POST EDIT. ADDED PROOFREAD. ADDED PP1

AWS Client VPN

AWS Client VPN: POST EDIT. ADDED PROOFREAD. ADDED PP1

Table of Contents

Was ist AWS Client VPN?

AWS Client VPN ist ein verwalteter clientbasierter VPN-Dienst, mit dem Sie sicher auf Ihre AWS Ressourcen und Ressourcen in Ihrem lokalen Netzwerk zugreifen können. Mit Client VPN können Sie von jedem Standort aus über einen OpenVPN-basierten VPN-Client auf Ihre Ressourcen zugreifen.

Inhalt

Funktionen von Client VPN

Client VPN bietet die folgenden Merkmale und Funktionen:

- Sichere Verbindungen – Der Service bietet eine sichere TLS-Verbindung von jedem Standort aus über den OpenVPN-Client.
- Verwalteter Dienst — Es handelt sich um einen AWS verwalteten Dienst, sodass der betriebliche Aufwand für die Bereitstellung und Verwaltung einer VPN-Fernzugriffslösung eines Drittanbieters entfällt.
- Hohe Verfügbarkeit und Elastizität — Die Lösung passt sich automatisch der Anzahl der Benutzer an, die eine Verbindung zu Ihren AWS Ressourcen und lokalen Ressourcen herstellen.
- Authentifizierung – Der Service unterstützt die Client-Authentifizierung mithilfe von Active Directory, die Verbundauthentifizierung und die zertifikatbasierte Authentifizierung.
- Detaillierte Kontrolle – Mit diesem Service können Sie benutzerdefinierte Sicherheitskontrollen implementieren, indem Sie netzwerkbasierte Zugriffsregeln definieren. Diese Regeln können unter Berücksichtigung der Granularität von Active Directory-Gruppen konfiguriert werden. Sie können die Zugriffskontrolle auch mit Sicherheitsgruppen implementieren.
- Benutzerfreundlichkeit — Es ermöglicht Ihnen den Zugriff auf Ihre AWS Ressourcen und lokalen Ressourcen über einen einzigen VPN-Tunnel.

- Verwaltbarkeit – Sie können Verbindungsprotokolle anzeigen, die Details zu Client-Verbindungsversuchen zur Verfügung stellen. Sie können aktive Client-Verbindungen auch verwalten, und zwar mit der Möglichkeit, diese Verbindungen zu beenden.
- Tiefe Integration — Es lässt sich in bestehende AWS Dienste integrieren, einschließlich AWS Directory Service Amazon VPC.

Komponenten von Client VPN

Die wichtigsten Konzepte für Client VPN sind die folgenden:

Client-VPN-Endpunkt

Ein Client VPN-Endpunkt ist die Ressource, die Sie erstellen und konfigurieren, um Client VPN-Sitzungen zu aktivieren und zu verwalten. Es handelt sich hier um den Beendigungspunkt für alle Client-VPN-Sitzungen.

Ziel-Netzwerk

Ein Ziel-Netzwerk ist das Netzwerk, das Sie einem Client VPN-Endpunkt zuordnen. Ein Subnetz aus einer VPC ist ein Ziel-Netzwerk. Durch das Zuordnen eines Subnetzes zu einem Client VPN-Endpunkt können Sie VPN-Sitzungen einrichten. Sie können mehrere Subnetze einem Client VPN-Endpunkt zuordnen, um eine hohe Verfügbarkeit zu gewährleisten. Alle Subnetze müssen sich in derselben VPC befinden. Jedes Subnetz muss einer anderen Availability Zone angehören.

Route

Jeder Client VPN-Endpunkt verfügt über eine Routing-Tabelle, die die verfügbaren Zielnetzwerkrouten beschreibt. Jede Route in der Routing-Tabelle gibt den Pfad für den Datenverkehr zu bestimmten Ressourcen oder zu Netzwerken an.

Autorisierungsregeln

Eine Autorisierungsregel beschränkt die Benutzer, die auf ein Netzwerk zugreifen können. Sie können für ein bestimmtes Netzwerk die Active Directory- oder Identitätsanbietergruppe konfigurieren, die Zugriff erhalten soll. Nur Benutzer, die dieser Gruppe angehören, können auf das angegebene Netzwerk zugreifen. Standardmäßig gibt es keine Autorisierungsregeln. Sie müssen Autorisierungsregeln konfigurieren, damit Benutzer auf Ressourcen und Netzwerke zugreifen können.

Client

Dies ist der Endbenutzer, der eine Verbindung mit dem Client VPN-Endpunkt herstellt, um eine VPN-Sitzung einzurichten. Die Endbenutzer müssen einen OpenVPN-Client herunterladen und die Client-VPN-Konfigurationsdatei verwenden, die Sie zum Einrichten einer VPN-Sitzung erstellt haben.

CIDR-Bereich des Clients

Ein IP-Adressbereich, aus dem Client-IP-Adressen zugewiesen werden sollen. Jeder Verbindung mit dem Client VPN-Endpunkt wird eine eindeutige IP-Adresse aus dem Client-CIDR-Bereich zugewiesen. Sie wählen den Client-CIDR-Bereich, zum Beispie, `10.2.0.0/16`.

Client-VPN-Ports

AWS Client VPN unterstützt die Ports 443 und 1194 sowohl für TCP als auch für UDP. Der Standard ist Port 443.

Client VPN-Netzwerkschnittstellen

Wenn Sie Ihrem Client VPN-Endpunkt ein Subnetz zuordnen, erstellen wir in diesem Subnetz Client VPN-Netzwerkschnittstellen. Der Datenverkehr, der vom Client VPN-Endpunkt an die VPC gesendet wird, wird über eine Client VPN-Netzwerkschnittstelle gesendet. Anschließend wird die Quell-Netzwerkadressübersetzung (SNAT) angewendet, wobei die Quell-IP-Adresse aus dem CIDR-Bereich des Clients in die Client VPN-Netzwerkschnittstellen-IP-Adresse übersetzt wird.

Verbindungsprotokollierung

Sie können die Verbindungsprotokollierung für Ihren Client VPN-Endpunkt aktivieren, um Verbindungsereignisse zu protokollieren. Sie können diese Informationen verwenden, um forensische Untersuchungen durchzuführen, zu analysieren, wie Ihr Client VPN-Endpunkt verwendet wird, oder Verbindungsprobleme zu debuggen.

Self-Service-Portal

Client VPN bietet Endbenutzern ein Self-Service-Portal als Webseite, auf der sie die neueste Version des AWS-VPN-Desktop-Clients und die neueste Version der Client-VPN-Endpunkt-Konfigurationsdatei herunterladen können, in der die für die Verbindung mit ihrem Endpunkt erforderlichen Einstellungen enthalten sind. Der Client-VPN-Endpunkt-Administrator kann ein Self-Service-Portal für den Client-VPN-Endpunkt aktivieren oder deaktivieren. Das Self-Service-Portal ist ein globaler Service, der durch Service-Stacks in den folgenden Regionen unterstützt wird: USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), Europa (Irland) und AWS GovCloud (USA West).

Arbeiten mit Client VPN

Sie können auf eine der folgenden Arten mit Client VPN arbeiten:

AWS Management Console

Die Konsole bietet eine webbasierte Benutzeroberfläche für Client VPN. Wenn Sie sich für eine registriert haben AWS-Konto, können Sie sich bei der Amazon VPC-Konsole anmelden und im Navigationsbereich Client VPN auswählen.

AWS Command Line Interface (AWS CLI)

Das AWS CLI bietet direkten Zugriff auf die öffentlichen Client-VPN-APIs. Sie wird unter Windows, macOS und Linux unterstützt. Weitere Informationen zu den ersten Schritten mit dem AWS CLI finden Sie im AWS Command Line Interface Benutzerhandbuch. Weitere Informationen zu den Befehlen für Client VPN finden Sie in der AWS CLI -Befehlsreferenz.

AWS Tools for Windows PowerShell

AWS bietet Befehle für eine breite Palette von AWS Angeboten für Benutzer, die in der PowerShell Umgebung Skripts erstellen. Weitere Informationen zu den ersten Schritten mit AWS Tools for Windows PowerShell finden Sie im AWS Tools for Windows PowerShell -Benutzerhandbuch. Weitere Informationen über die cmdlets für Client VPN finden Sie in der AWS Tools for Windows PowerShell -Cmdlet-Referenz.

Abfrage-API

Die Client VPN HTTPS Query API bietet Ihnen programmatischen Zugriff auf Client VPN und AWS. Mit der HTTPS-Query-API können Sie HTTPS-Anforderungen direkt an den Service richten. Wenn Sie die HTTPS-API nutzen, müssen Sie Code zur digitalen Signierung von Anfragen über Ihre Anmeldeinformationen einsetzen. Weitere Informationen finden Sie unter Aktionen für AWS Client VPN.

Preise für Client VPN

Ihnen wird jede Endpunktzuordnung und jede VPN-Verbindung auf Stundenbasis in Rechnung gestellt. Weitere Informationen finden Sie unter AWS Client VPN Preise.

Die Datenübertragung von Amazon EC2 ins Internet wird Ihnen in Rechnung gestellt. Weitere Informationen hierzu erhalten Sie unter Datenübertragung auf der Seite Amazon EC2.

Wenn Sie die Verbindungsprotokollierung für Ihren Client-VPN-Endpunkt aktivieren, müssen Sie in Ihrem Konto eine Protokollgruppe CloudWatch Logs erstellen. Für die Verwendung von Protokollgruppen fallen Gebühren an. Weitere Informationen finden Sie unter CloudWatch Amazon-Preise (wählen Sie unter Bezahlter Tarif die Option Logs aus).

Wenn Sie den Client Connect-Handler für Ihren Client VPN-Endpunkt aktivieren, müssen Sie eine Lambda-Funktion erstellen und aufrufen. Für den Aufruf von Lambda-Funktionen fallen Gebühren an. Weitere Informationen finden Sie unter AWS Lambda Preise.

Client-VPN-Endpunkte sind einem Zielnetzwerk zugeordnet, bei dem es sich um ein Subnetz in einer VPC handelt. Wenn diese VPC über ein Internet Gateway verfügt, verknüpfen wir Elastic IP-Adressen mit den Elastic Network Interfaces (ENIs) des Client-VPN. Diese Elastic IP-Adressen werden als genutzte öffentliche IPv4-Adressen berechnet. Weitere Informationen finden Sie auf der VPC-Preisseite auf der Registerkarte Öffentliche IPv4-Adresse.

Regeln und bewährte Verfahren von AWS Client VPN

Im Folgenden finden Sie die Regeln und bewährten Verfahren für AWS Client VPN

- Pro Benutzerverbindung wird eine Mindestbandbreite von 10 Mbit/s unterstützt. Die maximale Bandbreite pro Benutzerverbindung hängt von der Anzahl der Verbindungen ab, die zum Client-VPN-Endpunkt hergestellt werden.
- Client-CIDR-Bereiche dürfen sich mit dem lokalen CIDR der VPC, in der sich das zugeordnete Subnetz befindet, oder mit Routen, die der Routing-Tabelle des Client VPN-Endpunkts manuell hinzugefügt wurden, nicht überschneiden.
- Client-CIDR-Bereiche müssen eine Blockgröße von mindestens /22 haben und dürfen nicht größer als /12 sein.
- Ein Teil der Adressen im Client-CIDR-Bereich wird zur Unterstützung des Verfügbarkeitsmodells des Client VPN-Endpunkts verwendet und kann Clients nicht zugewiesen werden. Wir empfehlen daher, dass Sie einen CIDR-Block zuweisen, der die doppelte Anzahl von IP-Adressen enthält, die erforderlich sind, um die maximale Anzahl gleichzeitiger Verbindungen zu ermöglichen, die Sie auf dem Client VPN-Endpunkt unterstützen wollen.
- Der Client-CIDR-Bereich kann nicht mehr geändert werden, nachdem Sie den Client VPN-Endpunkt erstellt haben.
- Die Subnetze, die einem Client VPN-Endpunkt zugeordnet sind, müssen sich in derselben VPC befinden.

- Sie können nicht mehrere Subnetze derselben Availability Zone mit einem Client VPN-Endpunkt verknüpfen.
- Ein Client VPN-Endpunkt unterstützt keine Subnetzzuordnungen in einer Dedicated Tenancy-VPC.
- Client VPN unterstützt nur IPv4-Datenverkehr. Siehe Überlegungen zu IPv6 für AWS Client VPN für Details zu IPv6.
- Client VPN ist nicht mit FIPS (Federal Information Processing Standards) konform.
- Das Self-Service-Portal ist nicht für Clients verfügbar, die sich mittels gegenseitiger Authentifizierung authentifizieren.
- Wir empfehlen nicht, über IP-Adressen eine Verbindung zu einem Client-VPN-Endpunkt herzustellen. Da Client VPN ein verwalteter Service ist, kommt es gelegentlich zu Änderungen der IP-Adressen, in die der DNS-Name aufgelöst wird. Darüber hinaus werden in Ihren CloudTrail Protokollen Client-VPN-Netzwerkschnittstellen gelöscht und neu erstellt. Es wird empfohlen, eine Verbindung zu dem Client-VPN-Endpunkt mithilfe des bereitgestellten DNS-Namens herzustellen.
- IP-Weiterleitung wird derzeit nicht unterstützt, wenn Sie die AWS Client VPN Desktop-Anwendung verwenden. IP-Weiterleitung wird von anderen Clients unterstützt.
- Client VPN unterstützt keine multiregionale Replikation in AWS Managed Microsoft AD. Der Client-VPN-Endpunkt muss sich in derselben Region wie die AWS Managed Microsoft AD Ressource befinden.
- Wenn Multi-Faktor-Authentifizierung (MFA) für Ihr Active Directory deaktiviert ist, dürfen Benutzerpasswörter nicht im folgenden Format vorliegen.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Sie können von einem Computer aus keine VPN-Verbindung herstellen, wenn mehrere Benutzer am Betriebssystem angemeldet sind.
- Der Client-VPN-Dienst erfordert, dass die IP-Adresse, mit der der Client verbunden ist, mit der IP übereinstimmt, zu der der DNS-Name des Client-VPN-Endpunkts aufgelöst wird. Mit anderen Worten, wenn Sie einen benutzerdefinierten DNS-Eintrag für den Client-VPN-Endpunkt einrichten und dann den Datenverkehr an die tatsächliche IP-Adresse weiterleiten, auf die der DNS-Name des Endpunkts aufgelöst wird, funktioniert dieses Setup nicht mit kürzlich AWS bereitgestellten Clients. Diese Regel wurde hinzugefügt, um einen Server-IP-Angriff abzuwehren, wie hier beschrieben:. TunnelCrack
- Der Client-VPN-Dienst erfordert, dass die IP-Adressbereiche des lokalen Netzwerks (LAN) der Client-Geräte innerhalb der folgenden standardmäßigen privaten IP-Adressbereiche liegen: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`, oder `169.254.0.0/16`. Wenn festgestellt

wird, dass der LAN-Adressbereich des Clients außerhalb der oben genannten Bereiche liegt, überträgt der Client-VPN-Endpunkt automatisch die OpenVPN-Direktive „redirect-gateway block-local“ an den Client, wodurch der gesamte LAN-Verkehr in das VPN geleitet wird. Wenn Sie während VPN-Verbindungen LAN-Zugriff benötigen, wird daher empfohlen, die oben aufgeführten konventionellen Adressbereiche für Ihr LAN zu verwenden. Diese Regel wird durchgesetzt, um die Wahrscheinlichkeit eines lokalen Netzangriffs zu verringern, wie hier beschrieben:. TunnelCrack

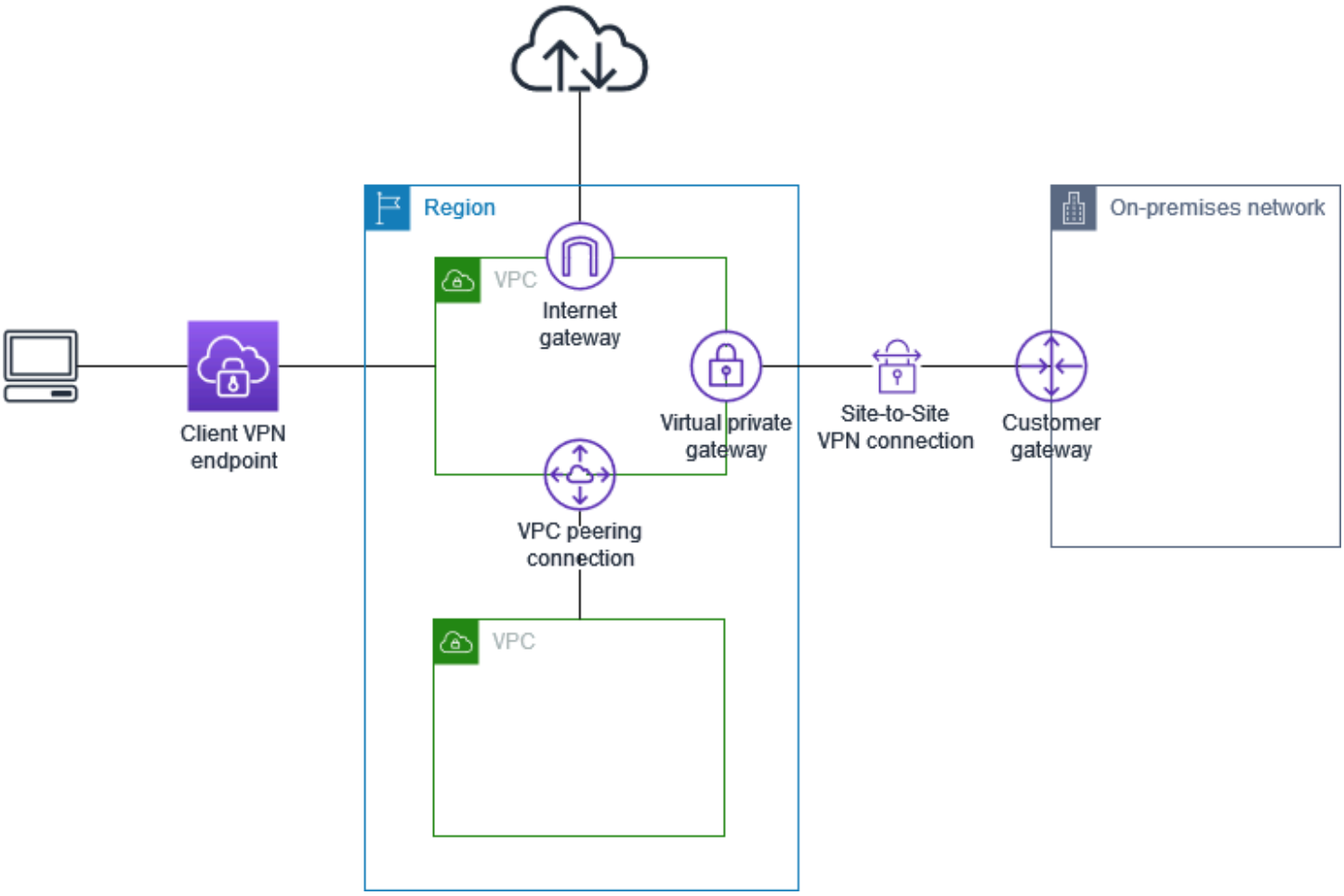
So funktioniert AWS Client VPN

Bei AWS Client VPN gibt es zwei Arten von Benutzern, die mit dem Client-VPN-Endpunkt interagieren: Administratoren und Clients.

Der Administrator ist für das Einrichten und Konfigurieren des Service verantwortlich. Dazu gehört das Erstellen des Client VPN-Endpunkts, das Zuordnen des Zielnetzwerks und das Konfigurieren der Autorisierungsregeln sowie das Einrichten von zusätzlichen Routen (falls erforderlich). Nachdem der Client VPN-Endpunkt eingerichtet und konfiguriert ist, lädt der Administrator die Client VPN-Endpunkt-Konfigurationsdatei herunter und verteilt sie an die Clients, die Zugriff benötigen. Die Client VPN-Endpunktkonfigurationsdatei enthält den DNS-Namen des Client VPN-Endpunkts und Authentifizierungsinformationen, die für eine VPN-Sitzung erforderlich sind. Weitere Informationen zum Festlegen des Service finden Sie unter Erste Schritte mit AWS-Client-VPN.

Der Client ist der Endbenutzer. Dies ist die Person, die eine Verbindung mit dem Client VPN-Endpunkt herstellt, um eine VPN-Sitzung zu erstellen. Der Client erstellt die VPN-Sitzung von seinem lokalen Computer oder Mobilgerät mit einer OpenVPN-basierten VPN-Client-Anwendung. Nachdem er die VPN-Sitzung eingerichtet hat, hat er sicheren Zugriff auf die Ressourcen in der VPC, in der sich das zugeordnete Subnetz befindet. Sie können auch auf andere Ressourcen in AWS oder auf ein Netzwerk oder andere Clients vor Ort zugreifen, wenn die gewünschten Routing- und Autorisierungsregeln konfiguriert wurden. Weitere Informationen zum Herstellen einer Verbindung mit einem Client VPN-Endpunkt für eine VPN-Sitzung finden Sie unter Erste Schritte im AWS-Benutzerhandbuch.

In der folgenden Grafik ist die grundlegende Client VPN-Architektur dargestellt.



Client-Authentifizierung

Die Kundenauthentifizierung wird am ersten Zugangspunkt in die AWS Cloud implementiert. Mit ihrer Hilfe wird ermittelt, ob Clients eine Verbindung mit dem Client VPN-Endpunkt herstellen dürfen. Wenn die Authentifizierung erfolgreich ist, stellen Clients eine Verbindung mit dem Client VPN-Endpunkt her und richtet eine VPN-Sitzung ein. Schlägt die Authentifizierung fehl, wird die Verbindung abgelehnt und der Client kann keine VPN-Sitzung einrichten.

Client VPN unterstützt die folgenden Clientauthentifizierungstypen:

- Active Directory-Authentifizierung (benutzerbasiert)
- Gegenseitige Authentifizierung (zertifikatbasiert)
- Single Sign-On (SAML-basierte Verbundauthentifizierung) (benutzerbasiert)

Sie können eine der oben aufgeführten Methoden allein oder eine Kombination aus gegenseitiger Authentifizierung mit einer benutzerbasierten Methode wie der folgenden verwenden:

- Gegenseitige Authentifizierung und Verbundauthentifizierung
- Gegenseitige Authentifizierung und Active Directory-Authentifizierung

> **Important**
>
> Um einen Client-VPN-Endpunkt zu erstellen, müssen Sie unabhängig von der Art der Authentifizierung AWS Certificate Manager, die Sie verwenden, ein Serverzertifikat bereitstellen. Weitere Informationen zur Erstellung und Bereitstellung eines Serverzertifikats finden Sie unter den Schritten in Gegenseitige Authentifizierung.

Active Directory-Authentifizierung

Client VPN bietet Active Directory-Unterstützung durch Integration mit AWS Directory Service. Mit der Active Directory-Authentifizierung werden Clients anhand vorhandener Active Directory-Gruppen identifiziert. Mithilfe von AWS Directory Service Client VPN kann eine Verbindung zu vorhandenen Active Directorys hergestellt werden, die in AWS oder in Ihrem lokalen Netzwerk bereitgestellt werden. Auf diese Weise können Sie die vorhandene Infrastruktur für die Client-Authentifizierung verwenden. Wenn Sie ein lokales Active Directory verwenden und kein vorhandenes AWS verwaltetes Microsoft AD haben, müssen Sie einen Active Directory Connector (AD Connector) konfigurieren. Sie können einen Active Directory-Server zur Authentifizierung der Benutzer verwenden. Weitere Informationen zur Active-Directory-Integration finden Sie im AWS Directory Service -Administratorhandbuch.

Client VPN unterstützt Multi-Factor-Authentifizierung (MFA), wenn diese für AWS Managed Microsoft AD oder AD Connector aktiviert ist. Wenn MFA aktiviert ist, müssen Clients einen Benutzernamen, ein Passwort und einen MFA-Code angeben, wenn sie sich mit einem Client VPN-Endpunkt verbinden. Weitere Informationen zur Aktivierung von MFA finden Sie unter Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD und Multi-Faktor-Authentifizierung für AD Connector im AWS Directory Service -Administratorhandbuch.

Informationen zu Kontingenten und Regeln zum Konfigurieren von Benutzern und Gruppen in Active Directory finden Sie unter Kontingente für Benutzer und Gruppen.

Gegenseitige Authentifizierung

Bei der gegenseitigen Authentifizierung verwendet Client VPN zur Authentifizierung zwischen Client und Server Zertifikate. Zertifikate sind eine digitale Methode zur Identifizierung. Sie werden von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellt. Der Server verwendet Client-Zertifikate zur Authentifizierung von Clients, wenn sie versuchen, eine Verbindung mit dem Client VPN-Endpunkt herzustellen. Sie müssen ein Serverzertifikat und -schlüssel sowie mindestens ein Client-Zertifikat und -Schlüssel erstellen.

Sie müssen das Serverzertifikat auf AWS Certificate Manager (ACM) hochladen und es angeben, wenn Sie einen Client-VPN-Endpunkt erstellen. Wenn Sie das Serverzertifikat in ACM hochladen, geben Sie auch die Zertifizierungsstelle (Certificate Authority, CA) an. Sie müssen das Client-Zertifikat nur dann in ACM hochladen, wenn die Zertifizierungsstelle des Client-Zertifikats von der Zertifizierungsstelle des Serverzertifikats abweicht. Weitere Informationen zu ACM finden Sie im AWS Certificate Manager -Benutzerhandbuch.

Sie können für jeden Client, der eine Verbindung mit dem Client VPN-Endpunkt herstellt, ein separates Client-Zertifikat und einen separaten Client-Schlüssel erstellen. Auf diese Weise können Sie ein bestimmtes Client-Zertifikat widerrufen, wenn ein Benutzer Ihre Organisation verlässt. In diesem Fall können Sie beim Erstellen des Client VPN-Endpunkts den ARN des Serverzertifikats für das Clientzertifikat angeben, vorausgesetzt, dass das Clientzertifikat von derselben Zertifizierungsstelle wie das Serverzertifikat ausgestellt wurde.

> **Note**
>
> Client VPN-Endpunkte unterstützen bei RSA nur Schlüsselgrößen von 1024-Bit und 2048-Bit. Außerdem muss das Clientzertifikat das CN-Attribut im Feld „Subject“ (Betreff) enthalten. Wenn das vom Client-VPN-Service verwendete Zertifikat aktualisiert wird, entweder durch automatische ACM-Rotation oder manuelles Importieren eines neuen Zertifikats, wird der Client-VPN-Endpunkt mit dem neueren Zertifikat aktualisiert. Dieser ist ein automatisierter Vorgang, der bis zu 24 Stunden dauern kann.

Linux/macOS

Im folgenden Verfahren wird OpenVPN easy-rsa zum Generieren der Server- und Client-Zertifikate sowie der Schlüssel verwendet. Anschließend werden das Serverzertifikat und der Schlüssel nach ACM hochgeladen. Weitere Informationen finden Sie in der Easy-RSA 3 Quickstart README-Datei.

So generieren Sie die Server- und Client-Zertifikate und Schlüssel und laden Sie nach ACM hoch

1. Klonen Sie das OpenVPN easy-rsa Repo auf Ihren On-Premise-Computer und navigieren Sie zum Ordner `easy-rsa/easyrsa3`.

   ```
   $ git clone https://github.com/OpenVPN/easy-rsa.git
   ```

   ```
   $ cd easy-rsa/easyrsa3
   ```

2. Initialisieren Sie eine neue PKI-Umgebung.

   ```
   $ ./easyrsa init-pki
   ```

3. Um eine neue Zertifizierungsstelle (Certificate Authority, CA) zu erstellen, führen Sie diesen Befehl aus und folgen Sie den Anweisungen.

   ```
   $ ./easyrsa build-ca nopass
   ```

4. Generieren Sie das Server-Zertifikat und den Schlüssel.

   ```
   $ ./easyrsa --san=DNS:server build-server-full server nopass
   ```

5. Generieren Sie das Client-Zertifikat und den Schlüssel.

   Stellen Sie sicher, dass das Client-Zertifikat und der private Client-Schlüssel gespeichert werden, da Sie diese zum Konfigurieren des Clients benötigen.

   ```
   $ ./easyrsa build-client-full client1.domain.tld nopass
   ```

   Sie können diesen Schritt optional für jeden Client (Endbenutzer) wiederholen, der ein Client-Zertifikat und einen Schlüssel benötigt.

6. Kopieren Sie das Server-Zertifikat und den Schlüssel sowie das Client-Zertifikat und den Schlüssel in einen benutzerdefinierten Ordner und wechseln Sie dann in den benutzerdefinierten Ordner.

   Bevor Sie die Zertifikate und Schlüssel kopieren, erstellen Sie den benutzerdefinierten Ordner mit dem Befehl `mkdir`. Das folgende Beispiel erstellt einen benutzerdefinierten Ordner in Ihrem Stammverzeichnis.

```
$ mkdir ~/custom_folder/
$ cp pki/ca.crt ~/custom_folder/
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

7. Laden Sie das Server-Zertifikat und den Schlüssel sowie das Client-Zertifikat und den Schlüssel auf ACM hoch. Stellen Sie sicher, dass Sie diese in die Region hochladen, in der Sie den Client VPN-Endpunkt erstellen möchten. Die folgenden Befehle verwenden AWS CLI zum Hochladen der Zertifikate. Informationen zum Hochladen der Zertifikate mit der ACM-Konsole finden Sie unter Importieren eines Zertifikats im AWS Certificate Manager - Benutzerhandbuch.

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

Sie müssen das Clientzertifikat nicht zwangsläufig zu ACM hochladen. Wenn das Server- und das Clientzertifikat von derselben Zertifizierungsstelle (CA) ausgestellt wurden, können Sie den ARN des Serverzertifikats beim Erstellen des Client-VPN-Endpunkts für den Server und den Client verwenden. In den oben aufgeführten Schritten wurden beide Zertifikate mithilfe derselben Zertifizierungsstelle erstellt. Die Schritte zum Hochladen des Clientzertifikats sind jedoch der Vollständigkeit halber enthalten.

Windows

Mit dem folgenden Verfahren wird die Software „Easy-RSA 3.x“ installiert und dazu verwendet, Server- und Clientzertifikate sowie die Schlüssel zu generieren.

So generieren Sie Server- und Client-Zertifikate und Schlüssel und laden Sie nach ACM hoch

1. Öffnen Sie die Seite mit den EasyRSA-Versionen und laden Sie die ZIP-Datei für Ihre Version von Windows herunter und extrahieren Sie sie.

2. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zu dem Speicherort, an den der Ordner „`EasyRSA-3.x`“ extrahiert wurde.
3. Führen Sie den folgenden Befehl aus, um die EasyRSA-3-Shell zu öffnen.

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. Initialisieren Sie eine neue PKI-Umgebung.

```
# ./easyrsa init-pki
```

5. Um eine neue Zertifizierungsstelle (Certificate Authority, CA) zu erstellen, führen Sie diesen Befehl aus und folgen Sie den Anweisungen.

```
# ./easyrsa build-ca nopass
```

6. Generieren Sie das Server-Zertifikat und den Schlüssel.

```
# ./easyrsa --san=DNS:server build-server-full server nopass
```

7. Generieren Sie das Client-Zertifikat und den Schlüssel.

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

   Sie können diesen Schritt optional für jeden Client (Endbenutzer) wiederholen, der ein Client-Zertifikat und einen Schlüssel benötigt.

8. Beenden Sie die EasyRSA-3-Shell.

```
# exit
```

9. Kopieren Sie das Server-Zertifikat und den Schlüssel sowie das Client-Zertifikat und den Schlüssel in einen benutzerdefinierten Ordner und wechseln Sie dann in den benutzerdefinierten Ordner.

   Bevor Sie die Zertifikate und Schlüssel kopieren, erstellen Sie den benutzerdefinierten Ordner mit dem Befehl `mkdir`. Im folgenden Beispiel wird ein benutzerdefinierter Ordner in Ihrem C:\-Laufwerk erstellt.

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
```

```
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. Laden Sie das Server-Zertifikat und den Schlüssel sowie das Client-Zertifikat und den Schlüssel auf ACM hoch. Stellen Sie sicher, dass Sie diese in die Region hochladen, in der Sie den Client VPN-Endpunkt erstellen möchten. Die folgenden Befehle verwenden den AWS CLI , um die Zertifikate hochzuladen. Informationen zum Hochladen der Zertifikate mit der ACM-Konsole finden Sie unter Importieren eines Zertifikats im AWS Certificate Manager - Benutzerhandbuch.

```
aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

Sie müssen das Clientzertifikat nicht zwangsläufig zu ACM hochladen. Wenn das Server- und das Clientzertifikat von derselben Zertifizierungsstelle (CA) ausgestellt wurden, können Sie den ARN des Serverzertifikats beim Erstellen des Client-VPN-Endpunkts für den Server und den Client verwenden. In den oben aufgeführten Schritten wurden beide Zertifikate mithilfe derselben Zertifizierungsstelle erstellt. Die Schritte zum Hochladen des Clientzertifikats sind jedoch der Vollständigkeit halber enthalten.

Erneuerung Ihres Serverzertifikats

Sie können ein abgelaufenes Serverzertifikat erneuern und erneut importieren. Je nachdem, welche Version von OpenVPN easy-rsa Sie verwenden, variiert das Verfahren. Weitere Informationen finden Sie in der Dokumentation zur Verlängerung und zum Widerruf von Easy-RSA 3-Zertifikaten.

Erneuern Sie Ihr Serverzertifikat

1. Führen Sie einen der folgenden Schritte aus:
   - Easy-RSA Version 3.1.x

- Führen Sie den Befehl „certificate renew“ aus.

```
$ ./easyrsa renew server nopass
```

- Easy-RSA versie 3.2.x

a. Führen Sie den Befehl expire aus.

```
$ ./easyrsa expire server
```

b. Signieren Sie ein neues Zertifikat.

```
$ ./easyrsa sign-req server server
```

2. Erstellen Sie einen benutzerdefinierten Ordner, kopieren Sie die neuen Dateien dorthin und navigieren Sie dann in den Ordner.

```
$ mkdir ~/custom_folder2
$ cp pki/ca.crt ~/custom_folder2/
$ cp pki/issued/server.crt ~/custom_folder2/
$ cp pki/private/server.key ~/custom_folder2/
$ cd ~/custom_folder2/
```

3. Importieren Sie die neuen Dateien in ACM. Achten Sie darauf, sie in derselben Region wie den Client-VPN-Endpunkt zu importieren.

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

Single Sign-On (SAML 2.0-basierte Verbundauthentifizierung)

AWS Client VPN unterstützt den Identitätsverbund mit Security Assertion Markup Language 2.0 (SAML 2.0) für Client-VPN-Endpunkte. Sie können Identitätsanbieter (IdPs) verwenden, die SAML 2.0 unterstützen, um zentralisierte Benutzeridentitäten zu erstellen. Anschließend können Sie einen Client VPN-Endpunkt für die Verwendung der SAML-basierten Verbundauthentifizierung konfigurieren und ihn dem IdP zuordnen. Benutzer stellen dann mithilfe ihrer zentralen Anmeldeinformationen eine Verbindung zum Client VPN-Endpunkt her.

Damit Ihr SAML-basierter IdP mit einem Client VPN-Endpunkt funktioniert, müssen Sie die folgenden Schritte ausführen.

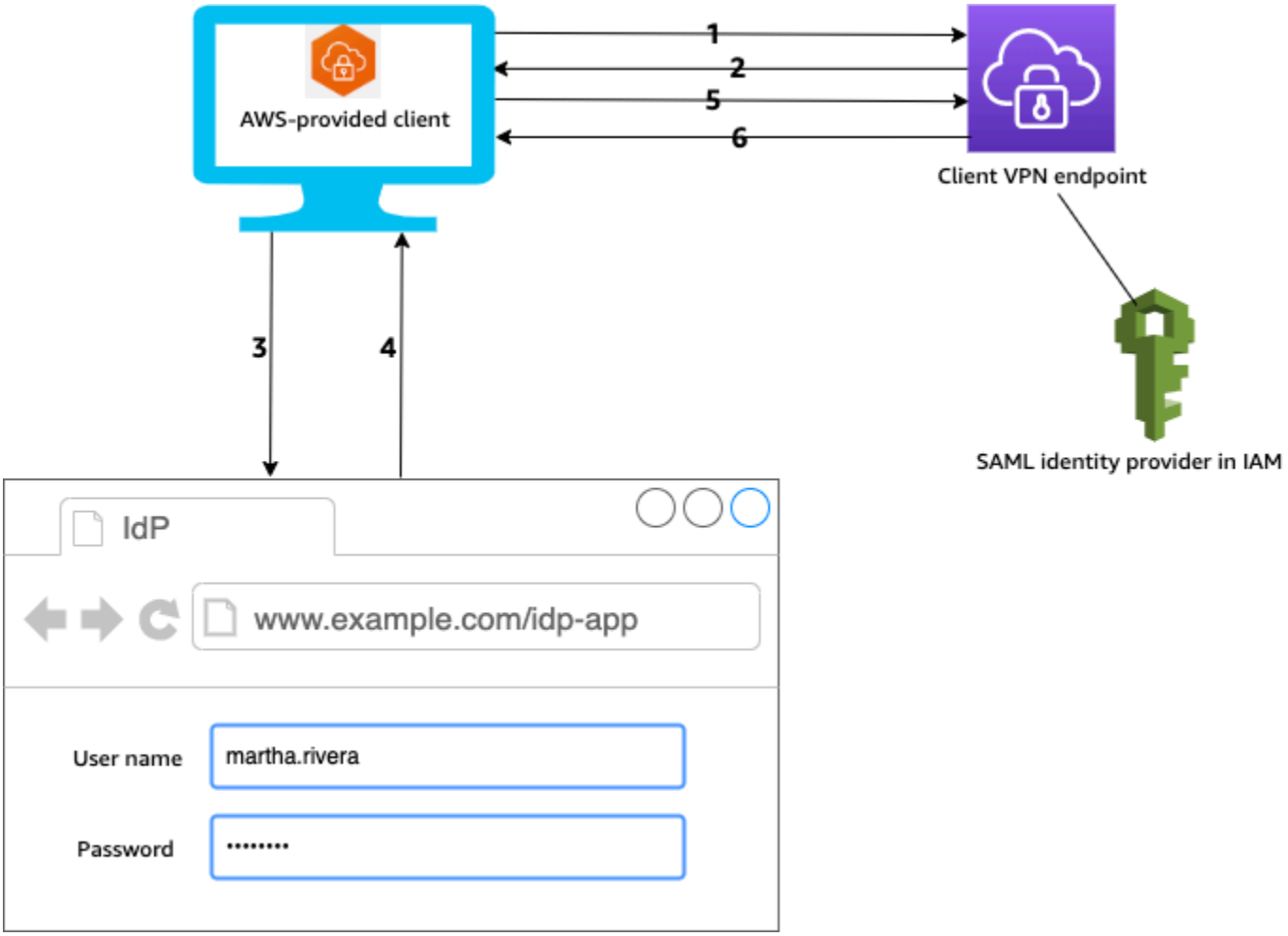
1. Erstellen Sie eine SAML-basierte App in Ihrem ausgewählten IdP, um sie mit einer vorhandenen App zu verwenden AWS Client VPN, oder verwenden Sie eine vorhandene App.
2. Konfigurieren Sie den Identitätsanbieter, um eine Vertrauensbeziehung mit einzurichte AWS. Ressourcen finden Sie unter Konfigurationsressourcen für SAML-basierte IdPs.
3. Generieren Sie in Ihrem IdP ein Verbundmetadatendokument, in dem Ihre Organisation als IdP beschrieben wird, und laden Sie es herunter. Dieses signierte XML-Dokument wird verwendet, um die Vertrauensbeziehung zwischen AWS und dem IdP herzustellen.
4. Erstellen Sie einen IAM-SAML-Identitätsanbieter in demselben AWS Konto wie der Client-VPN-Endpunkt. Der IAM-SAML-Identitätsanbieter definiert die Beziehung zwischen IdP und AWS Trust Ihrer Organisation anhand des vom IdP generierten Metadatendokuments. Weitere Informationen finden Sie unter Erstellen von IAM SAML-Identitätsanbietern im IAM-Benutzerhandbuch.
   Wenn Sie die Anwendungskonfiguration im IdP später aktualisieren, generieren Sie ein neues Metadatendokument und aktualisieren Sie Ihren IAM SAML-Identitätsanbieter.

   > **Note**
   >
   > Sie brauchen keine IAM-Rolle zu erstellen, um den IAM SAML-Identitätsanbieter zu verwenden.

5. Erstellen Sie einen Client VPN-Endpunkt. Legen Sie die Verbundauthentifizierung als Authentifizierungstyp fest und geben Sie den von Ihnen erstellten IAM SAML-Identitätsanbieter an. Weitere Informationen finden Sie unter Erstellen eines Client VPN-Endpunkts.
6. Exportieren Sie die Client-Konfigurationsdatei und verteilen Sie sie an Ihre Benutzer. Weisen Sie Ihre Benutzer an, die neueste Version des von AWS bereitgestellten Clients herunterzuladen und diese zum Laden der Konfigurationsdatei und Herstellen einer Verbindung mit dem Client VPN-Endpunkt zu verwenden. Wenn Sie das Self-Service-Portal für Ihren Client-VPN-Endpunkt aktiviert haben, weisen Sie Ihre Benutzer alternativ an, zum Self-Service-Portal zu gehen, um die Konfigurationsdatei und AWS den bereitgestellten Client abzurufen. Weitere Informationen finden Sie unter Zugriff auf das Self-Service-Portal.

Authentifizierungs-Workflow

Das folgende Diagramm bietet eine Übersicht zum Authentifizierungs-Workflow für einen Client VPN-Endpunkt, der die SAML-basierte Verbundauthentifizierung verwendet. Wenn Sie den Client VPN-Endpunkt erstellen und konfigurieren, geben Sie den IAM SAML-Identitätsanbieter an.



1. Der Benutzer öffnet den AWS bereitgestellten Client auf seinem Gerät und initiiert eine Verbindung zum Client-VPN-Endpunkt.
2. Der Client VPN-Endpunkt sendet eine IdP-URL und eine Authentifizierungsanforderung an den Client zurück (basierend auf den Informationen, die im IAM SAML-Identitätsanbieter bereitgestellt wurden).
3. Der AWS bereitgestellte Client öffnet ein neues Browserfenster auf dem Gerät des Benutzers. Der Browser gibt eine Anfrage an den IdP aus und zeigt eine Anmeldeseite an.
4. Der Benutzer gibt seine Anmeldeinformationen auf der Anmeldeseite ein und der IdP sendet eine signierte SAML-Assertion zurück an den Client.

5. Der AWS bereitgestellte Client sendet die SAML-Assertion an den Client-VPN-Endpunkt.
6. Der Client VPN-Endpunkt validiert die Assertion und erlaubt oder verweigert dem Benutzer den Zugriff.

Anforderungen und Überlegungen für die SAML-basierte Verbundauthentifizierung

Im Folgenden sind die Anforderungen und Überlegungen für die SAML-basierte Verbundauthentifizierung aufgeführt.

- Informationen zu Kontingenten und Regeln für die Konfiguration von Benutzern und Gruppen in einem SAML-basierten IdP finden Sie unter Kontingente für Benutzer und Gruppen.
- Die SAML-Assertion und die SAML-Dokumente müssen signiert sein.
- AWS Client VPN unterstützt nur die Bedingungen "AudienceRestriction" und "NotBefore und NotOnOrAfter" in SAML-Assertionen.
- Die maximal unterstützte Größe für SAML-Antworten beträgt 128 KB.
- AWS Client VPN stellt keine signierten Authentifizierungsanfragen bereit.
- Die einmalige SAML-Abmeldung wird nicht unterstützt. Benutzer können sich abmelden, indem sie die Verbindung zum AWS bereitgestellten Client trennen, oder Sie können die Verbindungen beenden.
- Client VPN-Endpunkte unterstützen nur einen einzelnen IdP.
- Multi-Factor Authentication (MFA) wird unterstützt, wenn sie in Ihrem IdP aktiviert ist.
- Benutzer müssen den AWS bereitgestellten Client verwenden, um eine Verbindung zum Client-VPN-Endpunkt herzustellen. Sie müssen Version 1.2.0 oder höher verwenden. Weitere Informationen finden Sie unter Herstellen einer Verbindung über den AWS bereitgestellten Client.
- Die folgenden Browser werden für die IdP-Authentifizierung unterstützt: Apple Safari, Google Chrome, Microsoft Edge und Mozilla Firefox.
- Der AWS bereitgestellte Client reserviert den TCP-Port 35001 auf den Geräten der Benutzer für die SAML-Antwort.
- Wenn das Metadatendokument für den IAM SAML-Identitätsanbieter mit einer falschen oder bösartigen URL aktualisiert wird, kann dies zu Authentifizierungsproblemen für Benutzer oder zu Phishing-Angriffen führen. Daher empfiehlt es sich, am IAM SAML-Identitätsanbieter vorgenommene Aktualisierungen mit AWS CloudTrail zu überwachen. Weitere Informationen finden Sie unter Protokollierung von IAM- und AWS STS -Anrufen mit AWS CloudTrail im IAM-Benutzerhandbuch.

- AWS Client VPN sendet über eine HTTP-Redirect-Bindung eine AuthN-Anfrage an den IdP. Daher sollte der IdP die HTTP-Redirect-Bindung unterstützen und sie sollte im Metadatendokument des IdP vorhanden sein.
- Für die SAML-Assertion müssen Sie ein E-Mail-Adressformat für das `NameID`-Attribut verwenden.

Konfigurationsressourcen für SAML-basierte IdPs

In der folgenden Tabelle sind die SAML-basierten Produkte aufgeführt IdPs , die wir für die Verwendung mit ihnen getestet haben AWS Client VPN, sowie Ressourcen, die Ihnen bei der Konfiguration des IdP helfen können.

IdP	Ressource
Okta	Authentifizieren AWS Client VPN Sie Benutzer mit SAML
Microsoft Azure Active Directory	Weitere Informationen finden Sie unter Tutorial: Azure Active Directory-Single-Sign-On-Integration (SSO) mit AWS ClientVPN auf der Microsoft-Dokumentationswebsite.
JumpCloud	Einmaliges Anmelden (SSO) mit AWS Client VPN
AWS IAM Identity Center	Verwenden von IAM Identity Center mit AWS Client VPN zur Authentifizierung und Autorisierung

Dienstanbieterinformationen zum Erstellen einer Anwendung

Um eine SAML-basierte App mit einem IdP zu erstellen, der nicht in der obigen Tabelle aufgeführt ist, verwenden Sie die folgenden Informationen, um die AWS Client VPN Service Provider-Informationen zu konfigurieren.

- Assertionsverbraucherdienst-URL: `http://127.0.0.1:35001`
- Zielgruppen-URI: `urn:amazon:webservices:clientvpn`

In der SAML-Antwort des IdP muss mindestens ein Attribut enthalten sein. Im Folgenden finden Sie einige Beispielattribute.

Attribut	Beschreibung
`FirstName`	Der Vorname des Benutzers.
`LastName`	Der Nachname des Benutzers.
`memberOf`	Die Gruppe oder Gruppen, zu der bzw. denen der Benutzer gehört.

> **Note**
>
> Das `memberOf`-Attribut ist für die Verwendung von gruppenbasierten Autorisierungsregeln für Active Directory oder SAML IdP erforderlich. Es wird auch zwischen Groß- und Kleinschreibung unterschieden, und es muss genau wie angegeben konfiguriert werden. Weitere Informationen finden Sie unter Netzwerkbasierte Autorisierung und Autorisierungsregeln.

Unterstützung des Self-Service-Portals

Wenn Sie das Self-Service-Portal für Ihren Client-VPN-Endpunkt aktivieren, melden sich Benutzer mit ihren SAML-basierten IdP-Anmeldeinformationen beim Portal an.

Wenn Ihr IdP mehrere Assertion Consumer Service (ACS) -URLs unterstützt, fügen Sie Ihrer App die folgende ACS-URL hinzu.

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Wenn Sie den Client-VPN-Endpunkt in einer GovCloud Region verwenden, verwenden Sie stattdessen die folgende ACS-URL. Wenn Sie dieselbe IDP-App für die Authentifizierung sowohl für Standard- als auch für GovCloud Regionen verwenden, können Sie beide URLs hinzufügen.

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Wenn Ihr IdP nicht mehrere ACS-URLs unterstützt, gehen Sie folgendermaßen vor:

1. Erstellen Sie eine zusätzliche SAML-basierte App in Ihrem IdP und geben Sie die folgende ACS-URL an.

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

2. Generieren und laden Sie ein Verbund-Metadaten-Dokument.
3. Erstellen Sie einen IAM-SAML-Identitätsanbieter in demselben AWS Konto wie der Client-VPN-Endpunkt. Weitere Informationen finden Sie unter Erstellen von IAM SAML-Identitätsanbietern im IAM-Benutzerhandbuch.

> **Note**
>
> Sie erstellen diesen IAM SAML-Identitätsanbieter zusätzlich zu dem, den Sie für die Haupt-App erstellen.

4. Erstellen Sie den Client VPN-Endpunkt und geben Sie die beiden von Ihnen erstellten IAM SAML-Identitätsanbieter an.

Client-Autorisierung

Client VPN unterstützt zwei Arten von Client-Autorisierung, Sicherheitsgruppen und (über Autorisierungsregeln) netzwerkbasierte Autorisierung.

Sicherheitsgruppen

Wenn Sie einen Client VPN-Endpunkt erstellen, können Sie die Sicherheitsgruppen von einer bestimmten VPC angeben, die auf den Client VPN-Endpunkt angewendet werden sollen. Wenn Sie ein Subnetz mit einem Client VPN-Endpunkt verknüpfen, wird automatisch die Standardsicherheitsgruppe der VPC angewendet. Sie können die Sicherheitsgruppen ändern, nachdem Sie den Client VPN-Endpunkt erstellt haben. Weitere Informationen finden Sie unter Anwenden einer Sicherheitsgruppe auf ein Zielnetzwerk. Die Sicherheitsgruppen sind den Client VPN-Netzwerkschnittstellen zugeordnet.

Sie können Client VPN-Benutzern den Zugriff auf Ihre Anwendungen in einer VPC ermöglichen, indem Sie den Sicherheitsgruppen Ihrer Anwendungen eine Regel hinzufügen, um den Datenverkehr von der Sicherheitsgruppe zuzulassen, die für die Zuordnung übernommen wurde.

So fügen Sie eine Regel hinzu, die Datenverkehr aus der Client VPN-Endpunkt-Sicherheitsgruppe zulässt

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe aus, die Ihrer Ressource oder Anwendung zugeordnet ist. Wählen Sie anschließend Actions (Aktionen), Edit inbound rules (Eingehende Regeln bearbeiten) aus.
4. Wählen Sie Add rule.
5. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus. Alternativ können Sie den Zugriff auf eine bestimmte Art von Datenverkehr einschränken, beispielsweise SSH.

   Geben Sie in Quelle die ID der Sicherheitsgruppe an, die dem Zielnetzwerk (Subnetz) für den Client VPN-Endpunkt zugeordnet ist.
6. Wählen Sie Save rules (Regeln speichern) aus.

Umgekehrt können Sie den Zugriff für Client VPN-Benutzer einschränken, indem Sie die Sicherheitsgruppe, die auf die Zuordnung angewendet wurde, nicht angeben oder indem Sie die Regel entfernen, die auf die Client VPN-Endpunkt-Sicherheitsgruppe verweist. Die von Ihnen benötigten Sicherheitsgruppenregeln sind möglicherweise auch von der Art des VPN-Zugriffs abhängig, den Sie konfigurieren möchten. Weitere Informationen finden Sie unter Szenarien und Beispiele für AWS Client-VPN.

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

Netzwerkbasierte Autorisierung

Die netzwerkbasierte Autorisierung wird mithilfe von Autorisierungsregeln implementiert. Für jedes Netzwerk, für das Sie den Zugriff aktivieren möchten, müssen Sie Autorisierungsregeln konfigurieren, die die Benutzer mit Zugriff beschränken. Sie können für ein bestimmtes Netzwerk die Active Directory- oder SAML-basierte IdP-Gruppe konfigurieren, die Zugriff erhalten soll. Nur Benutzer, die Mitglied der angegebenen Gruppe sind, können auf das angegebene Netzwerk zugreifen. Wenn Sie keine Active Directory- oder SAML-basierte Verbundauthentifizierung verwenden oder allen Benutzern Zugriff gewähren möchten, können Sie eine Regel angeben, die allen Clients Zugriff gewährt. Weitere Informationen finden Sie unter Autorisierungsregeln.

Verbindungsautorisierung

Sie können einen Client-Connect-Handler für Ihren Client-VPN-Endpunkt konfigurieren. Mit dem Handler können Sie eine benutzerdefinierte Logik ausführen, die eine neue Verbindung basierend auf Geräte-, Benutzer- und Verbindungsattributen autorisiert. Der Client-Connect-Handler wird ausgeführt, nachdem der Client-VPN-Service das Gerät und den Benutzer authentifiziert hat.

Um einen Client Connect-Handler für Ihren Client-VPN-Endpunkt zu konfigurieren, erstellen Sie eine AWS Lambda -Funktion, die Geräte-, Benutzer- und Verbindungsattribute als Eingaben verwendet und die Entscheidung an den Client-VPN-Service zurückgibt, eine neue Verbindung zuzulassen oder zu verweigern. Sie geben die Lambda-Funktion in Ihrem Client-VPN-Endpunkt an. Wenn sich Geräte mit Ihrem Client-VPN-Endpunkt verbinden, ruft der Client-VPN-Service für Sie die Lambda-Funktion auf. Nur Verbindungen, die von der Lambda-Funktion autorisiert wurden, dürfen sich mit dem Client-VPN-Endpunkt verbinden.

> **Note**
>
> Derzeit ist der einzige unterstützte Client-Connect-Handler-Typ eine Lambda-Funktion.

Anforderungen und Überlegungen

Nachfolgend werden Anforderungen und Überlegungen für den Client-Connect-Handler aufgeführt:

- Der Name der Lambda-Funktion muss mit dem `AWSClientVPN-`-Präfix beginnen.
- Qualifizierte Lambda-Funktionen werden unterstützt.
- Die Lambda-Funktion muss sich in derselben AWS Region und demselben AWS Konto wie der Client-VPN-Endpunkt befinden.
- Die Lambda-Funktion läuft nach 30 Sekunden ab. Dieser Wert kann nicht geändert werden.
- Die Lambda-Funktion wird synchron aufgerufen. Er wird nach der Geräte- und Benutzerauthentifizierung und vor der Auswertung der Autorisierungsregeln aufgerufen.
- Wenn die Lambda-Funktion für eine neue Verbindung aufgerufen wird und der Client-VPN-Service keine erwartete Antwort von der Funktion erhält, lehnt der Client-VPN-Service die Verbindungsanfrage ab. Dies kann beispielsweise auftreten, wenn die Lambda-Funktion gedrosselt wird, ein Timeout auftritt oder auf andere unerwartete Fehler trifft oder wenn die Antwort der Funktion nicht in einem gültigen Format vorliegt.

- Wir empfehlen, dass Sie die bereitgestellte Parallelität für die Lambda-Funktion konfigurieren, damit sie ohne Latenzschwankungen skaliert werden kann.
- Wenn Sie Ihre Lambda-Funktion aktualisieren, sind bestehende Verbindungen zum Client-VPN-Endpunkt nicht betroffen. Sie können die bestehenden Verbindungen beenden und Ihre Clients dann anweisen, neue Verbindungen herzustellen. Weitere Informationen finden Sie unter Beenden einer Client-Verbindung.
- Wenn Clients den AWS bereitgestellten Client verwenden, um eine Verbindung zum Client-VPN-Endpunkt herzustellen, müssen sie Version 1.2.6 oder höher für Windows und Version 1.2.4 oder höher für macOS verwenden. Weitere Informationen finden Sie unter Verbinden mit dem von AWS bereitgestellten Client.

Lambda-Schnittstelle

Die Lambda-Funktion verwendet Geräteattribute, Benutzerattribute und Verbindungsattribute als Eingaben vom Client-VPN-Service. Sie muss dann die Entscheidung an den Client-VPN-Service zurückgeben, ob die Verbindung zugelassen oder verweigert werden soll.

Anfrageschema

Die Lambda-Funktion verwendet einen JSON-Blob mit den folgenden Feldern als Eingabe.

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
    "aws-client-version": <AWS client version>,
    "groups": <group identifier>,
    "schema-version": "v3"
}
```

- `connection-id` – Die ID der Client-Verbindung mit dem Client-VPN-Endpunkt.
- `endpoint-id` – Die ID des Client-VPN-Endpunkts.
- `common-name` – Die Geräte-ID. In dem Client-Zertifikat, das Sie für das Gerät erstellen, identifiziert der allgemeine Name das Gerät eindeutig.

- `username` – Die Benutzer-ID, falls zutreffend. Bei der Active Directory-Authentifizierung ist dies der Benutzername. Bei der SAML-basierten föderierten Authentifizierung ist dies `NameID`. Bei gegenseitiger Authentifizierung ist dieses Feld leer.
- `platform` – Die Client-Betriebssystemplattform.
- `platform-version` – Die Version des Betriebssystems. Der Client-VPN-Service stellt einen Wert bereit, wenn die `--push-peer-info`-Richtlinie in der OpenVPN-Client-Konfiguration vorhanden ist, wenn Clients eine Verbindung zu einem Client-VPN-Endpunkt herstellen und wenn der Client die Windows-Plattform ausführt.
- `public-ip` – Die öffentliche IP-Adresse des sich verbindenden Geräts.
- `client-openvpn-version` – Die OpenVPN-Version, die der Client verwendet.
- `aws-client-version`— Die AWS Client-Version.
- `groups` – Die Gruppen-ID, falls zutreffend. Bei der Active-Directory-Authentifizierung ist dies eine Liste mit Active-Directory-Gruppen. Bei der SAML-basierten Verbundauthentifizierung ist dies eine Liste von Identitätsanbietergruppen (IdP-Gruppen). Bei gegenseitiger Authentifizierung ist dieses Feld leer.
- `schema-version` – Die Schema-Version Der Standardwert ist `v3`.

Antwortschema

Die Lambda-Funktion muss die folgenden Felder zurückgeben.

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v3"
}
```

- `allow` – Erforderlich. Ein boolescher Wert (`true` | `false`), der angibt, ob die neue Verbindung zugelassen oder verweigert werden soll.
- `error-msg-on-denied-connection` – Erforderlich. Eine Zeichenfolge von bis zu 255 Zeichen, die verwendet werden kann, um den Clients Schritte und Anleitungen zu übermitteln, wenn die Verbindung von der Lambda-Funktion verweigert wird. Bei Ausfällen während der Ausführung der Lambda-Funktion (z. B. aufgrund einer Drosselung) wird die folgende Standardnachricht an Clients zurückgegeben.

```
Error establishing connection. Please contact your administrator.
```

- `posture-compliance-statuses` – Erforderlich. Wenn Sie die Lambda-Funktion für das Posture Assessment verwenden, ist dies eine Liste der Status für das sich verbindende Gerät. Sie definieren die Statusnamen entsprechend Ihren Posture Assessment-Kategorien für Geräte, z. B. `compliant`, `quarantined`, `unknown` usw. Jeder Name kann bis zu 255 Zeichen lang sein. Sie können bis zu 10 Status angeben.
- `schema-version` – Erforderlich. Die Schemaversion. Der Standardwert ist `v3`.

Sie können dieselbe Lambda-Funktion für mehrere Client VPN-Endpunkte in derselben Region verwenden.

Weitere Informationen zum Erstellen einer Lambda-Funktion finden Sie unter Erste Schritte mit AWS Lambda im AWS Lambda -Entwicklerhandbuch.

Verwenden des Client-Connect-Handlers für das Posture Assessment

Sie können den Client Connect-Handler verwenden, um Ihren Client-VPN-Endpunkt in Ihre vorhandene Geräteverwaltungslösung zu integrieren, um die Einhaltung der Posture-Anforderungen der sich verbindenden Geräte zu evaluieren. Damit die Lambda-Funktion als Geräteautorisierungs-Handler funktioniert, verwenden Sie die gegenseitige Authentifizierung für Ihren Client-VPN-Endpunkt. Erstellen Sie ein eindeutiges Client-Zertifikat und einen Schlüssel für jeden Client (jedes Gerät), der sich mit dem Client-VPN-Endpunkt verbindet. Die Lambda-Funktion kann den eindeutigen allgemeinen Namen für das Client-Zertifikat (das vom Client-VPN-Service weitergegeben wird) verwenden, um das Gerät zu identifizieren und seinen Posture-Compliance-Status von Ihrer Geräteverwaltungslösung abzurufen. Sie können die gegenseitige Authentifizierung in Kombination mit einer benutzerbasierten Authentifizierung verwenden.

Alternativ können Sie ein grundlegendes Posture Assessment in der Lambda-Funktion selbst vornehmen. Sie können beispielsweise die Felder `platform` und `platform-version` bewerten, die vom Client-VPN-Service an die Lambda-Funktion übergeben werden.

> **Note**
>
> Der Verbindungshandler kann zwar verwendet werden, um eine Mindestversion der AWS Client VPN Anwendung zu erzwingen, aber das Feld `aws-client-version` im

Verbindungshandler gilt nur für die AWS Client VPN Anwendung und wird anhand von Umgebungsvariablen auf dem Benutzergerät aufgefüllt.

Aktivieren des Client-Connect-Handlers

Um den Client Connect-Handler zu aktivieren, erstellen oder ändern Sie einen Client-VPN-Endpunkt und geben Sie den Amazon-Ressourcennamen (ARN) der Lambda-Funktion an. Weitere Informationen erhalten Sie unter Erstellen eines Client VPN-Endpunkts und Ändern eines Client-VPN-Endpunkts.

Serviceverknüpfte Rolle

AWS Client VPN erstellt in Ihrem Konto automatisch eine mit dem Dienst verknüpfte Rolle namens AWSServiceRoleForClientVPNConnections. Die Rolle verfügt über Berechtigungen zum Aufrufen der Lambda-Funktion, wenn eine Verbindung zum Client-VPN-Endpunkt hergestellt wird. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Client VPN.

Überwachen von Fehlern bei der Verbindungsautorisierung

Sie können den Status der Verbindungsautorisierung von Verbindungen zum Client-VPN-Endpunkt anzeigen. Weitere Informationen finden Sie unter Anzeigen von Client-Verbindungen.

Wenn der Client Connect-Handler für das Posture Assessment verwendet wird, können Sie auch die Compliance-Status von Geräten, die sich mit Ihrem Client-VPN-Endpunkt verbinden, in den Verbindungsprotokollen anzeigen. Weitere Informationen finden Sie unter Verbindungsprotokollierung.

Wenn ein Gerät die Verbindungsautorisierung nicht besteht, gibt das `connection-attempt-failure-reason`-Feld in den Verbindungsprotokollen einen der folgenden Fehlergründe zurück:

- `client-connect-failed` – Die Lambda-Funktion verhinderte, dass die Verbindung hergestellt wurde.
- `client-connect-handler-timed-out` – Die Lambda-Funktion hat das Zeitlimit überschritten.
- `client-connect-handler-other-execution-error` – Die Lambda-Funktion ist auf einen unerwarteten Fehler gestoßen.
- `client-connect-handler-throttled` – Die Lambda-Funktion wurde gedrosselt.

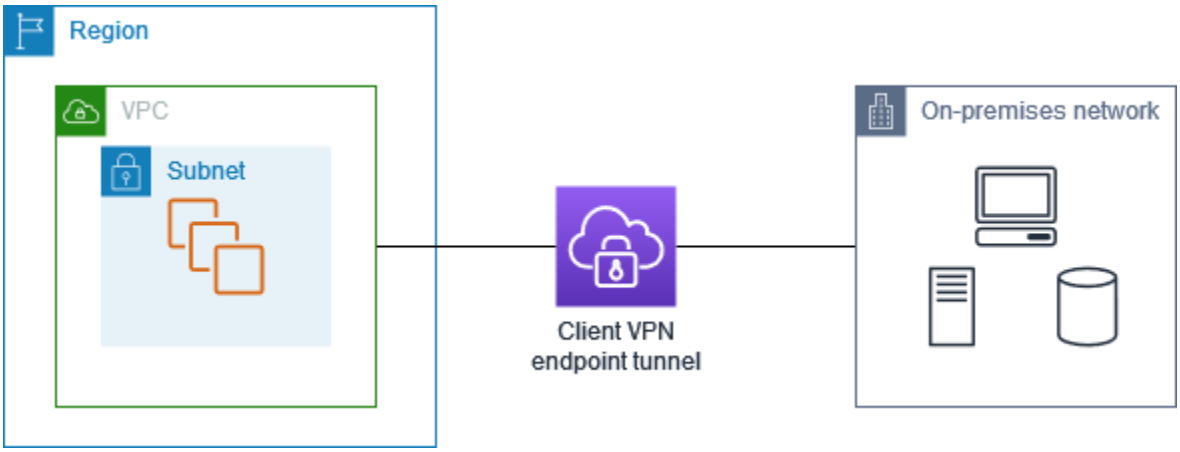
- `client-connect-handler-invalid-response` – Die Lambda-Funktion gab eine ungültige Antwort zurück.
- `client-connect-handler-service-error` – Während des Verbindungsversuchs ist ein serviceseitiger Fehler aufgetreten.

Split-Tunnel auf AWS Client VPN-Endpunkten

Wenn Sie einen Client VPN-Endpunkt haben, wird standardmäßig der gesamte Datenverkehr von Clients über den Client VPN-Tunnel geleitet. Wenn Sie Split-Tunnel auf dem Client-VPN-Endpunkt aktivieren, übertragen wir die Routen auf der Routing-Tabelle des Client-VPN-Endpunkts auf das Gerät, das mit dem Client-VPN-Endpunkt verbunden ist. Dadurch wird sichergestellt, dass nur Datenverkehr mit einem Ziel im Netzwerk, das mit einer Route aus der Client-VPN-Endpunkt-Routing-Tabelle übereinstimmt, über den Client-VPN-Tunnel geroutet wird.

Sie können einen Split-Tunnel-Client-VPN-Endpunkt verwenden, wenn Sie nicht möchten, dass der gesamte Benutzerdatenverkehr über den Client-VPN-Endpunkt geroutet wird.

Im folgenden Beispiel ist die Split-Tunnel-Funktion für den Client-VPN-Endpunkt aktiviert. Nur Datenverkehr, der für die VPC (`172.31.0.0/16`) bestimmt ist, wird über den Client-VPN-Tunnel geroutet. Datenverkehr, der für On-Premise-Ressourcen bestimmt ist, wird nicht über den Client-VPN-Tunnel geroutet.



Split-Tunnel-Vorteile

Split-Tunnel für Client VPN-Endpunkte bietet die folgenden Vorteile:

- Sie können das Routing von Datenverkehr von Clients optimieren, indem nur der von AWS bestimmte Datenverkehr den VPN-Tunnel durchquert.

- Sie können das Volumen des ausgehenden Datenverkehrs von AWS reduzieren, wodurch die Datenübertragungskosten gesenkt werden.

Überlegungen zum Routing

- Wenn Sie den Split-Tunnel-Modus aktivieren, werden alle Routen in der Routing-Tabelle des Client-VPN-Endpunkts der Routing-Tabelle des Clients hinzugefügt, wenn die VPN-Verbindung hergestellt wird. Diese Operation unterscheidet sich vom Standardverhalten, bei dem die Routing-Tabelle des Clients mit dem Eintrag `0.0.0.0/0` überschrieben wird, um den gesamten Datenverkehr über das VPN zu leiten.

  > **Note**
  >
  > Es wird nicht empfohlen, der Routing-Tabelle des Client-VPN-Endpunkts bei Verwendung des Split-Tunnel-Modus die Route `0.0.0.0/0` hinzuzufügen.

- Wenn der Split-Tunnel-Modus aktiviert ist, führt jede Änderung an der Routing-Tabelle der Client-VPN-Endpunkte dazu, dass alle Client-Verbindungen zurückgesetzt werden.

Aktivieren von Split-Tunnel

Sie können Split-Tunnel für einen neuen oder einen vorhandenen Client-VPN-Endpunkt aktivieren. Weitere Informationen finden Sie unter den folgenden Themen:

- Erstellen eines Client VPN-Endpunkts
- Ändern eines Client-VPN-Endpunkts

Verbindungsprotokollierung

Die Verbindungsprotokollierung ist eine Funktion von AWS Client VPN, mit der Sie Verbindungsprotokolle für Ihren Client-VPN-Endpunkt erfassen können.

Ein Verbindungsprotokoll enthält Verbindungsprotokolleinträge. Jeder Verbindungsprotokolleintrag enthält Informationen zu einem Verbindungsereignis, d. h., wenn ein Client (Endbenutzer) eine Verbindung herstellt, versucht, eine Verbindung herzustellen oder die Verbindung zu Ihrem Client VPN-Endpunkt trennt. Sie können diese Informationen verwenden, um forensische

Untersuchungen durchzuführen, zu analysieren, wie Ihr Client VPN-Endpunkt verwendet wird, oder Verbindungsprobleme zu debuggen.

Die Verbindungsprotokollierung ist in allen Regionen verfügbar, in denen AWS Client VPN verfügbar ist. Verbindungsprotokolle werden in einer CloudWatch Logs-Protokollgruppe in Ihrem Konto veröffentlicht.

> **Note**
>
> Fehlgeschlagene Versuche zur gegenseitigen Authentifizierung werden nicht protokolliert.

Verbindungsprotokolleinträge

Ein Verbindungsprotokolleintrag ist ein in JSON formatierter Blob von Schlüssel-Wert-Paaren. Im Folgenden finden Sie ein Beispiel für den Verbindungsprotokolleintrag.

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA",
    "username": "joe"
    }
```

Ein Verbindungsprotokolleintrag enthält die folgenden Schlüssel:

- `connection-log-type`: Der Typ des Verbindungsprotokolleintrags (`connection-attempt` oder `connection-reset`).
- `connection-attempt-status`: Der Status der Verbindungsanforderung (`successful`, `failed`, `waiting-for-assertion` oder `NA`).
- `connection-reset-status`: Der Status eines Verbindungsrücksetzereignisses (`NA` oder `assertion-received`).
- `connection-attempt-failure-reason`: Der Grund für den Verbindungsfehler, falls zutreffend.
- `connection-id`: Die ID der Verbindung.
- `client-vpn-endpoint-id`: Die ID des Client VPN-Endpunkts, mit dem die Verbindung hergestellt wurde.
- `transport-protocol`: Das Transportprotokoll, das für die Verbindung verwendet wurde.
- `connection-start-time`: Die Startzeit der Verbindung.
- `connection-last-update-time`: Die letzte Aktualisierungszeit der Verbindung. Dieser Wert wird regelmäßig in den Protokollen aktualisiert.
- `client-ip`: Die IP-Adresse des Clients, die dem Client VPN-Endpunkt aus dem Client-IPv4-CIDR-Bereich zugewiesen wird.
- `common-name`: Der Common Name des Zertifikats, das für die zertifikatbasierte Authentifizierung verwendet wird.
- `device-type`: Der Gerätetyp, der vom Endbenutzer für die Verbindung verwendet wird.
- `device-ip`: Die öffentliche IP-Adresse des Geräts.
- `port`: Die Portnummer für die Verbindung.
- `ingress-bytes`: Die Anzahl der eingehenden Bytes für die Verbindung. Dieser Wert wird regelmäßig in den Protokollen aktualisiert.
- `egress-bytes`: Die Anzahl der ausgehenden Bytes für die Verbindung. Dieser Wert wird regelmäßig in den Protokollen aktualisiert.
- `ingress-packets`: Die Anzahl der eingehenden Pakete für die Verbindung. Dieser Wert wird regelmäßig in den Protokollen aktualisiert.
- `egress-packets`: Die Anzahl der ausgehenden Pakete für die Verbindung. Dieser Wert wird regelmäßig in den Protokollen aktualisiert.
- `connection-end-time`: Die Endzeit der Verbindung. Der Wert ist „`NA`“, wenn die Verbindung noch ausgeführt wird oder der Verbindungsversuch fehlgeschlagen ist.

- `posture-compliance-statuses`: Die vom Client-Verbindungs-Handler zurückgegebenen Niveau-Compliance-Status, falls zutreffend.
- `username`: Der Benutzername wird aufgezeichnet, wenn eine benutzerbasierte Authentifizierung (AD oder SAML) für den Endpunkt verwendet wird.
- `connection-duration-seconds`: Die Dauer einer Verbindung in Sekunden. Entspricht der Differenz zwischen „connection-start-time“ und „connection-end-time“.

Weitere Informationen zum Aktivieren der Verbindungsprotokollierung finden Sie unter Arbeiten mit Verbindungsprotokollen.

Überlegungen zur Client-VPN-Skalierung

Berücksichtigen Sie beim Erstellen eines Client-VPN-Endpunkts die maximale Anzahl gleichzeitiger VPN-Verbindungen, die Sie unterstützen möchten. Sie sollten die Anzahl der Kunden berücksichtigen, die Sie derzeit unterstützen, und ob Ihr Client-VPN-Endpunkt bei Bedarf zusätzliche Anforderungen erfüllen kann.

Die folgenden Faktoren beeinflussen die maximale Anzahl gleichzeitiger VPN-Verbindungen, die auf einem Client-VPN-Endpunkt unterstützt werden können.

CIDR-Bereichsgröße des Clients

Wenn Sie einen Client-VPN-Endpunkt erstellen, müssen Sie einen Client-CIDR-Bereich angeben, bei dem es sich um einen IPv4-CIDR-Block zwischen einer /12- und /22-Netzmaske handelt. Jeder VPN-Verbindung mit dem Client-VPN-Endpunkt wird eine eindeutige IP-Adresse aus dem Client-CIDR-Bereich zugewiesen. Ein Teil der Adressen im Client-CIDR-Bereich wird auch zur Unterstützung des Verfügbarkeitsmodells des Client VPN-Endpunkts verwendet und kann Clients nicht zugewiesen werden. Sie können den Client-CIDR-Bereich nicht mehr ändern, nachdem Sie den Client-VPN-Endpunkt erstellt haben.

Im Allgemeinen empfehlen wir, dass Sie einen Client-CIDR-Bereich angeben, der die doppelte Anzahl von IP-Adressen (und damit gleichzeitigen Verbindungen) enthält, die Sie auf dem Client-VPN-Endpunkt unterstützen möchten.

Anzahl der zugehörigen Subnetze

Wenn Sie ein Subnetz mit einem Client-VPN-Endpunkt verknüpfen, ermöglichen Sie Benutzern, VPN-Sitzungen für den Client-VPN-Endpunkt einzurichten. Sie können einem Client-VPN-

Endpunkt mehrere Subnetze zuordnen, um eine hohe Verfügbarkeit zu ermöglichen und zusätzliche Verbindungskapazität zu aktivieren.

Im Folgenden finden Sie die Anzahl der unterstützten gleichzeitigen VPN-Verbindungen basierend auf der Anzahl der Subnetzzuordnungen für den Client-VPN-Endpunkt.

Subnetzzuordnungen	Unterstützte Anzahl von Verbindungen
1	7.000
2	36 500
3	66 500
4	96 500
5	126 000

Sie können nicht mehrere Subnetze derselben Availability Zone mit einem Client VPN-Endpunkt verknüpfen. Daher hängt die Anzahl der Subnetzzuordnungen auch von der Anzahl der Availability Zones ab, die in einer AWS-Region verfügbar sind.

Wenn Sie beispielsweise erwarten, 8 000 VPN-Verbindungen zu Ihrem Client-VPN-Endpunkt zu unterstützen, geben Sie eine minimale CIDR-Client-Bereichsgröße von `/18` (16 384 IP-Adressen) an und verknüpfen Sie mindestens 2 Subnetze mit dem Client-VPN-Endpunkt.

Wenn Sie sich nicht sicher sind, wie viele die erwarteten VPN-Verbindungen für Ihren Client-VPN-Endpunkt sind, empfehlen wir Ihnen, einen CIDR-Block der Größe `/16` oder größer anzugeben.

Weitere Informationen zu den Regeln und Einschränkungen für die Arbeit mit CIDR-Bereichen und Zielnetzwerken von Clients finden Sie unter Regeln und bewährte Verfahren von AWS Client VPN.

Weitere Informationen zu Kontingenten für Ihren Client-VPN-Endpunkt finden Sie unter AWS VPN-Kontingente für Kunden.

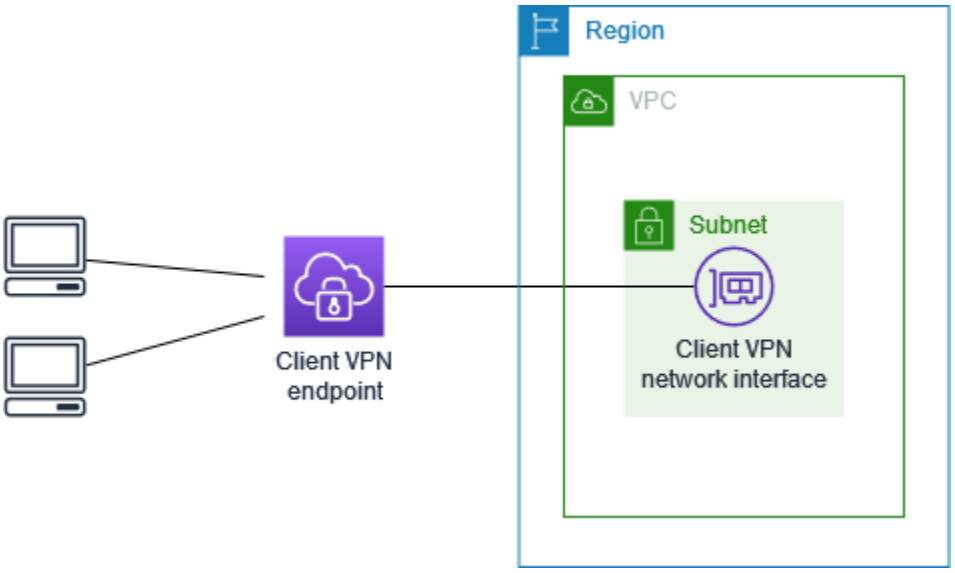
Szenarien und Beispiele für AWS Client-VPN

Dieser Abschnitt enthält Beispiele für das Erstellen und Konfigurieren des Client VPN-Zugriffs für Ihre Clients.

Inhalt

Mit AWS Client-VPN auf eine VPC zugreifen

Die Konfiguration für dieses Szenario umfasst eine einzige Ziel-VPC. Wir empfehlen diese Konfiguration, wenn Sie Clients den Zugriff auf die Ressourcen nur in einer einzelnen VPC gewähren.



Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Erstellen oder Identifizieren einer VPC mit mindestens einem Subnetz. Identifizieren Sie das Subnetz in der VPC, das dem Client-VPN-Endpunkt zugeordnet werden soll, und notieren Sie sich dessen IPv4-CIDR-Bereiche.

- Identifizieren Sie einen geeigneten CIDR-Bereich für die Client-IP-Adressen, der nicht mit der VPC-CIDR überlappt.
- Lesen Sie die Regeln und Einschränkungen für Client VPN-Endpunkte in Regeln und bewährte Verfahren von AWS Client VPN.

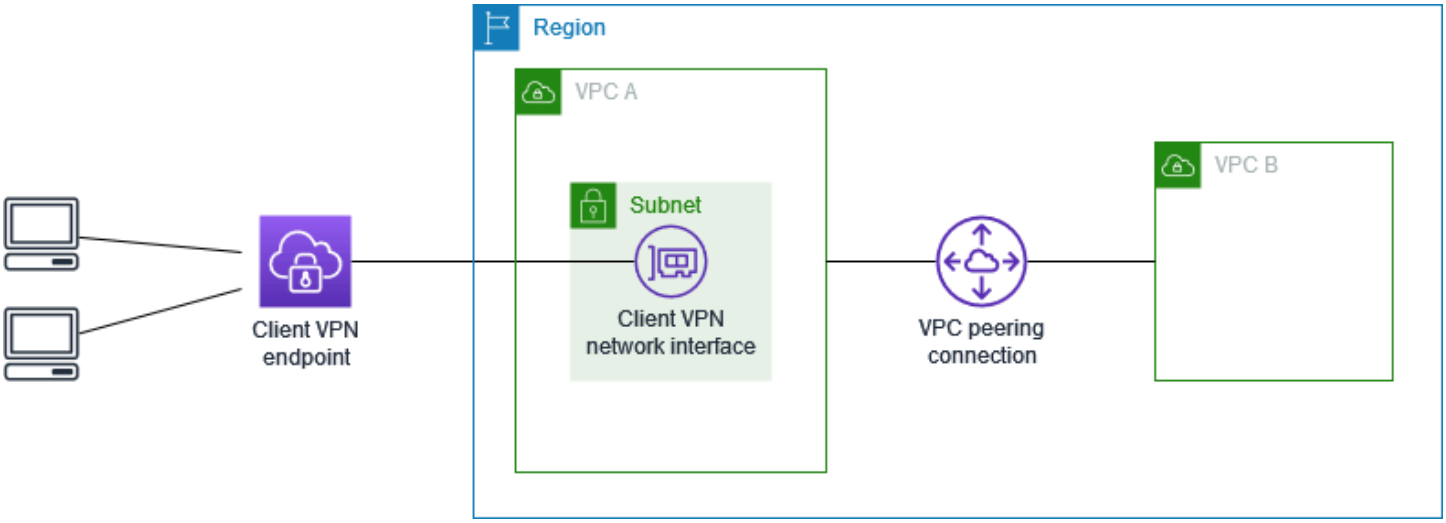
So implementieren Sie diese Konfiguration

1. Erstellen Sie einen Client VPN-Endpunkt in derselben Region wie die VPC. Führen Sie dazu die unter beschriebenen Schritte au Erstellen eines Client VPN-Endpunkts.
2. Verknüpfen Sie das Subnetz mit dem Client VPN-Endpunkt. Führen Sie dazu die unter Zuordnen eines Zielnetzwerk zu einem Client VPN-Endpunkt beschriebenen Schritte aus und wählen Sie das Subnetz und die VPC aus, die Sie zuvor identifiziert haben.
3. Fügen Sie eine Autorisierungsregel hinzu, um Clients den Zugriff auf die VPC zu gewähren. Führen Sie dazu die unter Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt beschriebenen Schritte aus und geben Sie unter Destination network (Zielnetzwerk) den IPv4 CIDR-Bereich der VPC ein.
4. Fügen Sie den Sicherheitsgruppen Ihrer Ressourcen eine Regel hinzu, die Datenverkehr aus der Sicherheitsgruppe zulässt, die in Schritt 2 auf die Subnetzzuordnung angewendet wurde. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Mit AWS Client-VPN auf eine per Peering verbundene VPC zugreifen

Die Konfiguration für dieses Szenario umfasst eine Ziel-VPC (VPC A), die per Peering mit einer zusätzlichen VPC (VPC B) verbunden ist. Wir empfehlen diese Konfiguration, wenn Sie Clients den Zugriff auf die Ressourcen in einer Ziel-VPC und anderen VPCs (wie VPC B), die per Peering damit verbunden sind, gewähren müssen.

> **Note**
>
> Das unten beschriebene Verfahren zum Zulassen des Zugriffs auf eine per Peering verbundene VPC ist nur erforderlich, wenn der Client-VPN-Endpunkt für den Split-Tunnelmodus konfiguriert wurde. Im Volltunnelmodus ist der Zugriff auf die per Peering verbundene VPC standardmäßig zulässig.



Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Erstellen oder Identifizieren einer VPC mit mindestens einem Subnetz. Identifizieren Sie das Subnetz in der VPC, das dem Client-VPN-Endpunkt zugeordnet werden soll, und notieren Sie sich dessen IPv4-CIDR-Bereiche.
- Identifizieren Sie einen geeigneten CIDR-Bereich für die Client-IP-Adressen, der nicht mit der VPC-CIDR überlappt.
- Lesen Sie die Regeln und Einschränkungen für Client VPN-Endpunkte in Regeln und bewährte Verfahren von AWS Client VPN.

So implementieren Sie diese Konfiguration

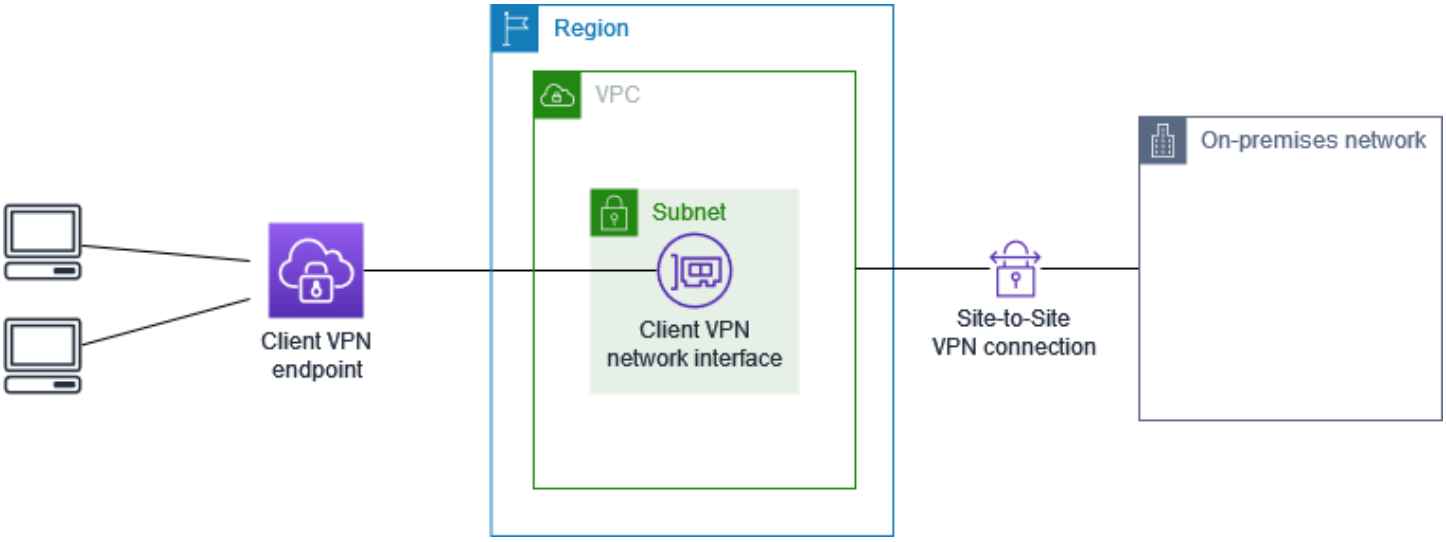
1. Richten Sie die VPC-Peering-Verbindung zwischen den VPCs ein. Befolgen Sie die Schritte unter Erstellen und Akzeptieren einer VPC-Peering-Verbindung im Amazon VPC Peering-Handbuch. Vergewissern Sie sich, dass Instances in VPC A mit Instances in VPC B über die Peer-Verbindung kommunizieren können.
2. Erstellen Sie einen Client VPN-Endpunkt in der gleichen Region wie die Ziel-VPC. Im obigen Beispiel ist dies VPC A. Führen Sie die unter Erstellen eines Client VPN-Endpunkts beschriebenen Schritte aus.
3. Ordnen Sie das identifizierte Subnetz dem Client-VPN-Endpunkt zu, den Sie erstellt haben. Führen Sie dazu die unter Zuordnen eines Zielnetzwerk zu einem Client VPN-Endpunkt beschriebenen Schritte aus, indem Sie das Subnetz und die VPC auswählen. Standardmäßig verknüpfen wir die Standardsicherheitsgruppe der VPC mit dem Client-VPN-Endpunkt.

Mithilfe der unter the section called “Anwenden einer Sicherheitsgruppe auf ein Zielnetzwerk” beschriebenen Schritte können Sie eine andere Sicherheitsgruppe zuordnen.

4. Fügen Sie eine Autorisierungsregel hinzu, um Clients Zugriff auf die Ziel-VPC zu gewähren. Führen Sie dazu die unter beschriebenen Schritte au Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt. Geben Sie als Zielnetzwerk den IPv4-CIDR-Bereich der VPC ein.
5. Fügen Sie eine Route hinzu, um den Datenverkehr an die per Peering verbundene VPC weiterzuleiten. Im obigen Beispiel ist dies VPC B. Führen Sie dazu die unter Endpunkt-Route erstellen beschriebenen Schritte aus. Geben Sie als Routen-Ziel den IPv4-CIDR-Bereich der per Peering verbundenen VPC ein. Wählen Sie als Ziel-VPC-Subnetz-ID das Subnetz aus, das mit dem Client-VPN-Endpunkt verknüpft ist.
6. Fügen Sie eine Autorisierungsregel hinzu, um Clients Zugriff auf die per Peering verbundene VPC zu gewähren. Führen Sie dazu die unter beschriebenen Schritte au Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt. Geben Sie als Zielnetzwerk den IPv4-CIDR-Bereich der VPC ein.
7. Fügen Sie den Sicherheitsgruppen Ihrer Ressourcen in VPC A und VPC B eine Regel hinzu, die Datenverkehr aus der Sicherheitsgruppe zulässt, auf die in Schritt 3 der Client-VPN-Endpunkt angewendet wurde. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Mit einem AWS Client VPN auf ein On-Premises-Netzwerk zugreifen

Die Konfiguration für dieses Szenario umfasst den Zugriff auf ein Netzwerk vor Ort. Wir empfehlen diese Konfiguration, wenn Sie Clients den Zugriff nur auf die Ressourcen in einem Netzwerk vor Ort gewähren müssen.



Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Erstellen oder Identifizieren einer VPC mit mindestens einem Subnetz. Identifizieren Sie das Subnetz in der VPC, das dem Client-VPN-Endpunkt zugeordnet werden soll, und notieren Sie sich dessen IPv4-CIDR-Bereiche.
- Identifizieren Sie einen geeigneten CIDR-Bereich für die Client-IP-Adressen, der nicht mit der VPC-CIDR überlappt.
- Lesen Sie die Regeln und Einschränkungen für Client VPN-Endpunkte in Regeln und bewährte Verfahren von AWS Client VPN.

So implementieren Sie diese Konfiguration

1. Aktivieren Sie die Kommunikation zwischen der VPC und Ihrem On-Premise-Netzwerk über eine AWS Site-to-Site-VPN-Verbindung. Führen Sie dazu die unter Erste Schritte im AWS Site-to-Site VPN-Benutzerhandbuch beschriebenen Schritte aus.

   > **Note**
   >
   > Alternativ können Sie dieses Szenario implementieren, indem Sie eine AWS Direct Connect-Verbindung zwischen Ihrer VPC und Ihrem Vor-Ort-Netzwerk verwenden. Weitere Informationen finden Sie im AWS Direct Connect-Benutzerhandbuch.

2. Testen Sie die AWS Site-to-Site-VPN-Verbindung, die Sie im vorherigen Schritt erstellt haben. Führen Sie dazu die unter Testen der Site-to-Site-VPN-Verbindung im AWS Site-to-Site VPN-

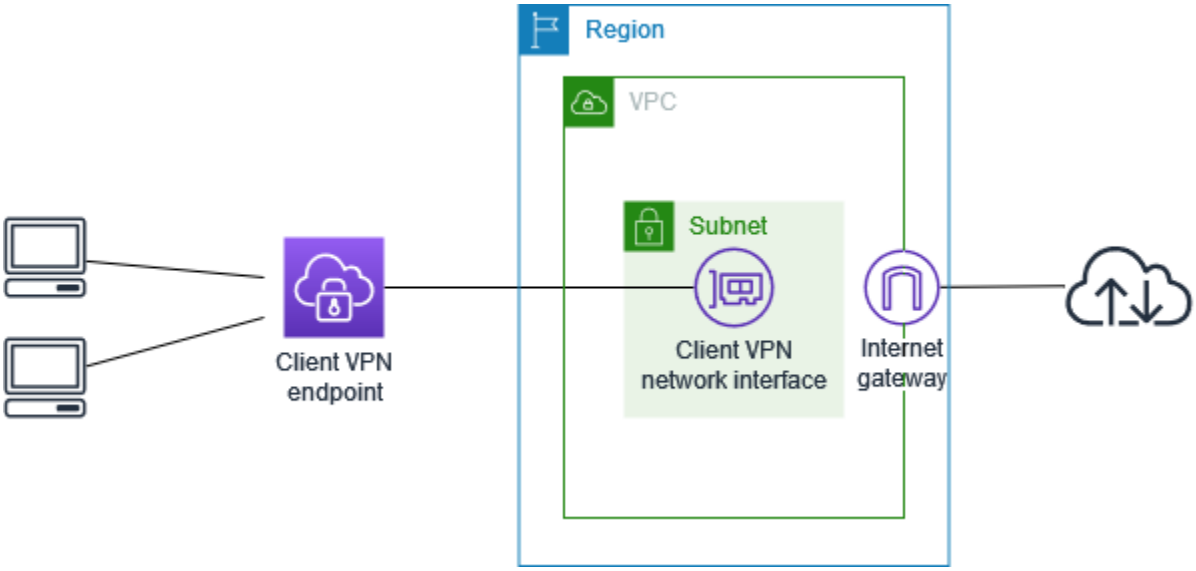
Benutzerhandbuch beschriebenen Schritte aus. Wenn die VPN-Verbindung wie erwartet funktioniert, fahren Sie mit dem nächsten Schritt fort.

3. Erstellen Sie einen Client VPN-Endpunkt in derselben Region wie die VPC. Führen Sie dazu die unter beschriebenen Schritte au Erstellen eines Client VPN-Endpunkts.
4. Verknüpfen Sie das Subnetz, das Sie zuvor mit dem Client VPN-Endpunkt identifiziert haben. Führen Sie dazu die unter Zuordnen eines Zielnetzwerk zu einem Client VPN-Endpunkt beschriebenen Schritte aus und wählen Sie die VPC und das Subnetz aus.
5. Fügen Sie eine Route hinzu, die den Zugriff auf die AWS Site-to-Site-VPN-Verbindung ermöglicht. Führen Sie dazu die unter Endpunkt-Route erstellen beschriebenen Schritte aus. Geben Sie für Routing-Ziel den IPv4-CIDR-Bereich der AWS Site-to-Site-VPN-Verbindung ein und wählen Sie für Subnetz-ID der Ziel-VPC das Subnetz aus, das Sie dem Client-VPN-Endpunkt zugeordnet haben.
6. Fügen Sie eine Autorisierungsregel hinzu, um Clients Zugriff auf die AWS Site-to-Site-VPN-Verbindung zu ermöglichen. Führen Sie dazu die unter Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt beschriebenen Schritte aus. Geben Sie für Zielnetzwerk den IPv4-CIDR-Verbindungsbereich der AWS Site-to-Site-VPN-Verbindung ein.

Mithilfe eines AWS Client VPN auf das Internet zugreifen

Die Konfiguration für dieses Szenario umfasst eine einzelne Ziel-VPC und Zugriff auf das Internet. Wir empfehlen diese Konfiguration, wenn Sie Clients den Zugriff auf die Ressourcen in einer einzelnen Ziel-VPC und Zugriff auf das Internet gewähren müssen.

Wenn Sie das Erste Schritte mit AWS-Client-VPN-Tutorial abgeschlossen haben, haben Sie dieses Szenario bereits implementiert.



Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Erstellen oder Identifizieren einer VPC mit mindestens einem Subnetz. Identifizieren Sie das Subnetz in der VPC, das dem Client-VPN-Endpunkt zugeordnet werden soll, und notieren Sie sich dessen IPv4-CIDR-Bereiche.
- Identifizieren Sie einen geeigneten CIDR-Bereich für die Client-IP-Adressen, der nicht mit der VPC-CIDR überlappt.
- Lesen Sie die Regeln und Einschränkungen für Client VPN-Endpunkte in Regeln und bewährte Verfahren von AWS Client VPN.

So implementieren Sie diese Konfiguration

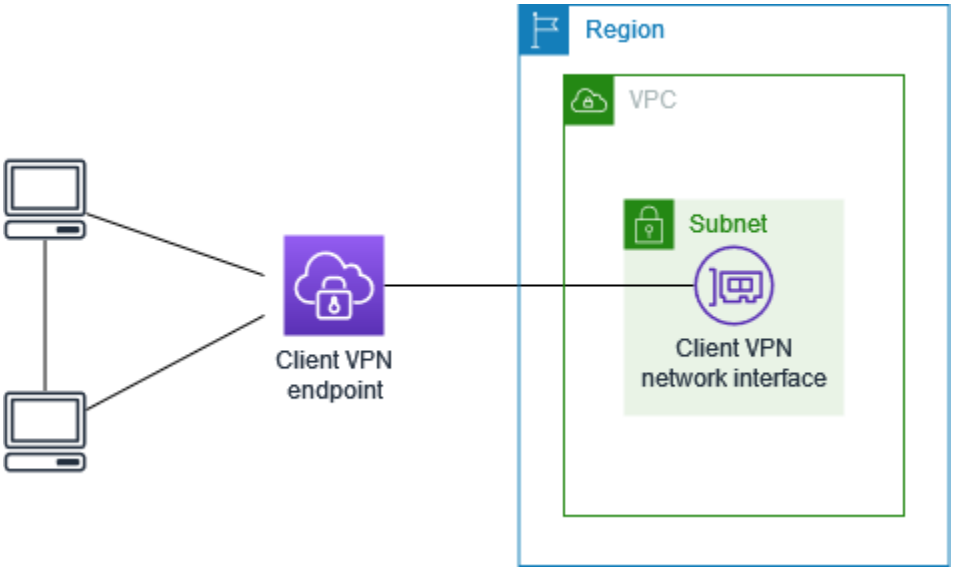
1. Stellen Sie sicher, dass die Sicherheitsgruppe, die Sie für den Client-VPN-Endpunkt verwenden werden, ausgehenden Datenverkehr zum Internet zulässt. Fügen Sie hierfür Regeln für ausgehenden Datenverkehr hinzu, die Datenverkehr zu 0.0.0.0/0 für HTTP- und HTTPS-Datenverkehr zulassen.
2. Erstellen Sie ein Internet-Gateway und fügen Sie es Ihrer VPC an. Weitere Informationen finden Sie unter Erstellen und Anfügen eines Internet-Gateways im Amazon VPC-Benutzerhandbuch.
3. Machen Sie Ihr Subnetz öffentlich zugänglich, indem Sie der Routing-Tabelle eine Route zum Internet-Gateway hinzufügen. Klicken Sie in der VPC-Konsole auf Subnets (Subnetze). Wählen Sie das Subnetz, das Sie mit dem Client VPN-Endpunkt verknüpfen möchten, aus. Klicken Sie auf Route Table (Routing-Tabelle) und wählen Sie die Routing-Tabellen-ID aus. Wählen Sie Actions (Aktionen), Edit routes (Routen bearbeiten) und Add route (Route hinzufügen) aus.

Geben Sie `0.0.0.0/0` für Destination (Ziel) ein und wählen Sie für Target (Ziel) das Internet-Gateway aus dem vorherigen Schritt aus.

4. Erstellen Sie einen Client VPN-Endpunkt in derselben Region wie die VPC. Führen Sie dazu die unter beschriebenen Schritte au Erstellen eines Client VPN-Endpunkts.
5. Verknüpfen Sie das Subnetz, das Sie zuvor mit dem Client VPN-Endpunkt identifiziert haben. Führen Sie dazu die unter Zuordnen eines Zielnetzwerk zu einem Client VPN-Endpunkt beschriebenen Schritte aus und wählen Sie die VPC und das Subnetz aus.
6. Fügen Sie eine Autorisierungsregel hinzu, um Clients den Zugriff auf die VPC zu gewähren. Führen Sie dazu die unter Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt beschriebenen Schritte aus und geben Sie unter Destination network to enable (Zu aktivierendes Ziel-Netzwerk) den IPv4 CIDR-Bereich der VPC ein.
7. Fügen Sie eine Route hinzu, die den Datenverkehr mit dem Internet ermöglicht. Führen Sie dazu die unter Endpunkt-Route erstellen beschriebenen Schritte aus. Geben Sie für Route destination (Routing-Ziel) `0.0.0.0/0` ein und wählen Sie für Target VPC Subnet ID (Subnetz-ID der Ziel-VPC) das Subnetz aus, das Sie mit dem Client VPN-Endpunkt verknüpft haben.
8. Fügen Sie eine Autorisierungsregel hinzu, um Clients den Zugriff auf das Internet zu gewähren. Führen Sie dazu die unter Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt beschriebenen Schritte durch. Für Destination network (Zielnetzwerk) geben Sie `0.0.0.0/0` ein.
9. Stellen Sie sicher, dass die Sicherheitsgruppen für die Ressourcen in Ihrer VPC über eine Regel verfügen, die den Zugriff aus der dem Client-VPN-Endpunkt zugeordneten Sicherheitsgruppe zulässt. Auf diese Weise können Ihre Clients auf die Ressourcen in Ihrer VPC zugreifen.

C-lient-to-client Zugriff mit AWS Client VPN

Die Konfiguration für dieses Szenario ermöglicht Clients den Zugriff auf eine einzelne VPC und ermöglicht es Clients, sich gegenseitig Datenverkehr zuzuleiten. Wir empfehlen diese Konfiguration, wenn die Clients, die eine Verbindung mit dem gleichen Client VPN-Endpunkt herstellen, auch miteinander kommunizieren müssen. Clients können miteinander kommunizieren, indem sie die eindeutige IP-Adresse verwenden, die ihnen aus dem CIDR-Bereich des Clients zugewiesen wird, wenn sie eine Verbindung mit dem Client VPN-Endpunkt herstellen.



Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Erstellen oder Identifizieren einer VPC mit mindestens einem Subnetz. Identifizieren Sie das Subnetz in der VPC, das dem Client-VPN-Endpunkt zugeordnet werden soll, und notieren Sie sich dessen IPv4-CIDR-Bereiche.
- Identifizieren Sie einen geeigneten CIDR-Bereich für die Client-IP-Adressen, der nicht mit der VPC-CIDR überlappt.
- Lesen Sie die Regeln und Einschränkungen für Client VPN-Endpunkte in Regeln und bewährte Verfahren von AWS Client VPN.

> **Note**
>
> Netzwerkbasierte Autorisierungsregeln, die Active-Directory-Gruppen oder SAML-basierte IdP-Gruppen verwenden, werden in diesem Szenario nicht unterstützt.

So implementieren Sie diese Konfiguration

1. Erstellen Sie einen Client VPN-Endpunkt in derselben Region wie die VPC. Führen Sie dazu die unter beschriebenen Schritte au Erstellen eines Client VPN-Endpunkts.
2. Verknüpfen Sie das Subnetz, das Sie zuvor mit dem Client VPN-Endpunkt identifiziert haben. Führen Sie dazu die unter Zuordnen eines Zielnetzwerk zu einem Client VPN-Endpunkt beschriebenen Schritte aus und wählen Sie die VPC und das Subnetz aus.

3. Fügen Sie eine Route zum lokalen Netzwerk in der Routing-Tabelle hinzu. Führen Sie dazu die unter beschriebenen Schritte au Endpunkt-Route erstellen. Geben Sie als Routenziel den CIDR-Bereich des Clients ein und geben Sie als Ziel-VPC-Subnetz-ID `local` an.
4. Fügen Sie eine Autorisierungsregel hinzu, um Clients den Zugriff auf die VPC zu gewähren. Führen Sie dazu die unter beschriebenen Schritte au Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt. Geben Sie als Zielnetzwerk den IPv4-CIDR-Bereich der VPC ein.
5. Fügen Sie eine Autorisierungsregel hinzu, um Clients den Zugriff auf den Client-CIDR-Bereich zu gewähren. Führen Sie dazu die unter beschriebenen Schritte au Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt. Geben Sie als Zielnetzwerk den CIDR-Bereich des Clients ein.

Den Zugriff auf Ihr Netzwerk mit AWS Client VPN beschränken

Sie können Ihren Client VPN-Endpunkt so konfigurieren, dass der Zugriff auf spezifische Ressourcen in Ihrer VPC eingeschränkt wird. Für die benutzerbasierte Authentifizierung können Sie auch den Zugriff auf Teile des Netzwerks basierend auf der Benutzergruppe, die auf den Client VPN-Endpunkt zugreift, einschränken.

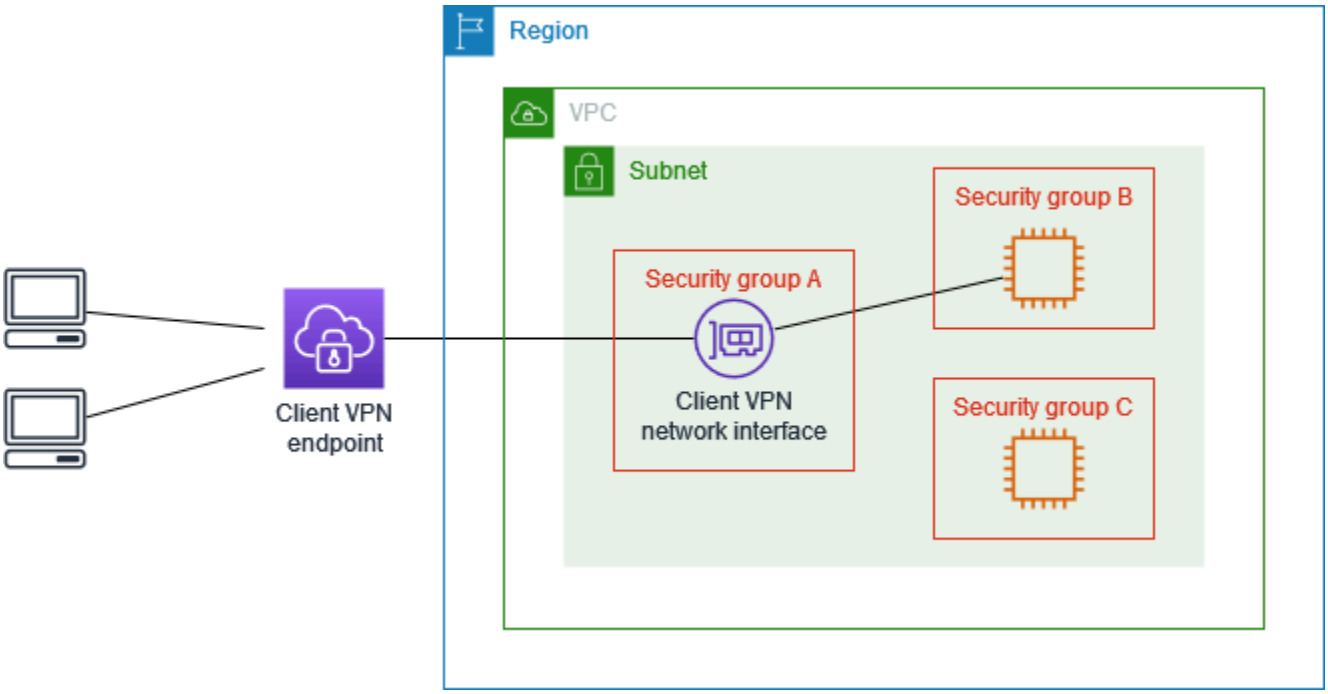
Den Zugriff mithilfe von Sicherheitsgruppen einschränken

Sie können den Zugriff auf bestimmte Ressourcen in Ihrer VPC zulassen oder verweigern, indem Sie Sicherheitsgruppenregeln hinzufügen oder entfernen, die sich auf die Sicherheitsgruppe beziehen, die auf die Zielnetzwerk-Zuordnung (die Client VPN-Sicherheitsgruppe) angewendet wurde. Diese Konfiguration erweitert das unter beschriebene Szenari Mit AWS Client-VPN auf eine VPC zugreifen. Diese Konfiguration wird zusätzlich zu den in diesem Szenario konfigurierten Autorisierungsregeln angewendet.

Um Zugriff auf eine spezifische Ressource zu gewähren, identifizieren Sie die Sicherheitsgruppe, die der Instance zugeordnet ist, auf der Ihre Ressource ausgeführt wird. Erstellen Sie dann eine Regel, die Datenverkehr aus der Client VPN-Sicherheitsgruppe zulässt.

In der folgenden Abbildung ist Sicherheitsgruppe A die Client-VPN-Sicherheitsgruppe, Sicherheitsgruppe B ist einer EC2-Instance zugeordnet und Sicherheitsgruppe C ist einer EC2-Instance zugeordnet. Wenn Sie der Sicherheitsgruppe B eine Regel hinzufügen, die den Zugriff von Sicherheitsgruppe A aus ermöglicht, können Clients auf die Instance zugreifen, die der Sicherheitsgruppe B zugeordnet ist. Wenn bei Sicherheitsgruppe C keine Regel den Zugriff

von Sicherheitsgruppe A aus erlaubt, können Clients nicht auf die Instance zugreifen, die der Sicherheitsgruppe C zugeordnet ist.



Bevor Sie beginnen, prüfen Sie, ob die Client VPN-Sicherheitsgruppe anderen Ressourcen in Ihrer VPC zugeordnet ist. Wenn Sie Regeln hinzufügen oder entfernen, die sich auf die Client VPN-Sicherheitsgruppe beziehen, können Sie den Zugriff auch für die anderen zugehörigen Ressourcen gewähren oder verweigern. Um dies zu verhindern, verwenden Sie eine Sicherheitsgruppe, die speziell für die Verwendung mit Ihrem Client VPN-Endpunkt erstellt wurde.

So erstellen Sie eine Sicherheitsgruppenregel

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe aus, die der Instance zugeordnet ist, auf der Ihre Ressource ausgeführt wird.
4. Wählen Sie Actions (Aktionen), Edit inbound rules (Eingangsregeln bearbeiten) aus.
5. Wählen Sie Add Rule (Regel hinzufügen) und gehen Sie wie folgt vor:

   - Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) oder einen bestimmten Datenverkehrstyp aus, den Sie zulassen möchten.
   - Wählen Sie für Source (Quelle) die Option Custom (Benutzerdefiniert) aus. Geben Sie dann die ID der Client VPN-Sicherheitsgruppe ein oder wählen Sie sie aus.

6. Wählen Sie Save rules (Regeln speichern) aus

Um den Zugriff auf eine spezifische Ressource zu entfernen, überprüfen Sie die Sicherheitsgruppe, die der Instance zugeordnet ist, auf der Ihre Ressource ausgeführt wird. Wenn es eine Regel gibt, die Datenverkehr aus der Client VPN-Sicherheitsgruppe zulässt, löschen Sie diese.

So prüfen Sie Ihre Sicherheitsgruppenregeln

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie Inbound Rules (Eingangsregeln) aus.
4. Überprüfen Sie die Liste der Regeln. Wenn es eine Regel gibt, bei der Source (Quelle) die Client VPN-Sicherheitsgruppe ist, wählen Sie Edit Rules (Regeln bearbeiten) aus. Wählen Sie dann Delete (Löschen) (das X-Symbol) für die Regel aus. Wählen Sie Save rules (Regeln speichern) aus.

Den Zugriff basierend auf Benutzergruppen einschränken

Wenn Ihr Client VPN-Endpunkt für die benutzerbasierte Authentifizierung konfiguriert ist, können Sie spezifischen Benutzergruppen Zugriff auf spezifische Teile des Netzwerks gewähren. Führen Sie dazu die folgenden Schritte aus:

1. Konfigurieren Sie Benutzer und Gruppen in AWS Directory Service oder Ihrem IdP. Weitere Informationen finden Sie unter den folgenden Themen:
   - Active Directory-Authentifizierung
   - Anforderungen und Überlegungen für die SAML-basierte Verbundauthentifizierung
2. Erstellen Sie eine Autorisierungsregel für Ihren Client VPN-Endpunkt, die einer bestimmten Gruppe den Zugriff auf das gesamte oder einen Teil Ihres Netzwerks ermöglicht. Weitere Informationen finden Sie unter Autorisierungsregeln.

Wenn Ihr Client VPN-Endpunkt für die gegenseitige Authentifizierung konfiguriert ist, können Sie keine Benutzergruppen konfigurieren. Wenn Sie eine Autorisierungsregel erstellen, müssen Sie allen Benutzern Zugriff gewähren. Um bestimmten Benutzergruppen den Zugriff auf spezifische Teile Ihres Netzwerks zu ermöglichen, können Sie mehrere Client VPN-Endpunkte erstellen. Führen Sie beispielsweise für jede Benutzergruppe, die auf Ihr Netzwerk zugreift, die folgenden Schritte aus:

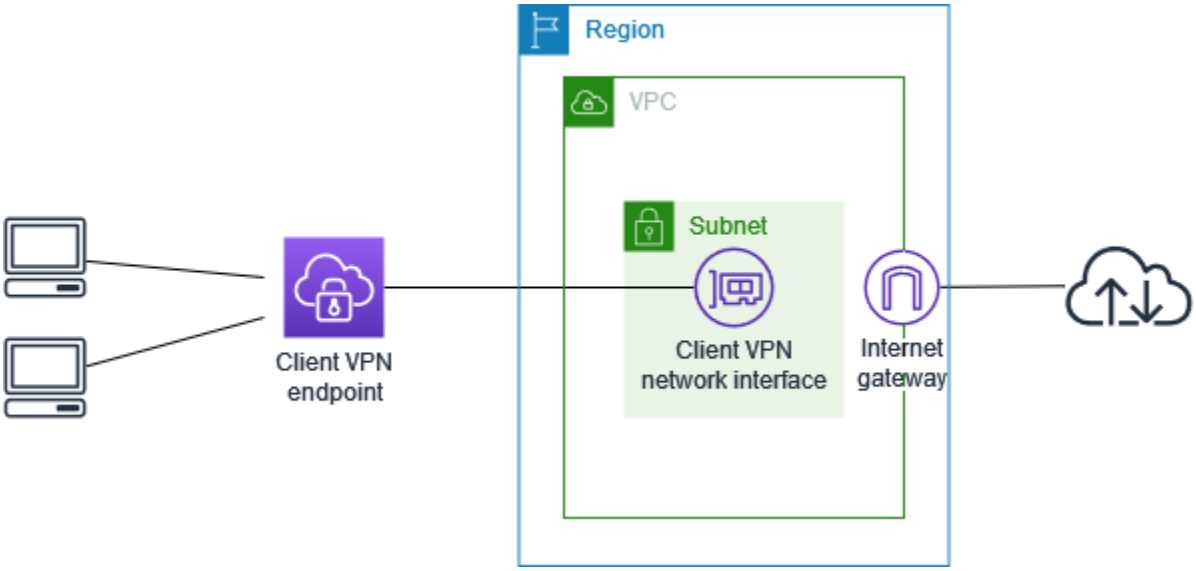
1. Erstellen Sie eine Gruppe von Server- und Clientzertifikaten und -schlüsseln für diese Benutzergruppe. Weitere Informationen finden Sie unter Gegenseitige Authentifizierung.
2. Erstellen Sie einen Client VPN-Endpunkt. Weitere Informationen finden Sie unter Erstellen eines Client VPN-Endpunkts.
3. Erstellen Sie eine Autorisierungsregel, die Zugriff auf das gesamte oder einen Teil Ihres Netzwerks gewährt. Beispielsweise können Sie für einen Client VPN-Endpunkt, der von Administratoren verwendet wird, eine Autorisierungsregel erstellen, die Zugriff auf das gesamte Netzwerk gewährt. Weitere Informationen finden Sie unter Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt.

Erste Schritte mit AWS-Client-VPN

In diesem Tutorial erstellen Sie einen Client-VPN-Endpunkt, der folgende Funktionen erfüllt:

- Bietet allen Clients Zugriff auf eine einzelne VPC.
- Bietet allen Clients Zugriff auf das Internet.
- Verwendet die gegenseitige Authentifizierung.

Das folgende Diagramm zeigt die Konfiguration Ihrer VPC und des Client VPN-Endpunkts nach Abschluss dieses Tutorials.



Schritte

- Voraussetzungen
- Schritt 1: Erstellen von Server- und Client-Zertifikaten
- Schritt 2: Erstellen eines Client VPN-Endpunkts
- Schritt 3: Zuordnen eines Zielnetzwerks
- Schritt 4: Hinzufügen einer Autorisierungsregel für die VPC
- Schritt 5: Erteilen des Zugriffs auf das Internet.
- Schritt 6: Überprüfen der Sicherheitsgruppen-Anforderungen
- Schritt 7: Herunterladen der Konfigurationsdatei für den Client-VPN-Endpunkt
- Schritt 8: Herstellen einer Verbindung zum Client-VPN-Endpunkt

Voraussetzungen

Stellen Sie vor Beginn dieses Erste-Schritte-Tutorials sicher, dass Sie über Folgendes verfügen:

- Die für die Arbeit mit Client VPN-Endpunkten erforderlichen Berechtigungen.
- Die Berechtigungen, die zum Importieren von Zertifikaten in AWS Certificate Manager erforderlich sind.
- Eine VPC mit mindestens einem Subnetz und einem Internet-Gateway. Die mit Ihrem Subnetz verknüpfte Routing-Tabelle muss über eine Route zum Internet-Gateway verfügen.

Schritt 1: Erstellen von Server- und Client-Zertifikaten

Dieses Tutorial verwendet die gegenseitige Authentifizierung. Bei der gegenseitigen Authentifizierung verwendet Client VPN Zertifikate zur Authentifizierung zwischen den Clients und dem Client-VPN-Endpunkt. Sie benötigen ein Serverzertifikat und einen Serverschlüssel sowie mindestens ein Client-Zertifikat und -einen Client-Schlüssel. Zumindest muss das Serverzertifikat in AWS Certificate Manager (ACM) importiert und beim Erstellen des Client-VPN-Endpunkts angegeben werden. Das Importieren des Client-Zertifikats in ACM ist optional.

Wenn Sie noch keine Zertifikate haben, die Sie für diesen Zweck verwenden können, können diese über das OpenVPN-Dienstprogramm easy-rsa erstellt werden. Ausführliche Schritte zum Generieren der Server- und Client-Zertifikate und Schlüssel unter Verwendung des OpenVPN-Dienstprogramms easy-rsa sowie zu deren Import in ACM finden Sie unter Gegenseitige Authentifizierung.

> **Note**
>
> Das Serverzertifikat muss mit AWS Certificate Manager (ACM) in derselben AWS-Region bereitgestellt werden, in der Sie den Client-VPN-Endpunkt erstellen, oder dorthin importiert werden.

Schritt 2: Erstellen eines Client VPN-Endpunkts

Ein Client VPN-Endpunkt ist die Ressource, die Sie erstellen und konfigurieren, um Client VPN-Sitzungen zu aktivieren und zu verwalten. Es handelt sich hier um den Beendigungspunkt für alle Client-VPN-Sitzungen.

So erstellen Sie einen Client VPN-Endpunkt

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client-VPN-Endpunkte) und dann Create Client VPN Endpoint (Client-VPN-Endpunkt erstellen) aus.
3. (Optional) Geben Sie ein Namens-Tag und eine Beschreibung für den Client-VPN-Endpunkt ein.
4. Geben Sie für Client IPv4-CIDR den IP-Adressbereich, in CIDR-Notation, ein, aus dem die Client-IP-Adressen zugewiesen werden.

   > **Note**
   >
   > Der IP-Adressbereich darf sich nicht mit dem Zielnetzwerk-Adressbereich, dem VPC-Adressbereich oder einer der Routen überschneiden, die dem Client-VPN-Endpunkt zugeordnet werden. Der Client-Adressbereich muss eine CIDR-Blockgröße von mindestens /22 und maximal /12 aufweisen. Sie können den Client-Adressbereich nicht mehr ändern, nachdem Sie den Client-VPN-Endpunkt erstellt haben.

5. Wählen Sie für Server certificate ARN (Serverzertifikats-ARN) den ARN des Serverzertifikats aus, das Sie in Schritt 1 erstellt haben.
6. Wählen Sie unter Authentication options (Authentifizierungsoptionen) Use mutual authentication (Wechselseitige Authentifizierung verwenden) und dann für Client certificate ARN (Client-Zertifikats-ARN) den ARN des Zertifikats aus, das Sie als Client-Zertifikat verwenden möchten.

   Wenn das Server- und das Client-Zertifikat von derselben Zertifizierungsstelle (CA) ausgestellt wurden, können Sie den ARN des Serverzertifikats sowohl für die Client- als auch für die Serverzertifikate verwenden. In diesem Szenario kann jedes Client-Zertifikat, das dem Serverzertifikat entspricht, zur Authentifizierung verwendet werden.
7. Behalten Sie die übrigen Standardeinstellungen bei und wählen Sie Create Client VPN endpoint (Client-VPN-Endpunkt erstellen) aus.

Nachdem Sie den Client VPN-Endpunkt erstellt haben, lautet sein Status `pending-associate`. Clients können nur eine VPN-Verbindung herstellen, nachdem Sie mindestens ein Zielnetzwerk verknüpft haben.

Weitere Informationen zu den Optionen, die Sie für einen eines Client VPN-Endpunkt angeben können, finden Sie unter Erstellen eines Client VPN-Endpunkts.

Schritt 3: Zuordnen eines Zielnetzwerks

Damit Clients eine VPN-Sitzung erstellen können, ordnen Sie dem Client-VPN-Endpunkt ein Zielnetzwerk zu. Ein Zielnetzwerk ist ein Subnetz in einer VPC.

Zuordnen eines Zielnetzwerks zu einem Client-VPN-Endpunkt

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den im vorherigen Verfahren erstellten Client-VPN-Endpunkt und anschließend Target network associations (Zielnetzwerkzuordnungen), Associate target network (Zielnetzwerk zuordnen) aus.
4. Wählen Sie für VPC die VPC aus, in der sich das Subnetz befindet.
5. Wählen Sie für Choose a subnet to associate (Zuzuordnendes Subnetz auswählen) das Subnetz aus, das dem Client-VPN-Endpunkt zugeordnet werden soll.
6. Wählen Sie Associate target network (Zielnetzwerk zuordnen) aus.
7. Wenn es die Autorisierungsregeln zulassen, genügt eine Subnetz-Zuordnung, damit Clients auf das gesamte Netzwerk einer VPC zugreifen können. Sie können zusätzliche Subnetze verknüpfen, um eine hohe Verfügbarkeit zu gewährleisten, falls eine Availability Zone beschädigt wird.

Wenn Sie dem Client VPN-Endpunkt das erste Subnetz zuordnen, geschieht Folgendes:

- Der Status des Client VPN-Endpunkts ändert sich in `available`. Clients können jetzt eine VPN-Verbindung herstellen, aber sie können erst auf Ressourcen in der VPC zugreifen, wenn Sie die Autorisierungsregeln hinzugefügt haben.
- Die lokale Route der VPC wird der Client VPN-Endpunkt-Routing-Tabelle automatisch hinzugefügt.
- Die Standard-Sicherheitsgruppe der VPC wird für den Client-VPN-Endpunkt automatisch angewendet.

Schritt 4: Hinzufügen einer Autorisierungsregel für die VPC

Damit Clients auf die VPC zugreifen können, muss es eine Route zur VPC in der Routing-Tabelle des Client-VPN-Endpunkts sowie eine Autorisierungsregel geben. Die Route wurde bereits im vorherigen

Schritt automatisch hinzugefügt. In diesem Tutorial soll allen Benutzern Zugriff auf die VPC gewährt werden.

So fügen Sie eine Autorisierungsregel für die VPC hinzu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt aus, zu dem die Autorisierungsregel hinzugefügt werden soll. Wählen Sie Authorization rules (Autorisierungsregeln) und dann Add authorization rule (Autorisierungsregel hinzufügen) aus.
4. Geben Sie unter Destination network to enable access (Zielnetzwerk, für das Zugriff erlaubt werden soll) den CIDR des Netzwerks ein, für das sie den Zugriff erlauben möchten. Wenn Sie beispielsweise den Zugriff auf die gesamte VPC erlauben möchten, geben Sie den IPv4-CIDR-Block der VPC an.
5. Wählen Sie unter Grant access to (Zugriff gewähren für) die Option Allow access to all users (Zugriff für alle Benutzer gewähren) aus.
6. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Autorisierungsregel ein.
7. Wählen Sie Add authorization rule (Autorisierungsregel hinzufügen) aus.

Schritt 5: Erteilen des Zugriffs auf das Internet.

Sie können den Zugriff auf zusätzliche Netzwerke, die mit der VPC verbunden sind, wie z. B. AWS-Dienste, per Peering verbundene VPCs und On-Premises-Netzwerke, erteilen. Für jedes zusätzliche Netzwerk fügen Sie dem Netzwerk in der Routing-Tabelle des Client-VPN-Endpunkts eine Route hinzu und konfigurieren eine Autorisierungsregel, um Clients Zugriff zu gewähren.

In diesem Tutorial soll allen Benutzern Zugriff auf das Internet sowie auf die VPC gewährt werden. Sie haben bereits den Zugriff auf die VPC konfiguriert, daher wird in diesem Schritt Zugriff auf das Internet erteilt.

So erteilen Sie Zugriff auf das Internet

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.

3. Wählen Sie den Client-VPN-Endpunkt aus, den Sie für dieses Tutorial erstellt haben. Wählen Sie Route Table (Routing-Tabelle) und dann Create Route (Route erstellen) aus.
4. Geben Sie für Route destination (Routing-Ziel), `0.0.0.0/0` ein. Geben Sie für Subnet ID for target network association (Subnetz-ID für die Zielnetzwerkzuordnung) die ID des Subnetzes ein, über das der Datenverkehr geleitet werden soll.
5. Klicken Sie auf Create Route (Route erstellen).
6. Wählen Sie Authorization rules (Autorisierungsregeln) und dann Add authorization rule (Autorisierungsregel hinzufügen) aus.
7. Geben Sie für Destination network to enable access (Zielnetzwerk, für das Zugriff erteilt werden soll) `0.0.0.0/0` ein und wählen Sie Allow access to all users (Zugriff für alle Benutzer gewähren) aus.
8. Wählen Sie Add authorization rule (Autorisierungsregel hinzufügen) aus.

Schritt 6: Überprüfen der Sicherheitsgruppen-Anforderungen

In diesem Tutorial wurden bei der Erstellung des Client-VPN-Endpunkts in Schritt 2 keine Sicherheitsgruppen angegeben. Somit wird automatisch die Standardsicherheitsgruppe für die VPC auf den Client-VPN-Endpunkt angewendet, wenn ein Zielnetzwerk zugeordnet wird. Folglich sollte die Standardsicherheitsgruppe für die VPC jetzt dem Client-VPN-Endpunkt zugeordnet werden.

Stellen Sie sicher, dass die folgenden Sicherheitsgruppen-Anforderungen erfüllt sind:

- Die Sicherheitsgruppe, die dem Subnetz zugeordnet ist, durch das Sie den Datenverkehr leiten (in diesem Fall die Standard-VPC-Sicherheitsgruppe), lässt ausgehenden Datenverkehr zum Internet zu. Fügen Sie zu diesem Zweck eine Regel für ausgehenden Datenverkehr hinzu, die den gesamten Datenverkehr zum Ziel-`0.0.0.0/0` zulässt.
- Die Sicherheitsgruppen für die Ressourcen in Ihrer VPC verfügen über eine Regel, die den Zugriff von der Sicherheitsgruppe zulässt, die auf den Client-VPN-Endpunkt (in diesem Fall die Standard-VPC-Sicherheitsgruppe) angewendet wird. Auf diese Weise können Ihre Clients auf die Ressourcen in Ihrer VPC zugreifen.

Weitere Informationen finden Sie unter Sicherheitsgruppen.

Schritt 7: Herunterladen der Konfigurationsdatei für den Client-VPN-Endpunkt

Der nächste Schritt besteht darin, die Client-VPN-Endpunkt-Konfigurationsdatei herunterzuladen und vorzubereiten. Die Konfigurationsdatei enthält die Client-VPN-Endpunktdetails und die Zertifikatsinformationen, die für eine VPN-Verbindung erforderlich sind. Diese Datei stellen Sie den Endbenutzern, die eine Verbindung mit dem Client-VPN-Endpunkt benötigen, zur Verfügung. Die Endbenutzer verwenden die Datei zur Konfiguration ihrer VPN-Client-Anwendung.

So laden Sie die Client VPN-Endpunkt-Konfigurationsdatei herunter und bereiten sie vor

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt aus, den Sie für dieses Tutorial erstellt haben, und wählen Sie Download client configuration (Client-Konfiguration herunterladen) aus.
4. Suchen Sie das Client-Zertifikat und den Schlüssel, die in Schritt 1 generiert wurden. Das Client-Zertifikat und den Schlüssel finden Sie an den folgenden Speicherorten im geklonten OpenVPN Easy-RSA-Repository:

   - Client-Zertifikat — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Client-Schlüssel — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`

5. Öffnen Sie die Client-VPN-Endpunktkonfigurationsdatei mit Ihrem bevorzugten Texteditor. Fügen Sie der Datei die Tags `<cert></cert>` und `<key></key>` hinzu. Platzieren Sie den Inhalt des Client-Zertifikats und den Inhalt des privaten Schlüssels zwischen den entsprechenden Tags:

   ```
   <cert>
   Contents of client certificate (.crt) file
   </cert>

   <key>
   Contents of private key (.key) file
   </key>
   ```

6. Speichern und schließen Sie die Client VPN-Endpunkt-Konfigurationsdatei.
7. Verteilen Sie die Client-VPN-Endpunkt-Konfigurationsdatei an Ihre Endbenutzer.

Weitere Hinweise zur Client VPN-Endpunkt-Konfigurationsdatei finden Sie unter Exportieren und Konfigurieren der Client-Konfigurationsdatei.

Schritt 8: Herstellen einer Verbindung zum Client-VPN-Endpunkt

Sie können über den von AWS bereitgestellten Client oder eine andere OpenVPN-basierte Client-Anwendung und die soeben erstellte Konfigurationsdatei eine Verbindung mit dem Client-VPN-Endpunkt herstellen. Weitere Informationen finden Sie im AWS Client VPN-Benutzerhandbuch.

Arbeiten mit AWS Client VPN

In den folgenden Themen wird erläutert, wie Sie mit Client-VPN arbeiten.

Inhalt

Zugriff auf das Self-Service-Portal

Nach der Aktivierung des Self-Service-Portals für Ihren Client-VPN-Endpunkt können Sie Ihren Kunden eine URL für das Self-Service-Portal bereitstellen. Kunden können in einem Webbrowser auf das Portal zugreifen und sich mit ihren benutzerbasierten Anmeldeinformationen anmelden. Kunden können die Konfigurationsdatei für Client-VPN-Endpunkte aus dem Portal herunterladen und die neueste Version des von AWS bereitgestellten Clients herunterladen.

Die folgenden Regeln gelten:

- Das Self-Service-Portal ist nicht für Clients verfügbar, die sich mittels gegenseitiger Authentifizierung authentifizieren.
- Die Konfigurationsdatei, die im Self-Service-Portal verfügbar ist, ist dieselbe Konfigurationsdatei, die Sie mit der Amazon VPC-Konsole oder der AWS CLI exportieren. Wenn Sie die Konfigurationsdatei anpassen müssen, bevor Sie sie an Clients verteilen, müssen Sie die angepasste Datei selbst an die Clients verteilen.

- Sie müssen die Self-Service-Portal-Option für Ihren Client-VPN-Endpunkt aktivieren, damit Clients auf das Portal zugreifen können. Wenn diese Option nicht aktiviert ist, können Sie Ihren Client-VPN-Endpunkt ändern, um ihn zu aktivieren.

Nachdem Sie die Self-Service-Portal-Option aktiviert haben, stellen Sie Ihren Kunden eine der folgenden URLs zur Verfügung:

- `https://self-service.clientvpn.amazonaws.com/`

  Wenn diese mit dieser URL auf das Portal zugreifen, müssen sie die ID des Client-VPN-Endpunkts eingeben, bevor sie sich anmelden können.
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  Ersetzen Sie *<endpoint-id>* in der vorherigen URL durch die ID Ihres Client-VPN-Endpunkts, z.B. `cvpn-endpoint-0123456abcd123456`.

Sie können die URL für das Self-Service-Portal auch in der Ausgabe des AWS CLI-Befehls describe-client-vpn-endpoints einsehen. Alternativ finden Sie die URL auf der Registerkarte Details auf der Seite Client VPN Endpoints (Client-VPN-Endpunkte) in der Amazon-VPC-Konsole.

Weitere Informationen zum Konfigurieren des Self-Service-Portals für die Verwendung mit föderierter Authentifizierung finden Sie unter Unterstützung des Self-Service-Portals.

Autorisierungsregeln

Autorisierungsregeln dienen als Firewall-Regeln, die den Zugriff auf Netzwerke regeln. Durch das Hinzufügen von Autorisierungsregeln gewähren Sie bestimmten Clients Zugriff auf das angegebene Netzwerk. Für jedes Netzwerk, für das Sie Zugriff gewähren möchten, sollten Sie eine Autorisierungsregel festlegen. Sie können einem Client VPN-Endpunkt mithilfe der Konsole und der AWS CLI Autorisierungsregeln hinzufügen.

> **Note**
>
> Client VPN verwendet bei der Auswertung von Autorisierungsregeln das längste übereinstimmende Präfix. Weitere Details finden Sie im Fehlerbehebungsthema Autorisierungsregeln für Active Directory-Gruppen, die nicht wie erwartet funktionieren und unter Routenpriorität im Benutzerhandbuch zu Amazon VPC.

Inhalt

Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt

So fügen Sie einem Client-VPN-Endpunkt mit AWS Management Console eine Autorisierungsregel hinzu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, zu dem Sie die Autorisierungsregel hinzufügen möchten, sowie die Optionen Authorization rules (Autorisierungsregeln) und Add authorization rule (Autorisierungsregel hinzufügen) aus.
4. Geben Sie für Destination network to enable access (Zielnetzwerk, für das Zugriff ermöglicht werden soll) die IP-Adresse des Netzwerks in CIDR-Notation ein, auf das Benutzer zugreifen sollen (z. B. den CIDR-Block Ihrer VPC).
5. Geben Sie an, welche Clients auf das angegebene Netzwerk zugreifen dürfen. Führen Sie für die Option For grant access to (Zum Gewähren von Zugriff auf) einen der folgenden Schritte aus:

   - Wenn Sie allen Clients Zugriff gewähren möchten, wählen Sie Allow access to all users (Allen Benutzern Zugriff gewähren) aus.
   - Um den Zugriff auf bestimmte Clients zu beschränken, wählen Sie Zugriff für Benutzer in einer bestimmten Zugriffsgruppe zulassen aus und geben Sie dann unter Zugriffsgruppen-ID die ID für die Gruppe ein, für die der Zugriff gewährt werden soll. Das kann beispielsweise die Sicherheits-ID (SID) einer Active Directory-Gruppe oder die ID/der Name einer Gruppe sein, die in einem SAML-basierten Identitätsanbieter (Identity Provider, IdP) definiert ist.
     - (Active Directory) Sie können das Microsoft Powershell-Cmdlet Get-ADGroup verwenden, um die SID abzurufen, z. B.:

       ```
       Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
       ```

Alternativ können Sie das Tool „Active Directory-Benutzer und -Computer“ öffnen, die Eigenschaften für die Gruppe anzeigen, zur Registerkarte „Attribut-Editor“ wechseln und den Wert für `objectSID` abrufen. Wählen Sie ggf. zuerst View (Ansicht), Advanced Features (Erweiterte Funktionen), um die Registerkarte „Attribut-Editor“ zu aktivieren.

- (SAML-basierte Verbundauthentifizierung) Die Gruppen-ID/der Gruppenname sollte mit den Gruppenattributinformationen übereinstimmen, die in der SAML-Assertion zurückgegeben werden.

6. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Autorisierungsregel ein.
7. Wählen Sie Add authorization rule (Autorisierungsregel hinzufügen) aus.

Hinzufügen einer Autorisierungsregel zu einem Client VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl authorize-client-vpn-ingress.

Entfernen einer Autorisierungsregel von einem Client VPN-Endpunkt

Indem Sie eine Autorisierungsregel löschen, entfernen Sie den Zugriff auf das angegebene Netzwerk.

Sie können Autorisierungsregeln aus einem Client VPN-Endpunkt über die Konsole oder die AWS CLI entfernen.

So entfernen Sie eine Autorisierungsregel aus einem Client VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, zu dem die Autorisierungsregel hinzugefügt wird, sowie die Option Authorization rules (Autorisierungsregeln) aus.
4. Wählen Sie die zu löschende Autorisierungsregel, Remove authorization rule (Autorisierungsregel entfernen) und dann Remove authorization rule (Autorisierungsregel entfernen) aus.

Entfernen einer Autorisierungsregel von einem Client VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl revoke-client-vpn-ingress.

Autorisierungsregeln anzeigen

Sie können Autorisierungsregeln für einen bestimmten Client VPN-Endpunkt mit der Konsole und der AWS CLI anzeigen.

So zeigen Sie Autorisierungsregeln an (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, für den die Autorisierungsregeln angezeigt werden sollen, und die Option Authorization rules (Autorisierungsregeln) aus.

So zeigen Sie Autorisierungsregeln an (AWS CLI)

Verwenden Sie den Befehl describe-client-vpn-authorization-rules.

Beispielszenarien für Autorisierungsregeln

In diesem Abschnitt wird beschrieben, wie Autorisierungsregeln für AWS Client VPN funktionieren. Der Abschnitt enthält wichtige Informationen zu Autorisierungsregeln, eine Beispielarchitektur und Beispielszenarien entsprechend der Beispielarchitektur.

Inhalt

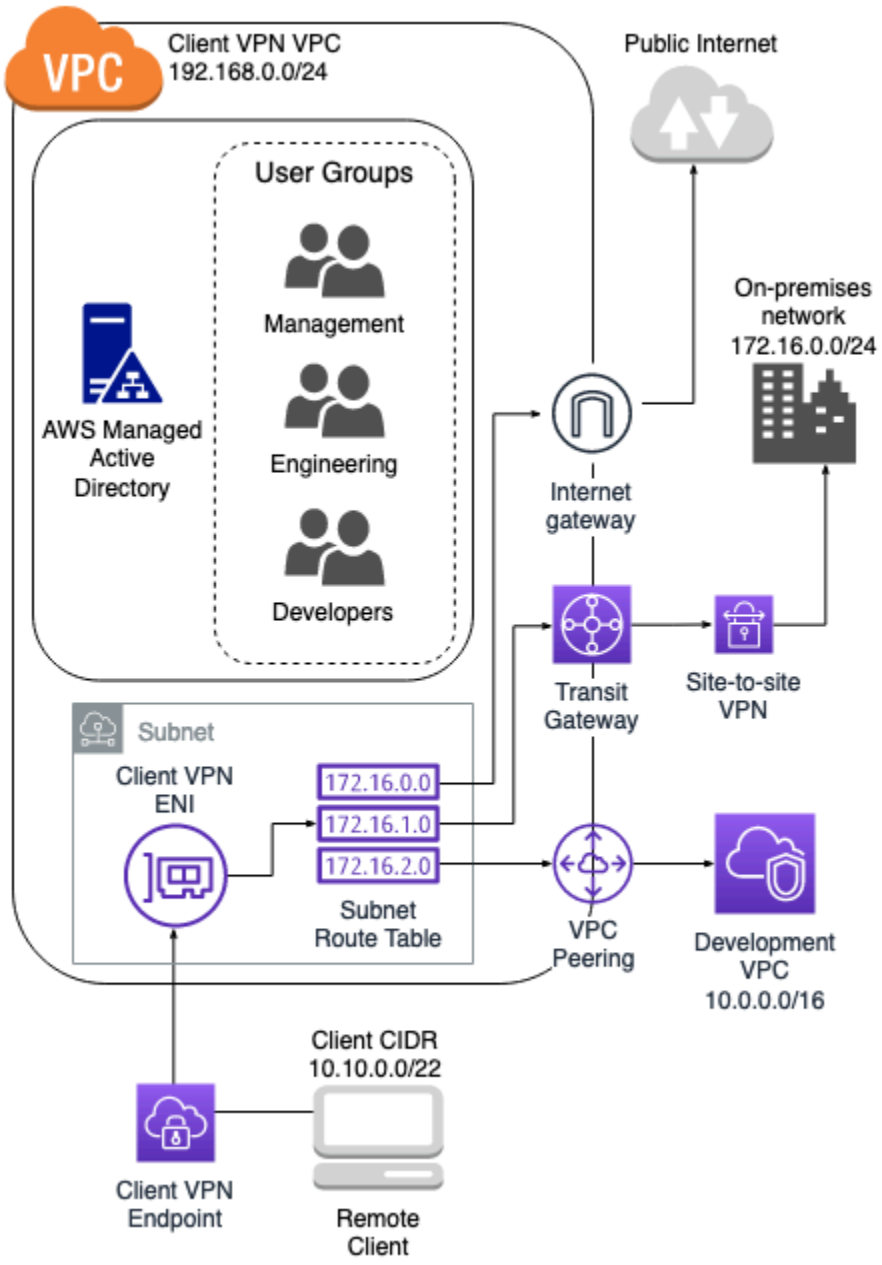
Wichtige Informationen zu Autorisierungsregeln

Die folgenden Punkte beschreiben einen Teil des Verhaltens von Autorisierungsregeln:

- Um den Zugriff auf ein Zielnetzwerk zu ermöglichen, muss eine Autorisierungsregel explizit hinzugefügt werden. Das Standardverhalten ist das Verweigern des Zugriffs.
- Sie können keine Autorisierungsregel zum Beschränken des Zugriffs auf ein Zielnetzwerk hinzufügen.
- Das CIDR `0.0.0.0/0` wird als Sonderfall behandelt. Es wird zuletzt verarbeitet, unabhängig von der Reihenfolge, in der die Autorisierungsregeln erstellt wurden.
- Sie können sich das CIDR `0.0.0.0/0` als „jedes Ziel“ oder „jedes Ziel, das nicht durch andere Autorisierungsregeln definiert wird“ vorstellen.
- Die längste Präfixübereinstimmung ist die Regel, die Vorrang hat.

Beispielarchitektur für Szenarien zu Autorisierungsregeln

Das folgende Diagramm zeigt die Beispielarchitektur, die für die Beispielszenarien in diesem Abschnitt verwendet wird.



Szenario 1: Zugriff auf ein einzelnes Ziel

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premis	S-xxxxx14	Falsch	172.16.0.0/24

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
es-Netzwerk für die Engineering-Gruppe			
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	S-xxxxx15	Falsch	10.0.0.0/16
Erlauben des Zugriffs auf eine Client-VPN-VPC für die Managergruppe	S-xxxxx16	Falsch	192.168.0.0/24

Resultierendes Verhalten

- Die Engineering-Gruppe kann nur auf `172.16.0.0/24` zugreifen.
- Die Entwicklungsgruppe kann nur auf `10.0.0.0/16` zugreifen.
- Die Managergruppe kann nur auf `192.168.0.0/24` zugreifen.
- Der gesamte restliche Datenverkehr wird vom Client-VPN-Endpunkt gelöscht.

> **Note**
>
> In diesem Szenario hat keine Benutzergruppe Zugriff auf das öffentliche Internet.

Szenario 2: Verwenden des CIDR für jedes Ziel (0.0.0.0/0)

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
	S-xxxxx14	Falsch	172.16.0.0/24

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premises-Netzwerk für die Engineering-Gruppe			
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	S-xxxxx15	Falsch	10.0.0.0/16
Erlauben des Zugriffs auf jedes Ziel für die Managergruppe	S-xxxxx16	Falsch	0.0.0.0/0

Resultierendes Verhalten

- Die Engineering-Gruppe kann nur auf `172.16.0.0/24` zugreifen.
- Die Entwicklungsgruppe kann nur auf `10.0.0.0/16` zugreifen.
- Die Managergruppe kann auf das öffentliche Internet und auf `192.168.0.0/24` zugreifen, jedoch nicht auf `172.16.0.0/24` oder `10.0.0/16`.

> **Note**
>
> Da in diesem Szenario keine Regeln auf `192.168.0.0/24` verweisen, wird der Zugriff auf dieses Netzwerk auch durch die Regel `0.0.0.0/0` ermöglicht.
> Eine Regel, die `0.0.0.0/0` enthält, wird immer zuletzt ausgewertet, unabhängig von der Reihenfolge, in der die Regeln erstellt wurden. Beachten Sie daher, dass die vor `0.0.0.0/0` ausgewerteten Regeln eine Rolle bei der Ermittlung spielen, welchen Netzwerken `0.0.0.0/0` Zugriff gewährt.

Szenario 3: Längere IP-Präfixübereinstimmung

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premises-Netzwerk für die Engineering-Gruppe	S-xxxxx14	Falsch	172.16.0.0/24
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	S-xxxxx15	Falsch	10.0.0.0/16
Erlauben des Zugriffs auf jedes Ziel für die Managergruppe	S-xxxxx16	Falsch	0.0.0.0/0
Erlauben des Zugriffs auf einen einzelnen Host in einer Entwicklungs-VPC für die Managergruppe	S-xxxxx16	Falsch	10.0.0.44/32

Resultierendes Verhalten

- Die Engineering-Gruppe kann nur auf `172.16.0.0/24` zugreifen.
- Die Entwicklungsgruppe kann auf `10.0.0.0/16` zugreifen, außer auf den einzelnen Host `10.0.2.119/32`.
- Die Managergruppe kann auf das öffentliche Internet, `192.168.0.0/24`, und einen einzelnen Host (`10.0.2.119/32`) innerhalb der Entwicklungs-VPC zugreifen, sie hat jedoch keinen Zugriff auf `172.16.0.0/24` oder einen der übrigen Hosts in der Entwicklungs-VPC.

> **Note**
>
> Hier sehen Sie, dass eine Regel mit einem längeren IP-Präfix Vorrang vor einer Regel mit einem kürzeren IP-Präfix hat. Wenn die Entwicklungsgruppe Zugriff auf `10.0.2.119/32` haben soll, muss eine zusätzliche Regel hinzugefügt werden, die dem Entwicklungsteam Zugriff auf `10.0.2.119/32` gewährt.

Szenario 4: Überlappendes CIDR (gleiche Gruppe)

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premises-Netzwerk für die Engineering-Gruppe	S-xxxxx14	Falsch	172.16.0.0/24
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	S-xxxxx15	Falsch	10.0.0.0/16
Erlauben des Zugriffs auf jedes Ziel für die Managergruppe	S-xxxxx16	Falsch	0.0.0.0/0
Erlauben des Zugriffs auf einen einzelnen Host in einer Entwicklungs-VPC für die Managergruppe	S-xxxxx16	Falsch	10.0.0.44/32

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein kleineres Subnetz innerhalb eines On-Premises-Netzwerks für die Engineering-Gruppe	S-xxxxx14	Falsch	172,160,128/ 25

Resultierendes Verhalten

- Die Entwicklungsgruppe kann auf `10.0.0.0/16` zugreifen, außer auf den einzelnen Host `10.0.2.119/32`.
- Die Managergruppe kann auf das öffentliche Internet, `192.168.0.0/24`, und einen einzelnen Host (`10.0.2.119/32`) innerhalb des Netzwerks `10.0.0.0/16` zugreifen, sie hat jedoch keinen Zugriff auf `172.16.0.0/24` oder einen der übrigen Hosts im Netzwerk `10.0.0.0/16`.
- Die Engineering-Gruppe hat Zugriff auf `172.16.0.0/24`, einschließlich des spezifischeren Subnetzes `172.16.0.128/25`.

Szenario 5: Zusätzliche Regel für 0.0.0.0/0

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premises-Netzwerk für die Engineering-Gruppe	S-xxxxx14	Falsch	172.16.0.0/24
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	S-xxxxx15	Falsch	10.0.0.0/16

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf jedes Ziel für die Managergruppe	S-xxxxx16	Falsch	0.0.0.0/0
Erlauben des Zugriffs auf einen einzelnen Host in einer Entwicklu ngs-VPC für die Managergruppe	S-xxxxx16	Falsch	10.0.0.44/32
Erlauben des Zugriffs auf ein kleineres Subnetz innerhalb eines On-Premises-Netzwerks für die Engineering-Gruppe	S-xxxxx14	Falsch	172,160,128/ 25
Erlauben des Zugriffs auf jedes Ziel für die Engineering-Gruppe	S-xxxxx14	Falsch	0.0.0.0/0

Resultierendes Verhalten

- Die Entwicklungsgruppe kann auf `10.0.0.0/16` zugreifen, außer auf den einzelnen Host `10.0.2.119/32`.
- Die Managergruppe kann auf das öffentliche Internet, `192.168.0.0/24`, und einen einzelnen Host (`10.0.2.119/32`) innerhalb des Netzwerks `10.0.0.0/16` zugreifen, sie hat jedoch keinen Zugriff auf `172.16.0.0/24` oder einen der übrigen Hosts im Netzwerk `10.0.0.0/16`.
- Die Engineering-Gruppe kann auf das öffentliche Internet, `192.168.0.0/24`, und `172.16.0.0/24` zugreifen, einschließlich des spezifischeren Subnetzes `172.16.0.128/25`.

> **Note**
>
> Beachten Sie, dass jetzt sowohl die Engineering- als auch die Managergruppe auf `192.168.0.0/24` zugreifen können. Dies liegt daran, dass beide Gruppen Zugriff auf `0.0.0.0/0` (jedes Ziel) haben und keine anderen Regeln auf `192.168.0.0/24` verweisen.

Szenario 6: Hinzufügen einer Regel für 192.168.0.0/24

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premises-Netzwerk für die Engineering-Gruppe	S-xxxxx14	Falsch	172.16.0.0/24
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	S-xxxxx15	Falsch	10.0.0.0/16
Erlauben des Zugriffs auf jedes Ziel für die Managergruppe	S-xxxxx16	Falsch	0.0.0.0/0
Erlauben des Zugriffs auf einen einzelnen Host in einer Entwicklungs-VPC für die Managergruppe	S-xxxxx16	Falsch	10.0.0.44/32
	S-xxxxx14	Falsch	172,160,128/ 25

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein Subnetz im On-Premises-Netzwerk für die Engineering-Gruppe			
Erlauben des Zugriffs auf jedes Ziel für die Engineering-Gruppe	S-xxxxx14	Falsch	0.0.0.0/0
Erlauben des Zugriffs auf eine Client-VPN-VPC für die Managergruppe	S-xxxxx16	Falsch	192.168.0.0/24

Resultierendes Verhalten

- Die Entwicklungsgruppe kann auf `10.0.0.0/16` zugreifen, außer auf den einzelnen Host `10.0.2.119/32`.
- Die Managergruppe kann auf das öffentliche Internet, `192.168.0.0/24`, und einen einzelnen Host (`10.0.2.119/32`) innerhalb des Netzwerks `10.0.0.0/16` zugreifen, sie hat jedoch keinen Zugriff auf `172.16.0.0/24` oder einen der übrigen Hosts im Netzwerk `10.0.0.0/16`.
- Die Engineering-Gruppe kann auf das öffentliche Internet, `172.16.0.0/24`, und `172.16.0.128/25` zugreifen.

> **Note**
>
> Beachten Sie, dass das Hinzufügen der Regel für den Zugriff der Managergruppe auf `192.168.0.0/24` dazu führt, dass die Entwicklungsgruppe nicht länger Zugriff auf dieses Zielnetzwerk hat.

Szenario 7: Zugriff für alle Benutzergruppen

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premises-Netzwerk für die Engineering-Gruppe	S-xxxxx14	Falsch	172.16.0.0/24
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	S-xxxxx15	Falsch	10.0.0.0/16
Erlauben des Zugriffs auf jedes Ziel für die Managergruppe	S-xxxxx16	Falsch	0.0.0.0/0
Erlauben des Zugriffs auf einen einzelnen Host in einer Entwicklungs-VPC für die Managergruppe	S-xxxxx16	Falsch	10.0.0.44/32
Erlauben des Zugriffs auf ein Subnetz im On-Premises-Netzwerk für die Engineering-Gruppe	S-xxxxx14	Falsch	172,160,128/ 25
Erlauben des Zugriffs auf alle Netzwerke	S-xxxxx14	Falsch	0.0.0.0/0

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
für die Engineering-Gruppe			
Erlauben des Zugriffs auf eine Client-VPN-VPC für die Managergruppe	S-xxxxx16	Falsch	192.168.0.0/24
Erlauben des Zugriffs für alle Gruppen	–	Wahr	0.0.0.0/0

Resultierendes Verhalten

- Die Entwicklungsgruppe kann auf `10.0.0.0/16` zugreifen, außer auf den einzelnen Host `10.0.2.119/32`.
- Die Managergruppe kann auf das öffentliche Internet, `192.168.0.0/24`, und einen einzelnen Host (`10.0.2.119/32`) innerhalb des Netzwerks `10.0.0.0/16` zugreifen, sie hat jedoch keinen Zugriff auf `172.16.0.0/24` oder einen der übrigen Hosts im Netzwerk `10.0.0.0/16`.
- Die Engineering-Gruppe kann auf das öffentliche Internet, `172.16.0.0/24`, und `172.16.0.128/25` zugreifen.
- Alle anderen Benutzergruppen, zum Beispiel „Admin-Gruppe“, können auf das öffentliche Internet zugreifen, jedoch nicht auf andere Zielnetzwerke, die in den anderen Regeln definiert sind.

Client-Zertifikatsperrlisten

Sie können Client-Zertifikatsperrlisten verwenden, um den Zugriff auf einen Client VPN-Endpunkt für bestimmte Client-Zertifikate zu widerrufen.

> **Note**
>
> Weitere Informationen über die Generierung der Server- und Client-Zertifikate und Schlüssel finden Sie unter Gegenseitige Authentifizierung

Weitere Informationen zur Anzahl der Einträge, die Sie einer Client-Zertifikatsperrliste hinzufügen können, finden Sie unter Client VPN-Kontingente.

Inhalt

Generieren einer Client-Zertifikatsperrliste

Linux/macOS

Im folgenden Verfahren generieren Sie eine Client-Zertifikatssperrliste mithilfe des Befehlszeilen-Dienstprogramms OpenVPN Easy-RSA.

So generieren Sie eine Client-Zertifikatssperrliste mit OpenVPN Easy-RSA

1. Melden Sie sich an dem Server an, auf dem die easyrsa-Installation gehostet wird, die zur Generierung des Zertifikats verwendet wurde.
2. Wechseln Sie in den `easy-rsa/easyrsa3`-Ordner in Ihrem lokalen Repository.

   ```
   $ cd easy-rsa/easyrsa3
   ```

3. Widerrufen Sie das Client-Zertifikat und erstellen Sie die Client-Widerrufsliste.

   ```
   $ ./easyrsa revoke client1.domain.tld
   $ ./easyrsa gen-crl
   ```

   Geben Sie `yes` ein, wenn Sie dazu aufgefordert werden.

Windows

Im folgenden Verfahren wird die OpenVPN-Software verwendet, um eine Client-Sperrliste zu generieren. Es wird davon ausgegangen, dass Sie die Schritte zur Verwendung der OpenVPN-Software zum Generieren der Client- und Serverzertifikate und Schlüssel befolgt haben.

So generieren Sie eine Client-Zertifikatssperrliste mit EasyRSA-Version 3.x.x

1. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Verzeichnis EasyRSA-3.x.x, was davon abhängt, wo es auf Ihrem System installiert ist.

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. Führen Sie die Datei „EasyRSA-Start.bat“ aus, um die EasyRSA-Shell zu starten.

```
C:\> .\EasyRSA-Start.bat
```

3. Sperren Sie in der EasyRSA-Shell das Client-Zertifikat.

```
# ./easyrsa revoke client_certificate_name
```

4. Geben Sie „yes“ (ja) ein, wenn Sie dazu aufgefordert werden.
5. Generieren Sie die Client-Sperrliste.

```
# ./easyrsa gen-crl
```

6. Die Client-Sperrliste wird am folgenden Speicherort erstellt:

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

So generieren Sie eine Client-Zertifikatssperrliste mit früheren EasyRSA-Versionen

1. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum OpenVPN-Verzeichnis.

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. Führen Sie die Datei `vars.bat` aus.

```
C:\> vars
```

3. Widerrufen Sie das Client-Zertifikat und erstellen Sie die Client-Widerrufsliste.

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

Importieren einer Client-Zertifikatsperrliste

Sie benötigen eine zu importierende Datei für die Client-Zertifikatssperrliste. Weitere Informationen zum Generieren einer Client-Zertifikatsperrliste finden Sie unter Generieren einer Client-Zertifikatsperrliste.

Sie können eine Client-Zertifikatssperrliste über die Konsole und die AWS CLI importieren.

So importieren Sie eine Client-Zertifikatssperrliste (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client VPN-Endpunkt aus, für den die Client-Zertifikatsperrliste importiert werden soll.
4. Wählen Sie Actions (Aktionen) und dann Import Client Certificate CRL (Client-Zertifikatsperrlisten importieren).
5. Geben Sie für Certificate Revocation List (Zertifikatssperrliste) den Inhalt der Client-Zertifikatssperrlistendatei ein und wählen Sie Import client certificate CRL (Client-Zertifikatssperrliste importieren) aus.

So importieren Sie eine Client-Zertifikatssperrliste (AWS CLI)

Verwenden Sie den Befehl import-client-vpn-client-certificate-revocation-list.

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-
revocation-list file://path_to_CRL_file --client-vpn-endpoint-id endpoint_id --
region region
```

Exportieren einer Client-Zertifikatsperrliste

Sie können Client-Zertifikatssperrlisten über die Konsole und die AWS CLI exportieren.

So exportieren Sie eine Client-Zertifikatssperrliste (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client VPN-Endpunkt aus, für den die Client-Zertifikatsperrliste exportiert werden soll.
4. Wählen Sie Actions (Aktionen), Export Client Certificate CRL (Client-Zertifikatsperrliste exportieren) und Export Client Certificate CRL (Client-Zertifikatsperrliste exportieren) aus.

So exportieren Sie eine Client-Zertifikatssperrliste (AWS CLI)

Verwenden Sie den Befehl export-client-vpn-client-certificate-revocation-list.

Client-Verbindungen

Verbindungen sind VPN-Sitzungen, die von Clients eingerichtet wurden. Eine Verbindung wird hergestellt, wenn ein Client erfolgreich eine Verbindung mit einem Client VPN-Endpunkt aufbaut.

Inhalt

Anzeigen von Client-Verbindungen

Sie können Client-Verbindungen über die Konsole und die AWS CLI anzeigen. Die Verbindungsinformationen enthalten die IP-Adresse, die aus dem CIDR-Bereich des Clients zugewiesen ist.

So zeigen Sie Client-Verbindungen an (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client VPN-Endpunkt aus, für den Sie die Client-Verbindungen anzeigen möchten.
4. Wählen Sie die Registerkarte Connections (Verbindungen) aus. Die Registerkarte Connections (Verbindungen) listet alle aktiven und beendeten Client-Verbindungen auf.

So zeigen Sie Client-Verbindungen an (AWS CLI)

Verwenden Sie den Befehl describe-client-vpn-connections.

Beenden einer Client-Verbindung

Wenn Sie eine Client-Verbindung beenden, wird die VPN-Sitzung beendet.

Sie können Client-Verbindungen über die Konsole und die AWS CLI beenden.

So beenden Sie eine Client-Verbindung (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client VPN-Endpunkt aus, mit dem der Client verbunden ist, und wählen Sie dann Verbindungen aus.
4. Wählen Sie die Verbindung aus, die Sie beenden möchten. Klicken Sie dann auf Terminate Connection (Verbindung beenden) und erneut auf Terminate Connection (Verbindung beenden).

So beenden Sie eine Client-Verbindung (AWS CLI)

Verwenden Sie den Befehl terminate-client-vpn-connections.

Client-Anmelde-Banner

AWS Client VPN bietet die Möglichkeit, in AWS-bereitgestellten Client-VPN-Desktopanwendungen ein Textbanner anzuzeigen, wenn eine VPN-Sitzung eingerichtet wird. Sie können den Inhalt des Textbanners so definieren, dass er Ihren regulatorischen und Compliance-Anforderungen entspricht. Es können maximal 1 400 UTF-8-kodierte Zeichen verwendet werden.

> **Note**
>
> Wenn ein Client-Anmelde-Banner aktiviert wurde, wird es nur bei neu erstellten VPN-Sitzungen angezeigt. Bestehende VPN-Sitzungen werden nicht unterbrochen, obwohl das Banner angezeigt wird, wenn eine vorhandene Sitzung wiederhergestellt wird.

Siehe Versionshinweise für den von AWS bereitgestellten Client im AWS Client VPN-Benutzerhandbuch, im Einzelheiten zu Client-Desktop-Anwendungen zu erfahren.

Inhalt

Konfigurieren Sie ein Client-Anmelde-Banner während der Erstellung eines Client-VPN-Endpunkts.

Ausführliche Schritte zum Aktivieren eines Client-Anmelde-Banners während der Erstellung eines Client-VPN-Endpunkts finden Sie unter Erstellen eines Client VPN-Endpunkts.

Konfigurieren eines Client-Anmelde-Banners für einen bestehenden Client-VPN-Endpunkt

Führen Sie die folgenden Schritte aus, um ein Client-Anmelde-Banner für einen bestehenden Client-VPN-Endpunkt zu konfigurieren.

Aktivieren eines Client-Anmelde-Banners für einen Client-VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den zu ändernden Client-VPN-Endpunkt aus, wählen Sie Actions (Aktionen) und dann Modify Client VPN Endpoint (Client VPN-Endpunkt ändern).
4. Scrollen Sie auf der Seite nach unten zum Abschnitt Other Parameters (Weitere Parameter).
5. Aktivieren Sie Enable client login banner (Banner für Client-Anmeldung aktivieren).
6. Geben Sie dann bei Client login banner text (Bannertext für die Client-Anmeldung) den Text ein, der in einem Banner auf AWS-bereitgestellten Clients angezeigt wird, wenn eine VPN-Sitzung eingerichtet wird. Verwenden Sie nur UTF-8-kodierte Zeichen, wobei maximal 1 400 Zeichen zulässig sind.
7. Wählen Sie Modify Client VPN Endpoint (Client-VPN-Endpunkt ändern) aus.

Aktivieren eines Client-Anmelde-Banners für einen Client-VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl modify-client-vpn-endpoint.

Deaktivieren eines Client-Anmelde-Banners für einen bestehenden Client-VPN-Endpunkt

Führen Sie die folgenden Schritte aus, um ein Client-Anmelde-Banner für einen bestehenden Client-VPN-Endpunkt zu deaktivieren.

Deaktivieren eines Client-Anmelde-Banners für einen Client-VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den zu ändernden Client-VPN-Endpunkt, Actions (Aktionen) und dann Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.
4. Scrollen Sie auf der Seite nach unten zum Abschnitt Other Parameters (Weitere Parameter).
5. Deaktivieren Sie Enable client login banner? (Banner für Client-Anmeldung aktivieren?).
6. Wählen Sie Modify Client VPN Endpoint (Client-VPN-Endpunkt ändern) aus.

Deaktivieren eines Client-Anmelde-Banners für einen Client-VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl modify-client-vpn-endpoint.

Ändern eines vorhandenen Bannertexts für einen Client-VPN-Endpunkt

Gehen Sie wie folgt vor, um vorhandenen Text auf einem Client-Anmelde-Banner zu ändern.

Ändern eines vorhandenen Bannertexts für einen Client-VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den zu ändernden Client-VPN-Endpunkt, Actions (Aktionen) und dann Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.
4. Vergewissern Sie sich, dass Enable client login banner? (Banner für Client-Anmeldung aktivieren?) aktiviert ist.
5. Ersetzen Sie dann bei Client login banner text (Bannertext für die Client-Anmeldung) den Text durch neuen Text, der in einem Banner auf AWS-bereitgestellten Clients angezeigt werden soll,

wenn eine VPN-Sitzung eingerichtet wird. Verwenden Sie nur UTF-8-kodierte Zeichen, wobei maximal 1 400 Zeichen zulässig sind.

6. Wählen Sie Modify Client VPN Endpoint (Client-VPN-Endpunkt ändern) aus.

Ändern eines Client-Anmelde-Banners für einen Client-VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl modify-client-vpn-endpoint.

Anzeigen des aktuell konfigurierten Anmelde-Banners

Gehen Sie wie folgt vor, um ein aktuell konfiguriertes Anmelde-Banner anzuzeigen.

Anzeigen des aktuellen Anmelde-Banners für einen Client-VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt aus, den Sie anzeigen möchten.
4. Stellen Sie sicher, dass die Registerkarte Details ausgewählt ist.
5. Zeigen Sie den aktuell konfigurierten Anmelde-Banner-Text neben Client login banner text (Text für Client-Anmelde-Banner) an.

Anzeigen des aktuell konfigurierten Anmelde-Banners für einen Client-VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl describe-client-vpn-endpoints.

Client VPN-Endpunkte

Alle Client-VPN-Sitzungen enden am Client-VPN-Endpunkt. Sie konfigurieren den Client-VPN-Endpunkt zur Verwaltung und Kontrolle aller VPN-Sitzungen.

Inhalt

Erstellen eines Client VPN-Endpunkts

Erstellen Sie einen Client-VPN-Endpunkt, damit Ihre Clients eine VPN-Sitzung einrichten können.

Das Client VPN muss im selben AWS-Konto erstellt werden, in dem das beabsichtigte Zielnetzwerk bereitgestellt wird.

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Folgendes erledigt ist:

- Überprüfen Sie die Regeln und Einschränkungen in Regeln und bewährte Verfahren von AWS Client VPN.
- Generieren Sie das Serverzertifikat und, falls erforderlich, das Client-Zertifikat. Weitere Informationen finden Sie unter Client-Authentifizierung.

So erstellen Sie einen Client VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) und dann Create Client VPN Endpoint (Client VPN-Endpunkt erstellen) aus.
3. (Optional) Geben Sie ein Namens-Tag und eine Beschreibung für den Client-VPN-Endpunkt ein.
4. Geben Sie für Client IPv4-CIDR den IP-Adressbereich, in CIDR-Notation, ein, aus dem die Client-IP-Adressen zugewiesen werden. Beispiel: `10.0.0.0/22`.

   > **Note**
   >
   > Der IP-Adressbereich darf sich nicht mit dem Zielnetzwerk-Adressbereich, dem VPC-Adressbereich oder einer der Routen überschneiden, die dem Client-VPN-Endpunkt zugeordnet werden. Der Client-Adressbereich muss eine CIDR-Blockgröße von mindestens /22 und maximal /12 aufweisen. Sie können den Client-Adressbereich nicht mehr ändern, nachdem Sie den Client-VPN-Endpunkt erstellt haben.

5. Geben Sie unter Server certificate ARN (Serverzertifikat-ARN) den ARN für das TLS-Zertifikat an, das vom Server verwendet wird. Clients nutzen zur Authentifizierung des Client VPN-Endpunkts, mit dem sie eine Verbindung herstellen, das Serverzertifikat.

> **Note**
>
> Das Serverzertifikat muss in AWS Certificate Manager (ACM) in der Region vorliegen, in der Sie den Client-VPN-Endpunkt erstellen. Das Zertifikat kann entweder mit ACM bereitgestellt oder in ACM importiert werden.

6. Geben Sie die Authentifizierungsmethode zum Authentifizieren von Clients an, die verwendet werden soll, wenn diese eine VPN-Verbindung herstellen. Sie müssen eine Authentifizierungsmethode auswählen.

   - Um die benutzerbasierte Authentifizierung zu verwenden, wählen Sie Benutzerbasierte Authentifizierung verwenden und dann eine der folgenden Optionen aus:
     - Active Directory-Authentifizierung: Wählen Sie diese Option für die Active Directory-Authentifizierung. Geben Sie bei Verzeichnis-ID die ID des zu verwendenden Active Directory-Verzeichnisses an.
     - Verbundauthentifizierung: Wählen Sie diese Option für die SAML-basierte Verbundauthentifizierung.

       Geben Sie für SAML-Anbieter-ARN den ARN des IAM-SAML-Identitätsanbieters an.

       (Optional) Geben Sie unter Self-service SAML provider ARN (ARN des Self-Service-SAML-Anbieters) ggf. den ARN des IAM SAML-Identitätsanbieters an, den Sie zur Unterstützung des Self-Service-Portals erstellt haben.
   - Wählen Sie für eine gegenseitige Authentifizierung Use mutual authentication (Gegenseitige Authentifizierung verwenden) aus und geben Sie für Client certificate ARN (Clientzertifikat-ARN) den ARN des in AWS Certificate Manager (ACM) bereitgestellten Clientzertifikats an.

   > **Note**
   >
   > Wenn das Server- und das Clientzertifikat von derselben Zertifizierungsstelle (CA) ausgestellt wurden, können Sie den ARN des Serverzertifikats für den Server und den Client verwenden. Wenn das Clientzertifikat von einer anderen Zertifizierungsstelle ausgestellt wurde, sollte der ARN des Clientzertifikats angegeben werden.

7. (Optional) Geben Sie für Verbindungsprotokollierung an, ob Daten über Clientverbindungen mithilfe von Amazon CloudWatch Logs protokolliert werden sollen. Aktivieren Sie Enable log details on client connections (Protokolldetails für Client-Verbindungen aktivieren). Geben Sie

unter CloudWatch Name der Protokollgruppe den Namen der zu verwendenden Protokollgruppe ein. Geben Sie für CloudWatch Name des Protokollstreams den Namen des zu verwendenden Protokollstreams ein oder lassen Sie diese Option leer, damit wir einen Protokollstream für Sie erstellen können.

8. (Optional) Aktivieren Sie unter Client Connect Handler die Option Enable client connect handler (Client-Connect-Handler aktivieren), um benutzerdefinierten Code auszuführen, der eine neue Verbindung mit dem Client-VPN-Endpunkt ermöglicht oder verweigert. Geben Sie unter Client Connect Handler-ARN, den Amazon-Ressourcennamen (ARN) der Lambda-Funktion an, die die Logik enthält, die Verbindungen zulässt oder verweigert.
9. (Optional) Geben Sie an, welche DNS-Server für die DNS-Auflösung verwendet werden sollen. Geben Sie für die Verwendung von benutzerdefinierten DNS-Servern für DNS Server 1 IP address (IP-Adresse von DNS-Server 1) und DNS Server 2 IP address (IP-Adresse von DNS-Server 2) die IP-Adressen der zu verwendenden DNS-Server ein. Zur Verwendung von VPC-DNS-Servern für DNS Server 1 IP address (IP-Adresse für DNS-Server 1) oder DNS Server 2 IP address (IP-Adresse für DNS Server 2) geben Sie die IP-Adressen ein und fügen die IP-Adresse für die VPC DNS-Server hinzu.

   > **Note**
   >
   > Stellen Sie sicher, dass die DNS-Servern von den Clients erreicht werden können.

10. (Optional) Standardmäßig verwendet der Client-VPN-Endpunkt das UDP-Transportprotokoll. Wenn Sie stattdessen das TCP-Transportprotokoll verwenden möchten, wählen Sie als Transport Protocol (Transportprotokoll) TCP aus.

    > **Note**
    >
    > UDP bietet in der Regel eine bessere Leistung als TCP. Sie können das Transportprotokoll nicht mehr ändern, nachdem Sie den Client-VPN-Endpunkt erstellt haben.

11. (Optional) Wenn der Endpunkt ein Client-VPN-Endpunkt mit geteiltem Tunnel sein soll, aktivieren Sie Enable split-tunnel (Split-Tunnel aktivieren). Standardmäßig ist Split Tunneling auf einem Client-VPN-Endpunkt deaktiviert.
12. (Optional) Wählen Sie unter VPC ID die VPC, die dem Client-VPN-Endpunkt zugeordnet werden soll. Wählen Sie unter Security Group IDs (Sicherheitsgruppen-IDs) eine oder mehrere der Sicherheitsgruppen der VPC aus, die für den Client-VPN-Endpunkt gelten sollen.

13. (Optional) Wählen Sie für VPN Port die VPN-Portnummer. Der Standardwert ist 443.
14. (Optional) Um eine Self-Service-Portal-URL für Kunden zu generieren, aktivieren Sie Enable self-service portal (Self-Service-Portal aktivieren).
15. (Optional) Wählen Sie bei Session timeout hours (Sitzungszeitüberschreitungsstunden) die gewünschte maximale VPN-Sitzungsdauer in Stunden aus den verfügbaren Optionen oder lassen Sie sie auf den Standardwert von 24 Stunden eingestellt.
16. (Optional) Geben Sie an, ob der Bannertext für die Client-Anmeldung aktiviert sein soll. Aktivieren Sie Enable client login banner (Banner für Client-Anmeldung aktivieren). Geben Sie bei Client Login Banner Text (Bannertext für die Client-Anmeldung) den Text ein, der in einem Banner auf AWS-bereitgestellten Clients angezeigt wird, wenn eine VPN-Sitzung eingerichtet wird. Nur UTF-8-kodierte Zeichen. Maximal 1 400 Zeichen.
17. Wählen Sie Create Client VPN endpoint (Client-VPN-Endpunkt erstellen) aus.

Führen Sie nach dem Erstellen des Client-VPN-Endpunkts die folgenden Schritte aus, um die Konfiguration abzuschließen und Clients das Herstellen einer Verbindung zu ermöglichen:

- Der anfängliche Status des Client VPN-Endpunkts ist `pending-associate`. Clients können erst dann eine Verbindung mit dem Client-VPN-Endpunkt herstellen, nachdem Sie das erste Zielnetzwerk zugeordnet haben.
- Erstellen Sie eine Autorisierungsregel, um anzugeben, welche Clients Zugriff auf das Netzwerk haben.
- Laden Sie die Konfigurationsdatei für den Client-VPN-Endpunkt herunter und bereiten Sie sie vor, um sie an Ihre Clients zu verteilen.
- Weisen Sie Ihre Kunden an, den von AWS bereitgestellten Client oder eine andere OpenVPN-basierte Clientanwendung zu verwenden, um eine Verbindung zum Client-VPN-Endpunkt herzustellen. Weitere Informationen finden Sie im AWS Client VPN-Benutzerhandbuch.

So erstellen Sie einen Client VPN-Endpunkt (AWS CLI)

Verwenden Sie den create-client-vpn-endpoint-Befehl.

Ändern eines Client-VPN-Endpunkts

Nachdem ein Client-VPN erstellt wurde, können Sie jede der folgenden Einstellungen ändern:

- Die Beschreibung.

- Das Serverzertifikat
- Die Client-Verbindungsprotokollierungsoptionen
- Die Client-Connect-Handler-Option
- Die DNS-Server
- Die Split-Tunnel-Option
- Routen (bei Verwendung der Split-Tunnel-Option)
- Zertifikatsperrliste (CRL)
- Autorisierungsregeln
- Die VPC- und Sicherheitsgruppenzuordnungen
- Die VPN-Portnummer
- Die Self-Service-Portal-Option
- Die maximale VPN-Sitzungsdauer
- Bannertext für Client-Anmeldung aktivieren oder deaktivieren
- Bannertext für Client-Anmeldung

> **Note**
>
> Nach der Annahme einer Anfrage vom Client-VPN-Service kann es bis zu 4 Stunden dauern, bis Änderungen an Client-VPN-Endpunkten wirksam werden, einschließlich Änderungen an der Client-Zertifikatsperrliste (Certificate Revocation List, CRL).
> Es ist nicht möglich, den Client-IPv4-CIDR-Bereich, die Authentifizierungsoptionen, das Client-Zertifikat und das Transportprotokoll zu ändern, nachdem der Client-VPN-Endpunkt erstellt wurde.

Wenn Sie einen der folgenden Parameter auf einem Client-VPN-Endpunkt ändern, wird die Verbindung zurückgesetzt:

- Das Serverzertifikat
- Die DNS-Server
- Die Split-Tunnel-Option (Unterstützung ein- oder ausschalten)
- Routen (wenn Sie die Split-Tunnel-Option verwenden)
- Zertifikatsperrliste (CRL)

- Autorisierungsregeln
- Die VPN-Portnummer

Sie können einen Client-VPN-Endpunkt mithilfe der Konsole oder der AWS CLI ändern.

So ändern Sie einen Client VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den zu ändernden Client-VPN-Endpunkt, Actions (Aktionen) und dann Modify Client VPN Endpoint (Client-VPN-Endpunkt ändern) aus.
4. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung für den Client-VPN-Endpunkt ein.
5. Geben Sie unter Server certificate ARN (Serverzertifikat-ARN) den ARN für das TLS-Zertifikat an, das vom Server verwendet wird. Clients nutzen zur Authentifizierung des Client VPN-Endpunkts, mit dem sie eine Verbindung herstellen, das Serverzertifikat.

   > **Note**
   >
   > Das Serverzertifikat muss in AWS Certificate Manager (ACM) in der Region vorliegen, in der Sie den Client-VPN-Endpunkt erstellen. Das Zertifikat kann entweder mit ACM bereitgestellt oder in ACM importiert werden.

6. Geben Sie an, ob Daten über Client-Verbindungen mit Amazon CloudWatch Logs protokolliert werden sollen. Führen Sie für Do you want to log details on client connections? (Möchten Sie Details zu Client-Verbindungen protokollieren) einen der folgenden Schritte aus:

   - Wenn Sie die Client-Verbindungsprotokollierung aktivieren möchten, aktivieren Sie die Option Enable log details on client connections (Protokolldetails für Client-Verbindungen aktivieren). Wählen Sie für CloudWatch Name der Protokollgruppe den Namen der zu verwendenden Protokollgruppe aus. Wählen Sie für CloudWatch Name des Protokollstreams den Namen des zu verwendenden Protokollstreams aus oder lassen Sie diese Option leer, damit wir einen Protokollstream für Sie erstellen können.
   - Wenn Sie die Client-Verbindungsprotokollierung deaktivieren möchten, deaktivieren Sie die Option Enable log details on client connections (Protokolldetails für Client-Verbindungen aktivieren).

7. Für Client Connect Handler gilt Folgendes: Wenn Sie den Client-Connect-Handler aktivieren möchten, aktivieren Sie die Option Enable client connect handler (Client-Connect-Handler aktivieren). Geben Sie unter Client Connect Handler-ARN, den Amazon-Ressourcennamen (ARN) der Lambda-Funktion an, die die Logik enthält, die Verbindungen zulässt oder verweigert.
8. Aktivieren oder deaktivieren Sie die Option Enable DNS servers (DNS-Server aktivieren). Geben Sie für die Verwendung von benutzerdefinierten DNS-Servern für DNS Server 1 IP address (IP-Adresse von DNS-Server 1) und DNS Server 2 IP address (IP-Adresse von DNS-Server 2) die IP-Adressen der zu verwendenden DNS-Server ein. Zur Verwendung von VPC-DNS-Servern für DNS Server 1 IP address (IP-Adresse für DNS-Server 1) oder DNS Server 2 IP address (IP-Adresse für DNS Server 2) geben Sie die IP-Adressen ein und fügen die IP-Adresse für die VPC DNS-Server hinzu.

   > **Note**
   >
   > Stellen Sie sicher, dass die DNS-Servern von den Clients erreicht werden können.

9. Aktivieren oder deaktivieren Sie die Option Enable split-tunnel (Split-Tunnel aktivieren). Standardmäßig ist Split Tunneling auf einem VPN-Endpunkt deaktiviert.
10. Wählen Sie unter VPC ID die VPC aus, die dem Client-VPN-Endpunkt zugeordnet werden soll. Wählen Sie unter Security Group IDs (Sicherheitsgruppen-IDs) eine oder mehrere der Sicherheitsgruppen der VPC aus, die für den Client-VPN-Endpunkt gelten sollen.
11. Wählen Sie für VPN Port die VPN-Portnummer. Der Standardwert ist 443.
12. Um eine Self-Service-Portal-URL für Kunden zu generieren, aktivieren Sie Enable self-service portal (Self-Service-Portal aktivieren).
13. Wählen Sie bei Session timeout hours (Sitzungszeitüberschreitungsstunden) die gewünschte maximale VPN-Sitzungsdauer in Stunden aus den verfügbaren Optionen aus oder lassen Sie sie auf den Standardwert von 24 Stunden eingestellt.
14. Aktivieren oder deaktivieren Sie Enable client login banner (Banner für Client-Anmeldung aktivieren). Wenn Sie das Banner für die Client-Anmeldung verwenden möchten, geben Sie den Text ein, der in einem Banner auf AWS-bereitgestellten Clients angezeigt wird, wenn eine VPN-Sitzung eingerichtet wird. Nur UTF-8-kodierte Zeichen. Maximal 1 400 Zeichen.
15. Wählen Sie Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.

Ändern eines Client-VPN-Endpunkts (AWS CLI)

Verwenden Sie den modify-client-vpn-endpoint-Befehl.

Anzeigen von Client VPN-Endpunkten

Sie können Informationen über Client VPN-Endpunkte mithilfe der Konsole oder der AWS CLI anzeigen.

So zeigen Sie Client-VPN-Endpunkte an (Konsole):

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client VPN-Endpunkt aus, den Sie anzeigen möchten.
4. Verwenden Sie die Registerkarten Details, Target network associations (Zielnetzwerkzuordnungen), Security groups (Sicherheitsgruppen), Authorization rules (Autorisierungsregeln), Route table (Routing-Tabelle), Connections (Verbindungen) und Tags, um Informationen über vorhandene Client-VPN-Endpunkte anzuzeigen.

   Sie können auch Filter verwenden, um Ihre Suche zu verfeinern.

So zeigen Sie Client-VPN-Endpunkte an (AWS CLI):

Verwenden Sie den describe-client-vpn-endpoints-Befehl.

Löschen eines Client-VPN-Endpunkts

Sie müssen die Zuordnung aller Zielnetzwerke trennen, bevor Sie einen Client-VPN-Endpunkt löschen können. Wenn Sie einen Client-VPN-Endpunkt löschen, ändert sich dessen Status zu `deleting` und Clients können sich nicht mehr mit diesem verbinden.

Sie können einen Client-VPN-Endpunkt löschen, indem Sie die Konsole oder die AWS CLI verwenden.

So löschen Sie einen Client VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt aus, den Sie löschen möchten. Wählen Sie Actions (Aktionen),Delete Client VPN endpoint (Client–VPN-Endpunkt löschen) aus.
4. Geben Sie Delete (Löschen) im Bestätigungsfenster an und wählen Sie Delete (Löschen) aus.

Löschen eines Client-VPN-Endpunkts (AWS CLI)

Verwenden Sie den delete-client-vpn-endpoint-Befehl.

Arbeiten mit Verbindungsprotokollen

Sie können die Verbindungsprotokollierung für einen neuen oder einen vorhandenen Client-VPN-Endpunkt aktivieren und mit der Erfassung von Verbindungsprotokollen beginnen.

Bevor Sie beginnen, müssen Sie eine CloudWatch Logs-Protokollgruppe in Ihrem Konto haben. Weitere Informationen finden Sie unter Arbeiten mit Protokollgruppen und Protokoll-Streams im Amazon CloudWatch Logs-Benutzerhandbuch. Für die Verwendung von CloudWatch Logs fallen Gebühren an. Weitere Informationen hierzu finden Sie unter Amazon CloudWatch – Preise.

Wenn Sie die Verbindungsprotokollierung aktivieren, können Sie den Namen eines Protokolldatenstroms in der Protokollgruppe angeben. Wenn Sie keinen Protokolldatenstrom angeben, erstellt der Client-VPN-Service einen für Sie.

Aktivieren der Verbindungsprotokollierung für einen neuen Client-VPN-Endpunkt

Sie können die Verbindungsprotokollierung aktivieren, wenn Sie einen neuen Client-VPN-Endpunkt mithilfe der Konsole oder der Befehlszeile erstellen.

So aktivieren Sie die Verbindungsprotokollierung für einen neuen Client-VPN-Endpunkt mit der Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client-VPN-Endpunkte) und dann Create Client VPN endpoint (Client-VPN-Endpunkt erstellen) aus.
3. Füllen Sie die Optionen aus, bis Sie den Abschnitt Connection Logging (Verbindungsprotokollierung) erreichen. Weitere Informationen zu diesen Optionen finden Sie unter Erstellen eines Client VPN-Endpunkts.
4. Aktivieren Sie unter Connection logging (Verbindungsprotokollierung) die Option Enable log details on client connections (Protokolldetails für Client-Verbindungen aktivieren.
5. Wählen Sie unter CloudWatch Logs log group name (CloudWatch Logs-Protokollgruppenname) den Namen der CloudWatch Logs-Protokollgruppe aus.

6. (Optional) Wählen Sie unter CloudWatch Logs log stream name (Cloud Watch Logs-Protokollstromname) den Namen des CloudWatch Logs-Protokolldatenstroms aus.
7. Wählen Sie Create Client VPN endpoint (Client-VPN-Endpunkt erstellen) aus.

So aktivieren Sie die Verbindungsprotokollierung für einen neuen Client-VPN-Endpunkt mit der AWS CLI

Verwenden Sie den Befehl create-client-vpn-endpoint und geben Sie den `--connection-log-options`-Parameter an. Sie können die Verbindungsprotokolle wie im folgenden Beispiel gezeigt im JSON-Format angeben.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Aktivieren der Verbindungsprotokollierung für einen vorhandenen Client-VPN-Endpunkt

Sie können die Verbindungsprotokollierung für einen vorhandenen Client-VPN-Endpunkt über die Konsole oder die Befehlszeile aktivieren.

So aktivieren Sie die Verbindungsprotokollierung für einen vorhandenen Client-VPN-Endpunkt mit der Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, wählen Sie Actions (Aktionen) und dann Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.
4. Aktivieren Sie unter Connection logging (Verbindungsprotokollierung) die Option Enable log details on client connections (Protokolldetails für Client-Verbindungen aktivieren.
5. Wählen Sie unter CloudWatch Logs log group name (CloudWatch Logs-Protokollgruppenname) den Namen der CloudWatch Logs-Protokollgruppe aus.
6. (Optional) Wählen Sie unter CloudWatch Logs log stream name (Cloud Watch Logs-Protokollstromname) den Namen des CloudWatch Logs-Protokolldatenstroms aus.
7. Wählen Sie Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.

So aktivieren Sie die Verbindungsprotokollierung für einen vorhandenen Client-VPN-Endpunkt mit der AWS CLI

Verwenden Sie den Befehl modify-client-vpn-endpoint und geben Sie den `--connection-log-options`-Parameter an. Sie können die Verbindungsprotokolle wie im folgenden Beispiel gezeigt im JSON-Format angeben.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Verbindungsprotokolle anzeigen

Sie können Ihre Verbindungsprotokolle mit der CloudWatch Logs-Konsole anzeigen.

So zeigen Sie die Verbindungsprotokolle über die Konsole an

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Log groups (Protokollgruppen) und danach die Protokollgruppe mit Ihrem Verbindungsprotokoll.
3. Wählen Sie den Protokolldatenstrom für Ihren Client-VPN-Endpunkt aus.

> **Note**
>
> In der Spalte Timestamp (Zeitstempel) wird die Uhrzeit angezeigt, zu der das Verbindungsprotokoll in CloudWatch Logs veröffentlicht wurde, nicht der Zeitpunkt der Verbindung.

Weitere Informationen zum Durchsuchen von Protokolldaten finden Sie unter Durchsuchen von Protokolldaten mit Filtermustern im Amazon CloudWatch Logs-Benutzerhandbuch.

Deaktivieren der Verbindungsprotokollierung

Sie können die Verbindungsprotokollierung für einen Client-VPN-Endpunkt über die Konsole oder die Befehlszeile deaktivieren. Wenn Sie die Verbindungsprotokollierung deaktivieren, werden vorhandene Verbindungsprotokolle in CloudWatch Logs nicht gelöscht.

So deaktivieren Sie Verbindungsprotokollierung mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, wählen Sie Actions (Aktionen) und dann Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.
4. Deaktivieren Sie unter Connection logging (Verbindungsprotokollierung) die Option Enable log details on client connections (Protokolldetails für Client-Verbindungen aktivieren.
5. Wählen Sie Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.

So deaktivieren Sie die Verbindungsprotokollierung mithilfe der AWS CLI

Verwenden Sie den Befehl modify-client-vpn-endpoint und geben Sie den `--connection-log-options`-Parameter an. Stellen Sie sicher, dass `Enabled` auf „`false`“ festgelegt ist.

Exportieren und Konfigurieren der Client-Konfigurationsdatei

Die Client VPN-Konfigurationsdatei ist die Datei, die von Clients (Benutzern) verwendet wird, um eine VPN-Verbindung mit dem Client VPN-Endpunkt herzustellen. Sie müssen diese Datei herunterladen (exportieren) und alle Clients verteilen, die auf das VPN zugreifen müssen. Wenn Sie das Self-Service-Portal für Ihren Client-VPN-Endpunkt aktiviert haben, können sich Clients alternativ beim Portal anmelden und die Konfigurationsdatei selbst herunterladen. Weitere Informationen finden Sie unter Zugriff auf das Self-Service-Portal.

Wenn Ihr Client-VPN-Endpunkt die gegenseitige Authentifizierung verwendet, müssen Sie das Client-Zertifikat und den privaten Schlüssel des Clients zu der OVPN-Konfigurationsdatei hinzufügen, die Sie herunterladen. Nach dem Hinzufügen der Informationen können Sie die OVPN-Datei in die OpenVPN-Client-Software importieren.

> **Important**
>
> Wenn Sie der Datei das Client-Zertifikat und die privaten Schlüsselinformationen des Clients nicht hinzufügen, können Clients, die die gegenseitige Authentifizierung verwenden, keine Verbindung zum Client-VPN-Endpunkt herstellen.

Standardmäßig aktiviert die Option „remote-random-hostname“ in der OpenVPN-Clientkonfiguration Platzhalter-DNS. Da DNS-Platzhalter aktiviert sind, speichert der Client die IP-Adresse des Endpunkts nicht zwischen und Sie können keinen Ping an den DNS-Namen des Endpunkts ausführen.

Wenn Ihr Client-VPN-Endpunkt die Active Directory-Authentifizierung verwendet und Sie nach der Verteilung der Client-Konfigurationsdatei Multi-Factor Authentication (MFA) in Ihrem Verzeichnis aktivieren, müssen Sie eine neue Datei herunterladen und an Ihre Clients weitergeben. Clients können nicht die vorherige Konfigurationsdatei verwenden, um eine Verbindung mit dem Client-VPN-Endpunkt herzustellen.

Exportieren der Client-Konfigurationsdatei

Sie können die Client-Konfiguration mithilfe der Konsole oder der AWS CLI exportieren.

So exportieren Sie die Client-Konfiguration (Konsole)

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, für den die Client-Konfiguration heruntergeladen werden soll, und dann die Option Download Client Configuration (Client-Konfiguration herunterladen) aus.

So exportieren Sie die Client-Konfiguration (AWS CLI)

Verwenden Sie den Befehl export-client-vpn-client-configuration und geben Sie den Namen der Ausgabedatei an.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id
 --output text>config_filename.ovpn
```

Fügen Sie das Client-Zertifikat und die Schlüsselinformationen (gegenseitige Authentifizierung) hinzu.

Wenn Ihr Client-VPN-Endpunkt die gegenseitige Authentifizierung verwendet, müssen Sie das Client-Zertifikat und den privaten Schlüssel des Clients zu der OVPN-Konfigurationsdatei hinzufügen, die Sie herunterladen.

Sie können das Clientzertifikat nicht ändern, wenn Sie die gegenseitige Authentifizierung verwenden.

Hinzufügen des Client-Zertifikats und der Schlüsselinformationen (gegenseitige Authentifizierung)

Verwenden Sie eine der folgenden Optionen.

(Option 1) Verteilen Sie das Client-Zertifikat und den Schlüssel zusammen mit der Client-VPN-Endpunktkonfigurationsdatei an Clients. Geben Sie in diesem Fall den Pfad zum Zertifikat und Schlüssel in der Konfigurationsdatei an. Öffnen Sie die Konfigurationsdatei mit Ihrem bevorzugten Texteditor und fügen Sie Folgendes an das Ende der Datei an. Ersetzen Sie */path/* durch den Speicherort des Client-Zertifikats und -Schlüssels (der Speicherort bezieht sich auf den Client, der eine Verbindung zum Endpunkt herstellt).

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(Option 2) Fügen Sie der Konfigurationsdatei den Inhalt des Client-Zertifikats in `<cert></cert>`-Tags und den Inhalt des privaten Schlüssels in `<key></key>`-Tags hinzu. Wenn Sie diese Option wählen, verteilen Sie nur die Konfigurationsdatei an Ihre Clients.

Wenn Sie separate Client-Zertifikate und Schlüssel für jeden Benutzer erstellt haben, der eine Verbindung zum Client-VPN-Endpunkt herstellt, wiederholen Sie diesen Schritt für jeden Benutzer.

Nachfolgend finden Sie ein Beispiel für das Format einer Client-VPN-Konfigurationsdatei, die das Client-Zertifikat und den Schlüssel enthält.

```
client
dev tun
proto udp
remote cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>
```

```
<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>

reneg-sec 0
```

Routen

Jeder Client VPN-Endpunkt verfügt über eine Routing-Tabelle, die die verfügbaren Zielnetzwerkrouten beschreibt. Jede Route in der Routing-Tabelle bestimmt, wohin der Netzwerkverkehr geleitet wird. Sie müssen für jede Client-VPN-Endpunkt-Route Autorisierungsregeln konfigurieren, um festzulegen, welche Clients Zugriff auf das Zielnetzwerk haben.

Wenn Sie ein Subnetz aus einer VPC mit einem Client-VPC-Endpunkt verknüpfen, wird eine Route für die VPC automatisch zur Routing-Tabelle des Client-VPN-Endpunkts hinzugefügt. Um den Zugriff für zusätzliche Netzwerke wie Peered VPCs, On-Premises-Netzwerke, das lokale Netzwerk (damit Clients miteinander kommunizieren können) oder das Internet zu ermöglichen, müssen Sie der Routing-Tabelle des Client-VPN-Endpunkts manuell eine Route hinzufügen.

> **Note**
>
> Wenn Sie dem Client-VPN-Endpunkt mehrere Subnetze zuordnen, sollten Sie sicherstellen, dass Sie für jedes Subnetz eine Route erstellen, wie hier Der Zugriff auf eine Peer-VPC, Amazon S3 oder das Internet erfolgt nur mit Unterbrechungen. beschrieben. Jedes zugeordnete Subnetz sollte einen identischen Satz von Routen aufweisen.

Inhalt

Überlegungen zum Split-Tunnel auf Client VPN-Endpunkten

Wenn Sie Split-Tunnel auf einem Client-VPN-Endpunkt verwenden, werden alle Routen, die in den Client-VPN-Routing-Tabellen enthalten sind, der Client-Routing-Tabelle hinzugefügt, wenn das VPN eingerichtet wird. Wenn Sie eine Route hinzufügen, nachdem das VPN eingerichtet ist, müssen Sie die Verbindung zurücksetzen, damit die neue Route an den Client gesendet wird.

Wir empfehlen, dass Sie die Anzahl der Routen, die das Client-Gerät verarbeiten kann, berücksichtigen, bevor Sie die Client-VPN-Endpunkt-Routing-Tabelle ändern.

Endpunkt-Route erstellen

Beim Erstellen einer Route geben Sie an, wie der Datenverkehr für das Zielnetzwerk geleitet werden soll.

Fügen Sie die Zielroute `0.0.0.0/0` hinzu, damit Clients Zugriff auf das Internet haben.

Sie können Routen zu einem Client-VPN-Endpunkt hinzufügen, indem Sie die Konsole und die AWS CLI verwenden.

So erstellen Sie eine Client VPN-Endpunkt-Route (Konsole):

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, dem die Route hinzugefügt werden soll, sowie die Optionen Route Table (Routing-Tabelle) und Create Route (Route erstellen) aus.
4. Geben Sie für Route destination (Routenziel) den IPv4-CIDR-Bereich für das Zielnetzwerk an. Beispiele:

   - Wenn Sie eine Route für die VPC des Client-VPN-Endpunkts hinzufügen möchten, geben Sie den IPv4-CIDR-Bereich der VPC ein.
   - Um eine Route für den Internetzugang hinzuzufügen, geben Sie `0.0.0.0/0` ein.
   - Wenn Sie eine Route für eine durch Peering verbundene VPC hinzufügen möchten, geben Sie den IPv4-CIDR-Bereich der durch Peering verbundenen VPCs ein.
   - Um eine Route für ein lokales Netzwerk hinzuzufügen, geben Sie den IPv4-CIDR-Bereich der AWS-Site-to-Site-VPN-Verbindung ein.
5. Wählen Sie für Subnet ID for target network association (Subnetz-ID für Zielnetzwerkzuordnung) das Subnetz aus, das dem Client-VPN-Endpunkt zugeordnet ist.

Wenn Sie eine Route für das lokale Client-VPN-Endpunktnetzwerk hinzufügen, wählen Sie `local` aus.

6. (Optional) Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Route ein.
7. Wählen Sie Create route (Route erstellen) aus.

So erstellen Sie einen Client VPN-Endpunkt-Route (AWS CLI)

Verwenden Sie den Befehl create-client-vpn-route.

Anzeigen von Endpunktrouten

Sie können die Routen für einen bestimmten Client-VPN-Endpunkt mithilfe der Konsole oder der AWS CLI anzeigen.

So zeigen Sie Client-VPN-Endpunkt-Routen an (Konsole):

1. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
2. Wählen Sie den Client-VPN-Endpunkt, für den Routen angezeigt werden sollen, und dann Route table (Routing-Tabelle) aus.

Anzeigen von Client-VPN-Endpunkt-Routen (AWS CLI)

Verwenden Sie den Befehl describe-client-vpn-routes.

Löschen einer Endpunktroute

Sie können nur Routen löschen, die Sie manuell hinzugefügt haben. Sie können keine Routen löschen, die automatisch hinzugefügt wurden, wenn Sie ein Subnetz mit dem Client-VPN-Endpunkt verknüpft haben. Zum Löschen von automatisch hinzugefügten Routen müssen Sie das Subnetz, das das Erstellen initiiert hat, vom Client-VPN-Endpunkt trennen.

Sie können eine Route von einem Client-VPN-Endpunkt löschen, indem Sie die Konsole oder die AWS CLI verwenden.

So löschen Sie eine Client VPN-Endpunktroute (Konsole):

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.

3. Wählen Sie den Client-VPN-Endpunkt, von dem Sie die Route löschen möchten, sowie die Option Route table (Routing-Tabelle) aus.
4. Wählen Sie die zu löschende Route und die Optionen Delete route (Route löschen) und Delete route (Route löschen) aus.

Löschen einer Client-VPN-Endpunktroute (AWS CLI)

Verwenden Sie den Befehl delete-client-vpn-route.

Zielnetzwerke

Ein Zielnetzwerk ist ein Subnetz in einer VPC. Ein Client VPN-Endpunkt benötigt mindestens ein Zielnetzwerk, damit sich Clients damit verbinden und eine VPN-Verbindung herstellen können.

Weitere Informationen zu den Zugriffsarten, die Sie konfigurieren können (z. B. Clients den Zugriff auf das Internet ermöglichen), finden Sie unter Szenarien und Beispiele für AWS Client-VPN.

Inhalt

Zuordnen eines Zielnetzwerk zu einem Client VPN-Endpunkt

Sie können einem Client VPN-Endpunkt ein oder mehrere Zielnetzwerke (Subnetze) zuweisen.

Die folgenden Regeln gelten:

- Das Subnetz muss einen CIDR-Block mit mindestens einer /27-Bitmaske haben, z. B. 10.0.0.0/27. Das Subnetz muss außerdem über mindestens 20 verfügbare IP-Adressen verfügen.
- Der CIDR-Block des Subnetzes darf sich nicht mit dem Client-CIDR-Bereich des Client VPN-Endpunkts überschneiden.
- Wenn Sie mehr als ein Subnetz mit einem Client VPN-Endpunkt verknüpfen, muss sich jedes Subnetz in einer anderen Availability Zone befinden. Wir empfehlen, dass Sie mindestens zwei Subnetze zuordnen, um für Availability Zone-Redundanz zu sorgen.

- Wenn Sie beim Erstellen des Client VPN-Endpunkts eine VPC angegeben haben, muss sich das Subnetz in eben dieser VPC befinden. Wenn Sie noch keine VPC mit dem Client VPN-Endpunkt verknüpft haben, können Sie ein beliebiges Subnetz aus irgendeiner VPC auswählen.

  Alle weiteren Subnetz-Zuordnungen müssen von derselben VPC stammen. Um ein Subnetz aus einer anderen VPC zuzuordnen, müssen Sie zunächst den Client VPC-Endpunkt modifizieren, indem Sie die ihm zugeordnete VPC ändern. Weitere Informationen finden Sie unter Ändern eines Client-VPN-Endpunkts.

Wenn Sie ein Subnetz mit einem Client VPN-Endpunkt verknüpfen, fügen wir automatisch die lokale Route der VPC hinzu, in der das verknüpfte Subnetz in der Routing-Tabelle des Client VPN-Endpunkts bereitgestellt wird.

> **Note**
>
> Nachdem Ihre Zielnetzwerke verknüpft sind und Sie Ihrer angehängten VPC zusätzliche CIDRs hinzufügen oder entfernen, müssen Sie einen der folgenden Vorgänge ausführen, um die lokale Route für Ihre Client-VPN-Endpunkt-Routing-Tabelle zu aktualisieren:
>
> - Trennen Sie Ihren Client-VPN-Endpunkt vom Zielnetzwerk und verknüpfen Sie dann den Client-VPN-Endpunkt mit dem Zielnetzwerk.
> - Fügen Sie die Route manuell hinzu oder entfernen Sie die Route aus der Routing-Tabelle des Client-VPN-Endpunkts.

Nachdem Sie das erste Subnetz mit dem Client VPN-Endpunkt verknüpft haben, ändert sich der Status des Client VPN-Endpunkts von `pending-associate` in `available`, und Clients können eine VPN-Verbindung herstellen.

So verknüpfen Sie ein Zielnetzwerk mit einem Client VPN-Endpunkt über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt aus, mit dem das Zielnetzwerk verknüpft werden soll. Wählen Sie dann Target network associations (Zielnetzwerkzuordnungen) und Associate target network (Zielnetzwerk zuordnen) aus.

4. Wählen Sie für VPC die VPC aus, in der sich das Subnetz befindet. Wenn Sie bei der Erstellung des Client VPN-Endpunkts eine VPC angegeben haben oder wenn Sie vorherige Subnetz-Zuordnungen haben, muss es sich um diese VPC handeln.
5. Wählen Sie für Choose a subnet to associate (Zuzuordnendes Subnetz auswählen) das Subnetz aus, das dem Client-VPN-Endpunkt zugeordnet werden soll.
6. Wählen Sie Associate target network (Zielnetzwerk zuordnen) aus.

Zuordnen eines Zielnetzwerk zu einem Client VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl associate-client-vpn-target-network.

Anwenden einer Sicherheitsgruppe auf ein Zielnetzwerk

Wenn Sie einen Client VPN-Endpunkt erstellen, können Sie die Sicherheitsgruppen angeben, die für das Zielnetzwerk gelten sollen. Wenn Sie das erste Zielnetzwerk mit einem Client VPN-Endpunkt verknüpfen, wenden wir automatisch die Standardsicherheitsgruppe der VPC an, in der sich das zugeordnete Subnetz befindet. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Sie können die Sicherheitsgruppen für den Client VPN-Endpunkt ändern. Welche Regeln der Sicherheitsgruppe Sie benötigen, hängt von der Art des VPN-Zugriffs ab, den Sie konfigurieren möchten. Weitere Informationen finden Sie unter Szenarien und Beispiele für AWS Client-VPN.

So wenden Sie eine Sicherheitsgruppe auf ein Zielnetzwerk an (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client VPN-Endpunkt aus, auf den die Sicherheitsgruppen angewendet werden sollen.
4. Wählen Sie Security Groups (Sicherheitsgruppen) und dann Apply Security Groups (Sicherheitsgruppen anwenden) aus.
5. Wählen Sie die entsprechende(n) Sicherheitsgruppe(n) unter Security group IDs (Sicherheitsgruppen-IDs) aus.
6. Wählen Sie Apply Security Groups (Sicherheitsgruppen anwenden) aus.

So wenden Sie eine Sicherheitsgruppe auf ein Zielnetzwerk an (AWS CLI)

Verwenden Sie den Befehl apply-security-groups-to-client-vpn-target-network.

Trennen eines Zielnetzwerks von einem Client VPN-Endpunkt

Wenn Sie die Zuordnung zu einem Zielnetzwerk aufheben, werden alle Routen gelöscht, die manuell zur Routing-Tabelle der Client-VPN-Endpunkte hinzugefügt wurden, sowie die Route, die beim Herstellen der Zielnetzwerkzuordnung automatisch erstellt wurde (die lokale Route der VPC). Wenn Sie die Zuordnung aller Zielnetzwerke zu einem Client VPN-Endpunkt aufheben, können Clients keine VPN-Verbindung mehr herstellen.

So heben Sie die Zuordnung eines Zielnetzwerks zu einem Client VPN-Endpunkt auf (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt, dem das Zielnetzwerk zugeordnet ist, und dann Target network associations (Zielnetzwerkzuordnungen) aus.
4. Wählen Sie das zu trennende Zielnetzwerk, die Option Disassociate (Zuordnung aufheben) und dann Disassociate target network (Zuordnung von Zielnetzwerk aufheben) aus.

Trennen eines Zielnetzwerks von einem Client VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl disassociate-client-vpn-target-network.

Anzeigen von Zielnetzwerken

Sie können die Zielnetzwerke, die mit einem Client VPN-Endpunkt verknüpft sind, mit der Konsole oder der AWS CLI anzeigen.

So zeigen Sie Zielnetzwerke an (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den entsprechenden Client-VPN-Endpunkt und anschließend Target network associations (Zielnetzwerkzuordnungen) aus.

So zeigen Sie Zielnetzwerke mit der AWS CLI an

Verwenden Sie den Befehl describe-client-vpn-target-networks.

Maximale VPN-Sitzungsdauer

AWS Client VPN bietet mehrere Optionen für die maximale VPN-Sitzungsdauer. Sie können eine kürzere maximale VPN-Sitzungsdauer konfigurieren, um Sicherheits- und Compliance-Anforderungen zu erfüllen. Die Sitzungsdauer beträgt standardmäßig 24 Stunden.

> **Note**
>
> Wenn der maximale Wert für die Dauer der VPN-Sitzung verringert wird, werden aktive VPN-Sitzungen, die älter als der neue Timeout-Wert sind, getrennt.

Siehe Versionshinweise für den von AWS bereitgestellten Client im AWS Client VPN-Benutzerhandbuch, im Einzelheiten zu Client-Desktop-Anwendungen zu erfahren.

Inhalt

Konfigurieren der maximalen VPN-Sitzung während der Erstellung eines Client-VPN-Endpunkts

Ausführliche Schritte zum Konfigurieren der maximalen VPN-Sitzung während der Erstellung eines Client-VPN-Endpunkts finden Sie unter Erstellen eines Client VPN-Endpunkts.

Anzeigen der maximalen VPN-Sitzungsdauer

Gehen Sie wie folgt vor, um die aktuelle maximale VPN-Sitzungsdauer anzuzeigen.

Anzeigen der aktuellen maximalen VPN-Sitzungsdauer für einen Client-VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client VPN-Endpunkte) aus.
3. Wählen Sie den Client-VPN-Endpunkt aus, den Sie anzeigen möchten.
4. Stellen Sie sicher, dass die Registerkarte Details ausgewählt ist.

5. Zeigen Sie die aktuelle maximale VPN-Sitzungsdauer neben Session timeout hours (Sitzungszeitüberschreitungsstunden) an.

Anzeigen der aktuellen maximalen VPN-Sitzungsdauer für einen Client-VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl describe-client-vpn-endpoints.

Ändern der maximalen VPN-Sitzungsdauer

Gehen Sie wie folgt vor, um die aktuelle maximale VPN-Sitzungsdauer zu ändern.

Ändern einer vorhandenen maximalen VPN-Sitzungsdauer für einen Client-VPN-Endpunkt (Konsole)

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints (Client-VPN-Endpunkte) aus.
3. Wählen Sie den zu ändernden Client-VPN-Endpunkt aus, wählen Sie Actions (Aktionen) und dann Modify Client VPN Endpoint (Client VPN-Endpunkt ändern).
4. Wählen Sie bei Session timeout hours (Sitzungszeitüberschreitungsstunden) die gewünschte maximale Dauer der VPN-Sitzung in Stunden aus.
5. Wählen Sie Modify Client VPN Endpoint (Client-VPN-Endpunkt ändern) aus.

Ändern einer vorhandenen maximalen VPN-Sitzungsdauer für einen Client-VPN-Endpunkt (AWS CLI)

Verwenden Sie den Befehl modify-client-vpn-endpoint.

Sicherheit in AWS Client VPN

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

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

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für AWS Client VPN gelten, finden Sie unter Im Rahmen des Compliance-Programms zugelassene AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

AWS Client VPN ist Teil des Service Amazon VPC. Weitere Informationen zur Sicherheit in Amazon VPC finden Sie unter Sicherheit im Amazon VPC-Benutzerhandbuch.

In dieser Dokumentation wird erläutert, wie das Modell der übergreifenden Verantwortlichkeit bei der Verwendung von Client-VPN zum Tragen kommt. Die folgenden Themen zeigen Ihnen, wie Sie Client-VPN zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren auch, wie Sie andere AWS-Services nutzen können, die Ihnen helfen, Ihre Client-VPN-Ressourcen zu überwachen und zu sichern.

Inhalt

Datenschutz in AWS Client VPN

Das AWS-Modell der geteilten Verantwortung gilt für den Datenschutz in AWS Client VPN. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfigurations- und Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

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

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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

Verschlüsselung während der Übertragung

AWS Client VPN bietet mit Transport Layer Security (TLS) 1.2 oder höher sichere Verbindungen von jedem Standort aus.

Richtlinie für den Datenverkehr zwischen Netzwerken

Einrichten eines netzwerkübergreifenden Zugriffs

Sie können es Clients ermöglichen, sich über einen Client VPN-Endpunkt mit Ihrer VPC und anderen Netzwerken zu verbinden. Weitere Informationen und Beispiele finden Sie unter Szenarien und Beispiele für AWS Client-VPN.

Beschränken des Zugriffs auf Netzwerke

Sie können Ihren Client VPN-Endpunkt so konfigurieren, dass der Zugriff auf spezifische Ressourcen in Ihrer VPC eingeschränkt wird. Für die benutzerbasierte Authentifizierung können Sie auch den Zugriff auf Teile des Netzwerks basierend auf der Benutzergruppe, die auf den Client VPN-Endpunkt zugreift, einschränken. Weitere Informationen finden Sie unter Den Zugriff auf Ihr Netzwerk mit AWS Client VPN beschränken.

Authentifizieren von Clients

Die Authentifizierung wird am ersten Eintrittspunkt in die AWS Cloud implementiert. Mit ihrer Hilfe wird ermittelt, ob Clients eine Verbindung mit dem Client VPN-Endpunkt herstellen dürfen. Wenn die Authentifizierung erfolgreich ist, stellen Clients eine Verbindung mit dem Client VPN-Endpunkt her und richtet eine VPN-Sitzung ein. Schlägt die Authentifizierung fehl, wird die Verbindung abgelehnt und der Client kann keine VPN-Sitzung einrichten.

Client VPN unterstützt die folgenden Clientauthentifizierungstypen:

- Active Directory-Authentifizierung (benutzerbasiert)
- Gegenseitige Authentifizierung (zertifikatbasiert)
- Single Sign-On (SAML-basierte Verbundauthentifizierung) (benutzerbasiert)

Identitäts- und Zugriffsmanagement für AWS Client VPN

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren steuern, wer für die Nutzung von

Client-VPN-Ressourcen authentifiziert (angemeldet) und autorisiert (mit Berechtigungen ausgestattet) werden kann. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Client VPN ausführen.

Servicebenutzer: Wenn Sie den Client-VPN-Service zur Ausführung Ihrer Aufgaben verwenden, stellt Ihnen Ihr Administrator die nötigen Anmeldeinformationen und Berechtigungen bereit. Wenn Sie für Ihre Arbeit weitere Client-VPN-Funktionen nutzen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Beachten Sie die Informationen unter Problembehandlung bei AWS Client-VPN-Identität und -Zugriff, falls Sie nicht auf eine Funktion in Client VPN zugreifen können.

Serviceadministrator: Wenn Sie in Ihrem Unternehmen für Client-VPN-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Client VPN. Es ist Ihre Aufgabe, zu bestimmen, auf welche Client-VPN-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Client VPN verwenden kann, finden Sie unter So funktioniert AWS Client VPN mit IAM.

IAM-Administrator: Wenn Sie IAM-Administrator sind, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Client VPN verfassen können. Beispiele für identitätsbasierte Client-VPN-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für Client VPN 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 Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

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

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

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-

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

Verbundidentität

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 einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

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

IAM-Rollen

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

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

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

Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

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

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

Verwalten des Zugriffs mit Richtlinien

Sie 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. Berechtigungen in den Richtlinien bestimmen, ob die 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 bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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

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

Identitätsbasierte Richtlinien

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

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie

mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

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

Zugriffssteuerungslisten (ACLs)

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

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

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.

- Service Control Policies (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 innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen 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 AWS Client VPN mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Client VPN verwenden, sollten Sie wissen, welche IAM-Funktionen Sie mit Client VPN verwenden können.

IAM-Funktionen, die Sie mit AWS Client VPN verwenden können

IAM-Feature	Client-VPN-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Client VPN 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 Client VPN

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen

ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

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

Beispiele für identitätsbasierte Richtlinien für Client VPN

Beispiele für identitätsbasierte Richtlinien für Client VPN finden Sie unter Beispiele für identitätsbasierte Richtlinien für Client VPN AWS.

Ressourcenbasierte Richtlinien in Client VPN

Unterstützt ressourcenbasierte Richtlinien	Nein

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

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

gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für Client VPN

Unterstützt Richtlinienaktionen	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 `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 Client-VPN-Aktionen finden Sie unter Von AWS Client VPN definierte Aktionen in der Serviceautorisierungsreferenz.

Richtlinienaktionen in Client VPN verwenden das folgende Präfix vor der Aktion:

```
ec2
```

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

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Beispiele für identitätsbasierte Client-VPN-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Client VPN AWS.

Richtlinienressourcen für Client VPN

Unterstützt Richtlinienressourcen	Ja

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

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

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

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

Eine Liste der Client-VPN-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Client VPN definierte Ressourcen in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Client VPN definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für Client VPN finden Sie unter Beispiele für identitätsbasierte Richtlinien für Client VPN AWS.

Richtlinienbedingungsschlüssel für Client VPN

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

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

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

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

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

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

Eine Liste der Client-VPN-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Client VPN in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Client VPN definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für Client VPN finden Sie unter Beispiele für identitätsbasierte Richtlinien für Client VPN AWS.

ACLs in Client VPN

Unterstützt ACLs	Nein

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

ABAC mit Client VPN

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 Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

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

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

Verwenden temporärer Anmeldeinformationen mit Client VPN

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 zu einer 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 Client VPN

Unterstützt Forward Access Sessions (FAS)	Ja

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

Servicerollen für Client VPN

Unterstützt Servicerollen	Ja

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**
>
> Wenn Berechtigungen für eine Servicerolle geändert werden, könnte dies die Client-VPN-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Client VPN dazu Anleitungen gibt.

Serviceverknüpfte Rollen für Client VPN

Unterstützt serviceverknüpfte Rollen	Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. 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 Client VPN AWS

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

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

Einzelheiten zu den von Client VPN definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Client VPN in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

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

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

und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem 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 Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

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 oder. AWS CLI AWS

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

```
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Problembehandlung bei AWS Client-VPN-Identität und -Zugriff

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

Themen

- Ich bin nicht autorisiert, eine Aktion in Client VPN auszuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Client-VPN-Ressourcen ermöglichen

Ich bin nicht autorisiert, eine Aktion in Client VPN auszuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `ec2:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `ec2:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien so aktualisiert werden, dass Sie eine Rolle an Client VPN übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Client VPN auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Client-VPN-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. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Client VPN diese Funktionen unterstützt, finden Sie unter So funktioniert AWS Client VPN 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 im IAM-Benutzerhandbuch unter Kontenübergreifender Ressourcenzugriff in IAM.

Verwenden von serviceverknüpften Rollen für Client VPN

AWS Client VPN verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, die direkt mit Client VPN verknüpft ist. Serviceverknüpfte Rollen werden von Client VPN vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Themen

Verwenden von Rollen für Client VPN

AWS Client VPN verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, die direkt mit Client VPN verknüpft ist. Serviceverknüpfte Rollen werden von Client VPN vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Cloud VPN, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Client VPN definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Client VPN die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und

Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Client-VPN-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Client VPN

Client VPN verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForClientVPN – Client VPN gestatten, Ressourcen im Zusammenhang mit Ihren VPN-Verbindungen zu erstellen und zu verwalten.

Die Rolle AWSServiceRoleForClientVPN vertraut darauf, dass der folgende Service die Rolle übernimmt:

- `clientvpn.amazonaws.com`

Die Rollenberechtigungsrichtlinie namens ClientVPNServiceRolePolicy gestattet Client VPN die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

- Aktion: `ec2:CreateNetworkInterface` für `Resource: "*"`
- Aktion: `ec2:CreateNetworkInterfacePermission` für `Resource: "*"`
- Aktion: `ec2:DescribeSecurityGroups` für `Resource: "*"`
- Aktion: `ec2:DescribeVpcs` für `Resource: "*"`
- Aktion: `ec2:DescribeSubnets` für `Resource: "*"`
- Aktion: `ec2:DescribeInternetGateways` für `Resource: "*"`
- Aktion: `ec2:ModifyNetworkInterfaceAttribute` für `Resource: "*"`
- Aktion: `ec2:DeleteNetworkInterface` für `Resource: "*"`
- Aktion: `ec2:DescribeAccountAttributes` für `Resource: "*"`

- Aktion: `ds:AuthorizeApplication` für `Resource: "*"`
- Aktion: `ds:DescribeDirectories` für `Resource: "*"`
- Aktion: `ds:GetDirectoryLimits` für `Resource: "*"`
- Aktion: `ds:UnauthorizeApplication` für `Resource: "*"`
- Aktion: `logs:DescribeLogStreams` für `Resource: "*"`
- Aktion: `logs:CreateLogStream` für `Resource: "*"`
- Aktion: `logs:PutLogEvents` für `Resource: "*"`
- Aktion: `logs:DescribeLogGroups` für `Resource: "*"`
- Aktion: `acm:GetCertificate` für `Resource: "*"`
- Aktion: `acm:DescribeCertificate` für `Resource: "*"`
- Aktion: `iam:GetSAMLProvider` für `Resource: "*"`
- Aktion: `lambda:GetFunctionConfiguration` für `Resource: "*"`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Client VPN

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie den ersten Client-VPN-Endpunkt in Ihrem Konto über die AWS Management Console, die AWS CLI oder die AWS-API erstellen, erstellt Client VPN die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie den ersten Client-VPN-Endpunkt in Ihrem Konto erstellen, erstellt Client VPN ebenfalls die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für Client VPN

Client VPN berechtigt Sie nicht zum Bearbeiten der serviceverknüpften Rolle AWSServiceRoleForClientVPN. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Client VPN

Wenn Sie Client VPN nicht mehr benötigen, empfehlen wir, die serviceverknüpfte Rolle AWSServiceRoleForClientVPN zu löschen.

Sie müssen zuerst die zugehörigen Client VPN-Ressourcen löschen. Auf diese Weise wird sichergestellt, dass Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen.

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um serviceverknüpfte Rollen zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Client-VPN-Rollen

Client VPN unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS-Regionen und -Endpunkte.

Verwenden von Rollen für die Verbindungsautorisierung

AWS Client VPN verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, die direkt mit Client VPN verknüpft ist. Serviceverknüpfte Rollen werden von Client VPN vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Cloud VPN, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Client VPN definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Client VPN die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Client-VPN-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie

über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Client VPN

Client VPN verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForClientVPNConnections – Serviceverknüpfte Rolle für Client-VPN-Verbindungen.

Die serviceverknüpfte Rolle AWSServiceRoleForClientVPNConnections vertraut darauf, dass die folgenden Services die Rolle übernehmen:

- `clientvpn-connections.amazonaws.com`

Die Rollenberechtigungsrichtlinie namens ClientVPNServiceConnectionsRolePolicy gestattet Client VPN die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

- Aktion: `lambda:InvokeFunction` für `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Client VPN

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie den ersten Client-VPN-Endpunkt in Ihrem Konto über die AWS Management Console, die AWS CLI oder die AWS-API erstellen, erstellt Client VPN die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie den ersten Client-VPN-Endpunkt in Ihrem Konto erstellen, erstellt Client VPN ebenfalls die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für Client VPN

Client VPN berechtigt Sie nicht zum Bearbeiten der serviceverknüpften Rolle AWSServiceRoleForClientVPNConnections. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Client VPN

Wenn Sie Client VPN nicht mehr benötigen, empfehlen wir, die serviceverknüpfte Rolle AWSServiceRoleForClientVPNConnections zu löschen.

Sie müssen zuerst die zugehörigen Client VPN-Ressourcen löschen. Auf diese Weise wird sichergestellt, dass Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen.

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um serviceverknüpfte Rollen zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Client-VPN-Rollen

Client VPN unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS-Regionen und -Endpunkte.

Ausfallsicherheit in AWS Client VPN

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und Availability Zones (Verfügbarkeitszonen, AZs). AWS-Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

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

Neben der globalen AWS-Infrastruktur stellt AWS Client VPN Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden.

Mehrere Zielnetzwerke für hohe Verfügbarkeit

Sie verknüpfen ein Zielnetzwerk mit einem Client VPN-Endpunkt, damit Clients VPN-Sitzungen einrichten können. Zielnetzwerke sind Subnetze in Ihrer VPC. Jedes Subnetz, das Sie mit dem Client VPN-Endpunkt verknüpfen, muss zu einer anderen Availability Zone gehören. Sie können mehrere Subnetze mit einem Client VPN-Endpunkt verknüpfen, um eine hohe Verfügbarkeit zu gewährleisten.

Sicherheit der Infrastruktur in AWS Client VPN

Als verwalteter Service ist AWS Client VPN durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden von AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Client VPN zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

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

Bewährte Methoden für die Sicherheit für AWS Client VPN

AWS Client VPN enthält eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Autorisierungsregeln

Verwenden Sie Autorisierungsregeln, um einzuschränken, welche Benutzer auf Ihr Netzwerk zugreifen können. Weitere Informationen finden Sie unter Autorisierungsregeln.

Sicherheitsgruppen

Verwenden Sie Sicherheitsgruppen, um zu steuern, auf welche Ressourcen Benutzer in Ihrer VPC zugreifen können. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Client-Zertifikatsperrlisten

Sie können Client-Zertifikatsperrlisten verwenden, um den Zugriff auf einen Client-VPN-Endpunkt für bestimmte Clientzertifikate zu widerrufen, zum Beispiel, wenn ein Benutzer Ihre Organisation verlässt. Weitere Informationen finden Sie unter Client-Zertifikatsperrlisten.

Überwachungstools

Verwenden Sie Überwachungs-Tools, um die Verfügbarkeit und Leistung Ihrer Client VPN-Endpunkte zu verfolgen. Weitere Informationen finden Sie unter Überwachen des AWS Client VPN.

Identity and Access Management

Verwalten Sie den Zugriff auf Client-VPN-Ressourcen und APIs, indem Sie IAM-Richtlinien für Ihre IAM-Benutzer und IAM-Rollen verwenden. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS Client VPN.

Überlegungen zu IPv6 für AWS Client VPN

Derzeit unterstützt der Client-VPN-Service das Routing von IPv6-Datenverkehr durch den VPN-Tunnel nicht. Es gibt jedoch Fälle, in denen IPv6-Datenverkehr in den VPN-Tunnel geroutet werden sollte, um ein IPv6-Leck zu verhindern. Ein IPv6-Leck kann auftreten, wenn sowohl IPv4 als auch IPv6 aktiviert und mit dem VPN verbunden sind, aber das VPN keinen IPv6-Datenverkehr in seinen Tunnel leitet. Wenn Sie in diesem Fall eine Verbindung zu einem IPv6-aktivierten Ziel herstellen, stellen Sie tatsächlich immer noch eine Verbindung mit Ihrer IPv6-Adresse her, die von Ihrem ISP bereitgestellt wird. Dadurch wird Ihre echte IPv6-Adresse lecken. In den folgenden Anweisungen wird erläutert, wie IPv6-Datenverkehr in den VPN-Tunnel weitergeleitet wird.

Die folgenden IPv6-bezogenen Direktiven sollten der Client-VPN-Konfigurationsdatei hinzugefügt werden, um ein IPv6-Leck zu verhindern:

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

Ein Beispiel könnte sein:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

In diesem Beispiel setzt `ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` die IPv6-Adresse des lokalen Tunnelgeräts auf `fd15:53b6:dead::2` und die IPv6-Adresse des Remote-VPN-Endpunkts auf `fd15:53b6:dead::1`.

Mit dem nächsten Befehl wird `route-ipv6 2000::/4` IPv6-Adressen von `2000:0000:0000:0000:0000:0000:0000:0000` auf `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` in die VPN-Verbindung routen.

> **Note**
>
> Für das „TAP“-Geräterouting in Windows wird beispielsweise der zweite Parameter von `ifconfig-ipv6` als Routenziel für `--route-ipv6` genutzt.

Organisationen sollten die beiden Parameter von `ifconfig-ipv6` selbst konfigurieren und können Adressen in `100::/64` (von `0100:0000:0000:0000:0000:0000:0000:0000` bis `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) oder `fc00::/7` (von `fc00:0000:0000:0000:0000:0000:0000:0000` bis `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`) verwenden. `100::/64` ist ein Nur-Verwerf-Addressblock und `fc00::/7` ist eindeutig-lokal.

Ein weiteres Beispiel:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

In diesem Beispiel leitet die Konfiguration den derzeit zugewiesenen IPv6-Datenverkehr an die VPN-Verbindung weiter.

Verifizierung

Ihre Organisation wird wahrscheinlich eigene Tests haben. Eine grundlegende Überprüfung besteht darin, eine vollständige Tunnel-VPN-Verbindung einzurichten und dann ping6 zu einem IPv6-Server unter Verwendung der IPv6-Adresse auszuführen. Die IPv6-Adresse des Servers sollte in dem vom `route-ipv6`-Befehl angegebenen Bereich liegen. Dieser Ping-Test sollte fehlschlagen. Dies kann sich jedoch ändern, wenn dem Client-VPN-Service in Zukunft IPv6-Unterstützung hinzugefügt wird. Wenn der Ping erfolgreich ist und Sie auf öffentliche Websites zugreifen können, wenn Sie im Voll-

Tunnelmodus verbunden sind, müssen Sie möglicherweise weitere Fehlerbehebungen durchführen. Sie können auch testen, indem Sie einige öffentlich verfügbare Tools wie ipleak.org nutzen.

Überwachen des AWS Client VPN

Die Überwachung ist ein wichtiger Teil der Aufrechterhaltung von Zuverlässigkeit, Verfügbarkeit und Performance von AWS Client VPN und Ihren anderen AWS-Lösungen. Sie können die folgenden Funktionen verwenden, um Ihre Client VPN-Endpunkte zu überwachen, Datenverkehrsmuster zu analysieren und Probleme mit Ihren Client VPN-Endpunkten zu beheben.

Amazon CloudWatch

Überwacht Ihre AWS-Ressourcen und die Anwendungen, die Sie in AWS ausführen, in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Beispielsweise können Sie mit CloudWatch die CPU-Auslastung oder andere Metriken Ihrer Amazon EC2-Instances erfassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im Amazon CloudWatch User Guide.

AWS CloudTrail

Erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

Amazon CloudWatch Logs

Erlaubt Ihnen, die Verbindungsversuche zu Ihrem AWS Client VPN-Endpunkt zu überwachen. Sie können die Verbindungsversuche und Verbindungsrücksetzungen für die Client VPN-Verbindungen anzeigen. Bei den Verbindungsversuchen können Sie sowohl die erfolgreichen als auch die fehlgeschlagenen Verbindungsversuche anzeigen. Sie können den CloudWatch Logs-Protokolldatenstrom angeben, um die Verbindungsdetails zu protokollieren. Weitere Informationen finden Sie unter Verbindungsprotokollierung und im Amazon CloudWatch Logs-Benutzerhandbuch.

CloudWatch-Metriken für AWS Client VPN

AWS Client VPN veröffentlicht für Ihre Client VPN-Endpunkte die folgenden Metriken an Amazon CloudWatch. Metriken werden alle fünf Minuten auf Amazon CloudWatch veröffentlicht.

Metrik	Beschreibung
ActiveConnectionsCount	Die Anzahl der aktiven Verbindungen zum Client VPN-Endpunkt. Einheiten: Anzahl
AuthenticationFailures	Die Anzahl von Authentifizierungsfehlern für den Client VPN-Endpunkt. Einheiten: Anzahl
CrlDaysToExpiry	Die Anzahl der Tage, bis die auf dem Client VPN-Endpunkt konfigurierte Zertifikatsperrliste (Certificate Revocation List, CRL) abläuft. Einheiten: Tage
EgressBytes	Die Anzahl der vom Client VPN-Endpunkt gesendeten Bytes. Einheiten: Byte
EgressPackets	Die Anzahl der vom Client VPN-Endpunkt gesendeten Pakete. Einheiten: Anzahl
IngressBytes	Die Anzahl der vom Client VPN-Endpunkt empfangenen Bytes. Einheiten: Byte
IngressPackets	Die Anzahl der vom Client VPN-Endpunkt empfangenen Pakete. Einheiten: Anzahl
SelfServicePortalClientConfigurationDownloads	Die Anzahl der Downloads der Client VPN-Endpunkt-Konfigurationsdatei aus dem Self-Service-Portal.

Metrik	Beschreibung
	Einheit: Anzahl

AWS Client VPN veröffentlicht die folgenden Metriken zur Statusbewertung für Ihre Client VPN-Endpunkte.

Metrik	Beschreibung
ClientConnectHandlerTimeouts	Die Anzahl der Timeouts beim Aufrufen des Client-Connect-Handlers für Verbindungen zum Client-VPN-Endpunkt. Einheiten: Anzahl
ClientConnectHandlerInvalidResponses	Die Anzahl der ungültigen Antworten, die vom Client-Connect-Handler für Verbindungen zum Client-VPN-Endpunkt zurückgegeben wurden. Einheiten: Anzahl
ClientConnectHandlerOtherExecutionErrors	Die Anzahl der unerwarteten Fehler beim Ausführen des Client-Connect-Handlers für Verbindungen zum Client-VPN-Endpunkt. Einheiten: Anzahl
ClientConnectHandlerThrottlingErrors	Die Anzahl der Drosselungsfehler beim Aufrufen des Client-Connect-Handlers für Verbindungen zum Client-VPN-Endpunkt. Einheiten: Anzahl
ClientConnectHandlerDeniedConnections	Die Anzahl der Verbindungen, die vom Client-Connect-Handler für Verbindungen zum Client-VPN-Endpunkt verweigert wurden. Einheiten: Anzahl

Metrik	Beschreibung
ClientConnectHandlerFailedServiceErrors	Die Anzahl der dienstseitigen Fehler beim Ausführen des Client-Connect-Handlers für Verbindungen zum Client-VPN-Endpunkt. Einheiten: Anzahl

Sie können die Metriken für Ihren Client VPN-Endpunkt nach Endpunkten filtern.

CloudWatch ermöglicht Ihnen, Statistiken zu diesen Datenpunkten als geordneten Satz von Zeitreihendaten, als Metriken bezeichnet, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können z. B. einen CloudWatch-Alarm erstellen, um eine bestimmte Metrik zu überwachen, und eine Aktion einleiten (z. B. Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb eines für Sie akzeptablen Bereichs liegt.

Weitere Informationen finden Sie im Amazon CloudWatch User Guide.

Anzeigen von CloudWatch-Metriken

Sie können folgendermaßen die Metriken zu Ihrem Client-VPN-Endpunkt anzeigen.

So zeigen Sie Metriken mit der CloudWatch-Konsole an:

Metriken werden zunächst nach dem Service-Namespace und anschließend nach den verschiedenen Dimensionskombinationen in den einzelnen Namespaces gruppiert.

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie unter All metrics den Metriknamespace ClientVPN aus.
4. Um die Metriken anzuzeigen, wählen Sie die Metrikdimension nach Endpunkt aus.

So zeigen Sie Metriken mit der a AWS CLI

Führen Sie bei der Eingabeaufforderung den folgenden Befehl aus, um die Metriken aufzulisten, die für den Client VPN zur Verfügung stehen:

```
aws cloudwatch list-metrics --namespace "AWS/ClientVPN"
```

CloudTrail-Protokolle für AWS Client-VPN

AWS Client VPN ist in AWS CloudTrail integriert, einen Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Services in Client VPN protokolliert. CloudTrail erfasst alle API-Aufrufe für Client VPN als Ereignisse. Die erfassten Aufrufe umfassen Anrufe von der Client VPN-Konsole und Codeaufrufe an die Client VPN-API-Operationen. Wenn Sie einen Trail erstellen, aktivieren Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3-Bucket, einschließlich Ereignissen für Client VPN. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die an Client VPN gestellte Anforderung, die anfordernde IP-Adresse, den Anforderer, den Zeitpunkt der Anforderung und weitere Details bestimmen.

Weitere Informationen über CloudTrail finden Sie im AWS CloudTrail-Leitfaden.

Informationen zu Client VPN in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Die in Client VPN auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen AWS-Serviceereignissen unter Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Wenn Sie eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto benötigen, bei denen auch Ereignisse für Client VPN berücksichtigt sind, erstellen Sie einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails

- Siehe Von CloudTrail unterstützte Services und Integrationen.
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien von mehreren Konten.

Alle Client VPN-Aktionen werden von CloudTrail protokolliert. Sie sind in der Amazon EC2-API-Referenzdokumentiert. Zum Beispiel generieren Aufrufe der Aktionen `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork` und `AuthorizeClientVpnIngress` Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

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

Weitere Informationen finden Sie unter dem CloudTrail userIdentity-Element.

Verstehen von Client VPN-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Weitere Informationen finden Sie unter Protokollierung von Amazon EC2-, Amazon EBS- und Amazon VPC-API-Aufrufe mit AWS CloudTrail in der Amazon EC2-API-Referenz.

AWS VPN-Kontingente für Kunden

Ihr AWS Konto hat die folgenden Kontingente, die früher als Limits bezeichnet wurden und sich auf Client-VPN-Endpunkte beziehen. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um eine Kontingenterhöhung für ein einstellbares Kontingent zu beantragen, wählen Sie Ja in der Spalte Anpassbar. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Client VPN-Kontingente

Name	Standard	Anpassbar
Autorisierungsregeln pro Client-VPN-Endpunkt	50	Ja
Client-VPN-Endpunkte pro Region	5	Ja
Gleichzeitige Client-Verbindungen pro Client-VPN-Endpunkt	Dieser Wert hängt von der Anzahl der Subnetzzuordnungen pro Endpunkt ab. • 1 — 20.000 • 2 - 36.500 • 3 - 66.500 • 4 - 96.500 • 5 - 126.000	Ja
Gleichzeitige Operationen pro Client-VPN-Endpunkt	10	Nein
Einträge in einer Client-Zertifikatssperrliste für Client-VPN-Endpunkte	20 000	Nein
Routen pro Client-VPN-Endpunkt	10	Ja

† Operationen umfassen:

- Verknüpfen oder Trennen von Subnetzen
- Erstellen oder löschen von Routen
- Erstellen oder löschen von eingehenden und ausgehenden Regeln
- Erstellen oder Löschen von Sicherheitsgruppen

Kontingente für Benutzer und Gruppen

Wenn Sie Benutzer und Gruppen für Active Directory oder einen SAML-basierten IdP konfigurieren, gelten die folgenden Kontingente:

- Benutzer können maximal 200 Gruppen angehören. Alle Gruppen nach der 200. Gruppe werden ignoriert.
- Die maximale Länge für die Gruppen-ID beträgt 255 Zeichen.
- Die maximale Länge für die Namens-ID beträgt 255 Zeichen. Zeichen nach dem 255. Zeichen werden abgeschnitten.

Allgemeine Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie Client VPN-Endpunkte verwenden:

- Wenn Sie Active Directory verwenden, um den Benutzer zu authentifizieren, muss der Client-VPN-Endpunkt demselben Konto angehören wie die AWS Directory Service Ressource, die für die Active Directory-Authentifizierung verwendet wird.
- Wenn Sie die SAML-basierte Verbundauthentifizierung verwenden, um einen Benutzer zu authentifizieren, muss der Client-VPN-Endpunkt zu demselben Konto gehören wie der IAM-SAML-Identitätsanbieter, den Sie erstellen, um die Beziehung zwischen IdP und Trust zu definieren.AWS Der IAM-SAML-Identitätsanbieter kann von mehreren Client-VPN-Endpunkten in demselben Konto gemeinsam genutzt werden. AWS

Fehlerbehebung bei AWS Client VPN

Das folgende Thema kann Ihnen bei der Behebung von Problemen helfen, die mit einem Client VPN-Endpunkt auftreten könnten.

Weitere Informationen zur Fehlerbehebung bei OpenVPN-basierter Software, mit der Clients eine Verbindung zu einem Client VPN herstellen, finden Sie unter Fehlerbehebung bei Ihrer Client-VPN-Verbindung im Benutzerhandbuch zu AWS Client VPN .

Allgemeine Probleme

DNS-Name des Client-VPN-Endpunkts konnte nicht aufgelöst werden

Problem

Ich kann den DNS-Namen des Client-VPN-Endpunkts nicht auflösen.

Ursache

Die Client-VPN-Endpunktkonfigurationsdatei enthält einen Parameter mit dem Namen `remote-random-hostname`. Dieser Parameter zwingt den Client, dem DNS-Namen eine zufällige Zeichenfolge voranzustellen, um das DNS-Caching zu verhindern. Einige Clients erkennen diesen Parameter nicht und stellen daher dem DNS-Namen nicht die erforderliche zufällige Zeichenfolge voran.

Lösung

Öffnen Sie die Client-VPN-Endpunktkonfigurationsdatei mit Ihrem bevorzugten Texteditor. Suchen Sie die Zeile, die den Client VPN-Endpunkt-DNS-Namen angibt. Stellen Sie ihm eine zufällige Zeichenfolge voran. Das Format lautet *`zufällige_zeichenfolge.angezeigter_DNS_name`*. Zum Beispiel:

- Ursprünglicher DNS-Name: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Geänderter DNS-Name: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Der Datenverkehr wird nicht zwischen Subnetzen aufgeteilt.

Problem

Ich versuche, den Netzwerkdatenverkehr zwischen zwei Subnetze aufzuteilen. Privater Datenverkehr sollte durch ein privates Subnetz geroutet werden, während Internet-Datenverkehr durch ein öffentliches Subnetz geroutet werden sollte. Es wird nur eine Route verwendet, obwohl ich beide Routen in die Client-VPN-Endpunkt-Routing-Tabelle aufgenommen habe.

Ursache

Sie können einem Client-VPN-Endpunkt mehrere Subnetze zuweisen, aber Sie können nur ein Subnetz pro Availability Zone zuweisen. Der Zweck der mehrfachen Subnetz-Zuordnung ist die Bereitstellung von Hochverfügbarkeits- und Availability Zone-Redundanz für Clients. Mit dem Client-VPN können Sie den Datenverkehr jedoch nicht selektiv zwischen den Subnetze aufteilen, die dem Client-VPN-Endpunkt zugeordnet sind.

Clients stellen eine Verbindung zu einem Client-VPN-Endpunkt basierend auf dem DNS-Round-Robin-Algorithmus her. Das bedeutet, dass ihr Datenverkehr durch jedes der zugehörigen Subnetze geroutet werden kann, wenn sie eine Verbindung herstellen. Daher kann es zu Verbindungsproblemen kommen, wenn sie in einem zugehörigen Subnetz landen, das nicht über die erforderlichen Routingeinträge verfügt.

Angenommen, Sie konfigurieren beispielsweise die folgenden Subnetz-Zuordnungen und Routen:

- Subnetzzuordnungen
  - Zuordnung 1: Subnetz-A (us-ost-1a)
  - Zuordnung 2: Subnetz-B (us-ost-1b)
- Routen
  - Route 1: 10.0.0.0/16 geroutet zu Subnetz-A
  - Route 2: 172.31.0.0/16 geroutet zu Subnetz-B

In diesem Beispiel können Clients, die beim Verbindungsaufbau in Subnetz-A landen, nicht auf Route 2 zugreifen, während Clients, die beim Verbindungsaufbau in Subnetz-B landen, nicht auf Route 1 zugreifen können.

Lösung

Vergewissern Sie sich, dass der Client-VPN-Endpunkt dieselben Routeneinträge mit Zielen für jedes zugehörige Netzwerk hat. Dadurch wird sichergestellt, dass Clients Zugriff auf alle Routen haben, unabhängig vom Subnetz, durch das ihr Datenverkehr geroutet wird.

Autorisierungsregeln für Active Directory-Gruppen, die nicht wie erwartet funktionieren

Problem

Ich habe Autorisierungsregeln für meine Active Directory-Gruppen konfiguriert, aber sie funktionieren nicht wie erwartet. Ich habe eine Autorisierungsregel für `0.0.0.0/0` hinzugefügt, um den Datenverkehr für alle Netzwerke zu autorisieren, aber für bestimmte Ziel-CIDRs schlägt der Datenverkehr immer noch fehl.

Ursache

Autorisierungsregeln werden für Netzwerk-CIDRs festgelegt. Autorisierungsregeln müssen Active Directory-Gruppen Zugriff auf bestimmte Netzwerk-CIDRs gewähren. Autorisierungsregelnn für `0.0.0.0/0` werden als Sonderfall behandelt und daher als letzte ausgewertet, unabhängig von der Reihenfolge, in der die Autorisierungsregelnn erstellt werden.

Angenommen, Sie erstellen drei Autorisierungsregeln in der folgenden Reihenfolge:

- Regel 1: Zugriff Gruppe 1 auf `10.1.0.0/16`
- Regel 2: Zugriff Gruppe 1 auf `0.0.0.0/0`
- Regel 3: Zugriff Gruppe 2 auf `0.0.0.0/0`
- Regel 4: Zugriff Gruppe 3 auf `0.0.0.0/0`
- Regel 5: Zugriff Gruppe 2 auf `172.131.0.0/16`

In diesem Beispiel werden Regel 2, Regel 3 und Regel 4 zuletzt ausgewertet. Gruppe 1 hat nur Zugriff auf `10.1.0.0/16`. Gruppe 2 hat nur Zugriff auf `172.131.0.0/16`. Gruppe 3 hat keinen Zugriff auf `10.1.0.0/16` oder `172.131.0.0/16`, aber sie hat Zugriff auf alle anderen Netzwerke. Wenn Sie Regel 1 und 5 entfernen, haben alle drei Gruppen Zugriff auf alle Netzwerke.

Client VPN verwendet bei der Auswertung von Autorisierungsregeln das längste übereinstimmende Präfix. Weitere Details finden Sie in unter Routenpriorität im Benutzerhandbuch zu Amazon VPC.

Lösung

Vergewissern Sie sich, dass Sie Autorisierungsregeln erstellen, die Active Directory-Gruppen explizit Zugriff auf bestimmte Netzwerk-CIDRs gewähren. Wenn Sie eine Autorisierungsregel für `0.0.0.0/0` hinzufügen, denken Sie daran, dass diese zuletzt ausgewertet wird und dass vorherige Autorisierungsregeln die Netzwerke, auf die sie Zugriff gewährt, einschränken können.

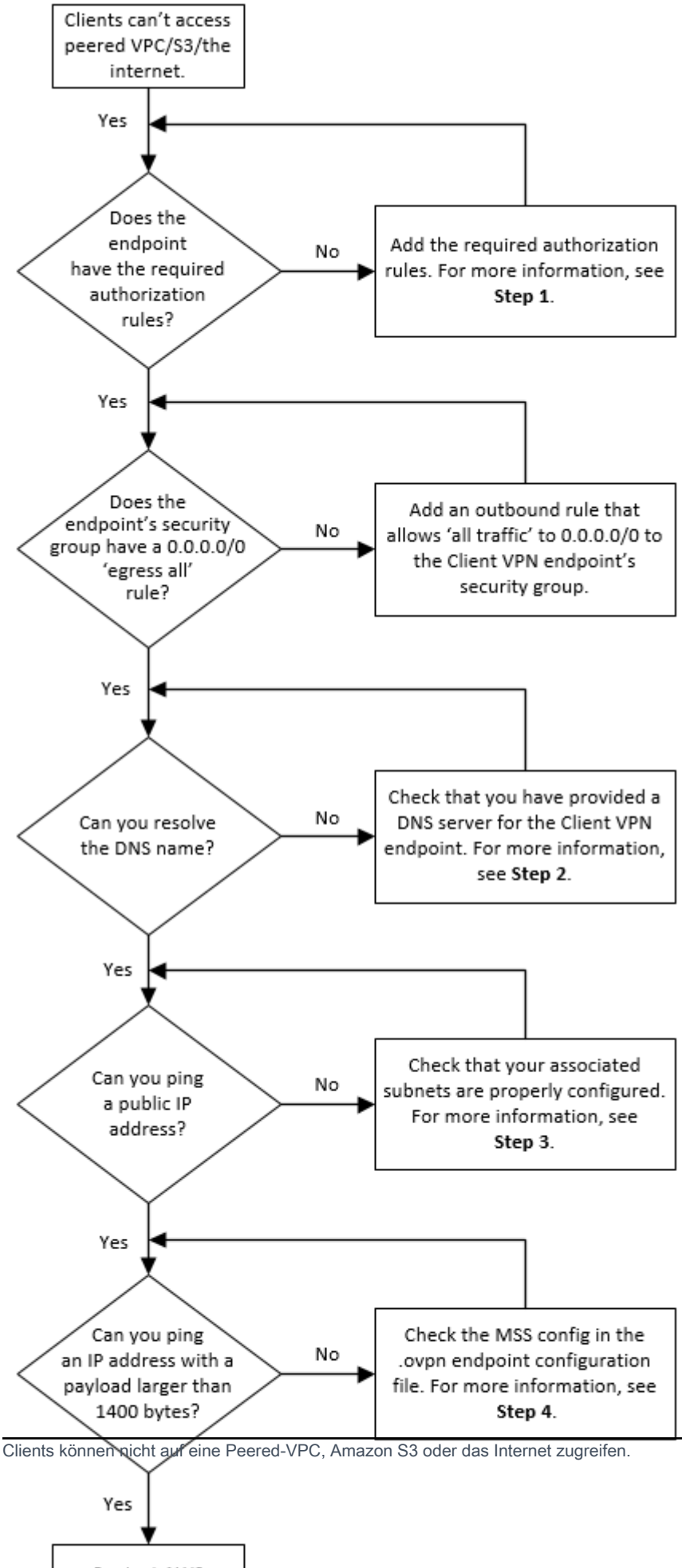
Clients können nicht auf eine Peered-VPC, Amazon S3 oder das Internet zugreifen.

Problem

Ich habe meine Client-VPN-Endpunkt-Routen korrekt konfiguriert, aber meine Clients können nicht auf eine Peer-VPC, Amazon S3 oder das Internet zugreifen.

Lösung

Das folgende Flussdiagramm enthält die Schritte zur Diagnose von Internet-, Peer-VPC- und Amazon S3-Verbindungsproblemen.


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. Für den Zugriff auf das Internet fügen Sie eine Autorisierungsregel für `0.0.0.0/0` hinzu.

   Für den Zugriff auf eine Peer-VPC fügen Sie der VPC eine Autorisierungsregel für den IPv4-CIDR-Bereich hinzu.

   Geben Sie für den Zugriff auf S3 die IP-Adresse des Amazon S3-Endpunkts an.
2. Prüfen Sie, ob Sie in der Lage sind, den DNS-Namen aufzulösen.

   Wenn Sie den DNS-Namen nicht auflösen können, vergewissern Sie sich, dass Sie die DNS-Server für den Client-VPN-Endpunkt angegeben haben. Wenn Sie Ihren eigenen DNS-Server verwalten, geben Sie seine IP-Adresse an. Vergewissern Sie sich, dass der DNS-Server von der VPC aus zugänglich ist.

   Wenn Sie sich nicht sicher sind, welche IP-Adresse für die DNS-Server angegeben werden soll, geben Sie den VPC-DNS-Resolver unter der IP-Adresse „.2“ in Ihrer VPC an.
3. Überprüfen Sie für Internetzugang, ob Sie eine öffentliche IP-Adresse oder eine öffentliche Website wie `amazon.com` pingen können. Wenn Sie keine Antwort erhalten, stellen Sie sicher, dass die Routing-Tabelle für die zugehörigen Subnetze eine Standardroute hat, die entweder auf ein Internet-Gateway oder ein NAT-Gateway verweist. Wenn die Route vorhanden ist, vergewissern Sie sich, dass das zugeordnete Subnetz nicht über Netzwerkzugriffskontrolllistenregeln verfügt, die den ein- und ausgehenden Datenverkehr blockieren.

   Wenn Sie eine Peer-VPC nicht erreichen können, überprüfen Sie, ob die Routing-Tabelle des zugehörigen Subnetze einen Routeneintrag für die Peer-VPC enthält.

   Wenn Sie Amazon S3 nicht erreichen können, überprüfen Sie, ob die Routing-Tabelle des zugehörigen Subnetzes einen Routeneintrag für den Gateway-VPC-Endpunkt enthält.
4. Prüfen Sie, ob Sie mit einem Payload von mehr als 1400 Bytes eine öffentliche IP-Adresse anpingen können. Verwenden Sie einen der folgenden Befehle:

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

Wenn Sie eine IP-Adresse mit einer Nutzlast von mehr als 1400 Bytes nicht per Ping erreichen können, öffnen Sie die `.ovpn`-Konfigurationsdatei für den Client-VPN-Endpunkt mit Ihrem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
mssfix 1328
```

Der Zugriff auf eine Peer-VPC, Amazon S3 oder das Internet erfolgt nur mit Unterbrechungen.

Problem

Ich habe zeitweilige Verbindungsprobleme, wenn ich eine Verbindung mit einer Peer-VPC, Amazon S3 oder dem Internet herstelle, aber der Zugriff auf das entsprechende Subnetz ist davon nicht betroffen. Ich muss die Verbindung trennen und wiederherstellen, um die Verbindungsprobleme zu lösen.

Ursache

Clients stellen eine Verbindung zu einem Client-VPN-Endpunkt basierend auf dem DNS-Round-Robin-Algorithmus her. Das bedeutet, dass ihr Datenverkehr durch jedes der zugehörigen Subnetze geroutet werden kann, wenn sie eine Verbindung herstellen. Daher kann es zu Verbindungsproblemen kommen, wenn sie in einem zugehörigen Subnetz landen, das nicht über die erforderlichen Routingeinträge verfügt.

Lösung

Vergewissern Sie sich, dass der Client-VPN-Endpunkt dieselben Routeneinträge mit Zielen für jedes zugehörige Netzwerk hat. Dadurch wird sichergestellt, dass Clients Zugriff auf alle Routen haben, unabhängig vom zugehörigen Subnetz, durch das ihr Datenverkehr geroutet wird.

Angenommen, Ihr Client-VPN-Endpunkt hat drei zugeordnete Subnetze (Subnetz A, B und C), und Sie möchten Ihren Clients den Internetzugriff ermöglichen. Dazu müssen Sie drei `0.0.0.0/0`-Routen hinzufügen - eine, die auf jedes zugehörige Subnetz verweist:

- Route 1: `0.0.0.0/0` für Subnetz A
- Route 2: `0.0.0.0/0` für Subnetz B

- Route 3: `0.0.0.0/0` für Subnetz C

Client-Software gibt TLS-Fehler zurück

Problem

Früher konnte ich meine Clients erfolgreich mit dem Client-VPN verbinden, aber jetzt gibt der OpenVPN-basierte Client einen der folgenden Fehler zurück, wenn er versucht, eine Verbindung herzustellen:

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

Mögliche Ursache 1

Wenn Sie die gegenseitige Authentifizierung verwenden und eine Client-Zertifikat-Widerrufsliste importiert haben, ist die Client-Zertifikat-Widerrufsliste möglicherweise abgelaufen. Während der Authentifizierungsphase prüft der Client-VPN-Endpunkt das Client-Zertifikat anhand der von Ihnen importierten Client-Zertifikat-Widerrufsliste. Wenn die Widerrufsliste für Client-Zertifikate abgelaufen ist, können Sie keine Verbindung mit dem Client-VPN-Endpunkt herstellen.

Lösung 1

Überprüfen Sie das Ablaufdatum Ihrer Client-Zertifikat-Widerrufsliste mit dem OpenSSL-Tool.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

Die Ausgabe zeigt das Ablaufdatum und die Uhrzeit an. Wenn die Widerrufsliste für Client-Zertifikate abgelaufen ist, müssen Sie eine neue Liste erstellen und sie für den Client-VPN-Endpunkt importieren. Weitere Informationen finden Sie unter Client-Zertifikatsperrlisten.

Mögliche Ursache 2

Das für den Client-VPN-Endpunkt verwendete Serverzertifikat ist abgelaufen.

Lösung 2

Überprüfen Sie den Status Ihres Serverzertifikats in der AWS Certificate Manager Konsole oder mithilfe der AWS CLI. Wenn das Serverzertifikat abgelaufen ist, erstellen Sie ein neues Zertifikat und laden Sie es auf ACM hoch. Ausführliche Schritte zum Generieren der Server- und Client-Zertifikate und Schlüssel unter Verwendung des OpenVPN-Dienstprogramms easy-rsa sowie zu deren Import in ACM finden Sie unter Gegenseitige Authentifizierung.

Alternativ könnte ein Problem mit der OpenVPN-basierten Software bestehen, die der Client zur Verbindung mit dem Client-VPN verwendet. Weitere Informationen zur Fehlerbehebung bei OpenVPN-basierter Software finden Sie unter Fehlerbehebung für Ihre Client-VPN-Verbindung im Benutzerhandbuch zu AWS Client VPN .

Client-Software gibt Fehler zum Benutzernamen und Passwort zurück (Active Directory-Authentifizierung)

Problem

Ich verwende die Active Directory-Authentifizierung für meinen Client-VPN-Endpunkt und konnte meine Clients früher erfolgreich mit dem Client-VPN verbinden. Jetzt erhalten die Clients jedoch Fehler zu ungültigen Benutzernamen und Passwörtern.

Mögliche Ursachen

Wenn Sie die Active Directory-Authentifizierung verwenden und Multi-Factor Authentication (MFA) aktiviert haben, nachdem Sie die Client-Konfigurationsdatei verteilt haben, enthält die Datei nicht die erforderlichen Informationen, um Benutzer zur Eingabe ihres MFA-Codes aufzufordern. Die Benutzer werden aufgefordert, nur ihren Benutzernamen und ihr Passwort einzugeben, und die Authentifizierung schlägt fehl.

Lösung

Laden Sie eine neue Client-Konfigurationsdatei herunter und verteilen Sie sie an Ihre Clients. Vergewissern Sie sich, dass die neue Datei die folgende Zeile enthält.

```
static-challenge "Enter MFA code " 1
```

Weitere Informationen finden Sie unter Exportieren und Konfigurieren der Client-Konfigurationsdatei. Testen Sie die MFA-Konfiguration für Ihr Active Directory, ohne den Client-VPN-Endpunkt zu verwenden, um zu überprüfen, ob MFA wie erwartet funktioniert.

Client-Software gibt Fehler bei Benutzernamen und Passwörtern zurück (Verbundauthentifizierung)

Problem

Der Versuch, sich mit einem Benutzernamen und einem Passwort mit Verbundauthentifizierung anzumelden und die Fehlermeldung „Die empfangenen Anmeldeinformationen waren falsch“ zu erhalten. Wenden Sie sich an Ihren IT-Administrator.“

Ursache

Dieser Fehler kann dadurch verursacht werden, dass nicht mindestens ein Attribut in der SAML-Antwort vom IdP enthalten ist.

Lösung

Stellen Sie sicher, dass mindestens ein Attribut in der SAML-Antwort des IdP enthalten ist. Weitere Informationen finden Sie unter Konfigurationsressourcen für SAML-basierte IdPs.

Clients können keine Verbindung herstellen (gegenseitige Authentifizierung)

Problem

Ich verwende die gegenseitige Authentifizierung für meinen Client-VPN-Endpunkt. Clients erhalten bei fehlgeschlagenen TLS-Schlüsselaushandlungen und Zeitüberschreitungsfehler Fehler.

Mögliche Ursachen

Die Konfigurationsdatei, die den Clients zur Verfügung gestellt wurde, enthält nicht das Client-Zertifikat und den privaten Schlüssel des Clients, oder das Zertifikat und der Schlüssel sind falsch.

Lösung

Stellen Sie sicher, dass die Konfigurationsdatei das richtige Client-Zertifikat und den richtigen Schlüssel enthält. Korrigieren Sie gegebenenfalls die Konfigurationsdatei und verteilen Sie sie erneut an Ihre Clients. Weitere Informationen finden Sie unter Exportieren und Konfigurieren der Client-Konfigurationsdatei.

Client gibt einen Fehler zurück, der besagt, dass die Anmeldeinformationen die maximale Größe überschreiten (Verbundauthentifizierung)

Problem

Ich verwende die Verbundauthentifizierung für meinen Client-VPN-Endpunkt. Wenn Clients ihren Benutzernamen und ihr Passwort im Browserfenster des SAML-basierten Identitätsanbieters (IdP) eingeben, wird ein Fehler angezeigt, dass die Anmeldeinformationen die maximal unterstützte Größe überschreiten.

Ursache

Die vom IdP zurückgegebene SAML-Antwort überschreitet die maximal unterstützte Größe. Weitere Informationen finden Sie unter Anforderungen und Überlegungen für die SAML-basierte Verbundauthentifizierung.

Lösung

Versuchen Sie, die Anzahl der Gruppen zu reduzieren, zu denen der Benutzer im IdP gehört, und versuchen Sie erneut, eine Verbindung herzustellen.

Client öffnet den Browser nicht (Verbundauthentifizierung)

Problem

Ich verwende die Verbundauthentifizierung für meinen Client-VPN-Endpunkt. Wenn Clients versuchen, eine Verbindung mit dem Endpunkt herzustellen, öffnet die Client-Software kein Browserfenster, sondern zeigt stattdessen ein Pop-up-Fenster für Benutzername und Passwort an.

Ursache

Die Konfigurationsdatei, die den Clients zur Verfügung gestellt wurde, enthält das `auth-federate`-Flag nicht.

Lösung

Exportieren Sie die neueste Konfigurationsdatei , importieren Sie sie in den von AWS bereitgestellten Client und versuchen Sie erneut, eine Verbindung herzustellen.

Client gibt einen Fehler zurück, der besagt, dass keine Ports verfügbar sind (Verbundauthentifizierung)

Problem

Ich verwende die Verbundauthentifizierung für meinen Client-VPN-Endpunkt. Wenn Clients versuchen, eine Verbindung mit dem Endpunkt herzustellen, gibt die Client-Software den folgenden Fehler zurück:

```
The authentication flow could not be initiated. There are no available ports.
```

Ursache

Der AWS von bereitgestellte Client erfordert die Verwendung von TCP-Port 35001, um die Authentifizierung abzuschließen. Weitere Informationen finden Sie unter Anforderungen und Überlegungen für die SAML-basierte Verbundauthentifizierung.

Lösung

Vergewissern Sie sich, dass das Client-Gerät den TCP-Port 35001 nicht blockiert oder für einen anderen Prozess verwendet.

VPN-Verbindung aufgrund von IP-Nichtübereinstimmung beendet

Problem

Die VPN-Verbindung wurde beendet und die Client-Software gibt den folgenden Fehler zurück: `"The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."`

Ursache

Der AWS von bereitgestellte Client erfordert, dass die IP-Adresse, mit der er verbunden ist, mit der IP des VPN-Servers übereinstimmt, der den Client-VPN-Endpunkt unterstützt. Weitere Informationen finden Sie unter Regeln und bewährte Verfahren von AWS Client VPN.

Lösung

Stellen Sie sicher, dass zwischen dem von AWS bereitgestellten Client und dem Client-VPN-Endpunkt kein DNS-Proxy vorhanden ist.

Weiterleiten von Datenverkehr an LAN funktioniert nicht wie erwartet

Problem

Der Versuch, den Datenverkehr nicht wie erwartet an das lokale Netzwerk (LAN) weiterzuleiten, wenn sich die LAN-IP-Adressbereiche nicht innerhalb der folgenden privaten Standard-IP-Adressbereiche befinden: `10.0.0.0/8`, `172.16.0.0/12192.168.0.0/16`, oder `169.254.0.0/16`.

Ursache

Wenn festgestellt wird, dass der Client-LAN-Adressbereich außerhalb des oben genannten Standardbereichs liegt, überträgt der Client-VPN-Endpunkt automatisch die OpenVPN-Richtlinie „redirect-gateway block-local“ an den Client und erzwingt den gesamten LAN-Datenverkehr in das VPN. Weitere Informationen finden Sie unter Regeln und bewährte Verfahren von AWS Client VPN.

Lösung

Wenn Sie während VPN-Verbindungen LAN-Zugriff benötigen, wird empfohlen, die oben aufgeführten herkömmlichen Adressbereiche für Ihr LAN zu verwenden.

Überprüfen des Bandbreitenlimits für einen Client-VPN-Endpunkt

Problem

Ich muss das Bandbreitenlimit für einen Client-VPN-Endpunkt überprüfen.

Ursache

Der Durchsatz hängt von mehreren Faktoren ab, z. B. von der Kapazität Ihrer Verbindung von Ihrem Standort aus und der Netzwerklatenz zwischen Ihrer Client-VPN-Desktop-Anwendung auf Ihrem Computer und dem VPC-Endpunkt. Es gibt auch ein Bandbreitenlimit von 10 Mbit/s pro Benutzerverbindung.

Lösung

Führen Sie die folgenden Befehle aus, um die Bandbreite zu überprüfen.

```
sudo iperf3 -s -V
```

Auf dem Client:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Dokumentverlauf für das Client-VPN-Benutzerhandbuch

Die folgende Tabelle beschreibt die Aktualisierungen des AWS-Client-VPN-Administratorhandbuchs.

Änderung	Beschreibung	Datum
Beispiele für Autorisierungsregeln	Beispielszenarien für Autorisierungsregeln hinzugefügt.	15. September 2022
Maximale VPN-Sitzungsdauer	Sie können eine kürzere maximale VPN-Sitzungsdauer konfigurieren, um Sicherheits- und Compliance-Anforderungen zu erfüllen.	20. Januar 2022
Client-Anmelde-Banner	Sie können auf AWS ein Textbanner aktivieren, das von Client-VPN-Desktop-Anwendungen zur Verfügung gestellt wird, wenn eine VPN-Sitzung eingerichtet wurde, um gesetzliche und Compliance-Anforderungen zu erfüllen.	20. Januar 2022
Client-Connect-Handler	Sie können den Client-Connect-Handler für Ihren Client VPN-Endpunkt aktivieren, um eine benutzerdefinierte Logik auszuführen, die neue Verbindungen autorisiert.	4. November 2020
Self-Service-Portal	Sie können ein Self-Service-Portal auf Ihrem Client VPN-Endpunkt für Ihre Clients aktivieren.	29. Oktober 2020
Client-zu-Client-Zugriff	Sie können Clients, die eine Verbindung zu einem Client	29. September 2020

	VPN-Endpunkt herstellen, ermöglichen, eine Verbindung miteinander herzustellen.	
SAML 2.0-basierte Verbundauthentifizierung	Sie können Client VPN-Benutzer mithilfe der SAML 2.0-basierten Verbundauthentifizierung authentifizieren.	19. Mai 2020
Festlegen von Sicherheitsgruppen während der Erstellung	Sie können eine VPC und Sicherheitsgruppen angeben, wenn Sie Ihren AWS-Client-VPN-Endpunkt erstellen.	5. März 2020
Konfigurierbare VPN-Ports	Sie können eine unterstützte VPN-Portnummer für Ihren AWS-Client-VPN-Endpunkt angeben.	16. Januar 2020
Unterstützung für Multi-Factor Authentication (MFA)	Ihr AWS-Client-VPN-Endpunkt unterstützt MFA, wenn dies für Ihr Active Directory aktiviert ist.	30. September 2019
Unterstützung für Split-Tunnel	Sie können Split-Tunnel auf Ihrem AWS-Client-VPN-Endpunkt aktivieren.	24. Juli 2019
Erstversion	In dieser Version wird AWS Client VPN eingeführt.	18. Dezember 2018

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.