



Administratorhandbuch

# AWS Client VPN



## AWS Client VPN: Administratorhandbuch

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

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, die Kunden zu verwirren oder Amazon in einer Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

---

# Table of Contents

Was ist AWS Client VPN? .....	1
Funktionen von Client VPN .....	1
Komponenten von Client VPN .....	2
Arbeiten mit Client VPN .....	4
Preise für Client VPN .....	5
Regeln und bewährte Verfahren .....	6
Netzwerk- und Bandbreitenanforderungen .....	6
Subnetz- und VPC-Konfiguration .....	8
Authentifizierung und Sicherheit .....	8
Verbindungs- und DNS-Anforderungen .....	9
Begrenzungen und Einschränkungen .....	9
So funktioniert Client VPN .....	11
Szenarien und Beispiele .....	12
Client-Authentifizierung .....	24
Active Directory-Authentifizierung .....	25
Gegenseitige Authentifizierung .....	25
Single Sign-On (SAML 2.0-basierte Verbundauthentifizierung) .....	32
Client-Autorisierung .....	38
Sicherheitsgruppen .....	38
Netzwerkbasierte Autorisierung .....	39
Erstellen Sie eine Gruppenregel für Endpunktssicherheit .....	39
Verbindungsautorisierung .....	40
Anforderungen und Überlegungen .....	40
Lambda-Schnittstelle .....	41
Verwenden Sie den Client Connect-Handler für die Beurteilung der Körperhaltung .....	43
Aktivieren Sie den Client-Connect-Handler .....	44
Serviceverknüpfte Rolle .....	44
Überwachen Sie Fehler bei der Verbindungsautorisierung .....	44
Split-Tunnel-Client VPN .....	45
Split-Tunnel-Vorteile .....	46
Überlegungen zum Routing .....	46
Split-Tunnel aktivieren .....	47
Verbindungsprotokollierung .....	47
Verbindungsprotokolleinträge .....	47

Überlegungen zur Skalierung .....	49
Erste Schritte mit Client VPN .....	52
Voraussetzungen .....	53
Schritt 1: Erstellen von Server- und Client-Zertifikaten .....	53
Schritt 2: Erstellen eines Client VPN-Endpunkts .....	53
Schritt 3: Zuordnen eines Zielnetzwerks .....	55
Schritt 4: Hinzufügen einer Autorisierungsregel für die VPC .....	56
Schritt 5: Erteilen des Zugriffs auf das Internet .....	57
Schritt 6: Überprüfen der Sicherheitsgruppen-Anforderungen .....	57
Schritt 7: Herunterladen der Konfigurationsdatei für den Client-VPN-Endpunkt .....	58
Schritt 8: Herstellen einer Verbindung zum Client-VPN-Endpunkt .....	59
Arbeiten mit Client VPN .....	60
Zugang zum Self-Service-Portal .....	61
Autorisierungsregeln .....	62
Wichtige Punkte .....	62
Beispiele .....	63
Fügen Sie eine Autorisierungsregel hinzu .....	76
Entfernen Sie eine Autorisierungsregel .....	77
Autorisierungsregeln anzeigen .....	77
Client-Zertifikatsperllisten .....	78
Generieren einer Client-Zertifikatsperlliste .....	79
Importieren einer Client-Zertifikatsperlliste .....	80
Exportieren einer Client-Zertifikatsperlliste .....	81
Client-Verbindungen .....	82
Anzeigen von Client-Verbindungen .....	82
Beenden einer Client-Verbindung .....	83
Banner für die Kundenanmeldung .....	83
Erstellung von Bannern .....	83
Konfigurieren Sie ein Client-Anmeldebanner für einen vorhandenen Endpunkt .....	84
Deaktivieren Sie ein Client-Login-Banner für einen Endpunkt .....	84
Ändern Sie den vorhandenen Bannertext .....	85
Ein aktuell konfiguriertes Login-Banner anzeigen .....	86
Durchsetzung der Client-Route .....	86
Voraussetzungen .....	86
Routing-Konflikte .....	87
Überlegungen .....	88

Aktivieren Sie die Client-Routenerzwingung .....	89
Deaktivieren Sie die Client-Routenerzwingung .....	90
Problembehandlung bei der Durchsetzung von IPv6 Client-Routen .....	90
Endpunkte .....	91
Anforderungen für die Erstellung von Client-VPN-Endpunkten .....	92
IP-Adresstypen .....	92
Änderung des Endpunkts .....	93
Endpunkt herstellen .....	95
-Endpunkte anzeigen .....	100
Ändern Sie einen Endpunkt .....	101
Löschen eines Endpunkts .....	104
Verbindungsprotokolle .....	104
Aktivieren der Verbindungsprotokollierung für einen neuen -Endpunkt .....	105
Verbindungsprotokollierung für einen vorhandenen -Endpunkt aktivieren .....	106
Verbindungsprotokolle anzeigen .....	107
Deaktivieren der Verbindungsprotokollierung .....	108
Export der Client-Konfigurationsdatei .....	108
Exportieren der Client-Konfigurationsdatei .....	109
Fügen Sie das Client-Zertifikat und die Schlüsselinformationen für die gegenseitige Authentifizierung hinzu .....	110
Routen .....	111
Überlegungen zur Verwendung von Split-Tunnel auf Client-VPN-Endpunkten .....	112
Endpunkt-Route erstellen .....	112
Anzeigen von Endpunkttroutes .....	113
Löschen einer Endpunktroute .....	114
Zielnetzwerke .....	114
Anforderungen für die Erstellung eines Zielnetzwerks .....	114
Ordnen Sie ein Zielnetzwerk einem Endpunkt zu .....	116
Anwenden einer Sicherheitsgruppe auf ein Zielnetzwerk .....	116
Anzeigen von Zielnetzwerken .....	117
Trennen Sie die Zuordnung eines Zielnetzwerks zu einem Endpunkt .....	118
Maximale Dauer der VPN-Sitzung .....	118
Konfigurieren Sie die maximale VPN-Sitzung bei der Erstellung eines Endpunkts .....	119
Anzeigen der maximalen VPN-Sitzungsdauer .....	119
Ändern Sie die maximale Dauer der VPN-Sitzung .....	120
Sicherheit .....	121

Datenschutz .....	122
Verschlüsselung während der Übertragung .....	123
Richtlinie für den Datenverkehr zwischen Netzwerken .....	123
Identitäts- und Zugriffsverwaltung .....	124
Zielgruppe .....	124
Authentifizierung mit Identitäten .....	125
Verwalten des Zugriffs mit Richtlinien .....	129
Wie AWS Client VPN funktioniert mit IAM .....	132
Beispiele für identitätsbasierte Richtlinien .....	138
Fehlersuche .....	141
Verwenden von serviceverknüpften Rollen .....	143
Ausfallsicherheit .....	147
Mehrere Zielnetzwerke für hohe Verfügbarkeit .....	147
Sicherheit der Infrastruktur .....	147
Bewährte Methoden .....	148
IPv6 Überlegungen .....	149
Die wichtigsten Komponenten des Supports IPv6 .....	149
IPv6 CIDR-Zuweisung an den Client .....	149
Anforderungen an die Kompatibilität .....	150
DNS-Support .....	150
Einschränkungen .....	150
Durchsetzung von Client-Routes für IPv6 .....	150
IPv6 Vermeidung von Leckagen (ältere Informationen) .....	151
Überwachen des Client VPN .....	153
CloudWatch Metriken .....	154
CloudWatch Metriken anzeigen .....	156
Kontingente .....	158
Client VPN-Kontingente .....	158
Kontingente für Benutzer und Gruppen .....	159
Allgemeine Überlegungen .....	160
Fehlerbehebung .....	161
Der DNS-Name des Client-VPN-Endpunkts konnte nicht aufgelöst werden .....	162
Der Datenverkehr wird nicht zwischen Subnetzen aufgeteilt .....	162
Autorisierungsregeln für Active Directory-Gruppen, die nicht wie erwartet funktionieren .....	164
Clients können nicht auf eine Peered-VPC, Amazon S3 oder das Internet zugreifen .....	165

Der Zugriff auf eine Peer-VPC, Amazon S3 oder das Internet erfolgt nur mit Unterbrechungen .....	168
Client-Software gibt TLS-Fehler zurück .....	169
Die Clientsoftware gibt Fehler in Bezug auf Benutzernamen und Kennwort zurück — Active Directory-Authentifizierung .....	170
Die Clientsoftware gibt Fehler in Bezug auf Benutzername und Passwort zurück — Verbundauthentifizierung .....	171
Clients können keine Verbindung herstellen — gegenseitige Authentifizierung .....	171
Der Client gibt den Fehler „Anmeldedaten überschreiten die maximale Größe“ zurück — Verbundauthentifizierung .....	172
Der Client öffnet den Browser nicht — Verbundauthentifizierung .....	172
Der Client gibt den Fehler „Keine verfügbaren Ports“ zurück — Verbundauthentifizierung .....	173
Die VPN-Verbindung wurde aufgrund einer IP-Nichtübereinstimmung beendet .....	173
Das Routing des Datenverkehrs zum LAN funktioniert nicht wie erwartet .....	174
Überprüfen Sie das Bandbreitenlimit für einen Endpunkt .....	174
Client-VPN-Tunnelkonnektivität .....	175
Voraussetzungen für die Netzwerkkonnektivität .....	176
Überprüfen Sie den Status Client VPN Client-VPN-Endpunkts .....	176
Überprüfen Sie die Client-Verbindungen .....	176
Überprüfen Sie die Client-Authentifizierung .....	177
Überprüfen Sie die Autorisierungsregeln .....	177
Client-VPN-Routen validieren .....	178
Überprüfen Sie die Sicherheitsgruppen und das Netzwerk ACLs .....	178
Testen Sie die Client-Konnektivität .....	179
Diagnostizieren Sie das Client-Gerät .....	179
Problembehandlung bei der DNS-Auflösung .....	180
Probleme mit der Leistung beheben .....	180
Client-VPN-Metriken überwachen .....	181
Überprüfen Sie die Client-VPN-Protokolle .....	181
Häufige Probleme und Lösungen .....	182
Dokumentverlauf .....	184

# 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.

## Themen

- [Funktionen von Client VPN](#)
- [Komponenten von Client VPN](#)
- [Arbeiten mit Client VPN](#)
- [Preise für Client VPN](#)
- [Regeln und bewährte Verfahren für die Verwendung AWS Client VPN](#)

## Funktionen von Client VPN

Client VPN bietet die folgenden Merkmale und Funktionen:

- Sichere Verbindungen — Stellt über den OpenVPN-Client von jedem Standort aus verschlüsselte TLS-Verbindungen her und gewährleistet so Datenschutz und Integrität.
- Managed Service — Eliminiert den betrieblichen Aufwand für die Bereitstellung und Wartung von VPN-Lösungen für den Fernzugriff von Drittanbietern durch ein vollständiges AWS-Management.
- Hohe Verfügbarkeit und Elastizität — Dynamische Skalierung für eine unterschiedliche Anzahl von Benutzern, die sich ohne manuelles Eingreifen mit Ihren AWS- und lokalen Ressourcen verbinden.
- Authentifizierung — Unterstützt mehrere Authentifizierungsmethoden, darunter Active Directory-Integration, Verbundauthentifizierung und zertifikatsbasierte Authentifizierung für flexibles Identitätsmanagement.
- Granulare Steuerung — Implementiert präzise Sicherheitskontrollen durch netzwerkbasierte Zugriffsregeln, die auf Active Directory-Gruppenebene konfiguriert werden können, und durch sicherheitsgruppenbasierte Zugriffskontrolle.
- Benutzerfreundlichkeit — Bietet einen einheitlichen Zugriff auf AWS- und lokale Ressourcen über einen einzigen VPN-Tunnel und vereinfacht so die Endbenutzererfahrung.

- Verwaltbarkeit — Bietet umfassende Transparenz durch detaillierte Verbindungsprotokolle und Verwaltungsfunktionen in Echtzeit, einschließlich der Möglichkeit, aktive Client-Verbindungen bei Bedarf zu überwachen und zu beenden.
- Umfassende Integration — Lässt sich nahtlos in bestehende AWS-Services, einschließlich Amazon VPC, integrieren AWS Directory Service und verbessert so die Konnektivitätsmöglichkeiten Ihrer Cloud-Infrastruktur.
- IPv6 Unterstützung — Ermöglicht vollständige IPv6 Konnektivität für Client-VPN-Endpunkte und unterstützt Verbindungen zu IPv6 Ressourcen in Ihren VPCs und von Clients in IPv6 Netzwerken für moderne Netzwerkanforderungen.

## 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 Zielnetzwerk Routen 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. Für IPv4 den Datenverkehr wählen Sie den CIDR-Bereich des Clients, zum Beispiel. `10.2.0.0/16` Weist dem IPv6 Verkehr AWS Client VPN automatisch den CIDR-Bereich des Clients zu.

### 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. Für IPv4 den Datenverkehr wird die Quell-Netzwerkadressübersetzung (SNAT) angewendet, bei der die Quell-IP-Adresse aus dem CIDR-Bereich des Clients in die IP-Adresse der Client-VPN-Netzwerkschnittstelle übersetzt wird. Für IPv6 den Datenverkehr wird SNAT nicht angewendet, sodass die IP-Adresse des verbundenen Benutzers besser einsehbar ist.

### 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-Endpoint-Administrator kann ein Self-Service-Portal für den Client-VPN-Endpoint 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 (US-West).

#### Art der Endpunkt-IP-Adresse

Der IP-Adressstyp für den Client-VPN-Endpoint, bei dem es sich um IPv4 IPv6, oder Dual-Stack ( IPv4 sowohl als auch IPv6) handeln kann.

#### Typ der IP-Adresse für den Verkehr

Der IP-Adressstyp für den Datenverkehr, der über den Client-VPN-Endpoint fließt. Dabei kann es sich um IPv4 IPv6, oder Dual-Stack ( IPv4 sowohl als auch IPv6) handeln. Dadurch werden die Art des internen Datenverkehrs (die tatsächliche Nutzlast oder der ursprüngliche Datenverkehr, der durch die VPN-Verbindung getunnelt wird), die CIDR-Bereiche der Clients, die Subnetzuweisung, die Routen und die Regeln pro Endpunkt bestimmt.

## Arbeiten mit Client VPN

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

#### AWS-Managementkonsole

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 das öffentliche 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 im [EC2 Abschnitt](#) der Amazon EC2 Command Line Reference.

#### 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. Für die Nutzung IPv6 von Dual-Stack-Endpunkten fallen keine zusätzlichen Kosten an. Sie werden zum gleichen Preis wie Endgeräte berechnet. IPv4 Weitere Informationen finden Sie unter [AWS Client VPN Preise](#).

Die Datenübertragung von Amazon ins Internet wird Ihnen EC2 in Rechnung gestellt. Weitere Informationen finden Sie unter [Datenübertragung](#) auf der Seite mit den EC2 Amazon-On-Demand-Preisen.

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 elastischen Client-VPN-Netzwerkschnittstellen (ENIs). 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.

### Note

Client-VPN-Endpoints benötigen Elastic IP-Adressen, wenn sie mit einem VPC-Subnetz verknüpft sind, das über ein Internet Gateway verfügt, da diese eine direkte Internetverbindung für VPN-Clients EIPs ermöglichen. Wenn sie eine Verbindung über einen Client-VPN-Endpunkt herstellen, benötigen sie eine öffentliche IP-Adresse, um mit Internetressourcen zu kommunizieren. Elastic erfüllt diesen IPs Zweck, indem es einen konsistenten, öffentlich zugänglichen Endpunkt bereitstellt. Diese EIPs sind an die elastischen Client-VPN-Netzwerkschnittstellen (ENIs) angeschlossen und sind für die Aufrechterhaltung eines stabilen, sicheren Internetzugangs für VPN-Clients bei gleichzeitiger ordnungsgemäßer Weiterleitung des Datenverkehrs unerlässlich. Da diese Elastic IP-Adressen für den Client-VPN-Dienst zugewiesen und aktiv genutzt werden, werden sie AWS entsprechend ihrem Standardpreismodell für zugewiesene und zugeordnete IPv4 IP-Adressen als genutzte öffentliche Adressen berechnet. EIPs

## Regeln und bewährte Verfahren für die Verwendung AWS Client VPN

In den folgenden Abschnitten werden die Regeln und bewährten Methoden für die Verwendung von beschrieben AWS Client VPN:

### Themen

- [Netzwerk- und Bandbreitenanforderungen](#)
- [Subnetz- und VPC-Konfiguration](#)
- [Authentifizierung und Sicherheit](#)
- [Verbindungs- und DNS-Anforderungen](#)
- [Begrenzungen und Einschränkungen](#)

### Netzwerk- und Bandbreitenanforderungen

- AWS Client VPN ist ein vollständig verwalteter Dienst, der automatisch skaliert wird, um zusätzlichen Benutzerverbindungen und Bandbreitenanforderungen gerecht zu werden. Jede Benutzerverbindung hat eine maximale Basisbandbreite von 50 Mbit/s.

Die tatsächliche Bandbreite, mit der Sie eine Verbindung über einen Client-VPN-Endpunkt herstellen, kann aufgrund verschiedener Faktoren variieren. Zu diesen Faktoren gehören die Paketgröße, die Zusammensetzung des Datenverkehrs (TCP/UDP-Mix), Netzwerkrichtlinien (Shaping oder Drosselung) in Zwischennetzwerken, Internetbedingungen, anwendungsspezifische Anforderungen und die Gesamtzahl der gleichzeitigen Benutzerverbindungen. Wenn Sie das maximale Bandbreitenlimit erreichen, können Sie über den AWS-Support eine Erhöhung beantragen.

- 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.
- Client VPN unterstützt IPv4 Dual-Stack-Verkehr (IPv4 sowohl als auch IPv6). IPv6 Weitere Informationen zur IPv6 Unterstützung finden Sie unter [IPv6 Überlegungen für AWS Client VPN](#).
- Die Quell-IP-Adresse wird in die IP-Adresse des Client-VPN-Endpunkts übersetzt.
  - Die ursprüngliche Quellportnummer des Clients bleibt unverändert.
- Client VPN führt Port Address Translation (PAT) nur durch, wenn gleichzeitig Benutzer eine Verbindung zu demselben Ziel herstellen. Die Portübersetzung erfolgt automatisch und ist notwendig, um mehrere gleichzeitige Verbindungen über denselben VPN-Endpunkt zu unterstützen.
  - Bei der Quell-IP-Übersetzung wird die Quell-IP-Adresse in die IP-Adresse des Client-VPN übersetzt.
  - Bei der Quell-Port-Übersetzung für einzelne Client-Verbindungen bleibt die ursprüngliche Quellportnummer möglicherweise unverändert.
  - Bei der Quellportübersetzung für mehrere Clients, die sich mit demselben Ziel verbinden (dieselbe Ziel-IP-Adresse und denselben Port), führt Client VPN eine Portübersetzung durch, um eindeutige Verbindungen sicherzustellen.

Wenn beispielsweise zwei Clients, Client 1 und Client 2, über einen Client-VPN-Endpunkt eine Verbindung zu demselben Zielserver und Port herstellen:

- Der ursprüngliche Port für Client 1 — zum Beispiel 9999 — könnte in einen anderen Port übersetzt werden, beispielsweise Port4306.
- Der ursprüngliche Port für Client 2 — zum Beispiel 9999 — könnte in einen eindeutigen Port übersetzt werden, der sich von Client 1 unterscheidet — zum Beispiel Port63922.
- Für IPv6 den Datenverkehr führt Client VPN keine Network Address Translation (NAT) durch. Dies bietet einen besseren Einblick in die IPv6 Adresse des verbundenen Benutzers.

## Subnetz- und VPC-Konfiguration

- 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 Subnetzuordnungen in einer Dedicated Tenancy-VPC.
- Für IPv6 Dual-Stack-Verkehr müssen die zugehörigen Subnetze CIDR-Bereiche IPv6 oder Dual-Stack-CIDR-Bereiche haben.
- Bei Dual-Stack-Endpunkten können Sie nicht mehr als ein Subnetz pro Availability Zone zuordnen.

## Authentifizierung und Sicherheit

- Das Self-Service-Portal ist nicht für Clients verfügbar, die sich mittels gegenseitiger Authentifizierung authentifizieren.
- 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*

- In AWS Client VPN verwendete Zertifikate müssen [RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile](#) entsprechen, einschließlich der in Abschnitt 4.2 des Memos angegebenen Zertifikatserweiterungen.
- Benutzernamen mit Sonderzeichen können Verbindungsfehler verursachen.

## Verbindungs- und DNS-Anforderungen

- 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.
- 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](#)
- Sie können einen AWS bereitgestellten Client verwenden, um eine Verbindung zu mehreren gleichzeitigen DNS-Sitzungen herzustellen. Damit die Namensauflösung jedoch ordnungsgemäß funktioniert, sollten die DNS-Server aller Verbindungen über synchronisierte Datensätze verfügen.
- 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](#)
- Wenn in Windows ein Full-Tunnel-Endpunkt verwendet wird, wird der gesamte DNS-Verkehr durch den Tunnel gezwungen, unabhängig vom IP-Adressstyp (IPv4 IPv6 oder Dual-Stack) des Endpunkts. Damit DNS funktioniert, muss ein DNS-Server eingerichtet und innerhalb des Tunnels erreichbar sein.

## Begrenzungen und Einschränkungen

- IP-Weiterleitung wird derzeit nicht unterstützt, wenn die AWS Client VPN Desktop-Anwendung verwendet wird. 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.
- Sie können von einem Computer aus keine VPN-Verbindung herstellen, wenn mehrere Benutzer am Betriebssystem angemeldet sind.
- Client-to-client Kommunikation wird für IPv6 Clients nicht unterstützt. Wenn ein IPv6 Client versucht, mit einem anderen IPv6 Client zu kommunizieren, wird der Datenverkehr unterbrochen.
- IPv6 und Dual-Stack-Endpunkte setzen voraus, dass Benutzergeräte und Internetdienstanbieter (ISPs) die entsprechende IP-Konfiguration unterstützen.

# Wie AWS Client VPN funktioniert

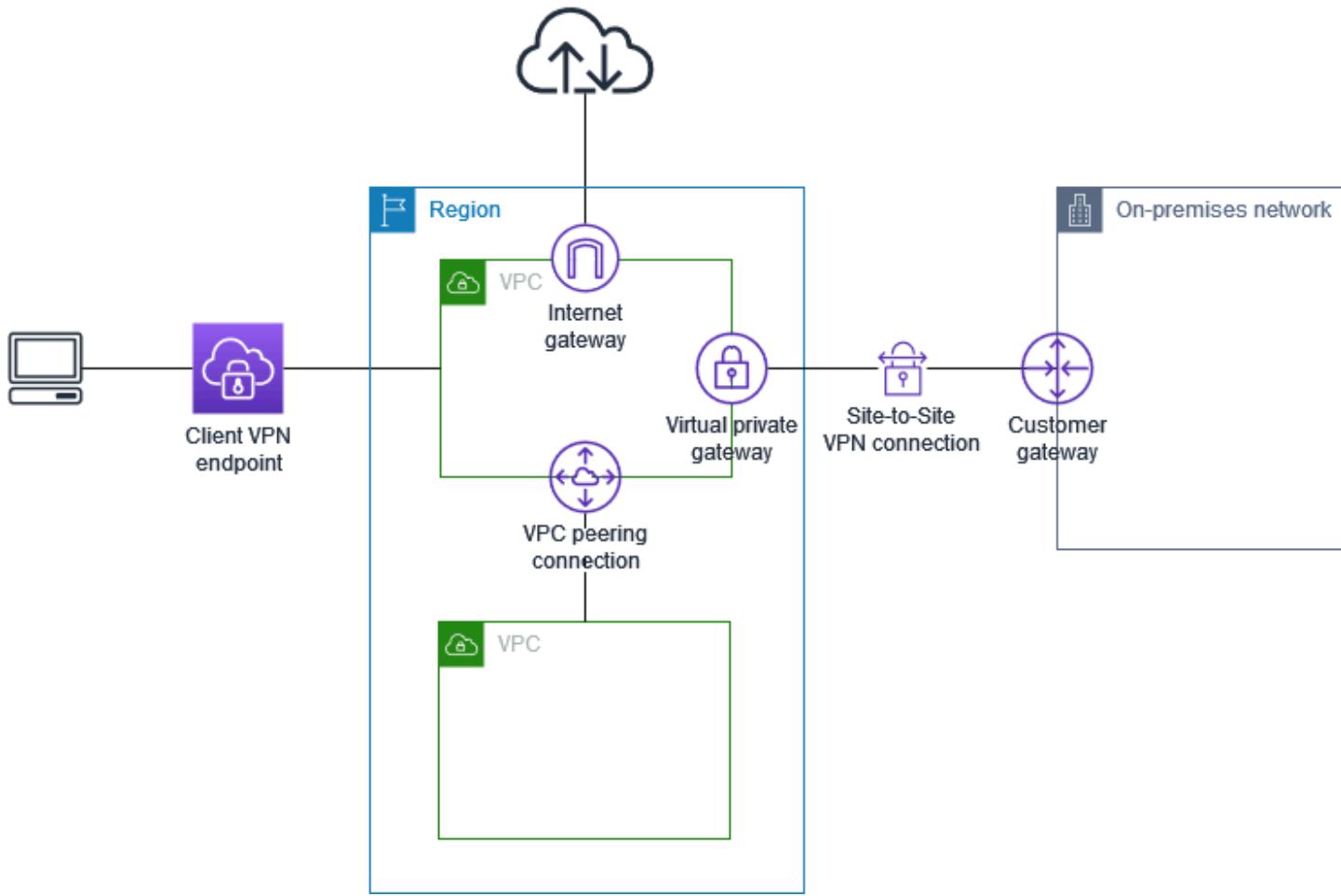
Bei AWS Client VPN gibt es zwei Arten von Benutzerpersönlichkeiten, die mit dem Client-VPN-Endpunkt interagieren: Administratoren und Clients.

Client VPN unterstützt IPv4 IPv6, und Dual-Stack-Konnektivität ( IPv4 sowohl als auch IPv6). Sie können Endpunkte erstellen, die entweder oder beides verwenden IPv4 IPv6, sodass Sie eine Verbindung zu IPv6 Ressourcen in Ihrem Netzwerk herstellen VPCs oder eine Verbindung zu Clients in Netzwerken herstellen können. IPv6 Diese Flexibilität hilft Unternehmen, die bereits eine Infrastruktur implementiert haben oder auf diese umsteigen IPv6 .

Der Administrator ist für das Einrichten und Konfigurieren des Service verantwortlich. Dazu gehört die Erstellung des Client-VPN-Endpunkts, die Zuordnung des Zielnetzwerks, die Konfiguration der Autorisierungsregeln und die Einrichtung zusätzlicher 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 Konfigurationsdatei für den Client-VPN-Endpunkt enthält den DNS-Namen des Client-VPN-Endpunkts und Authentifizierungsinformationen, die für die Einrichtung einer VPN-Sitzung erforderlich sind. Weitere Informationen zum Festlegen des Service finden Sie unter [Fangen Sie an 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 einem lokalen Netzwerk oder auf andere Clients zugreifen, wenn die erforderlichen Routen- und Autorisierungsregeln konfiguriert wurden. Weitere Informationen zum Herstellen einer Verbindung mit einem Client-VPN-Endpunkt, um eine VPN-Sitzung einzurichten, finden Sie unter [Erste Schritte im AWS Client VPN Benutzerhandbuch](#).

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



## Szenarien und Beispiele für Client-VPN

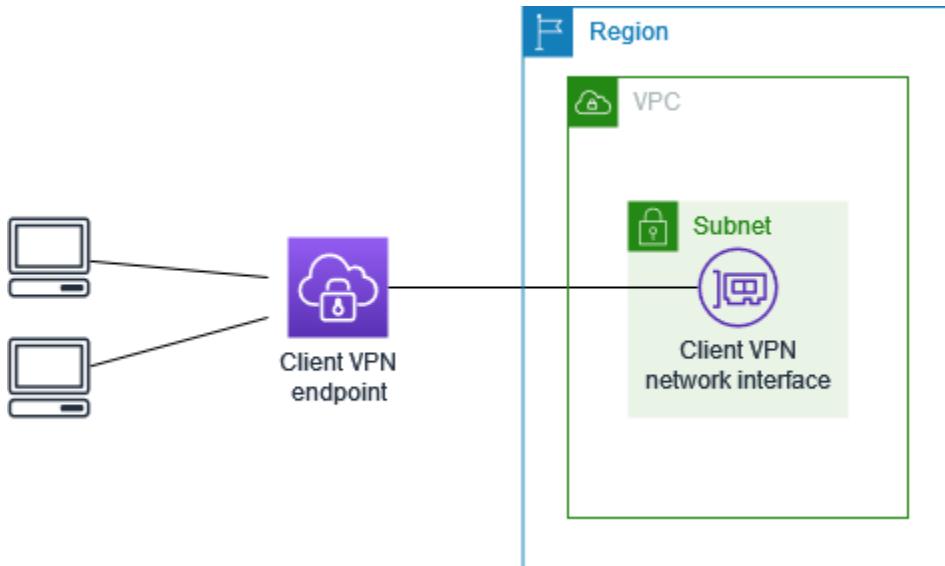
AWS Client VPN ist eine vollständig verwaltete VPN-Lösung für den Fernzugriff, mit der Sie Clients den sicheren Zugriff auf Ressourcen AWS sowohl innerhalb als auch in Ihrem lokalen Netzwerk ermöglichen. Es gibt mehrere Optionen für die Konfiguration des Zugriffs. Dieser Abschnitt enthält Beispiele für das Erstellen und Konfigurieren des Client VPN-Zugriffs für Ihre Clients.

### Szenarien

- [the section called “Auf eine VPC zugreifen”](#)
- [the section called “Auf eine per Peering verbundene VPC zugreifen”](#)
- [the section called “Auf ein On-Premise-Netzwerk zugreifen”](#)
- [the section called “Zugriff auf das Internet”](#)
- [the section called “Client-to-client-Zugriff”](#)
- [the section called “Den Zugriff auf Ihr Netzwerk einschränken”](#)

## Mit Client-VPN auf eine VPC zugreifen

Die AWS Client VPN Konfiguration für dieses Szenario umfasst eine einzelne 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 für die Verwendung 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 zu [Einen AWS Client VPN Endpunkt erstellen](#).
2. Verknüpfen Sie das Subnetz mit dem Client VPN-Endpunkt. Führen Sie dazu die unter [Verknüpfen Sie ein Zielnetzwerk mit einem AWS Client VPN Endpunkt](#) beschriebenen Schritte aus und wählen Sie das Subnetz und die VPC aus, die Sie zuvor identifiziert haben.

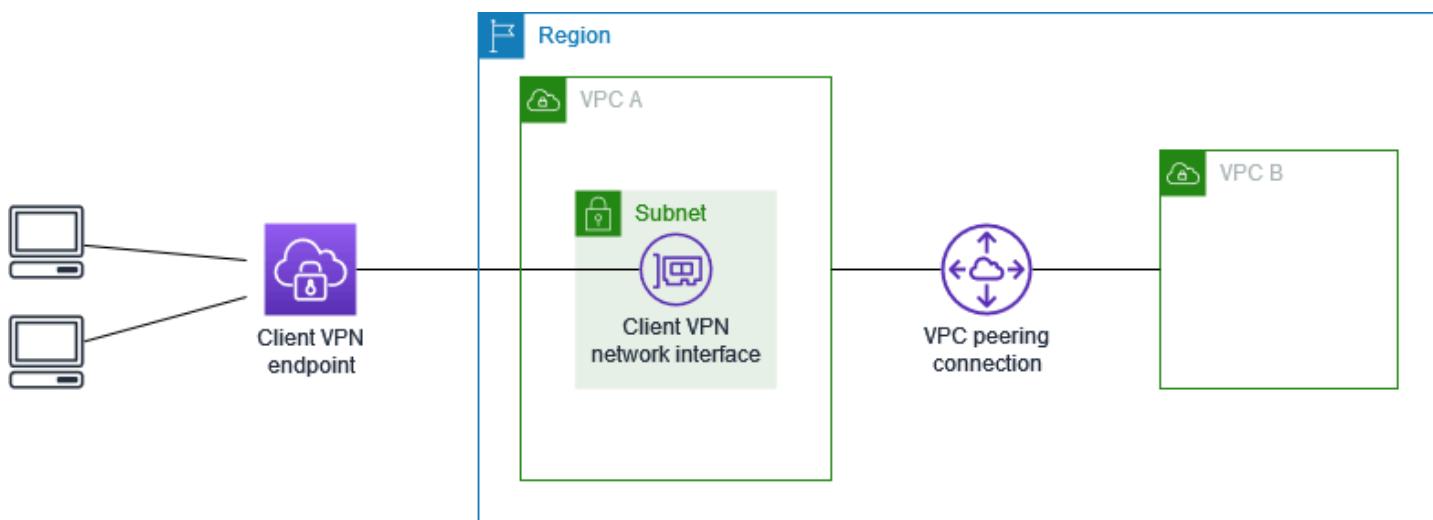
3. Fügen Sie eine Autorisierungsregel hinzu, um Clients den Zugriff auf die VPC zu gewähren. Führen Sie dazu die unter beschriebenen Schritte aus und geben Sie für Zielnetzwerk den IPv4 CIDR-Bereich der VPC ein. [Fügen Sie eine Autorisierungsregel hinzu](#)
4. Fügen Sie den Sicherheitsgruppen Ihrer Ressourcen 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 Client-VPN auf eine per Peering verbundene VPC zugreifen

Die AWS Client VPN Konfiguration für dieses Szenario umfasst eine Ziel-VPC (VPC A), die mit einer zusätzlichen VPC (VPC B) gepeert wird. Wir empfehlen diese Konfiguration, wenn Sie Clients Zugriff auf die Ressourcen innerhalb einer Ziel-VPC und auf andere Ressourcen gewähren müssen VPCs , die mit ihr gepeert werden (z. B. VPC B).

### Note

Das Verfahren zum Zulassen des Zugriffs auf eine Peering-VPC (wie im Netzwerkdigramm beschrieben) ist nur erforderlich, wenn der Client-VPN-Endpunkt für den Split-Tunnel-Modus 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 für die Verwendung AWS Client VPN](#).

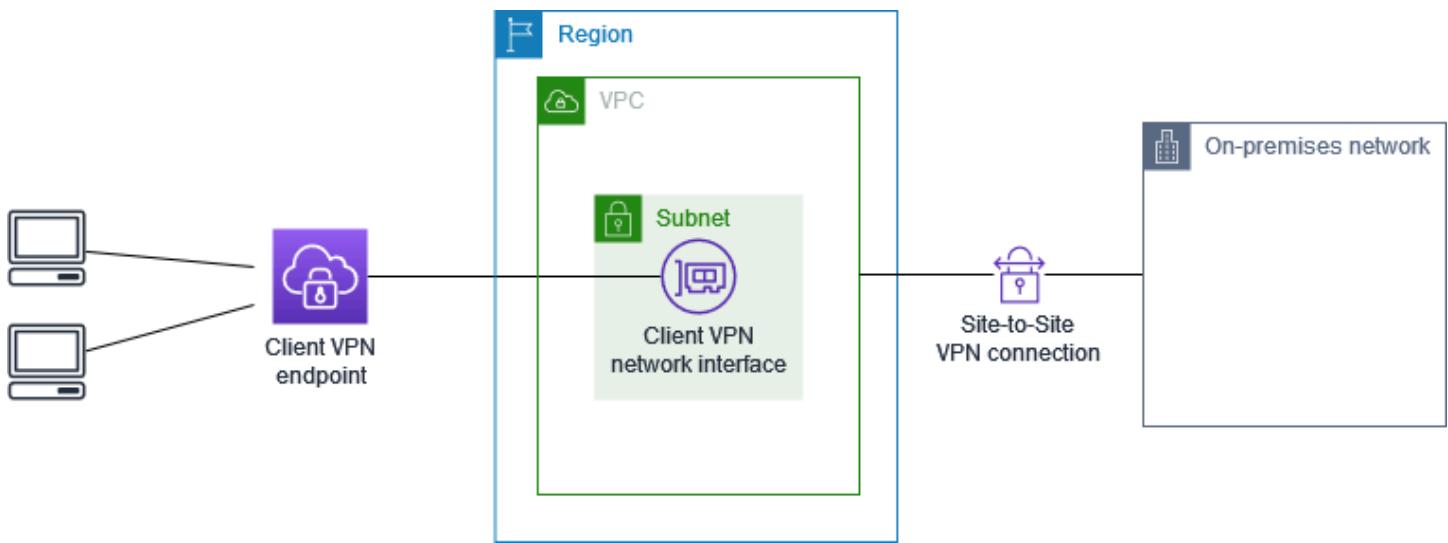
So implementieren Sie diese Konfiguration

1. Stellen Sie die VPC-Peering-Verbindung zwischen den her. VPCs 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 [Einen AWS Client VPN Endpunkt erstellen](#) beschriebenen Schritte aus.
3. Ordnen Sie das identifizierte Subnetz dem Client-VPN-Endpunkt zu, den Sie erstellt haben. Führen Sie dazu die unter [Verknüpfen Sie ein Zielnetzwerk mit einem AWS 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 [Fügen Sie eine Autorisierungsregel hinzu](#). Geben Sie für die Aktivierung des Zielnetzwerks 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 [Erstellen Sie eine AWS Client VPN Endpunktroute](#) beschriebenen Schritte aus. Geben Sie als Routenziele den IPv4 CIDR-Bereich der Peering-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 [Fügen Sie eine Autorisierungsregel hinzu](#). Geben Sie für Zielnetzwerk den IPv4 CIDR-Bereich der Peering-VPC ein.

- 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 Client VPN auf ein On-Premises-Netzwerk zugreifen

Die AWS Client VPN Konfiguration für dieses Szenario beinhaltet nur den Zugriff auf ein lokales Netzwerk. 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 für die Verwendung AWS Client VPN](#).

So implementieren Sie diese Konfiguration

- Ermöglichen Sie die Kommunikation zwischen der VPC und Ihrem eigenen lokalen 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**

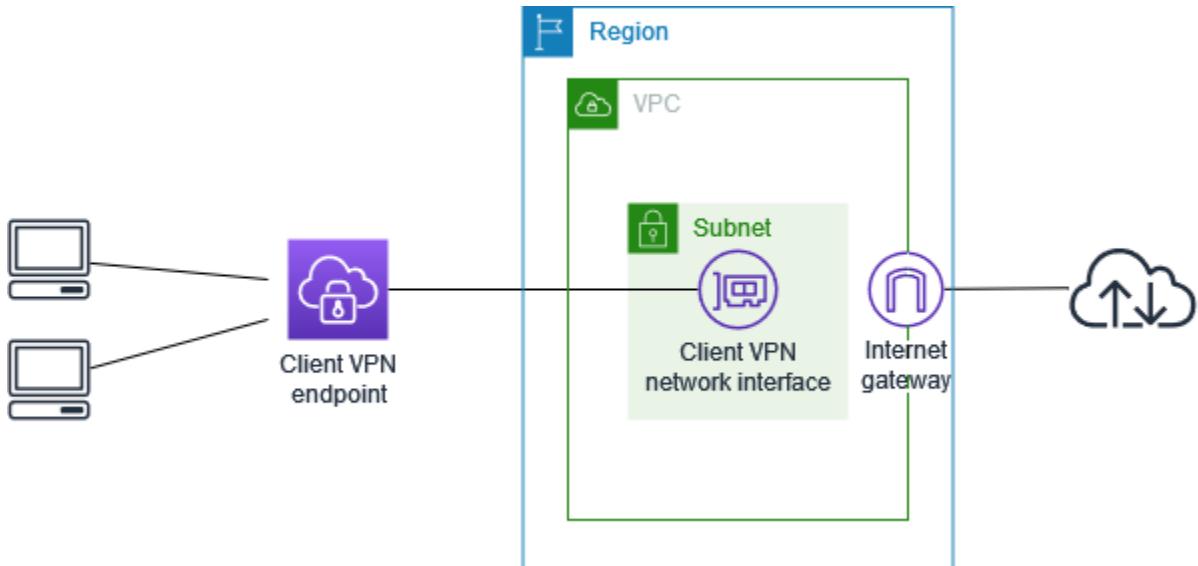
Alternativ können Sie dieses Szenario implementieren, indem Sie eine Direct Connect Verbindung zwischen Ihrer VPC und Ihrem lokalen Netzwerk verwenden. Weitere Informationen finden Sie im [Direct Connect -Benutzerhandbuch](#).

2. Testen Sie die AWS Site-to-Site VPN-Verbindung, die Sie im vorherigen Schritt erstellt haben. Führen Sie dazu die im AWS Site-to-Site VPN Benutzerhandbuch unter [Testen der Site-to-Site VPN-Verbindung](#) 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 [Einen AWS Client VPN Endpunkt erstellen](#).
4. Verknüpfen Sie das Subnetz, das Sie zuvor mit dem Client VPN-Endpunkt identifiziert haben. Führen Sie dazu die unter [Verknüpfen Sie ein Zielnetzwerk mit einem AWS 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 beschriebenen Schritte aus[Erstellen Sie eine AWS Client VPN Endpunktroute](#); geben Sie für Route destination den IPv4 CIDR-Bereich der AWS Site-to-Site VPN-Verbindung ein und wählen Sie für Target VPC Subnet ID das Subnetz aus, das Sie dem Client-VPN-Endpunkt zugeordnet haben.
6. Fügen Sie eine Autorisierungsregel hinzu, um Clients Zugriff auf die VPN-Verbindung zu gewähren. AWS Site-to-Site Führen Sie dazu die unter beschriebenen Schritte aus[Eine Autorisierungsregel zu einem AWS Client VPN Endpunkt hinzufügen](#); geben Sie für Zielnetzwerk den IPv4 CIDR-Bereich der AWS Site-to-Site VPN-Verbindung ein.

## Mithilfe eines Client VPN auf das Internet zugreifen

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

Wenn Sie das [Fangen Sie an 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 für die Verwendung AWS Client VPN](#).

So implementieren Sie diese Konfiguration

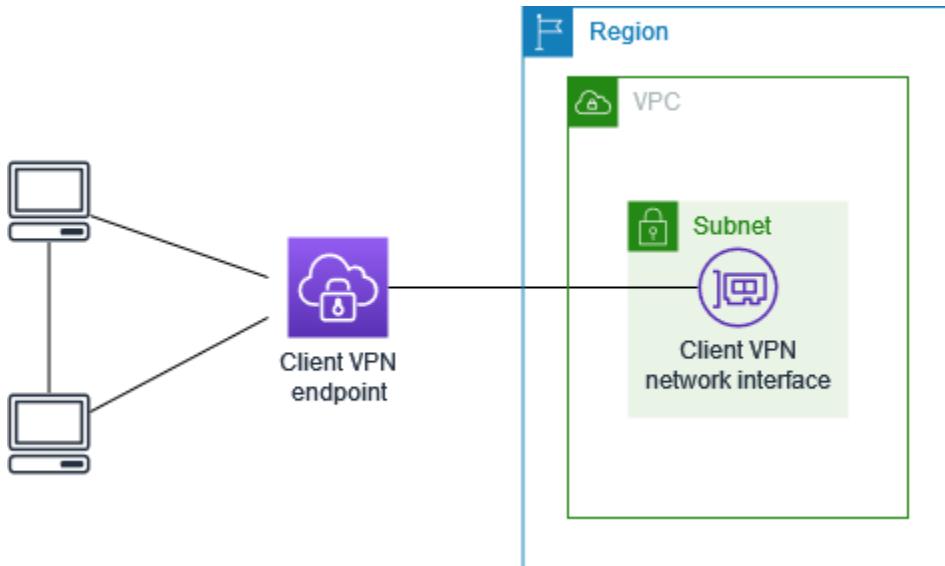
1. Stellen Sie sicher, dass die Sicherheitsgruppe, die Sie für den Client-VPN-Endpunkt verwenden werden, ausgehenden Datenverkehr zum Internet zulässt. Fügen Sie hierfür Regeln für ausgehenden Datenverkehr hinzu, die Datenverkehr zu 0.0.0.0/0 für HTTP- und HTTPS-Datenverkehr zulassen.
2. Erstellen Sie 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 [Einen AWS Client VPN Endpunkt erstellen](#).
5. Verknüpfen Sie das Subnetz, das Sie zuvor mit dem Client VPN-Endpunkt identifiziert haben. Führen Sie dazu die unter [Verknüpfen Sie ein Zielnetzwerk mit einem AWS 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 beschriebenen Schritte aus und geben Sie für Destination network to enable den IPv4 CIDR-Bereich der VPC ein. [Fügen Sie eine Autorisierungsregel hinzu](#)
7. Fügen Sie eine Route hinzu, die den Datenverkehr mit dem Internet ermöglicht. Führen Sie dazu die unter [Erstellen Sie eine AWS Client VPN Endpunktroute](#) 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 [Fügen Sie eine Autorisierungsregel hinzu](#) 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.

## Client-to-client Zugriff über Client VPN

Die AWS Client VPN Konfiguration für dieses Szenario ermöglicht Clients den Zugriff auf eine einzelne VPC und ermöglicht es den Clients, den Datenverkehr untereinander weiterzuleiten. 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 für die Verwendung 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 zu [Einen AWS Client VPN Endpunkt erstellen](#).
2. Verknüpfen Sie das Subnetz, das Sie zuvor mit dem Client VPN-Endpunkt identifiziert haben. Führen Sie dazu die unter [Verknüpfen Sie ein Zielnetzwerk mit einem AWS 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 [Erstellen Sie eine AWS Client VPN Endpunktroute](#). Geben Sie als Routenziele 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 [Fügen Sie eine Autorisierungsregel hinzu](#). Geben Sie für die Aktivierung des Zielnetzwerks 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 [Fügen Sie eine Autorisierungsregel hinzu](#). Geben Sie als Zielnetzwerk den CIDR-Bereich des Clients ein.

## Den Zugriff auf Ihr Netzwerk mit Client VPN beschränken

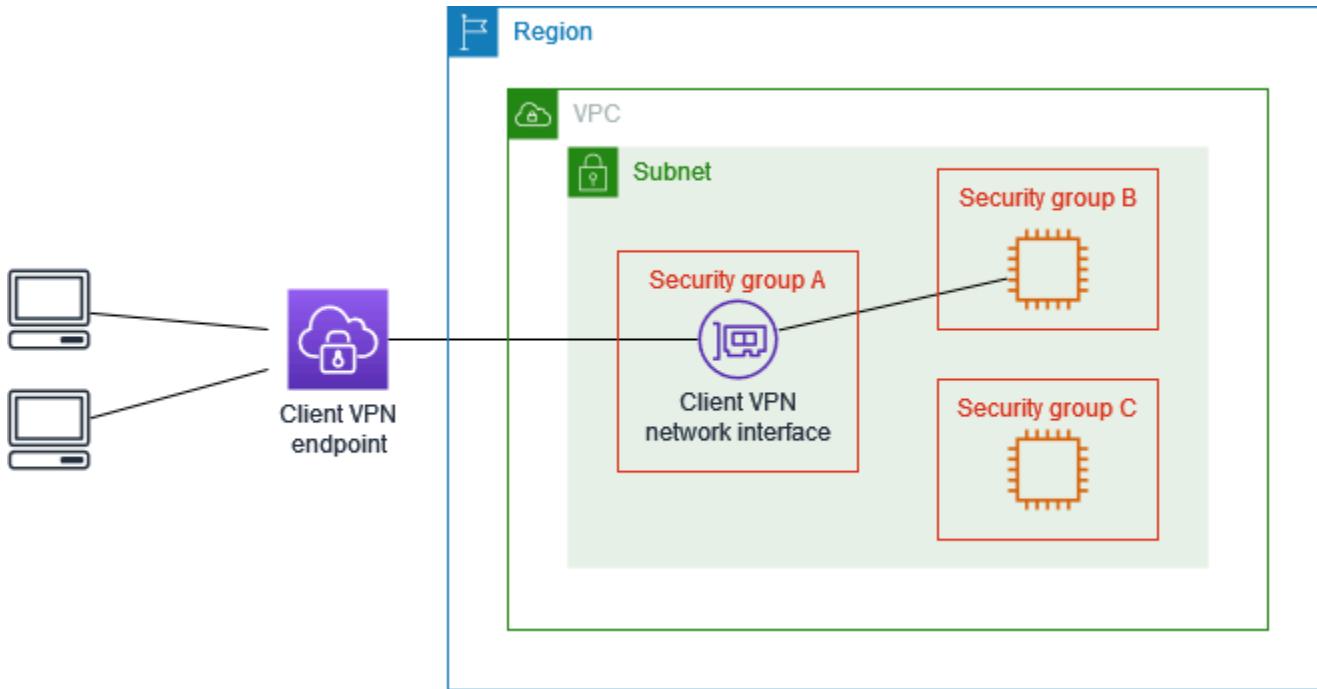
Sie können Ihren AWS Client VPN Endpunkt so konfigurieren, dass der Zugriff auf bestimmte Ressourcen in Ihrer VPC eingeschränkt wird. Für die benutzerbasierte Authentifizierung können Sie auch den Zugriff auf Teile des Netzwerks basierend auf der Benutzergruppe, die auf den Client VPN-Endpunkt zugreift, 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 Szenario [Mit 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 Instanz zugeordnet und Sicherheitsgruppe C ist einer EC2 Instanz 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 Directory Service oder Ihrem IdP. Weitere Informationen finden Sie unter den folgenden Themen:
  - [Active Directory-Authentifizierung im Client VPN](#)
  - [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 [AWS Client VPN 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 in AWS Client VPN](#).
2. Erstellen Sie einen Client VPN-Endpunkt. Weitere Informationen finden Sie unter [Einen AWS Client VPN Endpunkt erstellen](#).
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 [Fügen Sie eine Autorisierungsregel hinzu](#).

## Client-Authentifizierung in AWS Client VPN

Die Client-Authentifizierung 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 genannten Methoden alleine 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 in AWS Client VPN](#).

- Wenn Sie eine Kombination aus gegenseitiger Authentifizierung und benutzerbasierter Authentifizierung verwenden, müssen beide Methoden verwendet werden, um sich im VPN korrekt zu authentifizieren.

## Active Directory-Authentifizierung im Client VPN

Client VPN bietet Active Directory-Unterstützung durch Integration mit Directory Service. Mit der Active Directory-Authentifizierung werden Clients anhand vorhandener Active Directory-Gruppen identifiziert. Mithilfe von Directory Service Client VPN kann eine Verbindung zu vorhandenen Active Directories 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 in AWS Client VPN

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.

In AWS Client VPN verwendete Zertifikate müssen [RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile](#) entsprechen, einschließlich der in Abschnitt 4.2 des Memos angegebenen Zertifikatserweiterungen.

#### 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 Zertifikate, die mit dem Client-VPN-Dienst verwendet werden, aktualisiert werden, sei es durch automatische ACM-Rotation, manuelles Importieren eines neuen Zertifikats oder Metadaten-Updates für IAM Identity Center, aktualisiert der Client-VPN-Dienst den Client-VPN-Endpunkt automatisch mit dem neueren Zertifikat. Dies ist ein automatisierter Vorgang, der bis zu 5 Stunden dauern kann.

## Aufgaben

- [Aktivieren Sie die gegenseitige Authentifizierung für AWS Client VPN](#)
- [Erneuern Sie Ihr Serverzertifikat für AWS Client VPN](#)

### Aktivieren Sie die gegenseitige Authentifizierung für AWS Client VPN

Sie können die gegenseitige Authentifizierung in Client VPN entweder in Windows Linux/MacOS oder in Windows aktivieren.

## 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.

## Erneuern Sie Ihr Serverzertifikat für AWS Client VPN

Sie können ein abgelaufenes Client-VPN-Serverzertifikat erneuern und erneut importieren. Abhängig von der Version von OpenVPN easy-rsa, die Sie verwenden, variiert das Verfahren. Weitere Informationen finden Sie in der Dokumentation zur [Verlängerung und zum Widerruf von Easy-RSA 3-Zertifikaten](#).

Um Ihr Serverzertifikat zu erneuern

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 --san=DNS:server 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 \
  --certificate-arn
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

## Single Sign-On — SAML 2.0-basierte Verbundauthentifizierung — im Client VPN

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.

### Themen

- [SAML aktivieren für AWS Client VPN](#)
- [Authentifizierungs-Workflow](#)
- [Anforderungen und Überlegungen für die SAML-basierte Verbundauthentifizierung](#)
- [Konfigurationsressourcen für SAML-basierte IdPs](#)

### SAML aktivieren für AWS Client VPN

Sie können SAML für Single Sign-On für Client VPN aktivieren, indem Sie die folgenden Schritte ausführen. Wenn das Self-Service-Portal für Ihren Client VPN-Endpunkt aktiviert ist, weisen Sie Ihre Benutzer alternativ an, zum Self-Service-Portal zu gehen, um die Konfigurationsdatei und den von AWS bereitgestellten Client abzurufen. Weitere Informationen finden Sie unter [AWS Client VPN Zugang zum Self-Service-Portal](#).

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 einzurichten 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 Vertrauensstellung zwischen AWS und dem IdP einzurichten.

4. Erstellen Sie einen IAM-SAML-Identitätsanbieter in demselben AWS Konto wie der Client-VPN-Endpunkt.

Der IAM-SAML-Identitätsanbieter definiert die AWS IdP-zu-Vertrauens-Beziehung 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.

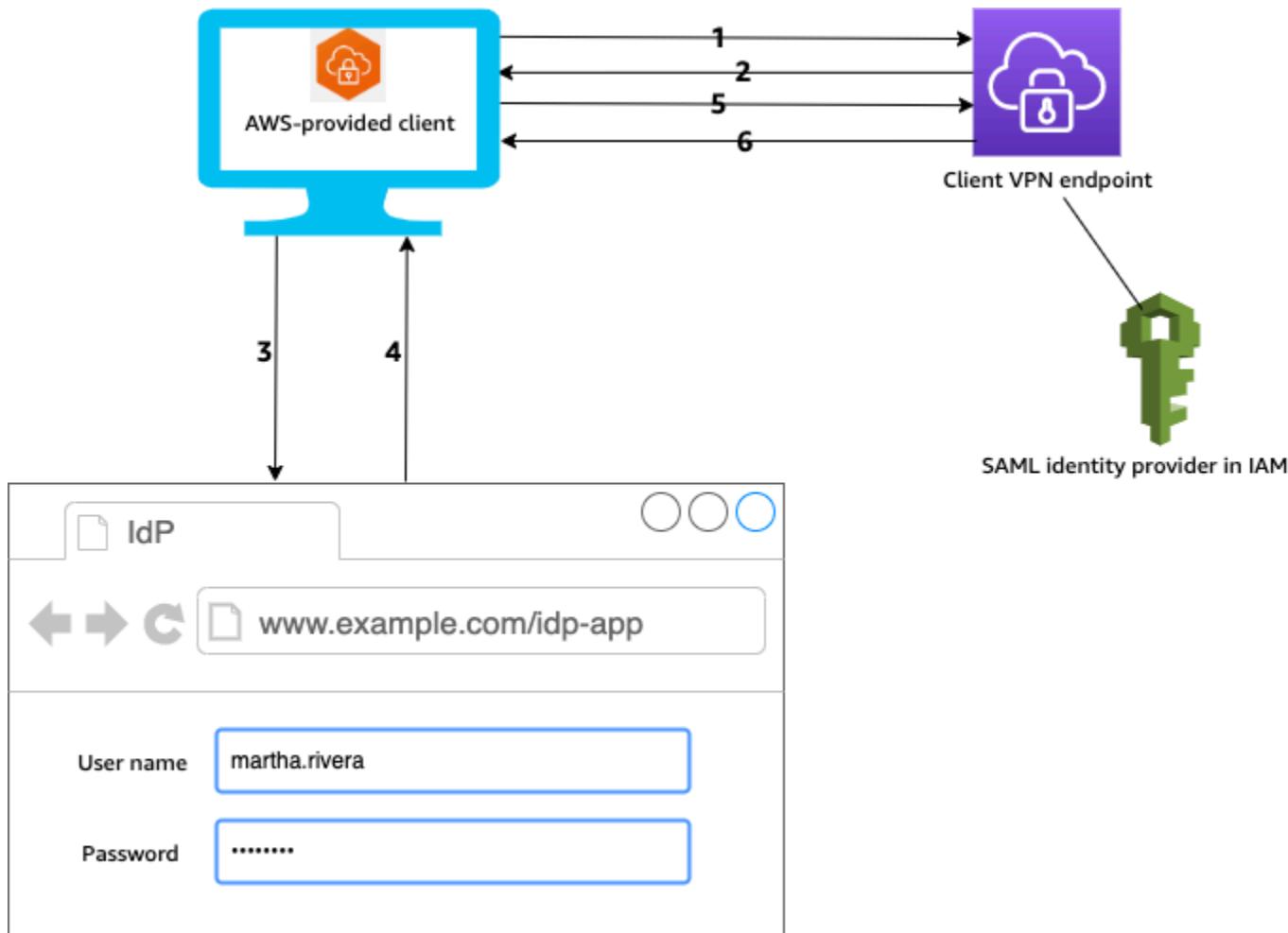
5. Erstellen Sie einen Client VPN-Endpunkt.

Legen Sie die Verbundauthentifizierung als Authentifizierungstyp fest und geben Sie den von Ihnen erstellten IAM SAML-Identitätsanbieter an. Weitere Informationen finden Sie unter [Einen AWS Client VPN Endpunkt erstellen](#).

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.

## 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 Kontingenzen 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 -Antwort 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.

- Wenn Zertifikate, die mit dem Client-VPN-Dienst verwendet werden, aktualisiert werden, sei es durch automatische ACM-Rotation, manuelles Importieren eines neuen Zertifikats oder Metadaten-Updates für IAM Identity Center, aktualisiert der Client-VPN-Dienst den Client-VPN-Endpunkt automatisch mit dem neueren Zertifikat. Dies ist ein automatisierter Vorgang, der bis zu 5 Stunden dauern kann.

## 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	<a href="#">Authentifizieren AWS Client VPN Sie Benutzer mit SAML</a>
Microsoft Entra ID (früher Azure Active Directory)	Weitere Informationen finden Sie unter <a href="#">Tutorial: Microsoft Entra Single Sign-On (SSO) -Integration mit AWS ClientVPN</a> auf der Microsoft-Dokumentationswebsite.
JumpCloud	<a href="#">Integrieren Sie mit AWS Client VPN</a>
AWS IAM Identity Center	<a href="#">Verwenden von IAM Identity Center mit AWS Client VPN zur Authentifizierung und Autorisierung</a>

## 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 [AWS Client VPN 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) unterstützt URLs, 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 hinzufügen. URLs

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

Wenn Ihr IdP nicht mehrere ACS unterstützt URLs, gehen Sie wie folgt 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.

## Kundenautorisierung in AWS Client VPN

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 [Wenden Sie eine Sicherheitsgruppe auf ein Zielnetzwerk an in AWS Client VPN](#). 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.

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 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 [AWS Client VPN Autorisierungsregeln](#).

### Aufgaben

- [Gruppenregel AWS Client VPN für Endpunktsicherheit erstellen](#)

## Gruppenregel AWS Client VPN für Endpunktsicherheit erstellen

Die Standardsicherheitsgruppe für die VPC, die angewendet wird, wenn Sie einem Client VPN ein Subnetz zuordnen, kann den Datenverkehr aus der Standardsicherheitsgruppe einschränken, den Sie zulassen möchten, und gleichzeitig Datenverkehr zulassen, den Sie nicht möchten. Gehen Sie wie folgt vor, um eine Client-VPN-Endpunktsicherheitsgruppenregel zu erstellen, die den Datenverkehr für eine Endpunktsicherheitsgruppe, die einer Ressource oder Anwendung zugeordnet ist, entweder zulässt oder einschränkt. Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter [Sicherheitsgruppen für Ihre VPC](#) im Amazon VPC-Benutzerhandbuch.

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 Regel hinzufügen aus.
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.

## Verbindungsauthorisierung in AWS Client VPN

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 Gerät-, 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 Gerät-, 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 Benutzeroauthentifizierung 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 [Eine AWS Client VPN Client-Verbindung beenden](#).
- 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. Falls bei der Ausführung der Lambda-Funktion Fehler auftreten (z. B. aufgrund von Drosselung), wird die folgende Standardnachricht vom Client-VPN-Dienst an die 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 Sie den Client Connect-Handler für die Beurteilung der Körperhaltung

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 Geräteauthorisierungs-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, das Feld `aws-client-version` im Verbindungshandler gilt jedoch nur für die AWS Client VPN Anwendung und wird anhand von Umgebungsvariablen auf dem Benutzergerät aufgefüllt.

## Aktivieren Sie den Client-Connect-Handler

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 [Einen AWS Client VPN Endpunkt erstellen](#) und [Einen AWS Client VPN Endpunkt ändern](#).

## Serviceverknüpfte Rolle

AWS Client VPN erstellt automatisch eine mit dem Dienst verknüpfte Rolle in Ihrem Konto namens `AWSServiceRoleForClientVPNCConnections`. 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 AWS Client VPN](#).

## Überwachen Sie Fehler bei der Verbindungsauthorisierung

Sie können den Status der Verbindungsauthorisierung von Verbindungen zum Client-VPN-Endpunkt anzeigen. Weitere Informationen finden Sie unter [AWS Client VPN Client-Verbindungen anzeigen](#).

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 für einen Endpunkt AWS Client VPN](#).

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

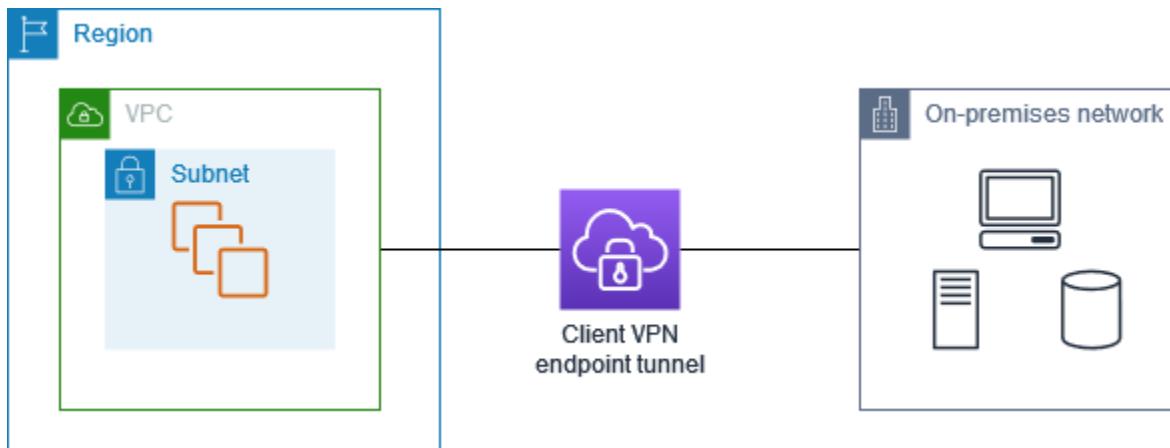
- `client-connect-failed` – Die Lambda-Funktion verhinderte, dass die Verbindung hergestellt wurde.
- `client-connect-handler-timed-out` – Die Lambda-Funktion hat das Zeitlimit überschritten.
- `client-connect-handler-other-execution-error` – Die Lambda-Funktion ist auf einen unerwarteten Fehler gestoßen.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

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 des Datenverkehrs von Clients optimieren, indem Sie nur den dafür vorgesehenen AWS Datenverkehr den VPN-Tunnel durchqueren lassen.
- Sie können das Volumen des ausgehenden Datenverkehrs von reduzieren AWS und damit die Kosten für die Datenübertragung senken.

## Überlegungen zum Routing

- Wenn Sie den Split-Tunnelmodus aktivieren, werden alle Routen in der Routentabelle des Client-VPN-Endpunkts zur Routentabelle 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

Das Hinzufügen einer `0.0.0.0/0`-Route zur Routentabelle des Client-VPN-Endpunkts bei Verwendung des Split-Tunnel-Modus kann zu Verbindungsunterbrechungen führen und wird nicht empfohlen

- 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.

## Split-Tunnel aktivieren

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

- [Einen AWS Client VPN Endpunkt erstellen](#)
- [Einen AWS Client VPN Endpunkt ändern](#)

## Verbindungsprotokollierung für einen Endpunkt AWS Client VPN

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

Ein Verbindungsprotokoll enthält Verbindungsprotokolleinträge, in denen Informationen über Verbindungsereignisse erfasst werden, z. B. wenn ein Client (Endbenutzer) eine Verbindung zu Ihrem Client-VPN-Endpunkt herstellt, versucht, eine Verbindung herzustellen oder die Verbindung 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 sie verfügbar AWS Client VPN ist. Verbindungsprotokolle werden in einer Protokollgruppe „ CloudWatch Protokolle“ 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 aus dem IPv4 CIDR-Bereich des Clients für den Client-VPN-Endpunkt zugewiesen wurde.

- **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 [AWS Client VPN Verbindungsprotokolle](#).

## 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 Clients berücksichtigen, die Sie derzeit unterstützen, und ob Ihr Client-VPN-Endpunkt skaliert werden kann, um bei Bedarf zusätzlichen Bedarf zu decken.

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 Subnetzuordnungen für den Client-VPN-Endpunkt.

Subnetzuordnungen	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 Subnetzuordnungen auch von der Anzahl der Availability Zones ab, die in einer Region verfügbar sind. AWS

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 für die Verwendung AWS Client VPN](#).

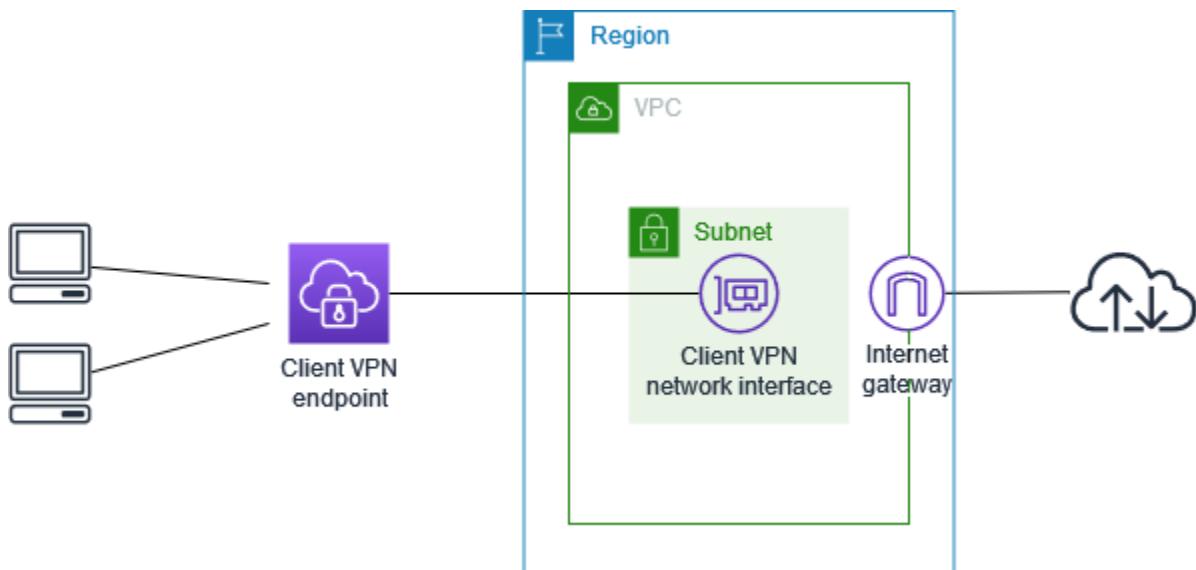
Weitere Informationen zu Kontingenzen für Ihren Client-VPN-Endpunkt finden Sie unter [AWS Client VPN Kontingente](#).

# Fangen Sie an mit AWS Client VPN

In diesem Tutorial erstellen Sie einen AWS Client VPN Endpunkt, der Folgendes tut:

- 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. Das Serverzertifikat muss mindestens in AWS Certificate Manager (ACM) importiert und angegeben werden, wenn Sie den Client-VPN-Endpunkt erstellen. 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 in AWS Client VPN](#).

 Note

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

## 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 einen IP-Adressbereich in CIDR-Notation an, aus dem Client-IP-Adressen zugewiesen werden sollen.

### 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. (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-Serven von den Clients erreicht werden können.

8. 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 Client VPN-Endpunkt angeben können, finden Sie unter [Einen AWS Client VPN Endpunkt erstellen](#).

## 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. Um beispielsweise den Zugriff auf die gesamte VPC zu ermöglichen, 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 Zugriff auf zusätzliche Netzwerke gewähren, die mit der VPC verbunden sind, z. B. AWS Dienste, Peering-Netzwerke VPCs, lokale Netzwerke und das Internet. 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 (Autorsierungsregeln) und dann Add authorization rule (Autorsierungsregel 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 (Autorsierungsregel 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 [AWS Client VPN Export von Endpunktkonfigurationsdateien](#).

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

Sie können mit dem AWS bereitgestellten Client oder einer anderen OpenVPN-basierten Client-Anwendung und der Konfigurationsdatei, die Sie gerade erstellt haben, eine Verbindung zum Client-VPN-Endpunkt herstellen. Weitere Informationen finden Sie im [AWS Client VPN -Benutzerhandbuch](#).

# Arbeite mit AWS Client VPN

In den folgenden Themen werden die wichtigsten administrativen Aufgaben erläutert, die für die Arbeit mit Client VPN erforderlich sind:

- Auf das Self-Service-Portal zugreifen — Konfigurieren Sie den Zugriff auf das Client-VPN-Self-Service-Portal, sodass Kunden die Client-VPN-Endpunkt konfigurationsdatei selbst herunterladen können. Informationen zum Zugriff auf das Self-Service-Portal finden Sie unter [the section called “Zugang zum Self-Service-Portal”](#).
- Autorisierungsregeln — Fügen Sie Autorisierungsregeln hinzu, um den Client-Zugriff auf bestimmte Netzwerke zu kontrollieren. Informationen zum Hinzufügen von Autorisierungsregeln finden Sie unter [the section called “Autorisierungsregeln”](#).
- Sperrlisten für Client-Zertifikate — Verwenden Sie Client-Zertifikatssperrenlisten, um den Zugriff auf einen Client-VPN-Endpunkt zu widerrufen. Informationen zu Sperrlisten für Client-Zertifikate finden Sie unter [the section called “Client-Zertifikatsperrenlisten”](#).
- Client-Verbindungen — Zeigt eine Client-Verbindung zu einem Client-VPN-Endpunkt an oder beendet sie. Hinweise zum Anzeigen oder Beenden einer Client-Verbindung finden Sie unter [the section called “Client-Verbindungen”](#).
- Kundenanmelde-Banner — Fügen Sie einer Client-VPN-Desktop-Anwendung ein Textbanner hinzu, wenn eine VPN-Sitzung eingerichtet wird. Sie können das Textbanner verwenden, um Ihre regulatorischen und Compliance-Anforderungen zu erfüllen. Informationen zu Login-Bannern finden Sie unter [the section called “Banner für die Kundenanmeldung”](#).
- Durchsetzung von Client-Routen — Erzwingen Sie vom Administrator definierte Routen auf Geräten, die über das VPN verbunden sind. Weitere Informationen zur Client-Routenerzwingung finden Sie unter [the section called “Durchsetzung der Client-Route”](#).
- Client-VPN-Endpunkte — Konfigurieren Sie Client-VPN-Endpunkte zur Verwaltung und Steuerung aller VPN-Sitzungen. Informationen zur Konfiguration von Endpunkten finden Sie unter [the section called “Endpunkte”](#).
- Verbindungsprotokolle — Aktivieren Sie die Verbindungsprotokollierung für neue oder bestehende Client-VPN-Endpunkte, um mit der Erfassung von Verbindungsprotokollen zu beginnen. Informationen zur Verbindungsprotokollierung finden Sie unter [the section called “Verbindungsprotokolle.”](#)
- Export der Client-Konfigurationsdatei — Konfigurieren Sie die Client-Konfigurationsdatei, die Client-VPN-Clients benötigen, um VPN-Verbindungen herzustellen. Nachdem Sie die Datei konfiguriert haben, laden Sie sie herunter (exportieren), um sie an die Clients zu verteilen. Weitere Hinweise

zum Exportieren einer Client-Konfigurationsdatei finden Sie unter [the section called “Export der Client-Konfigurationsdatei”](#).

- Routen — Konfigurieren Sie Autorisierungsregeln für jede Client-VPN-Route, um anzugeben, welche Clients Zugriff auf das Zielnetzwerk haben. Informationen zur Konfiguration von Autorisierungsregeln finden Sie unter [the section called “Autorisierungsregeln”](#).
- Zielnetzwerke — Ordnen Sie Zielnetzwerke einem Client-VPN-Endpunkt zu, damit Clients eine Verbindung zu diesem herstellen und eine VPN-Verbindung herstellen können. Informationen zu Zielnetzwerken finden Sie unter [the section called “Zielnetzwerke”](#).
- Maximale VPN-Sitzungsdauer — Legen Sie Optionen für die maximale VPN-Sitzungsdauer fest, um Ihre Sicherheits- und Compliance-Anforderungen zu erfüllen. Informationen zur maximalen Dauer einer VPN-Sitzung finden Sie unter [the section called “Maximale Dauer der VPN-Sitzung”](#).

## AWS Client VPN Zugang zum 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. Im Portal können Kunden die Client-VPN-Endpunktkonfigurationsdatei und die neueste Version des 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 exportieren. AWS CLI 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 Optionen zur Verfügung: URLs

- <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>* die vorherige URL durch die ID Ihres Client-VPN-Endpunkts, zum Beispiel `vpn-endpoint-0123456abcd123456`.

Sie können die URL für das Self-Service-Portal auch in der Ausgabe des [describe-client-vpn-endpoints](#) AWS CLI Befehls anzeigen. 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](#).

## AWS Client VPN 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 [Problembehandlung AWS Client VPN: Autorisierungsregeln für Active Directory-Gruppen funktionieren nicht wie erwartet](#) und unter [Routenpriorität](#) im Benutzerhandbuch zu Amazon VPC.

## 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.

## Themen

- [Beispielszenarien für Client-VPN-Autorisierungsregeln](#)
- [Eine Autorisierungsregel zu einem AWS Client VPN Endpunkt hinzufügen](#)
- [Eine Autorisierungsregel von einem AWS Client VPN Endpunkt entfernen](#)
- [AWS Client VPN Autorisierungsregeln anzeigen](#)

## Beispielszenarien für Client-VPN-Autorisierungsregeln

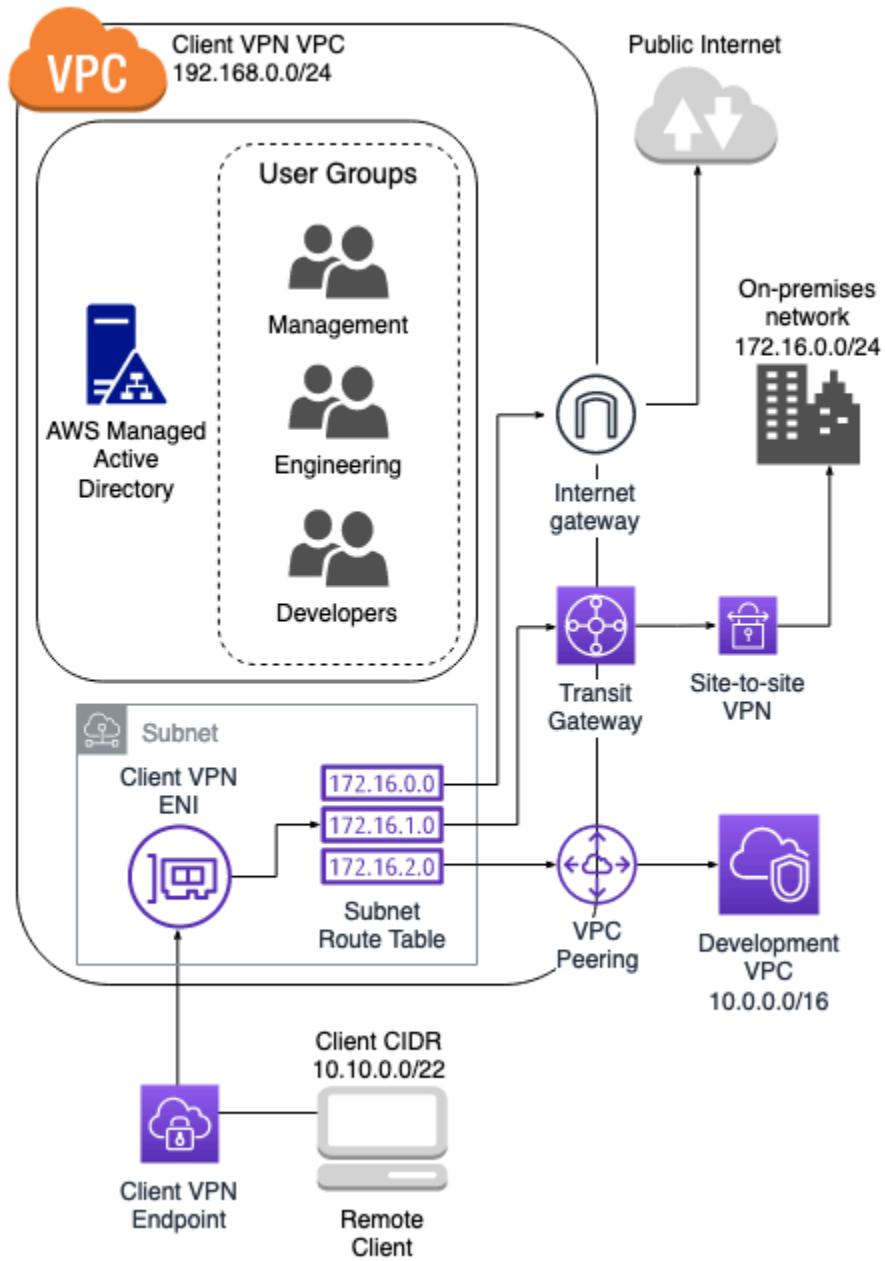
In diesem Abschnitt wird beschrieben, wie Autorisierungsregeln für funktionieren AWS Client VPN. Der Abschnitt enthält wichtige Informationen zu Autorisierungsregeln, eine Beispielarchitektur und Beispielszenarien entsprechend der Beispielarchitektur.

## Szenarien

- [the section called “Beispielarchitektur”](#)
- [the section called “Zugriff auf ein einziges Ziel”](#)
- [the section called “Verwenden Sie ein beliebiges Ziel \(0.0.0.0/0\) CIDR”](#)
- [the section called “Längere Übereinstimmung mit dem IP-Präfix”](#)
- [the section called “Überlappendes CIDR \(gleiche Gruppe\)”](#)
- [the section called “Zusätzliche 0.0.0.0/0-Regel”](#)
- [the section called “Fügen Sie eine Regel für 192.168.0.0/24 hinzu”](#)
- [the section called “SAML-Verbundauthentifizierung”](#)
- [the section called “Zugriff für alle Benutzergruppen”](#)

## Beispielarchitektur für Szenarien zu Autorisierungsregeln

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



Zugriff auf ein einziges Ziel

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
		Zugriff auf alle Benutzer erlauben	

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 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.

## Verwenden Sie ein beliebiges Ziel (0.0.0.0/0) CIDR

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR

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

## 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 10.0.0.0/16.

### 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.

## Längere Übereinstimmung mit dem IP-Präfix

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	10.0.2.119/32

### 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.

### 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	10.0.2.119/32
	S-xxxxx14	Falsch	172,160,128/ 25

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			

### 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.

### Zusätzliche 0.0.0.0/0-Regel

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 Entwicklungs-VPC für die Managergruppe	S-xxxxx16	Falsch	10.0.2.119/32
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.

Fügen Sie eine Regel für 192.168.0.0/24 hinzu

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	10.0.2.119/32
Erlauben des Zugriffs auf ein Subnetz im	S-xxxxx14	Falsch	172,160,128/ 25

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
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.

## SAML-Verbundauthentifizierung

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Erlauben des Zugriffs auf ein On-Premises-Netzwerk für die Engineering-Gruppe	Entwicklung	Falsch	172.16.0.0/24
Erlauben des Zugriffs auf eine Entwicklungs-VPC für die Entwicklungsgruppe	Entwickler	Falsch	10.0.0.0/16
Erlauben des Zugriffs auf eine Client-VPN-VPC für die Managergruppe	Manager	Falsch	192.168.0.0/24

### Resultierendes Verhalten

- Benutzer, die über SAML mit dem Gruppenattribut „Engineering“ authentifiziert wurden, können nur darauf zugreifen. 172.16.0.0/24
- Benutzer, die über SAML mit dem Gruppenattribut „Developers“ authentifiziert wurden, können nur darauf zugreifen. 10.0.0.0/16
- Benutzer, die über SAML mit dem Gruppenattribut „Manager“ authentifiziert wurden, können nur darauf zugreifen. 192.168.0.0/24
- Der gesamte restliche Datenverkehr wird vom Client-VPN-Endpunkt gelöscht.

 Note

Bei Verwendung der SAML-Verbundauthentifizierung entspricht das Gruppen-ID-Feld dem SAML-Attributwert, der die Gruppenmitgliedschaft des Benutzers identifiziert. Dieses Attribut

wird in Ihrem SAML-Identitätsanbieter konfiguriert und bei der Authentifizierung an Client VPN übergeben.

## 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	10.0.2.119/32
Erlauben des Zugriffs auf ein Subnetz im On-Premises-Netzwe	S-xxxxx14	Falsch	172,160,128/ 25

Regelbeschreibung	Gruppen-ID	Zugriff auf alle Benutzer erlauben	Ziel-CIDR
Netzwerk für die Engineering-Gruppe			
Erlauben des Zugriffs auf alle Netzwerke 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
Erlauben des Zugriffs für alle Gruppen	N/A	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.

## Eine Autorisierungsregel zu einem AWS Client VPN Endpunkt hinzufügen

Sie können eine Autorisierungsregel hinzufügen, um den Zugriff auf einen Client-VPN-Endpunkt zu gewähren oder einzuschränken, indem Sie die verwenden AWS-Managementkonsole. Eine Autorisierungsregel kann einem Client-VPN-Endpunkt entweder über die Amazon VPC-Konsole oder über die Befehlszeile oder API hinzugefügt werden.

Um einem Client-VPN-Endpunkt eine Autorisierungsregel hinzuzufügen, verwenden Sie AWS-Managementkonsole

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. Zum Beispiel die Sicherheits-ID (SID) einer Active Directory-Gruppe oder die einer Gruppe, die ID/name in einem SAML-basierten Identitätsanbieter (IdP) definiert ist.
    - (Active Directory) Um die SID abzurufen, können Sie das Microsoft ADGroup Powershell-Cmdlet [Get-](#) verwenden, zum Beispiel:

```
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 Gruppe ID/name 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 [authorize-client-vpn-ingress](#)-Befehl.

## Eine Autorisierungsregel von einem AWS Client VPN Endpunkt entfernen

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

Um Autorisierungsregeln zu entfernen (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 Autorisierungsregel hinzugefügt wurde, und wählen Sie dann Autorisierungsregeln aus.
4. Wählen Sie die zu löschenende Autorisierungsregel aus, wählen Sie Autorisierungsregel entfernen und klicken Sie dann erneut auf Autorisierungsregel entfernen, um das Löschen zu bestätigen.

Um Autorisierungsregeln zu entfernen (AWS CLI)

Verwenden Sie den [revoke-client-vpn-ingress](#)-Befehl.

## AWS Client VPN 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](#).

## AWS Client VPN Sperrlisten für Client-Zertifikate

Sperrlisten für Client-VPN-Clientzertifikate werden verwendet, um bestimmten Client-Zertifikaten den Zugriff auf einen Client-VPN-Endpunkt zu entziehen. Sie können entweder eine Sperrliste erstellen oder eine vorhandene Liste importieren. Sie können Ihre aktuelle Liste auch als Sperrlistendatei exportieren. Das Generieren einer Liste erfolgt mit der OpenVPN-Software unter Linux/macOS oder unter Windows. Import und Export können entweder über die Amazon VPC-Konsole oder über die AWS CLI erfolgen.

Weitere Informationen über die Generierung der Server- und Client-Zertifikate und Schlüssel finden Sie unter [Gegenseitige Authentifizierung in AWS Client VPN](#)

### Note

Wenn eine Sperrliste für Client-Zertifikate abgelaufen ist, können Sie keine Verbindung zum Client-VPN-Endpunkt herstellen. Sie müssen eine neue erstellen und sie in den Client-VPN-Endpunkt importieren.

Sie können einer Sperrliste für Client-Zertifikate nur eine begrenzte Anzahl von Einträgen hinzufügen. Weitere Hinweise zur Anzahl der Einträge, die Sie einer Sperrliste hinzufügen können, finden Sie unter [Client VPN-Kontingente](#).

### Aufgaben

- [Generieren Sie eine Sperrliste für AWS Client VPN Client-Zertifikate](#)
- [Eine Sperrliste für AWS Client VPN Client-Zertifikate importieren](#)
- [Exportieren einer Sperrliste für AWS Client VPN Client-Zertifikate](#)

## Generieren Sie eine Sperrliste für AWS Client VPN Client-Zertifikate

Sie können eine Sperrliste für Client-VPN-Zertifikate entweder auf einem Linux/macOS oder einem Windows-Betriebssystem erstellen. Die Sperrliste wird verwendet, um bestimmten Zertifikaten den Zugriff auf einen Client-VPN-Endpunkt zu entziehen. Weitere Informationen zu Sperrlisten für Client-Zertifikate finden Sie unter [Client-Zertifikatsperrlisten](#).

### 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 bei dem Server an, der die easyrsa-Installation hostet, mit der das Zertifikat generiert 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 ein, yes wenn Sie aufgefordert werden.

### Windows

Im folgenden Verfahren wird die OpenVPN-Software verwendet, um eine Client-Sperre 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 EasyRSA-Start.bat Datei 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 bei Aufforderung ein.

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 crt.pem
```

## Eine Sperrliste für AWS Client VPN Client-Zertifikate importieren

Sie benötigen eine Datei mit einer Sperrliste für Client-VPN-Clientzertifikate, die importiert werden können. Weitere Informationen zum Generieren einer Client-Zertifikatssperrliste finden Sie unter [Generieren Sie eine Sperrliste für AWS Client VPN Client-Zertifikate](#).

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

## So importieren Sie eine Client-Zertifikatssperlliste (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-Zertifikatssperlliste importiert werden soll.
4. Wählen Sie Actions (Aktionen) und dann Import Client Certificate CRL (Client-Zertifikatssperllisten importieren).
5. Geben Sie für Certificate Revocation List (Zertifikatssperlliste) den Inhalt der Client-Zertifikatssperllistendatei ein und wählen Sie Import client certificate CRL (Client-Zertifikatssperlliste importieren) aus.

## So importieren Sie eine Client-Zertifikatssperlliste (AWS CLI)

Verwenden Sie den `certificate-revocation-list` Befehl [import-client-vpn-client-](#).

```
$ 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 Sperrliste für AWS Client VPN Client-Zertifikate

Sie können Sperrlisten für Client-VPN-Clientzertifikate mithilfe der Konsole und der exportieren AWS CLI.

## So exportieren Sie eine Client-Zertifikatssperlliste (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-Zertifikatssperlliste exportiert werden soll.
4. Wählen Sie Actions (Aktionen), Export Client Certificate CRL (Client-Zertifikatssperlliste exportieren) und Export Client Certificate CRL (Client-Zertifikatssperlliste exportieren) aus.

## So exportieren Sie eine Client-Zertifikatssperlliste (AWS CLI)

Verwenden Sie den `certificate-revocation-list` Befehl [export-client-vpn-client-](#).

# AWS Client VPN Client-Verbindungen

AWS Client VPN Verbindungen sind aktive VPN-Sitzungen, die von Clients zu einem bestimmten Client-VPN-Endpunkt eingerichtet wurden, sowie Verbindungen, die innerhalb der letzten 60 Minuten für diesen Endpunkt beendet wurden. Eine Verbindung wird hergestellt, wenn ein Client erfolgreich eine Verbindung mit einem Client VPN-Endpunkt aufbaut. Durch das Beenden einer Sitzung wird die Client-Verbindung zum Client-VPN-Endpunkt beendet.

Sie können Client-VPN-Verbindungen anzeigen und beenden. Beim Anzeigen von Verbindungsinformationen werden Informationen wie die aus dem CIDR-Blockbereich des Clients zugewiesene IP-Adresse, die Endpunkt-ID und der Zeitstempel zurückgegeben. Durch das Beenden einer Sitzung wird die angegebene VPN-Verbindung zum Endpunkt beendet. Das Anzeigen und Beenden von Sitzungen kann entweder über die Amazon VPC-Konsole oder die AWS CLI erfolgen. Falls Sie keine Verbindung zum Endpunkt herstellen können und je nach dem Fehler, finden Sie hier die Schritte [Fehlerbehebung](#) zur Lösung des Problems.

## Aufgaben

- [AWS Client VPN Client-Verbindungen anzeigen](#)
- [Eine AWS Client VPN Client-Verbindung beenden](#)

## AWS Client VPN Client-Verbindungen anzeigen

Sie können die aktiven Client-VPN-Verbindungen entweder mit der Amazon VPC-Konsole oder der AWS CLI anzeigen.

So zeigen Sie Client-VPN-Clientverbindungen 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-VPN-Clientverbindungen an (AWS CLI)

Verwenden Sie den [describe-client-vpn-connections](#)-Befehl.

## Eine AWS Client VPN Client-Verbindung beenden

Sie können eine Client-VPN-Client-Verbindung mit der Amazon VPC-Konsole oder der AWS CLI beenden.

So beenden Sie eine Client-VPN-Clientverbindung (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 Verbindungen aus.
4. Wählen Sie die Verbindung aus, die Sie beenden möchten, klicken Sie auf Verbindung beenden und wählen Sie dann erneut Verbindung beenden, um die Kündigung zu bestätigen.

Um eine Client-VPN-Clientverbindung zu beenden (AWS CLI)

Verwenden Sie den [terminate-client-vpn-connections](#)-Befehl.

## AWS Client VPN Kunden-Login-Banner

AWS Client VPN bietet die Option, ein Textbanner auf AWS bereitgestellten Client-VPN-Desktop-Anwendungen 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 1400 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.

## Erstellung von Bannern

Anmeldebanner werden zunächst während der Erstellung des Client-VPN-Endpunkts erstellt und aktiviert. Die Schritte zum Aktivieren eines Client-Login-Banners bei der Erstellung eines Client-VPN-Endpunkts finden Sie unter [Einen AWS Client VPN Endpunkt erstellen](#).

## Aufgaben

- [Konfigurieren Sie ein Client-Login-Banner für einen vorhandenen AWS Client VPN Endpunkt](#)
- [Deaktivieren Sie ein Client-Login-Banner für einen vorhandenen AWS Client VPN Endpunkt](#)
- [Bestehenden Bannertext auf einem AWS Client VPN Endpunkt ändern](#)
- [Ein aktuell konfiguriertes AWS Client VPN Login-Banner anzeigen](#)

## Konfigurieren Sie ein Client-Login-Banner für einen vorhandenen AWS 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 als Bannertext für die Client-Anmeldung den Text ein, der auf den AWS bereitgestellten Clients in einem Banner 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 [modify-client-vpn-endpoint](#)-Befehl.

## Deaktivieren Sie ein Client-Login-Banner für einen vorhandenen AWS 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 [modify-client-vpn-endpoint](#)-Befehl.

## Bestehenden Bannertext auf einem AWS Client VPN Endpunkt ändern

Gehen Sie wie folgt vor, um den vorhandenen Text auf einem Anmeldebanner für einen Client VPN-Client 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 für den Bannertext für die Kundenanmeldung den vorhandenen Text durch neuen Text, der auf den AWS bereitgestellten Clients in einem Banner 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 [modify-client-vpn-endpoint](#)-Befehl.

## Ein aktuell konfiguriertes AWS Client VPN Login-Banner anzeigen

Gehen Sie wie folgt vor, um ein aktuell konfiguriertes Anmeldebanner für den Client VPN-Client 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 [describe-client-vpn-endpoints](#)-Befehl.

## AWS Client VPN Durchsetzung der Client-Route

Client Route Enforce hilft dabei, vom Administrator definierte Routen auf Geräten durchzusetzen, die über das VPN verbunden sind. Diese Funktion trägt zur Verbesserung Ihrer Sicherheitslage bei, indem sie sicherstellt, dass der Netzwerkverkehr, der von einem verbundenen Client ausgeht, nicht versehentlich aus dem VPN-Tunnel heraus gesendet wird.

Client Route Enforce überwacht die Haupt-Routingtabelle des verbundenen Geräts und stellt sicher, dass ausgehender Netzwerkverkehr gemäß den im Client-VPN-Endpunkt konfigurierten Netzwerkrouten in einen VPN-Tunnel geleitet wird. Dazu gehört das Ändern von Routingtabellen auf einem Gerät, falls Routen erkannt werden, die mit dem VPN-Tunnel in Konflikt stehen. Client Route Enforce unterstützt sowohl Adressfamilien als IPv4 auch IPv6 Adressfamilien.

## Voraussetzungen

Client Route Enforcement funktioniert nur mit den folgenden AWS bereitgestellten Client-VPN-Versionen:

- Windows-Version 5.2.0 oder höher (IPv4 Unterstützung)

- macOS Version 5.2.0 oder höher (IPv4 Unterstützung)
- Ubuntu Version 5.2.0 oder höher (Unterstützung) IPv4
- Windows-Version 5.3.0 oder höher (Unterstützung) IPv6
- macOS Version 5.3.0 oder höher (IPv6 Unterstützung)
- Ubuntu-Version 5.3.0 oder höher (Unterstützung) IPv6

Bei Dual-Stack-Endpunkten gilt die Einstellung für die Client-Routenerzwingung sowohl für beide als auch IPv4 für Stacks gleichzeitig. IPv6 Es ist nicht möglich, Client Route Enforce nur für einen Stack zu aktivieren.

## Routing-Konflikte

Während ein Client mit VPN verbunden ist, wird ein Vergleich zwischen der lokalen Routentabelle des Clients und den Netzwerk routen des Endpunkts durchgeführt. Ein Routingkonflikt tritt auf, wenn es eine Netzwerküberschneidung zwischen zwei Routing-Tabelleneinträgen gibt. Ein Beispiel für überlappende Netzwerke ist:

- 172.31.0.0/16
- 172.31.1.0/24

In diesem Beispiel stellen diese CIDR-Blöcke einen Routing-Konflikt dar. Dies 172.31.0.0/16 könnte beispielsweise der VPN-Tunnel CIDR sein. Da es spezifischer 172.31.1.0/24 ist, weil es ein längeres Präfix hat, hat es in der Regel Vorrang und leitet den VPN-Verkehr innerhalb des 172.31.1.0/24 IP-Bereichs möglicherweise zu einem anderen Ziel um. Dies könnte zu unbeabsichtigtem Routing-Verhalten führen. Wenn Client Route Enforcement jedoch aktiviert ist, wird letzteres CIDR entfernt. Bei der Verwendung dieser Funktion sollten potenzielle Routingkonflikte berücksichtigt werden.

Vollständige Tunnel-VPN-Verbindungen leiten den gesamten Netzwerkverkehr über die VPN-Verbindung. Daher können Geräte, die mit dem VPN verbunden sind, nicht auf lokale Netzwerkressourcen (LAN) zugreifen, wenn die Funktion Client Route Enforcement aktiviert ist. Wenn ein lokaler LAN-Zugriff erforderlich ist, sollten Sie den Split-Tunnel-Modus anstelle des Full-Tunnel-Modus verwenden. Weitere Hinweise zum Split-Tunnel finden Sie unter. [Split-Tunnel-Client VPN](#)

## Überlegungen

Die folgenden Informationen sollten vor der Aktivierung von Client Route Enforce berücksichtigt werden.

- Wenn zum Zeitpunkt der Verbindung ein Routingkonflikt erkannt wird, aktualisiert die Funktion die Routing-Tabelle des Clients, sodass der Datenverkehr in den VPN-Tunnel geleitet wird. Die Routen, die vor dem Verbindungsaufbau existierten und durch diese Funktion gelöscht wurden, werden wiederhergestellt.
- Die Funktion wird nur in der Haupt-Routingtabelle erzwungen und gilt nicht für andere Routing-Mechanismen. Die Durchsetzung wird beispielsweise nicht auf Folgendes angewendet:
  - richtlinienbasiertes Routing
  - Routing mit Schnittstellenbereich
- Client Route Enforce schützt den VPN-Tunnel, solange er geöffnet ist. Es besteht kein Schutz, nachdem der Tunnel getrennt wurde oder der Client erneut eine Verbindung herstellt.

## Auswirkungen von OpenVPN-Richtlinien auf die Durchsetzung von Cloud-Routen

Einige benutzerdefinierte Direktiven in der OpenVPN-Konfigurationsdatei haben spezifische Interaktionen mit Client Route Enforce:

- Die `route`-Direktive
  - Beim Hinzufügen von Routen zu einem VPN-Gateway. Zum Beispiel beim Hinzufügen der Route `192.168.100.0 255.255.255.0` zu einem VPN-Gateway.

Zu einem VPN-Gateway hinzugefügte Routen werden von Client Route Enforce ähnlich wie jede andere VPN-Route überwacht. Alle darin enthaltenen widersprüchlichen Routen werden erkannt und entfernt.

- Beim Hinzufügen von Routen zu einem Nicht-VPN-Gateway. Zum Beispiel das Hinzufügen der Route `192.168.200.0 255.255.255.0 net_gateway`.

Routen, die zu einem Nicht-VPN-Gateway hinzugefügt wurden, sind von der Client Route Enforcement ausgeschlossen, da sie den VPN-Tunnel umgehen. In ihnen sind widersprüchliche Routen zulässig. Im obigen Beispiel wird die Route von der Überwachung durch Client Route Enforce ausgeschlossen.

- Ähnlich wie IPv4 Routen werden IPv6 Routen, die einem VPN-Gateway hinzugefügt wurden, von Client Route Enforce überwacht, während Routen, die zu einem Nicht-VPN-Gateway hinzugefügt wurden, von der Überwachung ausgeschlossen werden.

## Ignorierte Routen

Routen zu den folgenden IPv4 Netzwerken werden von Client Route Enforcement ignoriert:

- 127.0.0.0/8— Reserviert für den lokalen Host
- 169.254.0.0/16— Reserviert für Link-Local-Adressen
- 224.0.0.0/4— Reserviert für Multicast
- 255.255.255.255/32— Reserviert für die Übertragung

Routen zu den folgenden IPv6 Netzwerken werden von Client Route Enforce ignoriert:

- ::1/128— Reserviert für Loopback
- fe80::/10— Reserviert für Link-Local-Adressen
- ff00::/8— Reserviert für Multicast

## Themen

- [Aktivieren Sie Client Route Enforce für einen Endpunkt AWS Client VPN](#)
- [Deaktivieren Sie die Client-Routenerzwingung von einem AWS Client VPN Endpunkt aus](#)
- [Problembehandlung bei IPv6 Client Route Enforcement](#)

## Aktivieren Sie Client Route Enforce für einen Endpunkt AWS Client VPN

Sie können Client Route Enforce auf vorhandenen Client-VPN-Endpunkten entweder über die Konsole oder die AWS CLI aktivieren.

So aktivieren Sie Client Route Enforce 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, den Sie ändern möchten, wählen Sie Aktionen und dann Client-VPN-Endpunkt ändern aus.

4. Scrollen Sie auf der Seite nach unten zum Abschnitt Other Parameters (Weitere Parameter).
5. Aktivieren Sie die Client-Routenerzwingung.
6. Wählen Sie Modify Client VPN Endpoint (Client-VPN-Endpunkt ändern) aus.

Um die Client-Routenerzwingung zu aktivieren, verwenden Sie den AWS CLI)

- Verwenden Sie den [modify-client-vpn-endpoint](#)-Befehl.

## Deaktivieren Sie die Client-Routenerzwingung von einem AWS Client VPN Endpunkt aus

Sie können Client Route Enforcement auf Client-VPN-Endpunkten entweder über die Konsole oder die AWS CLI deaktivieren.

Um Client Route Enforce über die Konsole zu deaktivieren

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 ändern möchten, wählen Sie Aktionen und dann Client-VPN-Endpunkt ändern aus.
4. Scrollen Sie auf der Seite nach unten zum Abschnitt Other Parameters (Weitere Parameter).
5. Schalten Sie die Client-Routenerzwingung aus.
6. Wählen Sie Modify Client VPN Endpoint (Client-VPN-Endpunkt ändern) aus.

Um Client Route Enforcement zu deaktivieren, verwenden Sie AWS CLI

- Verwenden Sie den [modify-client-vpn-endpoint](#)-Befehl.

## Problembehandlung bei IPv6 Client Route Enforcement

Wenn Sie Probleme mit der IPv6 Client-Routenerzwingung haben, sollten Sie die folgenden Schritte zur Fehlerbehebung in Betracht ziehen:

## Überprüfen Sie die Client-Version

Stellen Sie sicher, dass Sie den AWS VPN Client Version 5.3.0 oder höher verwenden, der für die Unterstützung von IPv6 Client Route Enforce erforderlich ist.

## Überprüfen Sie die Endpunktkonfiguration

Stellen Sie sicher, dass auf dem Endpunkt Client Route Enforcement aktiviert ist und dass er für IPv6 Dual-Stack-Verkehr konfiguriert ist.

## Untersuchen Sie die Client-Protokolle

Überprüfen Sie die AWS-VPN-Client-Protokolle auf Fehlermeldungen im Zusammenhang mit IPv6 Client Route Enforcement. Suchen Sie nach Einträgen, die IPv6 "" und „Client Route Enforcement“ oder „CRM“ enthalten.

## Überprüfen Sie die Routing-Tabelle

Verwenden Sie den entsprechenden Befehl für Ihr Betriebssystem, um die IPv6 Routingtabelle anzuzeigen:

- Windows: netsh interface ipv6 show route
- macOS: netstat -rn -f inet6
- Linux: ip -6 route

## Suchen Sie nach widersprüchlichen Routen

Suchen Sie nach IPv6 Routen, die mit den VPN-Routen in Konflikt geraten könnten. Achten Sie besonders auf Routen mit demselben Ziel, aber unterschiedlichen Gateways.

## Überprüfen Sie die ISP-Unterstützung IPv6

Stellen Sie sicher, dass Ihr Internetdienstanbieter (ISP) die Software ordnungsgemäß unterstützt. IPv6

Wenn Sie nach dem Ausführen dieser Schritte zur Fehlerbehebung weiterhin Probleme mit IPv6 Client Route Enforcement haben, wenden Sie sich an den AWS-Support, um weitere Support zu erhalten.

# AWS Client VPN Endpunkte

Alle AWS Client VPN Sitzungen stellen die Kommunikation mit einem Client-VPN-Endpunkt her. Sie können den Client-VPN-Endpunkt verwalten, um Client-VPN-Sitzungen mit diesem Endpunkt zu

erstellen, zu ändern, anzuzeigen und zu löschen. Endpoints können entweder mit der Amazon VPC-Konsole oder mit der CLI erstellt und geändert werden. AWS

## Anforderungen für die Erstellung von Client-VPN-Endpunkten

### Important

Ein Client-VPN-Endpunkt muss in demselben AWS Konto erstellt werden, in dem das vorgesehene Zielnetzwerk bereitgestellt wird. Sie müssen außerdem ein Serverzertifikat und, falls erforderlich, ein Client-Zertifikat generieren. Weitere Informationen finden Sie unter [Client-Authentifizierung in AWS Client VPN](#).

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

- Überprüfen Sie die Regeln und Einschränkungen in [Regeln und bewährte Verfahren für die Verwendung AWS Client VPN](#).
- Generieren Sie das Serverzertifikat und, falls erforderlich, das Client-Zertifikat. Weitere Informationen finden Sie unter [Client-Authentifizierung in AWS Client VPN](#).

## IP-Adresstypen

AWS Client VPN unterstützt Only-, IPv4 IPv6 -only- und Dual-Stack-Konfigurationen sowohl für Endpunktverbindbarkeit als auch für Datenverkehrs-Routing. Die folgende Anleitung hilft Ihnen bei der Auswahl des geeigneten IP-Adresstyps auf der Grundlage der Funktionen Ihres Client-Geräts, der Netzwerkinfrastruktur und der Anwendungsanforderungen.

### Adresstyp des Endpunkts

Der Adresstyp des Endpunkts bestimmt, welche IP-Protokolle Ihr Client-VPN-Endpunkt für Client-Verbindungen unterstützt. Diese Einstellung kann nach der Erstellung des Endpunkts nicht geändert werden.

Wählen Sie IPv4 -nur, wenn:

- Ihre Client-Geräte unterstützen nur IPv4 VPN-Verbindungen
- Ihre Sicherheitstools sind für die IPv4 Verkehrsinspektion optimiert

Wählen Sie „IPv6Nur“, wenn:

- Alle Client-Geräte unterstützen IPv6 Verbindungen in vollem Umfang
- Sie befinden sich in Netzwerken, in denen die IPv4 Adressen erschöpft sind

Wählen Sie Dual-Stack, wenn:

- Sie haben eine Mischung aus Client-Geräten mit unterschiedlichen IP-Funktionen
- Sie wechseln schrittweise von zu IPv4 IPv6

## Art der IP-Adresse für den Verkehr

Der Verkehrs-IP-Adresstyp steuert, wie Client VPN den Verkehr zwischen Clients und Ihren VPC-Ressourcen weiterleitet, unabhängig von den unterstützten Protokollen des Endpunkts.

Leiten Sie den Verkehr so weiter, IPv4 wenn:

- Unterstützung nur für Zielanwendungen in Ihrer VPC IPv4
- Sie haben komplexe IPv4 Sicherheitsgruppen und ein komplexes Netzwerk ACLs
- Sie stellen eine Verbindung zu älteren Systemen her

Leiten Sie den Verkehr so weiter IPv6 , wie wenn:

- Ihre VPC-Infrastruktur ist in erster Linie IPv6
- Sie möchten Ihre Netzwerkarchitektur zukunftssicher machen
- Sie haben moderne Anwendungen entwickelt für IPv6

## Änderung von Endpunkten

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)
- Zertifikatsperlliste (CRL)
- Autorisierungsregeln
- Die VPC- und Sicherheitsgruppenzuordnungen
- Die VPN-Portnummer
- Die Self-Service-Portal-Option
- Die maximale VPN-Sitzungsdauer
- Aktivieren oder deaktivieren Sie die automatische Wiederverbindung bei Sitzungs-Timeout
- 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-Zertifikatsperlliste (Certificate Revocation List, CRL).

Sie können den IPv4 CIDR-Bereich des Clients, die Authentifizierungsoptionen, das Client-Zertifikat oder das Transportprotokoll nicht 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)
- Zertifikatsperlliste (CRL)
- Autorisierungsregeln
- Die VPN-Portnummer

## Aufgaben

- [Einen AWS Client VPN Endpunkt erstellen](#)
- [AWS Client VPN Endpunkte anzeigen](#)
- [Einen AWS Client VPN Endpunkt ändern](#)
- [Löschen Sie einen AWS Client VPN Endpunkt](#)

## Einen AWS Client VPN Endpunkt erstellen

Erstellen Sie einen AWS Client VPN Endpunkt, damit Ihre Kunden eine VPN-Sitzung entweder mit der Amazon VPC-Konsole oder der Amazon VPC-Konsole einrichten können. AWS CLI Client VPN unterstützt bei der ersten Erstellung alle Kombinationen von Endpunkttypen (Split-Tunnel und Full-Tunnel) mit Datenverkehrstyp (IPv4 IPv6, und Dual-Stack).

Machen Sie sich mit den Anforderungen vertraut, bevor Sie einen Endpunkt erstellen. Weitere Informationen finden Sie unter [the section called “Anforderungen für die Erstellung von Client-VPN-Endpunkten”](#).

So erstellen Sie einen 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. (Optional) Geben Sie ein Namens-Tag und eine Beschreibung für den Client-VPN-Endpunkt ein.
4. Wählen Sie als Endpunkt-IP-Adresstyp den IP-Adresstyp für den Endpunkt aus:
  - IPv4: Der Endpunkt verwendet IPv4 Adressen für den externen VPN-Tunnelverkehr.
  - IPv6: Der Endpunkt verwendet IPv6 Adressen für den externen VPN-Tunnelverkehr.
  - Dual-Stack: Der Endpunkt verwendet IPv4 sowohl IPv6 Adressen als auch Adressen für den externen VPN-Tunnelverkehr.
5. Wählen Sie unter Verkehrs-IP-Adresstyp den IP-Adresstyp für den Datenverkehr aus, der über den Endpunkt fließt:
  - IPv4: Der Endpunkt unterstützt nur IPv4 Datenverkehr.
  - IPv6: Der Endpunkt unterstützt nur IPv6 Verkehr.
  - Dual-Stack: Der Endpunkt unterstützt IPv4 sowohl IPv6 Datenverkehr als auch.

6. Geben Sie für Client IPv4 CIDR einen IP-Adressbereich in CIDR-Notation an, aus dem Client-IP-Adressen zugewiesen werden sollen. Beispiel, 10.0.0.0/22. Dies ist erforderlich, wenn Sie für den IP-Adressstyp Traffic IPv4 oder Dual-Stack ausgewählt haben.

 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.
- Wenn Sie IPv6 als Endpunkt-IP-Adressstyp auswählen, ist das Feld Client IPv4 CIDR deaktiviert. Der Client-VPN-Endpunkt weist IPv6 Clientadressen aus einem zugehörigen Subnetz zu, und Sie können das Subnetz zuordnen, nachdem Sie den Endpunkt erstellt haben.

 Note

Für den IPv6 Datenverkehr müssen Sie keinen Client-CIDR-Bereich angeben. Amazon weist Kunden automatisch IPv6 CIDR-Bereiche zu.

7. 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 vorhanden sein, in der Sie den Client-VPN-Endpunkt erstellen. Das Zertifikat kann entweder mit ACM bereitgestellt oder in ACM importiert werden.

Die Schritte zum Bereitstellen oder Importieren eines Zertifikats in ACM finden Sie unter [AWS Certificate Manager Zertifikate](#) im AWS Certificate Manager Benutzerhandbuch.

8. 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.

- Um die gegenseitige Zertifikatsauthentifizierung zu verwenden, wählen Sie Gegenseitige Authentifizierung verwenden aus, und geben Sie dann für Client-Zertifikat-ARN den ARN des Client-Zertifikats an, das in AWS Certificate Manager (ACM) bereitgestellt wird.

#### 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.

- (Optional) Geben Sie für die Verbindungsprotokollierung an, ob Daten über Client-Verbindungen 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 Logs-Protokollgruppenname den Namen der zu verwendenden Protokollgruppe ein. Geben Sie CloudWatch unter Log-Log-Stream-Name den Namen des Log-Streams ein, der verwendet werden soll, oder lassen Sie diese Option leer, damit wir einen Log-Stream für Sie erstellen können.
- (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.

11. (Optional) Geben Sie an, welche DNS-Server für die DNS-Auflösung verwendet werden sollen. Um benutzerdefinierte DNS-Server zu verwenden, geben Sie für DNS-Server-1-IP-Adresse und DNS-Server-2-IP-Adresse die IPv4 Adressen der zu verwendenden DNS-Server an. Für IPv6 oder Dual-Stack-Endpunkte können Sie auch die Adressen für DNS-Server IPv6 1 und DNS-Server IPv6 2 angeben. 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.

12. (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.

13. (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.
14. (Optional) Wählen Sie unter VPC ID die VPC, die dem Client-VPN-Endpunkt zugeordnet werden soll. Wählen Sie für Sicherheitsgruppe IDs eine oder mehrere Sicherheitsgruppen der VPC aus, die auf den Client-VPN-Endpunkt angewendet werden sollen.
15. (Optional) Wählen Sie für VPN Port die VPN-Portnummer. Der Standardwert ist 443.
16. (Optional) Um eine [Self-Service-Portal-URL](#) für Kunden zu generieren, aktivieren Sie Enable self-service portal (Self-Service-Portal aktivieren).
17. (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.
18. (Optional) Wählen Sie unter Verbindung bei Sitzungtimeout trennen aus, ob Sie die Sitzung beenden möchten, wenn die maximale Sitzungszeit erreicht ist. Wenn Sie diese Option wählen,

müssen Benutzer manuell erneut eine Verbindung zum Endpunkt herstellen, wenn die Sitzung abgelaufen ist. Andernfalls versucht Client VPN automatisch, die Verbindung wiederherzustellen.

19. (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.
20. 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 Clients an, den AWS bereitgestellten Client oder eine andere OpenVPN-basierte Client-Anwendung 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 mit dem AWS CLI

Verwenden Sie den [create-client-vpn-endpoint](#)-Befehl.

Beispiel für die Erstellung eines IPv4 Endpunkts:

```
aws ec2 create-client-vpn-endpoint \
--client-cidr-block "172.31.0.0/16" \
--server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
--authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
--connection-log-options Enabled=false
```

## Beispiel für die Erstellung eines IPv6 Endpunkts:

```
aws ec2 create-client-vpn-endpoint \
--endpoint-ip-address-type "ipv6" \
--traffic-ip-address-type "ipv6" \
--server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
--authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
--connection-log-options Enabled=false
```

## Beispiel für die Erstellung eines Dual-Stack-Endpunkts:

```
aws ec2 create-client-vpn-endpoint \
--endpoint-ip-address-type "dual-stack" \
--traffic-ip-address-type "dual-stack" \
--client-cidr-block "172.31.0.0/16" \
--server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
--authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
--connection-log-options Enabled=false
```

## AWS Client VPN Endpunkte anzeigen

Sie können Informationen zu Client-VPN-Endpunkten mit der Amazon VPC-Konsole oder dem anzeigen. AWS CLI

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 (Autorsierungsregeln), 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.

## Einen AWS Client VPN Endpunkt ändern

Sie können einen Client-VPN-Endpunkt mithilfe der Amazon VPC-Konsole oder der AWS CLI ändern. Weitere Informationen zu den Feldern, die Sie bearbeiten können, finden Sie unter [the section called "Änderung des Endpunkts"](#).

### Einschränkungen

Bei der Änderung eines Endpunkts gelten die folgenden Einschränkungen

- 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-Zertifikatsperlliste (Certificate Revocation List, CRL).
- Sie können den IPv4 CIDR-Bereich des Clients, die Authentifizierungsoptionen, das Client-Zertifikat oder das Transportprotokoll nicht ändern, nachdem der Client-VPN-Endpunkt erstellt wurde.
- Sie können bestehende IPv4 Endpunkte sowohl für Endpunkt-IP- als auch für Verkehrs-IP-Typen auf Dual-Stack umstellen. Wenn Sie IPv6 -nur für Endpunkt-IP und Traffic-IP benötigen, müssen Sie einen neuen Endpunkt erstellen.
- Client VPN unterstützt keine Änderung des Endpunkttyps (IPv4, IPv6, Dual-Stack) oder des Datenverkehrstyps (IPv4, IPv6, Dual-Stack) nach der Erstellung.
- Das Ändern eines Client VPN mit einer bestimmten Kombination aus Endpunkttyp und Verkehrstyp wird nicht unterstützt. Sie können nicht zu einer anderen Kombination wechseln. Der Endpunkt muss gelöscht und mit der gewünschten Konfiguration neu erstellt werden.
- Client-to-client Die Kommunikation für IPv6 den Verkehr wird nicht unterstützt.

### Ändern eines Client-VPN-Endpunkts

Sie können einen Client-VPN-Endpunkt entweder mit der Konsole oder dem AWS CLI.

## So ändern Sie einen Client-VPN-Endpunkt 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 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. Für den Endpunkt-IP-Adresstyp können Sie einen vorhandenen IPv4 Endpunkt in Dual-Stack ändern. Diese Option ist nur für IPv4 Endpunkte verfügbar.
6. Für den IP-Adresstyp Traffic können Sie einen vorhandenen IPv4 Endpunkt in einen Dual-Stack-Endpunkt ändern. Diese Option ist nur für IPv4 Endpunkte verfügbar.
7. 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 vorhanden sein, in der Sie den Client-VPN-Endpunkt erstellen. Das Zertifikat kann entweder mit ACM bereitgestellt oder in ACM importiert werden.

8. Geben Sie an, ob Daten über Client-Verbindungen mithilfe von 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 unter CloudWatch Logs-Protokollgruppenname den Namen der zu verwendenden Protokollgruppe aus. Wählen Sie unter Name des CloudWatch Protokolldatenstroms den Namen des zu verwendenden Log-Streams aus, oder lassen Sie diese Option leer, damit wir einen Log-Stream 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).

9. 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.
10. Aktivieren oder deaktivieren Sie die Option Enable DNS servers (DNS-Server aktivieren). Um benutzerdefinierte DNS-Server zu verwenden, geben Sie für DNS-Server-1-IP-Adresse und DNS-Server-2-IP-Adresse die IPv4 Adressen der zu verwendenden DNS-Server an. Für IPv6 oder Dual-Stack-Endpunkte können Sie auch die Adressen für DNS-Server IPv6 1 und DNS-Server IPv6 2 angeben. 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.

11. Aktivieren oder deaktivieren Sie die Option Enable split-tunnel (Split-Tunnel aktivieren). Standardmäßig ist Split Tunneling auf einem VPN-Endpunkt deaktiviert.
12. Wählen Sie unter VPC ID die VPC aus, die dem Client-VPN-Endpunkt zugeordnet werden soll. Wählen Sie für Sicherheitsgruppe IDs eine oder mehrere Sicherheitsgruppen der VPC aus, die auf den Client-VPN-Endpunkt angewendet werden sollen.
13. Wählen Sie für VPN Port die VPN-Portnummer. Der Standardwert ist 443.
14. Um eine [Self-Service-Portal-URL](#) für Kunden zu generieren, aktivieren Sie Enable self-service portal (Self-Service-Portal aktivieren).
15. 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.
16. Wählen Sie für Disconnect on session timeout aus, ob Sie die Sitzung beenden möchten, wenn die maximale Sitzungszeit erreicht ist. Wenn Sie diese Option wählen, müssen Benutzer manuell erneut eine Verbindung zum Endpunkt herstellen, wenn die Sitzung abgelaufen ist. Andernfalls versucht Client VPN automatisch, die Verbindung wiederherzustellen.
17. 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.

## 18. Wählen Sie Modify Client VPN endpoint (Client-VPN-Endpunkt ändern) aus.

Um einen Client-VPN-Endpunkt mit dem zu ändern AWS CLI

Verwenden Sie den [modify-client-vpn-endpoint](#)-Befehl.

Beispiel für die Änderung eines IPv4 Endpunkts auf Dual-Stack:

```
aws ec2 modify-client-vpn-endpoint \
--client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
--endpoint-ip-address-type "dual-stack" \
--traffic-ip-address-type "dual-stack" \
--client-cidr-block "172.31.0.0/16"
```

## Löschen Sie einen AWS Client VPN Endpunkt

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.

## AWS Client VPN Verbindungsprotokolle

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

Verbindungsprotokolle zeigen die Reihenfolge der Protokollereignisse für den Client-VPN-Endpunkt. 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. In der Verbindungsprotokollierung werden dann die folgenden Informationen protokolliert: Verbindungsanfragen des Clients, Ergebnisse der Client-Verbindung (erfolgreich oder nicht erfolgreich), Gründe für erfolglose Verbindungsergebnisse und Zeitpunkt der Client-Beendigung vom Endpunkt aus.

Bevor Sie beginnen, muss Ihr Konto über eine Protokollgruppe „CloudWatch Protokolle“ verfügen. Weitere Informationen finden Sie unter [Arbeiten mit Protokollgruppen und Protokollstreams](#) im Amazon CloudWatch Logs-Benutzerhandbuch. Für die Nutzung von CloudWatch Logs fallen Gebühren an. Weitere Informationen finden Sie unter [CloudWatch Amazon-Preise](#).

Client-VPN-Verbindungsprotokolle können entweder mit der Amazon VPC-Konsole oder der AWS CLI erstellt werden.

## Aufgaben

- [Aktivieren der Verbindungsprotokollierung für einen neuen AWS Client VPN -Endpunkt](#)
- [Verbindungsprotokollierung für einen vorhandenen AWS Client VPN -Endpunkt aktivieren](#)
- [AWS Client VPN Verbindungsprotokolle anzeigen](#)
- [AWS Client VPN Verbindungsprotokollierung ausschalten](#)

## Aktivieren der Verbindungsprotokollierung für einen neuen AWS 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 [Einen AWS Client VPN Endpunkt erstellen](#).

4. Aktivieren Sie unter Connection logging (Verbindungsprotokollierung) die Option Enable log details on client connections (Protokolldetails für Client-Verbindungen aktivieren).
5. Wählen Sie unter Name der CloudWatch Logs-Protokollgruppe den Namen der CloudWatch Logs-Protokollgruppe aus.
6. (Optional) Wählen Sie unter Name des CloudWatch Logs-Log-Streams den Namen des CloudWatch Logs-Log-Streams aus.
7. Wählen Sie Create Client VPN endpoint (Client-VPN-Endpunkt erstellen) aus.

Um die Verbindungsprotokollierung für einen neuen Client-VPN-Endpunkt zu aktivieren, verwenden Sie den AWS CLI

Verwenden Sie den [create-client-vpn-endpoint](#)Befehl 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"  
}
```

## Verbindungsprotokollierung für einen vorhandenen AWS Client VPN - Endpunkt aktivieren

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 Name der CloudWatch Logs-Protokollgruppe den Namen der CloudWatch Logs-Protokollgruppe aus.
6. (Optional) Wählen Sie unter Name des CloudWatch Logs-Log-Streams den Namen des CloudWatch Logs-Log-Streams 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 [modify-client-vpn-endpoint](#)-Befehl 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"  
}
```

## AWS Client VPN Verbindungsprotokolle anzeigen

Sie können Ihre Client-VPN-Verbindungsprotokolle in 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 Zeitstempel wird die Zeit angezeigt, zu der das Verbindungsprotokoll in CloudWatch Logs veröffentlicht wurde, nicht die Uhrzeit der Verbindung.

Weitere Informationen zum Durchsuchen von Protokolldaten finden Sie unter [Suchen von Protokolldaten mithilfe von Filtermustern](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

## AWS Client VPN Verbindungsprotokollierung ausschalten

Sie können die Verbindungsprotokollierung für einen Client-VPN-Endpunkt über die Konsole oder die Befehlszeile deaktivieren. Wenn Sie die Verbindungsprotokollierung deaktivieren, werden bestehende CloudWatch Verbindungsprotokolle in den Protokollen 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.

Um die Verbindungsprotokollierung zu deaktivieren, verwenden Sie AWS CLI

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

## AWS Client VPN Export von Endpunktkonfigurationsdateien

Die AWS Client VPN Endpunktkonfigurationsdatei ist die Datei, die Clients (Benutzer) verwenden, 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 Kunden alternativ beim Portal anmelden und die Konfigurationsdatei selbst herunterladen. Weitere Informationen finden Sie unter [AWS Client VPN Zugang zum 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 Wildcard-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.

### Aufgaben

- [Exportieren Sie die AWS Client VPN Client-Konfigurationsdatei](#)
- [Fügen Sie das AWS Client VPN Client-Zertifikat und die Schlüsselinformationen für die gegenseitige Authentifizierung hinzu](#)

## Exportieren Sie die AWS Client VPN Client-Konfigurationsdatei

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

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 AWS Client VPN Client-Zertifikat und die Schlüsselinformationen für die 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. */path* Ersetzen Sie es durch den Speicherort des Client-Zertifikats und des Schlüssels (der Standort 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-0011abcabcabc1.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
```

## AWS Client VPN Routen

Jeder AWS Client VPN Endpunkt hat eine Routentabelle, in der die verfügbaren Zielnetzwerkrouuten beschrieben werden. 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 zu ermöglichen, z. B. lokale VPCs Peering-Netzwerke, das lokale Netzwerk (damit Clients miteinander kommunizieren können) oder das Internet, müssen Sie der Routentabelle 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 [Fehlerbehebung AWS Client VPN](#):

Der Zugriff auf eine Peer-VPC, Amazon S3 oder das Internet ist unterbrochen beschrieben.

Jedes zugeordnete Subnetz sollte einen identischen Satz von Routen aufweisen.

## Überlegungen zur Verwendung von 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.

### Aufgaben

- [Erstellen Sie eine AWS Client VPN Endpunktroute](#)
- [AWS Client VPN EndpunktRoutes anzeigen](#)
- [Löschen Sie eine AWS Client VPN Endpunktroute](#)

## Erstellen Sie eine AWS Client VPN Endpunktroute

Wenn Sie eine Client-VPN-Endpunktroute erstellen, geben Sie an, wie der Verkehr 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 unter Routenziele den IPv4 CIDR-Bereich für das Zielnetzwerk an. Beispiel:

- Um eine Route für die VPC des Client-VPN-Endpunkts hinzuzufügen, geben Sie den IPv4 CIDR-Bereich der VPC ein.
  - Um eine Route für den Internetzugang hinzuzufügen, geben Sie `0.0.0.0/0` ein.
  - Um eine Route für eine gepeerte VPC hinzuzufügen, geben Sie den CIDR-Bereich der gepeerten VPC ein. IPv4
  - Um eine Route für ein lokales Netzwerk hinzuzufügen, geben Sie den CIDR-Bereich der AWS Site-to-Site VPN-Verbindung ein. IPv4
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 [create-client-vpn-route](#)-Befehl.

## AWS Client VPN Endpunkttrouten anzeigen

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 [describe-client-vpn-routes](#)-Befehl.

## Löschen Sie eine AWS Client VPN Endpunktroute

Sie können nur Client-VPN-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 [delete-client-vpn-route](#)-Befehl.

## AWS Client VPN Zielnetzwerke

Ein Zielnetzwerk ist ein Subnetz in einer VPC. Ein AWS Client VPN Endpunkt muss über mindestens ein Zielnetzwerk verfügen, damit Clients eine Verbindung zu ihm herstellen und eine VPN-Verbindung herstellen können.

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

## Client-VPN-Zielnetzwerkanforderungen

Bei der Erstellung eines Zielnetzwerks gelten die folgenden Regeln:

- 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-Endpoint 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-Endpoint 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-Endpoint modifizieren, indem Sie die ihm zugeordnete VPC ändern. Weitere Informationen finden Sie unter [Einen AWS Client VPN Endpunkt ändern](#).

Wenn Sie ein Subnetz mit einem Client VPN-Endpoint 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 wurden und Sie weitere CIDRs zu Ihrer angeschlossenen VPC hinzufügen oder entfernen, müssen Sie einen der folgenden Schritte ausführen, um die lokale Route für Ihre Client-VPN-Endpoint-Routentabelle zu aktualisieren:

- Trennen Sie Ihren Client-VPN-Endpoint vom Zielnetzwerk und verknüpfen Sie dann den Client-VPN-Endpoint 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-Endpoint verknüpft haben, ändert sich der Status des Client VPN-Endpunkts von pending-associate in available, und Clients können eine VPN-Verbindung herstellen.

#### Aufgaben

- [Verknüpfen Sie ein Zielnetzwerk mit einem AWS Client VPN Endpunkt](#)
- [Wenden Sie eine Sicherheitsgruppe auf ein Zielnetzwerk an in AWS Client VPN](#)

- [AWS Client VPN Zielnetzwerke anzeigen](#)
- [Trennen Sie die Zuordnung eines Zielnetzwerks zu einem Endpunkt AWS Client VPN](#)

## Verknüpfen Sie ein Zielnetzwerk mit einem AWS Client VPN Endpunkt

Sie können einem Client-VPN-Endpunkt über die Amazon VPC-Konsole oder die CLI ein oder mehrere Zielnetzwerke (Subnetze) zuordnen. AWS Machen Sie sich mit den Anforderungen vertraut, bevor Sie ein Zielnetzwerk mit einem Client-VPN-Endpunkt verknüpfen. Siehe [Anforderungen für die Erstellung eines Zielnetzwerks.](#)

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](#).

## Wenden Sie eine Sicherheitsgruppe auf ein Zielnetzwerk an in AWS Client VPN

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 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 Sicherheitsgruppe aus IDs.
6. Wählen Sie Apply Security Groups (Sicherheitsgruppen anwenden) aus.

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

Verwenden Sie den client-vpn-target-network Befehl [apply-security-groups-to-](#).

## AWS Client VPN Zielnetzwerke anzeigen

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.

Um Zielnetzwerke mit dem anzeigen AWS CLI

Verwenden Sie den Befehl [describe-client-vpn-target-networks](#).

## Trennen Sie die Zuordnung eines Zielnetzwerks zu einem Endpunkt AWS Client VPN

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](#).

## AWS Client VPN Timeout für die maximale Dauer der VPN-Sitzung

AWS Client VPN bietet mehrere Optionen für die maximale VPN-Sitzungsdauer, d. h. die maximal zulässige Zeit für eine Client-Verbindung zum Client-VPN-Endpunkt. Sie können eine kürzere maximale VPN-Sitzungsdauer konfigurieren, um die Sicherheits- und Compliance-Anforderungen zu erfüllen. Die Sitzungsdauer beträgt standardmäßig 24 Stunden. Sobald Sie die maximale Sitzungsdauer festgelegt haben, können Sie steuern, was mit der Sitzung passiert, wenn diese Zeitüberschreitung erreicht ist. Mit der Option „Verbindung bei Sitzungstimeout trennen“ können Sie die Sitzung beenden oder automatisch versuchen, eine erneute Verbindung zum Endpunkt herzustellen. Wenn Sie eine Sitzung beenden, haben Sie mehr Kontrolle über die Endpunktssicherheit, indem Sie die maximale VPN-Sitzungsdauer durchsetzen. Wenn eine Sitzung so eingestellt ist, dass sie beendet wird, wenn die maximale Zeit erreicht ist, müssen Benutzer erneut eine Verbindung herstellen und ihre Authentifizierungsdaten angeben, um die VPN-Verbindung wiederherzustellen.

Wenn „Trennen bei Sitzungstimeout“ so eingestellt ist, dass die Verbindung automatisch wiederhergestellt wird und die maximale Sitzungszeit erreicht ist,

- Bei zwischengespeicherten Benutzeranmeldeinformationen (Active Directory) oder zertifikatsbasierter Authentifizierung (Mutual Authentication) wird automatisch eine neue Sitzung eingerichtet. Um die Verbindung vollständig zu trennen und nicht automatisch wieder herzustellen, sollten diese Benutzer die Verbindung manuell trennen.
- Bei der Verbundauthentifizierung (SAML) wird nicht automatisch eine neue Sitzung eingerichtet. Diese Benutzer müssen sich nach Ablauf des Sitzungstimeouts erneut authentifizieren, um die VPN-Verbindung wiederherzustellen.

 Note

- Wenn der Wert für die maximale VPN-Sitzungsdauer gegenüber dem aktuellen Wert verringert wird, werden alle aktiven VPN-Sitzungen, die länger als die neu festgelegte Dauer mit dem Endpunkt verbunden sind, getrennt.
- Wenn Sie die Option „Verbindung bei Sitzungstimeout trennen“ ändern, wird die neue Einstellung auf alle derzeit geöffneten Sitzungen angewendet.

## Konfigurieren Sie die maximale VPN-Sitzung bei der Erstellung eines Endpunkts AWS Client VPN

Die Dauer einer VPN-Sitzung wird bei der Erstellung eines Client-VPN-Endpunkts konfiguriert. Die Schritte [Einen AWS Client VPN Endpunkt erstellen](#) zum Erstellen eines Client-VPN-Endpunkts und zum Festlegen der maximalen Sitzungsdauer finden Sie unter.

### Aufgaben

- [AWS Client VPN Aktuelle maximale VPN-Sitzungsdauer anzeigen](#)
- [Ändern Sie die maximale AWS Client VPN Sitzungsdauer und das Timeout-Verhalten](#)

## AWS Client VPN Aktuelle maximale VPN-Sitzungsdauer anzeigen

Gehen Sie wie folgt vor, um die aktuelle maximale VPN-Sitzungsdauer für Client-VPN 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. Sehen Sie sich die aktuelle maximale VPN-Sitzungsdauer neben den Stunden für das Sitzungs-Timeout an und ob „Verbindung bei Timeout trennen“ aktiviert oder deaktiviert ist.

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

Verwenden Sie den [describe-client-vpn-endpoints](#)-Befehl.

## Ändern Sie die maximale AWS Client VPN Sitzungsdauer und das Timeout-Verhalten

Gehen Sie wie folgt vor, um die maximale Dauer einer bestehenden Client-VPN-Sitzung zu ändern und das Verhalten beim Trennen bei Sitzungstimeout 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 für Verbindung bei Sitzungstimeout aus, ob Sie eine Sitzung trennen möchten, wenn das maximale Sitzungstimeout erreicht ist. Standardmäßig ist dies deaktiviert, wenn Sie einen Endpunkt zum ersten Mal ändern.
6. 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 [modify-client-vpn-endpoint](#)-Befehl.

# Sicherheit in AWS Client VPN

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

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

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

AWS Client VPN ist Teil des Amazon VPC-Service. 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 lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Client-VPN-Ressourcen zu überwachen und zu sichern.

## Themen

- [Datenschutz in AWS Client VPN](#)
- [Identitäts- und Zugriffsmanagement für AWS Client VPN](#)
- [Resilienz in AWS Client VPN](#)
- [Infrastruktursicherheit in AWS Client VPN](#)
- [Bewährte Sicherheitsmethoden für AWS Client VPN](#)
- [IPv6 Überlegungen für AWS Client VPN](#)

# Datenschutz in AWS Client VPN

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

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

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

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Client VPN oder anderen Geräten arbeiten und die Konsole, die API oder AWS-Services verwenden AWS SDKs. AWS CLI 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 sichere Verbindungen von jedem Standort aus mithilfe von Transport Layer Security (TLS) 1.2 oder höher.

## 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 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 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](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Client VPN funktioniert mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Client VPN](#)
- [Problembehandlung bei AWS Client VPN Identität und Zugriff](#)
- [Verwenden von serviceverknüpften Rollen für AWS Client VPN](#)

## Zielgruppe

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 Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern 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. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Client VPN verwenden kann, finden Sie unter [Wie AWS Client VPN funktioniert 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 AWS Client VPN](#).

## Authentifizierung mit Identitäten

Bei der Authentifizierung melden Sie sich AWS mit Ihren Identitätsdaten an. 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-Managementkonsole 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 zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter [AWS Signature Version 4 für API-Anforderungen](#) im IAM-Benutzerhandbuch.

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

## AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-

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

## Verbundidentität

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

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

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

## IAM-Benutzer und -Gruppen

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

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

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen permanente langfristige Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

## IAM roles

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

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

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

gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

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

[IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.](#)

## Verwalten des Zugriffs mit Richtlinien

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

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

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

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

### Identitätsbasierte Richtlinien

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

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe

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

## Ressourcenbasierte Richtlinien

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

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

## Zugriffskontrolllisten () ACLs

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

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

## Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer

IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld **Principal** angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter [Resource Control Policies \(RCPs\)](#) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

## Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird,

ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

## Wie AWS Client VPN funktioniert 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
<a href="#">Identitätsbasierte Richtlinien</a>	Ja
<a href="#">Ressourcenbasierte Richtlinien</a>	Nein
<a href="#">Richtlinienaktionen</a>	Ja
<a href="#">Richtlinienressourcen</a>	Ja
<a href="#">Richtlinienbedingungsschlüssel (services spezifisch)</a>	Ja
<a href="#">ACLs</a>	Nein
<a href="#">ABAC (Tags in Richtlinien)</a>	Ja
<a href="#">Temporäre Anmeldeinformationen</a>	Ja
<a href="#">Prinzipalberechtigungen</a>	Ja
<a href="#">Servicerollen</a>	Ja
<a href="#">Service-verknüpfte Rollen</a>	Ja

## 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 [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

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

### Beispiele für identitätsbasierte Richtlinien für Client VPN

Beispiele für identitätsbasierte Richtlinien für Client VPN finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Client VPN](#).

### 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 [Kontoübergreifender 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 Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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

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

Eine Liste der Client-VPN-Aktionen finden Sie unter [Von AWS Client VPN definierte Aktionen](#) in der Serviceauthorisierungsreferenz.

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

ec2

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

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

Beispiele für identitätsbasierte Client-VPN-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Client VPN](#).

## Richtlinienressourcen für Client VPN

Unterstützt Richtlinienressourcen: Ja

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

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

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

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

Eine Liste der Client-VPN-Ressourcentypen und ihrer ARNs Typen finden Sie unter [Von AWS Client VPN definierte Ressourcen](#) in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen 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 AWS Client VPN](#).

## Richtlinienbedingungsschlüssel für Client VPN

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: 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 AWS Client VPN](#).

## ACLs im Client VPN

Unterstützt ACLs: Nein

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

## ABAC mit Client VPN

Unterstützt ABAC (Tags in Richtlinien): Ja

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

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

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

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

Weitere Informationen zu ABAC finden Sie unter [Definieren von Berechtigungen mit ABAC-Autorisierung](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

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

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

## Serviceübergreifende Principalberechtigungen 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.

## Serviceverknüpfte Rollen für Client VPN

Unterstützt dienstbezogene Rollen: Ja

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

## Beispiele für identitätsbasierte Richtlinien für AWS Client VPN

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

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

Einzelheiten zu den von Client VPN definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Client VPN](#) in der Service Authorization Reference.

## Themen

- [Bewährte Methoden für Richtlinien](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

## 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 Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie 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. Dies ist möglich, indem Sie die Aktionen definieren, die unter bestimmten Bedingungen für bestimmte Ressourcen ausgeführt werden können. Dies wird auch als Berechtigungen mit geringsten Rechten bezeichnet. 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 anzugeben, dass alle Anforderungen mit 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. CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.

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

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

## 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 durchzuführen: 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 durchzuführen: 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. Um die Aktion ausführen zu können, benötigt der Service jedoch Berechtigungen, die von einer 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. Für Dienste, die ressourcenbasierte Richtlinien oder

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

Weitere Informationen finden Sie hier:

- Informationen dazu, ob Client VPN diese Funktionen unterstützt, finden Sie unter [Wie AWS Client VPN funktioniert mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen in AWS-Konten Ihrem Besitz gewähren können, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto, dem Sie gehören](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourenzugriff in IAM](#) im IAM-Benutzerhandbuch.

## Verwenden von serviceverknüpften Rollen für AWS Client VPN

AWS Client VPN verwendet AWS Identity and Access Management (IAM) dienstgebundene Rollen. Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, die direkt mit Client VPN verknüpft ist. Dienstbezogene Rollen sind von Client VPN vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

### Themen

- [Rollen verwenden für AWS Client VPN](#)
- [Verwendung von Rollen für die Verbindungsauthorisierung in Client VPN;](#)

## Rollen verwenden für AWS Client VPN

AWS Client VPN verwendet AWS Identity and Access Management (IAM) dienstgebundene Rollen. Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, die direkt mit Client VPN verknüpft ist. Dienstbezogene Rollen sind von Client VPN vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

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.

#### Berechtigungen von serviceverknüpften Rollen für Client VPN

Client-VPN verwendet die dienstverknüpfte Rolle `AWSServiceRoleForClientVPN` — Erlaube Client VPN, Ressourcen im Zusammenhang mit Ihren VPN-Verbindungen zu erstellen und zu verwalten.

Die mit dem `AWSServiceRoleForClientVPN`-Dienst verknüpfte Rolle vertraut darauf, dass der folgende Dienst die Rolle übernimmt:

- `clientvpn.amazonaws.com`

Diese dienstverknüpfte Rolle verwendet den verwalteten Policy-Client. `VPNService RolePolicy` Die Berechtigungen für diese Richtlinie finden Sie unter [Client VPNService RolePolicy](#) in der Referenz für AWS verwaltete Richtlinien.

#### Eine serviceverknüpfte Rolle für Client VPN erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie den ersten Client-VPN-Endpunkt in Ihrem Konto mit der AWS-Managementkonsole, der oder der AWS CLI AWS API erstellen, erstellt Client VPN die dienstverknüpfte 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.

#### Eine dienstverknüpfte Rolle für Client VPN bearbeiten

Client VPN erlaubt es Ihnen nicht, die mit dem `AWSService RoleForClient VPN`-Dienst verknüpfte Rolle zu bearbeiten. 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 Beschreibung einer dienstbezogenen Rolle](#) im IAM-Benutzerhandbuch.

Löschen Sie eine dienstverknüpfte Rolle für Client VPN

Wenn Sie Client VPN nicht mehr verwenden müssen, empfehlen wir Ihnen, die mit dem AWSServiceRoleForClientVPN-Dienst verknüpfte Rolle 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.

Verwendung von Rollen für die Verbindungsauthorisierung in Client VPN;

AWS Client VPN verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, die direkt mit Client VPN verknüpft ist. Dienstbezogene Rollen sind von Client VPN vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

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.

Berechtigungen von serviceverknüpften Rollen für Client VPN

Client VPN verwendet die dienstverknüpfte Rolle mit dem Namen AWSServiceRoleForClientVPNConnections— Service Linked Role für Client-VPN-Verbindungen.

Die AWSService RoleForClient VPNCOnnections dienstgebundene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `clientvpn-connections.amazonaws.com`

Die Rollenberechtigungsrichtlinie mit dem Namen Client VPNService ConnectionsRolePolicy ermöglicht es Client-VPN, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- 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 serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

### Eine serviceverknüpfte Rolle für Client VPN erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie den ersten Client-VPN-Endpunkt in Ihrem Konto mit der AWS-Managementkonsole, der oder der AWS CLI AWS API erstellen, erstellt Client VPN die dienstverknüpfte 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.

### Eine dienstverknüpfte Rolle für Client VPN bearbeiten

Client VPN erlaubt es Ihnen nicht, die AWSService RoleForClient VPNCollections dienstverknüpfte Rolle zu bearbeiten. 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 Beschreibung einer dienstbezogenen Rolle](#) im IAM-Benutzerhandbuch.

### Löschen Sie eine dienstverknüpfte Rolle für Client VPN

Wenn Sie Client VPN nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForClientVPNCollectionsdienstverknüpfte Rolle 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 im IAM-Benutzerhandbuch unter [Löschen einer serviceverknüpften Rolle](#).

## Resilienz in AWS Client VPN

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

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

Zusätzlich zur AWS globalen Infrastruktur AWS Client VPN bietet es Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

## 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 einem Client VPN-Endpunkt zuordnen, um eine hohe Verfügbarkeit zu gewährleisten.

## Infrauktursicherheit in AWS Client VPN

Als verwalteter Dienst ist AWS Client VPN durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrauktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden 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 Systeme 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 Sicherheitsmethoden für AWS Client VPN

AWS Client VPN bietet 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-Zertifikatsperllisten

Sie können Client-Zertifikatsperllisten 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-Zertifikatsperllisten](#).

### Trennen Sie die Verbindung bei Sitzungs-Timeout

Trennen Sie eine Sitzung, wenn die maximale Client-VPN-Sitzungszeit erreicht ist, wodurch eine maximale VPN-Sitzungsdauer erzwungen wird. Weitere Informationen finden Sie unter [Maximale Dauer der VPN-Sitzung](#).

### Überwachungstools

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

## Identity and Access Management

Verwalten Sie den Zugriff auf Client-VPN-Ressourcen und APIs verwenden Sie IAM-Richtlinien für Ihre IAM-Benutzer und IAM-Rollen. Weitere Informationen finden Sie unter [Identitäts- und Zugriffsmanagement für AWS Client VPN](#).

# IPv6 Überlegungen für AWS Client VPN

Client VPN unterstützt jetzt neben den vorhandenen IPv4 Funktionen auch native IPv6 Konnektivität. Sie können Endpoints vom Typ „IPv6Nur“, „IPv4Nur“ oder „Dual-Stack“ ( IPv4 sowohl als auch IPv6) erstellen, um Ihre Netzwerkanforderungen zu erfüllen.

## Die wichtigsten Komponenten des Supports IPv6

Bei der Arbeit mit IPv6 Client VPN gibt es zwei wichtige Konfigurationsparameter:

### Typ der IP-Adresse des Endpunkts

Dieser Parameter definiert den Endpoint Management-IP-Typ, der den EC2 Instanztyp bestimmt, der für den Endpunkt bereitgestellt wird. Dieser IP-Typ wird für die Verwaltung des externen VPN-Tunnelverkehrs verwendet (der verschlüsselte Verkehr, der zwischen dem OpenVPN-Client und dem Server über das öffentliche Internet fließt).

### Art der IP-Adresse des Verkehrs

Dieser Parameter definiert die Art des Datenverkehrs, der durch den VPN-Tunnel fließt. Dieser IP-Typ wird für die Verwaltung des internen verschlüsselten Datenverkehrs (der eigentlichen Nutzlast), der Client-CIDR-Bereiche, der Subnetzzuweisung, der Routen und der Regeln pro Endpunkt verwendet.

## IPv6 CIDR-Zuweisung an den Client

Für IPv6 Client-CIDR müssen Sie keinen CIDR-Block angeben. Amazon weist Kunden automatisch CIDR-Bereiche zu IPv6 . Diese automatische Zuweisung ermöglicht „Nein-“ SNATing für IPv6 Tunnelverkehr und bietet so einen besseren Einblick in die IPv6 Adresse des verbundenen Benutzers.

## Anforderungen an die Kompatibilität

IPv6 und Dual-Stack-Endpunkte sind von Benutzergeräten und Internetdienstanbietern abhängig (ISPs):

- Benutzergeräte, auf denen der CVPN-Client ausgeführt wird, müssen die erforderliche IP-Konfiguration unterstützen, wie in der folgenden Kompatibilitätstabelle dargestellt.
- ISPs müssen die erforderliche IP-Konfiguration unterstützen, damit die Verbindung ordnungsgemäß funktioniert.
- Für IPv6 Dual-Stack-Verkehr müssen die zugehörigen VPC-Subnetze über IPv6 oder Dual-Stack-CIDR-Bereiche verfügen.

## DNS-Support

DNS wird auf allen Arten von Endpunkten unterstützt —, und Dual-Stack. IPv4 IPv6 Für IPv6 Endgeräte können Sie IPv6 DNS-Server mithilfe des Parameters konfigurieren. --dns-server-ipv6 AAAA-DNS-Einträge werden sowohl auf der Dienst- als auch auf der Clientseite unterstützt.

## Einschränkungen

Im Folgenden sind die Einschränkungen aufgeführt bei IPv6:

- Client-to-client (C2C) -Kommunikation wird für IPv6 Clients nicht unterstützt. Wenn ein IPv6 Client versucht, mit einem anderen IPv6 Client zu kommunizieren, wird der Datenverkehr unterbrochen.

## Durchsetzung von Client-Routes für IPv6

Client VPN unterstützt jetzt Client Routes Enforcement für IPv6 den Datenverkehr. Mit dieser Funktion wird sichergestellt, dass der IPv6 Netzwerkverkehr von verbundenen Clients den vom Administrator definierten Routen folgt und nicht versehentlich außerhalb des VPN-Tunnels gesendet wird.

Die wichtigsten Aspekte der Unterstützung von IPv6 Client Route Enforcement:

- Das bestehende `ClientRouteEnforcementOptions.enforced` Flag aktiviert CRE sowohl für Stacks als auch für IPv4 IPv6 Stacks.
- IPv6 Client Route Enforcement schließt bestimmte IPv6 Bereiche aus, um wichtige Funktionen aufrechtzuerhalten: IPv6

- ::1/128— Reserviert für Loopback
  - fe80::/10— Reserviert für Link-Local-Adressen
  - ff00::/8— Reserviert für Multicast
- IPv6 Client Route Enforcement ist in der AWS VPN-Client-Version 5.3.0 und höher unter Windows, macOS und Ubuntu verfügbar.

Ausführlichere Informationen zu CRE, einschließlich dessen Aktivierung und Konfiguration, finden Sie unter. [the section called “Durchsetzung der Client-Route”](#)

## IPv6 Vermeidung von Leckagen (ältere Informationen)

Bei älteren Konfigurationen, die den systemeigenen IPv6 Support nicht nutzen, müssen Sie möglicherweise trotzdem IPv6 Leckagen verhindern. IPv6 Ein Datenleck kann auftreten, wenn beide IPv4 aktiviert und mit dem VPN verbunden IPv6 sind, das VPN aber keinen IPv6 Datenverkehr in seinen Tunnel weiterleitet. In diesem Fall stellen Sie, wenn Sie eine Verbindung zu einem IPv6 aktivierte Ziel herstellen, tatsächlich immer noch eine Verbindung mit Ihrer von Ihrem ISP bereitgestellten IPv6 Adresse her. Dadurch wird Ihre echte IPv6 Adresse durchsickern. In den folgenden Anweisungen wird erklärt, wie Sie den IPv6 Datenverkehr in den VPN-Tunnel weiterleiten.

Die folgenden zugehörigen IPv6 Anweisungen sollten zu Ihrer Client-VPN-Konfigurationsdatei hinzugefügt werden, um IPv6 Datenlecks 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 `ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` wird die Adresse des lokalen Tunnelgeräts auf IPv6 0 fd15:53b6:dead::2 und die Adresse des Remote-VPN-Endpunkts IPv6 auf 0 festgelegt fd15:53b6:dead::1.

Der nächste Befehl `route-ipv6 2000::/4` leitet IPv6 Adressen von 2000:0000:0000:0000:0000:0000:0000 bis 2fff:ffff:ffff:ffff:ffff:ffff:ffff in die VPN-Verbindung weiter.

### Note

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

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 gesamten aktuell zugewiesenen IPv6 Datenverkehr in 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 unter Verwendung der IPv6 Adresse `ping6` zu einem IPv6 Server auszuführen. Die IPv6 Adresse des Servers sollte in dem durch den `route-ipv6` Befehl angegebenen Bereich liegen. Dieser Ping-Test sollte fehlschlagen. Dies kann sich jedoch ändern, wenn der Client-VPN-Dienst in future um IPv6 Unterstützung erweitert 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. Es gibt auch einige öffentlich verfügbare Tools.

# Überwachung AWS Client VPN

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Client VPN 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, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarne festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer EC2 Amazon-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

## AWS CloudTrail

Erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Alle Client-VPN-Aktionen werden von der [Amazon EC2 API-Referenz](#) protokolliert CloudTrail und sind in dieser dokumentiert.

## CloudWatch Amazon-Protokolle

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-Protokollstream angeben, um die Verbindungsdetails zu protokollieren. Weitere Informationen finden Sie unter [Verbindungsprotokollierung für einen Endpunkt AWS Client VPN](#) und im [Amazon CloudWatch Logs-Benutzerhandbuch](#).

## Themen

- [CloudWatch Amazon-Metriken für AWS Client VPN](#)

# CloudWatch Amazon-Metriken für AWS Client VPN

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

Metrik	Beschreibung
	Einheiten: Anzahl
SelfServicePortalClientConfigurationDownloads	Die Anzahl der Downloads der Client VPN-Endpunkt-Konfigurationsdatei aus dem Self-Service-Portal.
	Einheit: Anzahl

AWS Client VPN veröffentlicht die folgenden Kennzahlen zur [Statusbeurteilung](#) 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

Metrik	Beschreibung
ClientConnectHandlerDeniedConnections	<p>Die Anzahl der Verbindungen, die vom Client-Connect-Handler für Verbindungen zum Client-VPN-Endpunkt verweigert wurden.</p> <p>Einheiten: Anzahl</p>
ClientConnectHandlerFailedServiceErrors	<p>Die Anzahl der dienstseitigen Fehler beim Ausführen des Client-Connect-Handlers für Verbindungen zum Client-VPN-Endpunkt.</p> <p>Einheiten: Anzahl</p>

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

CloudWatch ermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, sogenannten Metriken, 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 beispielsweise einen CloudWatch Alarm erstellen, um eine bestimmte Metrik zu überwachen und eine Aktion einzuleiten (z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb des für Sie akzeptablen Bereichs liegt.

Weitere Informationen finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

## Aufgaben

- [Client-VPN-Endpunktmetriken in Amazon anzeigen CloudWatch](#)

## Client-VPN-Endpunktmetriken in Amazon anzeigen CloudWatch

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

## Um Metriken mit der CloudWatch Konsole anzuzeigen

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.

## Um Metriken mit dem AWS CLI anzuzeigen

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"
```

# AWS Client VPN Kontingente

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	200  Bei Dual-Stack-Endpunkten wird dieses Limit von beiden IPv4 Routen gemeinsam genutzt. IPv6	<a href="#">Ja</a>
Client-VPN-Endpunkte pro Region	5	<a href="#">Ja</a>
Gleichzeitige Client-Verbindungen pro Client-VPN-Endpunkt	Dieser Wert hängt von der Anzahl der Subnetzzuordnungen pro Endpunkt ab. <ul style="list-style-type: none"> <li>• 1 - 7.000</li> <li>• 2 - 36.500</li> <li>• 3 - 66.500</li> <li>• 4 - 96.500</li> <li>• 5 - 126.000</li> </ul>	<a href="#">Ja</a>

Name	Standard	Anpassbar
	Bei Dual-Stack-Endpunkten wird dieses Limit von Verbindungen gemeinsam genutzt. IPv4 IPv6	
Gleichzeitige Operationen pro Client-VPN-Endpunkt	10	Nein
Einträge in einer Client-Zertifikatssperrliste für Client-VPN-Endpunkte	20 000	Nein
VPN-Zielnetzwerkzuweisung für Routen pro Client	100  Bei Dual-Stack-Endpunkten wird dieses Limit von beiden IPv4 Routen gemeinsam genutzt. IPv6	<u>Ja</u>

† Operationen umfassen:

- Verknüpfen oder Trennen von Subnetzen
- 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 IdP-Vertrauens-Beziehung zu definieren. AWS Der IAM-SAML-Identitätsanbieter kann von mehreren Client-VPN-Endpunkten in demselben Konto gemeinsam genutzt werden. AWS

# Problembehebung AWS Client VPN

Die folgenden Abschnitte können Ihnen bei der Behebung von Problemen helfen, die Sie möglicherweise mit einem Client-VPN-Endpunkt haben.

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

- [Fehlerbehebung AWS Client VPN: Der DNS-Name des Client-VPN-Endpunkts konnte nicht aufgelöst werden](#)
- [Fehlerbehebung AWS Client VPN: Der Verkehr wird nicht zwischen Subnetzen aufgeteilt](#)
- [Problembehandlung AWS Client VPN: Autorisierungsregeln für Active Directory-Gruppen funktionieren nicht wie erwartet](#)
- [Fehlerbehebung AWS Client VPN: Kunden können nicht auf eine Peering-VPC, Amazon S3 oder das Internet zugreifen](#)
- [Fehlerbehebung AWS Client VPN: Der Zugriff auf eine Peer-VPC, Amazon S3 oder das Internet ist unterbrochen](#)
- [Fehlerbehebung AWS Client VPN: Die Client-Software gibt einen TLS-Fehler zurück, wenn versucht wird, eine Verbindung zu Client VPN herzustellen](#)
- [Fehlerbehebung AWS Client VPN: Die Client-Software gibt Benutzernamen- und Kennwortfehler zurück — Active Directory-Authentifizierung](#)
- [Fehlerbehebung AWS Client VPN: Die Client-Software gibt Benutzernamen- und Kennwortfehler zurück — Verbundauthentifizierung](#)
- [Problembehandlung AWS Client VPN: Clients können keine Verbindung herstellen — gegenseitige Authentifizierung](#)
- [Fehlerbehebung AWS Client VPN: Der Client gibt einen Fehler zurück, der die maximale Größe der Anmeldeinformationen in Client VPN überschreitet — Verbundauthentifizierung](#)
- [Fehlerbehebung AWS Client VPN: Der Client öffnet den Browser für einen Endpunkt nicht — Verbundauthentifizierung](#)
- [Fehlerbehebung AWS Client VPN: Der Client gibt den Fehler „Keine verfügbaren Ports“ zurück — Verbundauthentifizierung](#)
- [Fehlerbehebung AWS Client VPN: Eine Verbindung wurde aufgrund einer IP-Diskrepanz beendet](#)

- [Fehlerbehebung AWS Client VPN: Das Routing des Datenverkehrs zum LAN funktioniert nicht wie erwartet](#)
- [Fehlerbehebung AWS Client VPN: Überprüfen Sie das Bandbreitenlimit für einen Client-VPN-Endpunkt](#)
- [Fehlerbehebung AWS Client VPN: Probleme mit der Tunnelkonnektivität zu einer VPC](#)

## Fehlerbehebung AWS Client VPN: Der 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 DNS-Namen des Client-VPN-Endpunkts angibt, und stellen Sie ihr eine zufällige Zeichenfolge voran, sodass das Format lautet `random_string.displayed_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`

## Fehlerbehebung AWS Client VPN: Der Verkehr 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 Subnetzen 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.

# Problembehandlung AWS Client VPN: Autorisierungsregeln für Active Directory-Gruppen funktionieren nicht wie erwartet

## Problem

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

## Ursache

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

Stellen Sie sicher, dass Sie Autorisierungsregeln erstellen, die Active Directory-Gruppen explizit Zugriff auf ein bestimmtes Netzwerk gewähren CIDRs. 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.

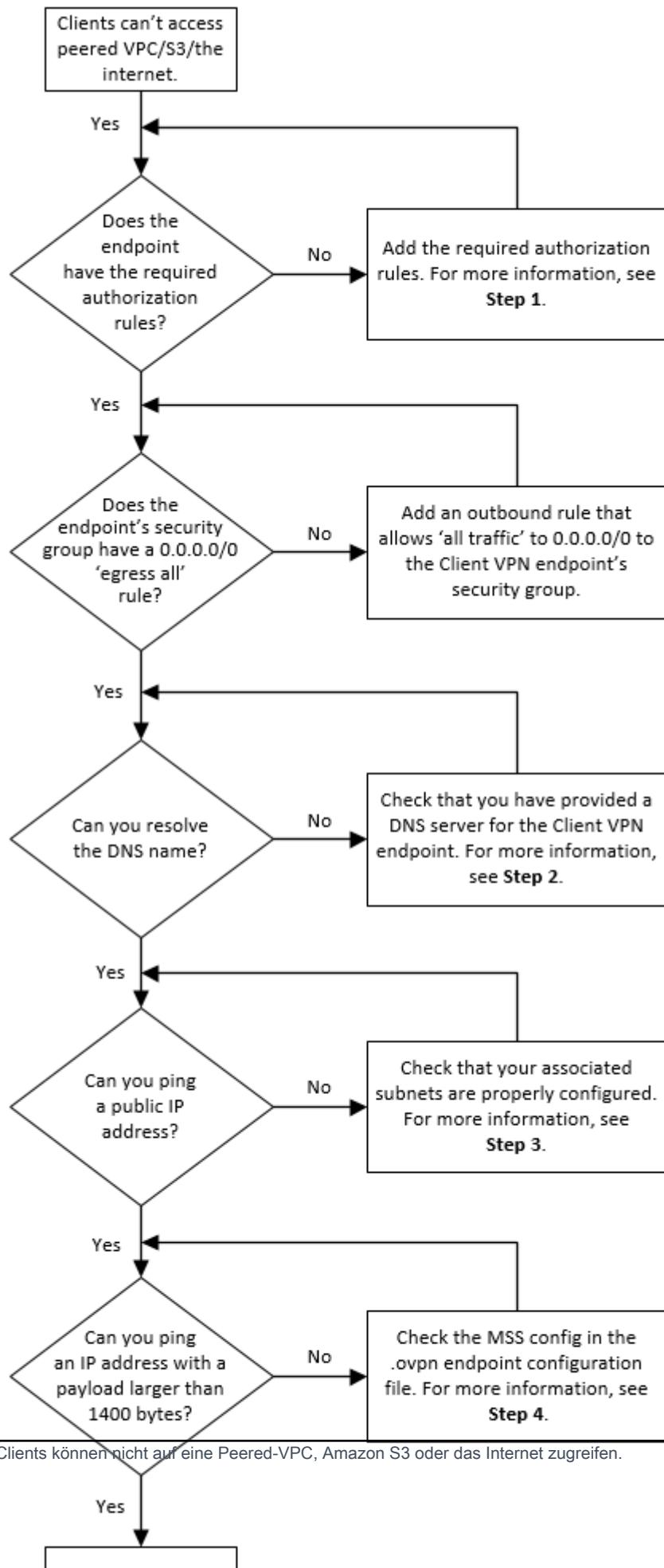
## Fehlerbehebung AWS Client VPN: Kunden können nicht auf eine Peering-VPC, Amazon S3 oder das Internet zugreifen

### 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.



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 eine Autorisierungsregel für den IPv4 CIDR-Bereich der VPC 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 Netzwerzugriffskontrolllistenregeln verfügt, die den ein- und ausgehenden Datenverkehr blockieren.

Wenn Sie eine Peer-VPC nicht erreichen können, überprüfen Sie, ob die Routing-Tabelle des zugehörigen Subnetzes 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

## Fehlerbehebung AWS Client VPN: Der Zugriff auf eine Peer-VPC, Amazon S3 oder das Internet ist unterbrochen

### 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

# Fehlerbehebung AWS Client VPN: Die Client-Software gibt einen TLS-Fehler zurück, wenn versucht wird, eine Verbindung zu Client VPN herzustellen

## 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 [AWS Client VPN Sperrlisten für Client-Zertifikate](#).

## 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 in AWS Client VPN](#).

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 .

## Fehlerbehebung AWS Client VPN: Die Client-Software gibt Benutzernamen- und Kennwortfehler 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 [AWS Client VPN Export von Endpunktkonfigurationsdateien](#). Testen Sie die MFA-Konfiguration für Ihr Active Directory, ohne den Client-VPN-Endpunkt zu verwenden, um zu überprüfen, ob MFA wie erwartet funktioniert.

# Fehlerbehebung AWS Client VPN: Die Client-Software gibt Benutzernamen- und Kennwortfehler zurück — Verbundauthentifizierung

## Problem

Beim Versuch, sich mit einem Benutzernamen und einem Passwort mit Verbundauthentifizierung anzumelden, wird der Fehler „Die erhaltenen Anmeldeinformationen waren falsch“ angezeigt. Wenden Sie sich an Ihren IT-Administrator.“

## Ursache

Dieser Fehler kann dadurch verursacht werden, dass in der SAML-Antwort des IdP nicht mindestens ein Attribut 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](#).

# Problembehandlung AWS Client VPN: 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 [AWS Client VPN Export von Endpunktkonfigurationsdateien](#).

## Fehlerbehebung AWS Client VPN: Der Client gibt einen Fehler zurück, der die maximale Größe der Anmeldeinformationen in Client VPN überschreitet — 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.

## Fehlerbehebung AWS Client VPN: Der Client öffnet den Browser für einen Endpunkt 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 auf den AWS bereitgestellten Client und versuchen Sie erneut, eine Verbindung herzustellen.

# Fehlerbehebung AWS Client VPN: Der Client gibt den Fehler „Keine verfügbaren Ports“ zurück — 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 bereitgestellte Client benötigt die Verwendung des TCP-Ports 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.

# Fehlerbehebung AWS Client VPN: Eine Verbindung wurde aufgrund einer IP-Diskrepanz 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 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 für die Verwendung AWS Client VPN](#).

## Lösung

Stellen Sie sicher, dass kein DNS-Proxy zwischen dem AWS angegebenen Client und dem Client-VPN-Endpunkt besteht.

## Fehlerbehebung AWS Client VPN: Das Routing des Datenverkehrs zum LAN funktioniert nicht wie erwartet

### Problem

Der Versuch, den Verkehr an ein lokales Netzwerk (LAN) weiterzuleiten, funktioniert nicht wie erwartet, wenn die LAN-IP-Adressbereiche nicht innerhalb der folgenden standardmäßigen privaten IP-Adressbereiche liegen: 10.0.0.0/8172.16.0.0/12,192.168.0.0/16, oder 169.254.0.0/16.

### Ursache

Wenn festgestellt wird, dass der LAN-Adressbereich des Clients außerhalb der oben genannten Standardbereiche 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. Weitere Informationen finden Sie unter [Regeln und bewährte Verfahren für die Verwendung AWS Client VPN](#).

### Lösung

Wenn Sie während VPN-Verbindungen LAN-Zugriff benötigen, wird empfohlen, die oben aufgeführten konventionellen Adressbereiche für Ihr LAN zu verwenden.

## Fehlerbehebung AWS Client VPN: Überprüfen Sie das Bandbreitenlimit 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. Pro Benutzerverbindung wird eine Mindestbandbreite von 10 Mbit/s unterstützt.

## 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
```

## Fehlerbehebung AWS Client VPN: Probleme mit der Tunnelkonnektivität zu einer VPC

Wenn Verbindungsprobleme mit Ihrer AWS Client VPN Verbindung auftreten, folgen Sie diesem systematischen Ansatz zur Fehlerbehebung, um das Problem zu identifizieren und zu lösen. Dieser Abschnitt enthält step-by-step Verfahren zur Diagnose häufiger Client-VPN-Verbindungsprobleme zwischen Remote-Clients und Amazon VPC-Ressourcen.

### Themen

- [Voraussetzungen für die Netzwerkkonnektivität](#)
- [Überprüfen Sie den Status Client VPN Client-VPN-Endpunkts](#)
- [Überprüfen Sie die Client-Verbindungen](#)
- [Überprüfen Sie die Client-Authentifizierung](#)
- [Überprüfen Sie die Autorisierungsregeln](#)
- [Client-VPN-Routen validieren](#)
- [Überprüfen Sie die Sicherheitsgruppen und das Netzwerk ACLs](#)
- [Testen Sie die Client-Konnektivität](#)
- [Diagnostizieren Sie das Client-Gerät](#)
- [Problembehandlung bei der DNS-Auflösung](#)
- [Probleme mit der Leistung beheben](#)
- [Client-VPN-Metriken überwachen](#)
- [Überprüfen Sie die Client-VPN-Protokolle](#)
- [Häufige Probleme und Lösungen](#)

## Voraussetzungen für die Netzwerkkonnektivität

Bevor Sie Probleme mit der Client-VPN-Konnektivität beheben, überprüfen Sie die folgenden Netzwerkvoraussetzungen:

- Stellen Sie sicher, dass das Client-VPN-Endpunkt-Subnetz über eine Internetverbindung verfügt (über Internet Gateway oder NAT-Gateway).
- Stellen Sie sicher, dass der Client-VPN-Endpunkt Subnetzen in verschiedenen Availability Zones zugeordnet ist, um eine hohe Verfügbarkeit zu gewährleisten.
- Stellen Sie sicher, dass die VPC über ausreichend IP-Adressraum verfügt und nicht mit den CIDR-Blöcken des Clients in Konflikt steht.
- Vergewissern Sie sich, dass die Zielsubnetze über die richtigen Routing-Tabellenzuordnungen verfügen.

## Überprüfen Sie den Status Client VPN Client-VPN-Endpunkts

Stellen Sie zunächst sicher, dass sich Ihr Client-VPN-Endpunkt im richtigen Status befindet:

1. Verwenden Sie den AWS CLI , um den Status des Client-VPN-Endpunkts zu überprüfen:

```
aws ec2 describe-client-vpn-endpoints --region your-region
```

2. Suchen Sie in der Ausgabe nach dem Endpunktstatus. Der Status sollte seinavailable.
3. Stellen Sie sicher, dass dem Endpunkt Zielnetzwerke (Subnetze) zugeordnet sind.
4. Wenn dies nicht der Fall istavailable, suchen Sie nach Fehlermeldungen oder ausstehenden Status, die auf Konfigurationsprobleme hinweisen könnten.

## Überprüfen Sie die Client-Verbindungen

Überprüfen Sie den Status der Client-Verbindungen zu Ihrem Client-VPN-Endpunkt:

1. Überprüfen Sie die aktiven Client-Verbindungen:

```
aws ec2 describe-client-vpn-connections --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. Überprüfen Sie den Verbindungsstatus und alle Fehlermeldungen in der Ausgabe.

3. Überprüfen Sie die Client-Authentifizierungsprotokolle auf fehlgeschlagene Authentifizierungsversuche.
4. Stellen Sie sicher, dass die Clients IP-Adressen vom konfigurierten Client-CIDR-Block erhalten.

 Note

Wenn Clients keine Verbindung herstellen können, liegt das Problem wahrscheinlich an der Authentifizierungskonfiguration, den Autorisierungsregeln oder der Netzwerkverbindlichkeit.

## Überprüfen Sie die Client-Authentifizierung

Authentifizierungsprobleme sind häufige Ursachen für Probleme mit der Client-VPN-Konnektivität:

- Stellen Sie bei der gegenseitigen Authentifizierung sicher, dass die Client-Zertifikate gültig und nicht abgelaufen sind.
- Überprüfen Sie für die Active Directory-Authentifizierung die Benutzeranmeldeinformationen und die Domänenkonnektivität.
- Überprüfen Sie für die SAML-basierte Verbundauthentifizierung die IdP-Konfiguration und die Benutzerberechtigungen.
- Ausführliche Fehlerinformationen finden Sie in den CloudWatch Authentifizierungsanmeldungen.
- Stellen Sie sicher, dass die auf dem Endpunkt konfigurierte Authentifizierungsmethode mit der Client-Konfiguration übereinstimmt.

## Überprüfen Sie die Autorisierungsregeln

Autorisierungsregeln steuern, auf welche Netzwerkressourcen Clients zugreifen können:

1. Aktuelle Autorisierungsregeln auflisten:

```
aws ec2 describe-client-vpn-authorization-rules --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. Stellen Sie sicher, dass Regeln für die Zielnetzwerke existieren, auf die Clients zugreifen müssen.

3. Vergewissern Sie sich, dass die Regeln die richtigen Active Directory-Gruppen angeben (falls Sie die AD-Authentifizierung verwenden).
4. Stellen Sie sicher, dass die Autorisierungsregeln den aktuellen active Status haben.

## Client-VPN-Routen validieren

Die richtige Routing-Konfiguration ist für die Client-VPN-Konnektivität unerlässlich:

1. Überprüfen Sie die Client-VPN-Endpunkttrouten:

```
aws ec2 describe-client-vpn-routes --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. Stellen Sie sicher, dass Routen für Zielnetzwerke existieren, auf die Clients zugreifen müssen.
3. Überprüfen Sie die Amazon VPC-Routentabellen, um sicherzustellen, dass der zurückkehrende Datenverkehr den Client-VPN-Endpunkt erreichen kann:

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-id" --region your-region
```

4. Stellen Sie sicher, dass die Zielnetzwerkzuordnungen korrekt konfiguriert sind.

## Überprüfen Sie die Sicherheitsgruppen und das Netzwerk ACLs

Sicherheitsgruppen und Netzwerke ACLs können den Client-VPN-Verkehr blockieren:

1. Suchen Sie in den Sicherheitsgruppen nach EC2 Zielinstanzen:

```
aws ec2 describe-security-groups --group-ids sg-xxxxxxxx --region your-region
```

2. Stellen Sie sicher, dass die Regeln für eingehenden Datenverkehr den Datenverkehr vom Client-VPN-CIDR-Block zulassen:
  - SSH (Port 22) von Client VPN CIDR: 10.0.0.0/16
  - HTTP (Port 80) von Client VPN CIDR: 10.0.0.0/16
  - HTTPS (Port 443) von Client VPN CIDR: 10.0.0.0/16
  - Benutzerdefinierte Anwendungs-Ports nach Bedarf

3. Stellen Sie für die Client-VPN-Endpunktsicherheitsgruppe (falls zutreffend) sicher, dass sie Folgendes zulässt:
  - UDP-Port 443 (OpenVPN) ab 0.0.0.0/0
  - Der gesamte ausgehende Datenverkehr zu VPC-CIDR-Blöcken
4. Stellen Sie sicher, dass das Netzwerk ACLs den Verkehr nicht blockiert. Das Netzwerk ACLs ist zustandslos, daher müssen sowohl Regeln für eingehenden als auch für ausgehenden Datenverkehr konfiguriert werden.
5. Überprüfen Sie sowohl die Regeln für eingehenden als auch für ausgehenden Datenverkehr für den spezifischen Datenverkehr, den Sie senden möchten.

## Testen Sie die Client-Konnektivität

Testen Sie die Konnektivität von Client-VPN-Clients zu Amazon VPC-Ressourcen:

1. Testen Sie von einem verbundenen Client-VPN-Client aus die Konnektivität zu Amazon VPC-Ressourcen:

```
ping vpc-resource-ip
traceroute vpc-resource-ip
```

2. Testen Sie die Konnektivität bestimmter Anwendungen:

```
telnet vpc-resource-ip port
```

3. Überprüfen Sie die DNS-Auflösung, wenn Sie private DNS-Namen verwenden:

```
nslookup private-dns-name
```

4. Testen Sie die Konnektivität zu Internetressourcen, wenn Split-Tunneling aktiviert ist.

## Diagnostizieren Sie das Client-Gerät

Führen Sie die folgenden Prüfungen auf dem Client-Gerät durch:

1. Stellen Sie sicher, dass die Client-Konfigurationsdatei (.ovpn) die richtigen Einstellungen enthält:
  - Richtige Serverendpunkt-URL

- Gültiges Client-Zertifikat und privater Schlüssel
  - Richtige Konfiguration der Authentifizierungsmethode
2. Überprüfen Sie die Client-Protokolle auf Verbindungsfehler:
- Windows: Ereignisanzeige → Anwendungs- und Dienstprotokolle → OpenVPN
  - macOS: Konsolen-App, suche nach „Tunnelblick“ oder „OpenVPN“
  - Linux: oder systemd journal /var/log/openvpn/
3. Testen Sie die grundlegende Netzwerkkonnektivität vom Client aus:

```
ping 8.8.8.8  
nslookup cvpn-endpoint-id.cvpn.region.amazonaws.com
```

## Problembehandlung bei der DNS-Auflösung

DNS-Probleme können den Zugriff auf Ressourcen verhindern, die private DNS-Namen verwenden:

1. Prüfen Sie, ob DNS-Server im Client-VPN-Endpunkt konfiguriert sind:

```
aws ec2 describe-client-vpn-endpoints --client-vpn-endpoint-ids cvpn-endpoint-id --  
query 'ClientVpnEndpoints[0].DnsServers'
```

2. Testen Sie die DNS-Auflösung vom Client aus:

```
nslookup private-resource.internal  
dig private-resource.internal
```

3. Überprüfen Sie die Route 53 53-Resolver-Regeln, wenn Sie eine benutzerdefinierte DNS-Auflösung verwenden.
4. Vergewissern Sie sich, dass Sicherheitsgruppen DNS-Verkehr (UDP/TCP-Port 53) vom Client-VPN-CIDR zu DNS-Servern zulassen.

## Probleme mit der Leistung beheben

Behebung von Leistungsproblemen mit Client-VPN-Verbindungen:

- Überwachen Sie die Bandbreitennutzung anhand von CloudWatch ingress/egress Byte-Metriken.
- Prüfen Sie anhand kontinuierlicher Ping-Tests von Clients, ob Pakete verloren gehen.

- Stellen Sie sicher, dass der Client-VPN-Endpunkt die Verbindungslimits nicht erreicht.
- Erwägen Sie die Verwendung mehrerer Client-VPN-Endpunkte für die Lastverteilung.
- Testen Sie an verschiedenen Kundenstandorten, um regionale Leistungsprobleme zu identifizieren.

## Client-VPN-Metriken überwachen

Überwachen Sie Client-VPN-Endpunktmetriken mit CloudWatch:

1. Überprüfen Sie die Messwerte für aktive Verbindungen:

```
aws cloudwatch get-metric-statistics \
--namespace AWS/ClientVPN \
--metric-name ActiveConnectionsCount \
--dimensions Name=Endpoint,Value=cvpn-endpoint-id \
--start-time start-time \
--end-time end-time \
--period 300 \
--statistics Average
```

2. Überprüfen Sie die Metriken für Authentifizierungsfehler:

```
aws cloudwatch get-metric-statistics \
--namespace AWS/ClientVPN \
--metric-name AuthenticationFailures \
--dimensions Name=Endpoint,Value=cvpn-endpoint-id \
--start-time start-time \
--end-time end-time \
--period 300 \
--statistics Sum
```

3. Überprüfen Sie andere verfügbare Metriken wie eingehende und ausgehende Bytes und Pakete.

## Überprüfen Sie die Client-VPN-Protokolle

Client-VPN-Verbindungsprotokolle enthalten detaillierte Informationen zu Verbindungsversuchen und Fehlern:

- Aktivieren Sie die Client-VPN-Verbindungsprotokollierung, falls sie nicht bereits konfiguriert ist.

- Überprüfen Sie die CloudWatch Protokolle auf Verbindungsversuche, Authentifizierungsfehler und Autorisierungsfehler.
- Suchen Sie nach bestimmten Fehlercodes und Meldungen, die auf die Hauptursache von Verbindungsproblemen hinweisen.
- Suchen Sie nach Mustern bei fehlgeschlagenen Verbindungen, die auf Konfigurationsprobleme hinweisen könnten.

## Häufige Probleme und Lösungen

Häufige Probleme, die sich auf die Client-VPN-Konnektivität auswirken können:

### Authentication failures (Authentifizierungsfehler)

Die Client-Zertifikate sind abgelaufen oder ungültig, oder die Active Directory-Anmeldeinformationen sind falsch. Überprüfen Sie die Authentifizierungskonfiguration und die Gültigkeit der Anmeldeinformationen.

### Fehlende Autorisierungsregeln

Clients können aufgrund fehlender oder falscher Autorisierungsregeln nicht auf Zielnetzwerke zugreifen. Fügen Sie die entsprechenden Autorisierungsregeln für die erforderlichen Netzwerke hinzu.

### Probleme beim Split-Tunneling

Der Datenverkehr wurde aufgrund der Split-Tunneling-Konfiguration falsch weitergeleitet. Überprüfen Sie die Split-Tunneling-Einstellungen und passen Sie sie nach Bedarf an.

### Erschöpfung des Client-IP-Pools

Keine verfügbaren IP-Adressen im CIDR-Block des Clients. Erweitern Sie den CIDR-Bereich des Clients oder trennen Sie die Verbindung zu ungenutzten Clients.

### MTU-Probleme

Große Pakete werden aufgrund von MTU-Größenbeschränkungen verworfen. Versuchen Sie, die MTU auf 1436 Byte einzustellen, oder aktivieren Sie Path MTU Discovery auf Client-Geräten.

### Probleme mit der DNS-Auflösung

Clients können private DNS-Namen nicht auflösen. Überprüfen Sie die DNS-Serverkonfiguration und stellen Sie sicher, dass DNS-Verkehr über Sicherheitsgruppen zugelassen wird.

## Überlappende IP-Bereiche

Die CIDR-Blöcke der Clients stehen in Konflikt mit lokalen Netzwerkbereichen. Suchen Sie nach überlappenden IP-Adressbereichen zwischen Client-CIDR und lokalen Netzwerken und lösen Sie diese.

## TLS-Handshake-Fehler

Die Verbindung schlägt während der TLS-Aushandlung fehl. Überprüfen Sie die Gültigkeit des Zertifikats, stellen Sie sicher, dass die richtigen Verschlüsselungssammlungen vorhanden sind, und stellen Sie sicher, dass die Client- und Serverzertifikate ordnungsgemäß konfiguriert sind.

## Verzögerungen bei der Weiterleitung der Route

Neue Routen stehen Kunden nicht sofort zur Verfügung. Warten Sie 1—2 Minuten für die Weiterleitung der Route, nachdem Sie Änderungen an den Client-VPN-Routen vorgenommen haben.

## Verbindungsabbruch/Instabilität

Häufige Verbindungsabbrüche oder instabile Verbindungen. Überprüfen Sie die Client-Geräte auf Netzwerküberlastung, Firewall-Interferenzen oder Energieverwaltungseinstellungen.

# Dokumentverlauf für das Client-VPN-Benutzerhandbuch

In der folgenden Tabelle werden die Aktualisierungen des AWS Client VPN Administratorhandbuchs beschrieben.

Änderung	Beschreibung	Datum
<a href="#"><u>IPv6 Unterstützung</u></a>	Client VPN ermöglicht jetzt die vollständige IPv6 Konnektivität für Client-VPN-Endpunkte und unterstützt Verbindungen zu IPv6 Ressourcen in Ihrem Netzwerk VPCs und von Clients in IPv6 Netzwerken.	25. August 2025
<a href="#"><u>Funktion zur Routendurchsetzung für Clients</u></a>	Hinzufügung der Funktion zur Durchsetzung von Client-Routen	20. April 2025
<a href="#"><u>Höheres Client-VPN-Kontingent</u></a>	Das Kontingent für Autorisierungsregeln pro Client-VPN-Endpunkt wurde von 50 auf 200 erhöht.	13. März 2025
<a href="#"><u>Support für die Unterbrechung der Verbindung bei Sitzungstimeout</u></a>	Das Sitzungs-Timeout unterstützt jetzt die Verbindung, wenn die maximale Sitzungsdauer erreicht ist.	13. Januar 2025
<a href="#"><u>Erhöhte Kontingente</u></a>	Die Kontingente für Autorisierungsregeln pro Client-VPN-Endpunkt und Routen pro Client-VPN-Endpunkt wurden von 50 bzw. 10 auf 100 erhöht.	19. Dezember 2024
<a href="#"><u>Beispiele für Autorisierungsregeln</u></a>	Beispieldaten für Autorisierungsregeln hinzugefügt.	15. September 2022

<a href="#"><u>Maximale VPN-Sitzungsdauer</u></a>	Sie können eine kürzere maximale VPN-Sitzungsdauer konfigurieren, um Sicherheits- und Compliance-Anforderungen zu erfüllen.	20. Januar 2022
<a href="#"><u>Client-Anmelde-Banner</u></a>	Sie können ein Textbanner auf den AWS bereitgestellten Client-VPN-Desktopanwendungen aktivieren, wenn eine VPN-Sitzung eingerichtet wird, um gesetzliche Vorschriften und Compliance-Anforderungen zu erfüllen.	20. Januar 2022
<a href="#"><u>Client-Connect-Handler</u></a>	Sie können den Client-Connect-Handler für Ihren Client-VPN-Endpunkt aktivieren, um eine benutzerdefinierte Logik auszuführen, die neue Verbindungen autorisiert.	4. November 2020
<a href="#"><u>Self-Service-Portal</u></a>	Sie können ein Self-Service-Portal auf Ihrem Client-VPN-Endpunkt für Ihre Clients aktivieren.	29. Oktober 2020
<a href="#"><u>Client-to-client Zugriff</u></a>	Sie können Clients, die eine Verbindung zu einem Client-VPN-Endpunkt herstellen, ermöglichen, eine Verbindung miteinander herzustellen.	29. September 2020
<a href="#"><u>SAML 2.0-basierte Verbundauthentifizierung</u></a>	Sie können Client-VPN-Benutzer mithilfe der SAML 2.0-basierten Verbundauthentifizierung authentifizieren.	19. Mai 2020

<a href="#"><u>Festlegen von Sicherheitsgruppen während der Erstellung</u></a>	Sie können eine VPC und Sicherheitsgruppen angeben, wenn Sie Ihren AWS Client VPN -Endpunkt erstellen.	5. März 2020
<a href="#"><u>Konfigurierbare VPN-Ports</u></a>	Sie können eine unterstützte VPN-Portnummer für Ihren AWS Client VPN Endpunkt angeben.	16. Januar 2020
<a href="#"><u>Unterstützung für Multi-Factor Authentication (MFA)</u></a>	Ihr AWS Client VPN Endpunkt unterstützt MFA, wenn es für Ihr Active Directory aktiviert ist.	30. September 2019
<a href="#"><u>Unterstützung für Split-Tunnel</u></a>	Sie können Split-Tunnel auf Ihrem Endpunkt aktivieren.	24. Juli 2019
<a href="#"><u>AWS Client VPN</u></a>	Mit 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.