrem Windows herzustellen WorkSpaces:

```
"An error occurred while launching your WorkSpace. Please try again."
```

Dieser Fehler tritt häufig auf, wenn der Windows-Desktop nicht mit PCoIP geladen werden WorkSpace kann. Überprüfen Sie, ob Folgendes der Fall ist:

- Diese Meldung wird angezeigt, wenn der Dienst PCoIP Standard Agent für Windows nicht ausgeführt wird. Stellen Sie mithilfe von RDP eine Verbindung her, um sicherzustellen, dass der Dienst ausgeführt wird, dass er automatisch gestartet wird und dass er über die Verwaltungsschnittstelle (eth0) kommunizieren kann.

- Wenn der PCoIP-Agent deinstalliert wurde, starten Sie ihn WorkSpace über die WorkSpaces Amazon-Konsole neu, um ihn automatisch neu zu installieren.

- Möglicherweise erhalten Sie diesen Fehler auch nach einer langen Verzögerung auf dem WorkSpaces Amazon-Client, wenn die WorkSpacesSicherheitsgruppe geändert wurde, um ausgehenden Datenverkehr einzuschränken. Durch die Einschränkung des ausgehenden Datenverkehrs wird verhindert, dass Windows für die Anmeldung mit den Verzeichniscontrollern kommuniziert. Stellen Sie sicher, dass Ihre Sicherheitsgruppen es Ihnen ermöglichen WorkSpaces , mit Ihren Verzeichniscontrollern an allen erforderlichen Ports über die primäre Netzwerkschnittstelle zu kommunizieren.

Eine weitere Ursache für diesen Fehler ist die Gruppenrichtlinie für die Zuweisung von Benutzerrechten. Wenn die folgende Gruppenrichtlinie falsch konfiguriert ist, können Benutzer nicht auf ihr Windows zugreifen WorkSpaces:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- Falsche Richtlinie:

Richtlinie: Access this computer from the network (Zugriff auf diesen Computer über das Netzwerk)

Einstellung: *Domain name (Domänenname)*\Domain Computers

Gewinner-Gruppenrichtlinienobjekt: Allow File Access (Dateizugriff zulassen)

- Korrekte Richtlinie:

  Richtlinie: Access this computer from the network (Zugriff auf diesen Computer über das Netzwerk)

  Setting: *Domain name (Domänenname)*\Domain Users

  Gewinner-Gruppenrichtlinienobjekt: Allow File Access (Dateizugriff zulassen)

> **Note**
>
> Diese Richtlinieneinstellung sollte auf Domänenbenutzer anstelle von Domänencomputern angewendet werden.

Weitere Informationen finden Sie unter Zugriff auf diesen Computer über das Netzwerk - Sicherheitsrichtlinieneinstellung und Konfigurieren von Sicherheitsrichtlinieneinstellungen in der Microsoft Windows-Dokumentation.

Meine Benutzer haben Probleme, wenn sie versuchen, sich WorkSpaces über WorkSpaces Web Access anzumelden

Amazon WorkSpaces verwendet eine spezielle Konfiguration des Anmeldebildschirms, damit sich Benutzer erfolgreich von ihrem Web Access-Client aus anmelden können.

Damit sich Web Access-Benutzer bei ihnen anmelden können WorkSpaces, müssen Sie eine Gruppenrichtlinieneinstellung und drei Sicherheitsrichtlinieneinstellungen konfigurieren. Wenn diese Einstellungen nicht korrekt konfiguriert sind, kann es bei Benutzern zu langen Anmeldezeiten oder schwarzen Bildschirmen kommen, wenn sie versuchen, sich bei ihren WorkSpaces anzumelden. Informationen zum Konfigurieren dieser Einstellungen finden Sie unter Amazon WorkSpaces Web Access aktivieren und konfigurieren.

> **Important**
>
> Ab dem 1. Oktober 2020 können Kunden den Amazon WorkSpaces Web Access-Client nicht mehr verwenden, um eine Verbindung zu Windows 7 Custom WorkSpaces oder zu Windows 7 Bring Your Own License (BYOL) WorkSpaces herzustellen.

Der WorkSpaces Amazon-Client zeigt für eine Weile einen grauen Bildschirm mit der Aufschrift „Wird geladen...“ an, bevor er zum Anmeldebildschirm zurückkehrt. Es wird keine andere Fehlermeldung angezeigt.

Dieses Verhalten weist normalerweise darauf hin, dass sich der WorkSpaces Client über Port 443 authentifizieren kann, aber keine Streaming-Verbindung über Port 4172 (PCoIP) oder Port 4195 (WSP) herstellen kann. Dies kann passieren, wenn Netzwerkvoraussetzungen nicht erfüllt sind. Probleme auf der Clientseite führen häufig dazu, dass die Netzwerkprüfung im Client fehlschlägt. Wählen Sie das Netzwerkprüfsymbol aus, um zu sehen, welche Zustandsprüfungen fehlschlagen. (Normalerweise ein rotes Dreieck mit einem Ausrufezeichen in der unteren rechten Ecke des Anmeldebildschirms für Clients ab 2.0 oder das Netzwerksymbol

in der oberen rechten Ecke von Clients ab 3.0).

> **Note**
>
> Die häufigste Ursache für dieses Problem ist eine Firewall oder ein Proxy auf Clientseite, durch die bzw. den der Zugriff über Port 4172 oder 4195 (TCP und UDP) verhindert wird. Wenn diese Zustandsprüfung fehlschlägt, überprüfen Sie die lokalen Firewalleinstellungen.

Wenn die Netzwerkprüfung erfolgreich ist, liegt möglicherweise ein Problem mit der Netzwerkkonfiguration von vor. WorkSpace Beispielsweise kann eine Windows-Firewallregel Port UDP 4172 oder 4195 auf der Verwaltungsschnittstelle blockieren. Stellen Sie WorkSpace mithilfe eines Remote Desktop Protocol (RDP) eine Connect zum Client her, um zu überprüfen, ob der die erforderlichen Portanforderungen WorkSpace erfüllt.

Meine Benutzer erhalten die Meldung "WorkSpace Status: Ungesund. Wir konnten Sie nicht mit Ihrem WorkSpace verbinden. Please try again in a few minutes."

Dieser Fehler weist normalerweise darauf hin, dass der SkyLightWorkSpacesConfigService Dienst nicht auf Zustandsprüfungen reagiert.

Wenn Sie Ihren gerade neu gestartet oder neu gestartet haben WorkSpace, warten Sie ein paar Minuten, und versuchen Sie es dann erneut.

Wenn der WorkSpace schon länger läuft und dieser Fehler immer noch angezeigt wird, stellen Sie eine Verbindung über RDP her, um zu überprüfen, ob der Dienst: SkyLightWorkSpacesConfigService

- Er wird ausgeführt.
- Er ist so konfiguriert, dass er automatisch gestartet wird.
- Er kann über die Verwaltungsschnittstelle (eth0) kommunizieren.
- Er wird nicht durch Antivirensoftware von Drittanbietern blockiert.

Meine Benutzer erhalten die Meldung „Dieses Gerät ist nicht berechtigt, auf das WorkSpace zuzugreifen. Please contact your administrator for assistance." (Dieses Gerät ist nicht berechtigt, auf den WorkSpace zuzugreifen. Wenden Sie sich an Ihren Administrator, um Unterstützung zu erhalten.)

Dieser Fehler weist darauf hin, dass IP-Zugriffskontrollgruppen für das WorkSpace Verzeichnis konfiguriert sind, die Client-IP-Adresse jedoch nicht auf der Zulassungsliste steht.

Überprüfen Sie die Einstellungen in Ihrem Verzeichnis. Vergewissern Sie sich, dass die öffentliche IP-Adresse, von der aus der Benutzer eine Verbindung herstellt, Zugriff auf die WorkSpace ermöglicht.

Meine Benutzer erhalten die Meldung „Kein Netzwerk. Netzwerkverbindung verloren. Überprüfen Sie Ihre Netzwerkverbindung oder kontaktieren Sie Ihren Administrator.“ wenn Sie versuchen, eine Verbindung zu einem WSP herzustellen WorkSpace

Wenn dieser Fehler auftritt und Ihre Benutzer keine Verbindungsprobleme haben, stellen Sie sicher, dass Port 4195 auf den Firewalls Ihres Netzwerks geöffnet ist. Für die WorkSpaces Verwendung des WorkSpaces Streaming Protocol (WSP) wurde der Port, der zum Streamen der Clientsitzung verwendet wurde, von 4172 auf 4195 geändert.

Der WorkSpaces Client gibt meinen Benutzern einen Netzwerkfehler, aber sie können andere netzwerkfähige Apps auf ihren Geräten verwenden

Die WorkSpaces Client-Anwendungen sind auf den Zugriff auf Ressourcen in der AWS Cloud angewiesen und benötigen eine Verbindung, die mindestens 1 Mbit/s Download-Bandbreite bietet. Wenn ein Gerät eine unterbrochene Verbindung zum Netzwerk hat, meldet die WorkSpaces Client-Anwendung möglicherweise ein Problem mit dem Netzwerk.

WorkSpaces erzwingt seit Mai 2018 die Verwendung von digitalen Zertifikaten, die von Amazon Trust Services ausgestellt wurden. Amazon Trust Services ist bereits eine vertrauenswürdige Root-CA auf den Betriebssystemen, die von unterstützt werden WorkSpaces. Wenn die Root-CA-Liste für das Betriebssystem nicht aktuell ist, kann das Gerät keine Verbindung herstellen WorkSpaces und der Client gibt einen Netzwerkfehler aus.

So erkennen Sie Verbindungsprobleme aufgrund von Zertifikatfehlern

- PCoIP-Zero-Clients – Die folgende Fehlermeldung wird angezeigt.

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- Andere Clients – Die Zustandsprüfungen schlagen fehl und es wird ein rotes Warndreieck für Internet angezeigt.

So beheben Sie Zertifikatfehler

- Windows-Clientanwendung

- PCoIP-Zero-Clients
- Andere Clientanwendungen

Windows-Clientanwendung

Wenden Sie bei Zertifikatfehlern eine der folgenden Lösungen an.

Lösung 1: Aktualisieren der Clientanwendung

Laden Sie die neueste Windows-Client-Anwendung von https://clients.amazonworkspaces.com/ us-iso-eastworkspaces-client-updates-dcaus-isob-east Die Clientanwendung stellt bei der Installation sicher, dass Ihr Betriebssystem Zertifikaten vertraut, die von Amazon Trust Services ausgestellt wurden.

Lösung 2: Hinzufügen von Amazon Trust Services zur lokalen Root-CA-Liste

1. Öffnen Sie https://www.amazontrust.com/repository/.
2. Laden Sie das Starfield-Zertifikat im DER-Format (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) herunter.
3. Öffnen Sie die Microsoft Management Console. (Führen Sie an der Eingabeaufforderung mmc aus.)
4. Wählen Sie Datei, Snap-In hinzufügen/entfernen, Zertifikate, Hinzufügen.
5. Wählen Sie auf der Seite Zertifikat-Snap-In die Option Computerkonto aus und klicken Sie auf Weiter. Behalten Sie die Standardeinstellung Lokaler Computer bei. Wählen Sie Finish (Abschließen). Wählen Sie OK aus.
6. Erweitern Sie Zertifikate (Lokaler Computer) und wählen Sie Vertrauenswürdige Stammzertifizierungsstellen. Wählen Sie Aktion, Alle Aufgaben, Importieren.
7. Befolgen Sie die Anweisungen des Assistenten zum Importieren des heruntergeladenen Zertifikats.
8. Beenden Sie die Client-Anwendung und starten Sie sie neu. WorkSpaces

Lösung 3: Bereitstellen von Amazon Trust Services als vertrauenswürdige CA mithilfe von Gruppenrichtlinien

Fügen Sie das Starfield-Zertifikat mithilfe der Gruppenrichtlinie zu den vertrauenswürdigen Root-CAs für die Domain hinzu. Weitere Informationen finden Sie unter Use Policy to Distribute Certificates (Verwenden von Richtlinien zum Verteilen von Zertifikaten).

PCoIP-Zero-Clients

Um eine direkte Verbindung zu einer Firmware-Version 6.0 oder höher WorkSpace herzustellen, laden Sie das von Amazon Trust Services ausgestellte Zertifikat herunter und installieren Sie es.

So fügen Sie Amazon Trust Services als vertrauenswürdige Root-CA hinzu

1. Öffnen Sie https://certs.secureserver.net/repository/.
2. Laden Sie das Zertifikat unter Starfield-Zertifikatkette mit dem Thumbprint 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58 herunter.
3. Laden Sie das Zertifikat auf den Zero Client hoch. Weitere Informationen finden Sie in der Teradici-Dokumentation unter Uploading Certificates (Hochladen von Zertifikaten) .

Andere Clientanwendungen

Fügen Sie das Starfield-Zertifikat (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) von Amazon Trust Services hinzu. Weitere Informationen zum Hinzufügen einer Root-CA finden Sie in der folgenden Dokumentation:

- Android: Zertifikate hinzufügen und entfernen
- Chrome OS: Clientzertifikate auf Chrome-Geräten verwalten
- macOS und iOS: Installing a CA's Root Certificate on Your Test Device

Meinen WorkSpace Benutzern wird die folgende Fehlermeldung angezeigt: „Das Gerät kann keine Verbindung zum Registrierungsservice herstellen. Check your network settings.“

Wenn ein Registrierungsdienst ausfällt, wird Ihren WorkSpace Benutzern auf der Seite Connection Health Check möglicherweise die folgende Fehlermeldung angezeigt: „Ihr Gerät kann keine Verbindung zum WorkSpaces Registrierungsdienst herstellen. Sie können Ihr Gerät nicht bei registrieren WorkSpaces. Please check your network settings."

Dieser Fehler tritt auf, wenn die WorkSpaces Client-Anwendung den Registrierungsdienst nicht erreichen kann. In der Regel passiert dies, wenn das WorkSpaces Verzeichnis gelöscht wurde. Um diesen Fehler zu beheben, stellen Sie sicher, dass der Registrierungscode gültig ist und einem laufenden Verzeichnis in der AWS Cloud entspricht.

Meine PCoIP-Null-Client-Benutzer erhalten die Fehlermeldung „Das angegebene Zertifikat ist aufgrund des Zeitstempels ungültig“.

Wenn Network Time Protocol (NTP) in Teradici nicht aktiviert ist, erhalten Ihre PCoIP-Null-Client-Benutzer möglicherweise Zertifikatfehler. Informationen zum Einrichten von NTP finden Sie unter Einrichten von PCoIP-Zero-Clients für WorkSpaces.

USB-Drucker und andere USB-Peripheriegeräte funktionieren nicht für PCoIP-Zero-Clients

Ab Version 20.10.4 des PCoIP-Agenten WorkSpaces deaktiviert Amazon die USB-Umleitung standardmäßig über die Windows-Registrierung. Diese Registrierungseinstellung wirkt sich auf das Verhalten von USB-Peripheriegeräten aus, wenn Ihre Benutzer PCoIP-Zero-Client-Geräte verwenden, um eine Verbindung zu ihren Geräten herzustellen. WorkSpaces

Wenn Sie WorkSpaces Version 20.10.4 oder höher des PCoIP-Agents verwenden, funktionieren USB-Peripheriegeräte erst mit PCoIP-Zero-Client-Geräten, wenn Sie die USB-Umleitung aktiviert haben.

> **Note**
>
> Wenn Sie virtuelle 32-Bit-Druckertreiber verwenden, müssen Sie diese Treiber zudem auf die 64-Bit-Versionen aktualisieren.

So aktivieren Sie die USB-Umleitung für PCoIP-Zero-Client-Geräte

Wir empfehlen, dass Sie diese Registrierungsänderungen über die Gruppenrichtlinie auf Ihren Computer übertragen. WorkSpaces Weitere Informationen finden Sie unter Konfiguration des Agents und Konfigurierbare Einstellungen in der Teradici-Dokumentation.

1. Legen Sie für den folgenden Registrierungsschlüsselwert 1 (aktiviert) fest:

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Teradici\ PCoIP\ pcoip_admin

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1

2. Legen Sie für den folgenden Registrierungsschlüsselwert 1 (aktiviert) fest:

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Teradici\ PCoIP\ pcoip_admin_defaults

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1

3. Wenn Sie dies noch nicht getan haben, melden Sie sich WorkSpace von ab und dann wieder an. Ihre USB-Geräte sollten jetzt funktionieren.

Meine Benutzer haben die Aktualisierung ihrer Windows- oder macOS-Clientanwendungen übersprungen und werden nicht aufgefordert, die neueste Version zu installieren.

Wenn Benutzer Updates für die Amazon WorkSpaces Windows-Client-Anwendung überspringen, wird der SkipThisVersionRegistrierungsschlüssel festgelegt und sie werden nicht mehr aufgefordert, ihre Clients zu aktualisieren, wenn eine neue Version des Clients veröffentlicht wird. Um auf die neueste Version zu aktualisieren, können Sie die Registrierung wie unter Aktualisieren der WorkSpaces Windows-Client-Anwendung auf eine neuere Version im WorkSpaces Amazon-Benutzerhandbuch beschrieben bearbeiten. Sie können auch den folgenden PowerShell Befehl ausführen:

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

Wenn Benutzer Updates für die Amazon WorkSpaces macOS-Client-Anwendung überspringen, wird die `SUSkippedVersion` Einstellung festgelegt und sie werden nicht mehr aufgefordert, ihre Clients zu aktualisieren, wenn eine neue Version des Clients veröffentlicht wird. Um auf die neueste Version zu aktualisieren, können Sie diese Einstellung wie unter Aktualisieren der WorkSpaces macOS-Client-Anwendung auf eine neuere Version im WorkSpaces Amazon-Benutzerhandbuch beschrieben zurücksetzen.

Meine Benutzer können die Android-Clientanwendung nicht auf ihren Chromebooks installieren

Version 2.4.13 ist die letzte Version der Amazon WorkSpaces Chromebook-Client-Anwendung. Da Google die Unterstützung für Chrome-Apps schrittweise einstellt, wird es keine weiteren Updates für die WorkSpaces Chromebook-Clientanwendung geben, und ihre Verwendung wird nicht unterstützt.

Für Chromebooks, die die Installation von Android-Anwendungen unterstützen, empfehlen wir, stattdessen die Android-Client-Anwendung zu verwenden. WorkSpaces

In einigen Fällen müssen Sie möglicherweise die Chromebooks Ihrer Benutzer aktivieren, um Android-Anwendungen installieren zu können. Weitere Informationen finden Sie unter Einrichten von Android für Chromebooks.

Meine Benutzer erhalten keine Einladungs-E-Mails oder E-Mails zum Zurücksetzen des Passworts.

Benutzer erhalten nicht automatisch Willkommens-E-Mails oder E-Mails zum Zurücksetzen des Kennworts für E-Mails WorkSpaces , die mit AD Connector oder einer vertrauenswürdigen Domain erstellt wurden. Einladungs-E-Mails werden auch nicht automatisch gesendet, wenn Benutzer bereits in Active Directory vorhanden sind.

Informationen zum manuellen Senden von Begrüßungs-E-Mails an diese Benutzer finden Sie unter Senden einer Einladungs-E-Mail.

Informationen zum Zurücksetzen von Benutzerpasswörtern finden Sie unter Einrichten der Active-Directory-Verwaltungstools für WorkSpaces.

Meine Benutzer sehen die Option „Passwort vergessen?“ auf dem Client-Anmeldebildschirm.

Wenn Sie AD Connector oder eine vertrauenswürdige Domain verwenden, können Ihre Benutzer ihre eigenen Passwörter nicht zurücksetzen. (Das Passwort vergessen? Die Option auf dem Anmeldebildschirm der WorkSpaces Client-Anwendung wird nicht verfügbar sein.) Weitere Informationen zum Zurücksetzen von Benutzerpasswörtern finden Sie unter Einrichten der Active-Directory-Verwaltungstools für WorkSpaces.

Ich erhalte die Meldung „Der Systemadministrator hat Richtlinien festgelegt, um diese Installation zu verhindern“, wenn ich versuche, Anwendungen unter Windows zu installieren WorkSpace

Sie können dieses Problem beheben, indem Sie die Gruppenrichtlinieneinstellung für Windows Installer ändern. Um diese Richtlinie für mehrere Personen WorkSpaces in Ihrem Verzeichnis bereitzustellen, wenden Sie diese Einstellung auf ein Gruppenrichtlinienobjekt an, das von einer EC2-Instanz aus mit der WorkSpaces Organisationseinheit (OU) verknüpft ist. Wenn Sie AD Connector verwenden, können Sie diese Änderungen von einem Domain-Controller aus vornehmen. Weitere Informationen zur Verwendung der Active-Directory-Verwaltungstools für die Arbeit mit Gruppenrichtlinienobjekten finden Sie unter Installieren der Active-Directory-Verwaltungstools im AWS Directory Service -Administratorhandbuch.

Das folgende Verfahren zeigt, wie Sie die Windows Installer-Einstellung für das WorkSpaces Gruppenrichtlinienobjekt konfigurieren.

1. Stellen Sie sicher, dass die neueste administrative WorkSpaces Gruppenrichtlinienvorlage in Ihrer Domäne installiert ist.
2. Öffnen Sie das Gruppenrichtlinien-Verwaltungstool auf Ihrem WorkSpace Windows-Client, navigieren Sie zum WorkSpaces Gruppenrichtlinienobjekt für Ihre WorkSpaces Computerkonten und wählen Sie es aus. Wählen Sie im Hauptmenü Action (Aktion), Edit (Bearbeiten).
3. Klicken Sie im Gruppenrichtlinienverwaltungseditor auf Computerkonfiguration, Richtlinien, Administrative Vorlagen, Klassische administrative Vorlagen, Windows-Komponenten und Windows Installer.
4. Öffnen Sie die Einstellung Turn Off Windows Installer (Windows Installer deaktivieren).
5. Ändern Sie im Dialogfeld Turn Off Windows Installer (Windows Installer deaktivieren) die Option Not Configured (Nicht konfiguriert) in Enabled (Aktiviert) und setzen Sie dann Disable Windows Installer (Windows Installer deaktivieren) auf Never (Nie).
6. Wählen Sie OK aus.
7. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
   - Starten Sie das neu WorkSpace (wählen Sie in der WorkSpaces WorkSpace Konsole das und dann Aktionen, Neustart WorkSpaces).
   - Geben Sie an einer administrativen Eingabeaufforderung gpupdate /force ein.

Nein, WorkSpaces in meinem Verzeichnis kann ich eine Verbindung zum Internet herstellen

WorkSpaces kann standardmäßig nicht mit dem Internet kommunizieren. Sie müssen explizit Internetzugriff anbieten. Weitere Informationen finden Sie unter Bereitstellen des Internetzugangs von Ihrem aus WorkSpace.

Mein WorkSpace hat seinen Internetzugang verloren

Wenn Sie den Internetzugang verloren haben und Sie WorkSpace über RDP keine Verbindung zum WorkSpace herstellen können, wird dieses Problem wahrscheinlich durch den Verlust der öffentlichen IP-Adresse für den WorkSpace verursacht. Wenn Sie die automatische Zuweisung von Elastic IP-Adressen auf Verzeichnisebene aktiviert haben, wird Ihrer WorkSpace beim Start eine Elastic IP-Adresse (aus dem von Amazon bereitgestellten Pool) zugewiesen. Wenn Sie jedoch eine Elastic IP-Adresse, die Sie besitzen WorkSpace, einer zuordnen und diese Elastic IP-Adresse später von der trennen WorkSpace, WorkSpace verliert diese ihre öffentliche IP-Adresse und sie erhält nicht automatisch eine neue aus dem von Amazon bereitgestellten Pool.

Um eine neue öffentliche IP-Adresse aus dem von Amazon bereitgestellten Pool dem zuzuordnen WorkSpace, müssen Sie den neu erstellen. WorkSpace Wenn Sie die nicht neu erstellen möchten WorkSpace, müssen Sie der eine weitere Elastic IP-Adresse zuordnen, deren Eigentümer Sie sind. WorkSpace

Es wird empfohlen, die elastic network interface von a nicht zu ändern, WorkSpace nachdem WorkSpace der gestartet wurde. Nachdem einer eine Elastic IP-Adresse zugewiesen wurde WorkSpace, WorkSpace behält sie dieselbe öffentliche IP-Adresse bei (es sei denn, die WorkSpace wird neu erstellt, in diesem Fall erhält sie eine neue öffentliche IP-Adresse).

Ich erhalte die Fehlermeldung „DNS unavailable“, wenn ich eine Verbindung zu meinem on-premises Verzeichnis herstellen möchte

Sie erhalten eine Fehlermeldung ähnlich der Folgenden, wenn Sie eine Verbindung zu Ihrem on-premises Verzeichnis herstellen möchten.

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector muss über TCP und UDP über Port 53 mit Ihrem on-premises DNS-Server kommunizieren können. Stellen Sie sicher, dass Ihre Sicherheitsgruppen und on-premises Firewalls die TCP- und UDP-Kommunikation über diesen Port erlauben.

Ich erhalte die Fehlermeldung „Connectivity issues detected“, wenn ich eine Verbindung zu meinem on-premises Verzeichnis herstellen möchte

Sie erhalten eine Fehlermeldung ähnlich der Folgenden, wenn Sie eine Verbindung zu Ihrem on-premises Verzeichnis herstellen möchten.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

AD Connector muss mit Ihren on-premises Domain-Controllern via TCP und UDP über folgende Ports kommunizieren können. Überprüfen Sie, ob Ihre Sicherheitsgruppen und on-premises Firewalls die TCP- und UDP-Kommunikation über diese Ports erlauben:

- 88 (Kerberos)
- 389 (LDAP)

Ich erhalte die Fehlermeldung „SRV record“, wenn ich eine Verbindung zu meinem on-premises Verzeichnis herstellen möchte

Sie erhalten eine Fehlermeldung ähnlich einer oder mehr der Folgenden, wenn Sie eine Verbindung zu Ihrem on-premises Verzeichnis herstellen möchten.

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

AD Connector muss beim Aufbau einer Verbindung zu Ihrem Verzeichnis SRV-Datensätze für `_ldap._tcp.`*`dns-domain-name`* und `_kerberos._tcp.`*`dns-domain-name`* abrufen. Sie erhalten diese Fehlermeldung, wenn der Service diese Datensätze nicht von den DNS-Servern abrufen kann, die Sie beim Aufbau einer Verbindung zu ihrem Verzeichnis angegeben haben. Stellen Sie sicher, dass Ihre DNS-Server diese SRV-Datensätze enthalten. Weitere Informationen finden Sie unter SRV Resource Records auf Microsoft TechNet.

Mein Windows WorkSpace wechselt in den Standbymodus, wenn es inaktiv bleibt

Um dieses Problem zu beheben, stellen Sie eine Verbindung mit dem her WorkSpace und ändern Sie den Energiesparplan auf Hochleistung, indem Sie wie folgt vorgehen:

1. Öffnen Sie in der WorkSpace Systemsteuerung und wählen Sie dann Hardware oder Hardware und Sound (der Name kann je nach Ihrer Windows-Version unterschiedlich sein).
2. Wählen Sie unter Energieoptionendie Option Energiesparplan auswählen.
3. Wählen Sie im Fenster Energiesparplan auswählen oder anpassen die Energiesparplan-Option Hohe Leistung und dann Planeinstellungen ändern aus.
   - Wenn die Option zur Auswahl des Energiesparplans Hohe Leistung deaktiviert ist, wählen Sie Einstellungen ändern, die derzeit nicht verfügbar sind aus. Wählen Sie dann den Energiesparplan Hohe Leistung aus.
   - Wenn der Plan Hohe Leistung nicht sichtbar ist, klicken Sie auf den Pfeil rechts neben Zusätzliche Pläne anzeigen, um ihn anzuzeigen, oder wählen Sie im linken Navigationsbereich die Option Energiesparplan erstellen aus. Wählen Sie dann Hohe Leistung aus, geben Sie dem Energiesparplan einen Namen und klicken Sie auf Weiter.
4. Vergewissern Sie sich, dass auf der Seite Einstellungen für den Plan ändern: Hohe Leistung die Option Bildschirm ausschalten und (falls verfügbar) Computer in den Standbymodus versetzen auf Nie festgelegt ist.
5. Wenn Sie Änderungen am Plan für hohe Leistung vorgenommen haben, wählen Sie Änderungen speichern aus (oder wählen Sie Erstellen aus, wenn Sie einen neuen Plan erstellen).

Wenn die oben beschriebenen Schritte das Problem nicht lösen, gehen Sie wie folgt vor:

1. Öffnen Sie in der WorkSpace Systemsteuerung und wählen Sie dann Hardware oder Hardware und Sound (der Name kann je nach Ihrer Windows-Version unterschiedlich sein).
2. Wählen Sie unter Energieoptionendie Option Energiesparplan auswählen.
3. Wählen Sie im Bereich Auswählen oder Anpassen eines Energiesparplans den Link Energiesparplaneinstellungen ändern rechts neben dem Energiesparplan Hochleistung. Wählen Sie dann den Link Erweiterte Energieeinstellungen ändern.
4. Wählen Sie im Dialogfeld Energieoptionen in der Liste der Einstellungen das Pluszeichen links neben Festplatte aus, um die relevanten Einstellungen anzuzeigen.

5. Vergewissern Sie sich, dass der Wert unter Festplatte ausschalten nach für Netzbetrieb größer als der Wert für On battery (Batteriebetrieb) ist (der Standardwert ist 20 Minuten).
6. Wählen Sie das Pluszeichen links neben PCI Express und verfahren Sie genauso für Verbindungszustand-Energieverwaltung.
7. Vergewissern Sie sich, dass die Einstellungen unter Verbindungszustand-Energieverwaltung Aus lauten.
8. Klicken Sie auf OK (oder Übernehmen, wenn Sie Ihre Einstellungen geändert haben), um das Dialogfeld zu schließen.
9. Klicken Sie im Bereich Change settings for the plan (Einstellungen für Plan ändern) auf Änderungen speichern, sofern Sie irgendwelche Einstellungen geändert haben.

Einer von mir WorkSpaces hat einen Zustand von **UNHEALTHY**

Der WorkSpaces Dienst sendet regelmäßig Statusanfragen an WorkSpace a. A WorkSpace wird markiertUNHEALTHY, wenn es auf diese Anfragen nicht reagiert. Häufige Ursachen für diesen Fehler sind:

- Eine Anwendung auf dem WorkSpace blockiert Netzwerkports, wodurch verhindert wird, dass die WorkSpace auf die Statusanfrage reagiert.
- Eine hohe CPU-Auslastung verhindert, dass die Statusanfrage rechtzeitig beantwortet wird. WorkSpace
- Der Computername von WorkSpace wurde geändert. Dadurch wird verhindert, dass ein sicherer Kanal zwischen WorkSpaces und dem eingerichtet wird WorkSpace.

Sie können versuchen, das Problem anhand der folgenden Methoden zu beheben:

- Starten Sie das WorkSpace von der WorkSpaces Konsole aus neu.
- Stellen Sie WorkSpace mithilfe des folgenden Verfahrens, das nur zur Fehlerbehebung verwendet werden sollte, eine Connect zu dem fehlerhaften Gerät her:

  1. Stellen Sie eine Connect zu einem WorkSpace Betriebsprogramm her, das sich im selben Verzeichnis wie das fehlerhafte befindet WorkSpace.
  2. Verwenden Sie im WorkSpace Betriebsmodus das Remote Desktop Protocol (RDP), um WorkSpace mithilfe der IP-Adresse des fehlerhaften Geräts eine Verbindung zu dem

fehlerhaften Gerät herzustellen. WorkSpace Je nach Ausmaß des Problems können Sie möglicherweise keine Verbindung zu dem fehlerhaften Gerät herstellen. WorkSpace

3. Stellen Sie bei einem fehlerhaften Gerät sicher WorkSpace, dass die Mindestanforderungen für den Anschluss erfüllt sind.

- Stellen Sie sicher, dass der SkyLightWorkSpacesConfigService Dienst auf Zustandsprüfungen reagieren kann. Lesen Sie zur Behebung dieses Problems Meine Benutzer erhalten die Meldung "WorkSpace Status: Ungesund. Wir konnten Sie nicht mit Ihrem WorkSpace verbinden. Please try again in a few minutes.".
- Erstellen Sie das WorkSpace von der WorkSpaces Konsole aus neu. Da die Neuerstellung eines möglicherweise zu Datenverlusten führen WorkSpace kann, sollte diese Option nur verwendet werden, wenn alle anderen Versuche, das Problem zu beheben, erfolglos waren.

Mein stürzt WorkSpace unerwartet ab oder wird neu gestartet

Wenn Ihr für PCoIP WorkSpace konfiguriertes Gerät wiederholt abstürzt oder neu startet und Ihre Fehlerprotokolle oder Absturzabbilder auf Probleme mit oder hinweisen`spacedeskHookUmode.dll`, `spacedeskHookKmode.sys` oder wenn Sie die folgenden Fehlermeldungen erhalten, müssen Sie möglicherweise den Webzugriff auf Folgendes deaktivieren: WorkSpace

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - Diese Schritte zur Fehlerbehebung gelten nicht für Geräte, die für WorkSpaces WorkSpaces das Streaming Protocol (WSP) konfiguriert sind. Sie gelten nur für diejenigen WorkSpaces , die für PCoIP konfiguriert sind.
> - Sie sollten Web Access nur deaktivieren, wenn Sie Ihren Benutzern die Verwendung von Web Access nicht erlauben.

Um den Webzugriff auf den zu deaktivieren WorkSpace, müssen Sie den Webzugriff im WorkSpaces Verzeichnis deaktivieren und den neu starten. WorkSpace

Derselbe Benutzername hat mehrere WorkSpace, aber der Benutzer kann sich nur mit einem der WorkSpaces

Wenn Sie einen Benutzer in Active Directory (AD) löschen, ohne zuerst seinen Benutzer zu löschen, WorkSpace und dann den Benutzer wieder zu Active Directory hinzufügen und einen neuen WorkSpace für diesen Benutzer erstellen, hat derselbe Benutzername jetzt zwei WorkSpaces im selben Verzeichnis. Wenn der Benutzer jedoch versucht, eine Verbindung zu seinem Original herzustellen WorkSpace, wird ihm die folgende Fehlermeldung angezeigt:

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

Darüber hinaus gibt die Suche nach dem Benutzernamen in der WorkSpaces Amazon-Konsole nur den neuen zurück WorkSpace, obwohl beide WorkSpaces noch existieren. (Sie können das Original finden, WorkSpace indem Sie nach der WorkSpace ID statt nach dem Benutzernamen suchen.)

Dieses Verhalten kann auch auftreten, wenn Sie einen Benutzer in Active Directory umbenennen, ohne ihn zuerst zu löschen WorkSpace. Wenn Sie dann ihren Benutzernamen wieder in den ursprünglichen Benutzernamen ändern und einen neuen WorkSpace für den Benutzer erstellen, hat derselbe Benutzername zwei WorkSpaces im Verzeichnis.

Dieses Problem tritt auf, weil Active Directory die Sicherheits-ID (SID) des Benutzers anstelle des Benutzernamens verwendet, um den Benutzer eindeutig zu identifizieren. Wenn ein Benutzer in Active Directory gelöscht und neu erstellt wird, wird dem Benutzer eine neue SID zugewiesen, auch wenn sein Benutzername unverändert bleibt. Bei der Suche nach einem Benutzernamen verwendet die WorkSpaces Amazon-Konsole die SID, um Active Directory nach Treffern zu durchsuchen. Die WorkSpaces Amazon-Clients verwenden die SID auch, um Benutzer zu identifizieren, wenn sie eine Verbindung herstellen WorkSpaces.

Führen Sie einen der folgenden Schritte aus, um dieses Problem zu beheben:

- Wenn dieses Problem aufgetreten ist, weil der Benutzer gelöscht und in Active Directory neu erstellt wurde, können Sie möglicherweise das ursprüngliche gelöschte Benutzerobjekt wiederherstellen, wenn Sie die Papierkorb-Funktion in Active Directory aktiviert haben. Wenn Sie das ursprüngliche Benutzerobjekt wiederherstellen können, stellen Sie sicher, dass der Benutzer eine Verbindung zu seinem ursprünglichen Objekt herstellen kann WorkSpace. Wenn dies möglich ist, können Sie das neue Objekt löschen, WorkSpace nachdem Sie alle Benutzerdaten manuell

gesichert und vom neuen WorkSpace auf das Original übertragen haben WorkSpace (falls erforderlich).

- Wenn Sie das ursprüngliche Benutzerobjekt nicht wiederherstellen können, löschen Sie das Original des Benutzers WorkSpace. Der Benutzer sollte WorkSpace stattdessen in der Lage sein, eine Verbindung zu seinem neuen Gerät herzustellen und es zu verwenden. Stellen Sie sicher, dass Sie alle Benutzerdaten manuell sichern und vom Original WorkSpace auf das neue übertragen WorkSpace.

> **Warning**
>
> Das Löschen von WorkSpace ist eine permanente Aktion und kann nicht rückgängig gemacht werden. Die Daten des WorkSpace Benutzers bleiben nicht erhalten und werden vernichtet. Wenn Sie Hilfe bei der Sicherung von Benutzerdaten benötigen, wenden Sie sich an den AWS -Support.

Ich habe Probleme, Docker mit Amazon zu verwenden WorkSpaces

Windows WorkSpaces

Verschachtelte Virtualisierung (einschließlich der Verwendung von Docker) wird unter Windows nicht unterstützt. WorkSpaces Weitere Informationen finden Sie in der Docker-Dokumentation.

Linux WorkSpaces

Um Docker unter Linux zu verwenden WorkSpaces, stellen Sie sicher, dass sich die von Docker verwendeten CIDR-Blöcke nicht mit den CIDR-Blöcken überschneiden, die in den beiden Elastic Network Interfaces (ENIs) verwendet werden, die mit dem verknüpft sind. WorkSpace Wenn Sie Probleme bei der Verwendung von Docker unter Linux WorkSpaces haben, wenden Sie sich an Docker, um Unterstützung zu erhalten.

Ich erhalte ThrottlingException bei einigen meiner API-Aufrufe Fehler

Die standardmäßig zulässige Rate für WorkSpaces API-Aufrufe ist eine konstante Rate von zwei API-Aufrufen pro Sekunde mit einer maximal zulässigen „Burst“ -Rate von fünf API-Aufrufen pro Sekunde. Die folgende Tabelle zeigt, wie das Burst-Ratenlimit für API-Anforderungen funktioniert.

Sekunde	Anzahl der gesendeten Anforderungen	Zulässige Nettoanforderungen	Details
1	0	5	Während der ersten Sekunde (zweite 1) sind fünf Anforderungen zulässig, bis zur maximalen Burst-Rate von fünf Aufrufen pro Sekunde.
2	2	5	Da in der 1. Sekunde zwei oder weniger Aufrufe ausgegeben wurden, ist die volle Burst-Kapazität von fünf Aufrufen weiterhin verfügbar.
3	5	5	Da in der 2. Sekunde nur zwei Aufrufe ausgegeben wurden, ist die volle Burst-Kapazität von fünf Aufrufen weiterhin verfügbar.
4	2	2	Da in der 3. Sekunde die volle Burst-Kapazität verwendet wurde, ist nur die konstante Rate von zwei Aufrufen pro Sekunde verfügbar.
5	3	2	Da keine verbleibende Burst-Kapazität vorhanden ist, sind derzeit nur zwei Aufrufe zulässig. Dies bedeutet, dass einer der drei API-Aufrufe gedrosselt wird. Der eine gedrosselte Aufruf reagiert nach kurzer Verzögerung.
6	0	1	Da einer der Aufrufe der 5. Sekunde in der 6. Sekunde wiederholt wird, gibt es aufgrund des konstanten Ratenlimits von zwei Aufrufen pro Sekunde in der 6. Sekunde nur Kapazität für einen zusätzlichen Aufruf.
7	0	3	Da in der Warteschlange nun keine gedrosselten API-Aufrufe mehr vorhanden sind, wird das Ratenlimit bis zum Burst Ratenlimit von fünf Aufrufen weiter erhöht.

Sekunde	Anzahl der gesendeten Anforderungen	Zulässige Nettoanforderungen	Details
8	0	5	Da in der 7. Sekunde keine Aufrufe ausgegeben wurden, ist die maximale Anzahl von Anforderungen zulässig.
9	0	5	Auch wenn in der 8. Sekunde keine Aufrufe ausgegeben wurden, erhöht sich das Ratenlimit nicht über fünf.

Meine Verbindung WorkSpace wird immer wieder unterbrochen, wenn ich sie im Hintergrund laufen lasse

Mac-Benutzer:innen sollten überprüfen, ob die Power-Nap-Funktion aktiviert ist. Falls sie aktiviert ist, sollte sie deaktiviert werden. Öffnen Sie Ihr Terminal und führen Sie den folgenden Befehl aus, um Power Nap auszuschalten:

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML-2.0-Verbund funktioniert nicht. Meine Benutzer sind nicht berechtigt, ihren WorkSpaces Desktop zu streamen.

Dies kann der Fall sein, da die integrierte Inlinerichtlinie für die IAM-Rolle für den SAML-2.0-Verbund keine Berechtigungen zum Streamen vom Verzeichnis-ARN (Amazon-Ressourcennamen) enthält. Die IAM-Rolle wird von dem Verbundbenutzer übernommen, der auf ein WorkSpaces Verzeichnis zugreift. Bearbeiten Sie die Rollenberechtigungen so, dass sie den Verzeichnis-ARN enthalten, und stellen Sie sicher, dass der Benutzer über einen WorkSpace im Verzeichnis verfügt. Weitere Informationen finden Sie unter SAML 2.0-Authentifizierung und Problembehandlung beim SAML 2.0-Verbund mit. AWS

Meine Benutzer werden alle 60 Minuten von ihrer WorkSpaces Sitzung getrennt.

Wenn Sie die SAML 2.0-Authentifizierung so konfiguriert haben WorkSpaces, müssen Sie je nach Ihrem Identitätsanbieter (IdP) möglicherweise die Informationen konfigurieren, an die der IdP im Rahmen der Authentifizierungsantwort als SAML-Attribute AWS weitergibt. Dies beinhaltet auch die Konfiguration des Attribute-Elements, wobei das Attribut `SessionDuration` auf `https://aws.amazon.com/SAML/Attributes/SessionDuration` festgelegt wird.

`SessionDuration` gibt an, wie lange eine Verbund-Streaming-Sitzung für Benutzer maximal aktiv bleiben kann, bevor eine erneute Authentifizierung erforderlich ist. Auch wenn es sich bei `SessionDuration` um ein optionales Attribut handelt, wird empfohlen, es in die SAML-Authentifizierungsantwort aufzunehmen. Wenn Sie dieses Attribut nicht angeben, wird für die Sitzungsdauer ein Standardwert von 60 Minuten festgelegt.

Um dieses Problem zu beheben, konfigurieren Sie Ihren IdP so, dass er den `SessionDuration`-Wert in die SAML-Authentifizierungsantwort einbezieht, und legen Sie den Wert wie erforderlich fest. Weitere Informationen finden Sie unter Schritt 5: Erstellen von Zusicherungen für die SAML-Authentifizierungsantwort.

Meine Benutzer erhalten einen Umleitungs-URI-Fehler, wenn sie einen Verbund mithilfe des vom SAML 2.0-Identitätsanbieter (IdP) initiierten Flow herstellen, oder es wird jedes Mal, wenn meine Benutzer versuchen, sich nach dem Verbund mit dem IdP vom WorkSpaces Client aus anzumelden, eine zusätzliche Instanz der Client-Anwendung gestartet.

Dieser Fehler tritt aufgrund einer ungültigen Relay-Status-URL auf. Stellen Sie sicher, dass der Relay-Status in Ihrem IdP-Verbund-Setup korrekt ist und dass die Benutzerzugriffs-URL und der Name des Relay-State-Parameters für Ihren IdP-Verbund in den WorkSpaces Verzeichniseigenschaften korrekt konfiguriert sind. Wenn sie gültig sind und das Problem weiterhin besteht, wenden Sie sich an den AWS Support. Weitere Informationen erhalten Sie unter Einrichten von SAML.

Meine Benutzer erhalten die Meldung „Etwas ist schief gelaufen: Beim Starten Ihrer Datei ist ein Fehler aufgetreten WorkSpace“, wenn sie versuchen, sich nach dem Verbund mit dem IdP bei der WorkSpaces Client-Anwendung anzumelden.

Überprüfen Sie die SAML-2.0-Zusicherungen für Ihren Verbund. Der Wert SAML Subject NameID muss mit dem WorkSpaces Benutzernamen übereinstimmen und entspricht in der Regel dem AccountName SaM-Attribut für den Active Directory-Benutzer. Darüber hinaus `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` muss das Attribute-Element, für das das `PrincipalTag:Email` Attribut festgelegt ist, mit der E-Mail-Adresse des WorkSpaces Benutzers übereinstimmen, wie sie im WorkSpaces Verzeichnis definiert ist. Weitere Informationen erhalten Sie unter Einrichten von SAML.

Meine Benutzer erhalten die Meldung „Tags können nicht validiert werden“, wenn sie versuchen, sich nach dem Verbund mit dem IdP bei der WorkSpaces Client-Anwendung anzumelden.

Überprüfen Sie die `PrincipalTag`-Attributwerte in den SAML 2.0-Zusicherungen für Ihren Verbund (z. B. `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`). Tag-Werte können Kombinationen aus den Zeichen `_ . : / = + - @`, Buchstaben, Zahlen und Leerzeichen enthalten. Weitere Informationen finden Sie unter Regeln für das Tagging in IAM und. AWS STS

Meine Benutzer erhalten die Meldung „Der Client und der Server können nicht kommunizieren, da sie keinen gemeinsamen Algorithmus haben“.

Dieses Problem kann auftreten, wenn Sie TLS 1.2 nicht aktivieren.

Mein Mikrofon oder meine Webcam funktionieren unter Windows nicht. WorkSpaces

Überprüfen Sie Ihre Datenschutzeinstellungen, indem Sie das Startmenü öffnen.

- Start > Einstellungen > Datenschutz > Kamera
- Start > Einstellungen > Datenschutz > Mikrofon

Wenn sie ausgeschaltet sind, schalten Sie sie ein.

Alternativ können WorkSpaces Administratoren ein Gruppenrichtlinienobjekt (GPO) erstellen, um das Mikrofon und/oder die Webcam nach Bedarf zu aktivieren.

Meine Benutzer können sich nicht mit zertifikatsbasierter Authentifizierung anmelden und werden entweder auf dem WorkSpaces Client- oder auf dem Windows-Anmeldebildschirm zur Eingabe des Kennworts aufgefordert, wenn sie eine Verbindung zu ihrer Desktopsitzung herstellen.

Die zertifikatbasierte Authentifizierung war für die Sitzung nicht erfolgreich. Wenn das Problem weiterhin besteht, kann ein Fehler bei der zertifikatbasierten Authentifizierung auf eines der folgenden Probleme zurückzuführen sein:

- Der WorkSpaces oder der Client wird nicht unterstützt. Die zertifikatsbasierte Authentifizierung wird mit Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) -Paketen unterstützt, die die neueste WorkSpaces Windows-Clientanwendung verwenden.
- Das WorkSpaces muss neu gestartet werden, nachdem die zertifikatsbasierte Authentifizierung im Verzeichnis aktiviert wurde. WorkSpaces
- WorkSpaces konnte nicht mit dem AWS Private CA Zertifikat kommunizieren oder AWS Private CA hat es nicht ausgestellt. Prüfen Sie AWS CloudTrail, um festzustellen, ob ein Zertifikat ausgestellt wurde. Weitere Informationen finden Sie unter Verwalten der zertifikatbasierten Authentifizierung.
- Der Domain-Controller hat kein Domain-Controllerzertifikat für die Smartcard-Anmeldung oder es ist abgelaufen. Weitere Informationen finden Sie unter Schritt 7, Konfigurieren von Domain-Controllern mit einem Domain-Controllerzertifikat zur Authentifizierung von Smartcard-Benutzern in Voraussetzungen.
- Das Zertifikat ist nicht vertrauenswürdig. Weitere Informationen finden Sie unter Schritt 7, Veröffentlichen der Zertifizierungsstelle in Active Directory in Voraussetzungen. `certutil -viewstore -enterprise NTAuth`Auf Domänencontrollern ausführen, um zu überprüfen, ob die Zertifizierungsstelle veröffentlicht wurde.
- Es befindet sich ein Zertifikat im Cache, aber die Attribute für den/die Benutzer:in, der/die das Zertifikat ungültig gemacht hat, haben sich geändert. Kontaktieren Sie uns AWS Support , um den Cache vor Ablauf des Zertifikats zu leeren (24 Stunden). Weitere Informationen finden Sie unter AWS Support -Center.
- Das userPrincipalName Format für das `UserPrincipalName` SAML-Attribut ist nicht richtig formatiert oder lässt sich nicht in die tatsächliche Domäne für den Benutzer auflösen. Weitere Informationen finden Sie in Schritt 1 in Voraussetzungen.

- Das (optionale) `ObjectSid`-Attribut in Ihrer SAML-Zusicherung stimmt nicht mit der Active-Directory-Sicherheitskennung (SID) für den in SAML_Subject `NameID` angegebenen Benutzer überein. Vergewissern Sie sich, dass die Attributzuweisung in Ihrem SAML-Verbund korrekt ist und dass Ihr SAML-Identitätsanbieter das SID-Attribut für den Active-Directory-Benutzer synchronisiert.
- Es gibt Gruppenrichtlinieneinstellungen, die die Active-Directory-Standardeinstellungen für die Smartcard-Anmeldung ändern oder Maßnahmen ergreifen, wenn eine Smartcard aus einem Smartcard-Lesegerät entfernt wird. Diese Einstellungen können zusätzlich zu den oben aufgeführten Fehlern zu unerwartetem Verhalten führen. Bei der zertifikatbasierten Authentifizierung wird dem Instance-Betriebssystem eine virtuelle Smartcard zugewiesen und nach Abschluss der Anmeldung entfernt. Überprüfen Sie die primären Gruppenrichtlinieneinstellungen für Smartcards und die Zusätzlichen Gruppenrichtlinieneinstellungen und Registrierungsschlüssel für Smartcards, einschließlich des Verhaltens beim Entfernen von Smartcards.
- Der CRL-Verteilungspunkt für die private Zertifizierungsstelle ist weder online noch vom Domänencontroller aus zugänglich. WorkSpaces Weitere Informationen finden Sie in Schritt 5 unter Voraussetzungen.
- Um zu überprüfen, ob es in der Domäne oder Gesamtstruktur veraltete Zertifizierungsstellen gibt, führen Sie `PKIVIEW.msc` die Zertifizierungsstelle zur Überprüfung aus. Wenn es veraltete Zertifizierungsstellen gibt, löschen Sie sie mithilfe der `PKIVIEW.msc` MMC manuell.
- Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Active Directory-Replikation funktioniert und ob es in der Domäne keine veralteten Domänencontroller gibt. `repadmin / replsum`

Zu den weiteren Schritten zur Problembehandlung gehört die Überprüfung der Windows-Ereignisprotokolle der WorkSpaces Instanz. Ein häufiges Ereignis, das im Windows-Sicherheitsprotokoll bei Anmeldefehlern überprüft werden sollte, ist Ereignis 4625: Ein Konto konnte nicht angemeldet werden.

Wenn das Problem weiterhin besteht, wenden Sie sich an AWS Support. Weitere Informationen finden Sie unter AWS Support -Center.

Ich versuche, etwas zu tun, für das Windows-Installationsmedien erforderlich sind, die aber WorkSpaces nicht bereitgestellt werden.

Wenn Sie ein von Amazon AWS bereitgestelltes öffentliches Paket verwenden, können Sie bei Bedarf die EBS-Snapshots für das Windows-Serverbetriebssystem verwenden, die von Amazon EC2 bereitgestellt werden.

Erstellen Sie aus diesen Snapshots ein EBS-Volume, hängen Sie es an Amazon EC2 an und übertragen Sie die Dateien nach Bedarf dorthin, WorkSpace wo die Dateien sind. Wenn Sie Windows 10 auf BYOL verwenden WorkSpaces und ein Installationsmedium benötigen, müssen Sie Ihr eigenes Installationsmedium vorbereiten. Weitere Informationen finden Sie unter Hinzufügen von Windows-Komponenten mit Installationsmedien. Da Sie ein EBS-Volume nicht direkt an ein anhängen können WorkSpace, müssen Sie es an eine Amazon EC2 EC2-Instance anhängen und die Dateien kopieren.

Ich möchte WorkSpaces mit einem vorhandenen AWS verwalteten Verzeichnis starten, das in einer nicht unterstützten WorkSpaces Region erstellt wurde.

Gehen Sie wie folgt vor, um Amazon WorkSpaces mithilfe eines Verzeichnisses in einer Region zu starten WorkSpaces, die derzeit nicht unterstützt wird.

> **Note**
>
> Wenn Sie beim Ausführen von AWS Command Line Interface Befehlen Fehler erhalten, stellen Sie sicher, dass Sie die neueste AWS CLI Version verwenden. Weitere Informationen finden Sie unter Sicherstellen, dass Sie eine aktuelle Version der AWS CLI ausführen.

Schritt 1: Erstellen eines VPC-Peerings (Virtual Private Cloud) mit einer anderen VPC in Ihrem Konto

1. Erstellen Sie eine VPC-Peering-Verbindung zu einer VPC in einer anderen Region. Weitere Informationen finden Sie unter Erstellen mit VPCs in demselben Konto und unterschiedlichen Regionen
2. Akzeptieren Sie die VPC-Peering-Verbindung. Weitere Informationen finden Sie unter Akzeptieren einer VPC-Peering-Verbindung.
3. Nachdem Sie die VPC-Peering-Verbindung aktiviert haben, können Sie Ihre VPC-Peering-Verbindungen mithilfe der Amazon VPC-Konsole, der AWS CLI oder einer API anzeigen.

Schritt 2: Routing-Tabellen für VPC-Peering in beiden Regionen aktualisieren

Aktualisieren Sie Ihre Routing-Tabellen, um die Kommunikation mit der Peer-VPC über IPv4 oder IPv6 zu aktivieren. Weitere Informationen finden Sie unter Aktualisieren der Routing-Tabellen für eine VPC-Peering-Verbindung.

Schritt 3: Erstellen Sie einen AD Connector und registrieren Sie Amazon WorkSpaces

1. Informationen zu den Voraussetzungen für AD Connector finden Sie unter AD Connector-Voraussetzungen.
2. Verbinden Sie Ihr vorhandenes Verzeichnis mit AD Connector. Weitere Informationen finden Sie unter Einen Konnektor erstellen.
3. Wenn sich der AD-Connector-Status in Aktiv ändert, öffnen Sie die AWS -Directory-Service-Konsole und wählen Sie dann den Hyperlink für Ihre Verzeichnis-ID aus.
4. Wählen Sie für AWS Apps und Dienste Amazon aus, WorkSpaces um den Zugriff WorkSpaces auf dieses Verzeichnis zu aktivieren.
5. Registrieren Sie das Verzeichnis bei WorkSpaces. Weitere Informationen finden Sie unter Registrieren eines Verzeichnisses mit WorkSpaces.

Ich möchte Firefox auf Amazon Linux 2 aktualisieren.

Schritt 1: Überprüfen, ob automatische Updates aktiviert sind

Um zu überprüfen, ob Autoupdate aktiviert ist, führen Sie den Befehl `systemctl status *os-update-mgmt.timer | grep enabled` auf Ihrem aus. WorkSpace In der Ausgabe sollte es zwei Zeilen geben, in denen das Wort `enabled` zu finden ist.

Schritt 2: Initiieren eines Updates

Firefox wird in Amazon Linux 2 normalerweise WorkSpaces zusammen mit allen anderen Softwarepaketen im System während des Wartungsfensters automatisch aktualisiert. Dies hängt jedoch davon ab, welchen Typ WorkSpaces Sie verwenden.

- Denn AlwaysOn WorkSpaces das wöchentliche Wartungsfenster ist am Sonntag von 00h00 bis 04h00, in der Zeitzone von. WorkSpace
- Denn AutoStop WorkSpaces ab dem dritten Montag im Monat und für bis zu zwei Wochen ist das Wartungsfenster täglich von ca. 00h00 bis 05:00 Uhr in der Zeitzone der Region für den geöffnet. AWS WorkSpace

Weitere Informationen zu Wartungsfenstern finden Sie unter Wartung. WorkSpace

Sie können auch einen sofortigen Aktualisierungszyklus einleiten, indem Sie Ihren Computer neu starten WorkSpace und nach 15 Minuten erneut eine Verbindung herstellen. Sie können Aktualisierungen auch einleiten, indem Sie Folgendes eingeben `sudo yum update`. Geben Sie `sudo yum install firefox` ein, um ein Update nur für Firefox einzuleiten.

Wenn Sie den Zugriff auf Amazon-Linux-2-Repositorys nicht konfigurieren können und Firefox lieber mithilfe von Binärdateien installieren möchten, die von Mozilla erstellt wurden, finden Sie weitere Informationen unter Firefox aus Mozilla-Builds installieren im Mozilla-Support. Wir empfehlen, die RPM-Version von Firefox vollständig zu deinstallieren, um sicherzustellen, dass Sie nicht versehentlich eine veraltete Version ausführen. Sie können die Version deinstallieren, indem Sie den Befehl `sudo yum remove firefox` ausführen.

Sie können die erforderlichen RPM-Pakete auch aus den Amazon-Linux-2-Repositorys herunterladen, indem Sie den Befehl `yumdownloader firefox` auf einem anderen Computer ausführen. Laden Sie dann die Repositorys von der Seite auf WorkSpaces, wo Sie sie mit einem Standardbefehl wie installieren können. `YUM sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`

> **Note**
>
> Der genaue Dateiname ändert sich je nach Paketversion.

Schritt 3: Überprüfen, ob das Firefox-Repository verwendet wird

Amazon Linux Extras stellt automatisch Firefox-Updates für Amazon Linux 2 bereit WorkSpaces. Bei Amazon Linux 2, das nach dem 31. Juli 2023 WorkSpaces erstellt wurde, ist das Firefox Extra-Repository bereits aktiviert. Führen Sie WorkSpace den folgenden Befehl aus, um zu überprüfen, ob Sie das Firefox Extra-Repository verwenden.

```
yum repolist | grep amzn2extra-firefox
```

Wenn das Firefox-Extra-Repository verwendet wird, sollte die Befehlsausgabe ungefähr so aussehen: `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10`. Sie ist leer, wenn das Firefox-Extra-Repository nicht verwendet wird. Wenn das Firefox-Extra-Repository nicht verwendet wird, können Sie versuchen, es manuell mit dem folgenden Befehl zu aktivieren:

```
sudo amazon-linux-extras install firefox
```

Wenn die Aktivierung des Firefox-Extra-Repositorys immer noch fehlschlägt, überprüfen Sie Ihren Internetzugang und stellen Sie sicher, dass Ihre VPC-Endpunkte nicht konfiguriert sind. Um weiterhin Firefox-Updates für Amazon Linux 2 WorkSpaces über YUM-Repositorys zu erhalten, stellen Sie sicher, dass WorkSpaces Sie Amazon Linux 2-Repositorys erreichen können. Weitere Informationen zum Zugriff auf Amazon-Linux-2-Repositorys ohne Internetzugang finden Sie in diesem Knowledge Center-Artikel.

Mein Benutzer kann sein Passwort mithilfe des WorkSpaces Clients zurücksetzen und ignoriert dabei die Einstellung Fine Grained Password Policy (FFGP), die für konfiguriert ist. AWS Managed Microsoft AD

Wenn der WorkSpaces Client Ihres Benutzers mit verknüpft ist AWS Managed Microsoft AD, muss er sein Passwort mithilfe der Standardkomplexitätseinstellung zurücksetzen.

Das Standardkennwort für Komplexität unterscheidet zwischen Groß- und Kleinschreibung und muss zwischen 8 und einschließlich 64 Zeichen lang sein. Es muss mindestens ein Zeichen aus jeder der folgenden Kategorien enthalten:

- Kleinbuchstaben (a bis z)
- Großbuchstaben (A bis Z)
- Zahlen (0 – 9)
- Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Vergewissern Sie sich, dass das Passwort keine nicht druckbaren Unicode-Zeichen wie Leerzeichen, Leerzeichen, Zeilenumbrüche und Nullzeichen enthält.

Wenn Ihre Organisation verlangt, dass Sie FFGP für durchsetzen WorkSpaces, wenden Sie sich an Ihren Active Directory-Administrator, um das Benutzerkennwort direkt aus dem Active Directory und nicht vom Client aus zurückzusetzen. WorkSpaces

Richtlinie zum Ende des Lebenszyklus von Amazon-WorkSpaces-Clientanwendungen

Die Richtlinie zum Ende des Lebenszyklus (EOL) von Amazon WorkSpaces gilt für bestimmte Hauptversionen (und alle entsprechenden Nebenversionen) von WorkSpaces, die keinen Support mehr erhalten und nicht mehr auf Kompatibilität mit neueren Versionen getestet werden.

Der Lebenszyklus einer WorkSpaces-Clientversion besteht aus drei Phasen: allgemeiner Support, technische Beratung und Ende des Lebenszyklus (EOL). Die allgemeine Supportphase beginnt am Tag der ersten Veröffentlichung eines WorkSpaces-Clients für eine feste Dauer. Während der allgemeinen Supportphase bietet das WorkSpaces-Support-Team umfassende Unterstützung bei Konfigurationsproblemen. Problemlösungen und Funktionsanfragen werden für diese Hauptversion und die zugehörigen Nebenversionen des WorkSpaces-Clients implementiert.

Technische Beratung wird vom Ende der allgemeinen Supportphase bis zum EOL-Datum bereitgestellt. Während der Phase der technischen Beratung erhalten Sie nur für unterstützte Konfigurationen Support und Beratung. Problemlösungen und Funktionsanfragen werden nur für die aktuellen Versionen des WorkSpaces-Clients implementiert. Für ältere Versionen werden sie nicht implementiert. Wenn während der Phase der technischen Beratung eine Fehlerbehebung erforderlich ist, plant AWS diese Fehlerbehebung für die anstehende öffentlich verfügbare Version. Sie haben dann die Möglichkeit, auf die neueste WorkSpaces-Version zu aktualisieren, um Support zu diesem Update zu erhalten.

EOL für eine Hauptversion tritt ein, wenn sowohl der allgemeine Support als auch die technische Beratung beendet sind. Nach dem EOL-Datum wird kein weiterer Support oder keine Wartung mehr angeboten. AWS stellt das Testen auf Kompatibilitätsprobleme ein. Wenn Sie weiterhin Support erhalten möchten, müssen Sie auf die neueste WorkSpaces-Clientversion aktualisieren.

In dieser Tabelle finden Sie weitere Informationen zur Unterstützung für bestimmte Versionen.

Windows-Client	Allgemeiner Support	Technische Beratung	EOL
2.x	2018	31. März 2023	31. August 2023

Linux-Client	Allgemeiner Support	Technische Beratung	EOL
4.x für Ubuntu 18.04	12. August 2021	31. März 2023	31. August 2023
3.x für Ubuntu 18.04	25. November 2019	31. März 2023	31. August 2023

macOS-Client	Allgemeiner Support	Technische Beratung	EOL
2.x	2019	31. März 2023	31. August 2023
1.x	2018	31. März 2023	31. August 2023

iPad-Client	Allgemeiner Support	Technische Beratung	EOL
1.x	2018	31. März 2023	31. August 2023

Android-Client	Allgemeiner Support	Technische Beratung	EOL
2.x	2019	31. März 2023	31. August 2023
1.x	2018	31. März 2023	31. August 2023

Web-Zugriff	Allgemeiner Support		
Google Chrome	Aktuelle Version plus zwei neueste Hauptversionen		
Firefox	Aktuelle Version plus zwei neueste Hauptversionen		

Web-Zugriff	Allgemeiner Support		
Microsoft Edge	Aktuelle Version plus zwei neueste Hauptversionen		

Nicht unterstützte Clients

Die folgenden WorkSpaces-Clients werden nicht unterstützt.

Betriebssystem	Client-Version	Allgemeiner Support	Technische Beratung	EOL	Hinweise
Windows	5.11	03. Juli 2023	1. Oktober 2023	1. Oktober 2023	Aufgrund von Qualitätsproblemen nicht unterstützt
Windows	5.10	19. Juni 2023	1. Oktober 2023	1. Oktober 2023	Aufgrund von Qualitätsproblemen nicht unterstützt
Windows	5.9	09. Mai 2023	1. Oktober 2023	1. Oktober 2023	Aufgrund von Qualitätsproblemen nicht unterstützt

EOL – Häufig gestellte Fragen

Ich verwende eine Version eines WorkSpaces-Clients, der sein EOL-Datum erreicht hat. Was muss ich tun, um auf eine unterstützte Version zu aktualisieren?

Gehen Sie zur Downloadseite des WorkSpaces-Clients, um eine vollständig unterstützte Version von WorkSpaces herunterzuladen und zu installieren.

Kann ich mit einem unterstützten WorkSpace eine Version des WorkSpaces-Clients verwenden, die ihr EOL-Datum erreicht hat?

Wir empfehlen dringend, Ihre Clients auf die neueste Version zu aktualisieren, da frühere Fehlerbehebungen und Funktionen nicht mehr auf Clientversionen angewendet werden, die ihr EOL-Datum erreicht haben. Wenn Sie eine Clientversion verwenden, deren EOL-Datum erreicht wurde, wenden Sie sich an das AWS-Support-Team, um weitere Informationen zu erhalten.

Ich verwende eine Version eines WorkSpaces-Clients, der sein EOL-Datum erreicht hat. Kann ich trotzdem Probleme damit melden?

Sie müssen zuerst auf eine unterstützte Version aktualisieren und versuchen, das Problem zu reproduzieren. Wenn das Problem mit der unterstützten Version weiterhin besteht, wenden Sie sich an das AWS-Support-Team.

Ich verwende eine unterstützte WorkSpaces-Clientversion auf einem Betriebssystem, das sein EOL-Datum erreicht hat. Kann ich trotzdem Probleme damit melden?

Technische Unterstützung und Software-Updates sind für Betriebssysteme, die das EOL-Datum erreicht haben, nicht mehr verfügbar und AWS bietet keinen Support für WorkSpaces-Clients, die Betriebssysteme verwenden, deren EOL-Datum erreicht wurde. Verwenden Sie ein unterstütztes Betriebssystem, um sicherzustellen, dass Sie Unterstützung für Ihre WorkSpaces-Clients erhalten.

Amazon- WorkSpaces Kontingente

Amazon WorkSpaces stellt verschiedene Ressourcen bereit, die Sie in Ihrem Konto in einer bestimmten Region verwenden können, darunter WorkSpaces, Images, Pakete, Verzeichnisse, Verbindungsaliase und IP-Kontrollgruppen. Wenn Sie Ihr Amazon-Web-Services-Konto erstellen, legen wir Standardkontingente (auch als Limits bezeichnet) für die Anzahl der Ressourcen fest, die Sie erstellen können.

Im Folgenden sind die Standardkontingente für WorkSpaces für Ihr AWS Konto aufgeführt. Sie können die Service-Quotas-Konsole verwenden, um Standardkontingente anzuzeigen und Kontingenterhöhungen für einstellbare Kontingente anzufordern.

In einigen Regionen, in denen Service Quotas nicht verfügbar sind, müssen Sie eine Supportanfrage einreichen, um eine Erhöhung des Limits zu beantragen. Weitere Informationen zu Kontingenten finden Sie unter Anzeigen von Service Quotas und Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ressource	Standard	Beschreibung	Einstellbar
WorkSpaces	1	Die maximale Anzahl von WorkSpaces in diesem Konto in der aktuellen Region.	Ja
Grafiken WorkSpaces	0	Die maximale Anzahl von Graphics WorkSpaces in diesem Konto in der aktuellen Region. **Note** Das Graphics-Paket wird nach dem 30. November 202 nicht mehr	Ja

Ressource	Standard	Beschreibung	Einstellbar
		unterstützt. Wir empfehlen, Ihr WorkSpaces zu Graphics.g4dn-Paket zu migrieren. Weitere Informationen finden Sie unter Migrieren eines WorkSpace.	
Graphics.g4dn WorkSpaces	0	Die maximale Anzahl von Graphics.g4dn WorkSpaces in diesem Konto in der aktuellen Region.	Ja
GraphicsPro WorkSpaces	0	Die maximale Anzahl von GraphicsPro WorkSpaces in diesem Konto in der aktuellen Region.	Ja
GraphicsPro.g4dn WorkSpaces	0	Die maximale Anzahl von GraphicsPro.g4dn WorkSpaces in diesem Konto in der aktuellen Region.	Ja

Ressource	Standard	Beschreibung	Einstellbar
Standby WorkSpaces	0	Die maximale Anzahl von WorkSpaces in diesem Konto in der aktuellen Region.	Ja
Bundles	50	Die maximale Anzahl von Bundles in diesem Konto in der aktuellen Region. Dieses Kontingent gilt nur für benutzerdefinierte Bundles, nicht für öffentliche Bundles.	Nein
Verbindungs-Aliasse	20	Die maximale Anzahl von Verbindungs-Aliassen in diesem Konto in der aktuellen Region.	Nein
Verzeichnisse	50	Die maximale Anzahl von Verzeichnissen, die für die Verwendung mit Amazon WorkSpaces in diesem Konto in der aktuellen Region registriert werden können.	Nein
Images	40	Die maximale Anzahl von Images Clustern in diesem Konto in der aktuellen Region.	Ja

Ressource	Standard	Beschreibung	Einstellbar
IP-Zugriffskontrollgruppen	100	Die maximale Anzahl von IP-Zugriffskontrollgruppen in diesem Konto in der aktuellen Region.	Nein
IP-Zugriffskontrollgruppen pro Verzeichnis	25	Die maximale Anzahl von IP-Zugriffskontrollgruppen pro Verzeichnis in diesem Konto in der aktuellen Region.	Nein
Regeln pro IP-Zugriffskontrollgruppe	10	Die maximale Anzahl von Regeln pro IP-Zugriffskontrollgruppe in diesem Konto in der aktuellen Region.	Nein

API-Drosselung

Die zulässige Rate beträgt zwei Aufrufe pro Sekunde. Weitere Informationen finden Sie unter Drosselungsausnahmen.

WorkSpaces Versionen des Host-Agents für das Streaming-Protokoll (WSP)

Der Host-Agent des WorkSpaces Streaming-Protokolls (WSP) ist ein Host-Agent, der in Ihrem ausgeführt wird. WorkSpace Er streamt Ihre Pixel WorkSpace an eine Client-Anwendung und umfasst Sitzungsfunktionen wie bidirektionales Audio- und Videosignal sowie Drucken. Weitere Informationen zum WorkSpaces Streaming Protocol (WSP) finden Sie unter Protokolle für Amazon WorkSpaces.

Wir empfehlen, die Host-Agent-Software auf dem neuesten Stand zu halten. Sie können Ihren manuell neu starten WorkSpaces , um den WSP-Host-Agenten zu aktualisieren. Der WSP-Host-Agent wird auch während des regulären WorkSpaces Standard-Wartungsfensters automatisch aktualisiert. Weitere Informationen zu Wartungsfenstern finden Sie unter WorkSpace Wartung. Für einige dieser Funktionen ist die neueste WorkSpaces Client-Version erforderlich. Weitere Informationen zu den neuesten Client-Versionen finden Sie unter WorkSpaces Clients.

In der folgenden Tabelle sind die Änderungen in den einzelnen Versionen des WSP-Host-Agenten beschrieben.

Veröffentlichung	Datum	Änderungen
• Ubuntu WorkSpaces - 2.1.0.1342	29. Februar 2024	• Die bevorzugte Webcam-Au flösung wurde auf 480x360 und 640x480 geändert. • Fehlerbehebungen und Leistungs verbesserungen.
• WorkSpaces Windows - 2.0.0.1425	22. Februar 2024	• Unterstützung für WebAuthn Sitzungsumleitungsanfragen von Webanwendungen, die in Remote-Browsern von Google Chrome oder Microsoft Edge ausgeführ t werden, wurde hinzugefügt. Diese Funktion fügt eine einmalige Browseraufforderung hinzu, in der

Veröffentlichung	Datum	Änderungen
		der Benutzer aufgefordert wird, die WebAuthn DCV-Umleitungserweiterung zu aktivieren. Sie wird nur auf Windows WorkSpaces - und WorkSpaces systemeigenen Clients unterstützt. • Es wurde ein Problem behoben, bei dem beim Einloggen manchmal ein weißer oder eingefrorener Bildschirm angezeigt wurde. • Fehlerbehebungen und Leistungsverbesserungen.
• Windows WorkSpaces - 2.0.0.1304	11. Januar 2024	• Ein Fehler im Zusammenhang mit möglichen Streaming-Einfrierungen beim Einloggen wurde behoben. • Ein Fehler im Zusammenhang mit der Protokollierung wurde behoben.

Veröffentlichung	Datum	Änderungen
• Windows - 2.0.0.1288 WorkSpaces	16. November 202	• Unterstützung für den Indirect Display Driver (IDD) unter Windows 10+ wurde hinzugefü gt, wodurch der CPU-Verbrauch gesenkt und die Streaming-Leistung verbessert wird. • Neue Gruppenrichtlinieneinstellung zum Aktivieren oder Deaktivieren des IDD-Treibers hinzugefügt. • Fehler im Zusammenhang mit der Transparenz von Bildern in der Zwischenablage wurden behoben. • Es wurden Fehler behoben, bei denen Windows-Skalierung sfaktoren beibehalten wurden. • Fehlerbehebungen und Leistungs verbesserungen.
• Windows WorkSpaces - 2.0.0.1164	13. Oktober 2023	• Unterstützung für VSync im virtuellen Bildschirmtreiber wurde hinzugefügt. • Es wurde eine neue Gruppenri chtlinieneinstellung hinzugefügt, um VSync zu aktivieren oder zu deaktivieren. • Probleme mit erneuten Verbindun gen und Zuverlässigkeit wurden verbessert. • Fehlerbehebungen und Leistungs verbesserungen.

Veröffentlichung	Datum	Änderungen
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu - 2.1.0.1086 WorkSpaces	18. August 2023	• Es wurde eine neue Einstellung hinzugefügt, um die Zeitzonen umleitung zu aktivieren oder zu deaktivieren. • Das Anmelde-Timeout wurde verlängert und eine Konfigura tionsoption hinzugefügt. • Das Gateway wurde verbessert, um schnellere erneute Verbindun gen nach einer Unterbrechung zu ermöglichen. • Fehlerbehebungen und Leistungs verbesserungen.
• Amazon Linux WorkSpaces - 2.0.0.907	30. Juni 2023	• Unterstützung für das DCV-Erwei terungs-SDK wurde hinzugefügt, um ISV-spezifische Integrationen zu ermöglichen. • Das Verhalten beim Trennen wurde geändert, sodass beim Abmelden die Sitzung des Benutzers beendet wird. • Unterstützung für die Zeitzonen umleitung wurde hinzugefügt. • Das Anmelde-Timeout wurde verlängert und eine Konfigura tionsoption hinzugefügt. • Probleme mit dem Upgrade wurden behoben. • Fehlerbehebungen und Leistungs verbesserungen.

Veröffentlichung	Datum	Änderungen
• Windows - 2.0.0.829 WorkSpaces	08. Juni 2023	• Das Verhalten beim Trennen wurde geändert, sodass beim Abmelden die Sitzung des Benutzers beendet wird. • Fehler im Zusammenhang mit der A/V-Synchronisierung und japanischen Tastaturen wurden behoben. • Die Zuverlässigkeit des WSP-Installers wurde verbessert.
• Ubuntu - 2.1.0.829 WorkSpaces	16. Mai 2023	• Das Verhalten beim Trennen wurde geändert, sodass beim Abmelden die Sitzung des Benutzers beendet wird. • Unterstützung für das DCV-Erweiterungs-SDK wurde hinzugefügt, um ISV-spezifische Integrationen zu ermöglichen. • Unterstützung für die Zeitzonenumleitung wurde hinzugefügt. • Probleme mit dem Upgrade wurden behoben.

Veröffentlichung	Datum	Änderungen
• Windows - 2.0.0.799 WorkSpaces	8. Mai 2023	• Verbesserter UDP-basierter QUIC-Transport mit verschied enen Bildqualitäts- und Leistungs optimierungen. • Unterstützung für das DCV-Erwei terungs-SDK wurde hinzugefügt, um ISV-spezifische Integrationen zu ermöglichen. • Es wurden neue Gruppenrichtlinien einstellungen hinzugefügt, um das Erweiterungs-SDK zu aktivieren oder zu deaktivieren. • Die Tastaturlayouts für Koreanisc h, Japanisch und Deutsch wurden verbessert. • Es wurden Fehler im Zusammenh ang mit Problemen beim Einfriere n von Sitzungen, Hardwareb eschleunigung, Druckerumleitung, Ausführlichkeit der Protokolle und Gruppenrichtlinieneinstellungen für Ziel-FPS behoben.

Note

- Informationen dazu, wie Sie Ihre Host-Agent-Version überprüfen können, finden Sie unter Welche Client- und Host-Betriebssysteme werden von der neuesten WSP-Version unterstützt?
- Informationen zum Aktualisieren Ihrer Host-Agent-Version finden Sie unter Wenn ich bereits eine WSP habe WorkSpace, wie aktualisiere ich sie? .
- Versionshinweise zur WSP macOS-Client-Version finden Sie in den Versionshinweisen im Abschnitt WorkSpaces macOS-Client-Anwendung des WorkSpaces Benutzerhandbuchs.

- Versionshinweise zur WSP Windows-Client-Version finden Sie in den Versionshinweisen im Abschnitt WorkSpaces Windows-Client-Anwendung des WorkSpaces Benutzerhandbuchs.

Von WSP unterstützte SDK-Erweiterung

Das Amazon WorkSpaces Streaming Protocol (WSP) basiert auf der NICE-DCV-Technologie und ermöglicht einen leistungsstarken Remotezugriff auf WorkSpaces-Instances für eine Vielzahl von Workloads und Anwendungsfällen. Mit dem NICE DCV Extension SDK können Entwickler die WSP-WorkSpaces-Erfahrung für Endbenutzer anpassen:

- Erleichterung der Unterstützung von kundenspezifischer Hardware.
- Verbesserung der Benutzerfreundlichkeit von Drittanbieteranwendungen in Remotesitzungen. Zum Beispiel das Hinzufügen eines lokalen Audioabschlusses für VoIP-Anwendungen oder der lokalen Videowiedergabe für Konferenzanwendungen.
- Bereitstellung von Barrierefreiheitssoftware wie Bildschirmlesegeräten mit Informationen über die Remotesitzung und über remote ausgeführte Anwendungen.
- Möglichkeit für Sicherheitssoftware, den Sicherheitsstatus des lokalen Endpunkts zu analysieren, um Richtlinien für den bedingten Zugriff zu ermöglichen.
- Durchführung beliebiger Datenübertragungen über eine etablierte Remotesitzung.

Informationen zu den ersten Schritten mit dem NICE DCV Extension SDK finden Sie in der Dokumentation zum NICE DCV Extension SDK. Das SDK selbst finden Sie im GitHub-Repository zum NICE DCV Extension SDK. Darüber hinaus finden Sie Integrationsbeispiele für das SDK im GitHub-Samples-Repository für das NICE DCV Extension SDK.

Die folgenden WorkSpaces-Clients werden nicht unterstützt.

- Streaming Protocol – WorkSpaces Streaming Protocol (WSP)
- WorkSpaces-Windows-Client – Windows: 5.9.0.4110 und höher.

> **Note**
>
> WorkSpaces-Android, iOS-Clients, Webzugriff unterstützt das NICE DCV Extension SDK nicht.

- Unterstützte WorkSpaces – Windows-, Linux- und Ubuntu-Server

Dokumentverlauf für WorkSpaces

In der folgenden Tabelle werden wichtige Änderungen am WorkSpaces-Service und dem Amazon WorkSpaces-Administratorhandbuch ab dem 1. Januar 2018 beschrieben. Wir aktualisieren die Dokumentation regelmäßig, um das Feedback, das Sie uns senden, einzuarbeiten.

Sie können den WorkSpaces-RSS-Feed abonnieren, um Benachrichtigungen über diese Aktualisierungen zu erhalten.

Änderung	Beschreibung	Datum
Aktualisieren der verwaltet en Richtlinie AmazonWor kSpacesAdmin	WorkSpaces hat die workspaces:Restore Workspace-Aktion zur verwalteten Richtlinie AmazonWorkSpacesAdmin hinzugefügt und Administr atoren Zugriff auf die Wiederherstellung von WorkSpaces gewährt.	17. Juli 2023
Von WSP unterstützte SDK-Erweiterung	Mit dem NICE DCV Extension SDK können Entwickler die WSP-WorkSpaces-Erfahrung für Endbenutzer anpassen.	25. Mai 2023
Versionen der Host-Agents für WorkSpaces Streaming Protocol (WSP)	Versionshinweise für WorkSpaces Streaming Protocol (WSP).	8. Mai 2023
Amazon WorkSpaces in AWS GovCloud (USA Ost) eingeführ t	Amazon WorkSpaces ist in der AWS GovCloud (USA Ost) verfügbar.	3. Mai 2023
Amazon WorkSpaces Webcam-Support	Amazon WorkSpaces unterstützt jetzt Audio-Video (AV) in Echtzeit, indem lokale Webcam-Vi	05. April 2021

	deoeingaben mithilfe des WorkSpaces Streaming Protocol (WSP) nahtlos an Windows-WorkSpaces-Desktops umgeleitet werden.	
Amazon-WorkSpaces-Smartcard-Unterstützung mit der WorkSpaces-macOS-Clientanwendung	Sie können jetzt die Amazon-WorkSpaces-macOS-Clientanwendung mit Common Access Card (CAC) und Personal Identity Verification (PIV) Smartcards verwenden. Die Smartcard-Unterstützung ist in WorkSpaces verfügbar, die das WorkSpaces Streaming Protocol (WSP) verwenden.	05. April 2021
Amazon-WorkSpaces-Paketverwaltungs-APIs	Die Amazon-WorkSpaces-Paketverwaltungs-APIs sind jetzt verfügbar. Diese API-Aktionen unterstützen das Erstellen, Löschen und Zuordnen von Abbildern für WorkSpaces-Pakete.	15. März 2021
Amazon WorkSpaces in Asien-Pazifik (Mumbai) eingeführt	Amazon WorkSpaces ist jetzt in der Region Asien-Pazifik (Mumbai) verfügbar.	8. März 2021

WorkSpaces Streaming Protocol (WSP)	Das WorkSpaces Streaming Protocol (WSP) ist jetzt sowohl für in der Lizenz enthaltene (Windows Server 2016) als auch für BYOL-Windows-10-basierte WorkSpaces für alle Pakettypen außer Graphics und GraphicsPro verfügbar . WSP ist auch für Linux-WorkSpaces in der Region AWS GovCloud (USA-West) verfügbar.	1. Dezember 2020
Smartcards	Amazon WorkSpaces unterstützt jetzt die Smartcard -Authentifizierung vor der Sitzung (Anmeldung) und während der Sitzung auf Windows- und Linux-Wor kSpaces in der Region AWS GovCloud (USA West).	1. Dezember 2020
Freigeben von benutzerd efinierten Abbildern	Sie können benutzerd efinierte WorkSpaces-Abbilde r innerhalb derselben Region für AWS-Konten freigeben. Im Empfängerkonto können diese Kopien dann verwendet werden, um Pakete zum Erstellen von Paketen und Starten neuer WorkSpaces zu erstellen.	1. Oktober 2020

Regionsübergreifende Umleitung	Sie können die regionsübergreifende Umleitung nutzen. Die regionsübergreifende Umleitung arbeitet mit Ihren DNS-Routing-Richtlinien (Domain Name System), die Ihre WorkSpaces-Benutzer zu alternativen WorkSpaces umleiten, wenn ihre primären WorkSpaces nicht verfügbar sind.	10. September 2020
Abonnieren von Microsoft Office 2016 oder 2019 für BYOL-WorkSpaces	Sie können jetzt Microsoft Office Professional 2016 oder 2019 abonnieren, die von AWS auf Bring-Your-Own-Windows-License-(BYOL)-WorkSpaces bereitgestellt werden.	3. September 2020
BYOL-Automatisierung in China (Ningxia)	Sie können die Bring-Your-Own-License (BYOL)-Lizenzautomatisierung zur Vereinfachung der Verwendung von Windows 10-Desktoplizenzen für Ihre WorkSpaces in China (Ningxia) verwenden.	2. April 2020

Image Checker	Mit dem Abbildüberprüfungstool können Sie feststellen, ob Ihr Windows-WorkSpace die Anforderungen für die Erstellung von Abbildern erfüllt. Image Checker führt eine Reihe von Tests auf dem WorkSpace durch, den Sie zum Erstellen des Abbilds verwenden möchten, und bietet Anleitungen zum Beheben gefundener Probleme.	30. März 2020
Migrieren von WorkSpaces	Mit der Amazon WorkSpaces-Migrationsfunktion können Sie einen WorkSpace von einem Bundle in ein anderes migrieren, wobei die Daten auf dem Benutzervolume beibehalten werden. Sie können diese Funktion verwenden, um WorkSpaces von der Windows 7-Desktopumgebung zur Windows 10-Desktopumgebung zu migrieren. Sie können diese Funktion auch verwenden, um WorkSpaces von einem öffentlichen oder benutzerdefinierten Bundle zu einem anderen zu migrieren.	9. Januar 2020

PrivateLink-Integration für Amazon-WorkSpaces-APIs	Sie können über einen Schnittstellenendpunkt in Ihrer Virtual Private Cloud (VPC) eine direkte Verbindung mit Amazon-WorkSpaces-API-Endpunkten herstellen, anstatt sich über das Internet zu verbinden. Wenn Sie einen VPC-Schnittstellenendpunkt verwenden, findet die Kommunikation zwischen Ihrer VPC und dem Amazon-WorkSpaces-API-Endpunkt vollständig und sicher innerhalb des AWS-Netzwerks statt.	25. November 2019
Linux-Client für Amazon WorkSpaces	Benutzer können nun den Linux-Client verwenden, um auf ihre WorkSpaces zuzugreifen.	25. November 2019
Amazon WorkSpaces in China (Ningxia) eingeführt	Amazon WorkSpaces ist jetzt in der Region China (Ningxia) verfügbar.	13. November 2019
Wiederherstellen des letzten bekannten fehlerfreien Status von WorkSpaces	Sie können die Wiederherstellungsfunktion verwenden, um einen WorkSpace auf den letzten bekannten fehlerfreien Zustand zurückzusetzen.	18. September 2019

FIPS-Endpunktverschlüsselung	Zur Einhaltung des Federal Risk and Authorization Management Program (FedRAMP) bzw. des Cloud Computing Security Requirements Guide (SRG) des US-Verteidigungsministeriums (Department of Defense, DoD) müssen Sie Amazon WorkSpaces so konfigurieren, dass es die Endpunktverschlüsselung für die Federal Information Processing Standards (FIPS) auf Verzeichnisebene verwendet.	12. September 2019
Kopieren von WorkSpace-Abbildern	Sie können Ihre Abbilder innerhalb derselben Region oder zwischen verschiedenen Regionen kopieren.	27. Juni 2019
Self-Service-WorkSpace-Verwaltungsfunktionen für Benutzer	Sie können Self-Service-WorkSpace-Verwaltungsfunktionen für Ihre Benutzer aktivieren, um ihnen mehr Kontrolle über ihre Erfahrung zu bieten.	19. November 2018
BYOL-Automatisierung	Sie können die Bring-Your-Own-License (BYOL)-Lizenzautomatisierung zur Vereinfachung der Verwendung Ihrer Windows 7- und Windows 10-Desktoplizenzen für Ihre WorkSpaces verwenden.	16. November 2018

PowerPro- und GraphicsPro-Pakete	Die PowerPro- und GraphicsPro-Pakete sind jetzt für WorkSpaces verfügbar.	18. Oktober 2018
Überwachen erfolgreicher WorkSpace-Anmeldungen	Sie können Ereignisse aus Amazon CloudWatch Events zum Überwachen von und Reagieren auf erfolgreiche WorkSpace-Anmeldungen verwenden.	17. September 2018
Web Access für Windows-10-WorkSpaces	Benutzer können jetzt mithilfe des Web Access-Clients auf WorkSpaces mit der Windows 10-Desktop-Umgebung zugreifen.	24. August 2018
URI-Anmeldung	Sie können Uniform Resource Identifiers (URIs) verwenden , um Benutzern den Zugriff auf ihre WorkSpaces zu gewähren.	31. Juli 2018
Amazon-Linux-WorkSpaces	Sie können Amazon-Linux-WorkSpaces für Ihre Benutzer bereitstellen.	26. Juni 2018
IP-Zugriffskontrollgruppen	Sie können kontrollieren, von welchen IP-Adressen die Benutzer auf ihre WorkSpaces zugreifen können.	30. April 2018
Direkte Upgrades	Sie können Ihre Windows 10-BYOL-WorkSpaces auf eine neuere Version von Windows 10 aktualisieren.	9. März 2018

Frühere Aktualisierungen

In der folgenden Tabelle sind wichtige Ergänzungen zum Amazon-WorkSpaces-Service und der einhergehenden Dokumentation vor dem 1. Januar 2018 enthalten.

Änderung	Beschreibung	Datum
Flexible Datenverarbeitungs-Optionen	Sie können für Ihre WorkSpaces zwischen den Paketen Value, Standard, Performance und Power wählen	22. Dezember 2017
Konfigurierbarer Speicher	Sie können die Größe der Stamm- und Benutzer-Volumes für Ihre WorkSpaces beim Start konfigurieren und die Größe dieser Volumes später erhöhen.	22. Dezember 2017
Kontrollieren des Gerätezugriffs	Sie können die Gerätetypen angeben, von denen aus ein Zugriff auf WorkSpaces möglich ist. Außerdem können Sie den Zugriff auf WorkSpaces auf vertrauenswürdige Geräte einschränken (auch bekannt als verwaltete Geräte).	19. Juni 2017
Inter-Forest-Vertrauensstellungen	Sie können eine Vertrauensstellung zwischen AWS Managed Microsoft AD und Ihrer on-premises Microsoft Active Directory-Domain einrichten und anschließend WorkSpaces für Benutzer in der on-premises Domain bereitstellen.	9. Februar 2017
Windows Server 2016-Bundles	Amazon WorkSpaces bietet Pakete mit der Windows-10-Desktoperfahrung von Windows Server 2016 an.	29. November 2016
Internetzugang	Sie können über WorkSpaces Web Access in einem Webbrowser auf Ihre Windows-WorkSpaces zugreifen.	18. November 2016

Änderung	Beschreibung	Datum
Stündliche WorkSpaces	Sie können Ihre WorkSpaces so konfigurieren, dass die Nutzung der Benutzer nach Stunden berechnet wird.	18. August 2016
Windows 10 BYOL	Sie können Ihre Desktoplizenz für Windows 10 in WorkSpaces nutzen (BYOL).	21. Juli 2016
Unterstützung von Markierungen	Sie können Tags verwenden, um Ihre WorkSpaces zu verwalten und zu überwachen.	17. Mai 2016
Gespeicherte Registrierungen	Jedes Mal, wenn Sie einen neuen Registrierungscode eingeben, wird dieser vom WorkSpaces-Client gespeichert. Dies erleichtert den Wechsel zwischen WorkSpaces in verschiedenen Verzeichnissen oder Regionen.	28. Januar 2016
Windows 7 BYOL, Chromebook-Client, WorkSpace-Verschlüsselung	Sie können Ihre Windows-7-Desktop-Lizenz in WorkSpaces (BYOL) nutzen und den Chromebook-Client und die WorkSpace-Verschlüsselung verwenden.	1. Oktober 2015
CloudWatch-Überwachung	Zusätzliche Informationen zur CloudWatch-Überwachung.	28. April 2015
Automatische Wiederherstellung der Sitzungsverbindung	Zusätzliche Informationen zur Funktion für die automatischen Wiederherstellung der Sitzungsverbindung in Client-Anwendungen mit WorkSpaces-Desktop.	31. März 2015
Öffentliche IP-Adresse	Sie können Ihren WorkSpaces eine öffentliche IP-Adresse automatisch zuweisen lassen.	23. Januar 2015
WorkSpaces im Asien-Pazifik (Singapur) eingeführt	WorkSpaces ist jetzt in der Region Asien-Pazifik (Singapur) verfügbar.	15. Januar 2015

Änderung	Beschreibung	Datum
Wert-Paket hinzugefügt, Standard-Paket-Updates, Office 2013 hinzugefügt	Das Wert-Paket ist verfügbar, die Standard-Paket-Hardware wurde aktualisiert und Microsoft Office 2013 ist in Plus-Paketen verfügbar.	6. November 2014
Abbild- und Bundle Support	Sie können ein Abbild eines von Ihnen angepassten WorkSpace und ein benutzerd efiniertes WorkSpace-Paket aus dem Abbild erstellen.	28. Oktober 2014
PCoIP-Zero-Client unterstützt	Sie können auf WorkSpaces-PCoIP-Zero-Clien t-Geräte zugreifen.	15. Oktober 2014
WorkSpaces in Asien-Pazifik (Tokio) eingeführt	WorkSpaces ist jetzt in der Region Asien-Paz ifik (Tokio) verfügbar.	26. August 2014
Support für lokalen Drucker	Sie können Unterstützung für lokale Drucker für WorkSpaces aktivieren.	26. August 2014
Multi-Faktor-Authentifizierung	Sie können die Multi-Faktor-Authentifizierung in verbundenen Verzeichnissen verwenden.	11. August 2014
Standard-OU-Unterstützung und Zieldomänen-Unters tützung	Sie können eine Standard-Organisationseinhe it (OU) auswählen, in der Ihre WorkSpace-Computer-Konten platziert werden, und eine separate Domain, in der Ihre WorkSpace-Computer-Konten erstellt werden.	7. Juli 2014
Zusätzliche Sicherhei tsgruppen	Sie können Ihren WorkSpaces eine Sicherhei tsgruppe hinzufügen.	7. Juli 2014
WorkSpaces in Asien-Pazifik (Sydney) eingeführt	WorkSpaces ist jetzt in der Region Asien-Paz ifik (Sydney) verfügbar.	15. Mai 2014
WorkSpaces in Europa (Irland) eingeführt	WorkSpaces ist jetzt in der Region Europa (Irland) verfügbar.	5. Mai 2014

Änderung	Beschreibung	Datum
Öffentliches Beta	WorkSpaces ist als öffentliche Beta-Version verfügbar.	25. März 2014

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.