Benutzerhandbuch

Amazon WorkSpaces Thin Client

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

Amazon WorkSpaces Thin Client: Benutzerhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist die Amazon WorkSpaces Thin Client Administratorkonsole? ... 1
Verwenden Sie zum ersten Mal? ... 1
Architektur ... 1
Einrichtung der Amazon WorkSpaces Thin Client-Administratorkonsole ... 4
Registrieren bei AWS ... 4
Erstellen eines IAM-Benutzers ... 4
Erste Schritte mit Ihrer VDI für Amazon WorkSpaces Thin Client-Administratorkonsole ... 6
Konfiguration von WorkSpaces Personal für WorkSpaces Thin Client ... 6
Bevor Sie beginnen ... 7
Schritt 1: Stellen Sie sicher, dass Ihr System die für WorkSpaces Personal erforderlichen Funktionen erfüllt ... 7
Schritt 2: Verwenden Sie die erweiterten Einstellungen, um Ihre zu starten WorkSpace ... 8
Geschäftskontinuität ... 9
Konfiguration von WorkSpaces Pools für WorkSpaces Thin Client ... 10
Bevor Sie beginnen ... 10
Erstellen Sie einen WorkSpaces Pool ... 11
Konfiguration des WorkSpaces Thin Client-Zugriffs ... 14
Konfiguration von AppStream 2.0 für Amazon WorkSpaces Thin Client ... 14
Schritt 1: Stellen Sie sicher, dass Ihr System die für AppStream Version 2.0 erforderlichen Funktionen erfüllt ... 15
Schritt 2: Richten Sie Ihre AppStream 2.0-Stacks ein ... 16
Konfiguration von Amazon WorkSpaces Secure Browser für Amazon WorkSpaces Thin Client ... 16
Schritt 1: Stellen Sie sicher, dass Ihr System die für Amazon WorkSpaces Secure Browser erforderlichen Funktionen erfüllt ... 17
Schritt 2: Richten Sie WorkSpaces Secure Browser-Portale ein ... 17
Die WorkSpaces Thin Client-Administratorkonsole starten ... 19
Abgedeckte Regionen ... 19
Starten der WorkSpaces Thin Client-Administratorkonsole ... 20
Verwenden der WorkSpaces Thin Client-Administratorkonsole ... 21
Umgebungen ... 22
Umgebungsliste ... 22
Details der Umgebung ... 24
Erstellen einer Umgebung ... 28

Bearbeiten einer Umgebung ... 31
Löschen einer Umgebung ... 32
Geräte ... 33
Geräteliste ... 33
Gerätedetails ... 36
Bearbeiten eines Gerätenamens ... 43
Zurücksetzen und Abmelden des Geräts ... 43
Archivieren eines Geräts ... 44
Löschen eines Geräts ... 44
Exportieren der Gerätedetails ... 45
Software-Updates ... 45
Aktualisieren der Umgebungssoftware ... 45
Aktualisieren der Gerätesoftware ... 46
WorkSpaces Thin Client-Softwareversionen ... 47
Verwendung von Tags auf WorkSpaces Thin Client-Ressourcen ... 60
Sicherheit ... 64
Datenschutz ... 64
Datenverschlüsselung ... 66
Verschlüsselung im Ruhezustand ... 67
Verschlüsselung während der Übertragung ... 82
Schlüsselverwaltung ... 82
Internet, Arbeit, Verkehr, Datenschutz ... 82
Identity and Access Management ... 82
Zielgruppe ... 83
Authentifizierung mit Identitäten ... 84
Verwalten des Zugriffs mit Richtlinien ... 88
So funktioniert Amazon WorkSpaces Thin Client mit IAM ... 91
Beispiele für identitätsbasierte Richtlinien ... 98
AWS verwaltete Richtlinien ... 103
Fehlerbehebung ... 108
Ausfallsicherheit ... 111
Schwachstellenanalyse und -management ... 112
Überwachen ... 113
CloudTrail protokolliert ... 113
CloudTrail Datenereignisse ... 115
CloudTrail Verwaltungsereignisse ... 116

CloudTrail Beispiele für Ereignisse 116
AWS CloudFormation Ressourcen 121
WorkSpaces Thin Client und AWS CloudFormation Vorlagen 121
Erfahren Sie mehr über AWS CloudFormation 121
AWS PrivateLink 123
Überlegungen 123
Erstellen eines Schnittstellenendpunkts 123
Erstellen einer Endpunktrichtlinie 124
Dokumentverlauf 126
..... cxxix

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?
- Architektur

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

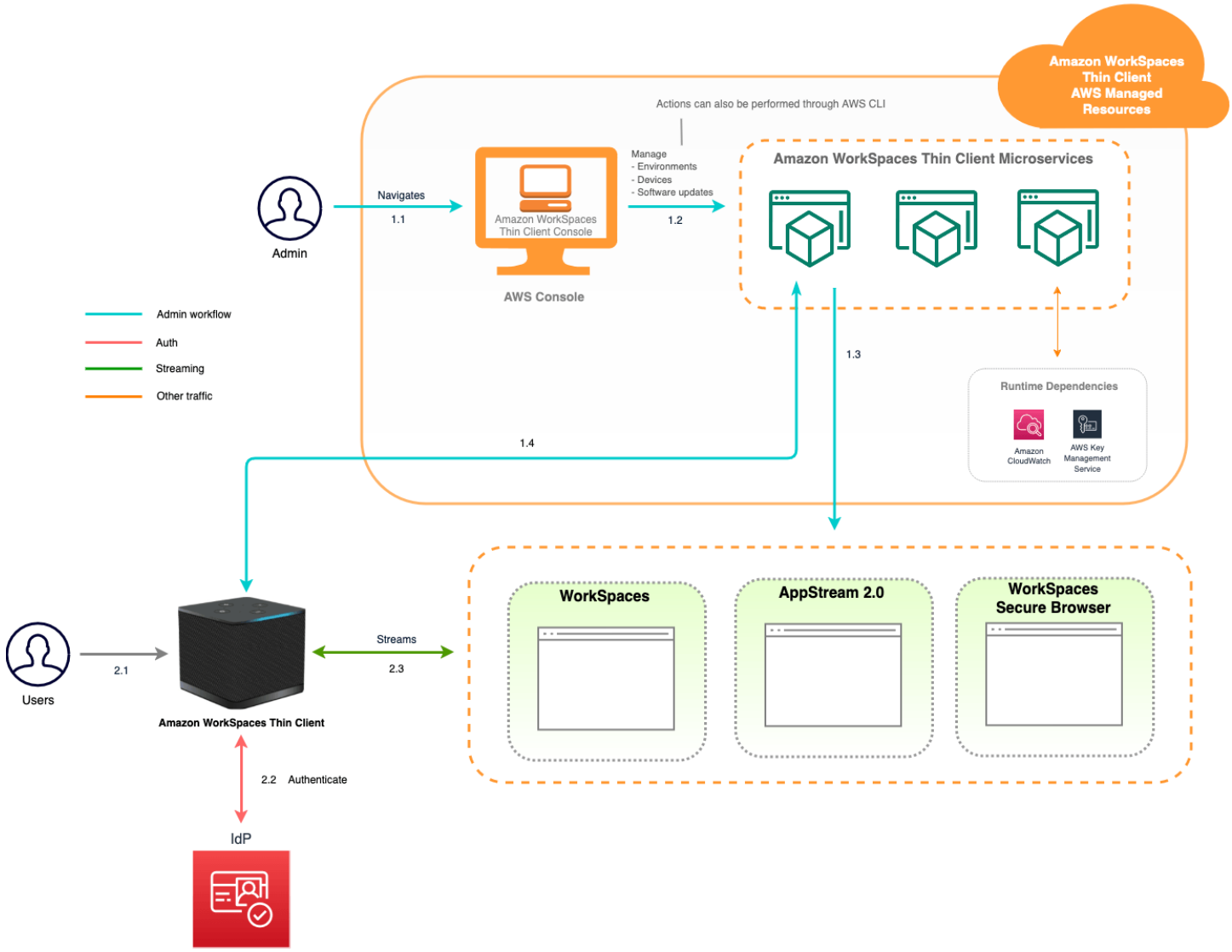
Je nach verwendetem VDI werden die Informationen für Ihren WorkSpaces Thin Client entweder über Verzeichnisse für WorkSpaces, Stacks für AppStream 2.0 und Webportal-Endpunkte für WorkSpaces Secure Browser abgerufen und verwaltet.

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
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
Admin workflow
Auth
Streaming
Other traffic
1.4
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
2.2 Authenticate
IdP

Einrichtung der Amazon WorkSpaces Thin Client-Administratorkonsole

Themen

- Registrieren bei AWS
- Erstellen eines IAM-Benutzers

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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

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 (Empfohlen)	Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS. 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 AWS CLI die Konfiguration für die Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch vornehmen.
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Folgen Sie den Anweisungen unter Erstellen eines IAM-Benutzers für den Notfallzugriff im IAM-Benutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff unter Zugriffsschlüssel für IAM-Benutzer verwalten im IAM-Benutzerhandbuch.

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 von WorkSpaces Personal für WorkSpaces Thin Client
- Konfiguration von WorkSpaces Pools für WorkSpaces Thin Client
- Konfiguration von AppStream 2.0 für Amazon WorkSpaces Thin Client
- Konfiguration von Amazon WorkSpaces Secure Browser für Amazon WorkSpaces Thin Client

Konfiguration von WorkSpaces Personal für WorkSpaces Thin Client

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

> **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 Personal.
- 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 für WorkSpaces Personal verwalten.
- Wenn Sie einen starten WorkSpace, aktivieren und konfigurieren Sie den WorkSpaces Thin Client-Webzugriff. Weitere Informationen finden Sie unter WorkSpaces Thin Client konfigurieren

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

Damit die WorkSpaces Thin Client-Administratorkonsole ordnungsgemäß mit Amazon WorkSpaces Personal funktioniert, 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 • Windows 10 (Bring-Your-Own-License) • Windows 11 • Windows 11 (Bring-Your-Own-License)
Unterstützte Pakete	• Microsoft Power mit Windows 10 (basierend auf Server 2016, 2019 und 2022) • Microsoft Power mit Windows 10 (basierend auf Server 2016, 2019 und 2022) w Office • Microsoft PowerPro mit Windows 10 (basierend auf Server 2016, 2019 und 2022) • Microsoft PowerPro mit Windows 10 (auf Server 2016, 2019 und 2022) w Office • Microsoft-Leistung mit Windows 10 (basieren d auf Server 2016, 2019 und 2022) • Microsoft-Leistung mit Windows 10 (basieren d auf Server 2016, 2019 und 2022) w Office
Unterstützte Protokolle	Nur DCV

Schritt 2: Verwenden Sie die erweiterten Einstellungen, um Ihre zu starten WorkSpace

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

1. Öffnen Sie die WorkSpaces Konsole unterhttps://console.aws.amazon.com/workspaces/v2/home/.
2. Wählen Sie eine der folgenden Verzeichnistypen und klicken Sie dann auf Weiter:
   - AWS Verwaltetes 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 aus.

Geschäftskontinuität

WorkSpaces Thin Client unterstützt die Geschäftskontinuität im Rahmen eines Business Continuity Plans (BCP). WorkSpaces Thin Client Business Continuity ist nur für die Verwendung mit WorkSpaces Personal verfügbar. Weitere Informationen zur Geschäftskontinuität finden Sie unter Business Continuity for WorkSpaces Personal im WorkSpaces Amazon-Administratorhandbuch.

Voraussetzungen

Damit Business Continuity auf WorkSpaces Thin Client funktioniert, müssen die folgenden Voraussetzungen erfüllt sein:

- Für die WorkSpaces regionsübergreifende Umleitung — Der DNS-Dienst und die Routing-Richtlinien wurden konfiguriert. Informationen zur Einrichtung dieser Richtlinien finden Sie unter Konfiguration Ihres DNS-Dienstes und Einrichten von DNS-Routingrichtlinien.
- Für Resilienz WorkSpaces in mehreren Regionen — WorkSpaces Es wurde ein Standby eingerichtet. Informationen dazu, wie Sie dies erstellen, finden Sie unter Einen Standby WorkSpace erstellen.
- Ein Verbindungsalias in der Region, die WorkSpaces Thin Client verwendet. Informationen zur Überprüfung Ihrer Region finden Sie unter Abgedeckte Regionen.

Konfiguration der Geschäftskontinuität für WorkSpaces Thin Client

Um WorkSpaces Personal DR auf Amazon WorkSpaces Thin Client zu aktivieren, müssen Sie Verbindungsaliase so konfigurieren, dass sie der Umgebung mithilfe des SDK zugeordnet werden.

Beispiel für eine Erklärung in einem Dokument zur Einrichtung der Notfallwiederherstellung:

Example

Ein Beispielbefehl, der die AWS CLI verwendet, um eine neue Umgebung mit einem WorkSpaces Verbindungsalias für den Streaming-Desktop zu erstellen:

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

*wsca-id*Ersetzen Sie es durch Ihren WorkSpaces persönlichen Verbindungsalias. Die ID des WorkSpaces Verbindungsalias finden Sie in der WorkSpaces Management Console oder im SDK.

Erfahrung für Endbenutzer

Sobald die Geschäftskontinuität konfiguriert ist, müssen die Geräte innerhalb der letzten 15 Tage registriert und aktiv sein. Sollten die WorkSpaces Thin Client-Verwaltungsdienste danach nicht mehr verfügbar sein, können Benutzer bis zu 24 Stunden lang mit ihren Sitzungen verbunden bleiben. In diesem Zustand empfängt das Gerät keine Softwareupdates, tauscht keine Haltungsinformationen aus und kann nicht aktiviert werden. Der entsprechende Geräteeintrag in der WorkSpaces Thin Client-Konsole zeigt nicht die neuesten Informationen an.

Wenn die WorkSpaces Thin Client-Geräteverwaltungsdienste länger als 24 Stunden nicht verfügbar sind, wird die folgende Fehlermeldung angezeigt:

„Es ist ein Fehler aufgetreten. Bitte versuchen Sie es noch einmal. Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren IT-Administrator. (Fehlercode: 3006).“

Konfiguration von WorkSpaces Pools für WorkSpaces Thin Client

Damit WorkSpaces Thin Client mit Amazon WorkSpaces Pools verwendet werden kann, muss Ihr SAML 2.0-Identitätsanbieter (IdP) für den Zugriff auf das WorkSpaces Pools-Verzeichnis konfiguriert werden. Amazon WorkSpaces Pools-Verzeichnisse sind ein nicht persistenter Pool, der einer Benutzergruppe WorkSpaces zugewiesen ist.

> **Note**
>
> Vor der ersten Verwendung der Konsole müssen Konfigurationen vorgenommen werden.

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.

Lesen und verstehen Sie die unter Bevor Sie mit der Verwendung von Active Directory with WorkSpaces Pools beginnen im WorkSpaces Amazon-Administratorhandbuch aufgeführten Konzepte, bevor Sie mit Ihrer Konfiguration fortfahren.

Erstellen Sie einen WorkSpaces Pool

Richten Sie einen Pool ein und erstellen Sie ihn, aus dem Benutzeranwendungen gestartet und gestreamt werden.

> **Note**
>
> Sie sollten ein Verzeichnis erstellen, bevor Sie einen WorkSpaces Pool erstellen. Weitere Informationen finden Sie unter SAML 2.0 konfigurieren und ein WorkSpaces Pools-Verzeichnisverzeichnis erstellen.

So richten Sie einen Pool ein und erstellen ihn

1. Öffnen Sie die WorkSpaces Konsole unterhttps://console.aws.amazon.com/workspaces/v2/home/.
2. Wählen Sie WorkSpacesim Navigationsbereich Pools aus.
3. Wählen Sie Create WorkSpaces Pools aus.
4. Unter Onboarding (optional) können Sie Optionen empfehlen auswählen, die auf meinem Anwendungsfall basieren, um Empfehlungen für den Typ zu erhalten, den WorkSpaces Sie verwenden möchten. Sie können diesen Schritt überspringen, wenn Sie wissen, dass Sie WorkSpaces Pools verwenden möchten.
5. Geben Sie WorkSpaces unter Konfigurieren die folgenden Details ein:
   - Geben Sie unter Name eine eindeutige Namenskennung für den Pool ein. Sonderzeichen sind nicht zulässig.
   - Geben Sie unter Beschreibung eine Beschreibung für den Pool ein (maximal 256 Zeichen).
   - Wählen Sie für Bundle aus den folgenden Optionen den Bundle-Typ aus, den Sie für Ihr Paket verwenden möchten WorkSpaces.
     - Verwenden Sie ein WorkSpaces Basispaket — Wählen Sie eines der Bundles aus der Drop-down-Liste aus. Weitere Informationen zu dem von Ihnen ausgewählten Bundle-Typ finden Sie unter Bundle-Details. Um die für Pools angebotenen Pakete zu vergleichen, wählen Sie Alle Bundles vergleichen aus.

- Verwenden Sie Ihr eigenes benutzerdefiniertes Paket — Wählen Sie ein Paket aus, das Sie zuvor erstellt haben. Informationen zum Erstellen eines benutzerdefinierten Pakets finden Sie unter Benutzerdefiniertes WorkSpaces Image und Paket für WorkSpaces Personal erstellen.

> **Note**
>
> BYOL ist derzeit für WorkSpaces Pools nicht verfügbar.

- Wählen Sie unter Maximale Sitzungsdauer in Minuten die maximale Zeitspanne aus, für die eine Streaming-Sitzung aktiv bleiben kann. Wenn Benutzer fünf Minuten vor Erreichen dieses Limits noch mit einer Streaming-Instance verbunden sind, werden sie aufgefordert, alle geöffneten Dokumente zu speichern, bevor sie getrennt werden. Nach Ablauf dieser Zeit wird die Instance beendet und durch eine neue Instance ersetzt. Die maximale Sitzungsdauer, die Sie in der WorkSpaces Pools-Konsole festlegen können, beträgt 5760 Minuten (96 Stunden). Die maximale Sitzungsdauer, die Sie mithilfe der WorkSpaces Pools-API und der CLI festlegen können, beträgt 432000 Sekunden (120 Stunden).
- Wählen Sie für Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) die Zeitspanne aus, für die eine Streaming-Sitzung aktiv bleiben kann, nachdem der Benutzer die Verbindung getrennt hat. Wenn Benutzer nach einer Verbindungstrennung oder Netzwerkunterbrechung innerhalb dieses Zeitraums erneut eine Verbindung herstellen möchten, werden sie wieder mit der vorherigen Sitzung verbunden. Andernfalls werden sie mit einer neuen Sitzung mit einer neuen Streaming-Instance verbunden.
- Wenn ein Benutzer die Sitzung beendet, indem er auf der Pools-Symbolleiste auf Sitzung beenden oder Abmelden klickt, gilt das Timeout für die Unterbrechung der Verbindung nicht. Stattdessen wird der Benutzer aufgefordert, alle geöffneten Dokumente zu speichern, und wird dann sofort von der Streaming-Instance getrennt. Die vom Benutzer verwendete Instance wird dann beendet.
- Wählen Sie für Idle disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung bei Leerlauf in Minuten) die Zeitspanne aus, für die Benutzer im Leerlauf (inaktiv) verbleiben können, bevor sie von ihrer Streaming-Sitzung getrennt werden und bevor das Zeitintervall unter Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) beginnt. Benutzer werden benachrichtigt, bevor sie aufgrund von Inaktivität getrennt werden. Wenn sie versuchen, vor Ablauf des unter Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) angegebenen Zeitintervalls wieder eine Verbindung mit der Streaming-Sitzung herzustellen, werden sie mit ihrer vorherigen Sitzung verbunden.

Andernfalls werden sie mit einer neuen Sitzung mit einer neuen Streaming-Instance verbunden. Die Einstellung wird durch den Wert „0“ deaktiviert. Wenn dieser Wert deaktiviert ist, werden Benutzer nicht aufgrund von Inaktivität getrennt.

> **Note**
>
> Benutzer gelten als inaktiv, wenn sie während ihrer Streaming-Sitzung keine Tastatur- oder Mauseingabe mehr machen. Bei Pools, die in eine Domäne eingebunden sind, beginnt der Countdown für das Timeout beim Trennen im Leerlauf erst, wenn sich die Benutzer mit ihrem Active Directory-Domänenkennwort oder mit einer Smartcard anmelden. Datei-Uploads und -Downloads, Audio-Eingabe, Audio-Ausgabe und Pixeländerungen gelten nicht als Benutzeraktivitäten. Wenn Benutzer nach Ablauf des Zeitintervalls unter Idle disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung bei Leerlauf in Minuten) weiterhin inaktiv sind, wird ihre Verbindung getrennt.

- Wählen Sie für Geplante Kapazitätsrichtlinien (optional) die Option Neue geplante Kapazität hinzufügen aus. Geben Sie das Start- und Enddatum sowie die Uhrzeit an, zu der die Mindest- und Höchstanzahl von Instances für Ihren Pool bereitgestellt werden soll, basierend auf der Mindestanzahl erwarteter gleichzeitiger Benutzer.
- Geben Sie für Richtlinien zur manuellen Skalierung (optional) die Skalierungsrichtlinien für Pools an, die verwendet werden sollen, um die Kapazität Ihres Pools zu erhöhen oder zu verringern. Erweitern Sie Richtlinien für manuelle Skalierung, um neue Skalierungsrichtlinien hinzuzufügen.

> **Note**
>
> Die Größe Ihres Pools ist durch die von Ihnen angegebene Mindest- und Höchstkapazität begrenzt.

- Wählen Sie Neue Scale-Out-Richtlinien hinzufügen und geben Sie die Werte für das Hinzufügen bestimmter Instances ein, wenn die angegebene Kapazitätsauslastung unter oder über dem angegebenen Schwellenwert liegt.
- Wählen Sie Neue Skalierungsrichtlinien hinzufügen und geben Sie die Werte für das Entfernen bestimmter Instances ein, wenn die angegebene Kapazitätsauslastung unter oder über dem angegebenen Schwellenwert liegt.

- Geben Sie für Tags den Schlüsselpaarwert an, den Sie verwenden möchten. Ein Schlüssel kann einer allgemeinen Kategorie angehören, wie zum Beispiel "Projekt", "Eigentümer" oder "Umgebung", die über bestimmte zugehörige Werte verfügen.

6. Wählen Sie auf der Seite Verzeichnis auswählen das Verzeichnis aus, das Sie erstellt haben. Um ein Verzeichnis zu erstellen, wählen Sie Verzeichnis erstellen. Weitere Informationen finden Sie unter Verzeichnisse für WorkSpaces Pools verwalten.
7. Wählen Sie Create WorkSpace Pool aus.

Konfiguration des WorkSpaces Thin Client-Zugriffs

Wenn Sie den Webzugriff für WorkSpaces Pools für die Verwendung von WorkSpaces Thin Client konfigurieren, müssen Sie die AWS Befehlszeilenschnittstelle verwenden.

1. Installieren oder aktualisieren Sie die AWS Command Line Interface.
2. Konfigurieren Sie Ihre AWS CLI Einstellungen.
3. Öffne das AWS CLI.
4. Führen Sie den folgenden Befehl aus `WORKSPACES_DIRECTORY_ID` und ersetzen Sie ihn `REGION` mit den entsprechenden Informationen:

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

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. Wenn Sie aufgefordert werden, die Env-Konsole zu erstellen, geben Sie Ihre IDP-Anmelde-URL ein.
Betriebssystem	Windows
Plattformtyp	Windows Server (2012 R2, 2016 oder 2019)
Zwischenablage	Deaktivieren Auf Stack-Ebene AppStream 2.0 konfiguriert
Übertragung von Dateien	Deaktivieren Auf Stack-Ebene AppStream 2.0 konfiguriert
Auf lokalem Gerät drucken	Deaktivieren Auf Stack-Ebene AppStream 2.0 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
Zwischenablage	Deaktivieren
Übertragung von Dateien	Deaktivieren
Auf lokales Gerät drucken	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
- Starten der WorkSpaces Thin Client-Administratorkonsole

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

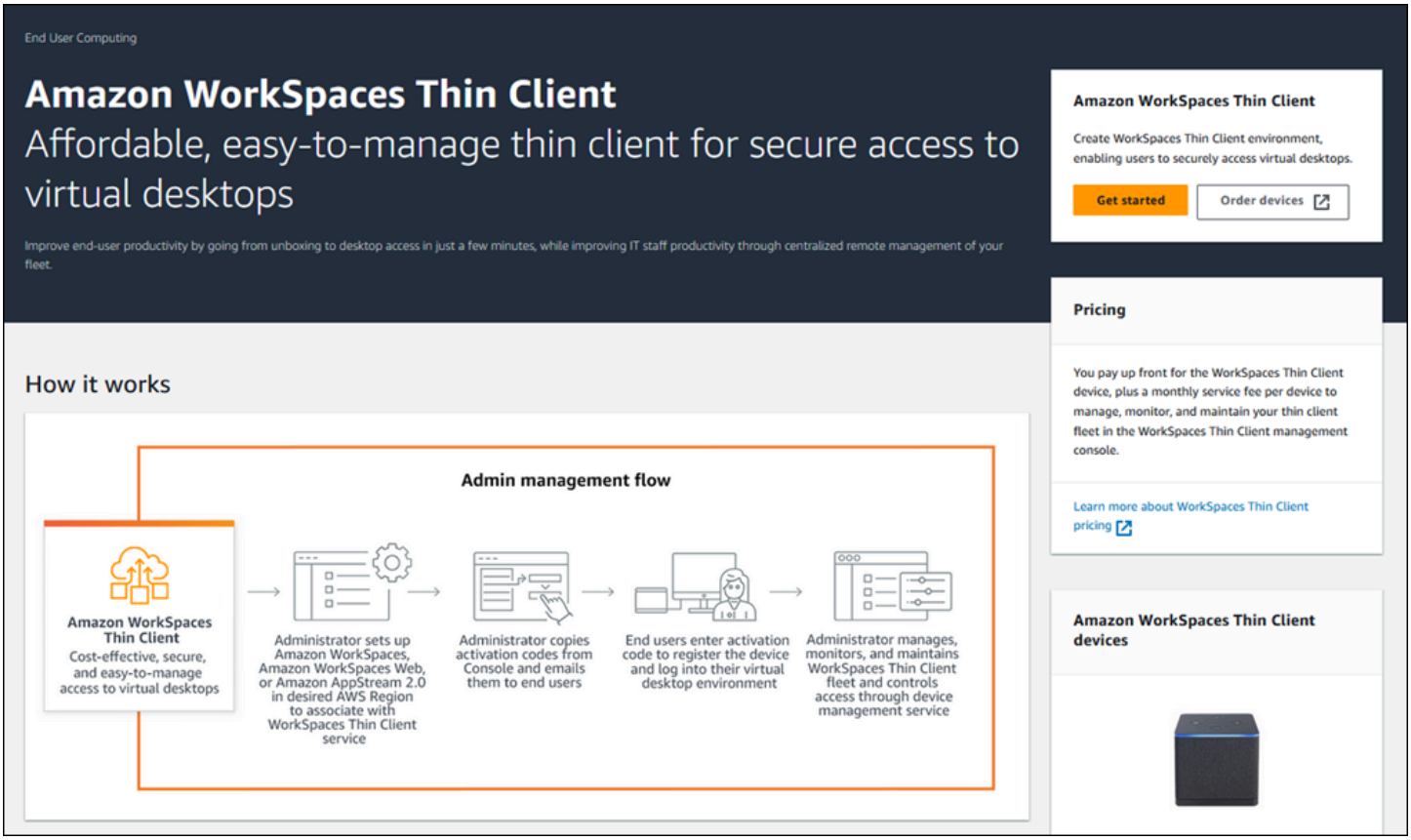
Name der Region	Region	Endpunkt	Link zur Konsole
Europa (Irland)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
Kanada (Zentral)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home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

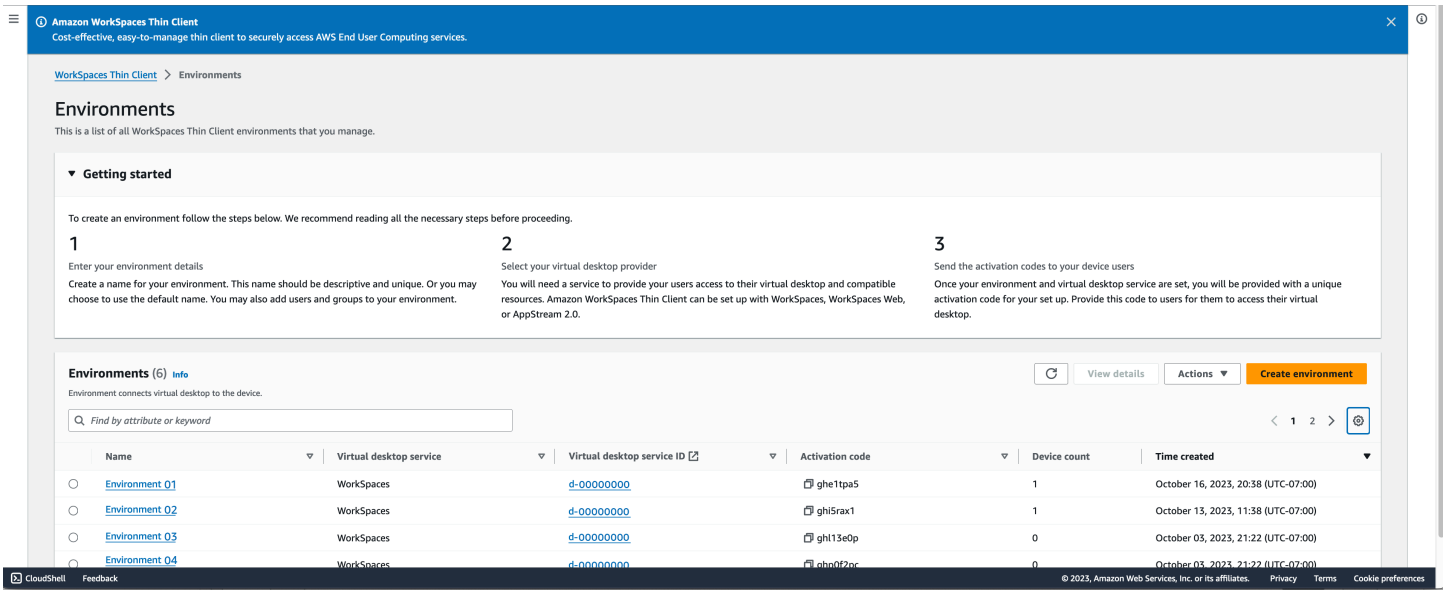
Umgebungen

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

Es gibt eine Reihe von Parametern für Ihre Umgebung, die Sie überprüfen müssen, sowie einige Maßnahmen, die Sie ergreifen können.



Details der Umgebungsliste

Die Parameter für Ihre Umgebung sind zur Überprüfung aufgeführt. In der folgenden Tabelle sind die einzelnen Elemente in der Zusammenfassung und ihre Funktionsweise aufgeführt.

Element	Beschreibung
Name	Die eindeutige Kennung, die dieser Umgebung zugeordnet ist.

Element	Beschreibung
Virtueller Desktop-Dienst	Der virtuelle Desktop-Anbieter, den diese Umgebung verwendet.
ID des virtuellen Desktop-Dienstes	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.
Anzahl der Geräte	Die Anzahl der WorkSpaces Thin Client-Ge räte, die auf diese Umgebung zugreifen.
Erstellungszeit	Datum und Uhrzeit der Erstellung der Umgebung.

Aktionen der Umgebungsliste

Es gibt eine Reihe von Aktionen, die Sie von hier aus ausführen können. Wählen Sie eine dieser Optionen aus, um die entsprechende Aktion auszuführen.

Element	Beschreibung
Suche	Durchsucht alle Umgebungen, die Sie verwalten.
(Aktualisieren)	Aktualisiert die Umgebungsliste.
View details (Details anzeigen)	Zeigt Umgebungsdetails an.
Aktionen	Öffnet eine Dropdownliste, in der Sie eine Umgebung bearbeiten oder löschen können.
Erstellen der -Umgebung	Startet den Prozess der Erstellung einer Umgebung.

Themen

- Details der Umgebung
- Erstellen einer Umgebung
- Bearbeiten einer Umgebung
- Löschen einer Umgebung

Details der Umgebung

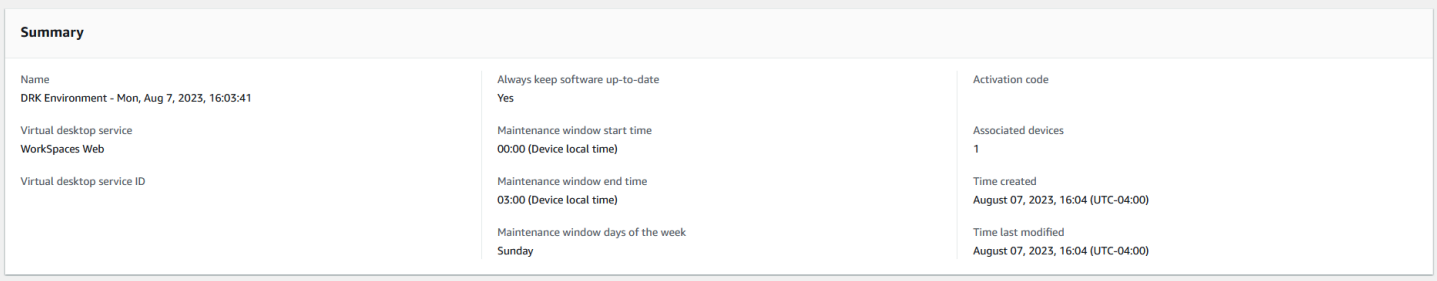
Wenn Sie eine Umgebung auswählen, zeigt die WorkSpaces Thin Client-Konsole die Details für diese Umgebung an, damit Sie sie überprüfen können. In der Konsole werden auch die Details über den Anbieter für virtuelle Desktops angezeigt, den diese Umgebung verwendet.

Themen

- Übersicht
- Details zur virtuellen Desktop-Umgebung

Übersicht

Der Abschnitt Zusammenfassung bietet einen allgemeinen Überblick über die wichtigsten Funktionen der WorkSpaces Thin Client-Umgebung. In der folgenden Tabelle sind die einzelnen Elemente in der Zusammenfassung und ihre Funktionsweise aufgeführt.



Element	Beschreibung
Name	Die eindeutige Kennung, die dieser Umgebung zugeordnet ist.
Virtueller Desktop-Dienst	Der virtuelle Desktop-Anbieter, den diese Umgebung verwendet.

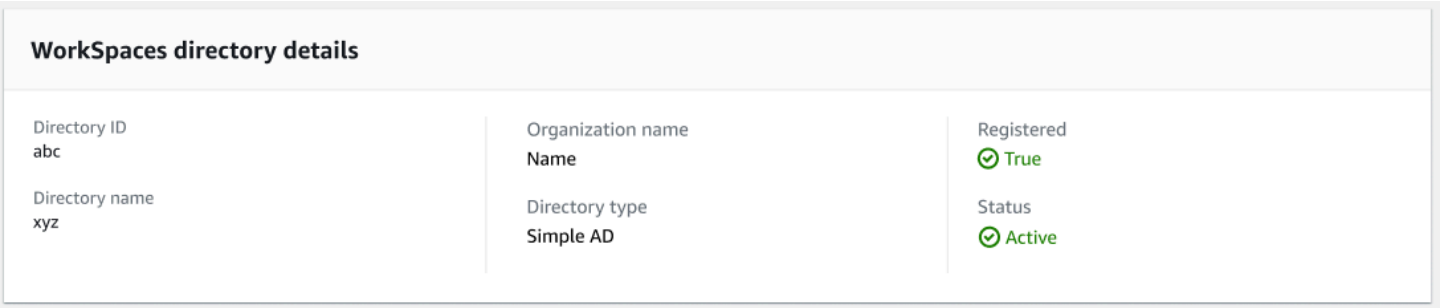
Element	Beschreibung
Name des virtuellen Desktop-Dienstes	Die eindeutige Kennung, die der Virtual Desktop Service Provider dieser Umgebung zuweist.
Aktivierungscode	Dieser Code wird von Endbenutzern für den Zugriff auf die virtuelle Desktop-Umgebung verwendet.
Bewahren Sie die Software immer auf up-to-date	Diese Einstellung ermöglicht automatische Softwareupdates.
Startzeit des Wartungsfensters	Die wöchentliche Uhrzeit, zu der automatische Softwareupdates beginnen.
Endzeit des Wartungsfensters	Die wöchentliche Uhrzeit, zu der automatische Softwareupdates abgeschlossen werden.
Wartungsfenster: Wochentage	Die Tage, an denen automatische Softwareupdates 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

WorkSpaces Thin Client-Umgebungen werden auf einer virtuellen Desktop-Oberfläche ausgeführt. Jede Schnittstelle hat einen anderen Satz von Parametern, die die dedizierte Umgebung steuern.

Details zum WorkSpaces Amazon-Verzeichnis

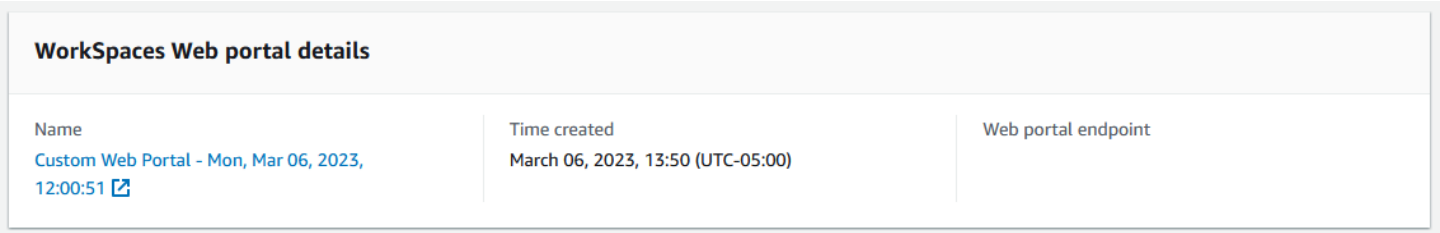
WorkSpaces Thin Client-Umgebungen, die auf Amazon ausgeführt werden, WorkSpaces verwenden Verzeichnisse, um ihre virtuellen Desktops zu erstellen und auszuführen. In der folgenden Tabelle sind die einzelnen Elemente detailliert und ihre Funktionsweise aufgeführt.



Element	Beschreibung
Verzeichnis-ID	Das mit dieser Umgebung verknüpfte WorkSpaces Amazon-Verzeichnis.
Name des Verzeichnisses	Die eindeutige Kennung, die mit diesem WorkSpaces Amazon-Verzeichnis verknüpft ist.
Name der Organisation	Der Name der Organisation, die das WorkSpaces Amazon-Verzeichnis kontrolliert.
Typ des Verzeichnisses	Das Format des WorkSpaces Amazon-Ve rzeichnisses.
Status "Registered"	Ob dieses WorkSpaces Amazon-Verzeichnis registriert ist.
Status	Ob dieses WorkSpaces Amazon-Verzeichnis aktiv ist.

Einzelheiten zum Amazon WorkSpaces Secure Browser-Portal

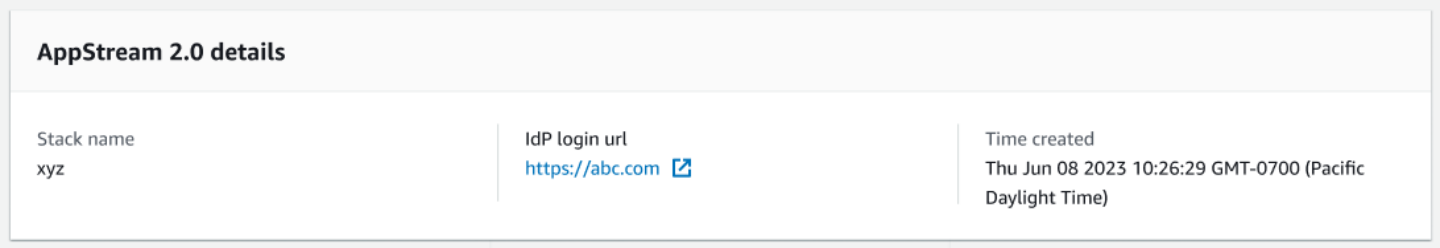
WorkSpaces Thin Client-Umgebungen, die auf Amazon WorkSpaces Secure Browser ausgeführt werden, verwenden Webportale, um ihre virtuellen Desktops zu erstellen und auszuführen. In der folgenden Tabelle sind die einzelnen Elemente detailliert und ihre Funktionsweise aufgeführt.



Element	Beschreibung
Name	Die eindeutige Kennung, die diesem WorkSpaces Secure Browser-Portal zugeordne t ist.
Erstellungszeit	Datum und Uhrzeit der Erstellung dieses WorkSpaces Secure Browser-Portals.
Webportal-Endpunkt	Die URL, die für den Zugriff auf Ihre virtuelle Desktop-Umgebung verwendet wurde.

AppStream 2.0-Einzelheiten

WorkSpaces Thin Client-Umgebungen werden auf AppStream 2.0-Informationsstapeln ausgeführt, um ihre virtuellen Desktops zu erstellen und auszuführen. In der folgenden Tabelle sind die einzelnen Elemente detailliert und ihre Funktionsweise aufgeführt.



Element	Beschreibung
Stack name	Der eindeutige Bezeichner, der 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
- Schritt 2: Auswählen Ihres virtuellen Desktop-Anbieters
- Schritt 3: Senden des Aktivierungscodes an die Gerätebenutzer

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 Service, 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.
   - 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.

> **Important**
>
> 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.
   - 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.
   - 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.

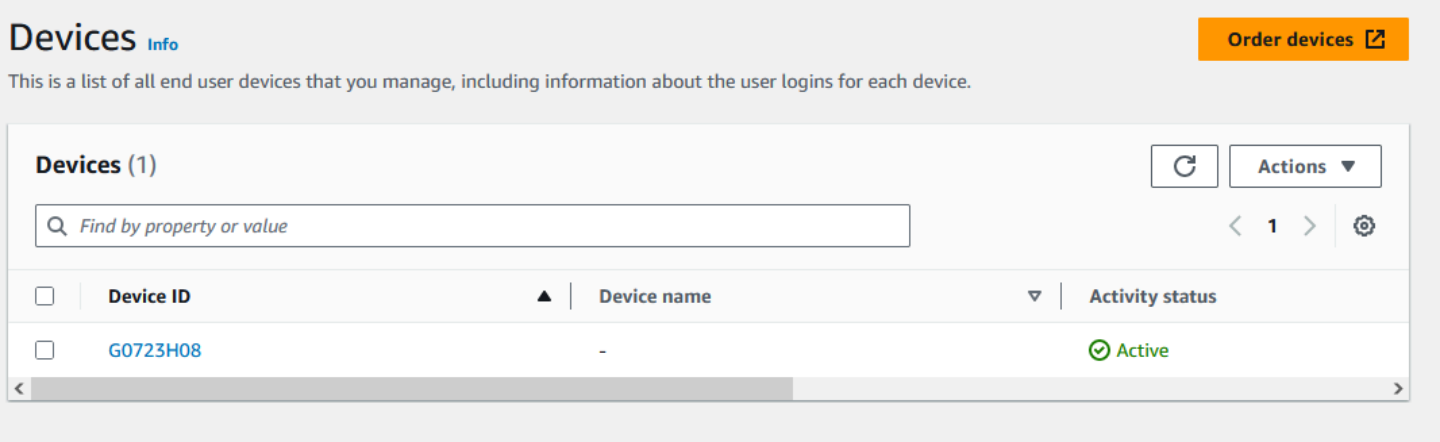
Geräte

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

Es gibt eine Reihe von Parametern für jedes Gerät in Ihrem Netzwerk, die Sie überprüfen können, sowie einige Maßnahmen, die Sie ergreifen können.



Gerätelistendetails

Die Parameter für Ihr Gerät werden zur Überprüfung aufgeführt. In der folgenden Tabelle sind die einzelnen Elemente in der Zusammenfassung und ihre Funktionsweise aufgeführt.

Element	Beschreibung
Geräte-ID	Die einem einzelnen Gerät zugewiesene Identifikationsnummer.
Gerätename	(optional) Der eindeutige Name, den Sie einem Gerät geben.
Status der Aktivität	Der aktuelle Status eines Geräts. Es gibt zwei Statuszustände:

Element	Beschreibung
	• Aktiv — In den letzten sieben Tagen mindestens einmal mit einem Netzwerk verbunden. • Inaktiv — In den letzten sieben Tagen wurde keine Verbindung zu einem Netzwerk hergestellt.
Registrierungsstatus	Bestätigung, dass ein Gerät eingerichtet wurde, mit diesem AWS-Konto verknüpft 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.

Element	Beschreibung
Softwarekonformität	Der Konformitätsstatus der Gerätesoftware. Es gibt zwei Statuszustände: • Konform • Nicht konform

Gerätelistenaktionen

Es gibt eine Reihe von Aktionen, die Sie von hier aus ausführen können. Wählen Sie eine dieser Optionen aus, um die entsprechende Aktion auszuführen.

Element	Beschreibung
Suche	Durchsucht alle Geräte, die Sie verwalten.
(Aktualisieren)	Aktualisiert die Geräteliste.
View details (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
- Bearbeiten eines Gerätenamens
- Zurücksetzen und Abmelden des Geräts

- Archivieren eines Geräts
- Löschen eines Geräts
- Exportieren der Gerätedetails

Gerätedetails

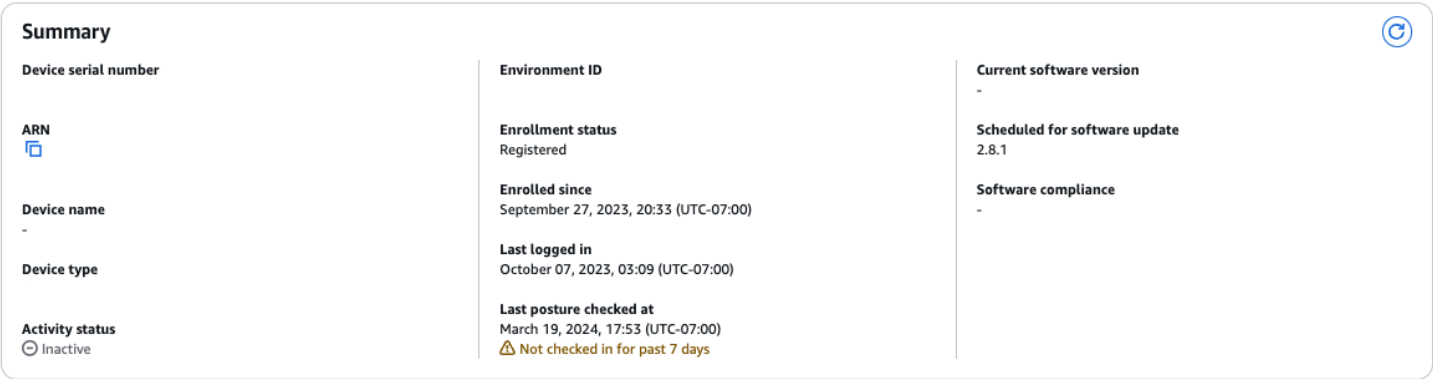
Wenn Sie ein Gerät auswählen, zeigt die WorkSpaces Thin Client-Konsole die Details für dieses Gerät an, damit Sie sie überprüfen können. Die Konsole zeigt auch die Details zum Netzwerktyp des Geräts und zu den angeschlossenen Peripheriegeräten an.

Themen

- Übersicht
- Einstellungen des Geräts
- Benutzeraktivität

Übersicht

Der Abschnitt Zusammenfassung bietet einen allgemeinen Überblick über die wichtigsten Funktionen des WorkSpaces Thin Client-Geräts. In der folgenden Tabelle sind die einzelnen Elemente in der Zusammenfassung und ihre Funktionsweise aufgeführt.



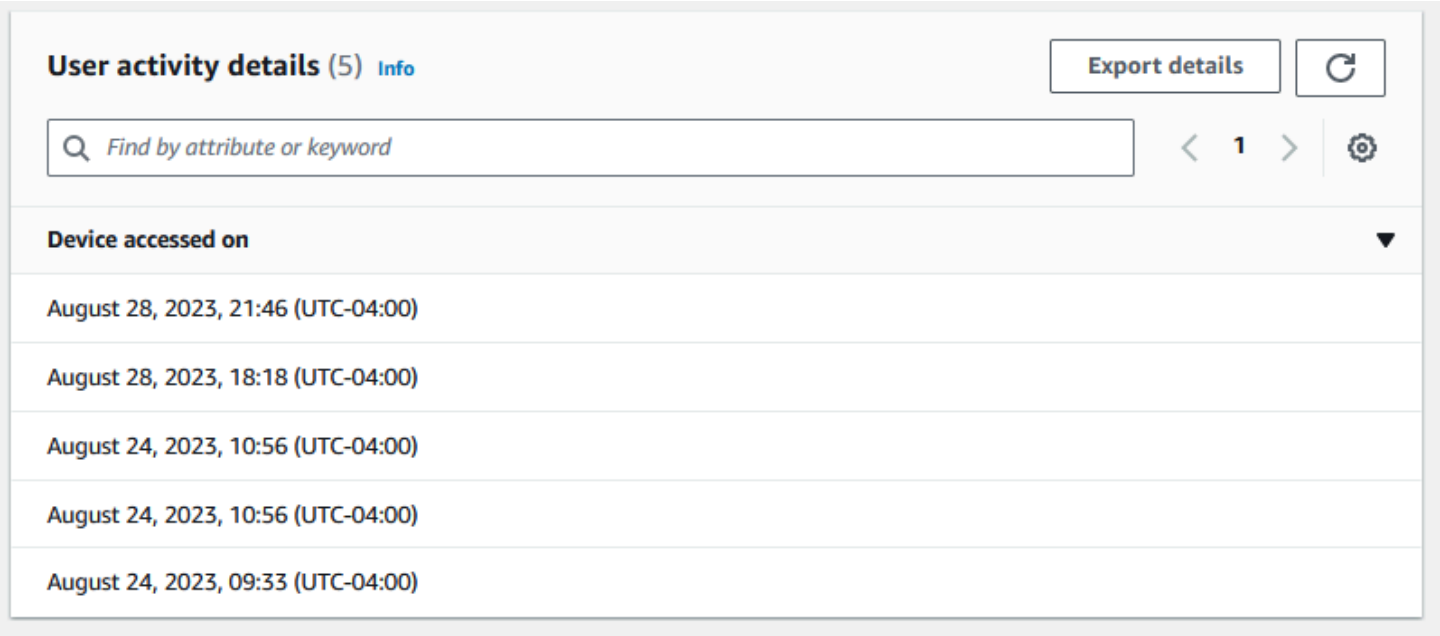
Element	Beschreibung
Seriennummer des Geräts	Die einem einzelnen Gerät zugewiesene Identifikationsnummer.

Element	Beschreibung
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.
Status der Aktivität	Der aktuelle Status dieses Geräts. Die beiden Statuszustände sind: • Aktiv • Inaktiv
Umgebungs-ID	Die Identifikationsnummer der Umgebung, die das Gerät verwendet.

Element	Beschreibung
Registrierungsstatus	Bestätigung, dass ein Gerät eingerichtet wurde, mit diesem AWS-Konto verknüpft 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.
Eingeschrieben seit	Das Datum, an dem das Gerät aktiviert wurde.
Zuletzt eingeloggt	Datum und Uhrzeit der letzten Anmeldung.
Letzte Überprüfung der Körperhaltung am	Datum und Uhrzeit des letzten Geräte-Check-ins.
Aktuelle Softwareversion	Die Softwareversion, die dieses Gerät derzeit verwendet.
Das Softwareupdate ist geplant	Die geplante Softwareversion auf dem Gerät.

Element	Beschreibung
Softwarekonformität	Bestätigung, dass das Softwareset gültig ist. Es gibt zwei Statusstatus: • Konform • Nicht konform

Benutzerprotokoll



Element	Beschreibung
Letzter Gerätezugriff	Datum und Uhrzeit der letzten Verwendung dieses Geräts.

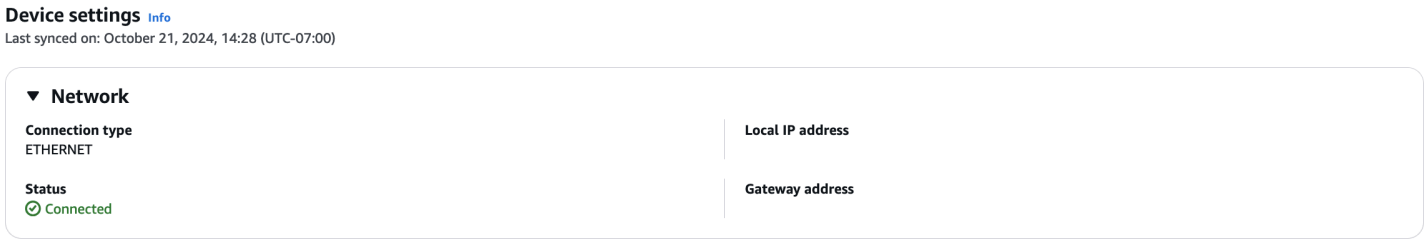
Einstellungen des Geräts

Die Parameter für Ihr Gerät sind zur Überprüfung aufgeführt. In der folgenden Tabelle sind die einzelnen Elemente und ihre Funktionsweise aufgeführt.

> **Note**
>
> Die Informationen zu den Geräteeinstellungen werden nur aktualisiert, wenn das Gerät online ist. Wenn das Gerät offline ist, sind einige Informationen möglicherweise veraltet.

Überschrift und Netzwerk

WorkSpaces Die Thin Client-Gerätedetails bieten einen Überblick über die Netzwerkverbindungen des Geräts. In der folgenden Tabelle sind die einzelnen Elemente und ihre Funktionsweise aufgeführt.

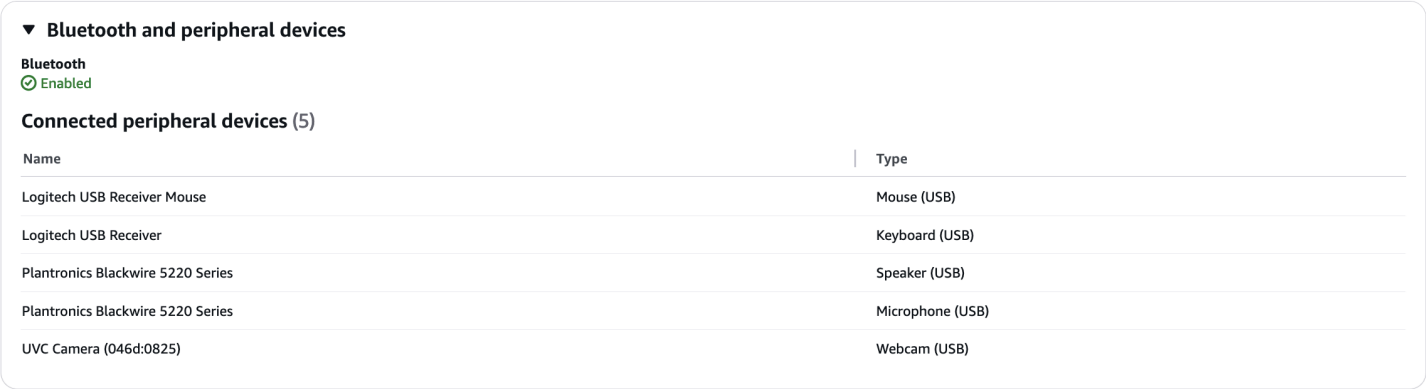


Element	Beschreibung
Zuletzt synchronisiert am	Datum und Uhrzeit der letzten Geräteein stellungen werden mit der Konsole synchroni siert.
Verbindungstyp	Die Art der Netzwerkverbindung, die vom Gerät verwendet wird. Der Verbindungstyp kann entweder Ethernet oder WLAN sein.
Status	Der Status des Netzwerks. Wenn das Gerät derzeit verbunden ist oder innerhalb der letzten 20 Minuten eine Verbindung hergestellt wurde, wird der Status als „verbunden“ angezeigt. Wenn das Netzwerk länger als 20 Minuten unterbrochen wurde, ändert sich der Status und zeigt die Zeit an, die vergangen ist, seit das Gerät zuletzt mit dem Internet verbunden war, z. B. „Letzte Verbindung vor 20 Minuten“.

Element	Beschreibung
Lokale IP-Adresse	Die lokale IP-Adresse des verbundenen Netzwerks.
Gateway-Adresse	Die Gateway-Adresse des verbundenen Netzwerks.

Bluetooth und Peripheriegeräte

WorkSpaces Die Thin Client-Gerätedetails enthalten eine Liste aller angeschlossenen Peripheriegeräte, die mit einem Gerät verbunden sind. In der folgenden Tabelle sind die einzelnen Elemente und ihre Funktionsweise aufgeführt.



Element	Beschreibung
Bluetooth	Der Bluetooth-Status des Geräts. Die beiden Statuszustände sind: • Enabled • Disabled
Angeschlossene Peripheriegeräte	Die Liste der Namen der angeschlossenen Peripheriegeräte, z. B. der Logitech-Maus, und der Typ der angeschlossenen Peripheriegeräte, z. B. Maus (USB).

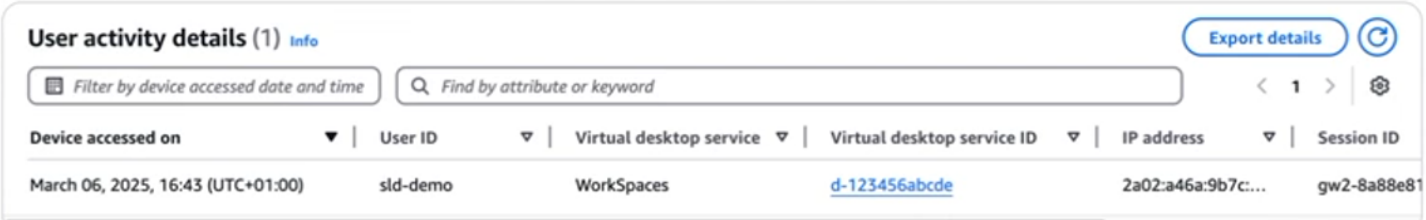
Stromversorgung und Ruhemodus

Jedes WorkSpaces Thin Client-Gerät verfügt über einen Energiesparmodus. In der folgenden Tabelle ist der Status dieses Modus aufgeführt.

Element	Beschreibung
Schalten Sie das Display danach aus	Der Zeitraum der Inaktivität, nach dem das Gerät sein Display ausschaltet.

Benutzeraktivität

Auf dieser Registerkarte wird das Protokoll der Einrichtungs- und Nutzungsinformationen eines bestimmten Geräts angezeigt. In der folgenden Tabelle sind alle Elemente dieses Protokolls aufgeführt.



Element	Beschreibung
Gerät, auf das zugegriffen wurde	Datum und Uhrzeit der Aktivierung des Geräts.
Benutzer-ID	Die Identifikationsnummer des Benutzers, der auf das Gerät zugreift.
Virtueller Desktop-Dienst	Der virtuelle Desktop-Dienst, den das Gerät verwendet.
ID des virtuellen Desktop-Dienstes	Die dem Benutzer zugeordnete ID-Nummer des virtuellen Desktop-Dienstes.

Element	Beschreibung
IP-Adresse	Die Identifikationsnummer der IP, die auf das Gerät zugreift.
Ereignistyp	Einzelheiten darüber, wie das Gerät verwendet wird.

> **Note**
>
> Mit Ausnahme von „ WorkSpaces Persönlich“ werden VDIs nur Ereignisse angezeigt, die von der Anmeldung ausgelöst wurden.

Sie können die Suchleiste über der Tabelle verwenden, um bestimmte Informationen in der Tabelle zu finden. Sie können die Tabellenergebnisse auch nach Datum und Uhrzeit filtern.

Sie können die Tabelle in eine CSV-Datei exportieren, indem Sie auf die Schaltfläche Details exportieren klicken.

Bearbeiten eines Gerätenamens

1. Wählen Sie das Gerät aus, das Sie bearbeiten möchten. Sie können entweder die Dropdownliste 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.

Exportieren der Gerätedetails

1. Wählen Sie das gewünschten Gerät aus, von dem aus Sie exportieren 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 Gerätedetails exportieren aus. Die Details für das ausgewählte Gerät werden in einem Tabellenformat 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
- Aktualisieren der Gerätesoftware
- WorkSpaces Thin Client-Softwareversionen

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
2.16.1	7-3-2025	• Die kritischen Sicherheitsprobleme CVE-2025-6554 von Chromium wurden behoben.
2.16.0	6-27-2025	• Benachrichtigungen für Netzwerklatenz hinzugefügt. • Es wurde die Möglichkeit hinzugefügt, Daten wiederherzustellen, wenn

Softwaresatz	Datum der Veröffentlichung	Änderungen
		der zweite Monitor während einer Sitzung dunkel wird. • Es wurde ein Problem behoben, bei dem Monitore einen weißen Bildschir m anzeigten oder sich nicht auto verlängerten, nachdem das Gerät aus dem Ruhemodus zurückgek ehrt war.
2.15.0	19.06.2025	• Unterstützung für lateiname rikanische, spanische und internationale englische Tastaturen hinzugefügt. • Endbenutzer erhalten Benachrichtigungen, wenn das Gerät über einen längeren Zeitraum keine Tastatur- oder Mausaktivität erkennt.
2.14.1	6-09-2025	• Behebung der kritische n Sicherheitsproblem e CVE-2025-5419 von Chromium.

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.13.0	3-31-2025	• Endverbraucher sehen die Umfrage zum Feedback zur Produktzufriedenheit als Benachrichtigung. • Integriert die Unterstützung von Funktionen in der Vorabversion für den FIDO2 Authentifizierungsablauf. Weitere Informationen finden Sie FIDO2 vor der Sitzung. • Das Gerät geht nicht in den Ruhemodus, wenn während der Sitzung gespielt audio/video wird. • Endbenutzer erhalten Benachrichtigungen, wenn der Monitor angeschlossen oder getrennt wird. • Das Gerät sammelt Diagnoseinformationen vom Betriebssystem, um den Service zu verbessern. • Behebt ein Problem, bei dem in den Einstellungen für das Installationsdatum der Software ein falsches Datum angezeigt wurde.
2.14.0	29.04.2025	• Verbesserungen der Benutzerfreundlichkeit und Bugfixes.

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.13.0	3-31-2025	• Endverbraucher sehen die Umfrage zum Feedback zur Produktzufriedenheit als Benachrichtigung. • Integriert die Unterstützung von Funktionen in der Vorabversion für den FIDO2 Authentifizierungsablauf. Weitere Informationen finden Sie FIDO2 vor der Sitzung. • Das Gerät geht nicht in den Ruhemodus, wenn während der Sitzung gespielt audio/video wird. • Endbenutzer erhalten Benachrichtigungen, wenn der Monitor angeschlossen oder getrennt wird. • Das Gerät sammelt Diagnoseinformationen vom Betriebssystem, um den Service zu verbessern. • Behebt ein Problem, bei dem in den Einstellungen für das Installationsdatum der Software ein falsches Datum angezeigt wurde.

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.12.0	1-30-2025	• Behebt ein Problem, bei dem der Endbenutzer beim Drücken der Zurück-Ta ste mit der Maus von der Sitzung abgemeldet wurde.
2.11.2	24-1-2025	• Behebt ein Problem, bei dem der Ton bei Anrufen mit Mausbewegungen zwischen Monitoren knisterte.
2.11.1	27.12.2024	• Behebt das Problem mit der automatischen Erweiterung von zwei Monitoren. • Kleinere Verbesserungen am VoiceView Etikett.
2.11.0	19.12.2024	• WorkSpaces Thin Client unterstützt jetzt Magnifier VoiceView .
2.10.0	22.11.2024	• Endbenutzer können eine Tastenkombination verwenden, um die Gerätesymbolleiste zu reduzieren.

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.9.0	28.10.2024	• Administratoren können jetzt die Geräteeinstellungen ihrer Endbenutzer in der AWS Konsole auf der Seite mit den Gerätedetails eines bestimmten Geräts einsehen. • WorkSpaces Thin Client unterstützt jetzt Monitore mit 2K-Auflösung für Einzelbildschirme. • Endbenutzer können Benachrichtigungen zur Netzwerkdiagnose auf ihren WorkSpaces Thin Client-Geräten sehen. • Endbenutzer können nun wählen, ob sie die Gerätesymbolleiste nach Belieben links oder rechts platzieren möchten. • Es wurde ein Problem behoben, bei dem das Gerät im Standbymodus oder im Leerlauf keine Softwareupdates installierte.
2.8.1	26.09.2024	• Es wurde ein kritisches Problem behoben, bei dem der zweite Monitor nicht eingeschaltet werden konnte, nachdem das Gerät aus dem Ruhemodus aufgewacht war.

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.8.0	09-06-2024	• Thin Client unterstützt Monitore mit 4K-Auflösung. • Benutzer können eine Verbindung zur VDI-Sitzung herstellen, auch wenn die WorkSpaces Thin Client-Geräteverwaltungsdienste vorübergehend nicht verfügbar sind. • Es wurde das Problem behoben, bei dem im Abschnitt „Benutzeraktivitätsdetails“ in der AWS Konsole doppelte Einträge angezeigt wurden. • Endbenutzer können die PrintScreen Option beim Streamen WorkSpaces auf dem WorkSpaces Thin Client verwenden.
2.7.1	27.08.2024	• Zero-Day-Korrekturen für die kritischen Sicherheitsprobleme CVE-2024-7971 und CVE-2024-7965 von Chromium.

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.7.0	29.07.2024	• Verbesserungen der Leistung des zweiten Monitors. • Es wurde ein Problem behoben, bei dem die Sprache der Werkzeugleiste beim Ändern der Gerätesprache nicht beeinflusst wurde. • Das Gerät sammelt jetzt Diagnoseinformationen für Serviceverbesserungen.
2.6.0	07-09-2024	• Benutzer können eingehende Softwareupdates zurückstellen, sodass sie ihre Arbeit ohne Unterbrechung beenden können. • Mithilfe der Geräteeinstellungen können Benutzer gespeicherte WiFi Netzwerke vergessen. • Verbesserungen der Leistung von audio/video Anrufen in der Sitzung. • Einige Benutzereinstellungen für die VDI-Sitzungen bleiben auch nach dem Neustart des Geräts erhalten.

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. • Die Home-Schaltfläche auf der Gerätesymbolleiste wurde in Anmelden umbenannt. • Verbesserungen der Leistung von audio/video Anrufen 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.

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.4.1	15.05.2024	• Zero-Day-Korrekturen für die kritischen Sicherheitsprobleme CVE-2024-4671 und CVE-2024-4761 von Chromium. • Es wurde das Problem behoben, das es ermöglichte, auf der WorkSpaces 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 Verwendung von Google Workspace als IDP für 2.0-Sitzung verhindert wurde. AppStream • 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. • Endbenutzer können jetzt festlegen, wie lange es dauert, bis das Gerät bei Inaktivität in den Ruhemodus wechselt. • Das Problem, dass die URL „about:blank“ auf dem zweiten Display angezeigt wurde, wurde behoben. • Das Problem, das zu einem weißen Bildschirm führte, wenn die erweiterte Anzeige geschlossen wurde, wurde behoben. • 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 (Vereinigtes Königreich), Französisch, Deutsch, Italienisch und Spanisch hinzugefügt.
2.1.2	26.01.2024	• Zero-Day-Fix für das kritische Sicherheitsproblem CVE-2024-0519 von Chromium. • Verbesserung der Latenz für Endbenutzer im Zusammenhang mit der Sperrfunktion. • Interne, mit Geräten verbundene Endpunkte 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.

- Sie können die Tags für ein Gerät in einer Umgebung so konfigurieren, dass sie bei der Registrierung eines Geräts automatisch angewendet werden.

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 Tags für eine bestehende Umgebung mithilfe der Konsole zu verwalten

1. Öffnen Sie die WorkSpaces Thin Client-Konsole.
2. Wählen Sie die Umgebung aus, um die zugehörige Detailseite zu öffnen
3. Wählen Sie Edit (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 Tags für ein vorhandenes Gerät mithilfe der Konsole zu verwalten

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 Tags für ein neues Gerät mit der Konsole zu verwalten

1. Öffnen Sie die WorkSpaces Thin Client-Konsole.
2. Wählen Sie die Umgebung aus, um die zugehörige Detailseite zu öffnen.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Führen Sie im Abschnitt Tags zur Geräteerstellung 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.

Wenn ein Gerät erstellt wurde, wird es in der Umgebung registriert und die Tags für die Geräteerstellung werden angewendet. Dies geschieht nur bei der Registrierung neuer Geräte. Zusätzlich wird das `aws:thinclient:environment-id` System-Tag mit der als Wert verwendeten Umgebungs-ID angewendet.

Um Tags für ein Softwareupdate mithilfe der Konsole zu verwalten

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 im Amazon WorkSpaces Thin Client

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon WorkSpaces Thin Client gelten, finden Sie unter AWS Services in Scope by Compliance Program AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. 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 gemeinsamen Verantwortung bei der Verwendung von WorkSpaces Thin Client anwenden können. In den folgenden Themen erfahren Sie, wie Sie WorkSpaces Thin Client konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie können auch lernen, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer WorkSpaces Thin Client-Ressourcen unterstützen.

Themen

- Datenschutz im Amazon WorkSpaces Thin Client
- Identitäts- und Zugriffsmanagement für Amazon WorkSpaces Thin Client
- Resilienz im Amazon WorkSpaces Thin Client
- Schwachstellenanalyse und -management im Amazon WorkSpaces Thin Client

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 Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- 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 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 dabei die Konsole, die API oder AWS-Services verwenden. AWS CLI AWS SDKs 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 Benutzer den Dienst nutzen. Wir verarbeiten diese Informationen gemäß der AWS Datenschutzerklärung.

Themen

- Datenverschlüsselung
- Datenverschlüsselung im Ruhezustand für Amazon WorkSpaces Thin Client
- Verschlüsselung während der Übertragung
- Schlüsselverwaltung
- Internet, Arbeit, Verkehr, Datenschutz

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 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 über die Gerätesymbolleiste ihren Bildschirm sperren, das Gerät neu starten oder herunterfahren. 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
  - Einrichtung und Pflege von IAM-Richtlinien
  - 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)
Environment name WorkSpaces Name der Thin Client-Umgebung	Aktiviert	Aktiviert
Gerätename WorkSpaces Name des Thin Client-Geräts	Aktiviert	Aktiviert
Einstellungen des Geräts WorkSpaces Einstellungen für Thin Client-Geräte	Aktiviert	Aktiviert

Datentyp	AWS-eigene Schlüssel verschlüsselung	Vom Kunden verwaltete Schlüsselverschlüsselung (optional)
Tags zur Geräteerstellung WorkSpaces Tags zur Geräteerstellung in der Thin-Client-Umgebung	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 AWS KMS

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

Amazon WorkSpaces Thin Client erfordert die Schlüsselrichtlinie, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Vorgänge zu verwenden:

- Senden Sie `GenerateDataKey`Anfragen an AWS KMS, um die Daten zu verschlüsseln.
- Senden Sie `Decrypt`Anfragen an AWS KMS, um die verschlüsselten Daten zu entschlüsseln.

Sie können den Zugriff des Dienstes auf den vom Kunden verwalteten Schlüssel jederzeit entfernen. 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 WorkSpaces Thin Client nicht zugreifen kann, gibt der Vorgang einen

`AccessDeniedException` Fehler zurück. Außerdem 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.

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

```
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

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.

Das Folgende ist der Environment-Verschlüsselungskontext:

```
"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.

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`,,`GenerateDataKey`, zur Überwachung von KMS-Vorgängen`Decrypt`, 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": "1.09",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

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

GenerateDataKey

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

Das folgende Beispielereignis zeichnet den Vorgang `GenerateDataKey` auf:

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-04-08T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
```

```
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

GenerateDataKey (by service)

Wenn Amazon WorkSpaces Thin Client die gespeicherten `GenerateDataKey` Geräteinformationen verwendet, wird der `GenerateDataKey` Vorgang zur Verschlüsselung der Daten verwendet.

Der `GenerateDataKey` Vorgang ist in der KMS-Schlüsselrichtlinienerklärung mit der Sid „Amazon WorkSpaces Thin Client Service zum Verschlüsseln und Entschlüsseln von Daten zulassen“ zulässig.

Das folgende Beispielereignis zeichnet den Vorgang auf GenerateDataKey :

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

```
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

Decrypt

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

Das folgende Beispielereignis zeichnet den Vorgang `Decrypt` auf:


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
```

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

Decrypt (by service)

Wenn das WorkSpaces Thin Client-Gerät auf Umgebungs- oder Geräteinformationen zugreift, wird der `Decrypt` Vorgang zur Entschlüsselung der Daten verwendet. Der `Decrypt` Vorgang ist in der KMS-Schlüsselrichtlinienerklärung mit der Sid „Amazon WorkSpaces Thin Client Service zum Verschlüsseln und Entschlüsseln von Daten zulassen“ zulässig.

Das folgende Beispielereignis zeichnet den `Decrypt` Vorgang auf, autorisiert durch: `Grant`

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
```

```
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```


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 finden Sie unter Bewährte Sicherheitsmethoden von AWS Key Management Service im Entwicklerhandbuch für AWS Key Management Service.

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.

Identitäts- und Zugriffsmanagement für Amazon WorkSpaces Thin Client

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um WorkSpaces Thin Client-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert Amazon WorkSpaces Thin Client mit IAM
- Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client
- AWS verwaltete Richtlinien für Amazon WorkSpaces Thin Client
- Fehlerbehebung bei Identität und Zugriff auf Amazon WorkSpaces Thin Client

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie im WorkSpaces Thin Client ausführen.

Dienstbenutzer — Wenn Sie den WorkSpaces Thin Client-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr WorkSpaces Thin Client-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie im WorkSpaces Thin Client nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Identität und Zugriff auf Amazon WorkSpaces Thin Client.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die WorkSpaces Thin Client-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf WorkSpaces Thin Client. Es ist Ihre Aufgabe, zu bestimmen, auf welche WorkSpaces Thin Client-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit WorkSpaces Thin Client verwenden kann, finden Sie unterSo funktioniert Amazon WorkSpaces Thin Client mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf WorkSpaces Thin Client schreiben 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

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

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

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, 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 AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, 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. Verwenden Sie diese nur, 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

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf 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 Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten 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 innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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 Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. 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 auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst 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.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 AWS CLI, der 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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 System zuordnen können AWS-Konto.

Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete 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.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) 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 darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon WorkSpaces Thin Client mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf WorkSpaces Thin Client verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen mit WorkSpaces Thin Client verwendet werden können.

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

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

Einen allgemeinen Überblick darüber, wie WorkSpaces Thin Client und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für Thin Client WorkSpaces

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 Thin Client WorkSpaces

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

Ressourcenbasierte Richtlinien innerhalb von Thin Client WorkSpaces

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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. 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 unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für WorkSpaces Thin Client

Unterstützt Richtlinienaktionen: Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. 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 Authorization Reference.

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

```
thinclient
```

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

```
"Action": [
      "thinclient:action1",
      "thinclient: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 mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 deren ARNs Eigenschaften finden Sie unter Von Amazon WorkSpaces Thin Client definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource 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

Bedingungsschlüssel für Richtlinien für WorkSpaces Thin Client

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der WorkSpaces Thin Client-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon WorkSpaces Thin Client in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen 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 im Thin Client WorkSpaces

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Thin Client WorkSpaces

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. 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 Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit WorkSpaces Thin Client verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. 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 von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, 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 auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst 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 kann die WorkSpaces Thin Client-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn WorkSpaces Thin Client Sie dazu anleitet.

Dienstbezogene Rollen für WorkSpaces Thin Client

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. 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

Standardmäßig sind Benutzer und Rollen nicht berechtigt, WorkSpaces Thin Client-Ressourcen zu erstellen oder zu ändern. 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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den vom WorkSpaces Thin Client definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Thin Client in der Service Authorization Reference.

Themen

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

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:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads

Berechtigungen zu 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 speziell auf Ihre Anwendungsfälle zugeschnitten 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. 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 mit 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 System 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 Sicherer API-Zugriff mit MFA 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 Thin Client-Konsole WorkSpaces

Um auf die Amazon WorkSpaces Thin Client-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den WorkSpaces Thin Client-Ressourcen in Ihrem aufzulisten und einzusehen 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.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Gewähren Sie Thin Client nur Lesezugriff WorkSpaces

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 beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder im Programm mithilfe der AWS-CLI oder AWS-API.

JSON

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

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

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 beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Gewähren Sie vollen Zugriff auf den Thin Client WorkSpaces

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen können, die WorkSpaces Thin Client-IAM-Benutzern vollen Zugriff gewährt. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen aller WorkSpaces Thin Client-Aktionen auf der Konsole oder im Programm mithilfe der AWS-CLI oder AWS-API.

JSON

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

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

AWS verwaltete Richtlinien für Amazon WorkSpaces Thin Client

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientReadOnlyAccess

Sie können die `AmazonWorkSpacesThinClientReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt volle Zugriffsberechtigungen für den WorkSpaces Thin Client-Dienst und seine Abhängigkeiten. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie AmazonWorkSpacesThinClientReadOnlyAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `thinclient`(WorkSpaces Thin Client) — Ermöglicht den schreibgeschützten Zugriff auf alle WorkSpaces Thin Client-Aktionen.
- `workspaces`(WorkSpaces) — Erlaubt Berechtigungen zur Beschreibung von WorkSpaces Verzeichnissen und Verbindungsaliasnamen. Dies wird verwendet, um zu überprüfen, ob Ihre WorkSpaces Ressourcen mit WorkSpaces Thin Client kompatibel sind. Es wird auch verwendet, um diese Ressourcen in der WorkSpaces Thin AWS Client-Konsole anzuzeigen.
- `workspaces-web`(WorkSpaces Secure Browser) — Ermöglicht Berechtigungen zur Beschreibung von WorkSpaces Secure Browser Portalen und Benutzereinstellungen. Dies wird verwendet, um zu überprüfen, ob Ihre WorkSpaces Secure Browser Ressourcen mit WorkSpaces Thin Client kompatibel sind. Es wird auch verwendet, um diese Ressourcen in der WorkSpaces Thin AWS Client-Konsole anzuzeigen.
- `appstream`(AppStream 2.0) — Erlaubt Berechtigungen zur Beschreibung von AppStream 2.0-Stacks. Dies wird verwendet, um zu überprüfen, ob Ihre AppStream 2.0-Ressourcen mit WorkSpaces Thin Client kompatibel sind. Es wird auch verwendet, um diese Ressourcen in der WorkSpaces Thin AWS Client-Konsole anzuzeigen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
```

```
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
}
```

AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientFullAccess

Sie können die `AmazonWorkSpacesThinClientFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt volle Zugriffsberechtigungen für den WorkSpaces Thin Client-Dienst und seine Abhängigkeiten. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie AmazonWorkSpacesThinClientFullAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `thinclient`(WorkSpaces Thin Client) — Ermöglicht den vollen Zugriff auf alle WorkSpaces Thin Client-Aktionen.
- `workspaces`(WorkSpaces) — Erlaubt Berechtigungen zur Beschreibung von WorkSpaces Verzeichnissen und Verbindungsaliasnamen. Dies wird verwendet, um zu überprüfen, ob Ihre WorkSpaces Ressourcen mit WorkSpaces Thin Client kompatibel sind. Es wird auch verwendet, um diese Ressourcen in der WorkSpaces Thin AWS Client-Konsole anzuzeigen.
- `workspaces-web`(WorkSpaces Secure Browser) — Ermöglicht Berechtigungen zur Beschreibung von WorkSpaces Secure Browser Portalen und Benutzereinstellungen. Dies wird verwendet, um zu überprüfen, ob Ihre WorkSpaces Secure Browser Ressourcen mit WorkSpaces Thin Client kompatibel sind. Es wird auch verwendet, um diese Ressourcen in der WorkSpaces Thin AWS Client-Konsole anzuzeigen.
- `appstream`(AppStream 2.0) — Erlaubt Berechtigungen zur Beschreibung von AppStream 2.0-Stacks. Dies wird verwendet, um zu überprüfen, ob Ihre AppStream 2.0-Ressourcen mit WorkSpaces Thin Client kompatibel sind. Es wird auch verwendet, um diese Ressourcen in der WorkSpaces Thin AWS Client-Konsole anzuzeigen.

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

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

WorkSpaces Thin Client-Updates für AWS verwaltete Richtlinien

Änderung	Beschreibung	Datum
AmazonWorkSpacesThinClientReadOnlyAccess—Aktualisierte Richtlinie	WorkSpaces Thin Client hat die Richtlinie aktualisiert und umfasst nun eingeschränkte Leseberechtigungen für Gerätedetails und WorkSpaces Verbindungsaliase.	9. Januar 2025

Änderung	Beschreibung	Datum
AmazonWorkSpacesThinClientFullAccess— Aktualisierte Richtlinie	WorkSpaces Thin Client hat die Richtlinie aktualisiert und nun eingeschränkte Leseberechtigungen für WorkSpaces Verbindungsaliase hinzugefügt.	9. Januar 2025
AmazonWorkSpacesThinClientReadOnlyAccess— Aktualisierte Richtlinie	WorkSpaces Thin Client hat die Richtlinie aktualisiert und umfasst nun eingeschränkte Leseberechtigungen für AppStream 2.0, WorkSpaces Web und WorkSpaces.	9. August 2024
AmazonWorkSpacesThinClientFullAccess – Neue Richtlinie	Bietet vollen Zugriff auf Amazon WorkSpaces Thin Client sowie eingeschränkten Zugriff auf die erforderlichen zugehörigen Services.	9. August 2024
AmazonWorkSpacesThinClientReadOnlyAccess – Neue Richtlinie	Bietet schreibgeschützten Zugriff auf Amazon WorkSpaces Thin Client und seine Abhängigkeiten.	19. Juli 2024
WorkSpaces Thin Client hat begonnen, Änderungen zu verfolgen	WorkSpaces Thin Client begann, Änderungen für seine AWS verwalteten Richtlinien nachzuverfolgen.	19. Juli 2024

Fehlerbehebung bei Identität und Zugriff auf Amazon WorkSpaces Thin Client

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit WorkSpaces Thin Client und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion im WorkSpaces Thin Client durchzuführen
- Ich möchte meine Zugriffsschlüssel anzeigen
- Ich bin Administrator und möchte anderen den Zugriff auf WorkSpaces Thin Client ermöglichen
- Ich möchte Personen außerhalb von mir den Zugriff auf meine Thin Client-Ressourcen AWS-Konto ermöglichen WorkSpaces

Ich bin nicht berechtigt, eine Aktion im WorkSpaces Thin Client durchzuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, 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 `thinclient:`*`ListDevices`*-Berechtigungen verfügt.

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

In diesem Fall bittet Mateo seinen Administrator, seine Richtlinien zu aktualisieren, damit er mithilfe der `thinclient:`*`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 Ihre AWS-Konto gewähren.

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 den Zugriff auf WorkSpaces Thin Client ermöglichen

Um anderen den Zugriff auf WorkSpaces Thin Client zu ermöglichen, müssen Sie den Personen oder Anwendungen, die Zugriff benötigen, die entsprechenden Berechtigungen erteilen. Wenn Sie Personen und Anwendungen verwalten, weisen Sie Benutzern oder Gruppen Berechtigungssätze zu, um deren Zugriffsebene zu definieren. AWS IAM Identity Center Mit Berechtigungssätzen werden automatisch IAM-Richtlinien erstellt und den IAM-Rollen zugewiesen, die der Person oder Anwendung zugeordnet sind. Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Berechtigungssätze.

Wenn Sie IAM Identity Center nicht verwenden, müssen Sie IAM-Entitäten (Benutzer oder Rollen) für die Personen oder Anwendungen erstellen, die Zugriff benötigen. Anschließend müssen Sie der Entität eine Richtlinie hinzufügen, die ihnen die richtigen Berechtigungen im WorkSpaces Thin Client gewährt. Nachdem die Berechtigungen erteilt wurden, geben Sie die Anmeldeinformationen an den Benutzer oder Anwendungsentwickler weiter. Sie werden diese Anmeldeinformationen für den Zugriff verwenden AWS. Weitere Informationen zum Erstellen von IAM-Benutzern, -Gruppen, -Richtlinien und -Berechtigungen finden Sie im IAM-Benutzerhandbuch unter IAM-Identitäten sowie Richtlinien und Berechtigungen in IAM.

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

Ich möchte Personen außerhalb von mir den Zugriff auf meine Thin Client-Ressourcen AWS-Konto ermöglichen WorkSpaces

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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob WorkSpaces Thin Client diese Funktionen unterstützt, finden Sie unter. So funktioniert Amazon WorkSpaces Thin Client mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Resilienz im Amazon WorkSpaces Thin Client

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander 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 Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet WorkSpaces Thin Client mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

Schwachstellenanalyse und -management im Amazon WorkSpaces Thin Client

Konfiguration und IT-Steuerung liegen in der gemeinsamen Verantwortung von Ihnen AWS und Ihnen. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Amazon WorkSpaces Thin Client ist kreuzintegriert mit Amazon WorkSpaces, Amazon AppStream 2.0 und WorkSpaces Web. Unter den folgenden Links finden Sie weitere Informationen zur Update-Verwaltung für jeden dieser Dienste:

- Verwaltung von Updates in Amazon AppStream 2.0
- Verwaltung von Updates in Amazon WorkSpaces
- Konfiguration und Schwachstellenanalyse in Amazon WorkSpaces Web

Überwachung von Amazon WorkSpaces Thin Client

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon WorkSpaces Thin Client und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um WorkSpaces Thin Client zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können die Benutzer und Konten, die angerufen haben AWS, die Quell-IP-Adresse, von der aus die Anrufe getätigt wurden, und den Zeitpunkt der Anrufe identifizieren. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

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

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

Amazon WorkSpaces Thin Client ist integriert AWS CloudTrail, ein Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst alle API-Aufrufe für WorkSpaces Thin Client als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der WorkSpaces Thin Client-Konsole und Codeaufrufen für die WorkSpaces Thin Client-API-Operationen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an den WorkSpaces Thin Client, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

Alle Amazon WorkSpaces Thin Client-Aktionen werden von der Amazon WorkSpaces Thin Client API-Referenz protokolliert CloudTrail und sind dort dokumentiert. Beispielsweise generieren Aufrufe von `DeleteDevice` und `GetSoftwareSet` Aktionen Einträge in den CloudTrail Protokolldateien. `CreateEnvironment`

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 Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.

- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die

Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

WorkSpaces Thin Client-Datenereignisse in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die auf oder in einer Ressource ausgeführt werden (z. B. die Registrierung eines Geräts durch einen Endbenutzer). Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Protokolliert standardmäßig CloudTrail keine Datenereignisse. Der CloudTrail Ereignisverlauf zeichnet keine Datenereignisse auf.

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preisgestaltung.

Sie können Datenereignisse für die WorkSpaces Thin Client-Ressourcentypen mithilfe der CloudTrail Konsole oder CloudTrail API-Operationen protokollieren. AWS CLI Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter Protokollieren von Datenereignissen mit dem AWS Management Console und Protokollieren von Datenereignissen mit dem AWS Command Line Interface im AWS CloudTrail -Benutzerhandbuch.

In der folgenden Tabelle sind die WorkSpaces Thin Client-Ressourcentypen aufgeführt, für die Sie Datenereignisse protokollieren können. In der Spalte Datenereignistyp (Konsole) wird der Wert angezeigt, den Sie in der Liste Datenereignistyp auf der CloudTrail Konsole auswählen können. In der Wertspalte resources.type wird der `resources.type` Wert angezeigt, den Sie bei der Konfiguration erweiterter Event-Selektoren mithilfe von oder angeben würden. AWS CLI CloudTrail APIs In der CloudTrail Spalte APIs Protokollierte Daten werden die API-Aufrufe angezeigt, die CloudTrail für den Ressourcentyp protokolliert wurden.

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten, die APIs protokolliert wurden CloudTrail
ThinClientDevice	`AWS::WorkSpacesThinClient::Device`	• RegisterDevice • UpdateDeviceDetails

Sie können erweiterte Event-Selektoren so konfigurieren, dass sie nach den Feldern `eventName`, `readOnly` und `resources.ARN` filtern, sodass nur die Ereignisse protokolliert werden, die für Sie wichtig sind. Weitere Informationen zu diesen Feldern finden Sie unter AdvancedFieldSelector in der API-Referenz zu AWS CloudTrail

WorkSpaces Ereignisse zur Verwaltung von Thin Clients in CloudTrail

Verwaltungsereignisse bieten Informationen über Verwaltungsvorgänge, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

Amazon WorkSpaces Thin Client protokolliert alle Vorgänge auf der WorkSpaces Thin Client-Steuerebene als Verwaltungsereignisse. Eine Liste der Vorgänge auf der Amazon WorkSpaces Thin Client-Kontrollebene, bei denen sich WorkSpaces Thin Client anmeldet CloudTrail, finden Sie in der Amazon WorkSpaces Thin Client API-Referenz.

WorkSpaces Beispiele für Thin Client-Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den `RegisterDevice` Vorgang demonstriert.

```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
```

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

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den `UpdateDeviceDetails` Vorgang demonstriert.

```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-10-21T17:46:27Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "UpdateDeviceDetails",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
```

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

```
            "keyboards": [
              {
                "name": "name",
                "type": "USB"
              }
            ],
            "mice": [
              {
                "name": "name",
                "type": "BLUETOOTH"
              }
            ],
            "sound": {
              "microphones": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ],
              "speakers": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ]
            },
            "webcams": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "USB"
              }
            ]
          },
          "powerAndSleep": {
            "sleepAfter": "FIFTEEN_MINUTES"
          }
        },
        "updatedAt": "2024-10-21T17:46:27.624Z"
      },
      "eventCategory": "Data"
```

```
    }
```

Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalt.

Erstellen von Amazon WorkSpaces Thin Client-Ressourcen mit AWS CloudFormation

Amazon WorkSpaces Thin Client ist integriert AWS CloudFormation, ein 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 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 Regionen bereit.

WorkSpaces Thin Client und AWS CloudFormation Vorlagen

Um Ressourcen für WorkSpaces Thin Client und verwandte Dienste bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation 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 den Formaten JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen bei den ersten Schritten mit Vorlagen zu helfen. AWS CloudFormation Weitere Informationen finden Sie unter Was ist AWS CloudFormation -Designer? im AWS CloudFormation -Benutzerhandbuch.

WorkSpaces Thin Client unterstützt die Erstellung von Umgebungen in. AWS CloudFormation Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Umgebungen, finden Sie in der Referenz zum Amazon WorkSpaces Thin Client-Ressourcentyp im AWS CloudFormation Benutzerhandbuch.

Erfahren Sie mehr über AWS CloudFormation

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

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

- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Greifen Sie über einen Schnittstellenendpunkt auf Amazon WorkSpaces Thin Client zu (AWS PrivateLink)

Sie können AWS PrivateLink es verwenden, 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 AWS Direct Connect eine Verbindung verwenden zu müssen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf WorkSpaces Thin Client zuzugreifen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellenendpunkt erstellen, der von AWS PrivateLink betrieben wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für Thin Client bestimmt ist. WorkSpaces

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

Überlegungen zum Thin Client WorkSpaces

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

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

Erstellen Sie einen Schnittstellenendpunkt 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-Anfragen an den WorkSpaces Thin Client stellen, indem Sie dessen standardmäßigen regionalen DNS-Namen verwenden. 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 standardmäßige Endpunktrichtlinie gewährt Ihnen vollen Zugriff auf WorkSpaces Thin Client über den Schnittstellenendpunkt. Um den Zugriff zu kontrollieren, 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 anhängen, gewährt sie allen Principals auf allen Ressourcen Zugriff auf die aufgelisteten WorkSpaces Thin Client-Aktionen.

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

```
        ],
        "Resource":"*"
      }
   ]
}
```

Dokumentenverlauf für das WorkSpaces Thin Client Administratorhandbuch

In der folgenden Tabelle wird der Dokumentationsverlauf für die Versionen des WorkSpaces Thin Client Administrator Guide beschrieben.

Änderung	Beschreibung	Datum
AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client hat Version 2 für AmazonWorkSpacesThinClientFullAccess verwaltete Richtlinien hinzugefügt.	9. Januar 2025
AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client hat Version 3 für AmazonWorkSpacesThinClientReadOnlyAccess verwaltete Richtlinien hinzugefügt.	9. Januar 2025
Protokollieren von Amazon WorkSpaces Thin Client-API-Aufrufen mit AWS CloudTrail Geräteeinstellungen Datenverschlüsselung im Ruhezustand für Amazon WorkSpaces Thin Client	Ein neuer Abschnitt für Datenereignisse wurde hinzugefügt. Neuer Abschnitt für Geräteeinstellungen hinzugefügt. Die KMS-Informationen im Abschnitt für Datenverschlüsselung im Ruhezustand wurden aktualisiert.	28. Oktober 2024
Geschäftskontinuität	Ein neuer Abschnitt für Geschäftskontinuität und Disaster Recovery wurde hinzugefügt.	6. September 2024

Änderung	Beschreibung	Datum
AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client hat eine AmazonWorkSpacesThinClientFullAccess verwaltete Richtlinie hinzugefügt.	9. August 2024
AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client hat Version 2 für AmazonWorkSpacesThinClientReadOnlyAccess verwaltete Richtlinien hinzugefügt.	9. August 2024
WorkSpaces Personal für WorkSpaces Thin Client konfigurieren	Das wurde für das neue WorkSpaces Personal aktualisiert.	7. August 2024
WorkSpaces Pools für WorkSpaces Thin Client konfigurieren	Neuer Abschnitt für neue WorkSpaces Pools hinzugefügt.	7. August 2024
AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client hat eine AmazonWorkSpacesThinClientReadOnlyAccess verwaltete Richtlinie hinzugefügt.	19. Juli 2024
AWS verwaltete Richtlinien für Amazon WorkSpaces Thin Client	Amazon WorkSpaces Thin Client hat begonnen, Änderungen nachzuverfolgen.	19. Juli 2024
Konfiguration WorkSpaces für Amazon WorkSpaces Thin Client	Die Betriebssystemliste wurde aktualisiert.	12. Februar 2024

Änderung	Beschreibung	Datum
Konfiguration von AppStream 2.0 für Amazon WorkSpaces Thin Client	Das Identity Provider-Verfahren 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.