POST EDIT. ADDED PROOFREAD. ADDED PP1

# Amazon WorkSpaces Thin Client

# Amazon WorkSpaces Thin Client: POST EDIT. ADDED PROOFREAD. ADDED PP1

# Table of Contents

# Was ist die Amazon WorkSpaces Thin Client Administratorkonsole?

Mit der Amazon WorkSpaces Thin Client-Administratorkonsole können Administratoren WorkSpaces Thin Client-Umgebungen und -Geräte über ein WorkSpaces Thin Client-Portal verwalten. Von dieser Webkonsole aus können Administratoren Umgebungen erstellen, Geräte verwalten und Parameter für WorkSpaces Thin Client-Benutzer in ihrem Netzwerk festlegen.

Virtuelle Desktop-Umgebungen, die Sie für WorkSpaces Thin Client verwenden, müssen in ihrer eigenen Konsole erstellt oder geändert werden.

> **Important**
>
> Damit die WorkSpaces Thin Client-Administratorkonsole ordnungsgemäß funktioniert, muss Ihr System zunächst bestimmte Anforderungen erfüllen. Diese Anforderungen sind unter Voraussetzungen und Konfigurationen aufgeführt.

Themen



## Verwenden Sie zum ersten Mal?

Wenn Sie die WorkSpaces Thin Client-Administratorkonsole zum ersten Mal verwenden, empfehlen wir Ihnen, zunächst die folgenden Abschnitte zu lesen:

- Die WorkSpaces Thin Client-Administratorkonsole starten
- Verwenden der WorkSpaces Thin Client-Administratorkonsole

## Architektur

Jeder WorkSpaces Thin Client ist einem Anbieter für virtuelle Desktopschnittstellen (VDI) zugeordnet. WorkSpaces Thin Client unterstützt drei VDI-Anbieter:

- Amazon WorkSpaces
- AppStream 2,0
- WorkSpaces Sicherer Browser von Amazon

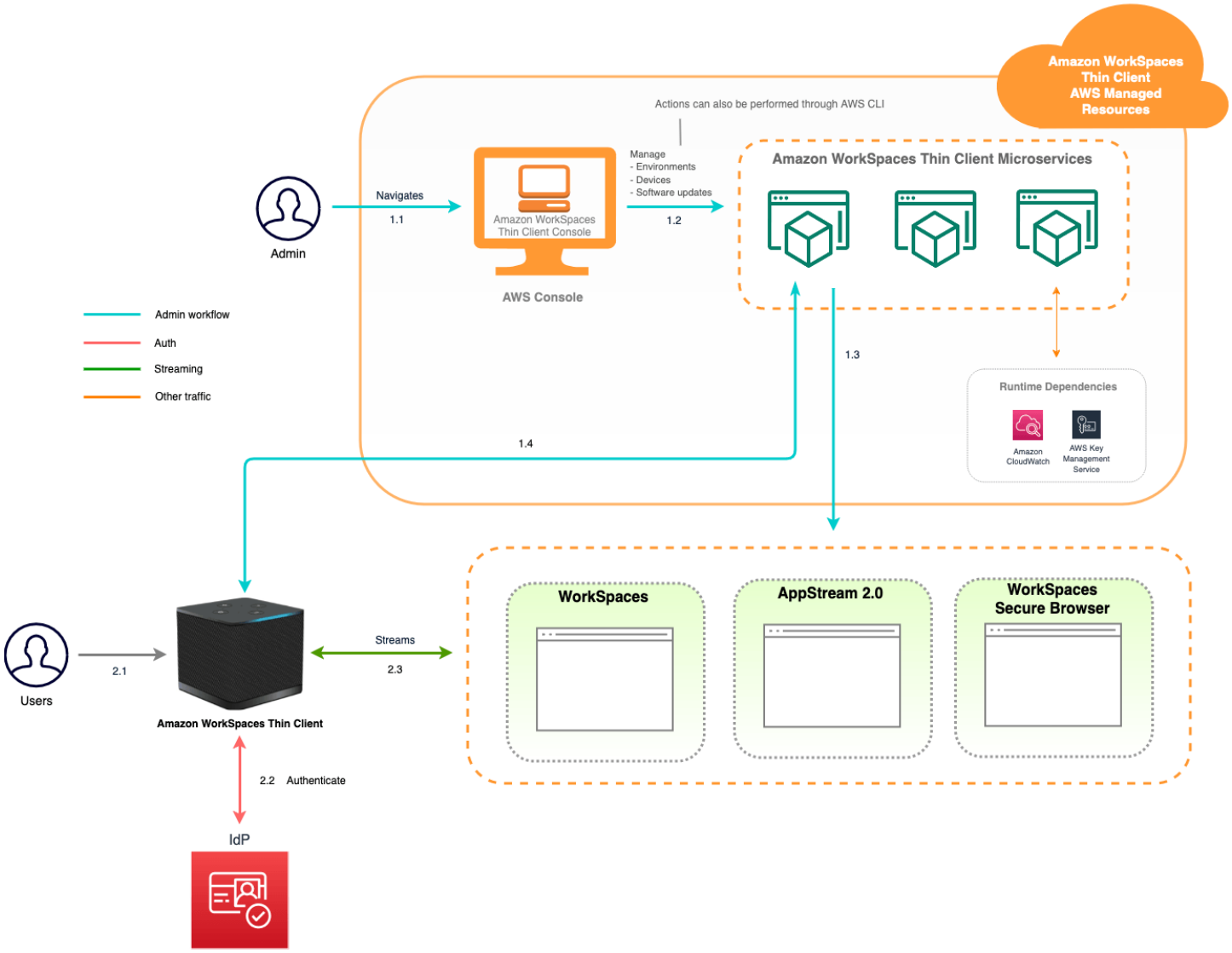
Je nach verwendetem VDI werden die Informationen für Ihren WorkSpaces Thin Client entweder über Verzeichnisse für WorkSpaces, Stacks für AppStream 2.0 und Webportal-Endpunkte für WorkSpaces Secure Browser abgerufen und verwaltet.

Weitere Informationen zu Amazon WorkSpaces finden Sie unter Erste Schritte mit der WorkSpaces Schnellinstallation. Verzeichnisse werden über das verwaltet AWS Directory Service, das die folgenden Optionen bietet: Simple AD, AD Connector oder AWS Directory Service für Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD. Weitere Informationen finden Sie im Administrationshandbuch zu AWS Directory Service.

Weitere Informationen zu AppStream 2.0 finden Sie unter Erste Schritte mit Amazon AppStream 2.0: Einrichtung mit Beispielanwendungen. AppStream 2.0 verwaltet die AWS Ressourcen, die für das Hosten und Ausführen Ihrer Anwendungen erforderlich sind, skaliert automatisch und bietet Ihren Benutzern bei Bedarf Zugriff. AppStream 2.0 bietet Benutzern Zugriff auf die Anwendungen, die sie benötigen, auf dem Gerät ihrer Wahl und bietet eine reaktionsschnelle, flüssige Benutzererfahrung, die sich nicht von nativ installierten Anwendungen unterscheidet.

Informationen zu WorkSpaces Secure Browser finden Sie unter Erste Schritte mit Amazon WorkSpaces Secure Browser. Amazon WorkSpaces Secure Browser ist ein vollständig verwalteter, Linux-basierter On-Demand-Service, der den sicheren Browserzugriff auf interne Websites und software-as-a-service (SaaS-) Anwendungen ermöglicht. Greifen Sie von vorhandenen Webbrowsern aus auf den Service zu, ohne den Verwaltungsaufwand für Infrastrukturmanagement, spezielle Clientsoftware oder Lösungen für Virtual Private Network (VPN).

Das folgende Diagramm zeigt die Architektur von WorkSpaces Thin Client.


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

# Einrichtung der Amazon WorkSpaces Thin Client-Administratorkonsole

Themen



## Registrieren bei AWS

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

## Erstellen eines IAM-Benutzers

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

| Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus. | Bis | Von | Sie können auch |
|---|---|---|---|
| Im IAM Identity Center<br><br>(Empfohlen) | Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS.<br><br>Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch. | Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center - Benutzerhandbuch. | Konfigurieren Sie den programmatischen Zugriff, indem Sie den AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch AWS CLI zu verwendenden konfigurieren. |
| In IAM<br><br>(Nicht empfohlen) | Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS. | Beachtung der Anweisungen unter Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe im IAM-Benutzerhandbuch. | Programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch konfigurieren. |

# Erste Schritte mit Ihrem VDI für Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client ist ein kostengünstiges Thin-Client-Gerät, das für die Zusammenarbeit mit AWS End User Computing Services entwickelt wurde und Ihnen sicheren, sofortigen Zugriff auf Anwendungen und virtuelle Desktops bietet.

Wählen Sie eine virtuelle Desktop-Infrastruktur (VDI) und konfigurieren Sie sie so, dass sie mit WorkSpaces Thin Client funktioniert.

> **Important**
>
> Damit die WorkSpaces Thin Client-Administratorkonsole ordnungsgemäß funktioniert, muss Ihr System zunächst bestimmte Anforderungen erfüllen. Diese Anforderungen sind im Konfigurationsverfahren für jeden Anbieter virtueller Desktops aufgeführt.

WorkSpaces Thin Client erfordert je nach Anbieter für virtuelle Desktops spezifische Softwarekonfigurationen.

Themen



## Konfiguration WorkSpaces für Amazon WorkSpaces Thin Client

Damit WorkSpaces Thin Client mit Amazon verwendet werden kann WorkSpaces, muss Ihr Service für den Zugriff auf die WorkSpaces Verzeichnisse konfiguriert werden. Amazon WorkSpaces werden anhand ihrer Verzeichnisnamen auf der Seite WorkSpaces Thin Client Create environment in der AWS Konsole aufgeführt.

> **Note**
>
> Konfigurationen müssen vorgenommen werden, bevor die Konsole zum ersten Mal verwendet wird. Es wird nicht empfohlen, die erforderlichen Funktionen zu ändern, nachdem Sie die Konsole verwendet haben.

## Bevor Sie beginnen

Stellen Sie sicher, dass Sie über ein AWS Konto verfügen, um ein Konto zu erstellen oder zu verwalten. WorkSpace Gerätebenutzer benötigen jedoch kein AWS Konto, um eine Verbindung herzustellen und sie zu WorkSpaces verwenden.

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

- Wenn Sie ein starten WorkSpace, wählen Sie ein WorkSpace Paket aus. Weitere Informationen finden Sie unter WorkSpaces Amazon-Pakete.
- Wählen Sie beim Start eines aus WorkSpace, welches Protokoll Sie mit Ihrem Paket verwenden möchten. Weitere Informationen finden Sie unter Protokolle für Amazon WorkSpaces.
- Wenn Sie eine starten WorkSpace, geben Sie die Profilinformationen für jeden Benutzer an, einschließlich Benutzername und E-Mail-Adresse. Benutzer vervollständigen ihre Profile, indem sie ein Passwort erstellen. Informationen über WorkSpaces und Benutzer werden in einem Verzeichnis gespeichert. Weitere Informationen finden Sie unter Verzeichnisse verwalten für WorkSpaces.
- Wenn Sie einen starten WorkSpace, aktivieren und konfigurieren Sie den WorkSpaces Webzugriff. Weitere Informationen finden Sie unter Amazon WorkSpaces Web Access aktivieren und konfigurieren

## Schritt 1: Stellen Sie sicher, dass Ihr System die WorkSpaces erforderlichen Funktionen erfüllt

Damit die WorkSpaces Thin Client-Administratorkonsole ordnungsgemäß mit Amazon funktioniert WorkSpaces, muss Ihr System die folgenden spezifischen Anforderungen erfüllen. In dieser Tabelle sind all diese unterstützten Funktionen und ihre Anforderungen aufgeführt.

| Funktion | Anforderung |
| --- | --- |
| Web-Zugriff | Aktiviert |
| Unterstütztes Betriebssystem | • Windows 10<br>• Windows 10 (Bring-Your-Own-License)<br>• Windows 11<br>• Windows 11 (Bring-Your-Own-License) |
| Unterstützte Pakete | • Microsoft Power mit Windows 10 (basierend auf Server 2016, 2019 und 2022)<br>• Microsoft Power mit Windows 10 (basierend auf Server 2016, 2019 und 2022) w Office<br>• Microsoft PowerPro mit Windows 10 (basierend auf Server 2016, 2019 und 2022)<br>• Microsoft PowerPro mit Windows 10 (auf Server 2016, 2019 und 2022) w Office<br>• Microsoft-Leistung mit Windows 10 (basieren d auf Server 2016, 2019 und 2022)<br>• Microsoft-Leistung mit Windows 10 (basieren d auf Server 2016, 2019 und 2022) w Office |
| Unterstützte Protokolle | Nur WSP |

## Schritt 2: Verwenden Sie das erweiterte Setup, um Ihr WorkSpace

Um das erweiterte Setup zu verwenden, um Ihr zu starten WorkSpace

1. Öffnen Sie die WorkSpaces Konsole unterhttps://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. Weitere Informationen finden Sie unter Konfigurieren einer VPC mit öffentlichen Subnetzen.
5. Überprüfen Sie Ihre Verzeichnisinformationen und wählen Sie Verzeichnis erstellen.

# Konfiguration von AppStream 2.0 für Amazon WorkSpaces Thin Client

AppStream 2.0-Instances werden auf der Grundlage von Stack-Namen aufgelistet und erfordern die Konfiguration einer IdP-Anmelde-URL auf der Seite „Umgebung erstellen“. Da die SAML-Authentifizierung für AppStream 2.0 nur die initiierte Authentifizierung unterstützt, muss der Administrator die richtige Anmelde-URL manuell eingeben.

> **Note**
>
> Konfigurationen müssen vorgenommen werden, bevor die Konsole zum ersten Mal verwendet werden kann. Es wird nicht empfohlen, die erforderlichen Funktionen zu ändern, nachdem Sie die Konsole verwendet haben.

## Schritt 1: Stellen Sie sicher, dass Ihr System die für AppStream Version 2.0 erforderlichen Funktionen erfüllt

Damit die WorkSpaces Thin Client-Administratorkonsole mit AppStream 2.0 ordnungsgemäß funktioniert, muss Ihr System die folgenden spezifischen Anforderungen erfüllen. In dieser Tabelle sind all diese unterstützten Funktionen und ihre Anforderungen aufgeführt.

| Funktion | Anforderung |
| --- | --- |
| Identitätsanbieter | Gehen Sie im AppStream 2.0-Administratorhandbuch zu Setting Up SAML, um einen Identity Provider zu erstellen.<br><br>Wenn Sie aufgefordert werden, die Env-Konsole zu erstellen, geben Sie Ihre IDP-Anmelde-URL ein. |

| Funktion | Anforderung |
| --- | --- |
| Betriebssystem | Windows |
| Plattformtyp | Windows Server (2012 R2, 2016 oder 2019) |
| Streaming-Protokoll | TCP-Streaming<br><br>Es gibt einen Mechanismus für automatisches Fallback für TCP, falls UDP nicht verfügbar ist. |
| Lokales Kopieren und Einfügen | Deaktivieren<br><br>Auf Stack-Ebene AppStream 2.0 konfiguriert |
| Teilen von lokalen Ordnern | Deaktivieren<br><br>Auf AppStream 2.0-Stack-Ebene konfiguriert |
| Lokales Drucken | Deaktivieren<br><br>Auf AppStream 2.0-Stack-Ebene konfiguriert |

Die Anforderung einer Bildschirmsperre durch SAML-Authentifizierung auf AppStream 2.0 wird ebenfalls unterstützt. Der Benutzerpool und die programmatische Authentifizierung werden auf dem WorkSpaces Thin Client nicht unterstützt.

## Schritt 2: Richten Sie Ihre AppStream 2.0-Stacks ein

Um Ihre Anwendungen zu streamen, erfordert AppStream 2.0 eine Umgebung, die eine Flotte, die einem Stack zugeordnet ist, und mindestens ein Anwendungs-Image umfasst. Gehen Sie wie folgt vor, um eine Flotte und einen Stack einzurichten und Benutzern Zugriff auf den Stack zu gewähren. Falls Sie dies noch nicht getan haben, empfehlen wir Ihnen, die Verfahren unter Erste Schritte mit AppStream 2.0: Einrichtung mit Beispielanwendungen auszuprobieren.

Wenn Sie ein zu verwendendes Image erstellen möchten, finden Sie weitere Informationen unter Tutorial: Erstellen eines benutzerdefinierten AppStream 2.0-Images mithilfe der AppStream 2.0-Konsole.

Wenn Sie planen, eine Flotte einer Active Directory-Domäne hinzuzufügen, konfigurieren Sie Ihre Active-Directory-Domain, bevor Sie wie folgt vorgehen. Weitere Informationen finden Sie unter Verwenden von Active Directory mit AppStream 2.0.

Aufgaben

- Erstellen einer Flotte
- Erstellen eines Stacks
- Erteilen des Zugriffs für Benutzer
- Bereinigen von Ressourcen

# Konfiguration von Amazon WorkSpaces Secure Browser für Amazon WorkSpaces Thin Client

Amazon WorkSpaces Secure Browser basieren auf ihren Webportal-Endpunkten auf der Seite WorkSpaces Thin Client Create environment in der AWS Konsole.

> **Note**
>
> Konfigurationen müssen vorgenommen werden, bevor die Konsole zum ersten Mal verwendet wird. Es wird nicht empfohlen, die erforderlichen Funktionen zu ändern, nachdem Sie die Konsole verwendet haben.

## Schritt 1: Stellen Sie sicher, dass Ihr System die für Amazon WorkSpaces Secure Browser erforderlichen Funktionen erfüllt

Damit die WorkSpaces Thin Client Administrator Console ordnungsgemäß mit Amazon WorkSpaces Secure Browser funktioniert, muss Ihr System die folgenden spezifischen Anforderungen erfüllen. In dieser Tabelle sind all diese unterstützten Funktionen und ihre Anforderungen aufgeführt.

| Funktion | Anforderung |
| --- | --- |
| Lokales Kopieren und Einfügen | Deaktivieren |
| Teilen von lokalen Ordnern | Deaktivieren |

> **Note**
>
> Die WorkSpaces Secure Browser-Erweiterung für Single Sign-On wird derzeit auf dem WorkSpaces Thin Client nicht unterstützt.

## Schritt 2: Richten Sie WorkSpaces Secure Browser-Portale ein

WorkSpaces Thin Client funktioniert mit der WorkSpaces Secure Browser VPC in einer bestimmten Konfiguration:

1. Erstellen Sie eine VPC mithilfe der AWS CodeBuild Cloudformation-Vorlage.
2. Richten Sie Ihren Identitätsanbieter ein.
3. Erstellen Sie ein Amazon WorkSpaces Secure Browser-Portal.
4. Testen Sie Ihr neues Amazon WorkSpaces Secure Browser-Portal.

# Die WorkSpaces Thin Client Administratorkonsole starten

WorkSpaces Thin Client ist ein kostengünstiges Thin Client-Gerät, das für die Zusammenarbeit mit AWS End User Computing Services entwickelt wurde und Ihnen sicheren, sofortigen Zugriff auf Anwendungen und virtuelle Desktops bietet.

Themen



## Abgedeckte Regionen

WorkSpaces Thin Client ist in den folgenden Regionen verfügbar.

In diesen Regionen ist nur die WorkSpaces Thin Client-Administratorkonsole verfügbar. WorkSpaces Thin Client-Geräte sind derzeit nur in den USA, Deutschland, Frankreich, Italien und Spanien erhältlich.

| Name der Region | Region | Endpunkt | Link zur Konsole |
|---|---|---|---|
| USA Ost (Nord-Virginia) | us-east-1 | thinclient.us-east-1.amazonaws.com | https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home |
| USA West (Oregon) | us-west-2 | thinclient.us-west-2.amazonaws.com | https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home |
| Asien-Pazifik (Mumbai) | ap-south-1 | thinclient.ap-south-1.amazonaws.com | https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home |

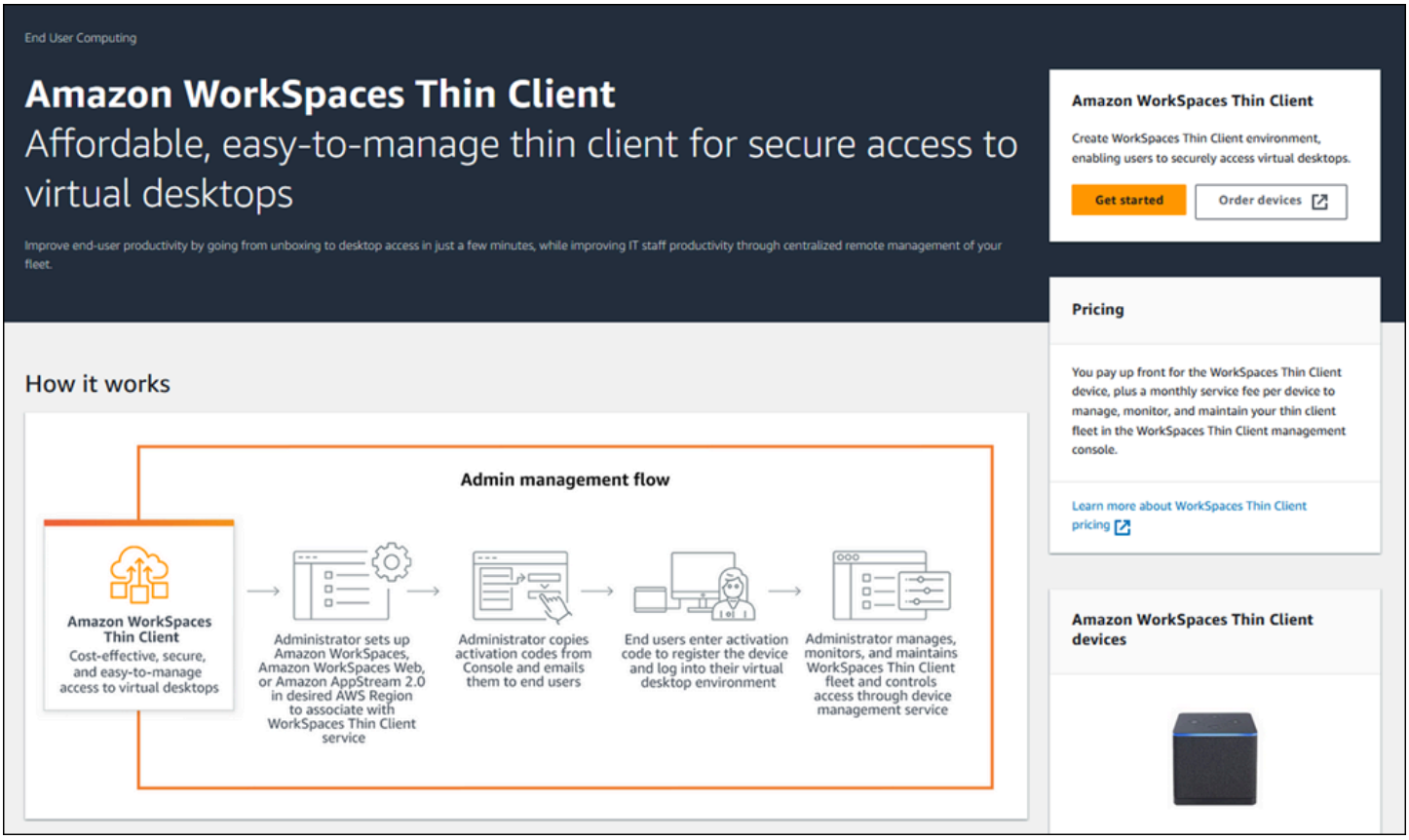
| Name der Region | Region | Endpunkt | Link zur Konsole |
|---|---|---|---|
| Europa (Irland) | eu-west-1 | thinclient.eu-west-1.amazonaws.com | https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home |
| Kanada (Zentral) | ca-central-1 | thinclient.ca-central-1.amazonaws.com | https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home |
| Europa (Frankfurt) | eu-central-1 | thinclient.eu-central-1.amazonaws.com | https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home |
| Europa (London) | eu-west-2 | thinclient.eu-west-2.amazonaws.com | https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home |

# Starten der WorkSpaces Thin Client-Administratorkonsole

Wenn Sie ein AWS Konto haben, können Sie die Administratorkonsole starten und zur WorkSpaces Thin Client-Konsole wechseln. Gehen Sie wie folgt vor, um die Konsole zu starten:

1. Loggen Sie sich in Ihr AWS Konto ein.
2. Greifen Sie auf die WorkSpaces Thin Client-Konsole zu.
3. Wählen Sie Erste Schritte und Sie werden zu Umgebungen weitergeleitet.

# Verwenden der WorkSpaces Thin Client-Administratorkonsole




Willkommen in der WorkSpaces Thin Client Administratorkonsole!

Von hier aus können Sie Ihre Flotte von WorkSpaces Thin Client-Geräten und Umgebungen für Ihr Team verwalten.

Informationen zum WorkSpaces Thin Client-Gerät finden Sie im WorkSpaces Thin Client-Benutzerhandbuch.

Fangen wir an!

Themen

- Umgebungen
- Geräte
- Software-Updates

# Umgebungen

Jedes WorkSpaces Thin Client-Gerät verwendet eine individuelle virtuelle Desktop-Umgebung, um auf seine Online-Ressourcen zuzugreifen. Benutzer greifen auf diese Umgebung zu, indem sie einen der folgenden Anbieter für virtuelle Desktops verwenden:

- Amazon WorkSpaces
- AppStream 2,0
- WorkSpaces Sicherer Browser von Amazon

## Umgebungsliste

### Details der Umgebungsliste

Name – Die dieser Umgebung zugeordnete eindeutige Kennung.

Virtueller Desktop-Service – Der virtuelle Desktop-Anbieter, den diese Umgebung verwendet.

Virtual Desktop Service ID — Die eindeutige Kennung, die der Virtual Desktop Service Provider dieser Umgebung zuweist.

Aktivierungscode — Der Code, der von Endbenutzern für den Zugriff auf die virtuelle Desktop-Umgebung verwendet wird.

Geräteanzahl — Die Anzahl der WorkSpaces Thin Client-Geräte, die auf diese Umgebung zugreifen.

### Aktionen der Umgebungsliste

Suche – Sucht alle Umgebungen, die Sie verwalten.

Aktualisieren – Aktualisiert die Umgebungsliste.

Details anzeigen – Zeigt Umgebungsdetails an.

Aktionen — Öffnet eine Dropdownliste, in der Sie eine Umgebung bearbeiten oder löschen können.

Umgebung erstellen – Startet den Prozess der Erstellung einer Umgebung.

Umgebung erstellen – Startet den Prozess der Erstellung einer Umgebung.

Themen

- Details der Umgebung

# Details der Umgebung

Wenn Sie eine Umgebung auswählen, zeigt die WorkSpaces Thin Client-Konsole die Details für diese Umgebung an, damit Sie sie überprüfen können. Die Konsole zeigt auch die Details über den Anbieter für virtuelle Desktops an, den diese Umgebung verwendet.

Themen



## Übersicht

Name – Die dieser Umgebung zugeordnete eindeutige Kennung.

Virtueller Desktop-Service – Der virtuelle Desktop-Anbieter, den diese Umgebung verwendet.

Virtual Desktop Service ID — Die eindeutige Kennung, die der Virtual Desktop Service Provider dieser Umgebung zuweist.

Aktivierungscode – Dieser Code wird von Endbenutzern für den Zugriff auf die virtuelle Desktop-Umgebung verwendet.

Software immer behalten up-to-date — Diese Einstellung aktiviert automatische Softwareupdates.

Startzeit des Wartungsfensters — Die Uhrzeit pro Woche, zu der automatische Softwareupdates beginnen.

Endzeit des Wartungsfensters — Die Uhrzeit pro Woche, zu der automatische Softwareupdates beendet werden.

Wartungsfenster-Wochentage – Die Tage, an denen automatische Softwareaktualisierungen stattfinden.

Zugeordnete Geräte — Die Anzahl der WorkSpaces Thin Client-Geräte, die auf diese Umgebung zugreifen.

Erstellungszeit — Datum und Uhrzeit der Erstellung dieser Umgebung.

### Details zur virtuellen Desktop-Umgebung

Details zum WorkSpaces Amazon-Verzeichnis

Verzeichnis-ID — Das mit dieser Umgebung verknüpfte WorkSpaces Amazon-Verzeichnis.

Verzeichnisname — Die eindeutige Kennung, die mit diesem WorkSpaces Amazon-Verzeichnis verknüpft ist.

Name der Organisation — Der Name der Organisation, die das WorkSpaces Amazon-Verzeichnis kontrolliert.

Verzeichnistyp — Das Format des WorkSpaces Amazon-Verzeichnisses.

Registriert — Ob dieses WorkSpaces Amazon-Verzeichnis registriert ist.

Status — Ob dieses WorkSpaces Amazon-Verzeichnis aktiv ist.

Einzelheiten zum Amazon WorkSpaces Secure Browser-Portal

Name — Die eindeutige Kennung, die mit diesem Amazon WorkSpaces Secure Browser-Portal verknüpft ist.

Erstellungszeit — Datum und Uhrzeit der Erstellung dieses AppStream 2.0-Stacks.

Webportal-Endpunkt – Die URL, die für den Zugriff auf Ihre virtuelle Desktop-Umgebung verwendet wird.

AppStream 2.0-Einzelheiten

Stack-Name — Die eindeutige Kennung, die diesem AppStream 2.0-Stack zugeordnet ist.

IdP-Anmelde-URL — Die URL des Identitätsanbieters, die für die An- und Abmeldung bei Ihrem AppStream 2.0-Stack verwendet wird.

Erstellungszeit — Datum und Uhrzeit der Erstellung dieses AppStream 2.0-Stacks.

## Erstellen einer Umgebung

Zu Beginn benötigt jedes Gerät einen AWS Endbenutzer-Computing-Dienst. WorkSpaces Thin Client verwendet die folgenden Dienste:

- Amazon WorkSpaces über ein zugewiesenes Verzeichnis
- AppStream 2.0 durch einen zugewiesenen Stack
- Amazon WorkSpaces Secure Browser über eine Webportal-Adresse

Sie müssen entweder einer vorhandenen Umgebung einen Service zuweisen oder eine neue erstellen.

> **Note**
>
> WorkSpaces Thin Client zeigt nur virtuelle Desktops in derselben Region an.

Themen



## Schritt 1: Eingeben der Umgebungsdetails

1. Geben Sie im Feld Umgebungsdetails einen Namen für Ihre Umgebung ein.
2. Um automatische Softwarepatches einzurichten, aktivieren Sie das Kontrollkästchen Software immer behalten up-to-date.

   > **Note**
   >
   > Wenn automatische Softwareupdates nicht aktiviert sind, erhalten die in dieser Umgebung registrierten Geräte erst dann Softwareupdates, wenn Sie das Update manuell übertragen oder wenn die Software ihr Ablaufdatum erreicht hat und das System ein Update erzwingt.
   > Außerdem wird die Version des Softwaresets des Geräts vom System bestimmt. Diese Version ist möglicherweise nicht die neueste.

3. Wählen Sie aus, wann Sie das Wartungsfenster für Ihre Umgebung planen möchten.

   - Systemweites Wartungsfenster anwenden — Die Umgebungssoftware wird jede Woche automatisch zu einer bestimmten Uhrzeit aktualisiert.

- Benutzerdefiniertes Wartungsfenster anwenden – Legen Sie einen Tag und eine Uhrzeit fest, zu der die Umgebungssoftware jede Woche aktualisiert werden soll.

4. Wählen Sie einen virtuellen Desktop-Service aus.

- Amazon WorkSpaces
- WorkSpaces Sicherer Browser von Amazon
- AppStream 2.0

## Schritt 2: Auswählen Ihres virtuellen Desktop-Anbieters

Sie benötigen einen Dienst, der Ihren Benutzern Zugriff auf ihren virtuellen Desktop und kompatible Ressourcen bietet.

> **Important**
>
> Damit die WorkSpaces Thin Client Administrator Console ordnungsgemäß funktioniert, muss Ihr System bestimmte Anforderungen erfüllen. Diese Anforderungen sind unter Voraussetzungen und Konfigurationen aufgeführt.
> Stellen Sie sicher, dass Ihr System diese Anforderungen erfüllt, bevor Sie Ihre Konsole einrichten.

Amazon verwenden WorkSpaces

Amazon WorkSpaces ist ein vollständig verwalteter Desktop-Virtualisierungsservice für Windows, mit dem Sie von jedem unterstützten Gerät aus auf Ressourcen zugreifen können.

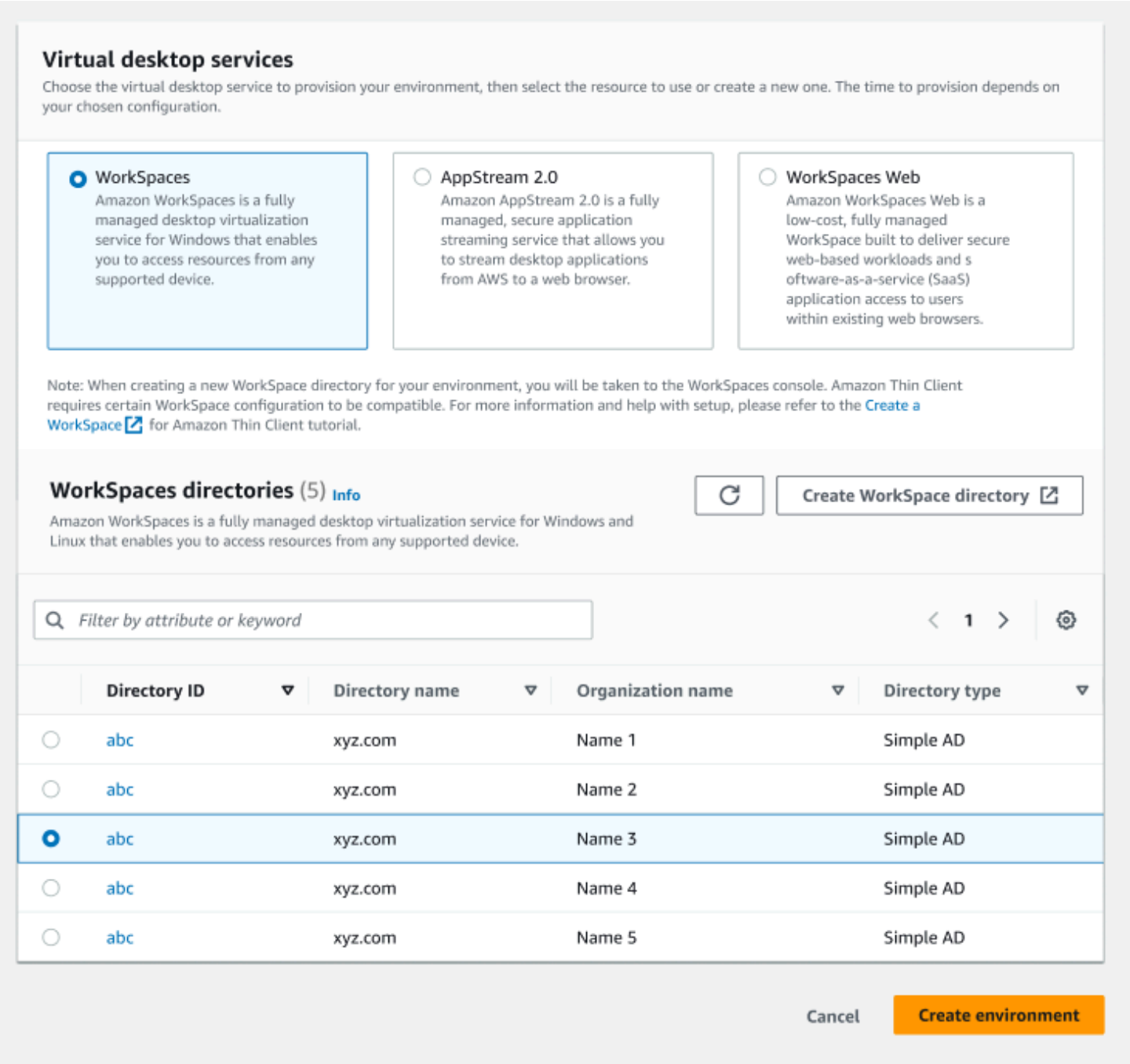
1. Gehen Sie wie folgt vor WorkSpaces, um Amazon zu verwenden:

- Wählen Sie das Verzeichnis aus, das Sie verwenden möchten. Sie können entweder die Dropdownliste durchsuchen oder die Verzeichnisse mithilfe des Suchfeldes durchsuchen.

> **Note**
>
> Wenn Sie Ihre vorhandenen Verzeichnisse nicht in der Liste sehen, überprüfen Sie in der WorkSpaces Management Console, ob sie die WorkSpaces Thin Client-Anforderungen erfüllen.

- Erstellen Sie ein Verzeichnis, indem Sie auf die Schaltfläche  WorkSpaces Verzeichnis erstellen klicken. Weitere Informationen zum Erstellen von WorkSpaces Verzeichnissen finden Sie unter Verzeichnisse verwalten für WorkSpaces.

2. Wählen Sie die Schaltfläche Umgebung erstellen.



Wenn Sie Ihre Umgebung erstellen, können Sie die Details später noch bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer Umgebung.

Verwenden von AppStream 2.0

AppStream 2.0 ist ein vollständig verwalteter, sicherer Anwendungsstreaming-Dienst, mit dem Sie Desktop-Anwendungen von AWS zu einem Webbrowser streamen können.

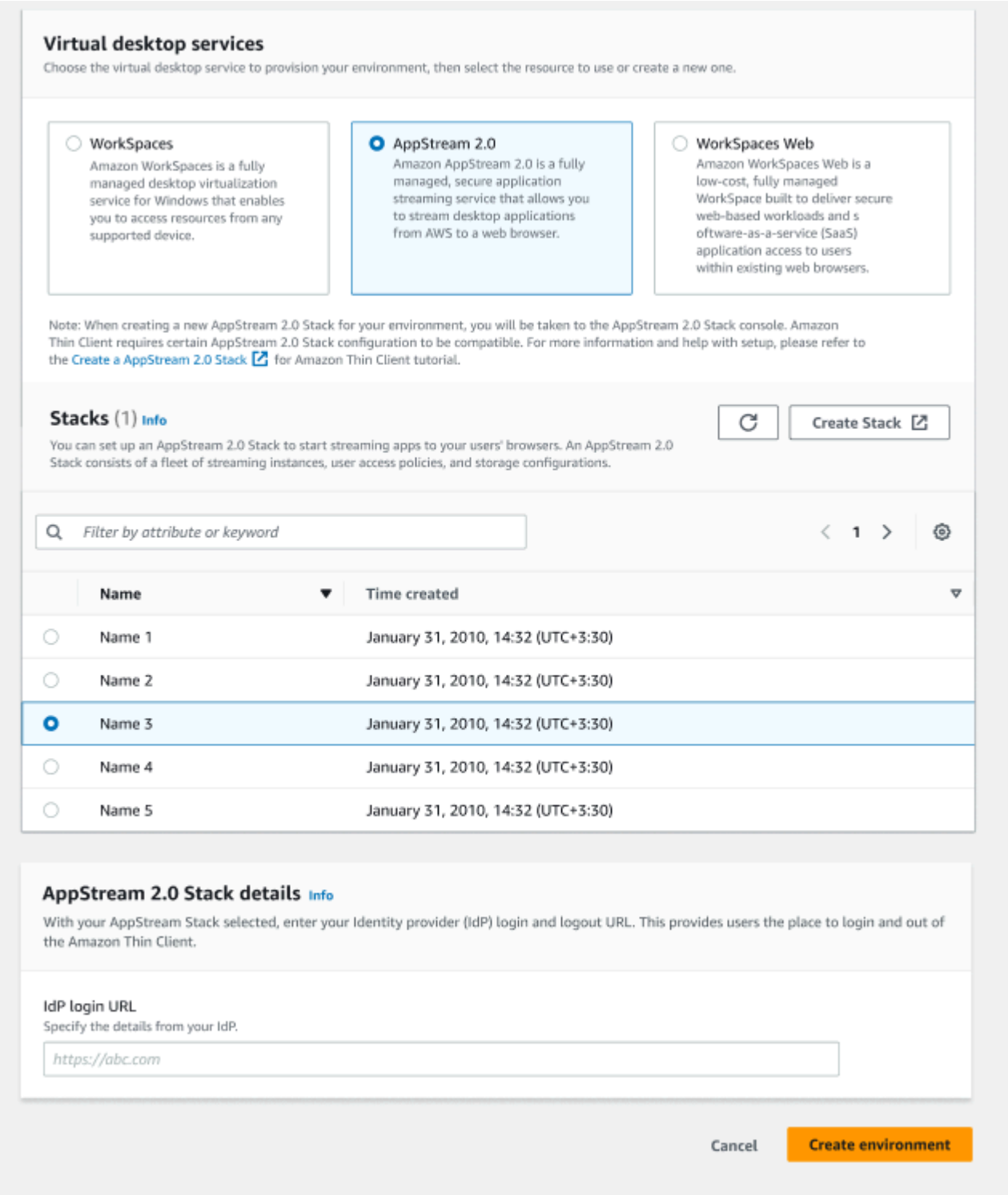
> **Warning**
>
> Um eine AppStream 2.0-Umgebung zu erstellen, müssen Sie auf `cli_follow_urlparam` eingestellt haben`false`. Um dies zu erreichen, gehen Sie wie folgt vor:
>
> - Führen Sie für ein Standardprofil den Befehl `aws configure set cli_follow_urlparam false` aus.
> - Führen Sie für ein Profil mit dem Namen `ProfileName` den Befehl `aws configure set cli_follow_urlparam false --profile ProfileName` aus.

1. Gehen Sie wie folgt vor, um AppStream 2.0 einzurichten:

   - Wählen Sie den Stack aus, den Sie verwenden möchten. Sie können entweder die Dropdownliste durchsuchen oder die Stapel mithilfe des Suchfeldes durchsuchen.

     > **Note**
     >
     > Wenn Sie Ihre vorhandenen Stacks nicht in der Liste sehen, überprüfen Sie in der AppStream 2.0 Management Console, ob sie die WorkSpaces Thin Client-Anforderungen erfüllen.

   - Erstellen Sie einen Stapel, indem Sie auf die Schaltfläche „Stapel erstellen“ klicken. Weitere Informationen zum Erstellen von AppStream 2.0-Stacks finden Sie unter Stapel erstellen.
2. Geben Sie die Anmelde- und Abmelde-URL Ihres Identitätsanbieters in das Feld IdP-Anmelde-URL ein. Dies bietet Benutzern einen Ort, an dem sie sich bei WorkSpaces Thin Client an- und abmelden können.
3. Wählen Sie die Schaltfläche Umgebung erstellen.




Nachdem Sie Ihre Umgebung erstellt haben, können Sie die Details später noch bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer Umgebung.

## Amazon WorkSpaces Secure Browser verwenden

Amazon WorkSpaces Secure Browser ist eine kostengünstige, vollständig verwaltete WorkSpaces Konsole, die darauf ausgelegt ist, Benutzern in vorhandenen Webbrowsern sichere webbasierte Workloads und Software-as-a-Service (SaaS) -Anwendungszugriff zu bieten.

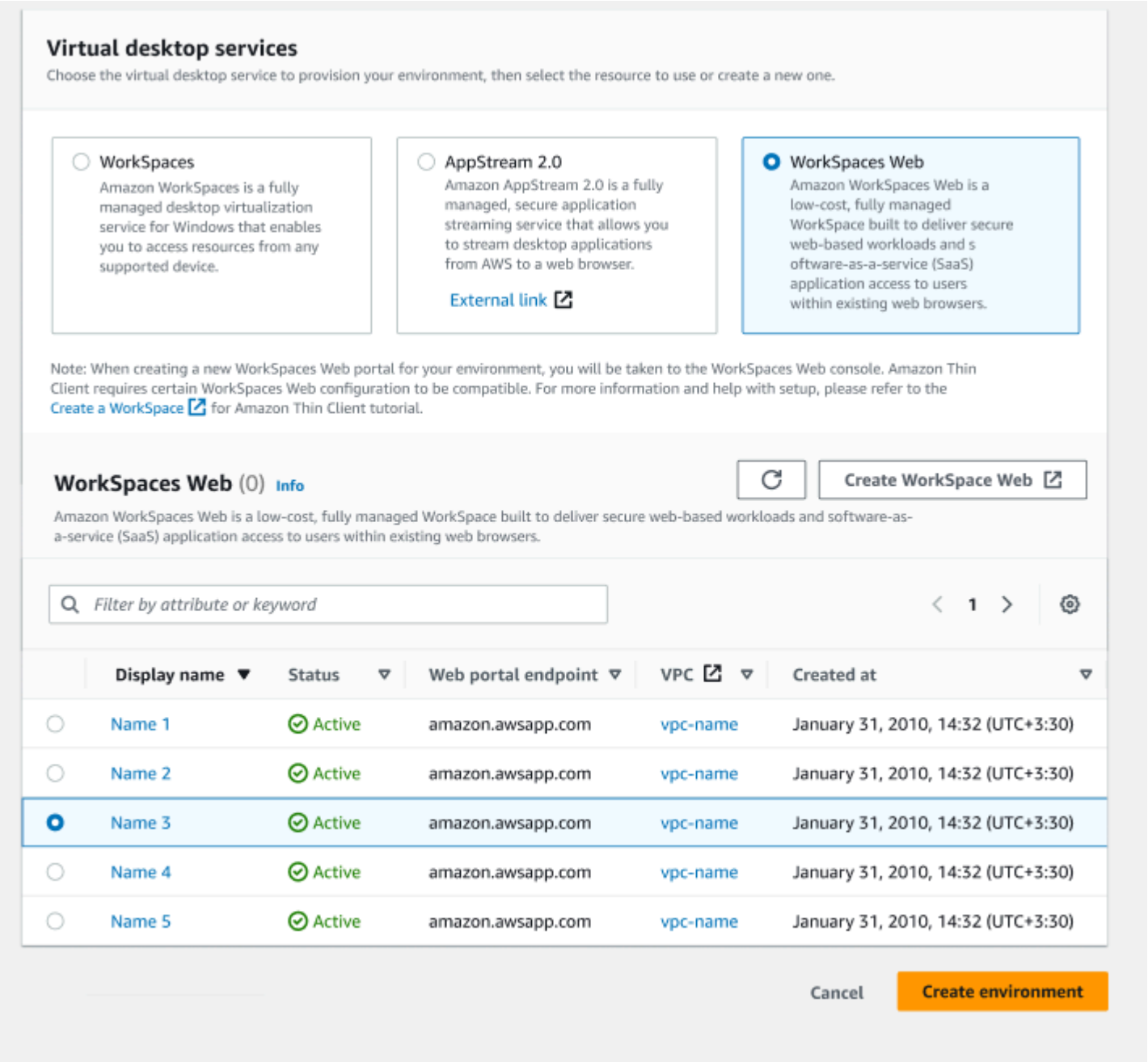
1. Gehen Sie wie folgt vor, um Amazon WorkSpaces Secure Browser einzurichten:

   - Wählen Sie das Webportal aus, das Sie für Ihre Umgebung verwenden möchten. Sie können entweder die Dropdownliste durchsuchen oder die Webportale mithilfe des Suchfeldes durchsuchen.

     > **Note**
     >
     > Wenn Sie Ihre vorhandenen Webportale nicht in der Liste sehen, überprüfen Sie in der WorkSpaces Secure Browser Management Console, ob sie die WorkSpaces Thin Client-Anforderungen erfüllen.

   - Erstellen Sie ein Webportal, indem Sie auf die Schaltfläche „ WorkSpaces Sicheren Browser erstellen“ klicken. Weitere Informationen zur Erstellung von WorkSpaces Secure Browser-Webportalen finden Sie unter Amazon WorkSpaces Secure Browser einrichten.

2. Wählen Sie die Schaltfläche Umgebung erstellen.




Nachdem Sie Ihre Umgebung erstellt haben, können Sie die Details später noch bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer Umgebung.

## Schritt 3: Senden des Aktivierungscodes an die Gerätebenutzer

Nachdem Sie Ihre Umgebung und den virtuellen Desktop-Dienst eingerichtet haben, erhalten Sie einen eindeutigen Aktivierungscode für Ihr Setup auf der AWS Management Console.

Stellen Sie diesen Aktivierungscode jedem Benutzer eines WorkSpaces Thin Client-Geräts zur Verfügung, damit dieser auf seinen virtuellen Desktop zugreifen kann.

Weitere Informationen dazu, wie Sie Ihren Gerätebenutzern bei der Einrichtung ihres Amazon WorkSpaces Thin Client helfen können, finden Sie im Thin Client-Benutzerhandbuch. WorkSpaces

## Bearbeiten einer Umgebung

Die WorkSpaces Thin Client-Verwaltungskonsole verwaltet virtuelle Desktop-Umgebungen für einzelne Benutzer. Von dieser Konsole aus können Sie virtuelle Desktop-Umgebungen bearbeiten oder löschen.

1. Wählen Sie die gewünschte Umgebung aus.

   > **Note**
   >
   > Sie können entweder die Dropdownliste durchsuchen oder die Umgebungen mithilfe des Suchfeldes durchsuchen.

2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie in der Drop-down-Liste Bearbeiten aus. Sie werden zum Fenster Umgebung bearbeiten weitergeleitet.
4. Bearbeiten Sie jedes der folgenden Elemente:

   - Ändern Sie den Namen Ihrer Umgebung im Feld Umgebungsname.
   - Ändern Sie das Kontrollkästchen für die Details zu Softwareupdates für automatische Softwarepatch-Updates.
   - Ändern Sie es, wenn Sie das Wartungsfenster für Ihre Umgebung planen möchten.

5. Wählen Sie die Schaltfläche Umgebung bearbeiten.

## Löschen einer Umgebung

> **Note**
>
> Sie können eine Umgebung nicht löschen, für die Geräte registriert sind. Zunächst müssen Sie alle Geräte in einer Umgebung abmelden und löschen.

1. Wählen Sie die zu löschende Umgebung aus. Sie können entweder die Dropdownliste durchsuchen oder die Umgebungen mithilfe des Suchfeldes durchsuchen.
2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie Löschen aus der Drop-down-Liste aus. Das Bestätigungsfenster „Umgebung löschen“ wird angezeigt.
4. Geben Sie im Bestätigungsfeld „löschen“ ein.
5. Wählen Sie die Schaltfläche Löschen aus.

# Geräte

Jeder WorkSpaces Thin Client-Endbenutzer verfügt über ein spezielles Gerät, das ihn mit seinen virtuellen Desktop-Umgebungen und Online-Ressourcen verbindet. Diese Geräte werden über die WorkSpaces Thin Client-Administratorkonsole am AWS Standort verwaltet.

Von dieser Konsole aus können Sie Geräte für Ihr Team bestellen.

## Geräteliste

### Gerätelistendetails

Geräte-ID – Die Identifikationsnummer, die einem einzelnen Gerät zugewiesen wurde.

Gerätename — (optional) Der eindeutige Name, den Sie einem Gerät geben.

Aktivitätsstatus — Der aktuelle Status eines Geräts. Es gibt zwei Statusstatus:

- Aktiv – In den letzten sieben Tagen mindestens einmal mit einem Netzwerk verbunden.
- Inaktiv – In den letzten sieben Tagen nicht mit einem Netzwerk verbunden.

Registrierungsstatus — Bestätigung, dass ein Gerät eingerichtet wurde, diesem AWS Konto zugeordnet ist und Teil einer bestimmten Umgebung ist. Es kann sich in einem der folgenden Zustände befinden:

- Registriert — Dies ist der Standardstatus.
- Abmeldung — Das Gerät befindet sich im Prozess Reset and Deregister.

> **Note**
>
> Sie können ein Gerät löschen, wenn es sich im Abmeldestatus befindet.

- Abgemeldet – Das Gerät wurde erfolgreich abgemeldet.

> **Note**
>
> Sie können ein Gerät nur löschen, wenn es sich entweder im Status Abmeldung oder Abmeldung befindet.

- Archiviert – Das Gerät ist archiviert.

Umgebungs-ID – Die Kennung der Umgebung, an die dieses Gerät angeschlossen ist.

Software-Konformität – Der Konformitätsstatus der Gerätesoftware. Es gibt zwei Statusstatus:

- Konform
- Nicht konform

## Gerätelistenaktionen

Suche – Durchsucht alle Geräte, die Sie verwalten.

Aktualisieren – Aktualisiert die Geräteliste.

Details anzeigen – Zeigt Gerätedetails an.

Aktionen — Öffnet eine Dropdownliste, in der Sie Folgendes tun können:

- Gerätenamen bearbeiten
- Abmelden
- Archiv
- Löschen
- Gerätedetails exportieren

Geräte bestellen – Startet den Bestellvorgang für Geräte.

Themen



# Gerätedetails

## Übersicht

Geräteseriennummer — Die Identifikationsnummer, die einem einzelnen Gerät zugewiesen wurde.

ARN — Die eindeutige Kennung für das Gerät im Format Amazon Resource Name (ARN).

Gerätename — Der Name, den Sie einem Gerät geben. Wenn Sie noch keinen Namen erstellt haben, können Sie ihm einen Namen geben, oder er erhält einen Standardnamen.

Gerätetyp — Der Typ des Endbenutzergeräts, das mit dem Konto verknüpft ist.

Aktivitätsstatus – Der aktuelle Status dieses Geräts. Die beiden Statusstatus sind:

- Aktiv
- Inaktiv

Umgebungs-ID — Die Identifikationsnummer der Umgebung, die das Gerät verwendet.

Registrierungsstatus — Bestätigung, dass ein Gerät eingerichtet wurde, diesem AWS Konto zugeordnet ist und Teil einer bestimmten Umgebung ist. Es kann sich in einem der folgenden vier Zustände befinden:

- Registriert — Dies ist der Standardstatus.
- Abmeldung — Das Gerät befindet sich im Prozess Reset and Deregister.
- Abgemeldet – Das Gerät wurde erfolgreich abgemeldet.

> **Note**
>
> Sie können das Gerät nur löschen, wenn es sich entweder im Status Abgemeldet oder Archiviert befindet.

- Archiviert — Dieses Gerät wurde vom Administrator als derzeit nicht in Betrieb markiert.

Registriert seit – Das Datum, an dem das Gerät aktiviert wurde.

Zuletzt angemeldet – Das Datum und die Uhrzeit der letzten Anmeldung.

Letzte Überprüfung des Zustands am — Datum und Uhrzeit des letzten Check-ins des Geräts.

Aktuelle Softwareversion – Die Softwareversion, die dieses Gerät derzeit verwendet.

Für das Softwareupdate geplant — Die geplante Softwareversion auf dem Gerät.

Software-Konformität – Bestätigung, dass der Softwaresatz gültig ist. Es gibt zwei Statusstatus:

- Konform
- Nicht konform

Benutzerprotokoll

Letzter Gerätezugriff — Datum und Uhrzeit der letzten Verwendung dieses Geräts.

## Bearbeiten eines Gerätenamens

1. Wählen Sie das Gerät aus, das Sie bearbeiten möchten. Sie können entweder die Drop-down-Liste durchsuchen oder über das Suchfeld nach einem Gerät suchen.
2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie in der Drop-down-Liste die Option Gerätenamen bearbeiten aus. Das Fenster Gerätenamen bearbeiten wird angezeigt.
4. Geben Sie den neuen Gerätenamen in das Bestätigungsfeld für den Gerätenamen ein.
5. Klicken Sie auf die Schaltfläche Speichern.

## Zurücksetzen und Abmelden des Geräts

1. Wählen Sie das Gerät aus, das Sie abmelden möchten. Sie können entweder die Dropdownliste durchsuchen oder über das Suchfeld nach dem Gerät suchen.
2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie aus der Drop-down-Liste die Option Abmelden aus. Das Fenster Abmelden wird angezeigt.
4. Geben Sie „abmelden“ in das Bestätigungsfeld ein.
5. Wählen Sie die Schaltfläche Abmelden.

> **Note**
>
> Durch die Abmeldung wird der Benutzer zwangsweise abgemeldet und das WorkSpaces Thin Client-Gerät muss während einer Sitzung neu gestartet werden.

## Archivieren eines Geräts

1. Wählen Sie das Gerät aus, das Sie archivieren möchten. Sie können entweder die Dropdownliste durchsuchen oder über das Suchfeld nach dem Gerät suchen.
2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie in der Drop-down-Liste die Option Archivieren aus. Das Fenster Archiv wird angezeigt.
4. Geben Sie in das Bestätigungsfeld „zurücksetzen und archivieren“ ein.
5. Wählen Sie die Schaltfläche Zurücksetzen und archivieren aus.

> **Note**
>
> Bei der Archivierung eines Geräts wird der Benutzer zwangsweise abgemeldet, sodass sein WorkSpaces Thin Client-Gerät während einer Sitzung neu gestartet werden muss.

## Löschen eines Geräts

1. Wählen Sie das Gerät aus, das Sie löschen möchten. Sie können entweder die Dropdownliste durchsuchen oder über das Suchfeld nach dem Gerät suchen.
2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie Löschen aus der Drop-down-Liste aus. Das Fenster Löschen wird angezeigt.
4. Geben Sie im Bestätigungsfeld „löschen“ ein.
5. Wählen Sie die Schaltfläche Löschen aus.

> **Note**
>
> Wenn das Gerät erfolgreich gelöscht wurde, muss der Benutzer das WorkSpaces Thin Client-Gerät an Amazon zurücksenden.

## Exportieren der Gerätedetails

1. Wählen Sie das gewünschten Gerät aus, von dem aus Sie exportieren möchten. Sie können entweder die Drop-down-Liste durchsuchen oder über das Suchfeld nach dem Gerät suchen.
2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie in der Drop-down-Liste Gerätedetails exportieren aus. Die Details für das ausgewählte Gerät werden in einem Tabellenkalkulationsformat heruntergeladen.

# Software-Updates

WorkSpaces Thin Client erfordert manchmal Softwareupdates, die neue Funktionen einführen und Sicherheitspatches anwenden. Diese Updates werden durch einen versionierten Softwaresatz dargestellt.

Ein Softwaresatz kann Updates für die Softwareanwendungen oder das Betriebssystem für das WorkSpaces Thin Client-Gerät enthalten. Von dieser Konsole aus können Sie wählen, ob die Software sofort aktualisiert werden soll, oder Sie können ein automatisches Update während des Wartungsfensters für die Umgebungen planen.

Eine Liste der veröffentlichten Softwaresets finden Sie unter Softwaresets für WorkSpaces Thin Client-Umgebungen.

Themen



## Aktualisieren der Umgebungssoftware

WorkSpaces Thin Client ist ein Computerdienst für AWS Endbenutzer, der Benutzern Zugriff auf virtuelle Desktops bietet. Diese virtuellen Desktops werden regelmäßig mit neuen Softwaresätzen aktualisiert. Gehen Sie wie folgt vor, um die Umgebungssoftware zu aktualisieren:

1. Wählen Sie das Softwareset aus der Liste unter Verfügbare Softwareupdates aus. Eine Liste der Softwaresets finden Sie unter Softwaresets für WorkSpaces Thin Client-Umgebungen.
2. Wählen Sie die Schaltfläche Installieren.
3. Wählen Sie oben auf der Seite Umgebungen aus.
4. Wählen Sie die zu aktualisierende Umgebung aus der Liste im Abschnitt Umgebungen aus.
5. Wählen Sie im Bereich Update planen aus, wann die Umgebung aktualisiert werden soll, indem Sie eine der folgenden Optionen wählen:

   - Software jetzt aktualisieren – Startet das Update der Umgebungssoftware auf allen registrierten Geräten.

     > **Note**
     >
     > Wenn Sie die Software jetzt aktualisieren, können alle aktiven Benutzersitzungen unterbrochen werden.

   - Software in jedem Wartungsfenster der Umgebung aktualisieren — Aktualisiert die Umgebungssoftware während des geplanten Wartungsfensters für die Umgebung.
6. Markieren Sie das Kästchen, um das Update zu autorisieren. Dieses Kästchen muss aktiviert werden, damit die Software aktualisiert werden kann.
7. Wählen Sie die Schaltfläche Installieren.

# Aktualisieren der Gerätesoftware

WorkSpaces Thin Client ist ein AWS Endbenutzer-Computing-Dienst, der ein Thin Client-Gerät bereitstellt, das Benutzer mit dedizierten virtuellen Desktops verbindet. Diese Geräte werden regelmäßig mit neuer Software aktualisiert. Gehen Sie wie folgt vor, um die Gerätesoftware zu aktualisieren:

1. Wählen Sie das Softwareset aus der Liste unter Verfügbare Softwareupdates aus.
2. Wählen Sie die Schaltfläche Installieren.
3. Wählen Sie oben auf der Seite die Option Gerät.
4. Wählen Sie das Gerät oder die Geräte, die aktualisiert werden sollen, aus der Liste im Bereich Geräte aus. Eine Liste der Softwaresets finden Sie unter Softwaresets für WorkSpaces Thin Client-Umgebungen.
5. Wählen Sie unter den Optionen Update planen aus, wann die Umgebung aktualisiert werden soll, indem Sie eine der folgenden wählen:

   - Software jetzt aktualisieren – Die Gerätesoftware wird sofort aktualisiert.

     > **Note**
     >
     > Wenn Sie die Software jetzt aktualisieren, können alle aktiven Benutzersitzungen unterbrochen werden.

   - Software in jedem Wartungsfenster des Geräts aktualisieren — Aktualisiert die Umgebungssoftware während des geplanten Wartungsfensters für das Gerät.
6. Markieren Sie das Kästchen, um das Update zu autorisieren. Dieses Kästchen muss aktiviert werden, damit die Software aktualisiert werden kann.
7. Wählen Sie die Schaltfläche Installieren.

# WorkSpaces Thin Client-Softwareversionen

WorkSpaces Thin Client ist ein AWS Endbenutzer-Computing-Dienst, der Benutzern Zugriff auf virtuelle Desktops auf einem Gerät bietet. Diese Geräte werden regelmäßig mit neuen Softwaresätzen aktualisiert. In der folgenden Tabelle werden alle veröffentlichten Softwaresets beschrieben. Administratoren können die AWS Managementkonsole verwenden, um verfügbare Softwaresets einzusehen.

| Softwaresatz | Datum der Veröffentlichung | Änderungen |
| --- | --- | --- |
| 2.5.0 | 13.06.2024 | • Es wurde das Problem behoben, bei dem das Gerät beim Aufwachen aus dem Ruhemodus vor dem Start der Sitzung kurz den Bildschirm zur Einrichtu ng von Tastatur und Maus anzeigte.<br>• Die Home-Schaltfläche auf der Gerätesymbolleiste wurde in Anmelden umbenannt.<br>• Verbesserungen der Leistung von Audio-/Vi deoanrufen in der Sitzung. |
| 2.4.3 | 29.05.2024 | • Zero-Day-Fix für das kritische Sicherheitsproblem CVE-2024-5274 von Chromium. |
| 2.4.2 | 17.05.2024 | • Zero-Day-Fix für das kritische Sicherheitsproblem CVE-2024-4947 von Chromium. |
| 2.4.1 | 15.05.2024 | • Zero-Day-Korrekturen für die kritischen Sicherhei tsprobleme CVE-2024-4671 und CVE-2024-4761 von Chromium.<br>• Es wurde das Problem behoben, das es ermöglich te, auf der WorkSpace |

| Softwaresatz | Datum der Veröffentlichung | Änderungen |
| --- | --- | --- |
| | | s Anmeldeseite mit der rechten Maustaste auf die Links AWS und Datenschutz zu klicken, um den Browser im eigenständigen Modus zu öffnen. |
| 2.4.0 | 05-09-2024 | • Es wurde ein Problem behoben, durch das „accounts.google.com“ blockiert und die Verwendun g von Google Workspace als IDP für 2.0-Sitzu ng verhindert wurde. AppStream<br>• Die Werkzeugleiste für Geräteeinstellungen wird mit einem Klick auf einen beliebigen Bereich auf dem Bildschirm automatisch zusammengeklappt. |

| Softwaresatz | Datum der Veröffentlichung | Änderungen |
| --- | --- | --- |
| 2.3.0 | 04-05-2024 | • Die Geräteeinstellungen werden in einer zusammeng eklappten Werkzeugleiste angezeigt, sodass der sichtbare Bildschirm besser genutzt werden kann.<br>• Endbenutzer können jetzt festlegen, wie lange es dauert, bis das Gerät bei Inaktivität in den Ruhemodus wechselt.<br>• Das Problem, dass die URL „about:blank“ auf dem zweiten Display angezeigt wurde, wurde behoben.<br>• Das Problem, das zu einem weißen Bildschirm führte, wenn die erweiterte Anzeige geschlossen wurde, wurde behoben.<br>• Die von Endbenutzern eingestellte Lautstärke bleibt jetzt auch bei Geräteneu starts erhalten. |
| 2.2.1 | 16.02.2024 | • Es wurde ein Problem behoben, das während des Anmeldevorgangs auftrat und Benutzer daran hinderte, sich bei einer mit SAML 2.0 WorkSpace s konfigurierten Authentif izierung anzumelden. |

| Softwaresatz | Datum der Veröffentlichung | Änderungen |
| --- | --- | --- |
| 2.2.0 | 02-08-2024 | • Unterstützung für ISO-Tastaturen mit den Sprachen Englisch (Großbritannien), Französisch, Deutsch, Italienisch und Spanisch hinzugefügt. |
| 2.1.2 | 26.01.2024 | • Zero-Day-Fix für das kritische Sicherheitsproblem CVE-2024-0519 von Chromium.<br>• Verbesserung der Latenz für Endbenutzer im Zusammenhang mit der Sperrfunktion.<br>• Interne Endgeräte, die mit Geräten verbunden sind, werden auf die Domäne „ThinClient*“ umgestellt. |
| 2.1.1 | 21.12.2023 | • Zero-Day-Fix für das kritische Sicherheitsproblem CVE-2023-7024 von Chromium. |
| 2.1.0 | 20.12.2023 | • Fügt den Geräteeinstellungen eine Home-Taste hinzu und aktiviert die Unterstützung von Metatasten. Auf diese Weise können Endbenutzer den Sperrbildschirm aufrufen, indem sie Meta+L drücken. |

| Softwaresatz | Datum der Veröffentlichung | Änderungen |
| --- | --- | --- |
| 2.0.1 | 12-06-2023 | • Zero-Day-Fix für das kritische Sicherheitsproblem CVE-2024-6345 von Chromium. |
| 2.0.0 | 15.11.2023 | • Erstversion |

# Verwendung von Tags auf WorkSpaces Thin Client-Ressourcen

Sie können die Ressourcen für Ihren WorkSpaces Thin Client organisieren und verwalten, indem Sie jeder Ressource Ihre eigenen Metadaten als 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. Sie können Tags als einfache und dennoch leistungsstarke Methode verwenden, um AWS-Ressourcen zu verwalten und Daten, einschließlich Rechnungsdaten, zu organisieren.

Wenn Sie einer vorhandenen Ressource Tags hinzufügen, werden diese Tags erst am ersten Tag des Folgemonats in Ihrem Kostenzuordnungsbericht angezeigt. Wenn Sie beispielsweise am 15. Juli Tags zu einem vorhandenen WorkSpaces Thin Client-Gerät hinzufügen, erscheinen die Tags erst am 1. August in Ihrem Kostenzuordnungsbericht. Weitere Informationen finden Sie unter Using Cost Allocation Tags im AWS Billing User Guide.

> **Note**
>
> Um Ihre WorkSpaces Thin Client-Ressourcen-Tags im Cost Explorer anzuzeigen, müssen Sie die Tags aktivieren, die Sie auf Ihre WorkSpaces Thin Client-Ressourcen angewendet haben. Folgen Sie dazu den Anweisungen unter Benutzerdefinierte Kostenzuordnungs-Tags aktivieren im AWS Billing Benutzerhandbuch.
> Tags werden 24 Stunden nach der Aktivierung angezeigt, aber es kann 4—5 Tage dauern, bis die mit diesen Tags verknüpften Werte im Cost Explorer angezeigt werden. Darüber hinaus müssen WorkSpaces Thin Client-Ressourcen, die mit Tags versehen wurden, während dieser Zeit Gebühren anfallen, damit Kostendaten im Cost Explorer angezeigt und bereitgestellt werden können. Der Cost Explorer zeigt nur Kostendaten aus dem Zeitpunkt an, als die Tags aktiviert wurden. Derzeit sind keine Verlaufsdaten verfügbar.

Ressourcen, die Sie taggen können:

- Sie können den folgenden Ressourcen bei ihrer Erstellung Tags hinzufügen: WorkSpaces Thin Client-Umgebungen.
- Sie können Tags zu vorhandenen Ressourcen der folgenden Typen hinzufügen: WorkSpaces Thin Client-Umgebungen, Geräten und Softwaresets.

Tag-Einschränkungen

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 128 Unicode-Zeichen
- Höchstwertlänge — 256 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 das `aws:` Präfix nicht in Ihren Tagnamen oder -Werten, da es für AWS die Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen.

Um die Tags für eine bestehende Umgebung mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die WorkSpaces Thin Client-Konsole.
2. Wählen Sie die Umgebung aus, um die zugehörige Detailseite zu öffnen
3. Wählen Sie Bearbeiten aus.
4. Führen Sie im Abschnitt Tags eine oder mehrere der folgenden Aktionen aus:.
   - Um ein Tag hinzuzufügen, wählen Sie Tag hinzufügen aus und bearbeiten anschließend die Werte für Schlüssel und Wert.
   - Um ein Tag zu aktualisieren, bearbeiten Sie den Wert von Value.
   - Um ein Tag zu löschen, klicken Sie neben dem Tag auf Entfernen.
5. Wenn Sie mit der Aktualisierung der Tags fertig sind, wählen Sie Speichern.

Um die Tags für ein vorhandenes Gerät mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die WorkSpaces Thin Client-Konsole.
2. Wählen Sie das Gerät aus, um die zugehörige Detailseite zu öffnen.
3. Wählen Sie Tags aus.
4. Wählen Sie Tags verwalten aus.
5. Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Um ein Tag hinzuzufügen, wählen Sie Tag hinzufügen aus und bearbeiten anschließend die Werte für Schlüssel und Wert.
- Um ein Tag zu aktualisieren, bearbeiten Sie den Wert von Value.
- Um ein Tag zu löschen, klicken Sie neben dem Tag auf Entfernen.

6. Wenn Sie mit der Aktualisierung der Tags fertig sind, wählen Sie Speichern.

Um die Tags für ein Softwareupdate mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die WorkSpaces Thin Client-Konsole.
2. Wählen Sie das Softwareupdate aus, um die zugehörige Detailseite zu öffnen.
3. Wählen Sie im Abschnitt Tags die Option Tags verwalten aus.
4. Führen Sie eine oder mehrere der folgenden Aktionen aus:

   - Um ein Tag hinzuzufügen, wählen Sie Tag hinzufügen aus und bearbeiten anschließend die Werte für Schlüssel und Wert.
   - Um ein Tag zu aktualisieren, bearbeiten Sie den Wert von Value.
   - Um ein Tag zu löschen, klicken Sie neben dem Tag auf Entfernen.

5. Wenn Sie mit der Aktualisierung der Tags fertig sind, wählen Sie Speichern.

# Sicherheit in Amazon WorkSpaces Thin Client

Die Cloud-Sicherheit bei AWS hat höchste Priorität. Als - AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die entwickelt wurden, um die Anforderungen der sicherheitssensibelsten Organisationen zu erfüllen.

Sicherheit ist eine geteilte Verantwortung zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS Services in der ausführt AWS Cloud. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Externe Prüfer testen und überprüfen im Rahmen der AWS Compliance-Programme regelmäßig die Wirksamkeit unserer Sicherheit. Informationen zu den Compliance-Programmen, die für Amazon WorkSpaces Thin Client gelten, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -ServicesIm.
- Sicherheit in der Cloud – Ihre Verantwortung 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.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von WorkSpaces Thin Client einsetzen können. Die folgenden Themen zeigen Ihnen, wie Sie WorkSpaces Thin Client konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie können auch erfahren, wie Sie andere - AWS Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer WorkSpaces Thin-Client-Ressourcen unterstützen.

Themen



# Datenschutz im Amazon WorkSpaces Thin Client

Das AWS Modell der gilt für den Datenschutz in Amazon WorkSpaces Thin Client. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der

alle Systeme laufen AWS Cloud. 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, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. 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, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen 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 AWS über eine Befehlszeilenschnittstelle oder 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 Thin Client oder anderen Geräten arbeiten und die Konsole, die API oder SDKs AWS-Services verwenden. AWS CLI AWS 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.

Amazon WorkSpaces Thin Client sammelt und stellt Informationen über die Nutzung von WorkSpaces Thin Client-Geräten durch Benutzer und deren Interaktion mit den virtuellen Desktop-

Diensten bereit. Zum Beispiel verfügbarer Speicher, Netzwerkdiagnosen, Netzwerkinformationen, Gerätekonnektivität, SAML-Anmeldeinformationen, Geräteidentifikationsinformationen und Absturzberichte. Diese Informationen werden verwendet, um Ihnen den Service zur Verfügung zu stellen, und können verwendet werden, um die Benutzererfahrung mit dem Service zu verbessern. Darüber hinaus können die Informationen ausschließlich zu dem Zweck, Ihnen den Service zur Verfügung zu stellen, in Länder außerhalb der AWS Region übertragen werden, in der die Benutzer den Dienst nutzen. Wir verarbeiten diese Informationen gemäß der AWS Datenschutzerklärung.

Themen



## Datenverschlüsselung

WorkSpaces Thin Client sammelt Umgebungs- und Geräteanpassungsdaten wie Benutzereinstellungen, Gerätekennungen, Informationen zum Identitätsanbieter und Streaming-Desktop-Identifikatoren. WorkSpaces Thin Client sammelt auch Sitzungszeitstempel. Die gesammelten Daten werden in Amazon DynamoDB und Amazon S3 gespeichert. WorkSpaces Thin Client verwendet AWS Key Management Service (KMS) für die Verschlüsselung.

Befolgen Sie die folgenden Richtlinien, um deine Inhalte zu schützen:

- Implementieren Sie den Zugriff mit den geringsten Rechten und erstellen Sie spezifische Rollen, die für WorkSpaces Thin Client-Aktionen verwendet werden.
- Schützen Sie Daten, end-to-end indem Sie einen vom Kunden verwalteten Schlüssel bereitstellen, sodass WorkSpaces Thin Client Ihre gespeicherten Daten mit den von Ihnen bereitgestellten Schlüsseln verschlüsseln kann.
- Seien Sie vorsichtig beim Teilen von Umgebungsaktivierungscodes und Benutzeranmeldeinformationen:
  - Administratoren müssen sich bei der WorkSpaces Thin Client-Konsole anmelden, und Benutzer müssen Aktivierungscodes für das WorkSpaces Thin Client-Setup angeben und sich mit ihren Anmeldeinformationen am Streaming-Desktop anmelden.

- Jeder mit physischem Zugriff kann einen WorkSpaces Thin Client einrichten, aber er kann keine Sitzung starten, wenn er nicht über einen gültigen Aktivierungscode und Benutzeranmeldedaten verfügt, um sich anzumelden.
- Benutzer können ihre Sitzungen explizit beenden, indem sie ihren Bildschirm sperren, das Gerät neu starten oder herunterfahren möchten, indem sie die Gerätesymbolleiste verwenden. Dadurch wird die Gerätesitzung verworfen und die Sitzungsanmeldeinformationen gelöscht.

WorkSpaces Thin Client schützt Inhalte und Metadaten standardmäßig, indem alle sensiblen Daten mit AWS KMS verschlüsselt werden. Wenn beim Anwenden vorhandener Einstellungen ein Fehler auftritt, kann ein Benutzer nicht auf neue Sitzungen zugreifen und Geräte können keine Softwareupdates anwenden.

## Datenverschlüsselung im Ruhezustand für Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client bietet standardmäßig Verschlüsselung, um vertrauliche Kundendaten im Speicher mithilfe AWS eigener Verschlüsselungsschlüssel zu schützen.

- AWS eigene Schlüssel — Amazon WorkSpaces Thin Client verwendet diese Schlüssel standardmäßig, um persönlich identifizierbare Daten automatisch zu verschlüsseln. Sie können AWS eigene Schlüssel nicht einsehen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme zum Schutz der Schlüssel ändern, die zur Verschlüsselung Ihrer Daten verwendet werden. Weitere Informationen finden Sie unter AWS -eigene Schlüssel im Entwicklerhandbuch zum AWS -Schlüsselverwaltungsdienst.

Die standardmäßige Verschlüsselung von Daten im Ruhezustand trägt dazu bei, den betrieblichen Aufwand und die Komplexität zu reduzieren, die mit dem Schutz vertraulicher Daten verbunden sind. Gleichzeitig können Sie damit sichere Anwendungen erstellen, die strenge Verschlüsselungsvorschriften und gesetzliche Auflagen erfüllen.

Sie können diese Verschlüsselungsebene zwar nicht deaktivieren oder einen alternativen Verschlüsselungstyp auswählen, aber Sie können eine zweite Verschlüsselungsebene über den vorhandenen AWS-eigenen Verschlüsselungsschlüsseln hinzufügen, indem Sie bei der Erstellung Ihrer Thin Client-Umgebung einen vom Kunden verwalteten Schlüssel auswählen:

- Vom Kunden verwaltete Schlüssel — Amazon WorkSpaces Thin Client unterstützt die Verwendung eines symmetrischen, vom Kunden verwalteten Schlüssels, den Sie erstellen, besitzen und

verwalten, um der vorhandenen AWS Verschlüsselung eine zweite Verschlüsselungsebene hinzuzufügen. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie Aufgaben wie die folgenden ausführen:

- Festlegung und Pflege wichtiger Richtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von Tags
- Erstellen von Schlüsselaliasen
- Planen von Schlüsseln für das Löschen

Weitere Informationen finden Sie unter Vom Kunden verwaltete Schlüssel im Entwicklerhandbuch zum AWS Key Management Service.

Die folgende Tabelle fasst zusammen, wie Amazon WorkSpaces Thin Client personenbezogene Daten verschlüsselt.

| Datentyp | AWS-eigene Schlüssel verschlüsselung | Vom Kunden verwaltete Schlüsselverschlüsselung (optional) |
|---|---|---|
| Umgebungsname<br><br>WorkSpaces Name der Thin Client-Umgebung | Aktiviert | Aktiviert |
| Gerätename<br><br>WorkSpaces Name des Thin Client-Geräts | Aktiviert | Aktiviert |

> **Note**
>
> Amazon WorkSpaces Thin Client aktiviert automatisch die Verschlüsselung im Ruhezustand, indem AWS eigene Schlüssel verwendet werden, um personenbezogene Daten kostenlos zu schützen.

Für die Verwendung eines vom Kunden verwalteten Schlüssels fallen jedoch AWS KMS-Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter AWS Key Management Service – Preise.

## So verwendet Amazon WorkSpaces Thin Client Zuschüsse in AWS KMS

Amazon WorkSpaces Thin Client benötigt eine Genehmigung, damit Sie Ihren vom Kunden verwalteten Schlüssel verwenden können.

Wenn Sie eine WorkSpaces Thin Client-Umgebung erstellen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, erstellt Amazon WorkSpaces Thin Client in Ihrem Namen einen Zuschuss, indem es eine CreateGrant Anfrage an AWS KMS sendet. Zuschüsse in AWS KMS werden verwendet, um Amazon WorkSpaces Thin Client Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

Wenn ein neues Thin Client-Gerät mit einem vom Kunden verwalteten Schlüssel in einer verschlüsselten WorkSpaces Thin Client-Umgebung registriert wird und der Name dieses Geräts geändert wird, erstellt Amazon WorkSpaces Thin Client in Ihrem Namen einen Zuschuss, indem es eine CreateGrant Anfrage an AWS KMS sendet. Zuschüsse in AWS KMS werden verwendet, um Amazon WorkSpaces Thin Client Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

Amazon WorkSpaces Thin Client benötigt den Zuschuss, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwenden zu können:

- Senden Sie Decrypt-Anfragen an AWS KMS, um die verschlüsselten Daten zu entschlüsseln

Sie können den Zugriff auf den Zuschuss jederzeit widerrufen oder dem Dienst den Zugriff auf den vom Kunden verwalteten Schlüssel entziehen. Wenn Sie dies tun, kann Amazon WorkSpaces Thin Client auf keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise versuchen, Umgebungsdetails abzurufen, auf die Amazon WorkSpaces Thin Client nicht zugreifen kann, gibt der Vorgang einen `AccessDeniedException` Fehler zurück. Darüber hinaus kann das WorkSpaces Thin Client-Gerät keine WorkSpaces Thin Client-Umgebung verwenden.

## Einen kundenverwalteten Schlüssel erstellen

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel mithilfe der AWS-Managementkonsole oder der AWS KMS-API-Operationen erstellen.

So erstellen Sie einen symmetrischen kundenverwalteten Schlüssel

Folgen Sie den Schritten zur Erstellen eines symmetrischen kundenverwalteten Schlüssels im Entwicklerhandbuch zum AWS Key Management Service.

Schlüsselrichtlinie

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf kundenverwaltete Schlüssel im Entwicklerhandbuch zum AWS Key Management Service.

Um Ihren vom Kunden verwalteten Schlüssel mit Ihren Amazon WorkSpaces Thin Client-Ressourcen zu verwenden, müssen die folgenden API-Operationen in der Schlüsselrichtlinie zugelassen sein:

- `kms:DescribeKey`— Stellt dem Kunden verwaltete Schlüsseldetails zur Verfügung, sodass Amazon WorkSpaces Thin Client den Schlüssel validieren kann.
- `kms:GenerateDataKey` – Ermöglicht die Verwendung des vom Kunden verwalteten Schlüssels zur Verschlüsselung der Daten.
- `kms:Decrypt` – Ermöglicht die Verwendung des vom Kunden verwalteten Schlüssels zur Entschlüsselung der Daten.
- `kms:CreateGrant` – Fügt einem vom Kunden verwalteten Schlüssel eine Gewährung hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS-Schlüssel, der den Zugriff auf die Grant-Operationen ermöglicht, die Amazon WorkSpaces Thin Client benötigt. Weitere Informationen finden Sie zur Verwendung von Gewährungen finden Sie im Entwicklerhandbuch zum AWS Key Management Service.

  Dadurch kann Amazon WorkSpaces Thin Client Folgendes tun:

  - `Decrypt` aufrufen, um die verschlüsselten Daten zu entschlüsseln.

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, die Sie für Amazon WorkSpaces Thin Client hinzufügen können:

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zum Festlegen von Berechtigungen in einer Richtlinie finden Sie im Entwicklerhandbuch zum AWS Key Management Service.

Weitere Informationen zur Fehlerbehebung beim Schlüsselzugriff finden Sie im Entwicklerhandbuch zum AWS Key Management Service.

## Angabe eines vom Kunden verwalteten Schlüssels für WorkSpaces Thin Client

Sie können einen vom Kunden verwalteten Schlüssel als zweite Verschlüsselungsebene für die folgenden Ressourcen festlegen:

- WorkSpaces Thin-Client-Umgebung

Wenn Sie eine Umgebung erstellen, können Sie den Datenschlüssel angeben, indem Sie einen angeben`kmsKeyArn`, den Amazon WorkSpaces Thin Client zur Verschlüsselung der identifizierbaren personenbezogenen Daten verwendet.

- `kmsKeyArn`— Eine Schlüssel-ID für einen AWS vom Kunden verwalteten KMS-Schlüssel. Geben Sie einen Schlüssel-ARN an.

Wenn der WorkSpaces Thin Client-Umgebung ein neues Thin Client-Gerät hinzugefügt wird, das WorkSpaces mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, erbt das WorkSpaces Thin Client-Gerät die Einstellung für den vom Kunden verwalteten Schlüssel aus der WorkSpaces Thin Client-Umgebung.

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, der zusätzliche kontextbezogene Informationen zu den Daten enthält.

AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen. Wenn Sie einen Verschlüsselungskontext in eine Anforderung zur Datenverschlüsselung aufnehmen, bindet AWS KMS den Verschlüsselungskontext an die verschlüsselten Daten. Um Daten zu entschlüsseln, müssen Sie denselben Verschlüsselungskontext in die Anfrage aufnehmen.

Amazon WorkSpaces Thin Client-Verschlüsselungskontext

Amazon WorkSpaces Thin Client verwendet bei allen kryptografischen AWS KMS-Vorgängen denselben Verschlüsselungskontext, wobei der Schlüssel `aws:thinclient:arn` und der Wert der Amazon-Ressourcenname (ARN) ist.

Im Folgenden ist der Environment-Verschlüsselungskontext dargestellt:

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

Der folgende Kontext ist der Geräteverschlüsselungskontext:

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

Verwenden des Verschlüsselungskontexts für die Überwachung

Wenn Sie einen symmetrischen, vom Kunden verwalteten Schlüssel verwenden, um Ihre WorkSpaces Thin Client-Umgebung und Gerätedaten zu verschlüsseln, können Sie den Verschlüsselungskontext auch in Prüfaufzeichnungen und Protokollen verwenden, um zu ermitteln, wie der vom Kunden verwaltete Schlüssel verwendet wird. Der Verschlüsselungskontext erscheint auch in Protokollen, die von AWS CloudTrail oder Amazon CloudWatch Logs generiert wurden.

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den vom Kunden verwalteten Schlüssel

Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als Bedingungen verwenden, um den Zugriff auf Ihren symmetrischen, vom Kunden verwalteten Schlüssel zu kontrollieren. Sie können Verschlüsselungskontext-Einschränkungen auch in einer Genehmigung verwenden.

Amazon WorkSpaces Thin Client verwendet bei Zuschüssen eine Einschränkung des Verschlüsselungskontextes, um den Zugriff auf den vom Kunden verwalteten Schlüssel in Ihrem Konto oder Ihrer Region zu kontrollieren. Eine Genehmigungseinschränkung erfordert, dass durch die Genehmigung ermöglichte Vorgänge den angegebenen Verschlüsselungskontext verwenden.

Im Folgenden finden Sie Beispiele für Schlüsselrichtlinienanweisungen zur Gewährung des Zugriffs auf einen vom Kunden verwalteten Schlüssel für einen bestimmten Verschlüsselungskontext. Die Bedingung in dieser Richtlinienanweisung setzt voraus, dass der `kms:Decrypt`-Aufruf eine Einschränkung des Verschlüsselungskontextes hat, die den Verschlüsselungskontext spezifiziert.

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
```

```
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

## Überwachung Ihrer Verschlüsselungsschlüssel für Amazon WorkSpaces Thin Client

Wenn Sie einen AWS vom Kunden verwalteten KMS-Schlüssel mit Ihren Amazon WorkSpaces Thin Client-Ressourcen verwenden, können Sie AWS CloudTrail oder Amazon CloudWatch Logs verwenden, um Anfragen zu verfolgen, die Amazon WorkSpaces Thin Client an AWS KMS sendet.

Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`DescribeKey`,, `CreateGrant` `GenerateDataKeyDecrypt`, `Decrypt` (mit`Grant`) zur Überwachung von KMS-Vorgängen, die von Amazon WorkSpaces Thin Client aufgerufen werden, um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden:

In den folgenden Beispielen sehen Sie sich `encryptionContext` die WorkSpaces Thin Client-Umgebung an. Ähnliche CloudTrail Ereignisse werden für das WorkSpaces Thin Client-Gerät aufgezeichnet.

DescribeKey

Amazon WorkSpaces Thin Client verwendet den `DescribeKey` Vorgang, um den vom Kunden verwalteten AWS KMS-Schlüssel zu verifizieren.

Das folgende Beispielereignis zeichnet den Vorgang `DescribeKey` auf:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


### CreateGrant

Amazon WorkSpaces Thin Client verwendet den `CreateGrant` Vorgang, um einen KMS-Grant zu erstellen, mit dem Sie Daten entschlüsseln können, wenn das Gerät darauf zugreift.

Das folgende Beispielereignis zeichnet den Vorgang `CreateGrant` auf:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
        "operations": ["Decrypt"],
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
```

```
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

### GenerateDataKey

Amazon WorkSpaces Thin Client verwendet den `GenerateDataKey` Vorgang, um Daten zu verschlüsseln.

Das folgende Beispielereignis zeichnet den Vorgang `GenerateDataKey` auf:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-03-12T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

### Decrypt

Amazon WorkSpaces Thin Client verwendet den `Decrypt` Vorgang zum Entschlüsseln von Daten.

Das folgende Beispielereignis zeichnet den Vorgang `Decrypt` auf:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
```

```
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt (using Grant)

Wenn das WorkSpaces Thin Client-Gerät auf Umgebungs- oder Geräteinformationen zugreift, wird der `Decrypt` Vorgang verwendet, der über einen KMS-Schlüssel zugelassen wird. `Grant`

Das folgende Beispielereignis zeichnet den `Decrypt` Vorgang auf, der über einen `Grant` autorisiert wurde:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
```

```
    "requestParameters": {
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```


## Weitere Informationen

Die folgenden Ressourcen bieten weitere Informationen zur Datenverschlüsselung im Ruhezustand:

- Weitere Informationen finden Sie unter Grundlegende Konzepte von AWS Key Management Service im Entwicklerhandbuch für AWS Key Management Service.
- Weitere Informationen zu bewährten Sicherheitsmethoden für AWS Key Management Service finden Sie im AWS Key Management Service Developer Guide.

## Verschlüsselung während der Übertragung

WorkSpaces Thin Client verschlüsselt Daten während der Übertragung über HTTPS und TLS 1.2. Sie können eine Anfrage an WorkSpaces Thin Client senden, indem Sie die Konsole oder direkte API-Aufrufe verwenden. Die übertragenen Anforderungsdaten werden verschlüsselt, indem sie über eine HTTPS- oder TLS-Verbindung gesendet werden. Anforderungsdaten können von der AWS Konsole, der AWS Befehlszeilenschnittstelle oder dem AWS SDK an den WorkSpaces Thin Client übertragen werden. Dazu gehören auch alle Softwareupdates auf dem Gerät.

Sowohl die Verschlüsselung während der Übertragung als auch sichere Verbindungen (HTTPS, TLS) sind standardmäßig konfiguriert.

## Schlüsselverwaltung

Sie können Ihren eigenen vom Kunden verwalteten AWS KMS-Schlüssel angeben, um Ihre Kundeninformationen zu verschlüsseln. Wenn Sie keinen Schlüssel angeben, verwendet WorkSpaces Thin Client einen AWS eigenen Schlüssel. Sie können Ihren Schlüssel mithilfe des AWS SDK festlegen.

## Internet, Arbeit, Verkehr, Datenschutz

Administratoren können WorkSpaces Thin Client-Sitzungsereignisse, einschließlich Startzeiten und Informationen zu ausstehenden Softwareupdates, einsehen. Diese Protokolle werden verschlüsselt und den Kunden sicher in der WorkSpaces Thin Client-Konsole zugestellt. Benutzerinformationen und weitere Details zu einzelnen Streaming-Desktop-Sitzungen werden von den Desktop-Diensten aufgezeichnet. Weitere Informationen finden Sie unter Überwachen von WorkSpaces, Monitoring and Reporting for AppStream 2.0 oder Benutzerzugriffsprotokollierung für das WorkSpaces Web.

# Identity and Access Management für Amazon WorkSpaces Thin Client

AWS Identity and Access Management (IAM) ist ein AWS-Service , mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer für die Nutzung von WorkSpaces Thin-Client-Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service , den Sie ohne zusätzliche Kosten verwenden können.

Themen

## Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in WorkSpaces Thin Client.

Service-Benutzer – Wenn Sie den WorkSpaces Thin-Client-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere WorkSpaces Thin Client-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf ein Feature in WorkSpaces Thin Client nicht zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung für Amazon WorkSpaces -Thin-Client-Identität und -Zugriff.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für WorkSpaces Thin-Client-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf WorkSpaces Thin Client. Ihre Aufgabe besteht darin, zu bestimmen, auf welche Funktionen und Ressourcen von WorkSpaces Thin Client Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit WorkSpaces Thin Client verwenden kann, finden Sie unter Funktionsweise von Amazon WorkSpaces Thin Client mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf WorkSpaces Thin Client verfassen können. Beispiele für identitätsbasierte WorkSpaces Thin-Client-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client.

# Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten bei anmelden. Sie müssen als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (bei angemeldet AWS) sein.

Sie können sich bei AWS als Verbundidentität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt werden. AWS IAM Identity Center (IAM Identity Center)-Benutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie AWS über einen Verbund auf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, um welchen Benutzertyp es sich handelt, können Sie sich bei der AWS Management Console oder im - AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung bei AWS finden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung - Benutzerhandbuch.

Wenn Sie AWS programmgesteuert auf zugreifen, AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (Command Line Interface, CLI) bereit, um Ihre Anforderungen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine - AWS Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenständigen Signieren von Anforderungen finden Sie unter Signieren von AWS API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. empfiehlt beispielsweise, AWS die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

## AWS-Konto Root-Benutzer

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet und Sie melden sich mit der E-Mail-Adresse und dem Passwort an, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für

Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

## Verbundidentität

Fordern Sie als bewährte Methode menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, auf, den Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen auf zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, die AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit AWS-Services Anmeldeinformationen auf zugreift, die über eine Identitätsquelle bereitgestellt werden. Wenn Verbundidentitäten auf zugreifen AWS-Konten, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen oder eine Verbindung zu einer Reihe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie für alle Ihre AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

## IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI - oder AWS -API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff: Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können AWS-Services Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anfragen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder -Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

## Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff in , AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anfügen. Eine Richtlinie ist ein Objekt in , AWS das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console, der AWS CLI oder der AWS -API abrufen.

### Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem anfügen können AWS-Konto. Verwaltete

Richtlinien umfassen AWS -verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

## Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services AWS WAF, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter Zugriffssteuerungsliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

## Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen:Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte

Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service-Kontrollrichtlinien (SCPs )– SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien:Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

### Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik zur Richtlinienbewertung im IAM-Benutzerhandbuch.

## Funktionsweise von Amazon WorkSpaces Thin Client mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf WorkSpaces Thin Client zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit WorkSpaces Thin Client verwenden können.

IAM-Funktionen, die Sie mit Amazon WorkSpaces Thin Client verwenden können

| IAM-Feature | WorkSpaces Unterstützung für Thin Client |
| --- | --- |
| Identitätsbasierte Richtlinien | Ja |

| IAM-Feature | WorkSpaces Unterstützung für Thin Client |
|---|---|
| Ressourcenbasierte Richtlinien | Nein |
| Richtlinienaktionen | Ja |
| Richtlinienressourcen | Ja |
| Bedingungsschlüssel für die Richtlinie | Ja |
| ACLs | Nein |
| ABAC (Tags in Richtlinien) | Ja |
| Temporäre Anmeldeinformationen | Ja |
| Hauptberechtigungen | Ja |
| Servicerollen | Nein |
| Serviceverknüpfte Rollen | Nein |

Einen Überblick über das Zusammenwirken von WorkSpaces Thin Client und anderen - AWS Services mit den meisten IAM-Funktionen finden Sie unter -AWS Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

## Identitätsbasierte Richtlinien für WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt Richtlinien auf Identitätsbasis. | Ja |

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen,

unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für WorkSpaces Thin Client

Beispiele für identitätsbasierte WorkSpaces Thin-Client-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client.

## Ressourcenbasierte Richtlinien in WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt ressourcenbasierte Richtlinien | Nein |

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen befinden AWS-Konten, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipal-Entität (Benutzer oder Rolle) die Berechtigung für den Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

## Richtlinienaktionen für WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt Richtlinienaktionen | Ja |

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben in der Regel denselben Namen wie die zugehörige AWS API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der WorkSpaces Thin-Client-Aktionen finden Sie unter Von Amazon WorkSpaces Thin Client definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in WorkSpaces Thin Client verwenden das folgende Präfix vor der Aktion:

```
workspaces-thin-client
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie durch Kommas, wie im folgenden Beispiel gezeigt:

```
"Action": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

Beispiele für identitätsbasierte WorkSpaces Thin-Client-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client.

## Richtlinienressourcen für WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt Richtlinienressourcen | Ja |

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der WorkSpaces Thin-Client-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon WorkSpaces Thin Client definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Amazon WorkSpaces Thin Client definierte Aktionen.

Beispiele für identitätsbasierte WorkSpaces Thin-Client-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client.

## Richtlinienbedingungsschlüssel für WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt servicespezifische Richtlini enbedingungsschlüssel | Ja |

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der WorkSpaces Thin-Client-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon WorkSpaces Thin Client in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon WorkSpaces Thin Client definierte Aktionen.

Beispiele für identitätsbasierte WorkSpaces Thin-Client-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client.

## ACLs in WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt ACLs | Nein |

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

## ABAC mit WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt ABAC (Tags in Richtlinien) | Ja |

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

## Verwenden temporärer Anmeldeinformationen mit WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt temporäre Anmeldeinformationen | Ja |

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich AWS Management Console mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn

Sie beispielsweise AWS über den SSO-Link (Single Sign-On) Ihres Unternehmens auf zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell mit der AWS CLI oder der AWS API erstellen. Sie können diese temporären Anmeldeinformationen dann verwenden, um auf zuzugreifen AWS. AWS empfohlen, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

## Serviceübergreifende Prinzipalberechtigungen für WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt Forward Access Sessions (FAS) | Ja |

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anfragen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder -Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

## Servicerollen für WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt Servicerollen | Nein |

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die Funktionalität von WorkSpaces Thin Client beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn WorkSpaces Thin Client dazu Anleitungen gibt.

### Serviceverknüpfte Rollen für WorkSpaces Thin Client

| | |
|---|---|
| Unterstützt serviceverknüpfte Rollen | Nein |

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

## Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von WorkSpaces Thin-Client-Ressourcen. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von WorkSpaces Thin Client definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen,

Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Thin Client in der Service-Autorisierungs-Referenz.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der WorkSpaces Thin Client-Konsole
- Gewähren Sie schreibgeschützten Zugriff auf WorkSpaces Thin Client
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Gewähren Sie vollen Zugriff auf WorkSpaces Thin Client

## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand WorkSpaces Thin-Client-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die -AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar AWS-Konto. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die für Ihre Anwendungsfälle spezifisch sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten:Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs:Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen,

dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn sie über eine bestimmte verwendet werden AWS-Service, z. B. AWS CloudFormation. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten:IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich – Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

## Verwenden der WorkSpaces Thin Client-Konsole

Um auf die Amazon- WorkSpaces Thin-Client-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den WorkSpaces Thin Client-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen für die Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

## Gewähren Sie schreibgeschützten Zugriff auf WorkSpaces Thin Client

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen können, die es IAM-Benutzern ermöglicht, eine WorkSpaces Thin-Client-Konfiguration anzuzeigen, aber keine Änderungen vorzunehmen.

Diese Richtlinie enthält Berechtigungen zum Abschließen dieser Aktion auf der Konsole oder dem Programm mithilfe der AWS CLI oder AWS API.

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

## Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder AWS API.

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

## Gewähren Sie vollen Zugriff auf WorkSpaces Thin Client

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen können, die den Benutzern von WorkSpaces Thin Client IAM Vollzugriff gewährt. Diese Richtlinie enthält Berechtigungen zum Abschließen aller WorkSpaces Thin Client-Aktionen auf der Konsole oder dem Programm mithilfe der AWS CLI oder AWS API.

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

# Fehlerbehebung für Amazon WorkSpaces -Thin-Client-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit WorkSpaces Thin Client und IAM auftreten können.

Themen



## Ich bin nicht autorisiert, eine Aktion in WorkSpaces Thin Client auszuführen

Wenn Sie von der AWS Management Console erfahren, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-thin-client-device`*-Ressource zu verwenden, jedoch nicht über `workspaces-thin-client:`*`ListDevices`*-Berechtigungen verfügt.

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

In diesem Fall bittet Mateo seinen Administrator, seine Richtlinien zu aktualisieren, damit er mithilfe der `workspaces-thin-client:`*`ListDevices`* Aktion auf die *`my-thin-client-device`* Ressource zugreifen kann.

## Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM-Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit anzeigen. Sie können Ihren geheimen Zugriffsschlüssel jedoch nicht erneut anzeigen. Wenn Sie den geheimen Zugriffsschlüssel verlieren, müssen Sie ein neues Zugriffsschlüsselpaar erstellen.

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID (z. B. `AKIAIOSFODNN7EXAMPLE`) und einem geheimen Zugriffsschlüssel (z. B. `wJalrXUtnFEMI/`

K7MDENG/bPxRfiCYEXAMPLEKEY). Ähnlich wie bei Benutzernamen und Passwörtern müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zusammen verwenden, um Ihre Anforderungen zu authentifizieren. Verwalten Sie Ihre Zugriffsschlüssel so sicher wie Ihren Benutzernamen und Ihr Passwort.

> **Important**
>
> Geben Sie Ihre Zugriffsschlüssel nicht an Dritte weiter, auch nicht für die Suche nach Ihrer kanonischen Benutzer-ID. Auf diese Weise können Sie jemandem dauerhaften Zugriff auf Ihr gewähren AWS-Konto.

Während der Erstellung eines Zugriffsschlüsselpaars werden Sie aufgefordert, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Speicherort zu speichern. Der geheime Zugriffsschlüssel ist nur zu dem Zeitpunkt verfügbar, an dem Sie ihn erstellen. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, müssen Sie Ihrem IAM-Benutzer neue Zugriffsschlüssel hinzufügen. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei Zugriffschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Anweisungen hierfür finden Sie unter Verwalten von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

## Ich bin Administrator und möchte anderen Zugriff auf WorkSpaces Thin Client gewähren

Um anderen Personen oder einer Anwendung Zugriff auf WorkSpaces Thin Client zu gewähren, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Anschließend müssen Sie der Entität eine Richtlinie anfügen, die dieser die richtigen Berechtigungen in WorkSpaces Thin Client gewährt.

Informationen zum Einstieg finden Sie unter Erstellen Ihrer ersten delegierten IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Weitere Informationen finden Sie unter Gewähren Sie vollen Zugriff auf WorkSpaces Thin Client.

## Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine WorkSpaces Thin Client-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem

die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob WorkSpaces Thin Client diese Funktionen unterstützt, finden Sie unter Funktionsweise von Amazon WorkSpaces Thin Client mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre AWS-Konten -Ressourcen in Ihrem Besitz finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

# Ausfallsicherheit in Amazon WorkSpaces Thin Client

Die AWS globale -Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit niedriger Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen -Infrastruktur stellt WorkSpaces derhin Client verschiedene Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden.

# Schwachstellenanalyse und -management in Amazon WorkSpaces Thin Client

Konfigurations- und IT-Kontrollen sind eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Weitere Informationen finden Sie im AWS Modell der geteilten Verantwortung.

Amazon WorkSpaces Thin Client ist in Amazon WorkSpaces, Amazon AppStream 2.0 und WorkSpaces Web integriert. Weitere Informationen zur Aktualisierungsverwaltung für jeden dieser Services finden Sie unter den folgenden Links:

- Update-Management in Amazon AppStream 2.0
- Update-Verwaltung in Amazon WorkSpaces
- Konfigurations- und Schwachstellenanalyse in Amazon WorkSpaces Web

# Überwachen von Amazon WorkSpaces Thin Client

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon WorkSpaces Thin Client und Ihren anderen - AWS Lösungen aufrechtzuerhalten. AWS bietet die folgenden Überwachungstools, um WorkSpaces Thin Client zu überwachen, Missstände zu melden und ggf. automatische Maßnahmen zu ergreifen:

- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit. Sie können Benutzer und Konten identifizieren, die aufgerufen haben AWS, die Quell-IP-Adresse, von der aus die Aufrufe getätigt wurden, und den Zeitpunkt der Aufrufe. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

# Protokollieren von Amazon- WorkSpaces Thin-Client-API-Aufrufen mit AWS CloudTrail

Amazon WorkSpaces Thin Client ist in integriert, einem Service AWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines - AWS Services in WorkSpaces Thin Client aufzeichnet. CloudTrail erfasst alle API-Aufrufe für WorkSpaces Thin Client als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der WorkSpaces Thin-Client-Konsole und Codeaufrufe der WorkSpaces Thin-Client-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für WorkSpaces Thin Client. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an WorkSpaces Thin Client gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

## WorkSpaces Thin-Client-Informationen in CloudTrail

CloudTrail wird beim Erstellen des Kontos AWS-Konto auf Ihrem aktiviert. Wenn eine Aktivität in WorkSpaces Thin Client auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen - AWS Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können in Ihrem AWS-

Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für WorkSpaces Thin Client, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der - AWS Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit. Darüber hinaus können Sie andere AWS -Services konfigurieren, um die in CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle WorkSpaces Thin-Client-Aktionen werden von protokolliert CloudTrail und sind in der Amazon-WorkSpaces Thin-Client-API-Referenz dokumentiert. Aufrufe der `GetSoftwareSet` Aktionen `CreateEnvironment`, `ListDevices`sund erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Root- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung von einem anderen - AWS Service gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

# Grundlegendes WorkSpaces zu Thin Client-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `GetDevice` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
```

```
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
    "eventID": "<event-id>",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
}
```

# Erstellen von Amazon- WorkSpaces Thin-Client-Ressourcen mit AWS CloudFormation

Amazon WorkSpaces Thin Client ist in integriert AWS CloudFormation, einem Service, der Sie bei der Modellierung und Einrichtung Ihrer - AWS Ressourcen unterstützt. Auf diese Weise können Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. Umgebungen) und diese Ressourcen für Sie AWS CloudFormation bereitstellt und konfiguriert.

Wenn Sie verwenden AWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre WorkSpaces Thin-Client-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen wiederholt in mehreren AWS-Konten und Regionen bereit.

## WorkSpaces Thin Client und AWS CloudFormation Vorlagen

Um Ressourcen für WorkSpaces Thin Client und verwandte Services bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation die Vorlagen verstehen. Vorlagen sind formatierte Textdateien im JSON- oder YAML-Format. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON- oder YAML-Formaten nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen den Einstieg in AWS CloudFormation Vorlagen zu erleichtern. Weitere Informationen finden Sie unter Was ist AWS CloudFormation -Designer? im AWS CloudFormation -Benutzerhandbuch.

WorkSpaces Thin Client unterstützt das Erstellen von Umgebungen in AWS CloudFormation. Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für Umgebungen, finden Sie in der Ressourcentypreferenz für Amazon WorkSpaces Thin Client im AWS CloudFormation -Benutzerhandbuch.

## Weitere Informationen über AWS CloudFormation

Weitere Informationen zu finden Sie AWS CloudFormation in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation API Referenz

- AWS CloudFormation Benutzerhandbuch für die -Befehlszeilenschnittstelle

# Zugriff auf Amazon WorkSpaces Thin Client über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können verwenden AWS PrivateLink , um eine private Verbindung zwischen Ihrer VPC und Amazon WorkSpaces Thin Client herzustellen. Sie können auf WorkSpaces Thin Client als VPC zugreifen, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine - AWS Direct Connect Verbindung zu verwenden. Instances in Ihrer VPC benötigen für den Zugriff auf WorkSpaces Thin Client keine öffentlichen IP-Adressen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellenendpunkt erstellen, der von unterstützt wird AWS PrivateLink. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Dies sind vom Anforderer verwaltete Netzwerkschnittstellen, die als Eintrittspunkt für Datenverkehr dienen, der für WorkSpaces Thin Client bestimmt ist.

Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

## Überlegungen für WorkSpaces Thin Client

Bevor Sie einen Schnittstellenendpunkt für WorkSpaces Thin Client einrichten, lesen Sie Überlegungen im AWS PrivateLink -Handbuch.

WorkSpaces Thin Client unterstützt Aufrufe aller API-Aktionen über den Schnittstellenendpunkt.

## Erstellen eines Schnittstellenendpunkts für WorkSpaces Thin Client

Sie können einen Schnittstellenendpunkt für WorkSpaces Thin Client erstellen, indem Sie entweder die Amazon-VPC-Konsole oder die AWS Command Line Interface (AWS CLI) verwenden. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für WorkSpaces Thin Client, indem Sie den folgenden Servicenamen verwenden:

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

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anforderungen an WorkSpaces Thin Client unter Verwendung des standardmäßigen regionalen DNS-Namens senden. Beispiel: `api.thinclient.us-east-1.amazonaws.com`

## Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die Standard-Endpunktrichtlinie bietet Ihnen vollen Zugriff auf WorkSpaces Thin Client über den Schnittstellenendpunkt. Um den Zugriff zu steuern, der WorkSpaces Thin Client von Ihrer VPC aus gewährt wird, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für WorkSpaces Thin-Client-Aktionen

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anfügen, gewährt sie Zugriff auf die aufgelisteten WorkSpaces Thin-Client-Aktionen für alle Prinzipale auf allen Ressourcen.

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

```
    ]
}
```

# Dokumentverlauf für das WorkSpaces Thin Client-Administratorhandbuch

In der folgenden Tabelle wird der Dokumentationsverlauf für Versionen des WorkSpaces Thin-Client-Administratorhandbuchs beschrieben.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| • Konfigurieren von WorkSpaces für Amazon WorkSpaces Thin Client<br>• Konfigurieren von AppStream 2.0 für Amazon WorkSpaces Thin Client | • Die Liste der Betriebss ysteme wurde aktualisiert.<br>• Das Verfahren für Identität sanbieter wurde aktualisiert. | 12. Februar 2024 |
| Erstversion | Erstversion | 26. November 2023 |

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.