



POST EDIT. ADDED PROOFREAD. ADDED PP1

# Amazon WorkSpaces Thin Client



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

Copyright © 2024 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 Administratorkonsole VDI für Amazon WorkSpaces Thin Client .....	6
WorkSpaces Personal für WorkSpaces Thin Client konfigurieren .....	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 das erweiterte Setup, um Ihr Workspace .....	8
Geschäftskontinuität .....	9
Konfiguration von WorkSpaces Pools für WorkSpaces Thin Client .....	10
Bevor Sie beginnen .....	10
Erstellen Sie einen WorkSpaces Pool .....	11
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 .....	14
Schritt 2: Richten Sie Ihre AppStream 2.0-Stacks ein .....	15
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 .....	16
Schritt 2: WorkSpaces Secure Browser-Portale einrichten .....	17
Die WorkSpaces Thin Client-Administratorkonsole starten .....	18
Abgedeckte Regionen .....	18
Starten der WorkSpaces Thin Client-Administratorkonsole .....	19
Verwenden der WorkSpaces Thin Client-Administratorkonsole .....	20
Umgebungen .....	21
Umgebungsliste .....	21
Details der Umgebung .....	22
Erstellen einer Umgebung .....	23
Bearbeiten einer Umgebung .....	27

Löschen einer Umgebung .....	28
Geräte .....	28
Geräteliste .....	29
Gerätedetails .....	30
Bearbeiten eines Gerätenamens .....	32
Zurücksetzen und Abmelden des Geräts .....	32
Archivieren eines Geräts .....	32
Löschen eines Geräts .....	33
Exportieren der Gerätedetails .....	33
Software-Updates .....	34
Aktualisieren der Umgebungssoftware .....	34
Aktualisieren der Gerätesoftware .....	35
WorkSpaces Thin Client-Softwareversionen .....	36
Verwendung von Tags auf WorkSpaces Thin Client-Ressourcen .....	44
Sicherheit .....	48
Datenschutz .....	48
Datenverschlüsselung .....	50
Verschlüsselung im Ruhezustand .....	51
Verschlüsselung während der Übertragung .....	66
Schlüsselverwaltung .....	66
Internet, Arbeit, Verkehr, Datenschutz .....	66
Identity and Access Management .....	67
Zielgruppe .....	67
Authentifizierung mit Identitäten .....	68
Verwalten des Zugriffs mit Richtlinien .....	72
So funktioniert Amazon WorkSpaces Thin Client mit IAM .....	75
Beispiele für identitätsbasierte Richtlinien .....	82
AWS verwaltete Richtlinien .....	87
Fehlerbehebung .....	92
Ausfallsicherheit .....	94
Schwachstellenanalyse und -management .....	95
Überwachen .....	96
CloudTrail -Protokolle .....	96
WorkSpaces Thin-Client-Informationen in CloudTrail .....	96
Grundlegendes WorkSpaces zu Thin Client-Protokolldateieinträgen .....	98
AWS CloudFormation -Ressourcen .....	100

---

WorkSpaces Thin Client und AWS CloudFormation Vorlagen .....	100
Weitere Informationen über AWS CloudFormation .....	100
AWS PrivateLink .....	102
Überlegungen .....	102
Erstellen eines Schnittstellenendpunkts .....	102
Erstellen einer Endpunktrichtlinie .....	103
Dokumentverlauf .....	105
.....	cvii

# 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](#)

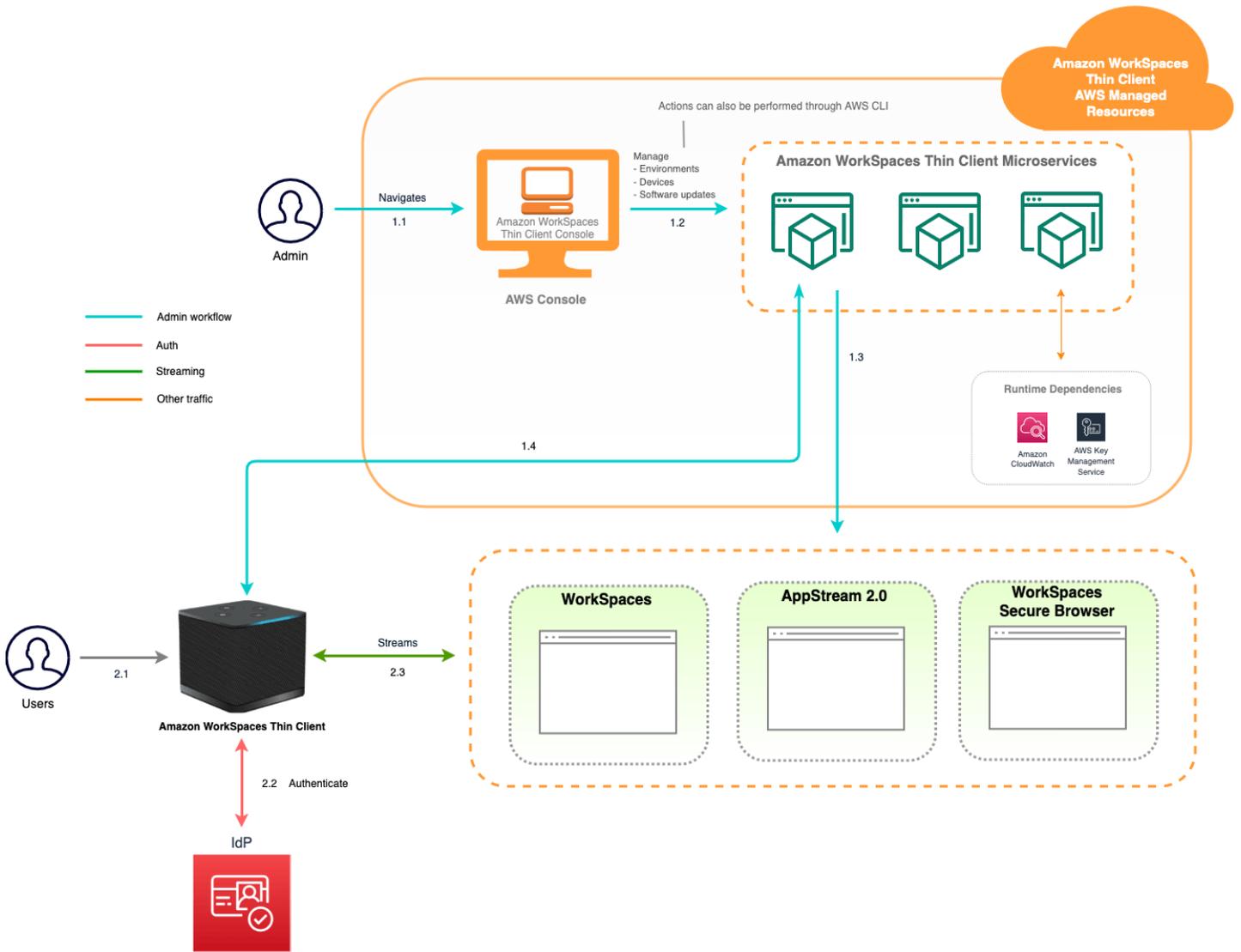
Je nach verwendetem VDI werden die Informationen für Ihren WorkSpaces Thin Client entweder über Verzeichnisse für WorkSpaces, Stacks für AppStream 2.0 und Webportal-Endpunkte für WorkSpaces Secure Browser abgerufen und verwaltet.

Weitere Informationen zu Amazon WorkSpaces finden Sie unter [Erste Schritte mit der WorkSpaces Schnellinstallation](#). Verzeichnisse werden über das verwaltete 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.



# 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/signup>.
2. Folgen Sie den Online-Anweisungen.

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

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

## Erstellen eines IAM-Benutzers

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

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

# Erste Schritte mit Ihrem VDI für Amazon WorkSpaces Thin Client

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

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

## Important

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

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

## Themen

- [WorkSpaces Personal für WorkSpaces Thin Client konfigurieren](#)
- [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](#)

## WorkSpaces Personal für WorkSpaces Thin Client konfigurieren

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 zum Erstellen oder Verwalten eines WorkSpace verfügen. 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 Profilingen 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 Webzugriff. Weitere Informationen finden Sie unter [Amazon WorkSpaces Web Access aktivieren und 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	<ul style="list-style-type: none"><li>• Windows 10</li><li>• Windows 10 (Bring-Your-Own-License)</li><li>• Windows 11</li><li>• Windows 11 (Bring-Your-Own-License)</li></ul>
Unterstützte Pakete	<ul style="list-style-type: none"><li>• Microsoft Power mit Windows 10 (basierend auf Server 2016, 2019 und 2022)</li><li>• Microsoft Power mit Windows 10 (basierend auf Server 2016, 2019 und 2022) w Office</li><li>• Microsoft PowerPro mit Windows 10 (basierend auf Server 2016, 2019 und 2022)</li><li>• Microsoft PowerPro mit Windows 10 (auf Server 2016, 2019 und 2022) w Office</li><li>• Microsoft-Leistung mit Windows 10 (basierend auf Server 2016, 2019 und 2022)</li><li>• Microsoft-Leistung mit Windows 10 (basierend auf Server 2016, 2019 und 2022) w Office</li></ul>
Unterstützte Protokolle	WSPnur

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

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

1. Öffnen Sie die WorkSpaces Konsole unter <https://console.aws.amazon.com/workspaces/>.
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 Verzeichnisisinformationen ein.

4. Wählen Sie zwei Subnetze in einer VPC aus zwei verschiedenen Availability Zones aus. Weitere Informationen finden Sie unter [Konfiguration eines VPC mit öffentlichen Subnetzen](#).
5. Überprüfen Sie Ihre Verzeichnisinformationen und wählen Sie Verzeichnis erstellen.

## 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 — DNS Service- und Routing-Richtlinien wurden konfiguriert. Informationen zur Einrichtung dieser Richtlinien finden [Sie unter DNS Dienst konfigurieren und Routing-Richtlinien einrichten DNS](#).
- Für Resilienz WorkSpaces in mehreren Regionen — Ein Standby WorkSpaces wurde 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 von zugeordnet werden. SDK

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

#### Example

Ein Beispielbefehl, mit AWS CLI dem eine neue Umgebung mithilfe eines WorkSpaces Verbindungsalias für den Streaming-Desktop erstellt wird:

```
aws workspaces-thin-client create-environment --region region --desktop-arn/  
arn:aws:workspaces:region:account:connection-aliases/wsc-a-id
```

Ersetzen *wscs-id* mit Ihrem WorkSpaces persönlichen Verbindungsalias. Die ID des WorkSpaces Verbindungsalias finden Sie in der WorkSpaces Management Console oder unter 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:

„Ein Fehler ist 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 zum Erstellen oder Verwalten eines Workspace verfügen. 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 Konfiguration von SAML 2.0 und Erstellen eines WorkSpaces Pools-Verzeichnisverzeichnisses](#).

So richten Sie einen Pool ein und erstellen ihn

1. Öffnen Sie die WorkSpaces Konsole unter <https://console.aws.amazon.com/workspaces/>.
2. Wählen Sie WorkSpaces im 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

BYOList 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 festlegen können, CLI 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 Verbindungs-Timeout 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 von AppStream 2.0 für Amazon WorkSpaces Thin Client

AppStream 2.0-Instances werden basierend auf Stack-Namen aufgelistet und erfordern eine IdP-Anmeldung, URL um auf der Seite „Umgebung erstellen“ konfiguriert zu werden. Da die SAML Authentifizierung für AppStream 2.0 nur die initiierte Authentifizierung unterstützt, muss der Administrator die richtige Anmeldung 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	<p>Gehen Sie SAML im <a href="#">AppStream 2.0-Administratorhandbuch</a> zu <a href="#">Einrichtung</a>, um einen Identity Provider zu erstellen.</p> <p>Wenn Sie aufgefordert werden, die Umgebungs konsole zu erstellen, geben Sie Ihren IDP Anmeldenamen URL ein.</p>

Funktion	Anforderung
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: WorkSpaces Secure Browser-Portale einrichten

WorkSpaces Thin Client funktioniert mit dem 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	Endpoint	Link zur Konsole
USA Ost (Nord-Virginia)	us-east-1	thinclient.us-east-1.amazonaws.com	<a href="https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home">https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home</a>
USA West (Oregon)	us-west-2	thinclient.us-west-2.amazonaws.com	<a href="https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home">https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home</a>
Asien-Pazifik (Mumbai)	ap-south-1	thinclient.ap-south-1.amazonaws.com	<a href="https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home">https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home</a>

Name der Region	Region	Endpoint	Link zur Konsole
Europa (Irland)	eu-west-1	thinclient.eu-west-1.amazonaws.com	<a href="https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home">https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home</a>
Kanada (Zentral)	ca-central-1	thinclient.ca-central-1.amazonaws.com	<a href="https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home">https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home</a>
Europa (Frankfurt)	eu-central-1	thinclient.eu-central-1.amazonaws.com	<a href="https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home">https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home</a>
Europa (London)	eu-west-2	thinclient.eu-west-2.amazonaws.com	<a href="https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home">https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home</a>

## 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

End User Computing

## Amazon WorkSpaces Thin Client

Affordable, easy-to-manage thin client for secure access to virtual desktops

Improve end-user productivity by going from unboxing to desktop access in just a few minutes, while improving IT staff productivity through centralized remote management of your fleet.

**Amazon WorkSpaces Thin Client**

Create WorkSpaces Thin Client environment, enabling users to securely access virtual desktops.

[Get started](#) [Order devices](#)

**Pricing**

You pay up front for the WorkSpaces Thin Client device, plus a monthly service fee per device to manage, monitor, and maintain your thin client fleet in the WorkSpaces Thin Client management console.

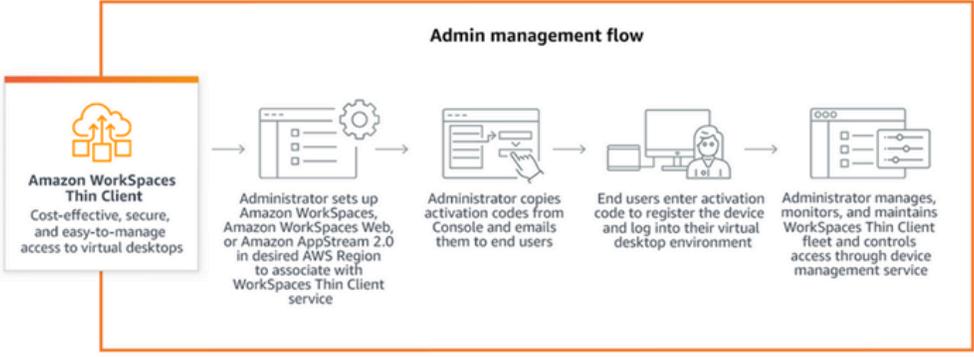
[Learn more about WorkSpaces Thin Client pricing](#)

**Amazon WorkSpaces Thin Client devices**



**How it works**

**Admin management flow**



**Amazon WorkSpaces Thin Client**  
Cost-effective, secure, and easy-to-manage access to virtual desktops

Administrator sets up Amazon WorkSpaces, Amazon WorkSpaces Web, or Amazon AppStream 2.0 in desired AWS Region to associate with WorkSpaces Thin Client service

Administrator copies activation codes from Console and emails them to end users

End users enter activation code to register the device and log into their virtual desktop environment

Administrator manages, monitors, and maintains WorkSpaces Thin Client fleet and controls access through device management service

Willkommen in der WorkSpaces Thin Client Administratorkonsole!

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

Informationen zum WorkSpaces Thin Client-Gerät finden Sie im [WorkSpaces Thin Client-Benutzerhandbuch](#).

Fangen wir an!

Themen

- [Umgebungen](#)
- [Geräte](#)
- [Software-Updates](#)

# Umgebungen

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

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

## Umgebungsliste

### Details der Umgebungsliste

Name – Die dieser Umgebung zugeordnete eindeutige Kennung.

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

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

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

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

### Aktionen der Umgebungsliste

Suche – Sucht alle Umgebungen, die Sie verwalten.

Aktualisieren – Aktualisiert die Umgebungsliste.

Details anzeigen – Zeigt [Umgebungsdetails](#) an.

Aktionen — Öffnet eine Dropdownliste, in der Sie eine Umgebung [bearbeiten](#) oder [löschen](#) können.

Umgebung erstellen – Startet den Prozess der [Erstellung einer Umgebung](#).

Umgebung erstellen – Startet den Prozess der [Erstellung einer Umgebung](#).

### Themen

- [Details der Umgebung](#)

- [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. Die Konsole zeigt auch die Details über den Anbieter für virtuelle Desktops an, den diese Umgebung verwendet.

Themen

- [Übersicht](#)
- [Details zur virtuellen Desktop-Umgebung](#)

## Übersicht

Name – Die dieser Umgebung zugeordnete eindeutige Kennung.

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

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

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

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

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

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

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

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

Erstellungszeit — Datum und Uhrzeit der Erstellung dieser Umgebung.

## Details zur virtuellen Desktop-Umgebung

Details zum WorkSpaces Amazon-Verzeichnis

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

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

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

Verzeichnistyp — Das Format des WorkSpaces Amazon-Verzeichnisses.

Registriert — Ob dieses WorkSpaces Amazon-Verzeichnis registriert ist.

Status — Ob dieses WorkSpaces Amazon-Verzeichnis aktiv ist.

Einzelheiten zum Amazon WorkSpaces Secure Browser-Portal

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

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

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

AppStream 2.0-Einzelheiten

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

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

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

## Erstellen einer Umgebung

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

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

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

 Note

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

## Themen

- [Schritt 1: Eingeben der Umgebungsdetails](#)
- [Schritt 2: Auswählen Ihres virtuellen Desktop-Anbieters](#)
- [Schritt 3: Senden des Aktivierungscode 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 Dienst, der Ihren Benutzern Zugriff auf ihren virtuellen Desktop und kompatible Ressourcen bietet.

### Important

Damit die WorkSpaces Thin Client Administrator Console ordnungsgemäß funktioniert, muss Ihr System bestimmte Anforderungen erfüllen. Diese Anforderungen sind unter [Voraussetzungen und Konfigurationen](#) aufgeführt.

Stellen Sie sicher, dass Ihr System diese Anforderungen erfüllt, bevor Sie Ihre Konsole einrichten.

## Amazon verwenden WorkSpaces

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

1. Gehen Sie wie folgt vor WorkSpaces, um Amazon zu verwenden:
  - Wählen Sie das Verzeichnis aus, das Sie verwenden möchten. Sie können entweder die Dropdownliste durchsuchen oder die Verzeichnisse mithilfe des Suchfeldes durchsuchen.
  - 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 Ihren Identity Provider-Login und Logout URL in das URLIdP-Anmeldefeld 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 Aktivierungscode 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-Verwaltungskonsolle 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“.

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“.
3. Wählen Sie Löschen aus der Drop-down-Liste aus. Das Bestätigungsfenster „Umgebung löschen“ wird angezeigt.
4. Geben Sie im Bestätigungsfeld „löschen“ ein.
5. Wählen Sie die Schaltfläche Löschen aus.

## Geräte

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

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

# Geräteliste

## Gerätelistendetails

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

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

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

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

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

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

### Note

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

- Abgemeldet – Das Gerät wurde erfolgreich abgemeldet.

### Note

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

- Archiviert – Das Gerät ist archiviert.

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

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

- Konform
- Nicht konform

## Gerätelistenaktionen

Suche – Durchsucht alle Geräte, die Sie verwalten.

Aktualisieren – Aktualisiert die Geräteliste.

Details anzeigen – Zeigt Gerätedetails an.

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

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

Geräte bestellen – Startet den Bestellvorgang für Geräte.

Themen

- [Gerätedetails](#)
- [Bearbeiten eines Gerätenamens](#)
- [Zurücksetzen und Abmelden des Geräts](#)
- [Archivieren eines Geräts](#)
- [Löschen eines Geräts](#)
- [Exportieren der Gerätedetails](#)

## Gerätedetails

### Übersicht

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

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

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

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

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

- Aktiv
- Inaktiv

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

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

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

 Note

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

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

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

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

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

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

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

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

- Konform
- Nicht konform

## Benutzerprotokoll

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

## Bearbeiten eines Gerätenamens

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

## Zurücksetzen und Abmelden des Geräts

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

### Note

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

## Archivieren eines Geräts

1. Wählen Sie das Gerät aus, das Sie archivieren möchten. Sie können entweder die Dropdownliste durchsuchen oder über das Suchfeld nach dem Gerät suchen.

2. Wählen Sie die Schaltfläche Aktionen aus.
3. Wählen Sie in der Drop-down-Liste die Option Archivieren aus. Das Fenster Archiv wird angezeigt.
4. Geben Sie in das Bestätigungsfeld „zurücksetzen und archivieren“ ein.
5. Wählen Sie die Schaltfläche Zurücksetzen und archivieren aus.

#### Note

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

## Löschen eines Geräts

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

#### Note

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

## Exportieren der Gerätedetails

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

# Software-Updates

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

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

Eine Liste der veröffentlichten [Softwaresets finden Sie unter Softwaresets für WorkSpaces Thin Client-Umgebungen](#).

Themen

- [Aktualisieren der Umgebungssoftware](#)
- [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
2.8.0	09-06-2024	<ul style="list-style-type: none"><li>• Thin Client unterstützt Monitore mit 4K-Auflösung.</li><li>• Benutzer können eine Verbindung zur VDI Sitzung herstellen, auch wenn die WorkSpaces Thin Client-Geräteverwaltungsdienste vorübergehend nicht verfügbar sind.</li><li>• Es wurde das Problem behoben, bei dem im Abschnitt „Benutzeraktivität details“ in der AWS Konsole doppelte Einträge angezeigt wurden.</li><li>• Endbenutzer können die PrintScreen Option beim Streamen WorkSpaces auf dem WorkSpaces Thin Client verwenden.</li></ul>

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.7.1	27.08.2024	<ul style="list-style-type: none"><li>• Zero-Day-Korrekturen für die kritischen Sicherheitsprobleme -2024-7971 und CVE -2024-7965 von Chromium. CVE</li></ul>
2.7.0	29.07.2024	<ul style="list-style-type: none"><li>• Verbesserungen der Leistung des zweiten Monitors.</li><li>• Es wurde ein Problem behoben, bei dem die Sprache der Werkzeugleiste beim Ändern der Gerätesprache nicht beeinflusst wurde.</li><li>• Das Gerät sammelt jetzt Diagnoseinformationen für Serviceverbesserungen.</li></ul>

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.6.0	07-09-2024	<ul style="list-style-type: none"><li>• Benutzer können eingehende Softwareupdates zurückstellen, sodass sie ihre Arbeit ohne Unterbrechung beenden können.</li><li>• Mithilfe der Geräteeinstellungen können Benutzer gespeicherte WiFi Netzwerke vergessen.</li><li>• Verbesserungen der Leistung von Audio-/Videoanrufen in der Sitzung.</li><li>• Einige Benutzereinstellungen für die VDI Sitzungen bleiben auch nach dem Neustart des Geräts erhalten.</li></ul>
2.5.0	13.06.2024	<ul style="list-style-type: none"><li>• Es wurde das Problem behoben, bei dem das Gerät beim Aufwachen aus dem Ruhemodus vor dem Start der Sitzung kurz den Bildschirm zur Einrichtung von Tastatur und Maus anzeigte.</li><li>• Die Home-Schaltfläche auf der Gerätesymbolleiste wurde in Anmelden umbenannt.</li><li>• Verbesserungen der Leistung von Audio-/Videoanrufen in der Sitzung.</li></ul>

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.4.3	29.05.2024	<ul style="list-style-type: none"><li>• Zero-Day-Fix für das kritische Sicherheitsproblem CVE -2024-5274 von Chromium.</li></ul>
2.4.2	17.05.2024	<ul style="list-style-type: none"><li>• Zero-Day-Fix für das kritische Sicherheitsproblem CVE -2024-4947 von Chromium.</li></ul>
2.4.1	15.05.2024	<ul style="list-style-type: none"><li>• Zero-Day-Korrekturen für die kritischen Sicherheitsprobleme -2024-4671 und CVE -2024-4761 von Chromium. CVE</li><li>• Das Problem, dass der Browser durch Klicken mit der rechten Maustaste auf AWS und Datenschutzzlinks auf WorkSpaces der Anmeldeseite geöffnet werden konnte, wurde behoben.</li></ul>

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.4.0	05-09-2024	<ul style="list-style-type: none"><li>• Es wurde ein Problem behoben, durch das „accounts.google.com“ blockiert und die Verwendung von Google Workspace als for 2.0-Sitzung verhindert wurde. IDP AppStream</li><li>• Die Werkzeuggestreife für Geräteeinstellungen wird mit einem Klick auf einen beliebigen Bereich auf dem Bildschirm automatisch zusammengeklappt.</li></ul>

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.3.0	04-05-2024	<ul style="list-style-type: none"><li>• Die Geräteeinstellungen werden in einer zusammeng eklappten Werkzeugleiste angezeigt, sodass der sichtbare Bildschirm besser genutzt werden kann.</li><li>• Endbenutzer können jetzt festlegen, wie lange es dauert, bis das Gerät bei Inaktivität in den Ruhemodus wechselt.</li><li>• Das Problem, dass „about:blank“ auf dem zweiten Display URL angezeigt wurde, wurde behoben.</li><li>• Das Problem, das zu einem weißen Bildschirm führte, wenn die erweiterte Anzeige geschlossen wurde, wurde behoben.</li><li>• Die von Endbenutzern eingestellte Lautstärke bleibt jetzt auch bei Geräteneu starts erhalten.</li></ul>
2.2.1	16.02.2024	<ul style="list-style-type: none"><li>• Es wurde ein Problem behoben, das während des Anmeldevorgangs auftrat und Benutzer daran hinderte, sich bei der mit SAML 2.0 WorkSpaces konfigurierten Authentifizierung anzumelden.</li></ul>

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.2.0	02-08-2024	<ul style="list-style-type: none"><li>• Unterstützung für ISO Tastaturen mit den Sprachen Englisch (Großbritannien), Französisch, Deutsch, Italienisch und Spanisch hinzugefügt.</li></ul>
2.1.2	26.01.2024	<ul style="list-style-type: none"><li>• Zero-Day-Fix für das kritische Sicherheitsproblem CVE -2024-0519 von Chromium.</li><li>• Verbesserung der Latenz für Endbenutzer im Zusammenhang mit der Sperrfunktion.</li><li>• Interne Endgeräte, die mit Geräten verbunden sind, werden auf die Domäne „ThinClient*“ umgestellt.</li></ul>
2.1.1	21.12.2023	<ul style="list-style-type: none"><li>• Zero-Day-Fix für das kritische Sicherheitsproblem CVE -2023-7024 von Chromium.</li></ul>
2.1.0	20-12-2023	<ul style="list-style-type: none"><li>• 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.</li></ul>

Softwaresatz	Datum der Veröffentlichung	Änderungen
2.0.1	12-06-2023	<ul style="list-style-type: none"><li>• Zero-Day-Fix für das kritische Sicherheitsproblem -2024-6345 von CVE Chromium.</li></ul>
2.0.0	15.11.2023	<ul style="list-style-type: none"><li>• Erstversion</li></ul>

# 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 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 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 in Amazon WorkSpaces Thin Client

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

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

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS Services in der ausführt AWS Cloud. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Externe Prüfer testen und überprüfen im Rahmen der [AWS Compliance-Programme](#) regelmäßig die Wirksamkeit unserer Sicherheit. Informationen zu den Compliance-Programmen, die für Amazon WorkSpaces Thin Client gelten, finden Sie unter [AWS Im Rahmen des Compliance-Programms zugelassene -ServicesIm](#).
- Sicherheit in der Cloud – Ihre Verantwortung wird durch den - AWS Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

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

Themen

- [Datenschutz im Amazon WorkSpaces Thin Client](#)
- [Identitäts- und Zugriffsmanagement für Amazon WorkSpaces Thin Client](#)
- [Ausfallsicherheit in Amazon WorkSpaces Thin Client](#)
- [Schwachstellenanalyse und -management in 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 im [Abschnitt Datenschutz FAQ](#). Informationen zum Datenschutz in Europa finden Sie im [AWS Shared Responsibility Model und](#) im GDPR Blogbeitrag im AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre 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 eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigen API, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter [Federal Information Processing Standard](#) ( ) 140-3. FIPS

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit WorkSpaces Thin Client oder anderen Geräten arbeiten und die Konsole AWS-Services verwenden, API, AWS CLI oder 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 einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

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 den 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 spezielle 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 Umgebungsaktivierungs-codes und Benutzeranmeldeinformationen:
  - Administratoren müssen sich bei der WorkSpaces Thin Client-Konsole anmelden, und Benutzer müssen Aktivierungs-codes 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 verschlüsselt werden. AWS KMS 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 - Schlüsselmanagementsdienst.

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 anderen Verschlüsselungstyp auswählen, aber Sie können eine zweite Verschlüsselungsebene über den vorhandenen AWS eigenen Verschlüsselungsschlüssel hinzufügen, indem Sie bei der Erstellung Ihrer Thin Client-Umgebung einen vom Kunden verwalteten Schlüssel wählen:

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

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

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

Weitere Informationen finden Sie unter vom [Kunden verwalteter Schlüssel](#) im AWS Key Management Service Developer Guide.

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

Datentyp	AWSVerschlüsselung mit eigenem Schlüssel	Vom Kunden verwaltete Schlüsselverschlüsselung (optional)
Umgebungsname  WorkSpaces Name der Thin <a href="#">Client-Umgebung</a>	Aktiviert	Aktiviert
Gerätename  WorkSpaces Name des Thin <a href="#">Client-Geräts</a>	Aktiviert	Aktiviert
Tags zur Geräteerstellung  WorkSpaces Tags zur Geräteerstellung in der <a href="#">Thin-Client-Umgebung</a>	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 [Preise für den AWS Key Management Service](#).

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

Amazon WorkSpaces Thin Client benötigt eine [Genehmigung](#), damit Sie Ihren vom Kunden verwalteten Schlüssel verwenden können.

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

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

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

- Senden Sie [Decrypt-Anfragen](#) an, AWS KMS um die verschlüsselten Daten zu entschlüsseln

Sie können den Zugriff auf den Zuschuss jederzeit widerrufen oder dem Dienst den Zugriff auf den vom Kunden verwalteten Schlüssel entziehen. Wenn Sie dies tun, kann Amazon WorkSpaces Thin Client auf keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise versuchen, [Umgebungsdetails abzurufen](#), auf die Amazon WorkSpaces Thin Client nicht zugreifen

kann, gibt der Vorgang einen `AccessDeniedException` Fehler zurück. Darüber hinaus kann das WorkSpaces Thin Client-Gerät keine WorkSpaces Thin Client-Umgebung verwenden.

## Einen kundenverwalteten Schlüssel erstellen

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel mithilfe der AWS Managementkonsole oder der AWS KMS API Operation 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 Vorgänge in der Schlüsselrichtlinie zulässig sein:

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

Dadurch kann Amazon WorkSpaces Thin Client Folgendes tun:

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

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

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

```
]
}
```

Weitere Informationen zum [Festlegen von Berechtigungen in einer Richtlinie](#) finden Sie im [Entwicklerhandbuch zum AWS Key Management Service](#).

Weitere Informationen zur [Fehlerbehebung beim Schlüsselzugriff](#) finden Sie im [Entwicklerhandbuch zum AWS Key Management Service](#).

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

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

- WorkSpaces [Thin-Client-Umgebung](#)

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

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

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 zum Verschlüsseln von Daten einbeziehen, wird der Verschlüsselungskontext AWS KMS an die verschlüsselten Daten gebunden. Um Daten zu entschlüsseln, müssen Sie denselben Verschlüsselungskontext in die Anfrage aufnehmen.

## Amazon WorkSpaces Thin Client-Verschlüsselungskontext

Amazon WorkSpaces Thin Client verwendet bei allen AWS KMS kryptografischen 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 Amazon CloudWatch Logs generiert wurden AWS CloudTrail](#) .

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

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

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

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

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

## Überwachung Ihrer Verschlüsselungsschlüssel für Amazon WorkSpaces Thin Client

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

Die folgenden Beispiele sind AWS CloudTrail Ereignisse für `DescribeKey`, `CreateGrantGenerateDataKey`, `Decrypt` (mit `Grant`) 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 AWS KMS Kunden verwalteten Schlüssel zu verifizieren.

Das folgende Beispielergebnis zeichnet den Vorgang `DescribeKey` auf:

```
{
  "eventVersion": "1.08",
```

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
  "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
  "accountId": "111122223333",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
      "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
      "accountId": "111122223333",
      "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2023-11-21T13:43:33Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "thinclient.amazonaws.com"
},
"eventTime": "2023-11-21T13:44:22Z",
"eventSource": "kms.amazonaws.com",
"eventName": "DescribeKey",
"awsRegion": "eu-west-1",
"sourceIPAddress": "thinclient.amazonaws.com",
"userAgent": "thinclient.amazonaws.com",
"requestParameters": {"keyId": "arn:aws:kms:eu-west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
"responseElements": null,
"requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:eu-west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
```

```
"recipientAccountId": "111122223333",  
"eventCategory": "Management"  
}
```

## CreateGrant

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

Das folgende Beispiereignis zeichnet den Vorgang CreateGrant auf:

```
{  
  "eventVersion": "1.08",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",  
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",  
    "accountId": "111122223333",  
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",  
    "sessionContext": {  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",  
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",  
        "accountId": "111122223333",  
        "userName": "Admin"  
      },  
      "webIdFederationData": {},  
      "attributes": {  
        "creationDate": "2023-11-21T13:43:33Z",  
        "mfaAuthenticated": "false"  
      }  
    },  
    "invokedBy": "thinclient.amazonaws.com"  
  },  
  "eventTime": "2023-11-21T13:44:23Z",  
  "eventSource": "kms.amazonaws.com",  
  "eventName": "CreateGrant",  
  "awsRegion": "eu-west-1",  
  "sourceIPAddress": "thinclient.amazonaws.com",  
  "userAgent": "thinclient.amazonaws.com",  
  "requestParameters": {  
    "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",  
    "operations": ["Decrypt"],  
  }  
}
```

```

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

```

## GenerateDataKey

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

Das folgende Beispiereignis zeichnet den Vorgang GenerateDataKey auf:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",

```

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

```

    "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

## Decrypt

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

Das folgende Beispiereignis zeichnet den Vorgang Decrypt auf:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-11-21T13:43:33Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "invokedBy": "thinclient.amazonaws.com"
},
"eventTime": "2023-11-21T13:44:25Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Decrypt",

```

```

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

```

## Decrypt (using Grant)

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

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

```

{
  "eventVersion": "1.08",
  "userIdentity": {

```

```

    "type": "AWSService",
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2023-11-21T13:44:23Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "eu-west-1",
  "sourceIPAddress": "thinclient.amazonaws.com",
  "userAgent": "thinclient.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
      "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventCategory": "Management"
}

```

## Weitere Informationen

Die folgenden Ressourcen bieten weitere Informationen zur Datenverschlüsselung im Ruhezustand:

- Weitere Informationen zu den [grundlegenden Konzepten von AWS Key Management Service](#) finden Sie im [AWS Key Management Service Developer Guide](#).
- Weitere Informationen zu [bewährten Sicherheitsmethoden für AWS Key Management Service](#) finden Sie im [AWS Key Management Service Developer Guide](#).

## Verschlüsselung während der Übertragung

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

Die Verschlüsselung bei der Übertragung ist standardmäßig konfiguriert, und 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 festlegen, indem Sie den verwenden AWS SDK.

## 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 AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um WorkSpaces Thin Client-Ressourcen zu verwenden. IAM ist eine AWS-Service , die 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 Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. 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 unter [Fehlerbehebung 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 Anfragen an Ihren IAM Administrator

senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen WorkSpaces Thin Client verwenden IAM kann, finden Sie unter [So funktioniert Amazon WorkSpaces Thin Client mit IAM](#).

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf WorkSpaces Thin Client zu verwalten. Beispiele für identitätsbasierte WorkSpaces Thin Client-Richtlinien, die Sie in verwenden könnenIAM, 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 sich als IAM Benutzer authentifizieren (angemeldet bei AWS) oder indem Sie eine IAM Rolle übernehmen. 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 (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportale 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 der 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, um Anfragen selbst zu [signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren](#).

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. 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 [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) AWS im IAM Benutzerhandbuch](#).

## AWS-Konto Root-Benutzer

Wenn Sie ein neues AWS-Konto erstellen, 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 und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich](#) sind. IAM

## 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 [IAMBenutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen

Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich](#) sind.

Eine [IAMGruppe](#) ist eine Identität, die eine Sammlung von IAM Benutzern spezifiziert. 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 IAMAdmins und 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 [Wann sollte ein IAM Benutzer \(statt einer Rolle\) erstellt werden?](#) im IAMBenutzerhandbuch.

## IAMRollen

Eine [IAMRolle](#) ist eine Identität innerhalb von Ihrem AWS-Konto, für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die [Rollen wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwenden URL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie [unter Verwenden von IAM Rollen](#) im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- **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 im IAMBenutzerhandbuch unter [Erstellen einer Rolle für einen externen Identitätsanbieter](#). Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, 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 verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) 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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM
- 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.
- Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine 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. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASANfragen 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 beim Stellen von FAS Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle — Eine Servicerolle ist eine [IAMRolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).
- Dienstbezogene Rolle — Eine dienstverknüpfte 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 dienstbezogene 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 IAMBenutzerhandbuch unter [Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt](#) werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden [Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle \(anstelle eines IAM Benutzers\) erstellt](#) werden.

## Verwalten des Zugriffs mit Richtlinien

Sie steuern 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. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter [Überblick über JSON Richtlinien](#).

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

## Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter [IAM Richtlinien erstellen im Benutzerhandbuch](#). IAM

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 zur Auswahl zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie finden Sie im IAM Benutzerhandbuch unter [Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien](#).

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 nicht IAM 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 AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bieten ACLs. 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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren 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 zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter [Berechtigungsgrenzen für IAM Entitäten](#).
- **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 Geräte 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. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) 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 im IAMBenutzerhandbuch unter [Sitzungsrichtlinien](#).

## 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 IAMBenutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

## So funktioniert Amazon WorkSpaces Thin Client mit IAM

Bevor Sie IAM den Zugriff auf WorkSpaces Thin Client verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen für die Nutzung mit WorkSpaces Thin Client verfügbar sind.

IAMFunktionen, die Sie mit Amazon WorkSpaces Thin Client verwenden können

IAMFunktion	WorkSpaces Thin Client-Unterstützung
<a href="#">Identitätsbasierte Richtlinien</a>	Ja
<a href="#">Ressourcenbasierte Richtlinien</a>	Nein
<a href="#">Richtlinienaktionen</a>	Ja
<a href="#">Richtlinienressourcen</a>	Ja
<a href="#">Bedingungsschlüssel für die Richtlinie</a>	Ja
<a href="#">ACLs</a>	Nein
<a href="#">ABAC(Tags in Richtlinien)</a>	Ja
<a href="#">Temporäre Anmeldeinformationen</a>	Ja
<a href="#">Hauptberechtigungen</a>	Ja
<a href="#">Servicerollen</a>	Nein
<a href="#">Serviceverknüpfte Rollen</a>	Nein

Einen allgemeinen Überblick darüber, wie WorkSpaces Thin Client und andere AWS Dienste mit den meisten IAM Funktionen funktionieren, finden Sie IAM im IAMBenutzerhandbuch unter [AWS Dienste, die mit funktionieren](#).

### Identitätsbasierte Richtlinien für WorkSpaces Thin Client

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter [IAMRichtlinien erstellen im Benutzerhandbuch](#). IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigernde Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der [Referenz zu den IAM JSON Richtlinienelementen](#) im IAMBenutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für WorkSpaces Thin Client

Beispiele für identitätsbasierte WorkSpaces Thin Client-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Thin Client](#)

## Ressourcenbasierte Richtlinien innerhalb von Thin Client WorkSpaces

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal 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 Prinzipalidentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. 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 [IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff](#).

## Richtlinienaktionen für WorkSpaces Thin Client

Unterstützt Richtlinienaktionen: Ja

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

Das `Action` Element 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, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API 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 festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Resource JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein Resource oder ein NotResource-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem [Amazon-Ressourcennamen \(ARN\)](#) anzugeben. 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 die ARN einzelnen Ressourcen spezifizieren 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 festlegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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

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

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMRichtlinienelemente: Variablen und Tags](#).

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontext-Schlüssel für AWS globale Bedingungen](#) im IAMBenutzerhandbuch.

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 WorkSpaces Thin Client

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In werden AWS 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, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement 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 finden Sie ABAC unter [Was ist? ABAC](#) im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter [Verwenden der attributebasierten Zugriffskontrolle \(ABAC\)](#). IAM

## Temporäre Zugangsdaten mit Thin Client verwenden WorkSpaces

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen [arbeiten können AWS-Services](#), finden Sie IAM im IAMBenutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort 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 Rollenwechsel finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. 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 unter IAM](#).

## Serviceübergreifende Prinzipalberechtigungen für WorkSpaces Thin Client

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine 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 AWS-Service an 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 beim Stellen von FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

## Service-Rollen für WorkSpaces Thin Client

Unterstützt Service-Rollen: Nein

Eine Service-Rolle ist eine [IAM-Rolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Service-Rolle von innen heraus erstellen, ändern und löschen IAM. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).

### Warning

Das Ändern der Berechtigungen für eine Service-Rolle kann die WorkSpaces Thin Client-Funktionalität beeinträchtigen. Bearbeiten Sie Service-Rollen 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 Service-Rolle, 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 dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter [AWS Dienste, die mit funktionieren](#). IAM 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 von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter [IAMRichtlinien erstellen](#) im IAMBenutzerhandbuch.

Einzelheiten zu den von WorkSpaces Thin Client definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Thin Client](#) in der Service Authorization Reference.

## Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwendung der WorkSpaces Thin Client-Konsole](#)
- [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 Ihren Benutzern und Workloads zunächst 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 AWS im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen](#).

- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie [IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen](#). IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen über gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMJSONRichtlinienelemente: Bedingung](#).
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter [IAMAccess Analyzer-Richtlinienvvalidierung](#) im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter [Konfiguration des MFA -geschützten API Zugriffs](#) im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter [Bewährte Sicherheitsmethoden IAM im IAM](#) Benutzerhandbuch. IAM

## Verwendung der WorkSpaces Thin Client-Konsole

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 den AWS CLI oder den anrufen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie 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 von AWS CLI oder AWSAPI.

```
{
  "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

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline-Richtlinien und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 IAM Client-Benutzern vollen Zugriff gewährt. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen aller WorkSpaces Thin Client-Aktionen auf der Konsole oder im Programm mithilfe von AWS CLI oder AWSAPI.

```

{
  "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 [kundenverwaltete 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 im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien](#).

### AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientReadOnlyAccess

Sie können die AmazonWorkSpacesThinClientFullAccess Richtlinie an Ihre IAM Identitäten anhängen. Diese Richtlinie gewährt volle Zugriffsberechtigungen für den WorkSpaces Thin Client-Dienst und seine Abhängigkeiten. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie [AmazonWorkSpacesThinClientReadOnlyAccess](#) im 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 WorkSpaces von Verzeichnissen. 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:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceDirectories"
      ]
    }
  ]
}
```

```
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowWorkSpacesWebAccess",
    "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 anhängen. Diese Richtlinie gewährt volle Zugriffsberechtigungen für den WorkSpaces Thin Client-Dienst und seine Abhängigkeiten. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie [AmazonWorkSpacesThinClientFullAccess](#) im 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. 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:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesWebAccess",
      "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
<a href="#">AmazonWorkSpacesThinClientReadOnlyAccess</a> — 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
<a href="#">AmazonWorkSpacesThinClientFullAccess</a> – Neue Richtlinie.	Bietet vollen Zugriff auf Amazon WorkSpaces Thin Client sowie eingeschränkten Zugriff auf die erforderlichen zugehörigen Services.	9. August 2024
<a href="#">AmazonWorkSpacesThinClientReadOnlyAccess</a> – 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 auftreten können IAM.

## 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 den WorkSpaces Thin Client ermöglichen](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine WorkSpaces Thin Client-Ressourcen ermöglichen](#)

## 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 zu verwenden, um Details zu einer fiktiven *my-thin-client-device* Ressource anzuzeigen, aber nicht über die fiktiven `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 Aktion auf die *my-thin-client-device* Ressource zugreifen kann.

`thinclient:ListDevices`

## Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit einsehen. 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/bPXRf1CYEXAMPLEKEY). 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 gewähren AWS-Konto.

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

## Ich bin Administrator und möchte anderen den Zugriff auf den 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 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 [IAMim IAMBenutzerhandbuch unter IAMIdentitäten und Richtlinien und Berechtigungen](#).

Weitere Informationen finden Sie unter [Gewähren Sie vollen Zugriff auf den Thin Client WorkSpaces](#)

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

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 auf einen anderen IAMBenutzer AWS-Konto , den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund [gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM

## Ausfallsicherheit in Amazon WorkSpaces Thin Client

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

kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS-Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

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

## Schwachstellenanalyse und -management in Amazon WorkSpaces Thin Client

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

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

- [Update-Management in Amazon AppStream 2.0](#)
- [Update-Verwaltung in Amazon WorkSpaces](#)
- [Konfigurations- und Schwachstellenanalyse in Amazon WorkSpaces Web](#)

# Überwachen von Amazon WorkSpaces Thin Client

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

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

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

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

Weitere Informationen zu CloudTrail finden Sie im [AWS CloudTrail -Benutzerhandbuch](#).

## WorkSpaces Thin-Client-Informationen in CloudTrail

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

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

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

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

Alle WorkSpaces Thin-Client-Aktionen werden von protokolliert CloudTrail und sind in der [Amazon-WorkSpaces Thin-Client-API-Referenz](#) dokumentiert. Aufrufe der GetSoftwareSet Aktionen CreateEnvironment, ListDevicesund erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

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

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

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

## Grundlegendes WorkSpaces zu Thin Client-Protokolldateieinträgen

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

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

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

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

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

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

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

## WorkSpaces Thin Client und AWS CloudFormation Vorlagen

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

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

## Weitere Informationen über AWS CloudFormation

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

- [AWS CloudFormation](#)
- [AWS CloudFormation Benutzerhandbuch](#)
- [AWS CloudFormation API Referenz](#)

- [AWS CloudFormation Benutzerhandbuch für die -Befehlszeilenschnittstelle](#)

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

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

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

Weitere Informationen finden Sie unter [Zugriff auf AWS-Services über AWS PrivateLink](#) im AWS PrivateLink -Leitfaden.

## Überlegungen für WorkSpaces Thin Client

Bevor Sie einen Schnittstellenendpunkt für WorkSpaces Thin Client einrichten, lesen [Sie Überlegungen](#) im AWS PrivateLink -Handbuch.

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

## Erstellen eines Schnittstellenendpunkts für WorkSpaces Thin Client

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

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

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

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

## Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

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

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

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

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf Services mit Endpunktrichtlinien](#) im AWS PrivateLink -Leitfaden.

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

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

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

```
]
}
```

# 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
<a href="#">Geschäftskontinuität</a>	Ein neuer Abschnitt für Geschäftskontinuität und Notfallwiederherstellung wurde hinzugefügt.	6. September 2024
<a href="#">AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientFullAccess</a>	Amazon WorkSpaces Thin Client hat eine AmazonWorkSpacesThinClientFullAccess verwaltete Richtlinie hinzugefügt.	9. August 2024
<a href="#">AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientReadOnlyAccess</a>	Amazon WorkSpaces Thin Client hat Version 2 für AmazonWorkSpacesThinClientReadOnlyAccess verwaltete Richtlinien hinzugefügt.	9. August 2024
<a href="#">WorkSpaces Personal für WorkSpaces Thin Client konfigurieren</a>	Das wurde für das neue WorkSpaces Personal aktualisiert.	7. August 2024
<a href="#">Konfiguration von WorkSpaces Pools für WorkSpaces Thin Client</a>	Neuer Abschnitt für neue WorkSpaces Pools hinzugefügt.	7. August 2024
<a href="#">AWS verwaltete Richtlinie: AmazonWorkSpacesThinClientReadOnlyAccess</a>	Amazon WorkSpaces Thin Client hat eine AmazonWorkSpacesThinClientR	19. Juli 2024

Änderung	Beschreibung	Datum
	eadOnlyAccess verwaltete Richtlinie hinzugefügt.	
<a href="#">AWS verwaltete Richtlinien für Amazon WorkSpaces Thin Client</a>	Amazon WorkSpaces Thin Client hat begonnen, Änderungen nachzuverfolgen.	19. Juli 2024
<a href="#">Konfiguration WorkSpaces für Amazon WorkSpaces Thin Client</a>	Die Betriebssystemliste wurde aktualisiert.	12. Februar 2024
<a href="#">Konfiguration von AppStream 2.0 für Amazon WorkSpaces Thin Client</a>	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.