



Benutzerhandbuch

AWS Datenübertragungsterminal



AWS Datenübertragungsterminal: Benutzerhandbuch

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

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

Table of Contents

Was ist ein Datenübertragungsterminal?	1
Features	1
Die wichtigsten Konzepte	2
Transferteam	2
Personal	3
Einrichtungen	3
Überlegungen zur Terminplanung	3
Anwendungsfälle	4
Zugehörige Services	5
Technische Anforderungen	6
Ausrüstung	6
Netzwerkanforderungen	6
Leistungsoptimierung	7
Weitere Informationen	8
Erste Schritte	9
Melden Sie sich an für ein AWS-Konto	9
Erstellen eines Benutzers mit Administratorzugriff	10
Vereinbaren Sie eine Reservierung	12
Erstellen Sie ein Transferteam	12
Aktualisierung der Transferteams auf Ihrem Data Transfer Terminal-Konto	13
Personal hinzufügen	14
Aktualisierung des Personals auf Ihrem Data Transfer Terminal-Konto	14
Reservierungsdetails angeben	15
Überprüfen und bestätigen Sie Ihre Reservierung	17
Änderungen an Ihrer Reservierung vornehmen	17
Führen Sie eine Datenübertragung durch	18
Was muss ich mitbringen	18
Die physische Adresse des Datenübertragungsterminals	18
Zugang zum Gebäude	19
Erwartete Ausrüstung in der Data Transfer Terminal Suite.	19
Problembehandlung bei Netzwerkverbindungen	20
Probleme mit der Verbindung von Geräten	20
Fehlerbehebung bei Verbindungen	20
Linux/Unix	21

Windows	22
Netzwerkdurchsatz	22
Sicherheit	24
Datenschutz	25
Datenverschlüsselung	26
Verschlüsselung während der Übertragung	26
Schlüsselverwaltung	27
Datenschutz für den Datenverkehr zwischen Netzwerken	28
Identity and Access Management	28
Zielgruppe	28
Authentifizierung mit Identitäten	29
Verwalten des Zugriffs mit Richtlinien	33
So funktioniert Data Transfer Terminal mit IAM	36
Beispiele für identitätsbasierte Richtlinien	43
Fehlerbehebung	47
API-Referenzen	48
Compliance-Validierung	52
Ausfallsicherheit	53
CloudTrail Logs	54
Informationen zum Datenübertragungsterminal in CloudTrail	54
Grundlegendes zu den Einträgen in der Protokolldatei des Data Transfer Terminal	55
Sicherheit der Infrastruktur	55
Dokumentverlauf	57
.....	Iviii

Was ist ein Datenübertragungsterminal?

AWS Das Data Transfer Terminal ist ein netzwerkfähiger, physischer Standort, an den Sie Ihre Datenspeichergeräte für eine schnelle Datenübertragung zu und von Ihrem Dienst mitnehmen können. AWS Cloud Laden Sie aus der Ferne erfasste Daten hoch, um den Zugriff auf remote erfasste Daten zu erleichtern.

Vereinbaren Sie vom aus eine Reservierung an einem unserer physischen Datenübertragungsterminals AWS Management Console, kommen Sie zu Ihrer geplanten Zeit an und laden Sie Ihre Daten mit Ihren eigenen Geräten auf Ihre AWS Cloud Dienste hoch. Nachdem Ihre geplante Reservierung abgeschlossen ist und Sie abreisen, wird die Anlage erneut gesichert und für die nächste geplante Reservierung bereit gemacht.

Note

AWS Das Datenübertragungsterminal ist derzeit nur AWS für Unternehmenskunden verfügbar.

So greifen Sie auf das Data Transfer Terminal zu:

- AWS Konsole des Datenübertragungsterminals: <https://console.aws.amazon.com/datatransferterminal>
- Einrichtungen des Datenübertragungsterminals: Der Standort der Einrichtungen des Datenübertragungsterminals wird angezeigt, sobald eine Reservierung in der Konsole vorgenommen wurde. Weitere Informationen finden Sie unter [Führen Sie eine Datenübertragung durch](#).

Features

Mit dem AWS Data Transfer Terminal können Sie Ihre Daten einfacher von entfernten Standorten aus in Ihren AWS Cloud Dienst übertragen. Im Folgenden sind einige der Vorteile von Data Transfer Terminal für Ihre Anforderungen beim Remote-Upload von Daten aufgeführt:

Sicher, privat und exklusiv

Jedes Datenübertragungsterminal ist ein sicherer, privater Ort, an dem Sie große Datenübertragungen zwischen Ihrem Datenspeichergerät und Ihren AWS Diensten über eine schnelle Netzwerkverbindung durchführen können.

Eine spezielle Reservierungskonsole

Erweitern Sie Ihr Transferteam um qualifiziertes Personal und vereinbaren Sie über die Data Transfer [Terminal-Konsole](#) eine Reservierung für ein AWS Data Transfer Terminal.

Glasfaser-Netzwerkverbindungen

Jedes Datenübertragungsterminal verfügt über zwei 100-Gigabit-Glasfaserverbindungen (Gbit/s) für schnelle Datenuploads und Redundanz. LR4

Steuerung Ihrer Datenspeichergeräte

Sie müssen Ihr Snowball-Gerät nicht versenden und warten, bis Ihre Daten in Ihre AWS Cloud Dienste hochgeladen wurden. Sie kontrollieren Ihre physischen Datenspeichergeräte während des gesamten Datenübertragungsprozesses und bringen Ihre Daten schneller dorthin, wo sie hin müssen.

Die wichtigsten Konzepte

Für die Verwendung des AWS Datenübertragungsterminals muss ein Prozessverantwortlicher eine Reservierung für einen Datenübertragungsterminal-Mitarbeiter vereinbaren. In den folgenden Abschnitten erfahren Sie mehr über die Terminologie des Datenübertragungsterminals.

Themen

- [Transferteam](#)
- [Personal](#)
- [Einrichtungen](#)

Transferteam

Ein Transferteam ist eine Gruppe von Mitarbeitern, die von einem AWS-Konto Eigentümer bestimmt wird und ausgewählt werden kann, um Datenübertragungen im Namen Ihrer Organisation durchzuführen. Die Einrichtung eines Transferteams umfasst die Benennung des Transferteams

und die Festlegung des Personals für das Team. Wir empfehlen Gruppen von vier oder weniger Datenübertragungsspezialisten für eine einzelne Reservierung.

Weitere Informationen finden Sie unter [Reservieren Sie ein Datenübertragungsterminal](#).

Personal

Personal bezieht sich auf Personen, die entweder Reservierungen vornehmen und verwalten oder die Einrichtungen des Datenübertragungsterminals aufsuchen und nutzen können. Das Personal kann entweder Prozessverantwortlicher oder Datenübertragungsspezialist oder beides sein.

Verantwortlicher für den Prozess

Ein Prozesseigentümer ist ein AWS-Konto Eigentümer, der Mitarbeiter zu seinem AWS Data Transfer Terminal-Konto hinzufügen, bearbeiten und daraus entfernen kann.

Spezialist für Datenübertragung

Ein Datenübertragungsspezialist ist eine Person, die sich für Datenupload-Transaktionen an Datenübertragungsterminals wenden kann. Dieses Personal muss vom Prozessverantwortlichen autorisiert und Ihrem AWS Data Transfer Terminal-Konto hinzugefügt werden. Für den Zugriff auf ein Datenübertragungsterminal ist ein von der Regierung ausgestellter Ausweis erforderlich.

Einrichtungen

Datenübertragungsterminals sind Datenknotenpunkte, die sich im gemeinsamen Besitz eines oder mehrerer Dienstanbieter befinden und von diesen verwaltet werden. Für den Zugriff auf die Datenübertragungsterminal-Suite müssen Spezialisten für Datenübertragungsterminals für jede Einrichtung einen von der Regierung ausgestellten Identitätsnachweis vorlegen, der mit ihren Reservierungsaufzeichnungen übereinstimmen muss.

Überlegungen zur Terminplanung

Reservierungen können in der Data Transfer Terminal-Konsole für eine Dauer von ein bis sechs Stunden an jedem Wochentag und das ganze Jahr über vorgenommen werden. Einzelreservierungen können nacheinander geplant werden, wobei zwischen den Reservierungen ein Abstand von mindestens einer Stunde eingehalten werden muss. Alle Reservierungen müssen mindestens 24 Stunden im Voraus erfolgen.

Die Zeit, die für eine Datenübertragung benötigt wird, hängt von der Geschwindigkeit der Upload-Leistung ab. Berücksichtigen Sie bei der Planung und Terminierung Ihrer Reservierung für das Datenübertragungsterminal die folgenden Faktoren, die sich auf die Upload-Leistung auswirken.

Ausrüstung

Einige Geräte können Einstellungen enthalten, die sich auf die Upload-Leistung auswirken können. Die empfohlenen Geschwindigkeiten für die Upload-Leistung finden Sie in Ihren Gerätespezifikationen.

Netzwerkbedingungen

Zeiten mit starkem Netzwerkverkehr wirken sich auf die Geschwindigkeit beim Hochladen von Daten aus und sollten bei der Auswahl eines Zeitpunkts für Ihre Datenübertragungssitzung berücksichtigt werden. Wenn Sie Ihre Datenübertragungssitzung außerhalb der Spitzenzeiten oder zu Zeiten mit geringerer Netzwerkaktivität planen, kann sich Ihre Upload-Geschwindigkeit verbessern.

Größe der Datenübertragung

Die Netzwerkkonnektivität des Data Transfer Terminal ist für große Datenübertragungen konzipiert. Die Größe der übertragenen Daten wirkt sich jedoch darauf aus, wie lange die Sitzung dauert.

Anwendungsfälle

Zwar kann jeder AWS Unternehmenskunde auf das Datenübertragungsterminalsystem zugreifen, in bestimmten Anwendungsszenarien kann es jedoch von größerem Nutzen sein.

Autonomes Fahren und fortschrittliche Fahrerassistenzsysteme (AD/ADAS): Automobilhersteller (OEM) und Zulieferer generieren große Datensätze aus ihren Flotten autonomer Fahrzeuge, die in zahlreichen Metropolen Nordamerika, Europas und der ASEAN betrieben und Daten sammeln. Mit dem Data Transfer Terminal können die von diesen Flottenfahrzeugen gesammelten Daten in den AWS Cloud Dienst hochgeladen und zur Schulung von AD/ADAS-Modellen verwendet werden.

Medien und Unterhaltung: Studios und andere Inhaltsersteller generieren digitale Video- und Audiodateien (AV) häufig an abgelegenen Orten. Es ist wichtig, dass diese AV-Dateien rechtzeitig in die Cloud hochgeladen werden, damit geografisch verteilte Produktions- und Bearbeitungsteams ihre Workflows parallel und in Echtzeit starten können. Durch die Verwendung des Data Transfer Terminal

zum Hochladen von Daten aus der Ferne können die Produktionszeiten verkürzt werden, was sich in geringeren Produktionskosten niederschlägt.

Karten, Photogrammetrie und 3D-Bilder: Organizations, die mit Kartierungs- oder Bildanwendungen arbeiten, sammeln Daten an entfernten Standorten und müssen diese visuellen Dateien zur Analyse oder Schulung in die AWS Cloud hochladen. Das Data Transfer Terminal minimiert die Zeit zwischen der Erfassung und Analyse dieser großen Datenmengen und hilft so, Geodaten up-to-date für Fahrer, Landwirte und andere Nutzer dieser Informationen aufzubewahren.

Zugehörige Services

Die folgenden Informationen AWS-Services bieten ein optimales Erlebnis bei der Verwendung von Data Transfer Terminal.

AWS-Service	Beschreibung
AWS Snowball Edge	AWS Das Data Transfer Terminal ergänzt die Snowball-Produkte, indem es einen Standort für einen schnelleren Upload in Ihre AWS Cloud bietet und so die Wartezeiten für den Zugriff auf Ihre Daten minimiert.
Amazon S3	Bringen Sie Ihr eigenes Gerät zu einem Datenübertragungsterminal, um Ihre Daten schnell und sicher auf Ihren Amazon S3 S3-Service hochzuladen.

Technische Voraussetzungen für die Nutzung des Datenübertragungsterminals

Bevor Sie eine Reservierung an einem Datenübertragungsterminal vereinbaren, müssen Sie sicherstellen, dass Sie über die für die Verbindung mit dem Netzwerk erforderlichen Geräte und Konfigurationen verfügen. Beachten Sie die folgenden Richtlinien für eine optimale Netzwerkkonnektivität und optimale Netzwerkerfahrung.

Ausrüstung

Für Ihre geplante Reservierung müssen Sie tragbare Verbindungsgeräte wie Monitore, eine Tastatur, eine Maus und einen Computer oder Laptop zum Datenübertragungsterminal mitbringen.

Ihre Hardware muss mit Glasfaserverbindungen (L4) funktionieren

Note

Als bewährte Methode zur Datensicherheit sollten Sie sicherstellen, dass Ihre Daten auf den Speichergeräten, die Sie zum Datenübertragungsterminal bringen, verschlüsselt und gesichert sind und dass Sie bei der Nutzung des Datenübertragungsterminals Datenverschlüsselungsrichtlinien anwenden. Weitere Informationen finden Sie unter [Sicherheit des AWS Datenübertragungsterminals](#)

Netzwerkanforderungen

Stellen Sie sicher, dass Ihr hochladendes Gerät, der Server oder die Appliance (Laptop) für die Verbindung mit dem Netzwerk vorbereitet ist und dass es DHCP unterstützt. Für ein optimales Daten-Upload-Erlebnis sollten Sie über Folgendes verfügen:

- Ein optischer 100G-QSFP-Transceiver QSFP28 LR4 (100GBASELR4), der mit den NIC- und LC-Anschlüssen für die Glasfaserkabelverbindungen kompatibel ist, die in der Datenübertragungsterminal-Anlage bereitgestellt werden.
- Automatische Konfiguration der IP-Adresse DHCP aktiviert. DNS-Server werden automatisch von DHCP zugewiesen.
- Up-to-date Software und NIC-Treiber.

Leistungsoptimierung

Beachten Sie die folgenden Empfehlungen, um den Durchsatz bei der Verwendung des AWS Datenübertragungsterminals zu maximieren.

- Empfohlene Hardware:
 - 100-Gbit/s-Netzwerkschnittstellenkarte
 - 16-Kern-CPU
 - 128 GB RAM
 - mehrere NVME-SSD-Laufwerke in einem RAID-Array
- Verwenden Sie die AWS Common Runtime (AWS CRT) -Bibliothek für Uploads mit dem AWS Command Line Interface SDK oder. AWS

Optimieren Sie die Amazon S3 S3-Übertragungseinstellungen, indem Sie die folgenden Parameter konfigurieren. Stellen Sie diese Werte unter dem `s3` Schlüssel der obersten Ebene in der AWS Konfigurationsdatei ein, dem Standardspeicherort `~/.aws/config`.

```
[default]
s3 =
  preferred_transfer_client = crt
  target_bandwidth = 100Gb/s
  max_concurrent_requests = 20
  multipart_chunksize = 16MB
```

Beachten Sie, dass alle Amazon S3 S3-Konfigurationswerte eingerückt und unter dem Schlüssel der obersten Ebene `s3` verschachtelt sind.

- Optional: Sie können die obigen Werte mithilfe des Befehls programmgesteuert festlegen. `aws configure set` Um beispielsweise die obigen Werte für das Standardprofil festzulegen, können Sie stattdessen die folgenden Befehle ausführen:

```
aws configure set default.s3.preferred_transfer_client crt
aws configure set default.s3.target_bandwidth 100Gb/s
aws configure set default.s3.max_concurrent_requests 20
aws configure set default.s3.multipart_chunksize 16MB
```

- Um diese Werte programmgesteuert für ein anderes Profil als das Standardprofil festzulegen, geben Sie das `--profile` Flag an. Um beispielsweise die Konfiguration für ein Profil mit dem Namen `test-profile` festzulegen, führen Sie einen Befehl wie im folgenden Beispiel aus.

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- Aktivieren Sie BBR (Linux) auf dem Gerät, um einen besseren Durchsatz zu erzielen.

```
sysctl -w net.core.default_qdisc=fq  
sysctl -w net.ipv4.tcp_congestion_control=bbp
```

Weitere Informationen

Weitere Informationen zu Amazon S3 AWS S3-Befehlszeilenkonfigurationen zur Optimierung Ihrer Netzwerkkonnektivität und -leistung finden Sie in den folgenden Ressourcen.

- [AWS CLI Amazon S3 S3-Konfiguration](#) in der AWS CLI Befehlsreferenz
- [Verwenden Sie einen leistungsstarken Amazon S3 S3-Client: AWS CRT-basierten Client](#) im Amazon S3 Amazon SDK for Java AppStream
- [Wie optimiere ich die Leistung, wenn AWS CLI ich große Dateien auf Amazon S3 hochlade?](#) im AWS Knowledge Center

Erste Schritte

Beginnen Sie mit der Fernübertragung von Daten zu Ihren AWS Cloud Diensten, indem Sie eine Reservierung in einem der Datenübertragungsterminals vornehmen. Zunächst benötigen Sie Geräte, die vom Datenübertragungsterminal unterstützt werden, und ein AWS Unternehmenskonto.

Lesen Sie den [Technische Voraussetzungen für die Nutzung des Datenübertragungsterminals](#) Abschnitt dieses Handbuchs, bevor Sie eine Reservierung für ein Datenübertragungsterminal vereinbaren, um sicherzustellen, dass Sie über Geräte mit den optimalen Konfigurationen für die Datenübertragung verfügen. Nicht alle Datenspeichergeräte und Netzwerkverbindungsgeräte sind mit den in den Suiten verfügbaren Glasfaser-Netzwerkverbindungen kompatibel.

Wenn Sie sich für anmelden AWS, werden Sie AWS-Konto automatisch für alle Dienste angemeldet AWS, einschließlich des Datenübertragungsterminals. Berechnet werden Ihnen aber nur die Services, die Sie nutzen.

Gehen Sie wie in den folgenden Abschnitten beschrieben vor, um das Data Transfer Terminal einzurichten.

Wenn Sie sich für Data Transfer Terminal anmelden AWS und es einrichten, können Sie optional die Anzeigesprache im ändern AWS Management Console. Weitere Informationen finden Sie unter [Changing the language of the AWS Management Console\(Ändern der Sprache der Konsole\)](#) im Handbuch Erste Schritte mit AWS Management Console .

Sobald Sie ein haben, können AWS-Konto Sie auf das Data Transfer Terminal zugreifen. Weitere Informationen zur Einrichtung und Verwendung des AWS Datenübertragungsterminals finden Sie unter [Reservieren Sie ein Datenübertragungsterminal](#).

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/die-Anmeldung>.
2. Folgen Sie den Online-Anweisungen.

Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscode auf der Telefontastatur.

Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu <https://aws.amazon.com/> gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS Management Console](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter [Benutzerzugriff mit der Standardeinstellung konfigurieren](#).AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal](#).

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

Anweisungen hierzu finden Sie unter [Berechtigungssatz erstellen](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Eine genaue Anleitung finden Sie unter [Gruppen hinzufügen](#) im AWS IAM Identity Center Benutzerhandbuch.

Reservieren Sie ein Datenübertragungsterminal

Um mit der Nutzung des AWS Datenübertragungsterminals beginnen zu können, müssen Sie über ein Konto verfügen AWS-Konto und an Ihrer Datenübertragungsterminal-Konsole unter <https://console.aws.amazon.com/datatransferterminal> angemeldet sein. Sobald Sie bei Ihrer Data Transfer Terminal-Konsole angemeldet sind, können Sie bestehende Reservierungen einsehen oder neue Reservierungen vornehmen. Um eine Reservierung zu vereinbaren, müssen Sie wie folgt vorgehen:

1. Erstellen Sie ein Transferteam. Sie müssen eine bestimmte Benutzergruppe erstellen, um eine Reservierung zu erstellen und auf das Datenübertragungsterminal zuzugreifen, um eine Datenübertragung durchzuführen. Weitere Informationen zu diesem Thema finden Sie unter [Erstellen Sie ein Transferteam](#).
2. Sobald Ihr Team eingerichtet ist, müssen Sie weitere Mitarbeiter hinzufügen. Weitere Informationen zum Hinzufügen von Personal zu Ihrem Transferteam finden Sie unter [Personal hinzufügen](#).
3. Der Prozessverantwortliche kann die Datenübertragung mit den Teams des Kontos planen. Weitere Informationen zum Planen der Reservierung finden Sie unter [Reservierungsdetails angeben](#).
4. Vergewissern Sie sich, dass die Reservierungsdetails korrekt sind, bevor Sie Ihre Anfrage abschicken. Nach dem Absenden kann eine Reservierungsanfrage mindestens 24 Stunden lang nicht geändert werden. Weitere Informationen finden Sie unter [Überprüfen und bestätigen Sie Ihre Reservierung](#).

Sobald Ihre Reservierung bearbeitet und bestätigt wurde, kann Ihr Transferteam zur geplanten Zeit auf das Datenübertragungsterminal zugreifen. Weitere Informationen finden Sie unter [Führen Sie eine Datenübertragung an der Datenübertragungsterminal-Einrichtung durch](#).

Erstellen Sie ein Transferteam

Um auf ein Datenübertragungsterminal zugreifen zu können, müssen Sie eine Reservierung im vereinbaren AWS Management Console. Melden Sie sich AWS-Konto an, um auf die Datenübertragungsterminal-Konsole zuzugreifen, und führen Sie die folgenden Schritte aus, um Ihre Reservierung zu vereinbaren.

1. Wählen Sie auf der Startseite des Data Transfer Terminals die Schaltfläche Erste Schritte aus.

2. Wenn in Ihrem Konto noch kein Transferteam eingerichtet ist, ist die Schaltfläche Reservierung erstellen deaktiviert. Sie müssen zunächst ein Transferteam erstellen und benennen.
 - a. Wählen Sie die Schaltfläche Transferteam erstellen.
 - b. Geben Sie dem Team einen Namen.
 - Der Name muss zwischen zwei und 64 Zeichen lang sein und mit einem Buchstaben oder einer Zahl beginnen.
 - Verwenden Sie nur Buchstaben, Zahlen, Punkte und Bindestriche. Sonderzeichen werden nicht erkannt.
 - Geben Sie keine sensiblen identifizierenden Informationen an.
 - c. Erstellen Sie eine Beschreibung des Transferteams.
 - Geben Sie eine Beschreibung an, anhand derer das Team leichter identifiziert werden kann. Beschreiben Sie beispielsweise den Zweck des Teams für einen bestimmten Zeitraum, eine Kampagne oder ein Projekt.
 - d. Wählen Sie die Schaltfläche Transferteam erstellen.

Sie kehren zur Seite Transferteam zurück und Ihr neu erstelltes Team wird im Bereich Transferteams angezeigt.

Aktualisierung der Transferteams auf Ihrem Data Transfer Terminal-Konto

Informationen zur Einrichtung eines neuen Transferteams finden Sie im [Reservieren Sie ein Datenübertragungsterminal](#) Abschnitt dieses Handbuchs.

Gehen Sie wie folgt vor, um ein Transferteam zu ändern oder zu entfernen:

1. Wählen Sie auf der Seite Transferteams das Transferteam aus, das Sie ändern möchten.
2. Um den Namen und die Beschreibung des Transferteams zu ändern, klicken Sie auf die Schaltfläche Bearbeiten.
3. Um Personal hinzuzufügen oder zu entfernen, wählen Sie die Registerkarte Personal aus und führen Sie die unter Wie ändere ich Personal zu meinem Konto, füge es hinzu oder entferne es von meinem Konto beschriebenen Schritte aus? Abschnitt dieser häufig gestellten Fragen.
4. Informationen zum Hinzufügen oder Stornieren einer Reservierung für das ausgewählte Transferteam finden Sie im [Aktualisierung des Personals auf Ihrem Data Transfer Terminal-Konto](#) Abschnitt dieser häufig gestellten Fragen.

Personal hinzufügen

Erweitern Sie Ihr Transferteam um Prozessverantwortliche und Datenübertragungsspezialisten, um die Datenübertragung einzurichten und auf das Datenübertragungsterminal zuzugreifen. Gehen Sie wie folgt vor, um Ihrem Transferteam Personal hinzuzufügen:

1. Wählen Sie auf der Seite Transferteams die gewünschte Transferteamkarte aus den im Abschnitt Transferteams aufgelisteten Karten aus. Die Übersichtsseite des Transferteams wird angezeigt.
2. Wählen Sie die Registerkarte Personal und dann die Schaltfläche Person registrieren, um Mitarbeiter zum Transferteam hinzuzufügen.
3. Füllen Sie auf der Seite Personal registrieren die Felder mit den erforderlichen Informationen über die Person aus, die Sie dem Transferteam hinzufügen möchten.
 - a. Personal-Alias: Erstellen Sie einen eindeutigen Alias, um die Person zu identifizieren.
 - Der Alias wird verwendet, um Mitarbeiter zu identifizieren und gleichzeitig ihre Identität zu schützen.
 - Er kann bis zu 64 Zeichen lang sein und Buchstaben, Zahlen und Bindestriche enthalten.
 - Sonderzeichen sind nicht zulässig.
 - b. Vorname: Geben Sie den Vornamen der Person so an, wie er auf ihrem amtlichen Ausweis steht.
 - c. Nachname: Geben Sie den Vor- oder Nachnamen der Person an, so wie er auf dem von der Regierung ausgestellten Ausweis steht.
 - d. E-Mail-Adresse: Geben Sie eine gute E-Mail-Adresse an, unter der die Person Reservierungsinformationen und Anweisungen für den Zugang zum Datenübertragungsterminal erhalten kann.
4. Wählen Sie die Schaltfläche Person registrieren, um das Hinzufügen der Person zu Ihrem Transferteam abzuschließen.

Aktualisierung des Personals auf Ihrem Data Transfer Terminal-Konto

Das Ändern vorhandener Mitarbeiter in Ihrem Konto in der Data Transfer Terminal-Konsole wird derzeit nicht unterstützt. AWS Besitzer von Data Transfer Terminal Process können derzeit nur Personal hinzufügen oder löschen.

Gehen Sie wie folgt vor, um Personal aus Ihrem Data Transfer Terminal-Konto zu entfernen:

1. Wählen Sie auf der Seite Transferteams das Transferteam aus, das dem Personal zugeordnet ist, das Sie entfernen möchten.
2. Wählen Sie auf der Übersichtsseite des ausgewählten Transferteams die Registerkarte Personal aus.
3. Klicken Sie auf das Optionsfeld neben dem Alias, den Sie entfernen möchten. Beachten Sie, dass Sie den Alias der Person nur sehen können, wenn Sie ihr Profil löschen.
4. Wählen Sie die Schaltfläche Löschen. Es erscheint eine Warnung zur Bestätigung der beabsichtigten Aktion für das ausgewählte Personal. Klicken Sie auf die Schaltfläche Löschen, um fortzufahren. Oben auf der Konsole erscheint ein Banner, das bestätigt, dass das Personal erfolgreich gelöscht wurde.

Reservierungsdetails angeben

Die folgenden Anweisungen führen Sie Schritt für Schritt durch die Planung Ihrer Reservierung für das Data Transfer Terminal in der AWS Management Console. Informationen zur Verwendung des Datenübertragungsterminals finden Sie unter [Führen Sie eine Datenübertragung durch](#).

1. Wählen Sie auf der Registerkarte Bevorstehende Reservierungen die Schaltfläche Reservierung vornehmen aus.
2. Füllen Sie die Felder auf der Seite Reservierungsdetails angeben aus.
 - a. Auswahl des Transferteams: Das als Standard ausgewählte Transferteam wird zuerst angezeigt. Wenn du ein anderes Team auswählen möchtest, klicke auf den Dropdown-Pfeil, um es aus der Liste der verfügbaren Transferteams auszuwählen.
 - b. Prozessverantwortlicher: Wählen Sie den Personal-Alias aus, der für die Verwaltung der Reservierung verantwortlich sein soll.
 - Für eine Reservierung ist nur ein Prozessverantwortlicher zulässig, und bei diesem muss es sich um einen autorisierten Mitarbeiter Ihres Unternehmens handeln AWS-Konto.

Der Prozessverantwortliche kann auch als einer der Datenübertragungsspezialisten für die Durchführung der Datenübertragungsaktivität hinzugezogen werden.
 - c. Spezialist für Datenübertragung: Wählen Sie das Personal aus, das Zugriff auf das Datenübertragungsterminal haben soll, um die Datenübertragungsaktivität abzuschließen. Sie können je nach Bedarf mehr als ein Personal auswählen.

- Es empfiehlt sich, Ihr Transferteam auf nicht mehr als vier (4) Datenübertragungsspezialisten zu beschränken.
- d. Informationen zum Datenübertragungsterminal: Geben Sie die Einrichtung des Datenübertragungsterminals, das gewünschte Datum und die genaue Uhrzeit für die Datenübertragungssitzung an.
- i. Einrichtung des Datenübertragungsterminals: Klicken Sie auf den Dropdown-Pfeil, um eine Datenübertragungsterminal-Einrichtung auszuwählen.

 Note

Bei der Reservierung werden nur Beschreibungen der Einrichtungen zur Verfügung gestellt. Zusätzliche Standortinformationen finden Sie in der Reservierungsbestätigungs-E-Mail.

- ii. Datum und Uhrzeit des Datenübertragungsterminals: Klicken Sie in das Feld Datum und Uhrzeit für Ihre Reservierung suchen, um den Kalender anzuzeigen und Ihre Reservierung zu planen.
- Reservierungen müssen mindestens 24 Stunden im Voraus und nicht mehr als sechs (6) Monate im Voraus erfolgen und können nur maximal sechs (6) Stunden dauern. Eine einzelne Reservierung kann sich über mehr als einen Tag erstrecken, um gegebenenfalls Übernachtungsszenarien zu berücksichtigen.
 - Die Uhrzeit wird im 24-Stunden-Format angezeigt und kann nur in Schritten von ganzen Stunden reserviert werden.
 - Um aufeinanderfolgende Reservierungen vorzunehmen, müssen Sie separate Reservierungen mit einem Abstand von mindestens einer Stunde zwischen den einzelnen Datenübertragungssitzungen erstellen.
 - Weitere Informationen finden Sie unter [Überlegungen zur Terminplanung](#).
3. Bestätigen Sie, dass die Reservierungsdetails korrekt sind, und klicken Sie dann auf die Schaltfläche Erstellen, um fortzufahren. Dadurch gelangen Sie zur Bestätigungsseite, die eine Zusammenfassung Ihrer Reservierung enthält.

Überprüfen und bestätigen Sie Ihre Reservierung

Nachdem Sie die Details Ihrer Reservierung angegeben haben, klicken Sie auf die Schaltfläche Weiter, um zur Übersichtsseite zu gelangen. Überprüfen Sie die Details Ihrer Reservierungsanfrage für das Data Transfer Terminal auf der Seite Überprüfen und erstellen.

- Wenn Sie mit der Anfrage zufrieden sind, klicken Sie auf die Schaltfläche Erstellen.
- Wenn Sie Ihre Reservierung ändern müssen, klicken Sie auf die Schaltfläche Zurück.

Sobald die Reservierungsanfrage eingereicht wurde, erhält der Prozessverantwortliche eine E-Mail mit der Bestätigung, dass die Anfrage eingegangen ist und bearbeitet wird. Sobald die Anfrage genehmigt wurde, bestätigt eine weitere E-Mail die Reservierung und enthält Anweisungen zum Auffinden und Zugreifen auf das Datenübertragungsterminal. Informationen zum Zugriff auf das Datenübertragungsterminal finden Sie unter [Führen Sie eine Datenübertragung durch](#).

Änderungen an Ihrer Reservierung vornehmen

Es gibt eine Bearbeitungszeit von 24 Stunden, bevor Änderungen an Ihrer Reservierungsanfrage für das Data Transfer Terminal vorgenommen werden können.

Rufen Sie nach Ablauf der Bearbeitungszeit in der Konsole die Seite Transferteams auf, um Ihre Reservierung einzusehen, zu bearbeiten oder zu löschen.

1. Suchen Sie die gewünschte Reservierung auf der Karte des Teams und wählen Sie sie aus.
2. Klicken Sie auf das Menü Aktionen und wählen Sie die gewünschte Aktion aus.
 - Ansicht: Wenn Sie die Option „Ansicht“ auswählen, können Sie die Details Ihrer Reservierung einschließlich Datum, Uhrzeit, Ort und zugewiesenem Personal einsehen.
 - Bearbeiten: Sie können die Details der Reservierung ändern, einschließlich Datum, Uhrzeit, Ort und zugewiesenes Personal. Beachten Sie, dass Änderungen 24 Stunden vor dem gewünschten Reservierungsdatum vorgenommen werden müssen und dass die Änderungen nicht sofort akzeptiert und angewendet werden. Ihr Prozessverantwortlicher erhält eine Bestätigung der aktualisierten Anfrage.
 - Löschen: Mit der Option Löschen können Sie Ihre Reservierung stornieren. Die Stornierungsanfrage muss mindestens 24 Stunden vor dem geplanten Reservierungstermin gestellt werden. Der Prozessverantwortliche erhält eine Bestätigung der stornierten Reservierung, sobald die Anfrage genehmigt wurde.

Führen Sie eine Datenübertragung an der Datenübertragungsterminal-Einrichtung durch

Das Datenübertragungsterminal ist ein sicherer, gemeinsam genutzter Standort, der einen sicheren Zugriff auf das AWS Netzwerk ermöglicht. Um auf das Datenübertragungsterminal zugreifen zu können, stellen Sie sicher, dass Sie eine Bestätigungs-E-Mail mit der Beschreibung des Standorts und den Zugangsanweisungen erhalten. Weitere Informationen zum Zugriff auf und zur Nutzung des Datenübertragungsterminals finden Sie in den folgenden Themen.

Themen

- [Was muss ich mitbringen](#)
- [Die physische Adresse des Datenübertragungsterminals](#)
- [Zugang zum Gebäude](#)
- [Erwartete Ausrüstung in der Data Transfer Terminal Suite.](#)

Was muss ich mitbringen

Datenübertragungsspezialisten sollten die für eine Datenübertragung erforderlichen Geräte mitbringen, z. B. einen Laptop, Flash-Laufwerke, Solid-State-Laufwerke (SSDs) und [AWS Snowball Edge](#). Stellen Sie sicher, dass Ihre Ausrüstung für die Verwendung der Glasfasernetzwerkabel am Datenübertragungsterminal optimiert ist. Weitere Informationen zu optimalen Geräten und Konfigurationen finden Sie unter [Technische Voraussetzungen für die Nutzung des Datenübertragungsterminals](#).

Sie sind für die Installation, Verwendung und Demontage der Geräte und Gegenstände verantwortlich, die Sie und die zugehörigen Datenübertragungsspezialisten in die Einrichtung des Datenübertragungsterminals mitbringen. Alles, was mit in die Suite gebracht wird, muss bei der Abreise entfernt werden. AWS Data Transfer Terminal ist nicht verantwortlich für vergessene oder verlorene Gegenstände.

Die physische Adresse des Datenübertragungsterminals

Die physische Adresse des Datenübertragungsterminals wird nicht angegeben. Stattdessen erhalten der in der Reservierung angegebene Prozessverantwortliche und die in der Reservierung

angegebenen Datenübertragungsspezialisten eine E-Mail mit dem durchsuchbaren öffentlichen Namen des Datenübertragungsterminals. AWS Das Datenübertragungsterminal verwendet dasselbe Standortidentifikationssystem, mit dem Sie im Internet nach dem öffentlichen Namen suchen können, um die Einrichtung des Datenübertragungsterminals AWS Direct Connect zu finden. Wenn Sie keine E-Mail mit diesen Informationen haben, bestätigen Sie mit Ihrem AWS Data Transfer Terminal Account Manager, dass Sie zum Transferteam gehören und dass Ihre E-Mail-Informationen korrekt sind.

Zugang zum Gebäude

Um Zugang zum Datenübertragungsterminal zu erhalten, muss jeder Datenübertragungsspezialist einen Identitätsnachweis oder einen von der Regierung ausgestellten Ausweis vorlegen. Sobald Sie das Gebäude betreten haben, begleitet Sie der Sicherheitsdienst zu Ihrer Datenübertragungsterminal-Suite.

Erwartete Ausrüstung in der Data Transfer Terminal Suite.

Jedes Datenübertragungsterminal sollte nur über zwei (2) Glasfaserkabel, einen Tisch oder Schreibtisch und Stühle verfügen. Wenn sich noch andere Geräte oder Gegenstände im Raum befinden, melden Sie dies [Support](#)sofort.

Behebung von Problemen mit der Netzwerkverbindung

Wenn bei der Verwendung des AWS Datenübertragungsterminals Probleme bei der Verbindung mit dem Netzwerk auftreten, z. B. wenn Sie keine Internetverbindung herstellen können oder die Verbindungsgeschwindigkeit langsam ist, sollten Sie die folgenden Tipps zur Problembehandlung beachten.

Themen

- [Probleme mit der Verbindung von Geräten](#)
- [Fehlerbehebung bei Verbindungen](#)
- [Netzwerkdurchsatz](#)

Probleme mit der Verbindung von Geräten

Wenn Sie in der Data Transfer Terminal Suite Schwierigkeiten haben, eine physische Verbindung herzustellen, sollten Sie Folgendes beachten:

- Jede Datenübertragungsterminaleinrichtung wird über zwei (2) Singlemode-LC-Glasfaserkabel verfügen. Wenn eines oder beide Kabel fehlen, wenden Sie sich sofort an den [AWS Support](#).
- Wenn ein Glasfaserkabel nicht funktioniert, versuchen Sie zuerst, das Kabel zu rollen. Wenn Sie immer noch keine Verbindung mit dem ersten Kabel herstellen können, versuchen Sie es mit dem anderen Kabel.

Wenn Sie die Kabel immer noch nicht für die Verbindung verwenden können, wenden Sie sich umgehend an den [AWS Support](#).

Fehlerbehebung bei Verbindungen

Wenn Sie Ihre Geräte anschließen können, aber keine Verbindung zum Netzwerk herstellen können, versuchen Sie es mit den folgenden Vorschlägen zur Problembehebung.

- Vergewissern Sie sich, dass Ihre Gerätekonfiguration die angegebenen Netzwerkanforderungen erfüllt. Weitere Informationen finden Sie unter [Technische Voraussetzungen für die Nutzung des Datenübertragungsterminals](#).
- Wechseln Sie zu dem anderen Glasfaserkabel, um eine Verbindung herzustellen.

- Starten Sie Ihr Gerät neu, während Sie die Glasfaserkabel angeschlossen lassen.
- Führen Sie grundlegende Netzwerkdiagnosen am Gerät durch, um Folgendes sicherzustellen:
 - DHCP ist aktiviert
 - Der verbundenen Netzwerkschnittstelle ist eine IP-Adresse zugewiesen
 - DNS-Server sind konfiguriert
 - Die Systemuhr ist mit NTP synchronisiert

Wenn Sie immer noch keine Verbindung herstellen können, wenden Sie sich an den [AWS Support](#) und stellen Sie ihm die folgenden Ausgaben zur Verfügung, je nachdem, welches Betriebssystem (OS) auf Ihrem Gerät ausgeführt wird.

Linux/Unix

- Rufen Sie IP-Adressen und Routing-Informationen in einem Terminal oder einer Befehlszeilenschnittstelle (CLI) ab. Stellen Sie sicher, dass der Netzwerkschnittstelle eine IP-Adresse zugewiesen ist und dass der Routentabelle eine Standardroute mit einer Standard-Gateway-Adresse hinzugefügt wurde.

```
ip address show
ip route show
```

- Wenn es nicht auf dem Gerät installiert `iproute2` ist und `ip` Befehle nicht verfügbar sind, verwenden Sie alternativ die folgenden Befehle:

```
ifconfig
netstat -rn
```

- Sammeln Sie DNS-Serverinformationen. Hier sollten zwei IP-Adressen angezeigt werden, die mit dem `nameserver` Schlüsselwort beginnen.

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

- Sammeln Sie die Ergebnisse der grundlegenden Konnektivitätstests. Ersetzen Sie die `default_gateway_address` durch die IP-Adresse des zugewiesenen Standard-Gateways.

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
```

```
tracert s3.amazonaws.com
```

- Sammeln Sie die Ergebnisse des HTTPS-Konnektivitätstests. Der folgende Befehl sollte eine HTTP 200 OK Antwort von Amazon S3 anzeigen.

```
curl -i https://s3.amazonaws.com/ping
```

Windows

- Rufen Sie die IP-Adresse, das Routing und die DNS-Serverinformationen in der Befehlszeile ab. Stellen Sie sicher, dass der Netzwerkschnittstelle eine IP-Adresse und zwei DNS-Server zugewiesen sind und dass der Routentabelle eine Standardroute mit einer Standard-Gateway-Adresse hinzugefügt wurde.

```
ipconfig /all  
route print
```

- Erfassen Sie die Ergebnisse der grundlegenden Konnektivitätstests in der Befehlszeile. Ersetzen Sie das `default_gateway_address` durch die IP-Adresse des zugewiesenen Standard-Gateways.

```
ping <default_gateway_address>  
ping s3.amazonaws.com  
tracert s3.amazonaws.com
```

- Sammeln Sie die Ergebnisse des HTTPS-Konnektivitätstests unter PowerShell. Der folgende Befehl sollte eine HTTP 200 OK Antwort anzeigen.

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

Netzwerkdurchsatz

Der Netzwerkdurchsatz, der die tatsächliche Datenübertragungsrate in einem Netzwerk misst, kann durch verschiedene Faktoren beeinflusst werden. Folgendes kann sich auf Ihre Datenübertragungsgeschwindigkeiten auswirken:

- **Hardware:** Die Hardwarekomponenten des Geräts können zu verringerten Verbindungsgeschwindigkeiten beim Hochladen von Daten führen. Die im Gerät verwendete CPU und die Festplatten könnten an ihre Leistungsgrenzen stoßen. Erwägen Sie die Verwendung von NVME SSDs in einem RAID-Array. Stellen Sie sicher, dass Sie die AWS CRT-Bibliothek verwenden, um eine bessere Leistung zu erzielen und die CPU-Auslastung zu senken.
- **Verschlüsselungsaufwand:** Sichere Übertragungen wie HTTPS erhöhen die Verarbeitungszeit aufgrund des Verschlüsselungsaufwands.
- **Latenz:** Latenz bezieht sich auf die Zeit, die ein Datenpaket benötigt, um von der Quelle zum Ziel zu gelangen. Beim Hochladen in einen Amazon S3 S3-Bucket in einer anderen geografischen Region kann eine hohe Latenz beobachtet werden, was zu Verzögerungen bei der Datenübertragung und einem geringeren Durchsatz führen kann. Es hat sich bewährt, Datenübertragungen innerhalb derselben Region durchzuführen, wann immer dies möglich ist.
- **Paketverlust:** Verlorene Pakete müssen erneut übertragen werden, wodurch die Datenübertragung verlangsamt wird.

Sicherheit des AWS Datenübertragungsterminals

AWS Das Datenübertragungsterminal bietet eine sichere Umgebung für Datenübertragungen zum und vom AWS Cloud. Wie jede andere physische Netzwerkglasfaserverbindung bietet auch die Datenübertragungsterminal-Verbindung keine Standardverschlüsselung. Daher sind Sie dafür verantwortlich, die bewährten Methoden zur Datenverschlüsselung durchzusetzen, um sicherzustellen, dass Ihre Datenübertragung sicher ist.

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

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der [AWS](#) . Weitere Informationen zu den Compliance-Programmen, die für AWS Data Transfer Terminal gelten, finden Sie unter [AWS Services im Umfang nach Compliance-Programm AWS](#) .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Data Transfer Terminal anwenden können. In den folgenden Themen erfahren Sie, wie Sie Ihre Daten bei der Nutzung des Data Transfer Terminal-Dienstes sichern können. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, mit denen Sie Ihre Data Transfer Terminal-Ressourcen überwachen und sichern können.

Themen

- [Datenschutz im AWS Datenübertragungsterminal](#)
- [Identitäts- und Zugriffsmanagement für das Datenübertragungsterminal](#)
- [Überprüfung der Einhaltung der Vorschriften für das AWS Datenübertragungsterminal](#)
- [Belastbarkeit des AWS Datenübertragungsterminals](#)

- [Protokollierung und Überwachung im Datenübertragungsterminal](#)
- [Sicherheit der Infrastruktur im AWS Datenübertragungsterminal](#)

Datenschutz im AWS Datenübertragungsterminal

Das AWS [Modell](#) der mit gilt für den Datenschutz im AWS Data Transfer Terminal. Wie in diesem Modell beschrieben, AWS ist es verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter [Arbeiten mit CloudTrail Pfaden](#) im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-3](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit dem Data Transfer Terminal oder anderen Geräten AWS-Services über die Konsole, API oder arbeiten. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

AWS Das Data Transfer Terminal bietet Zugriff auf eine Hochgeschwindigkeits-Netzwerkverbindung, über die Sie Daten sicher zwischen selbstverwalteten Speichersystemen und AWS Speicherdiensten übertragen können. Wie Ihre Speicherdaten bei der Übertragung verschlüsselt werden, hängt zum Teil von den auf Ihren Geräten aktivierten Richtlinien und den Diensten ab, an die Ihre Daten übertragen werden. Die Verwaltung der Daten und deren Verschlüsselung bei der Übertragung liegen in der Verantwortung der Person, die das Data Transfer Terminal verwendet.

Verschlüsselung im Ruhezustand

AWS Das Datenübertragungsterminal verschlüsselt alle Daten im Ruhezustand.

Das Datenübertragungsterminal erfasst nur Daten, die für Reservierungen erforderlich sind, einschließlich der Vor- und Nachnamen sowie der E-Mail-Adressen der Personen, die sowohl für die Teilnahme als auch für die Buchung der Reservierung angegeben wurden. Der Zweck dieser Datenerfassung besteht darin, die Reservierungsdetails zu bestätigen und den Zugang zum Zimmer für die Durchführung der Datenübertragung sicherzustellen. Diese Transaktionsinformationen werden nicht länger als 35 Tage gesichert, AWS Kontoinformationen werden jedoch 10 Jahre lang aufbewahrt.

Verschlüsselung während der Übertragung

AWS Das Datenübertragungsterminal verschlüsselt keine Daten während der Übertragung. Daten entstehen encrypted-in-transit, wenn Sie mit den API-Endpunkten des Data Transfer Terminal interagieren, um Transferteams einzurichten, Personal hinzuzufügen und Reservierungen in der Konsole zu planen. Im Rahmen des Modells AWS mit geteilter Verantwortung haben Sie die Wahl, wie Sie über das Data Transfer Terminal eine Verbindung herstellen. AWS-Services Wir

empfehlen Ihnen dringend, sich für die AWS-Services Verwendung von starken encryption-in-transit Verbindungen wie TLS 1.2 und 1.3 zu entscheiden.

Verwenden Sie beispielsweise nur verschlüsselte Verbindungen über HTTPS (TLS), indem Sie die [aws:SecureTransport](#) Bedingung in Ihren Amazon S3 S3-Bucket-Richtlinien verwenden, wie in der Bucket-Richtlinie unten dargestellt.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "RestrictToTLSRequestsOnly",
    "Action": "s3:",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/"
    ],
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    },
    "Principal": "*"
  }]
}
```

Weitere Informationen zur Datenverschlüsselung bei der Übertragung mit anderen AWS-Services, z. B. Amazon S3, finden Sie unter [Schützen von Daten mit serverseitiger Verschlüsselung](#) im Amazon S3 S3-Benutzerhandbuch.

Schlüsselverwaltung

AWS Das Data Transfer Terminal unterstützt vom Kunden verwaltete Schlüssel nicht direkt. Verwenden Sie den Support für vom Kunden verwaltete Schlüssel, der für die AWS Dienste verfügbar ist, mit denen Sie während Ihrer Reservierung des Data Transfer Terminals eine Verbindung herstellen. Weitere Informationen zu vom Kunden verwalteten Schlüsseln und zur Verschlüsselung Ihrer gespeicherten Daten finden Sie im Abschnitt [AWS KMS-Schlüssel](#) im [AWS Key Management Service Developer Guide](#).

Datenschutz für den Datenverkehr zwischen Netzwerken

Der Zugriff auf die Data Transfer Terminal-Konsole erfolgt über einen veröffentlichten Dienst APIs. Die Ressourcen des Datenübertragungsterminals sind unabhängig von der Virtual Private Cloud (VPC).

Identitäts- und Zugriffsmanagement für das Datenübertragungsterminal

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

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert Data Transfer Terminal mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal AWS](#)
- [Problembehandlung bei der Identität und dem Zugriff auf das AWS Datenübertragungsterminal](#)
- [API-Referenzen für Datenübertragungsterminals: Aktionen und Ressourcen](#)

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie im Data Transfer Terminal ausführen.

Dienstbenutzer — Wenn Sie den Data Transfer Terminal-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr Funktionen von Data Transfer Terminal 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 in Data Transfer Terminal nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter [Problembehandlung bei der Identität und dem Zugriff auf das AWS Datenübertragungsterminal](#).

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen des Data Transfer Terminal verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Data Transfer Terminal. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen des Data Transfer Terminal Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Data Transfer Terminal verwenden kann, finden Sie unter [So funktioniert Data Transfer Terminal mit IAM](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Data Transfer Terminal schreiben können. Beispiele für identitätsbasierte Richtlinien von Data Transfer Terminal, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal AWS](#)

Authentifizierung mit Identitäten

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

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

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS 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 zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen

kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter [AWS Signature Version 4 für API-Anforderungen](#) im IAM-Benutzerhandbuch.

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

AWS-Konto Root-Benutzer

Wenn Sie 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. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

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

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu

IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen 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 [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie [von einer Benutzer- zu einer IAM-Rolle \(Konsole\) wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Methoden für die Übernahme einer Rolle](#) im IAM-Benutzerhandbuch.

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

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert,

so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter \(Verbund\)](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle – Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

- **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer Service-Verknüpfung ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-Verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Auf Amazon ausgeführte Anwendungen EC2** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden](#).

Verwalten des Zugriffs mit Richtlinien

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

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

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

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter [Auswählen zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

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

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

Zugriffskontrolllisten (ACLs)

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

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

Weitere Richtlinientypen

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

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Dienststeuerungsrichtlinien (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations Benutzerhandbuch.
- **Ressourcenkontrollrichtlinien (RCPs)** — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich

auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter [Resource Control Policies \(RCPs\)](#) im AWS Organizations Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

So funktioniert Data Transfer Terminal mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf das Data Transfer Terminal verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit Data Transfer Terminal verfügbar sind.

IAM-Feature	Unterstützung für das Data Transfer Terminal
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein

IAM-Feature	Unterstützung für das Data Transfer Terminal
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Nein
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie Data Transfer Terminal und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für Data Transfer Terminal

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal

Beispiele für identitätsbasierte Richtlinien von Data Transfer Terminal finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal AWS](#)

Ressourcenbasierte Richtlinien im Data Transfer Terminal

Unterstützt ressourcenbasierte Richtlinien: Nein

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

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

Richtlinienaktionen für das Datenübertragungsterminal

Unterstützt Richtlinienaktionen: Ja

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

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

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

Eine Liste der Data Transfer Terminal-Aktionen finden Sie unter [Von AWS Data Transfer Terminal definierte Aktionen](#) in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen im Data Transfer Terminal wird vor der Aktion das folgende Präfix verwendet:

```
datatransferterminal
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte Richtlinien von Data Transfer Terminal finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal AWS](#)

Richtlinienressourcen für das Datenübertragungsterminal

Unterstützt Richtlinienressourcen: Ja

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

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

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

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

Eine Liste der Datentransfer-Terminal-Ressourcentypen und der zugehörigen ARNs Typen finden Sie unter [Von AWS Data Transfer Terminal definierte Ressourcen](#) in der Serviceautorisierungsreferenz. Informationen zu den Aktionen, mit denen Sie den ARN jeder Ressource angeben können, finden Sie unter [Vom AWS Data Transfer Terminal definierte Aktionen](#).

Beispiele für identitätsbasierte Richtlinien von Data Transfer Terminal finden Sie unter. [Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal AWS](#)

Bedingungsschlüssel für Richtlinien für das Datenübertragungsterminal

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

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

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

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

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel für das Data Transfer Terminal finden Sie unter [Bedingungsschlüssel für das AWS Data Transfer Terminal](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Von AWS Data Transfer Terminal definierte Aktionen](#).

Beispiele für identitätsbasierte Richtlinien von Data Transfer Terminal finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal AWS](#)

ACLs im Datenübertragungsterminal

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 Datenübertragungsterminal

Unterstützt ABAC (Tags in Richtlinien): Nein

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

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

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im 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 ABAC finden Sie unter [Definieren von Berechtigungen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit dem Data Transfer Terminal

Unterstützt temporäre Anmeldeinformationen: Ja

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

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln von einer Benutzerrolle zu einer IAM-Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Serviceübergreifende Prinzipalberechtigungen für Data Transfer Terminal

Unterstützt Forward Access Sessions (FAS): Nein

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

Dienstrollen für das Datenübertragungsterminal

Unterstützt Servicerollen: Nein

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

 Warning

Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität des Data Transfer Terminal beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn Data Transfer Terminal Sie dazu anleitet.

Dienstbezogene Rollen für Data Transfer Terminal

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer [AWS-Service](#) verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

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

Beispiele für identitätsbasierte Richtlinien für Data Transfer Terminal AWS

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Data Transfer Terminal-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien \(Konsole\)](#) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden, einschließlich des Formats von ARNs für jeden der Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Data Transfer Terminal](#) in der Referenz zur Serviceautorisierung.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Data Transfer Terminal-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

Bewährte Methoden für Richtlinien

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

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn

diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation
B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.

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

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Data Transfer Terminal-Konsole

Um auf die AWS Data Transfer Terminal-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Data Transfer Terminal-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

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

Um sicherzustellen, dass Benutzer und Rollen die Data Transfer Terminal-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch das Data Transfer Terminal *ConsoleAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter [Hinzufügen von Berechtigungen zu einem Benutzer](#) im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam: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": "*"
    }
  ]
}
```

Problembehandlung bei der Identität und dem Zugriff auf das AWS Datenübertragungsterminal

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Data Transfer Terminal und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion im Data Transfer Terminal auszuführen](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Data Transfer Terminal-Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion im Data Transfer Terminal auszuführen

Wenn Sie Reservierungen in der AWS Data Transfer Terminal-Konsole nicht anzeigen oder planen können, verfügen Sie möglicherweise nicht über die erforderlichen Berechtigungen. Wenden Sie sich an Ihren Kontoadministrator, um eine IAM-Identitätsrichtlinie zu konfigurieren, die Ihnen Zugriff und entsprechende Berechtigungen gewährt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Data Transfer Terminal-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 Data Transfer Terminal diese Funktionen unterstützt, finden Sie unter [So funktioniert Data Transfer Terminal mit IAM](#)
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).

- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

API-Referenzen für Datenübertragungsterminals: Aktionen und Ressourcen

Bei der Erstellung von AWS Identity and Access Management (IAM-) Richtlinien kann Ihnen diese Seite helfen, die Beziehung zwischen den API-Vorgängen des AWS Data Transfer Terminal, den entsprechenden Aktionen, für deren Ausführung Sie Berechtigungen erteilen können, und den AWS Ressourcen, für die Sie die Berechtigungen erteilen können, zu verstehen.

Im Allgemeinen gehen Sie wie folgt vor, um Data Transfer Terminal-Berechtigungen zu Ihrer Richtlinie hinzuzufügen:

- Geben Sie eine Aktion im Action Element an. Der Wert beinhaltet ein `datatransferterminal:` Präfix und den Namen der API-Operation. Beispiel, `datatransferterminal:CreateTask`.
- Geben Sie eine AWS Ressource an, die sich auf die Aktion im Resource Element bezieht.

Sie können AWS Bedingungsschlüssel auch in Ihren Data Transfer Terminal-Richtlinien verwenden. Eine vollständige Liste der AWS Schlüssel finden Sie unter [Verfügbare Schlüssel](#) im IAM-Benutzerhandbuch.

API-Operationen des Datenübertragungsterminals und entsprechende Aktionen

CreateTransferTeam

Aktion: `datatransferterminal:CreateTransferTeam`

Ressource: `None`

GetTransferTeam

Aktion: `datatransferterminal:GetTransferTeam`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

UpdateTransferTeam

Aktion: `datatransferterminal:UpdateTransferTeam`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

DeleteTransferTeam

Aktion: `datatransferterminal>DeleteTransferTeam`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

ListTransferTeams

Aktion: `datatransferterminal>ListTransferTeams`

Ressource: `None`

RegisterPerson

Aktion: `datatransferterminal:RegisterPerson`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

GetPerson

Aktion: `datatransferterminal:GetPerson`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId/person/PersonId`

Abhängige Aktion: `datatransferterminal:GetTransferTeam`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

DeregisterPerson

Aktion: `datatransferterminal:DeregisterPerson`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId/person/PersonId`

Abhängige Aktion: `datatransferterminal:GetTransferTeam`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

ListPersons

Aktion: `datatransferterminal:ListPersons`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

CreateReservation

Aktion: `datatransferterminal:CreateReservation`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

Abhängige Aktion: `datatransferterminal:GetTransferTeam`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

Abhängige Aktion: `datatransferterminal:GetPerson`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId/person/PersonId`

Abhängige Aktion: `datatransferterminal:GetFacility`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal::Region:Account:transfer-team/TransferTeamId/facility/FacilityId`

GetReservation

Aktion: `datatransferterminal:GetReservation`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId/reservation/ReservationId`

Abhängige Aktion: `datatransferterminal:GetTransferTeam`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

UpdateReservation

Aktion: `datatransferterminal:UpdateReservation`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId/reservation/ReservationId`

Abhängige Aktion: `datatransferterminal:GetTransferTeam`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

Abhängige Aktion: `datatransferterminal:GetPerson`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId/person/PersonId`

DeleteReservation

Aktion: `datatransferterminal>DeleteReservation`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId/person/PersonId`

Abhängige Aktion: `datatransferterminal:GetTransferTeam`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

ListReservations

Aktion: `datatransferterminal>ListReservations`

Ressource: `arn:aws::Partition:datatransferterminal:Region:Account:transfer-team/TransferTeamId`

ListFacilities

Aktion: `datatransferterminal>ListFacilities`

Ressource: `None`

GetFacility

Aktion: `datatransferterminal:GetFacility`

Ressource: `arn:aws::Partition:datatransferterminal:::facility/FacilityId`

GetFacilityAvailability

Aktion: `datatransferterminal:GetFacilityAvailability`

Ressource: `arn:aws::Partition:datatransferterminal:::facility/FacilityId/availability`

Abhängige Aktion: `datatransferterminal:GetFacility`

Abhängige Ressource: `arn:aws::Partition:datatransferterminal:::facility/FacilityId/availability`

Überprüfung der Einhaltung der Vorschriften für das AWS Datenübertragungsterminal

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Compliance und Governance im Bereich Sicherheit](#) – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- [Referenz für berechnigte HIPAA-Services](#) – Listet berechnigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmapen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und

die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.

- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#)— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steurelementreferenz](#).
- [Amazon GuardDuty](#) — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Belastbarkeit des AWS Datenübertragungsterminals

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

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

AWS Das Datenübertragungsterminal ist an Standorten auf der ganzen Welt verfügbar. Sie können eine Verbindung zu jedem herstellen, auf AWS-Region das über das Internet zugegriffen werden kann.

Protokollierung und Überwachung im Datenübertragungsterminal

AWS Data Transfer Terminal ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes im Data Transfer Terminal bereitstellt. CloudTrail erfasst alle API-Aufrufe für das Data Transfer Terminal als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Data Transfer Terminal-Konsole und Code-Aufrufe an die API-Operationen des Data Transfer Terminal. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für das Data Transfer Terminal. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an das Data Transfer Terminal gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

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

Informationen zum Datenübertragungsterminal in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn im Datenübertragungsterminal eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich der Ereignisse für das Datenübertragungsterminal, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittle die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

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

Alle Aktionen des Data Transfer Terminal werden von protokolliert CloudTrail und sind im [API-Referenzen für Datenübertragungsterminals: Aktionen und Ressourcen](#) Abschnitt dieses Handbuchs dokumentiert.

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

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

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

Grundlegendes zu den Einträgen in der Protokolldatei des Data Transfer Terminal

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 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, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Sicherheit der Infrastruktur im AWS Datenübertragungsterminal

Als verwalteter Service ist AWS Data Transfer Terminal durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper [Amazon Web Services: Sicherheitsprozesse im Überblick](#) beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf das Data Transfer Terminal zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder neuer. Clients müssen außerdem Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Dokumentenverlauf für das Data Transfer Terminal — Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen in den einzelnen Versionen des AWS Data Transfer Terminal User Guide beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Das Startdatum der Originaldokumentation.	Dezember 2024
Layout aktualisieren	Aktualisierungen des Dokumentlayouts und geringfügige Änderungen am Wortlaut und Inhalt.	Januar 2025

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.