



Guida per l'amministratore

AWS Client VPN



AWS Client VPN: Guida per l'amministratore

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è AWS Client VPN?	1
Caratteristiche di Client VPN	1
Componenti di Client VPN	2
Utilizzo di Client VPN	3
Prezzi per Client VPN	4
Regole e migliori pratiche	5
Come funziona Client VPN	7
Autenticazione client	8
Autenticazione Active Directory	9
Autenticazione reciproca	10
Single Sign-On (autenticazione federata basata su SAML 2.0)	15
Autorizzazione client	20
Gruppi di sicurezza	20
Autorizzazione di rete	21
Autorizzazione di connessione	21
Requisiti e considerazioni	22
Interfaccia Lambda	22
Utilizzo dell'handler delle connessioni client per la valutazione dell'assetto	24
Abilitazione dell'handler delle connessioni client	25
Ruolo collegato ai servizi	25
Monitoraggio degli errori di autorizzazione della connessione	25
Split-tunnel di Client VPN	26
Vantaggi dello split-tunnel	27
Considerazioni sul routing	27
Enabling-split-tunnel	27
Registrazione delle connessioni	27
Voci di log del registro di connessione	28
Considerazioni sul dimensionamento	30
Scenari ed esempi	32
Accesso a un VPC	32
Accesso a un VPC con peering	33
Accesso a una rete on-premise	35
Accesso a Internet	37
Client-to-client Accesso C	38

Limitare l'accesso a un VPC in peering	40
Limitare l'accesso utilizzando i gruppi di sicurezza	40
Limitare l'accesso in base ai gruppi di utenti	42
Tutorial sulle nozioni di base	44
Prerequisiti	45
Fase 1: Generare i certificati e le chiavi server e client	45
Fase 2: Creare un endpoint Client VPN	45
Fase 3: Associazione di una rete target	46
Fase 4: Aggiungere una regola di autorizzazione per il VPC	47
Fase 5: Fornire l'accesso a Internet.	48
Fase 6: Verificare i requisiti del gruppo di sicurezza	49
Fase 7: Scaricare il file di configurazione dell'endpoint Client VPN	49
Fase 8: Connettersi all'endpoint Client VPN	50
Utilizzo di Client VPN	51
Accedere al portale self-service	51
Regole di autorizzazione	52
Aggiunta di una regola di autorizzazione a un endpoint Client VPN	53
Rimozione di una regola di autorizzazione da un endpoint Client VPN	54
Visualizzazione delle regole di autorizzazione	54
Scenari di esempio	55
Elenchi di revoche di certificati client	66
Generazione di un elenco di revoche di certificati client	66
Importazione di un elenco di revoche di certificati client	68
Esportazione di un elenco di revoche di certificati client	69
Connessioni client	69
Visualizzazione delle connessioni client	69
Terminazione di una connessione client	70
Banner di accesso del client	70
Configurare un banner di accesso client durante la creazione di un endpoint Client VPN	71
Configurare un banner di accesso client per un endpoint Client VPN esistente	71
Disabilitare un banner di accesso client per un endpoint Client VPN esistente	72
Modificare il testo del banner esistente su un endpoint Client VPN	72
Visualizzare il banner di accesso attualmente configurato	73
Endpoint Client VPN	73
Creare un endpoint Client VPN	74
Modifica un endpoint Client VPN.	77

Visualizzare gli endpoint Client VPN	80
Elimina un endpoint Client VPN.	81
Log delle connessioni	81
Abilitazione della registrazione delle connessioni per un nuovo endpoint Client VPN	82
Abilitazione della registrazione delle connessioni per un endpoint Client VPN esistente	83
Visualizzare i log delle connessioni.	84
Disattivazione della registrazione della connessione	84
Esportazione e configurazione del file di configurazione del client	85
Esportazione del file di configurazione del client	85
Aggiunta delle informazioni sul certificato del client e la chiave (autenticazione reciproca)	86
Route	87
Considerazioni per lo split-tunnel su endpoint Client VPN	88
Creazione di una route dell'endpoint	88
Visualizzazione delle route dell'endpoint	89
Eliminazione di una route dell'endpoint	90
Reti target	90
Associare una rete di destinazione a un endpoint Client VPN	90
Applicazione di un gruppo di sicurezza a una rete target	92
Annullare l'associazione di una rete di destinazione da un endpoint Client VPN	93
Visualizzazione delle reti target	93
Durata massima della sessione VPN	94
Configurare la sessione VPN massima durante la creazione di un endpoint Client VPN	94
Visualizzare la durata massima della sessione VPN corrente	94
Modificare la durata massima della sessione VPN	95
Sicurezza	96
Protezione dei dati	97
Crittografia in transito	98
Riservatezza del traffico Internet	98
Gestione dell'identità e degli accessi	98
Destinatari	99
Autenticazione con identità	100
Gestione dell'accesso con policy	103
Come funziona AWS Client VPN con IAM	106
Esempi di policy basate su identità	113
Risoluzione dei problemi	116
Utilizzo di ruoli collegati ai servizi	118

Resilienza	122
Più reti di destinazione per un'elevata disponibilità	123
Sicurezza dell'infrastruttura	123
Best practice	124
Considerazioni su IPv6	124
Monitoraggio di Client VPN	127
Metriche di CloudWatch	127
Visualizza i parametri CloudWatch	130
Log di CloudTrail	131
Informazioni su Client VPN in CloudTrail	131
Informazioni sulle voci dei file di log di Client VPN	132
Quote	133
Quote Client VPN	133
Quote di utenti e gruppi	134
Considerazioni generali	134
Risoluzione dei problemi	135
Impossibile risolvere il nome DNS dell'endpoint Client VPN	135
Il traffico non viene suddiviso tra sottoreti	136
Regole di autorizzazione per i gruppi di Active Directory non funzionano come previsto	137
I client non possono accedere a un VPC in peering, ad Amazon S3 o a Internet	138
Accesso intermittente a un VPC in peering, ad Amazon S3 o a Internet	141
Il software client restituisce l'errore TLS	142
Il software client restituisce errori di nome utente e password (autenticazione di Active Directory)	143
Il software client restituisce gli errori relativi al nome utente e alla password (autenticazione federata)	143
I client non sono in grado di connettersi (autenticazione reciproca)	144
Client restituisce un errore di superamento delle dimensioni massime delle credenziali (autenticazione federata)	144
Il client non apre il browser (autenticazione federata)	145
Il client non restituisce un errore nessuna porta disponibile (autenticazione federata)	145
Connessione VPN interrotta a causa della mancata corrispondenza dell'IP	146
Il routing del traffico verso la LAN non funziona come previsto	146
Verifica del limite di larghezza di banda per un endpoint Client VPN	147
Cronologia dei documenti	148
.....	cl

Che cos'è AWS Client VPN?

AWS Client VPN è un servizio VPN gestito, basato su cloud, che consente di controllare in modo sicuro l'accesso alle risorse AWS e alle risorse nella tua rete on-premise. Con Client VPN, puoi accedere alle risorse da qualsiasi luogo tramite un client VPN basato su OpenVPN.

Indice

- [Caratteristiche di Client VPN](#)
- [Componenti di Client VPN](#)
- [Utilizzo di Client VPN](#)
- [Prezzi per Client VPN](#)
- [Regole e best practice di AWS Client VPN](#)

Caratteristiche di Client VPN

Client VPN offre le seguenti caratteristiche e funzionalità:

- **Connessioni sicure:** offre una connessione sicura TLS da qualsiasi luogo tramite il client OpenVPN.
- **Servizio gestito:** è un servizio gestito AWS che rimuove gli oneri operativi di distribuzione e gestione di una soluzione VPN di accesso remoto di terze parti.
- **Disponibilità elevata ed elasticità:** viene automaticamente dimensionato al numero di utenti che si connettono alle risorse AWS e alle risorse in locale.
- **Autenticazione:** supporta l'autenticazione client utilizzando Active Directory, l'autenticazione federata e l'autenticazione basata su certificati.
- **Controllo granulare:** consente di implementare controlli di sicurezza personalizzati tramite la definizione di regole di accesso di rete. Tali regole possono essere configurate a livello di gruppi di Active Directory. Puoi implementare il controllo degli accessi anche utilizzando i gruppi di sicurezza.
- **Facilità d'uso:** consente di accedere alle risorse AWS e alle risorse locali utilizzando un singolo tunnel VPN.
- **Gestibilità:** consente di visualizzare i log di connessione che forniscono informazioni sui tentativi di connessione dei client. Puoi inoltre gestire le connessioni client attive con la possibilità di terminarle.

- **Massima integrazione:** si integra con i servizi AWS esistenti, incluso AWS Directory Service e Amazon VPC.

Componenti di Client VPN

Di seguito sono elencati i concetti fondamentali relativi a Client VPN:

Endpoint Client VPN

L'endpoint Client VPN è la risorsa che crei e configuri per abilitare e gestire le sessioni Client VPN. È il punto di chiusura per tutte le sessioni VPN client.

Rete target

Una rete target è la rete che associ a un endpoint Client VPN. Una sottorete di un VPC è una rete target. L'associazione di una sottorete a un endpoint Client VPN ti consente di stabilire le sessioni VPN. Puoi associare più sottoreti a un endpoint Client VPN per elevata disponibilità. Tutte le sottoreti devono provenire dallo stesso VPC. Ogni sottorete deve appartenere a una zona di disponibilità diversa.

Route

Ogni endpoint Client VPN ha una tabella di routing che descrive le route disponibili della rete di destinazione. Ogni route nella tabella di routing specifica il percorso del traffico a determinate risorse o reti.

Regole di autorizzazione

Una regola di autorizzazione limita gli utenti che possono accedere a una rete. Per una rete specificata, configuri il gruppo di Active Directory o provider di identità (IdP) a cui è consentito accedere. Solo gli utenti appartenenti a questo gruppo possono accedere alla rete specificata. Per impostazione predefinita, non sono definite regole di autorizzazione ed è necessario configurarle per consentire agli utenti di accedere alle risorse e alle reti.

Client

La connessione dell'utente finale all'endpoint Client VPN per stabilire una sessione VPN. Gli utenti finali devono scaricare un client OpenVPN e utilizzare il file di configurazione VPN Client creato per stabilire una sessione VPN.

Intervallo CIDR client

Intervallo di indirizzi IP da cui assegnare gli indirizzi IP del client. A ogni connessione all'endpoint Client VPN viene assegnato un indirizzo IP univoco dall'intervallo CIDR del client. Si sceglie l'intervallo CIDR client, ad esempio, 10.2.0.0/16.

Porte Client VPN

AWS Client VPN supporta le porte 443 e 1194 sia per TCP che per UDP. La porta 443 è predefinita.

Interfacce di rete Client VPN

Quando associ una sottorete all'endpoint Client VPN, vengono create le interfacce di rete Client VPN nella sottorete. Il traffico inviato al VPC dall'endpoint Client VPN viene inviato tramite un'interfaccia di rete Client VPN. Viene quindi applicata la Source Network Address Translation (SNAT), dove l'indirizzo IP di origine dell'intervallo CIDR client viene convertito nell'indirizzo IP dell'interfaccia di rete Client VPN.

Registrazione delle connessioni

Puoi abilitare la registrazione delle connessioni per l'endpoint Client VPN per registrare gli eventi di connessione. Puoi utilizzare queste informazioni per eseguire analisi forensi, analizzare come l'endpoint Client VPN viene utilizzato o eseguire il debug dei problemi di connessione.

Portale self-service

VPN Cliente fornisce un portale self-service come pagina Web per consentire agli utenti finali di scaricare la versione più recente del Client Desktop AWS VPN e la versione più recente del file di configurazione dell'endpoint di VPN Cliente che contiene le impostazioni necessarie per connettersi al proprio endpoint. L'amministratore dell'endpoint VPN Cliente può abilitare o disabilitare un portale self-service per l'endpoint di VPN Cliente. Il portale self-service è un servizio globale supportato da stack di servizi nelle seguenti regioni: Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Tokyo), Europa (Irlanda) e AWS GovCloud (Stati Uniti occidentali).

Utilizzo di Client VPN

Puoi utilizzare Client VPN in uno dei modi seguenti:

AWS Management Console

La console Amazon VPC fornisce un'interfaccia utente basata sul Web per Client VPN. Se hai eseguito la registrazione di un account Account AWS, puoi effettuare l'accesso alla console [Amazon VPC](#) e selezionare Client VPN nel riquadro di navigazione.

AWS Command Line Interface (AWS CLI)

AWS CLI fornisce l'accesso diretto alle API pubbliche di Client VPN. ed è supportata su Windows, macOS e Linux. Per ulteriori informazioni su come iniziare a utilizzare AWS CLI, consulta la [Guida per l'utente di AWS Command Line Interface](#). Per ulteriori informazioni sui comandi per Client VPN, consulta [Riferimento per i comandi della AWS CLI](#).

AWS Tools for Windows PowerShell

AWS fornisce comandi per un'ampia gamma di AWS offerte per coloro che eseguono script nell'ambiente. PowerShell Per ulteriori informazioni su come iniziare a utilizzare AWS Tools for Windows PowerShell, consulta la [Guida per l'utente di AWS Tools for Windows PowerShell](#). Per ulteriori informazioni sui cmdlet per Client VPN, consulta la [Documentazione di riferimento dei cmdlet di AWS Tools for Windows PowerShell](#).

API della query

L'API della query HTTPS Client VPN consente di accedere a livello di programmazione a Client VPN e AWS. L'API della query HTTPS ti consente di eseguire richieste HTTPS direttamente al servizio. Quando utilizzi le API HTTPS, devi includere il codice per firmare in modo digitale le richieste utilizzando le tue credenziali. Per ulteriori informazioni, consulta [Operazioni di AWS Client VPN](#).

Prezzi per Client VPN

Ti viene addebitato un addebito per ogni associazione di endpoint e ogni connessione VPN su base oraria. Per ulteriori informazioni, consulta [Prezzi di AWS Client VPN](#).

Ti viene addebitato un costo per il trasferimento dei dati da Amazon EC2 a Internet. Per ulteriori informazioni, consulta [Trasferimento dati](#) sulla pagina dei prezzi on demand di Amazon EC2.

Se abiliti la registrazione delle connessioni per il tuo endpoint Client VPN, devi creare un gruppo di log CloudWatch Logs nel tuo account. Si applicano addebiti per l'utilizzo dei gruppi di log. Per ulteriori informazioni, consulta [CloudWatch i prezzi di Amazon](#) (in Piano a pagamento, scegli Logs).

Se attivi l'handler di connessioni client per l'endpoint Client VPN devi creare e richiamare una funzione Lambda. Per richiamare le funzioni Lambda sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di AWS Lambda](#).

Gli endpoint Client VPN sono associati a una rete di destinazione, che è una sottorete in un VPC. Se questo VPC dispone di un Internet Gateway, associamo gli indirizzi IP elastici alle interfacce di rete elastiche (ENI) di Client VPN. Questi indirizzi IP elastici vengono addebitati come indirizzi IPv4 pubblici in uso. Per ulteriori informazioni, consulta la scheda Indirizzo IPv4 pubblico nella pagina dei prezzi del [VPC](#).

Regole e best practice di AWS Client VPN

Di seguito sono riportate le regole e le migliori pratiche per AWS Client VPN

- Esiste un limite di larghezza di banda di 10 Mbps per connessione utente.
- Gli intervalli CIDR client non possono sovrapporsi al CIDR locale del VPC in cui si trova la sottorete associata o a eventuali route aggiunte manualmente alla tabella di routing dell'endpoint Client VPN.
- L'intervallo CIDR del client deve avere una dimensione di blocco di almeno /22 e non superiore a /12.
- Una parte degli indirizzi nell'intervallo CIDR del client viene utilizzata per supportare il modello di disponibilità dell'endpoint Client VPN e non può essere assegnata ai client. Pertanto, ti consigliamo di assegnare un blocco CIDR contenente il doppio del numero di indirizzi IP richiesti per abilitare il numero massimo di connessioni simultanee che si intende supportare nell'endpoint Client VPN.
- L'intervallo CIDR del client non può essere modificato dopo aver creato l'endpoint Client VPN.
- Le sottoreti associate a un endpoint Client VPN devono trovarsi nello stesso VPC.
- Non è possibile associare più sottoreti dalla stessa zona di disponibilità a un endpoint Client VPN.
- Un endpoint Client VPN non supporta le associazioni di sottorete in un VPC di istanza dedicata a tenant singolo.
- Client VPN supporta solo il traffico IPv4. Consulta [Considerazioni IPv6 per AWS Client VPN](#) per i dettagli relativi a IPv6.
- Client VPN non è conforme agli standard FIPS (Federal Information Processing Standards).
- Il portale self-service non è disponibile per i client che eseguono l'autenticazione reciproca.
- Non consigliamo di connetterti a un endpoint Client VPN utilizzando gli indirizzi IP. Poiché Client VPN è un servizio gestito, occasionalmente verranno visualizzati gli indirizzi IP che il nome DNS

risolve per modificare. Inoltre, vedrai le interfacce di rete Client VPN eliminate e ricreate nei tuoi CloudTrail log. Si consiglia di connettersi all'endpoint Client VPN utilizzando il nome DNS fornito.

- L'inoltro IP non è attualmente supportato quando si utilizza l'applicazione desktop AWS Client VPN. L'inoltro IP è supportato da altri client.
- Client VPN non supporta la replica multi-regione in AWS Managed Microsoft AD. L'endpoint Client VPN deve trovarsi nella stessa regione della risorsa AWS Managed Microsoft AD.
- Se l'autenticazione a più fattori è disabilitata per Active Directory, il formato della password utente non può essere il seguente.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Non è possibile stabilire una connessione VPN da un computer se ci sono più utenti connessi al sistema operativo.
- Il servizio Client VPN richiede che l'indirizzo IP a cui è connesso il client corrisponda all'IP a cui si risolve il nome DNS dell'endpoint Client VPN. In altre parole, se imposti un record DNS personalizzato per l'endpoint Client VPN e poi inoltri il traffico all'indirizzo IP effettivo su cui si risolve il nome DNS dell'endpoint, questa configurazione non funzionerà con i client forniti di recente. AWS Questa regola è stata aggiunta per mitigare un attacco IP al server come descritto qui: [TunnelCrack](#)
- Il servizio Client VPN richiede che gli intervalli di indirizzi IP della rete locale (LAN) dei dispositivi client rientrino nei seguenti intervalli di indirizzi IP privati standard: 10.0.0.0/8, 16.0.0.0/12, 192.168.0.0/16, o 169.254.0.0/16. Se viene rilevato che l'intervallo di indirizzi LAN del client non rientra negli intervalli precedenti, l'endpoint Client VPN invierà automaticamente la direttiva OpenVPN «redirect-gateway block-local» al client, forzando tutto il traffico LAN a entrare nella VPN. Pertanto, se è necessario l'accesso alla LAN durante le connessioni VPN, si consiglia di utilizzare gli intervalli di indirizzi convenzionali sopra elencati per la rete LAN. Questa regola viene applicata per mitigare le possibilità di un attacco alla rete locale, come descritto qui: [TunnelCrack](#)

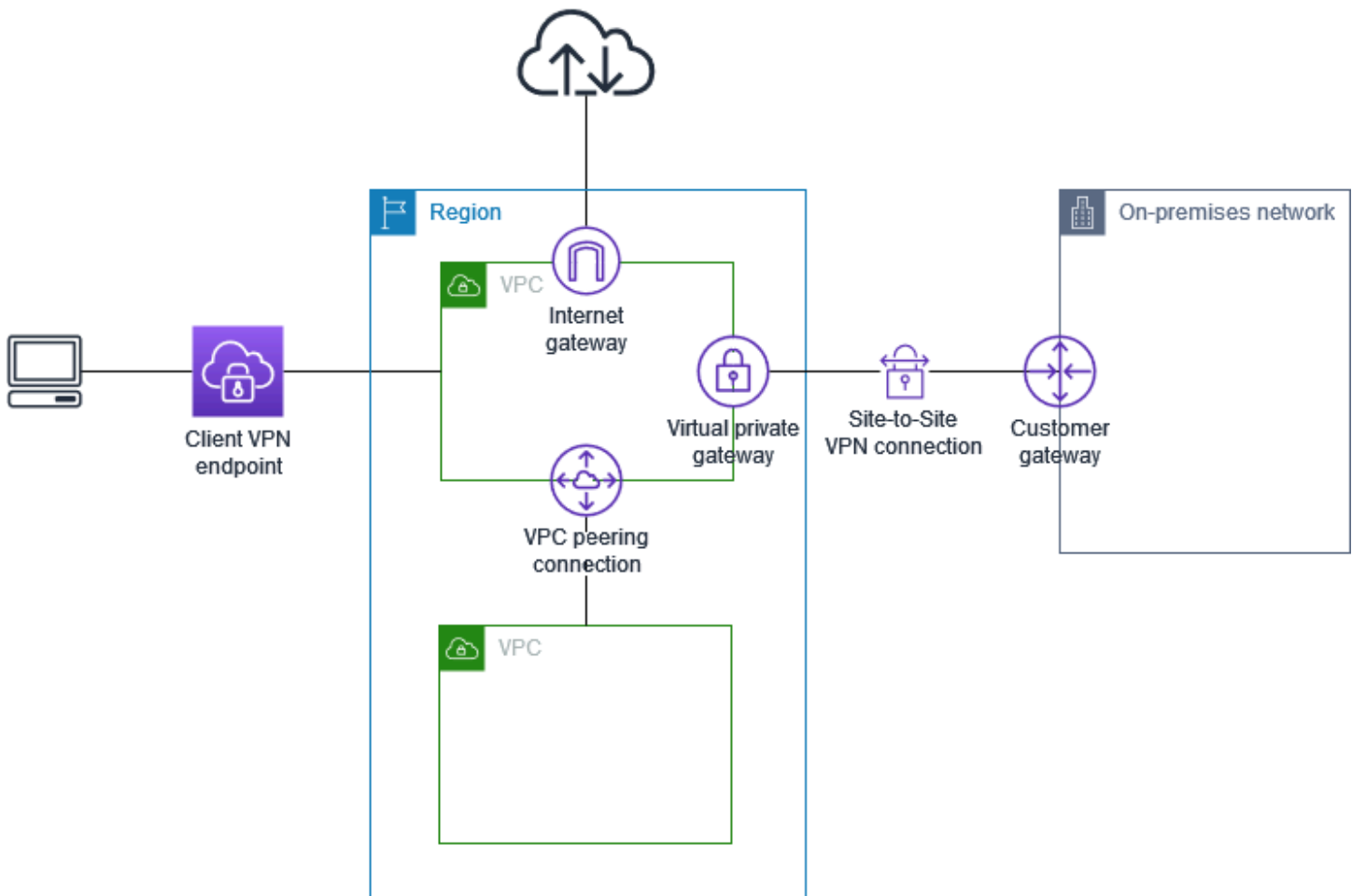
Come funziona AWS Client VPN

Con AWS Client VPN ci sono due tipi di utenti che interagiscono con l'endpoint Client VPN: amministratori e client.

L'amministratore è responsabile dell'impostazione e della configurazione del servizio. Queste attività includono la creazione dell'endpoint Client VPN, l'associazione della rete di destinazione, la configurazione delle regole di autorizzazione e l'impostazione di route aggiuntive (se necessario). Una volta impostato e configurato l'endpoint Client VPN, l'amministratore scarica il file di configurazione dell'endpoint Client VPN e lo distribuisce ai client che devono accedere. Il file di configurazione dell'endpoint Client VPN include il nome DNS dell'endpoint Client VPN e le informazioni di autenticazione necessarie per stabilire una sessione VPN. Per ulteriori informazioni sulla configurazione del servizio, consulta [Nozioni di base su AWS Client VPN](#).

Il client è l'utente finale. È la persona che si connette all'endpoint Client VPN per stabilire una sessione VPN. Il client stabilisce la sessione VPN dal proprio computer locale o dispositivo mobile utilizzando un'applicazione client VPN basata su OpenVPN. Dopo aver stabilito la sessione VPN, può accedere in modo sicuro alle risorse del VPC in cui si trova la sottorete associata. Può anche accedere ad altre risorse in AWS, in una rete locale o in altri client, se sono state configurate le regole di routing e autorizzazione richieste. Per ulteriori informazioni sulla connessione a un endpoint Client VPN per stabilire una sessione VPN, consulta [Nozioni di base](#) nella Guida per l'utente di AWS Client VPN.

L'immagine riportata di seguito illustra l'architettura Client VPN di base.



Autenticazione client

L'autenticazione del client viene implementata al primo punto di ingresso nel AWS Cloud. È utilizzata per determinare se i client sono autorizzati a connettersi all'endpoint Client VPN. Se l'autenticazione va a buon fine, i client si connettono all'endpoint Client VPN e stabiliscono una sessione VPN. Se l'autenticazione ha esito negativo, la connessione viene negata e il client non è in grado di stabilire una sessione VPN.

Client VPN offre i seguenti tipi di autenticazione client:

- [Autenticazione di Active Directory](#) (basata sull'utente)
- [Autenticazione reciproca](#) (basata su certificato)
- [Single Sign-On \(autenticazione federata basata su SAML\)](#) (basata sull'utente)

È possibile utilizzare uno dei metodi elencati in precedenza da soli o una combinazione di autenticazione reciproca con un metodo basato sull'utente, come il seguente:

- Autenticazione reciproca e autenticazione federata
- Autenticazione reciproca e autenticazione di Active Directory

Important

Per creare un endpoint Client VPN, è necessario fornire un certificato server in AWS Certificate Manager, indipendentemente dal tipo di autenticazione utilizzato. Per ulteriori informazioni sulla creazione e il provisioning di un certificato server, consulta le fasi in [Autenticazione reciproca](#).

Autenticazione Active Directory

Client VPN fornisce supporto per Active Directory mediante l'integrazione con AWS Directory Service. Con l'autenticazione Active Directory, i client vengono autenticati rispetto a gruppi di Active Directory esistenti. Utilizzando AWS Directory Service, Client VPN può connettersi alle Active Directory esistenti fornite nella AWS o nella rete locale. In questo modo puoi utilizzare l'infrastruttura di autenticazione client esistente. Se si utilizza un Active Directory locale e non si dispone di un AWS Managed Microsoft AD, è necessario configurare un connettore Active Directory (AD Connector). Puoi utilizzare un server Active Directory per autenticare gli utenti. Per ulteriori informazioni sull'integrazione di Active Directory, consulta [Guida per l'amministratore di AWS Directory Service](#).

Client VPN supporta l'autenticazione a più fattori (MFA) quando è abilitata per AWS Managed Microsoft AD o AD Connector. Se l'autenticazione MFA è abilitata, i client devono immettere un nome utente, una password e un codice MFA quando si connettono a un endpoint Client VPN. Per ulteriori informazioni sull'abilitazione di MFA, consulta [Abilitazione dell'autenticazione a più fattori per AWS Managed Microsoft AD](#) e [Abilitazione dell'autenticazione a più fattori per AD Connector](#) nella Guida per l'amministratore di AWS Directory Service .

Per le quote e le regole per la configurazione di utenti e gruppi in Active Directory, consulta [Quote di utenti e gruppi](#).

Autenticazione reciproca

Con l'autenticazione reciproca, Client VPN utilizza i certificati per eseguire l'autenticazione tra client e server. I certificati sono un modulo digitale di identificazione emesso da un'autorità di certificazione (CA). Il server utilizza i certificati client per autenticare i client quando tentano di connettersi all'endpoint Client VPN. È necessario creare un certificato server e una chiave e almeno un certificato client e una chiave.

È necessario caricare il certificato del server su AWS Certificate Manager (ACM) e specificarlo quando si crea un endpoint Client VPN. Quando si carica il certificato del server in ACM, si specifica anche l'autorità di certificazione (CA). Il certificato client deve essere caricato su ACM solo quando la CA del certificato client è diversa da quella del certificato server. Per ulteriori informazioni su ACM, consulta la [Guida per l'utente di AWS Certificate Manager](#).

Puoi creare un certificato client e una chiave separati per ogni client che si connette all'endpoint Client VPN. Questo consente di revocare un certificato client specifico se un utente lascia l'organizzazione. In questo caso, quando crei l'endpoint Client VPN puoi specificare il certificato ARN del server per il certificato client, a condizione che il certificato client sia stato emesso dalla stessa autorità di certificazione del certificato server.

Note

Un endpoint Client VPN supporta solo chiavi RSA a 1024 bit e 2048 bit. Inoltre, il certificato client deve avere l'attributo CN nel campo Subject (Oggetto).

Quando i certificati utilizzati con il servizio VPN Client vengono aggiornati, tramite la rotazione automatica di ACM, l'importazione manuale di un nuovo certificato o gli aggiornamenti dei metadati in Centro identità IAM, il servizio VPN Client aggiorna automaticamente l'endpoint VPN Client con il certificato più recente. Questo è un processo automatizzato che può richiedere fino a 24 ore.

Linux/macOS

La seguente procedura utilizza OpenVPN easy-rsa per generare i certificati e le chiavi server e client e caricare il certificato e la chiave server in ACM. Per ulteriori informazioni, consulta il file [README di Easy-RSA 3 Quickstart](#).

Per generare i certificati e le chiavi server e client e caricarli in ACM

1. Clonare il repository OpenVPN easy-rsa sul computer locale e passare alla cartella easy-rsa/easyrsa3.

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

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

2. Inizializzare un nuovo ambiente PKI.

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

3. Per creare una nuova autorità di certificazione (CA), eseguire questo comando e seguire le istruzioni.

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

4. Generare il certificato e la chiave server.

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

5. Generare il certificato e la chiave client.

Salvare il certificato e la chiave privata client perché saranno necessari quando si configura il client.

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

Facoltativamente, è possibile ripetere questa fase per ogni client (utente finale) che richiede un certificato client e una chiave.

6. Copiare il certificato e la chiave server e il certificato e la chiave client in una cartella personalizzata e quindi passare alla cartella personalizzata.

Prima di copiare i certificati e le chiavi, creare la cartella personalizzata utilizzando il comando `mkdir`. Nell'esempio seguente viene creata una cartella personalizzata nella directory home.

```
$ 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. Carica il certificato e la chiave server e il certificato e la chiave client in ACM. Assicurati di caricarli nella stessa regione in cui desideri creare l'endpoint Client VPN. I seguenti comandi utilizzano l'interfaccia a riga di comando di AWS CLI per caricare i certificati. Per caricare i certificati utilizzando la console ACM, consulta [Importazione di un certificato](#) nella Guida per l'utente di AWS Certificate Manager .

```
$ 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
```

Non è necessario caricare il certificato client su ACM. Se i certificati server e client sono stati emessi dalla stessa certification authority (CA), quando crei l'endpoint Client VPN sarà possibile utilizzare l'ARN del certificato server sia per il server che per il client. Nei passaggi precedenti, per creare entrambi i certificati è stata utilizzata la stessa CA. Tuttavia, per completezza sono stati inclusi i passaggi per caricare il certificato client.

Windows

La procedura seguente installa il software Easy-RSA 3.x e lo utilizza per generare i certificati e le chiavi server e client.

Per generare i certificati e le chiavi server e client e caricarli in ACM

1. Apri la pagina delle [versioni di EasyRSA](#) e scarica il file ZIP della tua versione di Windows ed estrailo.
2. Apri un prompt dei comandi e passa alla posizione in cui è stata estratta la cartella EasyRSA-3.x.
3. Eseguire il comando seguente per aprire la shell di EasyRSA 3.

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

4. Inizializzare un nuovo ambiente PKI.

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

5. Per creare una nuova autorità di certificazione (CA), eseguire questo comando e seguire le istruzioni.

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

6. Generare il certificato e la chiave server.

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

7. Generare il certificato e la chiave client.

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

Facoltativamente, è possibile ripetere questa fase per ogni client (utente finale) che richiede un certificato client e una chiave.

8. Uscire dalla shell EasyRSA 3.

```
# exit
```

9. Copiare il certificato e la chiave server e il certificato e la chiave client in una cartella personalizzata e quindi passare alla cartella personalizzata.

Prima di copiare i certificati e le chiavi, creare la cartella personalizzata utilizzando il comando `mkdir`. Nell'esempio seguente viene creata una cartella personalizzata nell'unità C:\.

```
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
```

- Carica il certificato e la chiave server e il certificato e la chiave client in ACM. Assicurati di caricarli nella stessa regione in cui desideri creare l'endpoint Client VPN. I seguenti comandi utilizzano il AWS CLI per caricare i certificati. Per caricare i certificati utilizzando la console ACM, consulta [Importazione di un certificato](#) nella Guida per l'utente di AWS Certificate Manager .

```
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
```

Non è necessario caricare il certificato client su ACM. Se i certificati server e client sono stati emessi dalla stessa certification authority (CA), quando crei l'endpoint Client VPN sarà possibile utilizzare l'ARN del certificato server sia per il server che per il client. Nei passaggi precedenti, per creare entrambi i certificati è stata utilizzata la stessa CA. Tuttavia, per completezza sono stati inclusi i passaggi per caricare il certificato client.

Rinnovo del certificato del server

È possibile rinnovare e importare un certificato del server scaduto con la procedura seguente.

- Esecuzione del comando di rinnovo del certificato.

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

- Crea una cartella personalizzata, copia i nuovi file, quindi accedi alla cartella.

```
$ 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/
```

- Importa i nuovi file in ACM. Assicurati di importarli nella stessa regione dell'endpoint client VPN.

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

Single Sign-On (autenticazione federata basata su SAML 2.0)

AWS Client VPN supporta la federazione delle identità con Security Assertion Markup Language 2.0 (SAML 2.0) per gli endpoint Client VPN. Puoi utilizzare provider di identità (IdPs) che supportano SAML 2.0 per creare identità utente centralizzate. Puoi quindi configurare un endpoint Client VPN per utilizzare l'autenticazione federata basata su SAML e associarlo al provider di identità. Gli utenti si connettono quindi all'endpoint Client VPN utilizzando le credenziali centralizzate.

Per consentire al provider di identità basato su SAML di utilizzare un endpoint Client VPN, è necessario eseguire le operazioni seguenti.

1. Crea un'app basata su SAML nell'IdP prescelto da utilizzare con AWS Client VPN o utilizza un'app esistente.
2. Configurare il provider di identità per stabilire una relazione di trust con AWS. Per le risorse, consulta [Risorse di configurazione IdP basate su SAML](#).
3. Nel provider di identità, generare e scaricare un documento di metadati della federazione che descrive l'organizzazione come un provider di identità. Questo documento XML firmato viene utilizzato per stabilire la relazione di fiducia tra AWS e l'IdP.
4. Crea un provider di identità IAM SAML nello stesso AWS account dell'endpoint Client VPN. Il provider di identità IAM SAML definisce la relazione AWS IdP-trust dell'organizzazione utilizzando il documento di metadati generato dall'IdP. Per ulteriori informazioni, consulta [Creazione di provider di identità SAML IAM](#) nella Guida per l'utente di IAM. Se in seguito aggiorni la configurazione dell'app nel provider di identità, genera un nuovo documento di metadati e aggiorna il provider di identità SAML IAM.

Note

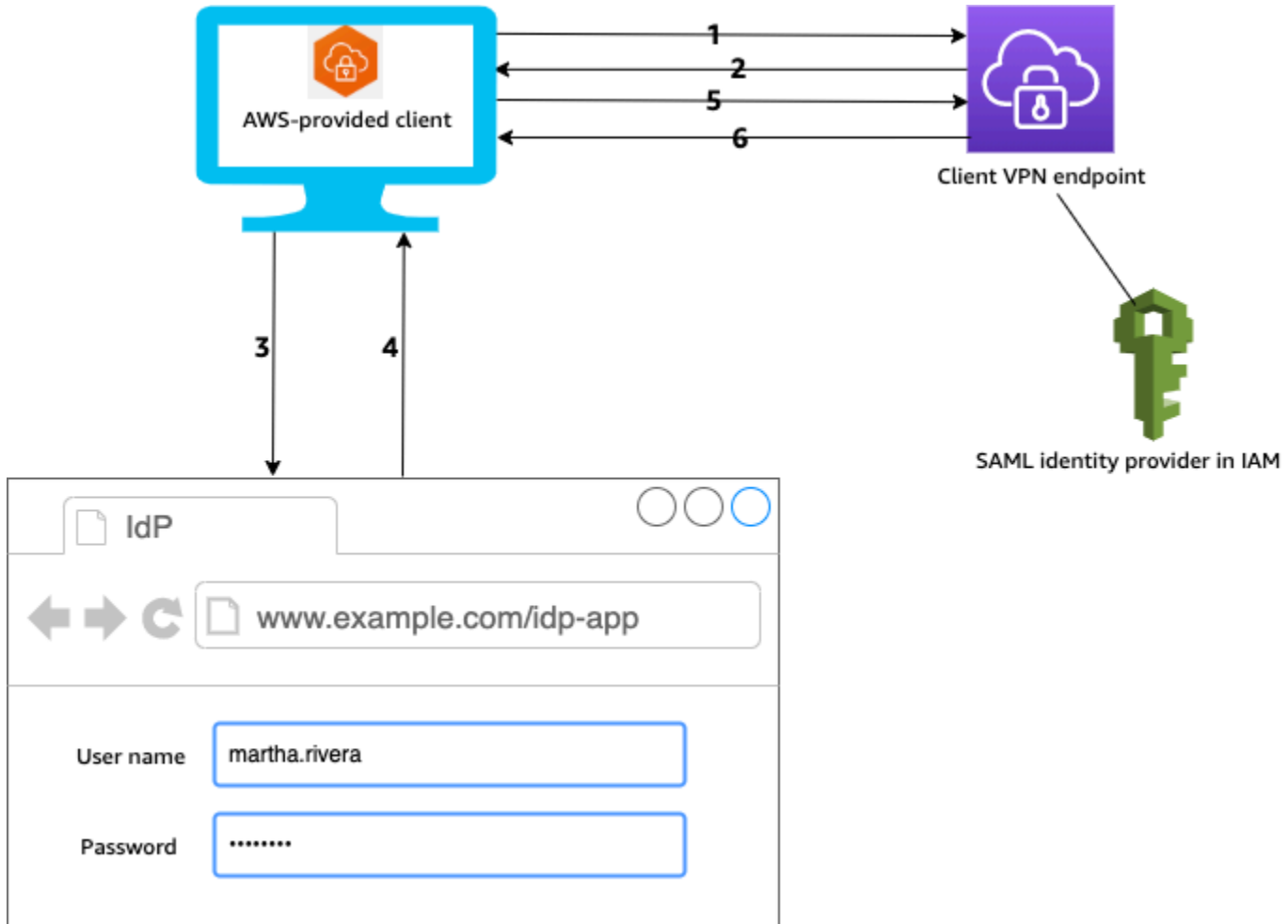
Non è necessario creare un ruolo IAM per utilizzare il provider di identità SAML IAM.

5. Crea un endpoint Client VPN. Specifica l'autenticazione federata come tipo di autenticazione e specifica il provider di identità SAML IAM che hai creato. Per ulteriori informazioni, consulta [Creare un endpoint Client VPN](#).
6. Esportare il [file di configurazione del client](#) e distribuirlo agli utenti. Chiedi agli utenti di scaricare la versione più recente del [client fornito da AWS](#) e di utilizzarla per caricare il file di configurazione ed eseguire la connessione all'endpoint Client VPN. In alternativa, se hai abilitato il portale self-service per il tuo endpoint Client VPN, chiedi ai tuoi utenti di accedere al portale self-service per

ottenere il file di configurazione e il client fornito. AWS Per ulteriori informazioni, consulta [Accedere al portale self-service](#).

Flusso di lavoro di autenticazione

Nel diagramma seguente viene fornita una panoramica del flusso di lavoro di autenticazione per un endpoint Client VPN che utilizza l'autenticazione federata basata su SAML. Quando crei e configuri l'endpoint Client VPN, specifichi il provider di identità SAML IAM.



1. L'utente apre il client AWS fornito sul proprio dispositivo e avvia una connessione all'endpoint Client VPN.
2. L'endpoint Client VPN invia un URL di provider di identità e una richiesta di autenticazione al client, in base alle informazioni fornite nel provider di identità SAML IAM.
3. Il client AWS fornito apre una nuova finestra del browser sul dispositivo dell'utente. Il browser effettua una richiesta al provider di identità e visualizza una pagina di accesso.

4. L'utente immette le proprie credenziali nella pagina di accesso e il provider di identità invia un'asserzione SAML firmata al client.
5. Il client AWS fornito invia l'asserzione SAML all'endpoint Client VPN.
6. L'endpoint Client VPN convalida l'asserzione e consente o rifiuta l'accesso all'utente.

Requisiti e considerazioni per l'autenticazione federata basata su SAML

Di seguito sono riportati i requisiti e le considerazioni per l'autenticazione federata basata su SAML.

- Per le quote e le regole per la configurazione di utenti e gruppi in un provider di identità basato su SAML, consulta [Quote di utenti e gruppi](#).
- L'asserzione SAML e i documenti SAML devono essere firmati.
- AWS Client VPN supporta solo le condizioni "AudienceRestriction" e "NotBefore e NotOnOrAfter" nelle asserzioni SAML.
- La dimensione massima supportata per le risposte SAML è di 128 KB.
- AWS Client VPN non fornisce richieste di autenticazione firmate.
- La disconnessione singola SAML non è supportata. Gli utenti possono disconnettersi disconnettendosi dal client AWS fornito oppure è possibile [interrompere le](#) connessioni.
- Un endpoint Client VPN supporta solo un singolo provider di identità.
- Multi-factor authentication (MFA) è supportata quando è abilitata nel provider di identità.
- Gli utenti devono utilizzare il client AWS fornito per connettersi all'endpoint Client VPN. È richiesta la versione 1.2.0 o successiva. Per ulteriori informazioni, consulta [Connect using the AWS provided client](#).
- Per l'autenticazione IdP sono supportati i seguenti browser: Apple Safari, Google Chrome, Microsoft Edge e Mozilla Firefox.
- Il client AWS fornito riserva la porta TCP 35001 sui dispositivi degli utenti per la risposta SAML.
- Se il documento di metadati per il provider di identità SAML IAM viene aggiornato con un URL errato o dannoso, si possono verificare problemi di autenticazione per gli utenti o generare attacchi di phishing. Pertanto, si consiglia di utilizzare AWS CloudTrail per monitorare gli aggiornamenti che vengono effettuati al provider di identità SAML IAM. Per ulteriori informazioni, consulta [Registrazione di chiamate IAM e AWS STS con AWS CloudTrail](#) nella Guida per l'utente di IAM.
- AWS Client VPN invia una richiesta AuthN all'IdP tramite un'associazione di reindirizzamento HTTP. Pertanto, il provider di identità dovrebbe supportare l'associazione di reindirizzamento HTTP e deve essere presente nel documento di metadati del provider di identità.

- Per l'asserzione SAML, è necessario utilizzare un formato di indirizzo e-mail per l'attributo NameID.

Risorse di configurazione IdP basate su SAML

La tabella seguente elenca i modelli basati su SAML con IdPs AWS Client VPN cui abbiamo testato l'utilizzo e le risorse che possono aiutarti a configurare l'IdP.

IdP	Risorsa
Okta	Autentica AWS Client VPN gli utenti con SAML
Microsoft Azure Active Directory	Per altre informazioni, vedi Tutorial: Integrazione single sign-on (SSO) di Azure Active Directory con AWS ClientVPN nel sito Web della documentazione Microsoft.
JumpCloud	Single Sign-On (SSO) con AWS Client VPN
AWS IAM Identity Center	Utilizzo di IAM Identity Center con AWS Client VPN per l'autenticazione e l'autorizzazione

Informazioni sul fornitore di servizi per la creazione di un'app

Per creare un'app basata su SAML utilizzando un IdP non elencato nella tabella precedente, utilizza le seguenti informazioni per configurare le informazioni sul fornitore di servizi. AWS Client VPN

- URL ACS (Assertion Consumer Service): `http://127.0.0.1:35001`
- URI audience: `urn:amazon:webservices:clientvpn`

Almeno un attributo deve essere incluso nella risposta SAML dell'IdP. Di seguito vengono mostrati degli attributi di esempio.

Attributo	Descrizione
FirstName	Il nome dell'utente.
LastName	Il cognome dell'utente.

Attributo	Descrizione
memberOf	Il gruppo o i gruppi a cui appartiene l'utente.

Note

L'attributo `memberOf` è necessario per utilizzare le regole di autorizzazione basate sui gruppi Active Directory o SAML IdP. Gli attributi fanno distinzione tra maiuscole e minuscole e devono essere configurati esattamente come specificato. Per ulteriori informazioni, consulta [Autorizzazione di rete](#) e [Regole di autorizzazione](#).

Supporto per il portale self-service

Se abiliti il portale self-service per l'endpoint Client VPN, gli utenti accedono al portale utilizzando le proprie credenziali del provider di identità basate su SAML.

Se il tuo provider di identità supporta molteplici URL Assertion Consumer Service (ACS), aggiungi il seguente URL ACS all'app.

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

Se utilizzi l'endpoint Client VPN in una GovCloud regione, utilizza invece il seguente URL ACS. Se utilizzi la stessa app IDP per l'autenticazione sia per gli standard che per le GovCloud regioni, puoi aggiungere entrambi gli URL.

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

Se il provider di identità non supporta molteplici URL ACS, effettua le seguenti operazioni:

1. Crea un'app aggiuntiva basata su SAML nel provider di identità e specifica il seguente URL ACS.

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

2. Genera e scarica un documento di metadati della federazione.
3. Crea un provider di identità IAM SAML nello stesso AWS account dell'endpoint Client VPN. Per ulteriori informazioni, consulta [Creazione di provider di identità SAML IAM](#) nella Guida per l'utente di IAM.

Note

Crei questo provider di identità SAML IAM in aggiunta a quello [creato per l'app principale](#).

4. [Crea l'endpoint Client VPN](#) e specifica entrambi i provider di identità SAML IAM creati.

Autorizzazione client

Il client VPN supporta due tipi di autorizzazione: i gruppi di sicurezza e l'autorizzazione di rete (tramite le regole di autorizzazione).

Gruppi di sicurezza

Quando crei un endpoint Client VPN, puoi specificare i gruppi di sicurezza da un VPC specifico da applicare all'endpoint Client VPN. Quando associ una sottorete a un endpoint Client VPN, il gruppo di sicurezza predefinito del VPC viene applicato automaticamente. Puoi modificare i gruppi di sicurezza dopo aver creato l'endpoint Client VPN. Per ulteriori informazioni, consulta [Applicazione di un gruppo di sicurezza a una rete target](#). I gruppi di sicurezza sono associati alle interfacce di rete Client VPN.

Puoi consentire agli utenti Client VPN di accedere alle applicazioni in un VPC aggiungendo una regola ai gruppi di sicurezza delle applicazioni per consentire il traffico dal gruppo di sicurezza applicato all'associazione.

Per aggiungere una regola che consenta il traffico dal gruppo di sicurezza degli endpoint Client VPN

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Scegliere il gruppo di sicurezza associato alla risorsa o all'applicazione e scegliere Operazioni, Modifica le regole in entrata.
4. Scegliere Add rule (Aggiungi regola).
5. In Type (Tipo), selezionare All traffic (Tutto il traffico). In alternativa, è possibile limitare l'accesso a un tipo specifico di traffico, ad esempio SSH.

Per Source (Origine), specifica l'ID del gruppo di sicurezza associato alla rete di destinazione (sottorete) per l'endpoint Client VPN.

6. Scegliere Save rules (Salva regole).

Puoi limitare l'accesso per gli utenti Client VPN non specificando il gruppo di sicurezza applicato all'associazione o rimuovendo la regola che fa riferimento al gruppo di sicurezza dell'endpoint Client VPN. Le regole del gruppo di sicurezza necessarie potrebbero dipendere anche dal tipo di accesso VPN che si desidera configurare. Per ulteriori informazioni, consulta [Scenari ed esempi per AWS Client VPN](#).

Per ulteriori informazioni sui gruppi di sicurezza, consulta [Gruppi di sicurezza per il VPC](#) nella Guida per l'utente di Amazon VPC.

Autorizzazione di rete

L'autorizzazione di rete viene implementata utilizzando le regole di autorizzazione. Per ogni rete di cui desideri abilitare l'accesso, devi configurare le regole di autorizzazione per limitare gli utenti che possono accedere. Per una rete specificata, configuri il gruppo di Active Directory o il gruppo IdP basato su SAML a cui è consentito accedere. Solo gli utenti che appartengono al gruppo specificato sono in grado di accedere alla rete specificata. Se non usi Active Directory o l'autenticazione federata basata su SAML o se desideri autorizzare l'accesso per tutti gli utenti, puoi specificare una regola che conceda l'accesso a tutti i client. Per ulteriori informazioni, consulta [Regole di autorizzazione](#).

Autorizzazione di connessione

Puoi configurare un handler di connessioni client per l'endpoint Client VPN. L'handler consente di eseguire una logica personalizzata che autorizza una nuova connessione, in base agli attributi del dispositivo, dell'utente e della connessione. L'handler delle connessioni client viene eseguito dopo che il servizio Client VPN ha autenticato il dispositivo e l'utente.

Per configurare un handler delle connessioni client per l'endpoint Client VPN, crea una funzione AWS Lambda che prende gli attributi del dispositivo, dell'utente e della connessione come input e restituisce una decisione al servizio Client VPN per consentire o negare una nuova connessione. Specifica la funzione Lambda nell'endpoint Client VPN. Quando i dispositivi si connettono all'endpoint Client VPN, il servizio Client VPN richiama la funzione Lambda per conto dell'utente. Solo le connessioni autorizzate dalla funzione Lambda possono connettersi all'endpoint Client VPN.

Note

Attualmente, l'unico tipo di handler delle connessioni client supportato è una funzione Lambda.

Requisiti e considerazioni

Di seguito sono riportati i requisiti e le considerazioni per l'handler delle connessioni client:

- Il nome della funzione Lambda deve iniziare con il prefisso `AWSClientVPN-`.
- Sono supportate le funzioni Lambda complete.
- La funzione Lambda deve trovarsi nella stessa AWS regione e nello stesso AWS account dell'endpoint Client VPN.
- Il timeout della funzione Lambda si verifica dopo 30 secondi. Questo valore non può essere modificato.
- La funzione Lambda viene richiamata in modo sincrono. Viene richiamata dopo l'autenticazione del dispositivo e dell'utente e prima che vengano valutate le regole di autorizzazione.
- Se la funzione Lambda viene richiamata per una nuova connessione e il servizio Client VPN non ottiene una risposta prevista dalla funzione, il servizio Client VPN rifiuta la richiesta di connessione. Ad esempio, ciò può verificarsi se la funzione Lambda viene limitata, se si verifica un errore imprevisto o se la risposta della funzione non è in un formato valido.
- Consigliamo di configurare la [concorrenza con provisioning](#) per la funzione Lambda per consentirne la scalabilità senza fluttuazioni di latenza.
- Se aggiorni la funzione Lambda, le connessioni esistenti all'endpoint Client VPN non sono interessate. Puoi terminare le connessioni esistenti e quindi indicare ai client di stabilire nuove connessioni. Per ulteriori informazioni, consulta [Terminazione di una connessione client](#).
- Se i client utilizzano il client AWS fornito per connettersi all'endpoint Client VPN, devono utilizzare la versione 1.2.6 o successiva per Windows e la versione 1.2.4 o successiva per macOS. Per ulteriori informazioni, consulta [Connessione mediante il client fornito da AWS](#).

Interfaccia Lambda

La funzione Lambda accetta gli attributi del dispositivo, gli attributi dell'utente e gli attributi della connessione come input dal servizio Client VPN. Deve quindi restituire una decisione al servizio Client VPN se consentire o negare la connessione.

Schema di richiesta

La funzione Lambda accetta un blob JSON contenente i seguenti campi come input.

```
{
```

```
"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`: l'ID della connessione client all'endpoint Client VPN.
- `endpoint-id`: l'ID dell'endpoint Client VPN.
- `common-name`: l'identificatore del dispositivo. Nel certificato client creato per il dispositivo, il nome comune identifica in modo univoco il dispositivo.
- `username`: l'identificatore dell'utente, se applicabile. Per l'autenticazione di Active Directory, questo è il nome utente. Per l'autenticazione federata basata su SAML, questo è NameID. Per l'autenticazione reciproca, questo campo è vuoto.
- `platform`: la piattaforma del sistema operativo client.
- `platform-version`: la versione del sistema operativo. Il servizio Client VPN fornisce un valore quando la direttiva `--push-peer-info` è presente nella configurazione del client OpenVPN quando i client si connettono a un endpoint Client VPN e quando il client è in esecuzione sulla piattaforma Windows.
- `public-ip`: l'indirizzo IP pubblico del dispositivo di connessione.
- `client-openvpn-version`: la versione OpenVPN utilizzata dal client.
- `aws-client-version`— La versione del client. AWS
- `groups`: l'identificatore del gruppo, se applicabile. Per l'autenticazione Active Directory, questo sarà un elenco di gruppi di Active Directory. Per l'autenticazione federata basata su SAML, questo sarà un elenco di gruppi di provider di identità (IdP). Per l'autenticazione reciproca, questo campo è vuoto.
- `schema-version`: la versione dello schema. Il valore di default è v3.

Schema di risposta

La funzione Lambda deve restituire i seguenti campi.

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

- `allow`: obbligatorio. Un valore booleano (`true` | `false`) che indica se consentire o negare la nuova connessione.
- `error-msg-on-denied-connection`: obbligatorio. Una stringa di massimo 255 caratteri che può essere utilizzata per fornire fasi e indicazioni ai client se la connessione viene negata dalla funzione Lambda. In caso di errori durante l'esecuzione della funzione Lambda (ad esempio a causa del throttling) il seguente messaggio predefinito viene restituito ai client.

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

- `posture-compliance-statuses`: obbligatorio. Se usi la funzione Lambda per la [valutazione dell'assetto](#), questo è l'elenco degli stati per il dispositivo di collegamento. Puoi definire i nomi degli stati in base alle categorie di valutazione dell'assetto per i dispositivi, ad esempio `compliant`, `quarantined`, `unknown` e così via. Ogni nome può contenere al massimo 255 caratteri. È possibile specificare fino a 10 stati.
- `schema-version`: obbligatorio. Versione dello schema. Il valore di default è `v3`.

Puoi utilizzare la stessa funzione Lambda per più endpoint Client VPN nella stessa regione.

Per ulteriori informazioni sulla creazione di una funzione Lambda, consulta [Nozioni di base su AWS Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

Utilizzo dell'handler delle connessioni client per la valutazione dell'assetto

Puoi utilizzare l'handler delle connessioni client per integrare l'endpoint Client VPN con la soluzione di gestione dei dispositivi esistente per valutare la conformità dell'assetto dei dispositivi di connessione. Perché la funzione Lambda funzioni come handler di autorizzazione del dispositivo, utilizza [l'autenticazione reciproca](#) per l'endpoint Client VPN. Crea un certificato e una chiave client univoci per ogni client (dispositivo) che si conatterà all'endpoint Client VPN. La funzione Lambda può utilizzare il nome comune univoco per il certificato client (passato dal servizio Client VPN) per identificare il

dispositivo e recuperare lo stato di conformità dell'assetto dalla soluzione di gestione del dispositivo. Puoi utilizzare l'autenticazione reciproca combinata con l'autenticazione basata sull'utente.

In alternativa, puoi eseguire una valutazione dell'assetto di base nella funzione Lambda stessa. Ad esempio, puoi valutare i campi `platform` e `platform-version` che vengono passati alla funzione Lambda dal servizio Client VPN.

Note

Sebbene il gestore di connessione possa essere utilizzato per imporre una versione minima AWS Client VPN dell'applicazione, il campo `aws-client-version` del gestore di connessione è applicabile solo all'AWS Client VPN applicazione e viene compilato dalle variabili di ambiente sul dispositivo utente.

Abilitazione dell'handler delle connessioni client

Per abilitare l'handler delle connessioni client, crea o modifica un endpoint Client VPN e specifica l'Amazon Resource Name (ARN) della funzione Lambda. Per ulteriori informazioni, consulta [Creare un endpoint Client VPN](#) e [Modifica un endpoint Client VPN](#).

Ruolo collegato ai servizi

AWS Client VPN crea automaticamente un ruolo collegato al servizio nell'account chiamato `AWSServiceRoleForClientVPNConnections`. Il ruolo dispone delle autorizzazioni per richiamare la funzione Lambda quando viene effettuata una connessione all'endpoint Client VPN. Per ulteriori informazioni, consulta [Utilizzo dei ruoli collegati ai servizi per Client VPN](#).

Monitoraggio degli errori di autorizzazione della connessione

Puoi visualizzare lo stato di autorizzazione delle connessioni all'endpoint Client VPN. Per ulteriori informazioni, consulta [Visualizzazione delle connessioni client](#).

Quando l'handler delle connessioni client viene utilizzato per la valutazione dell'assetto, puoi inoltre visualizzare gli stati di conformità dell'assetto dei dispositivi che si connettono all'endpoint Client VPN nei log delle connessioni. Per ulteriori informazioni, consulta [Registrazione delle connessioni](#).

Se un dispositivo non ottiene l'autorizzazione della connessione, il campo `connection-attempt-failure-reason` nei log delle connessioni restituisce uno dei seguenti motivi di errore:

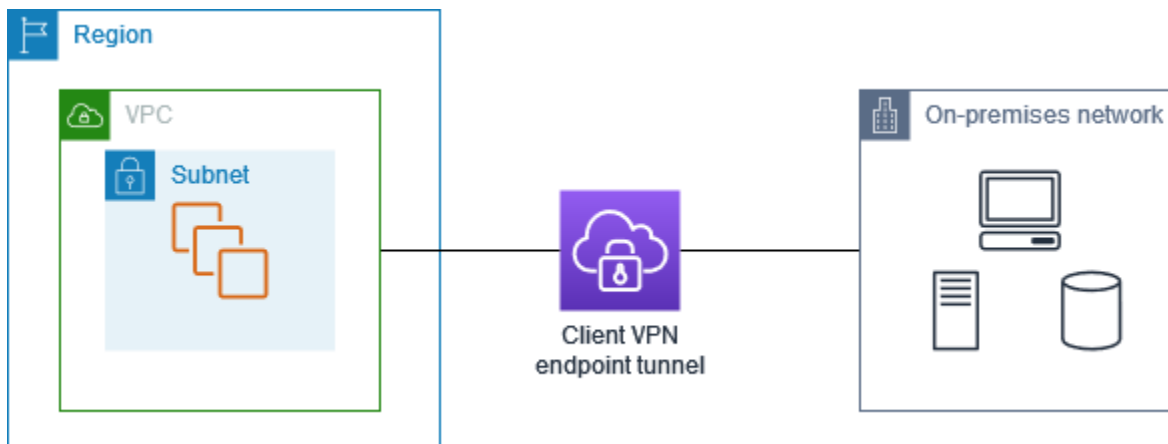
- `client-connect-failed`: la funzione Lambda ha impedito di stabilire la connessione.
- `client-connect-handler-timed-out`: si è verificato il timeout della funzione Lambda.
- `client-connect-handler-other-execution-error`: la funzione Lambda ha riscontrato un errore imprevisto.
- `client-connect-handler-throttled`: la funzione Lambda è stata limitata.
- `client-connect-handler-invalid-response`: la funzione Lambda ha restituito una risposta non valida.
- `client-connect-handler-service-error`: si è verificato un errore sul lato servizio durante il tentativo di connessione.

Split-tunnel sugli endpoint AWS Client VPN

Per impostazione predefinita, quando hai un endpoint Client VPN, tutto il traffico proveniente dai client viene instradato attraverso il tunnel Client VPN. Quando abiliti lo split-tunnel sull'endpoint Client VPN, verrà eseguito il push delle route sulla [tabella di routing dell'endpoint Client VPN](#) al dispositivo collegato all'endpoint Client VPN. Ciò garantisce che solo il traffico con una destinazione alla rete corrispondente a una route della tabella di routing dell'endpoint Client VPN viene instradato tramite il tunnel Client VPN.

Puoi utilizzare lo split-tunnel di un endpoint Client VPN quando non desideri che tutto il traffico utente venga instradato attraverso l'endpoint Client VPN.

Nell'esempio seguente, lo split-tunnel è attivato sull'endpoint Client VPN. Solo il traffico destinato al VPC ($172.31.0.0/16$) viene instradato attraverso il tunnel Client VPN. Il traffico destinato alle risorse locali non viene instradato tramite il tunnel Client VPN.



Vantaggi dello split-tunnel

Lo split-tunnel su endpoint Client VPN offre i seguenti vantaggi:

- È possibile ottimizzare il routing del traffico dai client facendo in modo che solo il traffico destinato ad AWS attraversi il tunnel VPN.
- È possibile ridurre il volume del traffico in uscita da AWS, riducendo quindi i costi di trasferimento dei dati.

Considerazioni sul routing

- Quando abiliti lo split-tunnel, tutte le route presenti nella tabella di instradamento dell'endpoint Client VPN vengono aggiunte alla tabella di instradamento del client quando viene stabilita la connessione VPN. Questa operazione è diversa dall'operazione predefinita, che sovrascrive la tabella di instradamento del client con la voce `0.0.0.0/0` per instradare tutto il traffico sulla VPN.

Note

Non è consigliabile aggiungere una route `0.0.0.0/0` alla tabella di instradamento dell'endpoint Client VPN quando si utilizza la modalità split-tunnel.

- Quando è abilitata la modalità split-tunnel, qualsiasi modifica alla tabella di routing degli endpoint Client VPN comporterà la reimpostazione di tutte le connessioni client.

Enabling-split-tunnel

Puoi abilitare lo split-tunnel su un endpoint Client VPN nuovo o esistente. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Creare un endpoint Client VPN](#)
- [Modifica un endpoint Client VPN.](#)

Registrazione delle connessioni

La registrazione delle connessioni è una funzionalità di AWS Client VPN che consente di acquisire log di connessione per l'endpoint Client VPN.

Un log delle connessioni contiene le voci di log del registro delle connessioni. Ogni voce di log del registro delle connessioni contiene informazioni su un evento di connessione, ovvero quando un client (utente finale) si connette, tenta di connettersi o si disconnette dall'endpoint Client VPN. Puoi utilizzare queste informazioni per eseguire analisi forensi, analizzare come l'endpoint Client VPN viene utilizzato o eseguire il debug dei problemi di connessione.

La registrazione delle connessioni è disponibile in tutte le regioni in cui è disponibile AWS Client VPN. I log delle connessioni vengono pubblicati in un gruppo di log CloudWatch Logs nel tuo account.

Note

I tentativi di autenticazione reciproca falliti non vengono registrati.

Voci di log del registro di connessione

Una voce di log del registro delle connessioni è un BLOB formattato JSON di coppie chiave-valore. Di seguito è riportato un esempio di voce di log del registro delle connessioni.

```
{
  "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"
}
```

Una voce di log del registro connessioni contiene le seguenti chiavi:

- `connection-log-type`: il tipo di voce di log delle connessioni (`connection-attempt` o `connection-reset`).
- `connection-attempt-status`: lo stato della richiesta di connessione (`successful`, `failed`, `waiting-for-assertion` o `NA`).
- `connection-reset-status`: lo stato di un evento di reimpostazione della connessione (`NA` o `assertion-received`).
- `connection-attempt-failure-reason`: il motivo dell'errore di connessione, se applicabile.
- `connection-id`: l'ID della connessione.
- `client-vpn-endpoint-id`: l'ID dell'endpoint Client VPN a cui è stata effettuata la connessione.
- `transport-protocol`: il protocollo di trasporto utilizzato per la connessione.
- `connection-start-time`: l'ora di inizio della connessione.
- `connection-last-update-time`: l'ora dell'ultimo aggiornamento della connessione. Questo valore viene periodicamente aggiornato nei registri.
- `client-ip`: l'indirizzo IP del client, allocato dall'intervallo CIDR IPv4 del client per l'endpoint Client VPN.
- `common-name`: il nome comune del certificato utilizzato per l'autenticazione basata su certificati.
- `device-type`: il tipo di dispositivo utilizzato per la connessione dall'utente finale.
- `device-ip`: l'indirizzo IP pubblico del dispositivo.
- `port`: il numero di porta per la connessione.
- `ingress-bytes`: il numero di byte in ingresso (in ingresso) per la connessione. Questo valore viene periodicamente aggiornato nei registri.
- `egress-bytes`: il numero di byte in uscita (in uscita) per la connessione. Questo valore viene periodicamente aggiornato nei registri.
- `ingress-packets`: il numero di pacchetti in ingresso (inbound) per la connessione. Questo valore viene periodicamente aggiornato nei registri.
- `egress-packets`: il numero di pacchetti in uscita (outbound) per la connessione. Questo valore viene periodicamente aggiornato nei registri.
- `connection-end-time`: l'ora di fine della connessione. Il valore è `NA` se la connessione è ancora in corso o se il tentativo di connessione non è riuscito.
- `posture-compliance-statuses`: gli stati di conformità dell'assetto restituiti dall'[handler di connessioni client](#), se applicabili.

- `username` - Il nome utente viene registrato quando viene utilizzata l'autenticazione basata sull'utente (AD o SAML) per l'endpoint.
- `connection-duration-seconds` - La durata in secondi di una connessione. Uguale alla differenza tra “ora di avvio della connessione” e “ora di fine della connessione”.

Per ulteriori informazioni sull'abilitazione della registrazione delle connessioni, consulta [Operazioni con i log delle connessioni](#).

Considerazioni sul dimensionamento delle VPN client

Quando si crea un endpoint VPN client, considerare il numero massimo di connessioni VPN simultanee che si prevede di supportare. È necessario tenere conto del numero di clienti attualmente supportati e se l'endpoint VPN client può soddisfare una domanda aggiuntiva, se necessario.

I seguenti fattori influiscono sul numero massimo di connessioni VPN simultanee che possono essere supportate in un endpoint VPN client.

Intervallo dimensioni CIDR cliente

Quando si [crea un endpoint VPN client](#), è necessario specificare un intervallo CIDR cliente, ovvero un block CIDR IPv4 compreso tra una maschera di rete /12 e /22. Ad ogni connessione all'endpoint Client VPN viene assegnato un indirizzo IP univoco dall'intervallo CIDR del client. Una parte degli indirizzi nell'intervallo CIDR del client viene utilizzata per supportare il modello di disponibilità dell'endpoint Client VPN e non può essere assegnata ai client. Non è possibile modificare il client CIDR dopo aver creato l'endpoint Client VPN.

In generale, si consiglia di specificare un intervallo CIDR client che contiene il doppio del numero di indirizzi IP (e quindi connessioni simultanee) che si prevede di supportare nell'endpoint VPN client.

Numero di subnet associate

Quando si [associa una subnet](#) ad un endpoint VPN client, è possibile consentire agli utenti di stabilire sessioni VPN all'endpoint VPN client. È possibile associare più subnet a un endpoint VPN client per un'elevata disponibilità e per abilitare capacità di connessione aggiuntiva.

Di seguito è riportato il numero di connessioni VPN simultanee supportate in base al numero di associazioni di subnet per l'endpoint VPN client.

Associazioni di sottorete	Numero di connessioni supportate
1	7.000
2	36.500
3	66.500
4	96.500
5	126.000

Non è possibile associare più sottoreti dalla stessa zona di disponibilità a un endpoint Client VPN. Pertanto, il numero di associazioni della sottorete dipende anche dal numero di zone di disponibilità presenti in una regione AWS.

Ad esempio, se si prevede di supportare 8.000 connessioni VPN all'endpoint VPN client, specificare una dimensione minima dell'intervallo CIDR client /18 (16.384 indirizzi IP) e associare almeno 2 subnet all'endpoint VPN client.

Se non si è certi del numero di connessioni VPN previste per l'endpoint VPN client, si consiglia di specificare una dimensione /16 CIDR block o larger.

Per ulteriori informazioni sulle regole e sulle limitazioni per l'utilizzo con gli intervalli CIDR client e le reti di destinazione, vedi [Regole e best practice di AWS Client VPN](#).

Per ulteriori informazioni sulle quote per l'endpoint VPN client, vedi [Quote AWS Client VPN](#).

Scenari ed esempi per AWS Client VPN

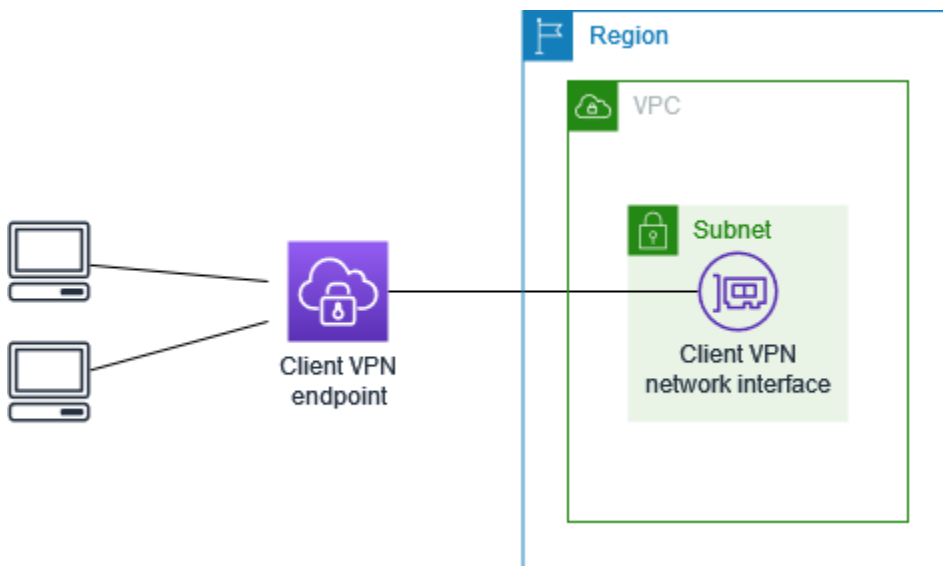
In questa sezione vengono forniti gli esempi per la creazione e la configurazione dell'accesso Client VPN per i client.

Indice

- [Accesso a un VPC utilizzando AWS Client VPN](#)
- [Accesso a un VPC con peering utilizzando AWS Client VPN](#)
- [Accesso a una rete on-premise utilizzando AWS Client VPN](#)
- [Accesso a Internet utilizzando AWS Client VPN](#)
- [Client-to-client Accesso C tramite AWS Client VPN](#)
- [Limitazione dell'accesso alla propria rete utilizzando AWS Client VPN](#)

Accesso a un VPC utilizzando AWS Client VPN

La configurazione per questo scenario include un singolo VPC target. Consigliamo questa configurazione se devi fornire ai client l'accesso alle risorse di un singolo VPC.



Prima di iniziare, esegui queste attività:

- Creare o identificare un VPC con almeno una sottorete. Identifica la sottorete nel VPC che vuoi associare all'endpoint Client VPN e annota gli intervalli CIDR IPv4.

- Identificare un intervallo CIDR adatto per gli indirizzi IP client che non si sovrappongono al CIDR VPC.
- Esamina le regole e le limitazioni per gli endpoint Client VPN in [Regole e best practice di AWS Client VPN](#).

Per implementare questa configurazione

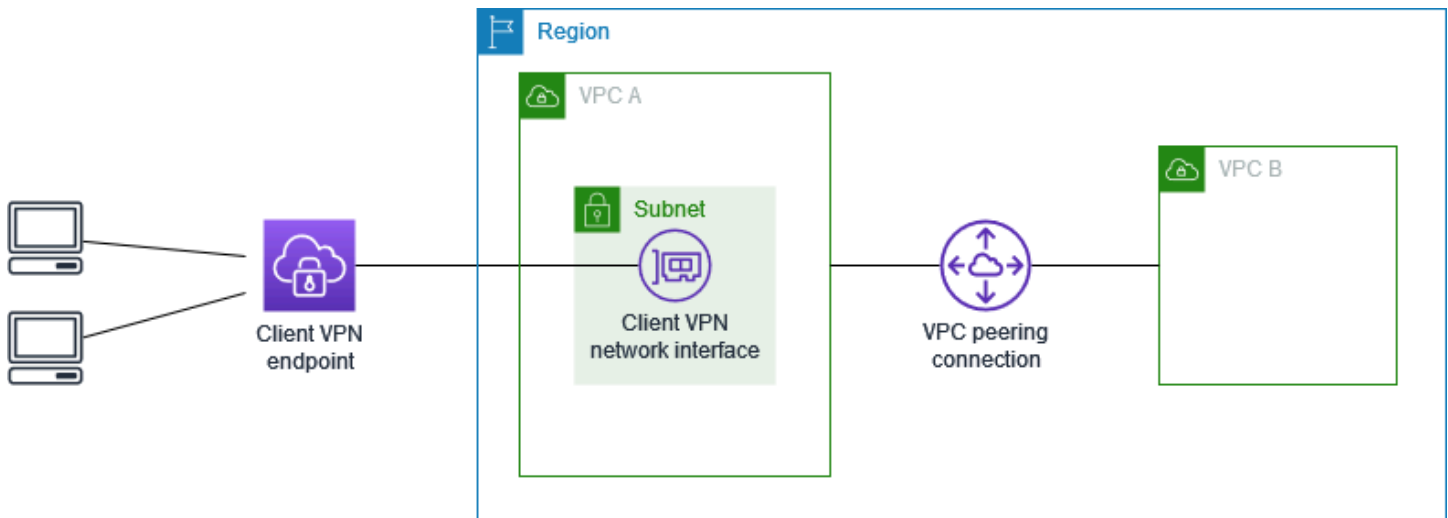
1. Crea un endpoint Client VPN nella stessa regione del VPC. Per eseguire questa operazione, attieniti alla procedura descritta in [Creare un endpoint Client VPN](#).
2. Associa la sottorete all'endpoint Client VPN. Per eseguire questa operazione, attieniti alla procedura descritta in [Associare una rete di destinazione a un endpoint Client VPN](#) e seleziona la sottorete e il VPC identificati in precedenza.
3. Aggiungere una regola di autorizzazione per concedere ai client l'accesso al VPC. Per eseguire questa operazione, attieniti alla procedura descritta in [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#) e per Destination network (Rete di destinazione) immetti l'intervallo CIDR IPv4 del VPC.
4. Aggiungere una regola ai gruppi di sicurezza delle risorse per consentire il traffico dal gruppo di sicurezza applicato all'associazione di sottorete nella fase 2. Per ulteriori informazioni, consulta [Gruppi di sicurezza](#).

Accesso a un VPC con peering utilizzando AWS Client VPN

La configurazione per questo scenario include un VPC di destinazione (VPC A) connesso in peering con un VPC (VPC B) aggiuntivo. Consigliamo questa configurazione se devi fornire ai client l'accesso alle risorse all'interno di un VPC di destinazione e di altri VPC connessi in peering (ad esempio VPC B).

Note

La procedura per consentire l'accesso a un VPC con peering descritto di seguito, è necessaria solo se l'endpoint Client VPN è stato configurato per la modalità split-tunnel. In modalità full-tunnel, l'accesso al VPC con peering sarebbe consentito per impostazione predefinita.



Prima di iniziare, esegui queste attività:

- Creare o identificare un VPC con almeno una sottorete. Identifica la sottorete nel VPC che vuoi associare all'endpoint Client VPN e annota gli intervalli CIDR IPv4.
- Identificare un intervallo CIDR adatto per gli indirizzi IP client che non si sovrappongono al CIDR VPC.
- Esamina le regole e le limitazioni per gli endpoint Client VPN in [Regole e best practice di AWS Client VPN](#).

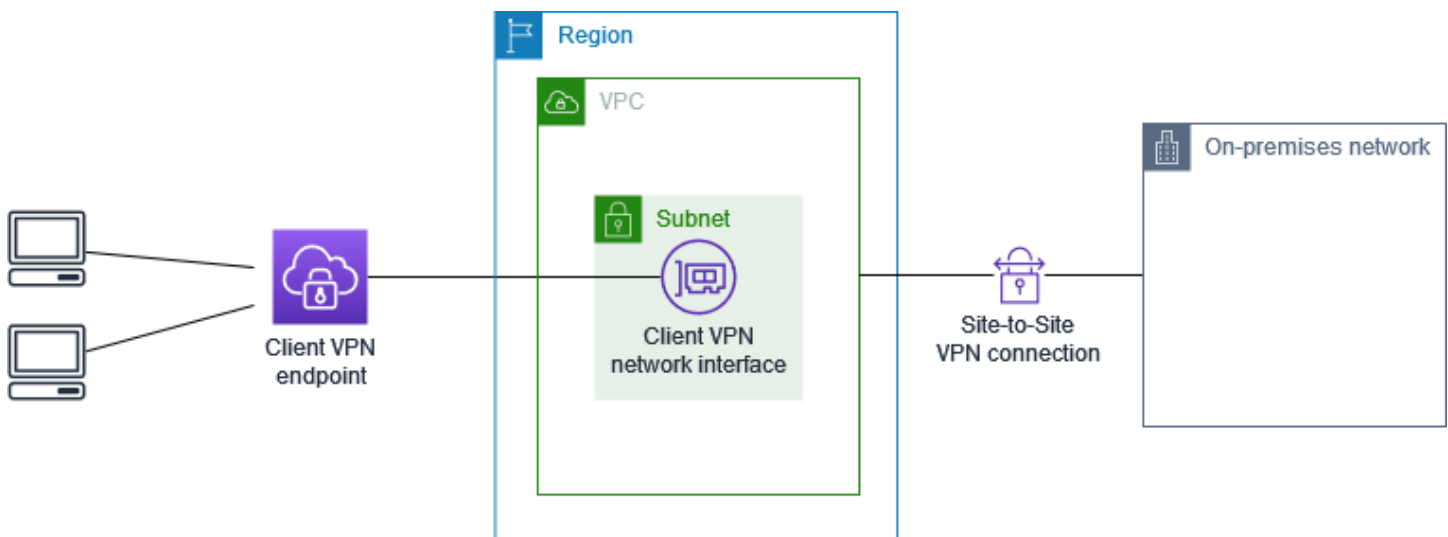
Per implementare questa configurazione

1. Stabilire la connessione peering tra i VPC. Segui i passaggi indicati in [Creazione e accettazione di una connessione peering VPC](#) nella Guida al peering di Amazon VPC. Verifica che le istanze in VPC A possano comunicare con le istanze in VPC B utilizzando la connessione di peering.
2. Crea un endpoint Client VPN nella stessa regione del VPC di destinazione. Nell'esempio precedente è il VPC A. Esegui le fasi descritte in [Creare un endpoint Client VPN](#).
3. Associa la sottorete identificata in precedenza all'endpoint Client VPN creato. Per eseguire questa operazione, attieniti alla procedura descritta in [Associare una rete di destinazione a un endpoint Client VPN](#) e seleziona il VPC e la sottorete. Per impostazione predefinita, associamo il gruppo di sicurezza predefinito del VPC all'endpoint client VPN. È possibile associare un gruppo di sicurezza diverso utilizzando i passaggi descritti in [the section called "Applicazione di un gruppo di sicurezza a una rete target"](#).
4. Aggiungere una regola di autorizzazione per concedere ai client l'accesso al VPC di destinazione. Per eseguire questa operazione, attieniti alla procedura descritta in [Aggiunta di](#)

- [una regola di autorizzazione a un endpoint Client VPN](#). Per abilitare la rete di destinazione , immettere l'intervallo CIDR IPv4 del VPC.
5. Aggiungere una route per indirizzare il traffico al VPC in peering. Nel diagramma, questo è VPC B. Per eseguire questa operazione, attieniti alla procedura descritta in [Creazione di una route dell'endpoint](#). Per Rinstradamento, immettere l'intervallo CIDR IPv4 del VPC in peering. Per ID sottorete del VPC di destinazione seleziona la sottorete associata all'endpoint Client VPN.
 6. Aggiungere una regola di autorizzazione per concedere ai client l'accesso al VPC in peering. Per eseguire questa operazione, attieniti alla procedura descritta in [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#). Per rete di destinazione , immettere l'intervallo CIDR IPv4 del VPC.
 7. Aggiungere una regola ai gruppi di sicurezza per le istanze nel VPC A e nel VPC B per consentire il traffico dal gruppo di sicurezza applicato all'ndpoint del lient VPN nella fase 3. Per ulteriori informazioni, consulta [Gruppi di sicurezza](#).

Accesso a una rete on-premise utilizzando AWS Client VPN

La configurazione per questo scenario include l'accesso a una rete locale. Consigliamo questa configurazione se devi fornire ai client l'accesso alle risorse all'interno di una rete locale.




Prima di iniziare, esegui queste attività:

- Creare o identificare un VPC con almeno una sottorete. Identifica la sottorete nel VPC che vuoi associare all'endpoint Client VPN e annota gli intervalli CIDR IPv4.
- Identificare un intervallo CIDR adatto per gli indirizzi IP client che non si sovrappongono al CIDR VPC.

- Esamina le regole e le limitazioni per gli endpoint Client VPN in [Regole e best practice di AWS Client VPN](#).

Per implementare questa configurazione

1. Abilita la comunicazione tra il VPC e la rete locale tramite una connessione AWS Site-to-Site VPN. Per eseguire questa operazione, attieniti alla procedura descritta in [Nozioni di base](#) nella Guida per l'utente di AWS Site-to-Site VPN.

 Note

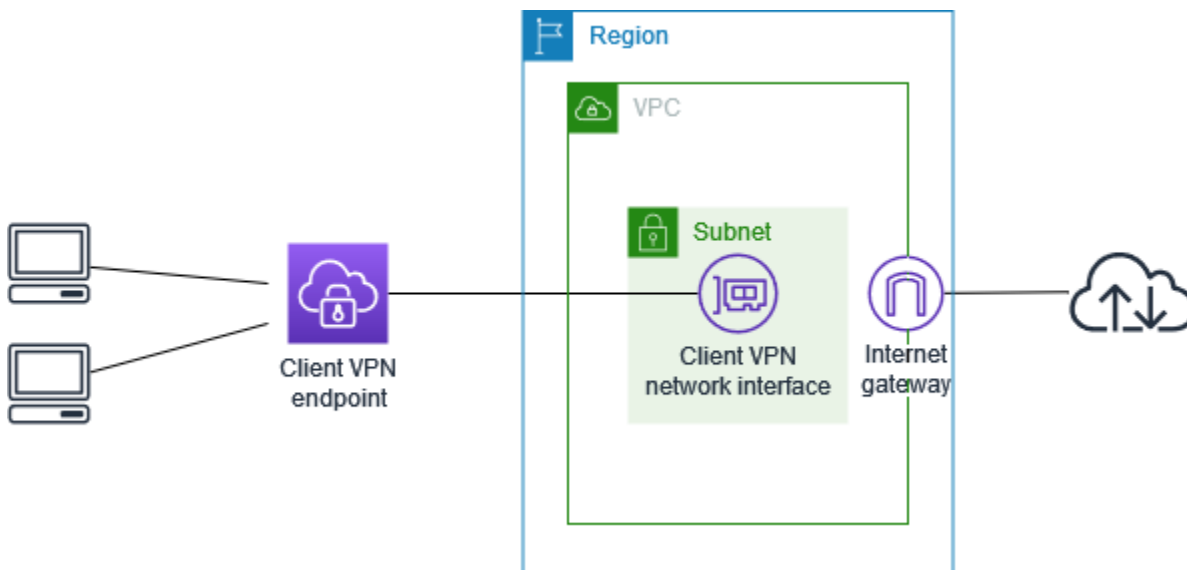
In alternativa, è possibile implementare questo scenario utilizzando una connessione AWS Direct Connect tra il VPC e la rete locale. Per ulteriori informazioni, consulta la [Guida per l'utente AWS Direct Connect](#).

2. Verifica la connessione AWS Site-to-Site VPN creata nella fase precedente. Per eseguire questa operazione, attieniti alla procedura descritta in [Test della connessione Site-to-Site VPN](#) nella Guida per l'utente di AWS Site-to-Site VPN. Se la connessione VPN funziona come previsto, continuare con la fase successive.
3. Crea un endpoint Client VPN nella stessa regione del VPC. Per eseguire questa operazione, attieniti alla procedura descritta in [Creare un endpoint Client VPN](#).
4. Associa la sottorete identificata in precedenza all'endpoint Client VPN. Per eseguire questa operazione, attieniti alla procedura descritta in [Associare una rete di destinazione a un endpoint Client VPN](#) e seleziona il VPC e la sottorete.
5. Aggiungi una route che consente l'accesso alla connessione AWS Site-to-Site VPN. Per eseguire questa operazione, attieniti alla procedura descritta in [Creazione di una route dell'endpoint](#); per Route destination (Destinazione route), immetti l'intervallo CIDR IPv4 della connessione AWS Site-to-Site VPN e per Target VPC Subnet ID (ID sottorete VPC target), seleziona la sottorete associata all'endpoint Client VPN.
6. Aggiungi una regola di autorizzazione per consentire ai client di accedere alla connessione AWS Site-to-Site VPN. Per eseguire questa operazione, attieniti alla procedura descritta in [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#); per Destination network (Rete di destinazione), immetti l'intervallo CIDR IPv4 della connessione AWS Site-to-Site VPN.

Accesso a Internet utilizzando AWS Client VPN

La configurazione per questo scenario include un singolo VPC target e l'accesso a Internet. Consigliamo questa configurazione se devi concedere ai client l'accesso alle risorse all'interno di un singolo VPC target e consentire l'accesso a Internet.

Se hai completato il tutorial [Nozioni di base su AWS Client VPN](#) hai già implementato questo scenario.



Prima di iniziare, esegui queste attività:

- Creare o identificare un VPC con almeno una sottorete. Identifica la sottorete nel VPC che vuoi associare all'endpoint Client VPN e annota gli intervalli CIDR IPv4.
- Identificare un intervallo CIDR adatto per gli indirizzi IP client che non si sovrappongono al CIDR VPC.
- Esamina le regole e le limitazioni per gli endpoint Client VPN in [Regole e best practice di AWS Client VPN](#).

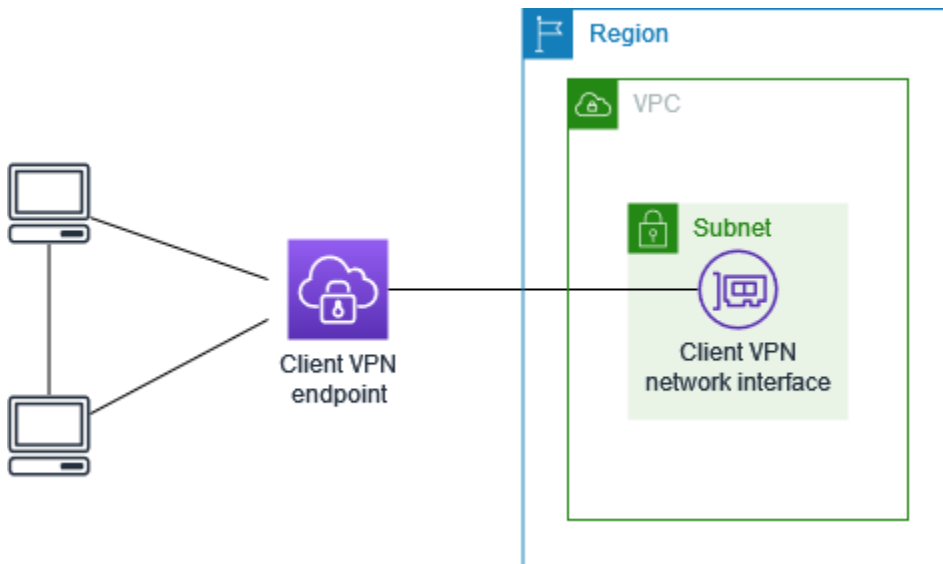
Per implementare questa configurazione

1. Verifica che il gruppo di sicurezza che verrà utilizzato per l'endpoint Client VPN consenta il traffico in uscita verso Internet. Per eseguire questa operazione, aggiungere le regole in uscita che consentono il traffico HTTP e HTTPS verso 0.0.0.0/0.
2. Creare un gateway Internet e collegarlo al VPC. Per ulteriori informazioni, consulta [Creazione e collegamento di un Internet Gateway](#) nella Guida per l'utente di Amazon VPC.

3. Rendere pubblica la sottorete aggiungendo una route al gateway Internet per instradare la tabella di routing. Nella console del VPC scegli Subnets (Sottoreti), seleziona la sottorete da associare all'endpoint Client VPN, scegli Route Table (Tabella di routing) e quindi scegli l'ID della tabella di routing. Scegliere Operazioni, Modifica route e Aggiungi route. Per Destinazione immettere $0.0.0.0/0$ e per Target scegliere il gateway Internet del passaggio precedente.
4. Crea un endpoint Client VPN nella stessa regione del VPC. Per eseguire questa operazione, attieniti alla procedura descritta in [Creare un endpoint Client VPN](#).
5. Associa la sottorete identificata in precedenza all'endpoint Client VPN. Per eseguire questa operazione, attieniti alla procedura descritta in [Associare una rete di destinazione a un endpoint Client VPN](#) e seleziona il VPC e la sottorete.
6. Aggiungere una regola di autorizzazione per concedere ai client l'accesso al VPC. Per eseguire questa operazione attieniti alla procedura descritta in [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#) e per Destination network to enable (Rete di destinazione da abilitare) immetti l'intervallo CIDR IPv4 del VPC.
7. Aggiungere una route che consenta il traffico verso Internet. Per eseguire questa operazione attieniti alla procedura descritta in [Creazione di una route dell'endpoint](#). Per Route destination (Destinazione ruote) immetti $0.0.0.0/0$ e per Target VPC Subnet ID (ID sottorete VPC target) seleziona la sottorete associata all'endpoint Client VPN.
8. Aggiungere una regola di autorizzazione per concedere ai client l'accesso a Internet. Per eseguire questa operazione attieniti alla procedura descritta in [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#). Per Destination network (Rete di destinazione) immetti $0.0.0.0/0$.
9. Assicurarsi che i gruppi di sicurezza per le risorse nel VPC dispongano di una regola che consenta l'accesso dal gruppo di sicurezza associato con l'endpoint del client VPN. Ciò consente ai client di accedere alle risorse nel VPC.

lient-to-client Accesso C tramite AWS Client VPN

La configurazione di questo scenario consente ai client di accedere a un singolo VPC e consente ai client di instradare il traffico tra loro. È consigliabile questa configurazione se anche i client che si connettono allo stesso endpoint Client VPN devono comunicare tra loro. I client possono comunicare tra loro utilizzando l'indirizzo IP univoco assegnato loro dall'intervallo CIDR client quando si connettono all'endpoint Client VPN.



Prima di iniziare, esegui queste attività:

- Creare o identificare un VPC con almeno una sottorete. Identifica la sottorete nel VPC che vuoi associare all'endpoint Client VPN e annota gli intervalli CIDR IPv4.
- Identificare un intervallo CIDR adatto per gli indirizzi IP client che non si sovrappongono al CIDR VPC.
- Esamina le regole e le limitazioni per gli endpoint Client VPN in [Regole e best practice di AWS Client VPN](#).

Note

Regole di autorizzazione basate sulla rete che utilizzano gruppi Active Directory o gruppi IdP basati su SAML non sono supportate in questo scenario.

Per implementare questa configurazione

1. Crea un endpoint Client VPN nella stessa regione del VPC. Per eseguire questa operazione, attieniti alla procedura descritta in [Creare un endpoint Client VPN](#).
2. Associa la sottorete identificata in precedenza all'endpoint Client VPN. Per eseguire questa operazione, attieniti alla procedura descritta in [Associare una rete di destinazione a un endpoint Client VPN](#) e seleziona il VPC e la sottorete.

3. Aggiungere un instradamento alla rete locale nella tabella di routing. Per eseguire questa operazione, attieniti alla procedura descritta in [Creazione di una route dell'endpoint](#). Per Destinazione routing, immettere l'intervallo CIDR del client e per ID sottorete VPC di destinazione, specificare `local`.
4. Aggiungere una regola di autorizzazione per concedere ai client l'accesso al VPC. Per eseguire questa operazione, attieniti alla procedura descritta in [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#). Per abilitare la rete di destinazione, immettere l'intervallo CIDR IPv4 del VPC.
5. Aggiungere una regola di autorizzazione per concedere ai client l'accesso all'intervallo CIDR. Per eseguire questa operazione, attieniti alla procedura descritta in [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#). Per abilitare la rete di destinazione, immettere l'intervallo CIDR del client.

Limitazione dell'accesso alla propria rete utilizzando AWS Client VPN

Puoi configurare l'endpoint Client VPN in modo da limitare l'accesso a risorse specifiche nel VPC. Per l'autenticazione basata sull'utente puoi anche limitare l'accesso a parti della rete, in base al gruppo di utenti che accede all'endpoint Client VPN.

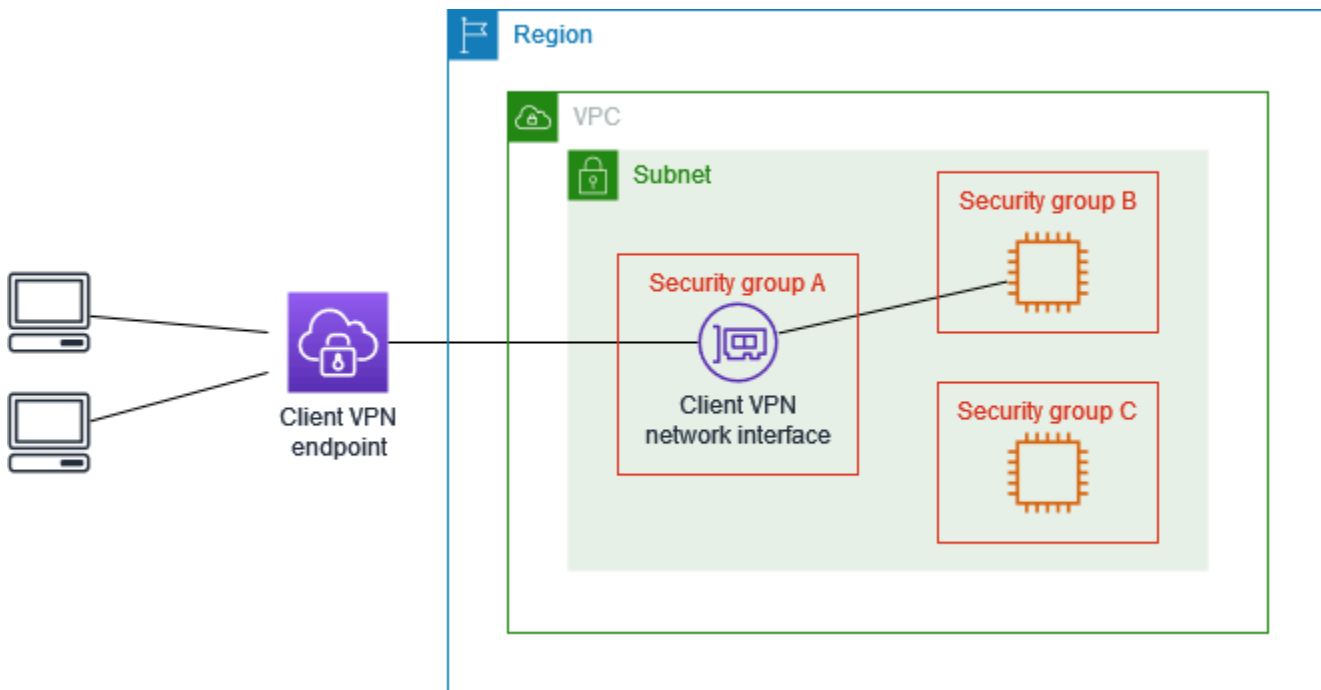
Limitare l'accesso utilizzando i gruppi di sicurezza

Puoi concedere o rifiutare l'accesso a risorse specifiche nel VPC aggiungendo o rimuovendo regole del gruppo di sicurezza che fanno riferimento al gruppo di sicurezza applicato all'associazione di rete di destinazione (il gruppo di sicurezza Client VPN). Questa configurazione espande lo scenario illustrato in [Accesso a un VPC utilizzando AWS Client VPN](#), e viene applicata in aggiunta alla regola di autorizzazione configurata in tale scenario.

Per concedere l'accesso a una risorsa specifica, identificare il gruppo di sicurezza associato all'istanza in cui è in esecuzione la risorsa. Quindi, crea una regola che abiliti il traffico dal gruppo di sicurezza Client VPN.

Nel diagramma seguente, il gruppo di sicurezza A è il gruppo di sicurezza del Client VPN, il gruppo di sicurezza B è associato a un'istanza EC2 e il gruppo di sicurezza C è associato a un'istanza EC2. Se aggiungi una regola al gruppo di sicurezza B che consente l'accesso dal gruppo di sicurezza A, i client possono accedere all'istanza associata al gruppo di sicurezza B. Se il gruppo di sicurezza C

non dispone di una regola che consenta l'accesso dal gruppo di sicurezza A, i client non possono accedere all'istanza associata al gruppo di sicurezza C.



Prima di iniziare, controlla se il gruppo di sicurezza Client VPN è associato ad altre risorse nel VPC. Se aggiungi o rimuovi regole che fanno riferimento al gruppo di sicurezza Client VPN, puoi consentire o rifiutare l'accesso anche per altre risorse associate. Per evitare ciò, utilizza un gruppo di sicurezza creato appositamente per l'utilizzo con l'endpoint Client VPN.

Per creare una regola per il gruppo di sicurezza

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Scegliere il gruppo di sicurezza associato all'istanza in cui la risorsa è in esecuzione.
4. Scegliere Actions (Operazioni), Edit inbound rules (Modifica regole in entrata).
5. Scegliere Add rule (Aggiungi regola), quindi effettuare le seguenti operazioni:
 - In Type (Tipo), scegliere All traffic (Tutto il traffico) o un tipo di traffico specifico che si desidera consentire.
 - In Source (Origine), scegli Custom (Personalizzato), quindi immetti o scegli l'ID del gruppo di sicurezza Client VPN.
6. Scegliere Save rules (Salva regole).

Per rimuovere l'accesso a una risorsa specifica, controllare il gruppo di sicurezza associato all'istanza in cui è in esecuzione la risorsa. Se esiste una regola che consente il traffico dal gruppo di sicurezza Client VPN, eliminala.

Per verificare le regole del gruppo di sicurezza

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Scegliere Inbound Rules (Regole in entrata).
4. Rivedere l'elenco delle regole. Se esiste una regola in cui Source (Origine) è il gruppo di sicurezza Client VPN, scegli Edit Rules (Modifica regole) e seleziona Delete (Elimina) (icona x) per la regola. Scegliere Salva regole.

Limitare l'accesso in base ai gruppi di utenti

Se l'endpoint Client VPN è configurato per l'autenticazione basata sull'utente, puoi concedere a gruppi specifici di utenti l'accesso a parti specifiche della rete. Per farlo, completa le seguenti fasi.

1. Configurare utenti e gruppi in AWS Directory Service o nel proprio IdP. Per ulteriori informazioni, consultare i seguenti argomenti:
 - [Autenticazione Active Directory](#)
 - [Requisiti e considerazioni per l'autenticazione federata basata su SAML](#)
2. Crea una regola di autorizzazione per l'endpoint Client VPN che consenta a un gruppo specificato di accedere a tutta la rete o a parte di essa. Per ulteriori informazioni, consulta [Regole di autorizzazione](#).

Se l'endpoint Client VPN è configurato per l'autenticazione reciproca, non è possibile configurare i gruppi di utenti. Quando si crea una regola di autorizzazione, è necessario concedere l'accesso a tutti gli utenti. Per consentire a gruppi specifici di utenti di accedere a parti specifiche della rete, puoi creare più endpoint Client VPN. Ad esempio, per ogni gruppo di utenti che accede alla rete, effettuare le seguenti operazioni:

1. Creare un set di certificati e chiavi server e client per quel gruppo di utenti. Per ulteriori informazioni, consulta [Autenticazione reciproca](#).
2. Crea un endpoint Client VPN. Per ulteriori informazioni, consulta [Creare un endpoint Client VPN](#).

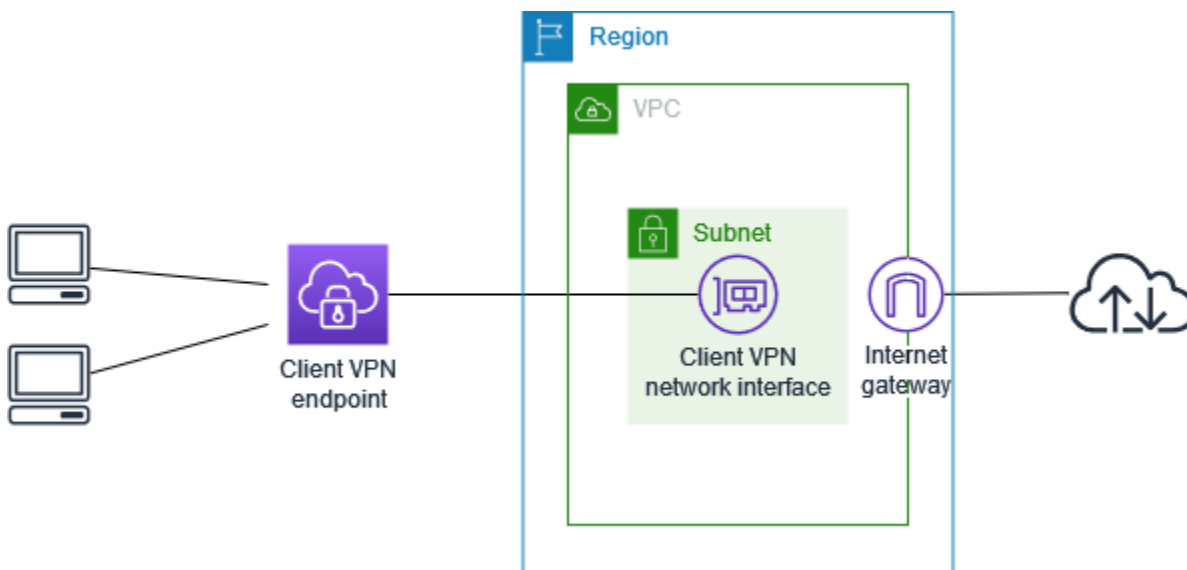
3. Creare una regola di autorizzazione che conceda l'accesso a tutta la rete o a parte di essa. Ad esempio, per un endpoint Client VPN utilizzato dagli amministratori, puoi creare una regola di autorizzazione che conceda l'accesso all'intera rete. Per ulteriori informazioni, consulta [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#).

Nozioni di base su AWS Client VPN

In questo tutorial crei un endpoint Client VPN che ha le seguenti caratteristiche:

- Fornisce a tutti i client l'accesso a un singolo VPC.
- Fornisce a tutti i clienti l'accesso a Internet.
- Utilizza l'[autenticazione reciproca](#).

Il diagramma seguente rappresenta la configurazione del VPC e dell'endpoint Client VPN dopo aver completato questo tutorial.



Fasi

- [Prerequisiti](#)
- [Fase 1: Generare i certificati e le chiavi server e client](#)
- [Fase 2: Creare un endpoint Client VPN](#)
- [Fase 3: Associazione di una rete target](#)
- [Fase 4: Aggiungere una regola di autorizzazione per il VPC](#)
- [Fase 5: Fornire l'accesso a Internet.](#)
- [Fase 6: Verificare i requisiti del gruppo di sicurezza](#)
- [Fase 7: Scaricare il file di configurazione dell'endpoint Client VPN](#)
- [Fase 8: Connettersi all'endpoint Client VPN](#)

Prerequisiti

Prima di iniziare questo tutorial introduttivo, assicurati di disporre di quanto segue:

- Le autorizzazioni necessarie per l'utilizzo degli endpoint Client VPN.
- Le autorizzazioni necessarie per importare i certificati in AWS Certificate Manager.
- VPC con almeno una subnet e un gateway Internet. La tabella di routing associata alla sottorete deve disporre di una route per il gateway Internet.

Fase 1: Generare i certificati e le chiavi server e client

Questo tutorial utilizza l'autenticazione reciproca. Con l'autenticazione reciproca, il Client VPN utilizza i certificati per eseguire l'autenticazione tra client ed endpoint Client VPN. È necessario creare un certificato server e una chiave e almeno un certificato client e una chiave. Come minimo, il certificato del server dovrà essere importato in AWS Certificate Manager (ACM) e specificato quando crei l'endpoint Client VPN. L'importazione del certificato client in ACM è facoltativa.

Se non si dispone già di certificati da utilizzare per questo scopo, possono essere creati utilizzando la utility OpenVPN easy-rsa. Per le fasi dettagliate per generare i certificati e le chiavi server e client utilizzando la [Utility OpenVPN easy-rsa](#) e importarli in ACM vedi [Autenticazione reciproca](#).

Note

Il certificato del server deve essere fornito con o importato in AWS Certificate Manager (ACM) nella stessa regione AWS in cui verrà creato l'endpoint Client VPN.

Fase 2: Creare un endpoint Client VPN

L'endpoint Client VPN è la risorsa che crei e configuri per abilitare e gestire le sessioni Client VPN. È il punto di cessazione di tutte le sessioni VPN client.

Per creare un endpoint Client VPN

1. Apri alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Endpoint del client VPN e quindi scegli Create Client VPN Endpoint (Crea un endpoint del client VPN).

3. (Facoltativo) Fornisci un nome tag e una descrizione per l'endpoint Client VPN.
4. Per Client IPv4 CIDR (CIDR IPv4 client), specificare un intervallo di indirizzi IP in notazione CIDR entro cui assegnare gli indirizzi IP del client.

Note

L'intervallo di indirizzi non può sovrapporsi all'intervallo di indirizzi della rete di destinazione, all'intervallo di indirizzi VPC, né ad alcun routing che verrà associato all'endpoint Client VPN. L'intervallo di indirizzi client deve essere al minimo /22 e non superiore a /12 delle dimensioni del blocco CIDR. Non è possibile modificare l'intervallo di indirizzi del client dopo aver creato l'endpoint Client VPN.

5. Per Certificato server ARN, seleziona l'ARN del certificato server generato in [Fase 1](#).
6. In Opzioni autenticazione, selezionare Use mutual authentication (Utilizza autenticazione reciproca) e per Client certificate ARN (ARN del certificato client), selezionare l'ARN del certificato che desideri utilizzare come certificato del client.

Se i certificati server e client sono stati rilasciati dalla stessa autorità di certificazione (CA), è possibile specificare l'ARN del certificato server sia per il server che per il client. In questo scenario, qualsiasi certificato client corrispondente al certificato del server può essere utilizzato per l'autenticazione.

7. Mantenere le restanti impostazioni predefinite e selezionare Create Client VPN Endpoint (Crea un endpoint del client VPN).

Una volta creato, lo stato dell'endpoint Client VPN è `pending-associate`. I client possono stabilire una connessione VPN solo dopo aver associato almeno una rete target.

Per ulteriori informazioni sulle opzioni che puoi specificare per un endpoint Client VPN, consulta [Creare un endpoint Client VPN](#).

Fase 3: Associazione di una rete target

Per consentire ai client di stabilire una sessione VPN, è necessario associare una rete target all'endpoint Client VPN. Una rete target è una sottorete in un VPC.

Per associare una rete di destinazione a un endpoint Client VPN

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.

2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN creato nella procedura precedente, quindi scegli Associazioni di rete di destinazione, Associate target network (Associa la rete di destinazione).
4. Per VPC, scegliere il VPC in cui si trova la sottorete.
5. Per Sottorete da associare scegli la sottorete da associare all'endpoint Client VPN.
6. Scegli Associate target network (Associa rete di destinazione).
7. Se consentito dalle regole di autorizzazione, un'associazione sottorete è sufficiente per permettere ai client di accedere all'intera rete di un VPC. Puoi associare sottoreti aggiuntive per fornire un'elevata disponibilità nel caso in cui una delle zone di disponibilità sia danneggiata.

Quando associ la prima sottorete all'endpoint Client VPN si verificano i seguenti eventi:

- Lo stato dell'endpoint Client VPN diventa `available`. I client possono ora stabilire una connessione VPN, ma non possono accedere alle risorse nel VPC finché non vengono aggiunte le regole di autorizzazione.
- La route locale del VPC viene aggiunta automaticamente alla tabella di routing dell'endpoint Client VPN.
- Il gruppo di sicurezza predefinito del VPC viene automaticamente applicato all'endpoint del Client VPN.

Fase 4: Aggiungere una regola di autorizzazione per il VPC

Affinché i client possano accedere al VPC, è necessario che vi sia un routing verso il VPC nella tabella di routing dell'endpoint Client VPN e una regola di autorizzazione. Il percorso è già stato aggiunto automaticamente nella fase precedente. In questo tutorial, concediamo l'accesso al VPC a tutti gli utenti.

Per aggiungere una regola di autorizzazione per il VPC

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui è stata aggiunta la regola di autorizzazione. Scegli Regole di autorizzazione, quindi scegli Add authorization rule (Aggiungi regola di autorizzazione).

4. Per Rete di destinazione da abilitare, immettere il CIDR della rete per la quale si desidera consentire l'accesso. Ad esempio, per consentire l'accesso all'intero VPC, specificare il blocco CIDR IPv4 del VPC.
5. In Grant access to (Consenti accesso a), scegliere Allow access to all users (Consenti accesso a tutti gli utenti).
6. (Opzionale) In Descrizione immettere una breve descrizione della regola di autorizzazione.
7. Scegliere Add authorization rule (Aggiungi regola di autorizzazione).

Fase 5: Fornire l'accesso a Internet.

È possibile fornire l'accesso alle reti aggiuntive connesse al VPC, ad esempio i servizi AWS, i VPC in peering, le reti on-premise e Internet. Per ogni rete aggiuntiva, devi aggiungere un routing alla rete e nella tabella di routing dell'endpoint del Client VPN e configurare una regola di autorizzazione per concedere l'accesso ai client.

Per questo tutorial, vogliamo concedere a tutti gli utenti l'accesso a Internet e anche al VPC. Hai già configurato l'accesso al VPC, quindi questo passaggio riguarda l'accesso a Internet.

Fornire l'accesso a Internet

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN creato per questo tutorial. Scegli Tabella di routing, quindi scegli Create Route (Crea routing).
4. Per Route destination (Destinazione route), immettere `0.0.0.0/0`. Per ID sottorete per associazione rete di destinazione, specifica l'ID della sottorete in cui instradare il traffico.
5. Selezionare Create Route (Crea route).
6. Scegli Regole di autorizzazione, quindi scegli Add authorization rule (Aggiungi regola di autorizzazione).
7. Per Destination network to enable access (Rete di destinazione per abilitare l'accesso), immettere `0.0.0.0/0` e scegliere Allow access to all users (Consenti accesso a tutti gli utenti).
8. Scegliere Add authorization rule (Aggiungi regola di autorizzazione).

Fase 6: Verificare i requisiti del gruppo di sicurezza

In questo tutorial, non sono stati specificati gruppi di sicurezza durante la creazione dell'endpoint Client VPN nel passaggio 2. Ciò significa che il gruppo di sicurezza predefinito per il VPC viene applicato automaticamente all'endpoint Client VPN quando viene associata una rete di destinazione. Di conseguenza, il gruppo di sicurezza predefinito per il VPC dovrebbe ora essere associato all'endpoint Client VPN.

Verifica i seguenti requisiti del gruppo di sicurezza

- Il gruppo di sicurezza associato alla sottorete in cui si sta instradando il traffico (in questo caso il gruppo di sicurezza VPC predefinito) consente il traffico in uscita verso Internet. Per fare ciò, aggiungi una regola in uscita che consenta tutto il traffico verso la destinazione `0.0.0.0/0`.
- I gruppi di sicurezza per le risorse nel VPC devono disporre di una regola che consenta l'accesso dal gruppo di sicurezza applicato all'endpoint Client VPN (in questo caso il gruppo di sicurezza VPC predefinito). Ciò consente ai client di accedere alle risorse nel VPC.

Per ulteriori informazioni, consulta [Gruppi di sicurezza](#).

Fase 7: Scaricare il file di configurazione dell'endpoint Client VPN

Il passaggio seguente consiste nello scaricare e preparare il file di configurazione dell'endpoint Client VPN. Il file di configurazione include le informazioni sul certificato e sull'endpoint Client VPN necessarie per stabilire una connessione VPN. Puoi fornire questo file agli utenti finali che devono connettersi all'endpoint del Client VPN. L'utente finale utilizza il file per configurare l'applicazione client VPN.

Per scaricare e preparare il file di configurazione dell'endpoint Client VPN

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN creato per questo tutorial e quindi scegli Download della configurazione del client.
4. Individuare il certificato client e la chiave che sono stati generati nel [passaggio 1](#). Il certificato e la chiave client sono disponibili nelle seguenti posizioni del repository OpenVPN easy-rsa clonato:
 - Certificato clien — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`

- Chiave clien — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Apri il file di configurazione dell'endpoint Client VPN utilizzando l'editor di testo preferito. Aggiungi i tag `<cert></cert>` e `<key></key>` al file. Inserire il contenuto del certificato del client e il contenuto della chiave privata tra i tag corrispondenti, come segue:

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

6. Salva e chiudi il file di configurazione dell'endpoint Client VPN.
7. Distribuisci il file di configurazione dell'endpoint Client VPN agli utenti finali.

Per ulteriori informazioni sul file di configurazione dell'endpoint Client VPN, consulta [Esportazione e configurazione del file di configurazione del client](#).

Fase 8: Connettersi all'endpoint Client VPN

Puoi connetterti all'endpoint Client VPN utilizzando il client fornito da AWS o un'altra applicazione client basata su OpenVPN e il file di configurazione appena creato. Per ulteriori informazioni, consulta la [Guida per l'utente AWS Client VPN](#).

Utilizzo di AWS Client VPN

I seguenti argomenti spiegano come utilizzare Client VPN.

Indice

- [Accedere al portale self-service](#)
- [Regole di autorizzazione](#)
- [Elenchi di revoche di certificati client](#)
- [Connessioni client](#)
- [Banner di accesso del client](#)
- [Endpoint Client VPN](#)
- [Operazioni con i log delle connessioni](#)
- [Esportazione e configurazione del file di configurazione del client](#)
- [Route](#)
- [Reti target](#)
- [Durata massima della sessione VPN](#)

Accedere al portale self-service

Se hai abilitato il portale self-service per l'endpoint Client VPN puoi fornire ai client l'URL del portale self-service. I client possono accedere al portale in un browser Web e utilizzare le proprie credenziali basate sull'utente per accedere. Nel portale, i client possono scaricare il file di configurazione dell'endpoint Client VPN e scaricare la versione più recente del client fornito da AWS.

Si applicano le regole seguenti:

- Il portale self-service non è disponibile per i client che eseguono l'autenticazione reciproca.
- Il file di configurazione disponibile nel portale self-service è lo stesso file di configurazione esportato utilizzando la console Amazon VPC o AWS CLI. Se è necessario personalizzare il file di configurazione prima di distribuirlo ai client, devi distribuire il file personalizzato ai client manualmente.
- È necessario abilitare l'opzione del portale self-service per l'endpoint Client VPN perché in caso contrario i client non possono accedere al portale. Se questa opzione non è abilitata, è possibile modificare l'endpoint Client VPN per abilitarla.

Dopo aver abilitato l'opzione del portale self-service, fornisci ai client uno dei seguenti URL:

- <https://self-service.clientvpn.amazonaws.com/>

Se i client accedono al portale utilizzando questo URL, devono immettere l'ID dell'endpoint Client VPN prima di accedere.

- <https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>>

Sostituisci *<endpoint-id>* nell'URL precedente con l'ID dell'endpoint Client VPN, ad esempio `cvpn-endpoint-0123456abcd123456`.

Puoi inoltre visualizzare l'URL del portale self-service nell'output del comando [describe-client-vpn-endpoints](#) della AWS CLI. In alternativa, l'URL è disponibile nella scheda Dettagli della pagina Endpoint del client VPN nella console Amazon VPC.

Per ulteriori informazioni sulla configurazione del portale self-service per l'utilizzo con l'autenticazione federata, consulta [Supporto per il portale self-service](#).

Regole di autorizzazione

Le regole di autorizzazione fungono da regole di firewall che concedono l'accesso alle reti. Aggiungendo le regole di autorizzazione, viene concesso l'accesso alla rete specificata a client specifici. Per ciascuna rete per cui vuoi concedere l'accesso, è necessario disporre di una regola di autorizzazione. Puoi aggiungere regole di autorizzazione a un endpoint Client VPN utilizzando la console e la AWS CLI.

Note

Durante la valutazione delle regole di autorizzazione, la VPN client utilizza la corrispondenza prefisso più lunga. Per maggiori dettagli, consulta l'argomento per la risoluzione dei problemi [Regole di autorizzazione per i gruppi di Active Directory non funzionano come previsto](#) e [Priorità della route](#) nella Guida per l'utente di Amazon VPC.

Indice

- [Aggiunta di una regola di autorizzazione a un endpoint Client VPN](#)
- [Rimozione di una regola di autorizzazione da un endpoint Client VPN](#)

- [Visualizzazione delle regole di autorizzazione](#)
- [Scenari di esempio per le regole di autorizzazione](#)

Aggiunta di una regola di autorizzazione a un endpoint Client VPN

Come aggiungere una regola di autorizzazione a un endpoint VPN client tramite AWS Management Console

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui aggiungere la regola di autorizzazione, scegli Authorization rules (Regole autorizzazione), quindi Authorize authorization rule (Aggiungi regola autorizzazione).
4. Per Rete di destinazione, immettere l'indirizzo IP, in notazione CIDR, della rete a cui gli utenti devono accedere (ad esempio, il blocco CIDR del VPC).
5. Specificare i client che possono accedere alla rete specificata. Per Grant access to (Concedi l'accesso a), procedere in uno dei seguenti modi:
 - Per concedere l'accesso a tutti i clienti, scegliere Allow access to all users (Consenti l'accesso a tutti gli utenti).
 - Per limitare l'accesso a client specifici, scegliere Consenti l'accesso agli utenti in un gruppo di accesso specifico, quindi per ID gruppo di accesso, immettere l'ID per il gruppo cui concedere l'accesso. Ad esempio, l'identificatore di sicurezza (SID) di un gruppo di Active Directory o l'ID/ nome di un gruppo definito in un provider di identità basato su SAML.
 - (Active Directory) Per ottenere il SID è possibile utilizzare il cmdlet [Get-ADGroup](#) di Microsoft Powershell, ad esempio:

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

In alternativa, aprire lo strumento Utenti e computer di Active Directory, visualizzare le proprietà del gruppo, passare alla scheda Editor attributi e ottenere il valore per objectSID. Se necessario, selezionare prima View (Visualizza), Advanced Features (Funzioni avanzate) per abilitare la scheda Editor attributi.

- (Autenticazione federata basata su SAML) L'ID/nome del gruppo deve corrispondere alle informazioni sugli attributi del gruppo restituite nell'asserzione SAML.

6. In Descrizione immettere una breve descrizione della regola di autorizzazione.
7. Scegliere Add authorization rule (Aggiungi regola di autorizzazione).

Per aggiungere una regola di autorizzazione a un endpoint VPN client (AWS CLI)

Utilizza il comando [authorize-client-vpn-ingress](#).

Rimozione di una regola di autorizzazione da un endpoint Client VPN

Per eliminare una regola di autorizzazione, rimuovi l'accesso alla rete specificata.

Puoi rimuovere le regole di autorizzazione da un endpoint Client VPN utilizzando la console e la AWS CLI.

Per rimuovere una regola di autorizzazione da un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui è stata aggiunta la regola di autorizzazione e scegli Regole autorizzazione.
4. Selezionare la regola di autorizzazione da eliminare, scegliere Remove authorization rule (Elimina la regola di autorizzazione) e scegli Remove authorization rule (Elimina la regola di autorizzazione).

Per rimuovere una regola di autorizzazione da un endpoint Client VPN (AWS CLI)

Utilizza il comando [revoke-client-vpn-ingress](#).

Visualizzazione delle regole di autorizzazione

Puoi visualizzare le regole di autorizzazione per un determinato endpoint Client VPN utilizzando la console e la AWS CLI.

Per visualizzare le regole di autorizzazione (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN per cui visualizzare le regole di autorizzazione e scegli Autorizzazione.

Per visualizzare le regole di autorizzazione (AWS CLI)

Utilizza il comando [describe-client-vpn-authorization-rules](#).

Scenari di esempio per le regole di autorizzazione

In questa sezione viene descritto come funzionano le regole di autorizzazione per AWS Client VPN. Include punti chiave per comprendere le regole di autorizzazione, un'architettura di esempio e l'illustrazione di scenari di esempio corrispondenti all'architettura di esempio.

Indice

- [Punti chiave per comprendere le regole di autorizzazione](#)
- [Architettura di esempio per scenari di regole di autorizzazione](#)
- [Scenario 1: accesso a una destinazione singola](#)
- [Scenario 2: utilizzo di qualsiasi CIDR di destinazione \(0.0.0.0/0\)](#)
- [Scenario 3: corrispondenza del prefisso IP più lungo](#)
- [Scenario 4: CIDR sovrapposto \(stesso gruppo\)](#)
- [Scenario 5: regola 0.0.0.0/0 aggiuntiva](#)
- [Scenario 6: aggiunta della regola per 192.168.0.0/24](#)
- [Scenario 7: accesso per tutti i gruppi di utenti](#)

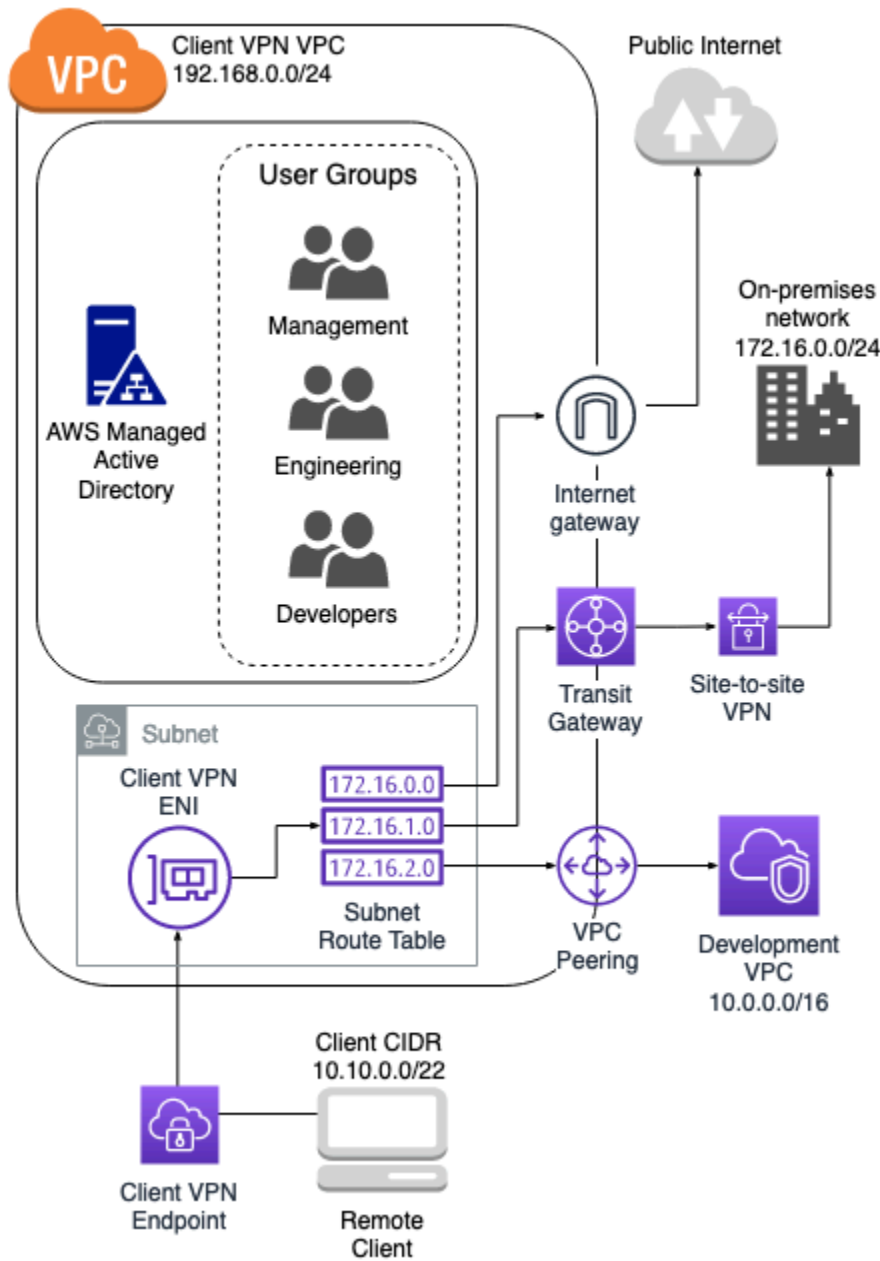
Punti chiave per comprendere le regole di autorizzazione

I seguenti punti illustrano alcuni dei comportamenti delle regole di autorizzazione:

- Per consentire l'accesso a una rete di destinazione, è necessario aggiungere esplicitamente una regola di autorizzazione. Il comportamento predefinito prevede la negazione dell'accesso.
- Non è possibile aggiungere una regola di autorizzazione per limitare l'accesso a una rete di destinazione.
- Il CIDR `0.0.0.0/0` viene trattato come un caso speciale. Viene elaborato per ultimo, a prescindere dall'ordine di creazione delle regole di autorizzazione.
- Il CIDR `0.0.0.0/0` può essere considerato come "qualsiasi destinazione" o "qualsiasi destinazione non definita da altre regole di autorizzazione".
- La corrispondenza del prefisso più lungo è la regola che ha la precedenza.

Architettura di esempio per scenari di regole di autorizzazione

Il diagramma seguente mostra l'architettura di esempio utilizzata per gli scenari di esempio riportati in questa sezione.



Scenario 1: accesso a una destinazione singola

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo	S-xxxxx15	False	10.0.0.0/16
Fornisce al gruppo di manager l'accesso al VPC del client VPN	S-xxxxx16	False	192.168.0.0/24

Comportamento risultante

- Il gruppo di progettazione può accedere solo a 172.16.0.0/24.
- Il gruppo di sviluppo può accedere solo a 10.0.0.0/16.
- Il gruppo di manager può accedere solo a 192.168.0.0/24.
- Tutto l'altro traffico viene eliminato dall'endpoint del Client VPN.

Note

In questo scenario, nessun gruppo di utenti ha accesso alla rete Internet pubblica.

Scenario 2: utilizzo di qualsiasi CIDR di destinazione (0.0.0.0/0)

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
	S-xxxxx14	False	172.16.0.0/24

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di progettazione l'accesso alla rete on-premise			
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo	S-xxxxx15	False	10.0.0.0/16
Fornisce al gruppo di manager l'accesso a qualsiasi destinazione	S-xxxxx16	False	0.0.0.0/0

Comportamento risultante

- Il gruppo di progettazione può accedere solo a 172.16.0.0/24.
- Il gruppo di sviluppo può accedere solo a 10.0.0.0/16.
- Il gruppo di manager può accedere alla rete Internet pubblica e a 192.168.0.0/24, ma non può accedere a 172.16.0.0/24 o 10.0.0.0/16.

Note

In questo scenario, poiché nessuna regola fa riferimento a 192.168.0.0/24, l'accesso a tale rete è fornito anche dalla regola 0.0.0.0/0.

Una regola contenente 0.0.0.0/0 viene sempre valutata per ultima indipendentemente dall'ordine in cui sono state create le regole. Per questo motivo, tenere presente che le regole valutate prima di 0.0.0.0/0 svolgono un ruolo nel determinare a quali reti 0.0.0.0/0 concede l'accesso.

Scenario 3: corrispondenza del prefisso IP più lungo

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo	S-xxxxx15	False	10.0.0.0/16
Fornisce al gruppo di manager l'accesso a qualsiasi destinazione	S-xxxxx16	False	0.0.0.0/0
Fornisce l'accesso al gruppo di manager a un singolo host in un VPC di sviluppo	S-xxxxx16	False	10.0.1.66/32

Comportamento risultante

- Il gruppo di progettazione può accedere solo a 172.16.0.0/24.
- Il gruppo di sviluppo può accedere a 10.0.0.0/16, eccetto per l'host singolo 10.0.2.119/32.
- Il gruppo di manager può accedere alla rete Internet pubblica, 192.168.0.0/24, e a un singolo host (10.0.2.119/32) all'interno del VPC di sviluppo, ma non ha accesso a 172.16.0.0/24 o a uno qualsiasi degli host rimanenti nel VPC di sviluppo.

Note

Qui è possibile vedere come una regola con un prefisso IP più lungo ha la precedenza su una regola con un prefisso IP più breve. Se si desidera che il gruppo di sviluppo abbia accesso a 10.0.2.119/32, è necessario aggiungere una regola aggiuntiva che consenta al team di sviluppo di accedere a 10.0.2.119/32.

Scenario 4: CIDR sovrapposto (stesso gruppo)

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo	S-xxxxx15	False	10.0.0.0/16
Fornisce al gruppo di manager l'accesso a qualsiasi destinazione	S-xxxxx16	False	0.0.0.0/0
Fornisce al gruppo di manager l'accesso a un singolo host nel VPC di sviluppo	S-xxxxx16	False	10.0.1.66/32
Fornisce al gruppo di progettazione l'accesso a una	S-xxxxx14	False	172,16,0,128/25

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
sottorete più piccola all'interno della rete on-premise.			

Comportamento risultante

- Il gruppo di sviluppo può accedere a 10.0.0.0/16, eccetto per l'host singolo 10.0.2.119/32.
- Il gruppo di manager può accedere alla rete Internet pubblica, 192.168.0.0/24, e a un singolo host (10.0.2.119/32) all'interno della rete 10.0.0.0/16, ma non ha accesso a 172.16.0.0/24 o a uno qualsiasi degli host rimanenti nella rete 10.0.0.0/16.
- Il gruppo di progettazione ha accesso a 172.16.0.0/24, inclusa la sottorete più specifica 172.16.0.128/25.

Scenario 5: regola 0.0.0.0/0 aggiuntiva

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo	S-xxxxx15	False	10.0.0.0/16
Fornisce al gruppo di manager l'accesso a qualsiasi destinazione	S-xxxxx16	False	0.0.0.0/0

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di manager l'accesso a un singolo host nel VPC di sviluppo	S-xxxxx16	False	10.0.1.66/32
Fornisce al gruppo di progettazione l'accesso a una sottorete più piccola all'interno della rete on-premise.	S-xxxxx14	False	172.16.0.128/25
Fornisce al gruppo di progettazione l'accesso a qualsiasi destinazione	S-xxxxx14	False	0.0.0.0/0

Comportamento risultante

- Il gruppo di sviluppo può accedere a 10.0.0.0/16, eccetto per l'host singolo 10.0.2.119/32.
- Il gruppo di manager può accedere alla rete Internet pubblica, 192.168.0.0/24, e a un singolo host (10.0.2.119/32) all'interno della rete 10.0.0.0/16, ma non ha accesso a 172.16.0.0/24 o a uno qualsiasi degli host rimanenti nella rete 10.0.0.0/16.
- Il gruppo di progettazione può accedere alla rete Internet pubblica, 192.168.0.0/24, e a 172.16.0.0/24, inclusa la sottorete più specifica 172.16.0.128/25.

Note

Si noti che sia il gruppo di progettazione che quello di manager possono ora accedere a 192.168.0.0/24. Questo perché entrambi i gruppi hanno accesso a 0.0.0.0/0 (qualsiasi destinazione) e nessun'altra regola fa riferimento a 192.168.0.0/24.

Scenario 6: aggiunta della regola per 192.168.0.0/24

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo	S-xxxxx15	False	10.0.0.0/16
Fornisce al gruppo di manager l'accesso a qualsiasi destinazione	S-xxxxx16	False	0.0.0.0/0
Fornisce al gruppo di manager l'accesso a un singolo host nel VPC di sviluppo	S-xxxxx16	False	10.0.1.66/32
Fornisce al gruppo di progettazione l'accesso a una sottorete nella rete on-premise	S-xxxxx14	False	172,16,0,128/25
Fornisce al gruppo di progettazione l'accesso a qualsiasi destinazione	S-xxxxx14	False	0.0.0.0/0

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di manager l'accesso al VPC del client VPN	S-xxxxx16	False	192.168.0.0/24

Comportamento risultante

- Il gruppo di sviluppo può accedere a 10.0.0.0/16, eccetto per l'host singolo 10.0.2.119/32.
- Il gruppo di manager può accedere alla rete Internet pubblica, 192.168.0.0/24, e a un singolo host (10.0.2.119/32) all'interno della rete 10.0.0.0/16, ma non ha accesso a 172.16.0.0/24 o a uno qualsiasi degli host rimanenti nella rete 10.0.0.0/16.
- Il gruppo di progettazione può accedere alla rete Internet pubblica, 172.16.0.0/24 e a 172.16.0.128/25.

Note

Si noti come l'aggiunta della regola per l'accesso del gruppo di manager a 192.168.0.0/24 fa sì che il gruppo di sviluppo non abbia più accesso a quella rete di destinazione.

Scenario 7: accesso per tutti i gruppi di utenti

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
	S-xxxxx15	False	10.0.0.0/16

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo			
Fornisce al gruppo di manager l'accesso a qualsiasi destinazione	S-xxxxx16	False	0.0.0.0/0
Fornisce al gruppo di manager l'accesso a un singolo host nel VPC di sviluppo	S-xxxxx16	False	10.0.1.66/32
Fornisce al gruppo di progettazione l'accesso a una sottorete nella rete on-premise	S-xxxxx14	False	172,16,0,128/25
Fornisce al gruppo di progettazione l'accesso a tutte le reti	S-xxxxx14	False	0.0.0.0/0
Fornisce al gruppo di manager l'accesso al VPC del client VPN	S-xxxxx16	False	192.168.0.0/24
Fornisce l'accesso a tutti i gruppi	N/D	True	0.0.0.0/0

Comportamento risultante

- Il gruppo di sviluppo può accedere a `10.0.0.0/16`, eccetto per l'host singolo `10.0.2.119/32`.
- Il gruppo di manager può accedere alla rete Internet pubblica, `192.168.0.0/24`, e a un singolo host (`10.0.2.119/32`) all'interno della rete `10.0.0.0/16`, ma non ha accesso a `172.16.0.0/24` o a uno qualsiasi degli host rimanenti nella rete `10.0.0.0/16`.
- Il gruppo di progettazione può accedere alla rete Internet pubblica, `172.16.0.0/24` e a `172.16.0.128/25`.
- Qualsiasi altro gruppo di utenti, ad esempio "gruppo di amministratori", può accedere alla rete Internet pubblica, ma non a qualsiasi altra rete di destinazione definita nelle altre regole.

Elenchi di revoche di certificati client

Puoi utilizzare gli elenchi di revoche di certificati client per revocare l'accesso a un endpoint Client VPN per certificati client specifici.

Note

Per ulteriori informazioni sulla creazione di certificati e chiavi server e client, consulta [Autenticazione reciproca](#)

Per ulteriori informazioni sul numero di voci che è possibile aggiungere a un elenco di revoche di certificati client, consulta [Quote Client VPN](#).

Indice

- [Generazione di un elenco di revoche di certificati client](#)
- [Importazione di un elenco di revoche di certificati client](#)
- [Esportazione di un elenco di revoche di certificati client](#)

Generazione di un elenco di revoche di certificati client

Linux/macOS

Nella seguente procedura, viene generato un elenco di revoche di certificati client utilizzando la utility a riga di comando OpenVPN `easy-rsa`.

Per generare un elenco di revoche di certificati client utilizzando OpenVPN easy-rsa

1. Accedi al server che ospita l'installazione di easyrsa utilizzata per generare il certificato.
2. Passare alla cartella `easy-rsa/easyrsa3` nel repository locale.

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

3. Revocare il certificato client e generare l'elenco di revoche client.

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

Digitare `yes` quando richiesto.

Windows

La procedura seguente utilizza il software OpenVPN per generare un elenco di revoche client. Si presuppone che sia stata eseguita la [procedura per l'utilizzo del software OpenVPN](#) per generare i certificati e le chiavi client e server.

Per generare un elenco di revoche di certificati client utilizzando EasyRSA versione 3.x.x

1. Aprire un prompt dei comandi e accedere alla directory `EasyRSA-3.x.x`, che dipenderà da dove la directory è installata sul sistema.

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

2. Eseguire il file "EasyRSA-Start.bat" per avviare la shell EasyRSA.

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

3. Nella shell EasyRSA, revocare il certificato client.

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

4. Digitare "yes" quando richiesto.
5. Generare l'elenco di revoche client.

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

6. L'elenco di revocche client verrà creato nella seguente posizione:

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

Per generare un elenco di revocche di certificati client utilizzando le versioni precedenti di EasyRSA

1. Aprire un prompt dei comandi e passare alla directory di OpenVPN.

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

2. Esegui il file vars.bat.

```
C:\> vars
```

3. Revocare il certificato client e generare l'elenco di revocche client.

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

Importazione di un elenco di revocche di certificati client

È necessario avere un file con l'elenco di revocche di certificati client da importare. Per ulteriori informazioni sulla creazione di un elenco di revocche di certificati client, consulta [Generazione di un elenco di revocche di certificati client](#).

Puoi importare un elenco di revocche di certificati client utilizzando la console e la AWS CLI.

Per importare un elenco di revocche di certificati client (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN per cui importare l'elenco di revocche di certificati client.
4. Scegliere Operazioni, quindi Import Client Certificate CRL (Importa elenco di revocche di certificati client).
5. Per Elenco di revocche di certificati, immettere il contenuto del file con l'elenco di revocche di certificati client e scegliere Import CRL (Importa elenco di revocche di certificati).

Per importare un elenco di revoche di certificati client (AWS CLI)

Utilizza il comando [import-client-vpn-client-certificate-revocation-list](#).

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

Esportazione di un elenco di revoche di certificati client

Puoi esportare gli elenchi di revoche di certificati client utilizzando la console e la AWS CLI.

Per esportare un elenco di revoche di certificati client (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN per cui esportare l'elenco di revoche di certificati client.
4. Scegliere Operazioni, selezionare Export Client Certificate CRL (Esporta elenco di revoche di certificati clienti), quindi scegliere Export Client Certificate CRL (Esporta elenco di revoche di certificati clienti).

Per esportare una revoca di certificato client (AWS CLI)

Utilizza il comando [export-client-vpn-client-certificate-revocation-list](#).

Connessioni client

Le connessioni sono sessioni VPN stabilite dai client. Viene stabilita una connessione quando un client si connette a un endpoint Client VPN.

Indice

- [Visualizzazione delle connessioni client](#)
- [Terminazione di una connessione client](#)

Visualizzazione delle connessioni client

Puoi visualizzare le connessioni client utilizzando la console e la AWS CLI. Le informazioni di connessione includono l'indirizzo IP assegnato dall'intervallo CIDR del client.

Per visualizzare le connessioni client (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN per cui visualizzare le connessioni client.
4. Scegliere la scheda Connessioni. Nella scheda Connessioni sono elencate tutte le connessioni client attive e terminate.

Per visualizzare le connessioni client (AWS CLI)

Utilizza il comando [describe-client-vpn-connections](#).

Terminazione di una connessione client

Quando una connessione client viene terminata, la sessione VPN viene chiusa.

Puoi terminare le connessioni client utilizzando la console e la AWS CLI.

Per terminare una connessione client (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui è connesso il client e scegli Connections (Connessioni).
4. Selezionare la connessione da terminare, scegliere Terminate Connection (Termina connessione) e quindi Terminate Connection (Termina connessione).

Per terminare una connessione client (AWS CLI)

Utilizza il comando [terminate-client-vpn-connections](#).

Banner di accesso del client

AWS Client VPN fornisce la possibilità di visualizzare un banner di testo su applicazioni desktop Client VPN fornite da AWS quando viene stabilita una sessione VPN. Puoi definire il contenuto del banner di testo per soddisfare le tue esigenze normative e di conformità. È possibile utilizzare un massimo di 1400 caratteri codificati UTF-8.

Note

Quando un banner di accesso client è abilitato, viene visualizzato solo nelle sessioni VPN appena create. Le sessioni VPN esistenti non vengono interrotte, anche se il banner viene visualizzato quando viene ristabilita una sessione esistente.

Consulta [Note di rilascio per il client fornito da AWS](#) nella Guida per l'utente di AWS Client VPN per informazioni dettagliate sulle applicazioni desktop client.

Indice

- [Configurare un banner di accesso client durante la creazione di un endpoint Client VPN](#)
- [Configurare un banner di accesso client per un endpoint Client VPN esistente](#)
- [Disabilitare un banner di accesso client per un endpoint Client VPN esistente](#)
- [Modificare il testo del banner esistente su un endpoint Client VPN](#)
- [Visualizzare il banner di accesso attualmente configurato](#)

Configurare un banner di accesso client durante la creazione di un endpoint Client VPN

Per la procedura dettagliata per abilitare un banner di accesso client durante la creazione di un endpoint Client VPN, consulta [Creare un endpoint Client VPN](#).

Configurare un banner di accesso client per un endpoint Client VPN esistente

Attieniti alla seguente procedura per configurare un banner di accesso client per un endpoint Client VPN esistente.

Abilitare il banner di accesso client su un endpoint Client VPN (console)

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da modificare, scegli Actions (Operazioni), quindi Modify Client VPN Endpoint (Modifica l'endpoint Client VPN).
4. Scorri verso il basso la pagina fino alla sezione Other parameters (Altri parametri).

5. Attiva Enable client login banner (Abilita il banner di accesso client).
6. In Client Login Banner Text (Testo banner di accesso client), inserisci il testo che verrà visualizzato in un banner sui client forniti da AWS quando viene stabilita una sessione VPN. Utilizza solo caratteri codificati UTF-8, con un massimo di 1400 caratteri consentiti.
7. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Abilitare un banner di accesso client su un endpoint Client VPN (AWS CLI)

Utilizza il comando [modify-client-vpn-endpoint](#).

Disabilitare un banner di accesso client per un endpoint Client VPN esistente

Attieniti alla seguente procedura per disabilitare un banner di accesso client per un endpoint Client VPN esistente.

Disabilitare il banner di accesso client su un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da modificare, scegli Operazioni, quindi Modify Client VPN Endpoint (Modifica l'endpoint Client VPN).
4. Scorri verso il basso la pagina fino alla sezione Altri parametri (Altri parametri).
5. Disattiva Enable client login banner? (Abilitare il banner di accesso client?).
6. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Disattiva un banner di accesso client su un endpoint Client VPN (AWS CLI)

Utilizza il comando [modify-client-vpn-endpoint](#).

Modificare il testo del banner esistente su un endpoint Client VPN

Attieniti alla seguente procedura per modificare il testo esistente su un banner di accesso client.

Modificare il testo del banner esistente su un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.

2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da modificare, scegli Operazioni, quindi Modify Client VPN Endpoint (Modifica l'endpoint Client VPN).
4. Per Enable client login banner? (Abilita il banner di accesso client?), verifica che sia attivo.
5. In Testo banner di accesso client, sostituisci il testo esistente con il nuovo testo che verrà visualizzato in un banner sui client forniti da AWS quando viene stabilita una sessione VPN. Utilizza solo caratteri codificati UTF-8, con un massimo di 1400 caratteri.
6. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Modificare il banner di accesso client su un endpoint Client VPN (AWS CLI)

Utilizza il comando [modify-client-vpn-endpoint](#).

Visualizzare il banner di accesso attualmente configurato

Per visualizzare un banner di accesso attualmente configurato, utilizza la procedura riportata di seguito.

Visualizzare il banner di accesso corrente per un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da visualizzare.
4. Verifica che la scheda Dettagli.
5. Visualizza il testo del banner di accesso attualmente configurato accanto a Testo del banner di accesso client.

Visualizzare il banner di accesso attualmente configurato per un endpoint Client VPN (AWS CLI)

Utilizza il comando [describe-client-vpn-endpoints](#).

Endpoint Client VPN

Tutte le sessioni VPN del client terminano nell'endpoint Client VPN. Puoi configurare l'endpoint Client VPN per gestire e controllare tutte le sessioni VPN del client.

Indice

- [Creare un endpoint Client VPN](#)
- [Modifica un endpoint Client VPN.](#)
- [Visualizzare gli endpoint Client VPN](#)
- [Elimina un endpoint Client VPN.](#)

Creare un endpoint Client VPN

Crea un endpoint Client VPN per consentire ai client di stabilire una sessione VPN.

Client VPN deve essere creato nello stesso account AWS in cui viene assegnata la rete di destinazione.

Prerequisiti

Prima di iniziare, assicurati di disporre di quanto riportato di seguito:

- Esamina le regole e le limitazioni in [Regole e best practice di AWS Client VPN](#).
- Genera il certificato server e, se necessario, il certificato client. Per ulteriori informazioni, consulta [Autenticazione client](#).


Per creare un endpoint Client VPN (console)

1. Apri alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN) e quindi scegli Create Client VPN Endpoint (Crea un endpoint del client VPN).
3. (Facoltativo) Fornisci un nome tag e una descrizione per l'endpoint Client VPN.
4. Per Client IPv4 CIDR (CIDR IPv4 client), specificare un intervallo di indirizzi IP in notazione CIDR entro cui assegnare gli indirizzi IP del client. Ad esempio, 10.0.0.0/22.

Note

L'intervallo di indirizzi non può sovrapporsi con l'intervallo di indirizzi della rete target, l'intervallo di indirizzi VPC né ad alcun percorso che verrà associato all'endpoint Client VPN. L'intervallo di indirizzi client deve essere al minimo /22 e non superiore a /12 delle dimensioni del blocco CIDR. Non è possibile modificare l'intervallo di indirizzi del client dopo aver creato l'endpoint Client VPN.

5. Per Server certificate ARN (ARN del certificato server), specificare l'ARN per il certificato TLS utilizzato dal server. I client utilizzano il certificato server per autenticare l'endpoint Client VPN a cui si connettono.

 Note


Il certificato server deve essere presente in AWS Certificate Manager (ACM) nella regione in cui si sta creando l'endpoint VPN client. Il certificato può essere fornito con ACM o importato in ACM.

6. Specificare il metodo di autenticazione da utilizzare per autenticare i client quando stabiliscono una connessione VPN. È necessario selezionare un metodo di autenticazione.
 - Per utilizzare l'autenticazione basata sull'utente, selezionare Usa l'autenticazione basata sull'utente, quindi scegliere una delle opzioni seguenti:
 - Autenticazione di Active Directory: scegliere questa opzione per l'autenticazione di Active Directory. Per ID directory, specificare l'ID della Active Directory da utilizzare.
 - Autenticazione federata: scegliere questa opzione per l'autenticazione federata basata su SAML.

Per ARN del provider SAML, specificare l'ARN del provider di identità SAML IAM.

(Facoltativo) Per Self-service SAML provider ARN (ARN del provider SAML self-service) specifica l'ARN del provider di identità SAML IAM creato per [supportare il portale self-service](#), se applicabile.

- Per utilizzare l'autenticazione reciproca del certificato, selezionare Utilizza autenticazione reciproca e per ARN del certificato client, specificare l'ARN del certificato client di cui è stato effettuato il provisioning in AWS Certificate Manager (ACM).


 Note

Se i certificati server e client sono stati rilasciati dalla stessa certification authority (CA), è possibile utilizzare l'ARN del certificato server sia per il server che per il client. Se il certificato client è stato emesso da una CA differente, sarà necessario specificare l'ARN del certificato client.

7. (Facoltativo) Per la registrazione delle connessioni, specifica se registrare i dati sulle connessioni client utilizzando Amazon CloudWatch Logs. Attivare Abilita i dettagli del registro sulle


connessioni client. Per il nome del gruppo di log CloudWatch Logs, inserisci il nome del gruppo di log da utilizzare. Per CloudWatch Logs log stream name, inserisci il nome del log stream da utilizzare o lascia vuota questa opzione per consentirci di creare un flusso di log per te.

8. (Facoltativo) Per Handler di connessioni client, attiva Abilita handler connessioni client per eseguire codice personalizzato che consente o nega una nuova connessione all'endpoint Client VPN. Per Client Connect Handler ARN (ARN handler di connessioni client) specifica l'ARN (Amazon Resource Name) della funzione Lambda che contiene la logica che consente o nega le connessioni.
9. (Facoltativo) Specificare i server DNS da utilizzare per la risoluzione DNS. Per usare i server DNS personalizzati, specificare per DNS Server 1 IP address (Indirizzo IP 1 del server DNS) e DNS Server 2 IP address (Indirizzo IP 2 del server DNS) gli indirizzi IP dei server DNS da utilizzare. Per usare il server DNS del VPC, per DNS Server 1 IP address (Indirizzo IP 1 server DNS) o DNS Server 2 IP address (Indirizzo IP 2 server DNS), specificare gli indirizzi IP e aggiungere l'indirizzo IP del server DNS del VPC.

 Note

Accertarsi che il server DNS possa essere raggiunto dal client.

10. (Facoltativo) Per impostazione predefinita, l'endpoint del client VPN utilizza il protocollo di trasporto UDP. Per utilizzare invece il protocollo di trasporto TCP, per Protocollo di trasporto, selezionare TCP.

 Note

Di solito, il protocollo UDP offre prestazioni migliori rispetto al TCP. Non è possibile modificare il protocollo di trasporto dopo aver creato l'endpoint Client VPN.

11. (Facoltativo) Affinché l'endpoint sia un endpoint Client VPN split-tunnel, seleziona Enable split-tunnel (Abilita split-tunnel). Per impostazione predefinita, lo split-tunnel su un endpoint Client VPN è disabilitato.
12. (Facoltativo) Per VPC ID (ID VPC) scegli il VPC da associare all'endpoint Client VPN. Per Security Group IDs (ID gruppi di sicurezza) scegli uno o più gruppi di sicurezza del VPC da applicare all'endpoint Client VPN.
13. (Facoltativo) Per VPN port (Porta VPN), scegliere il numero di porta VPN. Il valore predefinito è 443.

14. (Facoltativo) Per generare un [URL del portale self-service](#) per i client attiva Enable self-service portal (Abilita portale self-service).
15. (Opzionale) In Session timeout hours (Ore di timeout della sessione), scegliere la durata massima desiderata della sessione VPN in ore dalle opzioni disponibili o lasciare l'impostazione predefinita di 24 ore.
16. (Facoltativo) Specificare se abilitare il testo del banner di accesso client. Attiva Enable client login banner (Abilita il banner di accesso client). Quindi, per Client Login Banner Text (Testo banner di accesso client) inserire il testo che verrà visualizzato in un banner sui client forniti da AWS quando viene stabilita una sessione VPN. Solo caratteri codificati UTF-8. Massimo 1400 caratteri.
17. Selezionare Create Client VPN Endpoint (Crea endpoint VPN client).

Dopo aver creato l'endpoint Client VPN, esegui le operazioni seguenti per completare la configurazione e consentire ai client di connettersi:

- Lo stato iniziale dell'endpoint Client VPN è `pending-associate`. I client possono connettersi all'endpoint Client VPN solo dopo aver associato la prima [rete di destinazione](#).
- Aggiungere una [regola di autorizzazione](#) per specificare quali client hanno accesso alla rete.
- Scarica e prepara il [file di configurazione](#) dell'endpoint Client VPN da distribuire ai client.
- Indica ai client di utilizzare il client fornito da AWS o un'altra applicazione client basata su OpenVPN per connettersi all'endpoint Client VPN. Per ulteriori informazioni, consulta la [AWS Client VPN Guida per l'utente](#).

Per creare un endpoint Client VPN (AWS CLI)

Utilizza il comando [create-client-vpn-endpoint](#).

Modifica un endpoint Client VPN.

Dopo aver creato un Client VPN, puoi modificare una delle seguenti impostazioni:

- Descrizione
- Certificato del server
- Opzioni di registrazione della connessione client
- L'opzione dell'handler di connessioni client

- Server DNS
- Opzione split-tunnel
- Route (quando si utilizza l'opzione split-tunnel)
- Creazione di un elenco di revoche di certificati (CRL)
- Regole di autorizzazione
- VPC e associazioni gruppi di sicurezza
- Numero di porta VPN
- L'opzione del portale self-service
- La durata massima della sessione VPN
- Abilitare o disabilitare il testo del banner di accesso client
- Testo del banner di accesso client

Note

Le modifiche agli endpoint Client VPN, incluse le modifiche all'elenco di revoche di certificati (CRL), avranno effetto fino a 4 ore dopo l'accettazione di una richiesta dal servizio Client VPN.

Non è possibile modificare l'intervallo CIDR IPv4 del client, le opzioni di autenticazione o il protocollo di trasporto dopo che l'endpoint Client VPN è stato creato.

Quando si modifica uno dei seguenti parametri in un endpoint VPN client, la connessione viene reimpostata:

- Certificato del server
- Server DNS
- Opzione tunnel diviso (attivazione o disattivazione del support)
- Percorsi (quando si utilizza l'opzione del tunnel diviso)
- Creazione di un elenco di revoche di certificati (CRL)
- Regole di autorizzazione
- Numero di porta VPN

Puoi modificare un endpoint Client VPN utilizzando la console o la AWS CLI.

Per modificare un endpoint Client VPN (console)

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da modificare, scegli Operazioni, quindi Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).
4. Per Description (Descrizione), immetti una breve descrizione dell'endpoint Client VPN.
5. Per Server certificate ARN (ARN del certificato server), specificare l'ARN per il certificato TLS utilizzato dal server. I client utilizzano il certificato server per autenticare l'endpoint Client VPN a cui si connettono.

Note

Il certificato server deve essere presente in AWS Certificate Manager (ACM) nella regione in cui si sta creando l'endpoint VPN client. Il certificato può essere fornito con ACM o importato in ACM.

6. Specificare se registrare i dati sulle connessioni client utilizzando Amazon CloudWatch Logs. Per Do you want to log the details on client connections? (Vuoi registrare i dettagli sulle connessioni client?), procedere in uno dei seguenti modi:
 - Per attivare la registrazione delle connessioni client, attivare Enable log details on client connections (Abilita i dettagli del registro sulle connessioni client). Per il nome del gruppo di log CloudWatch Logs, seleziona il nome del gruppo di log da utilizzare. Per CloudWatch Logs log stream name, selezionate il nome del log stream da utilizzare o lasciate vuota questa opzione per consentirci di creare un flusso di log per voi.
 - Per disattivare la registrazione della connessione client, disattivare Abilita i dettagli del registro sulle connessioni client.
7. Per Handler di connessioni client, per attivare l'[handler di connessioni client](#) attivare Enable client connect handler (Abilita l'handler delle connessioni client). Per Client Connect Handler ARN (ARN handler di connessioni client) specifica l'ARN (Amazon Resource Name) della funzione Lambda che contiene la logica che consente o nega le connessioni.
8. Attivare o disattivare Enable DNS servers (Abilita server DNS). Per usare i server DNS personalizzati, specificare per DNS Server 1 IP address (Indirizzo IP 1 del server DNS) e DNS Server 2 IP address (Indirizzo IP 2 del server DNS) gli indirizzi IP dei server DNS da utilizzare. Per usare il server DNS del VPC, per DNS Server 1 IP address (Indirizzo IP 1 server DNS) o

DNS Server 2 IP address (Indirizzo IP 2 server DNS), specificare gli indirizzi IP e aggiungere l'indirizzo IP del server DNS del VPC.

Note

Accertarsi che il server DNS possa essere raggiunto dal client.

9. Attivare o disattivare Enable split-tunnel (Abilita split-tunnel). Per impostazione predefinita, lo split-tunnel su un endpoint VPN è disabilitato.
10. Per ID VPC, scegli il VPC da associare all'endpoint Client VPN. Per Security Group IDs (ID gruppi di sicurezza) scegli uno o più gruppi di sicurezza del VPC da applicare all'endpoint Client VPN.
11. Per VPN port (Porta VPN), scegli il numero di porta VPN. Il valore predefinito è 443.
12. Per generare un [URL del portale self-service](#) per i client, attiva Enable self-service portal (Abilita portale self-service).
13. (Opzionale) In Ore di timeout della sessione, scegliere la durata massima desiderata della sessione VPN in ore dalle opzioni disponibili o lasciare l'impostazione predefinita di 24 ore.
14. Abilitare o disabilitare Enable client login banner (Abilita il banner di accesso client. Se si desidera usare il banner di accesso del client, inserire il testo che verrà visualizzato in un banner sui client forniti da AWS quando viene stabilita una sessione VPN. Solo caratteri codificati UTF-8. Massimo 1400 caratteri).
15. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Per modifica un endpoint Client VPN (AWS CLI)

Utilizza il comando [modify-client-vpn-endpoint](#).

Visualizzare gli endpoint Client VPN

Puoi visualizzare informazioni sugli endpoint Client VPN utilizzando la console o la AWS CLI.

Per visualizzare gli endpoint Client VPN (console)

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da visualizzare.

4. Utilizzo delle schede Dettagli, Associazioni rete di destinazione, Gruppi di sicurezza, Regole di autorizzazione, Tabella di routing, Connessioni e Tag per visualizzare informazioni sugli endpoint Client VPN esistenti.

È possibile utilizzare i filtri per migliorare la ricerca.

Visualizzare gli endpoint Client VPN (AWS CLI)

Utilizza il comando [describe-client-vpn-endpoints](#).

Elimina un endpoint Client VPN.

È necessario annullare l'associazione di tutte le reti di destinazione prima di eliminare l'endpoint Client VPN. Quando elimini un endpoint Client VPN, lo stato diventa `deleting` e i client non sono più in grado di connettersi.

Puoi eliminare un endpoint Client VPN utilizzando la console o la AWS CLI.

Per eliminare un endpoint Client VPN (console)

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da eliminare. Scegli Operazioni, Delete Client VPN endpoint (Elimina l'endpoint Client VPN).
4. Scegliere Delete (Elimina), quindi scegliere Delete (Elimina) nella finestra di conferma.

Per eliminare un endpoint Client VPN (AWS CLI)

Utilizza il comando [delete-client-vpn-endpoint](#).

Operazioni con i log delle connessioni

Puoi abilitare la registrazione (logging) delle connessioni per un endpoint Client VPN nuovo o esistente e avviare l'acquisizione dei registri delle connessioni.

Prima di iniziare, devi avere un gruppo di log CloudWatch Logs nel tuo account. Per ulteriori informazioni, consultare [Utilizzo di gruppi di registri e flussi di registro](#) nella Guida per l'utente di

Amazon CloudWatch Logs. Vengono applicati costi aggiuntivi per l'utilizzo di CloudWatch Logs. Per ulteriori informazioni, consulta [Prezzi di Amazon CloudWatch](#).

Quando attivi la registrazione delle connessioni, puoi specificare il nome di un flusso di log nel gruppo di log. Se non specifichi un flusso di log, il servizio Client VPN ne crea uno automaticamente.

Abilitazione della registrazione delle connessioni per un nuovo endpoint Client VPN

Puoi abilitare la registrazione delle connessioni quando crei un nuovo endpoint Client VPN utilizzando la console o la riga di comando.

Per abilitare la registrazione delle connessioni per un nuovo endpoint Client VPN tramite la console

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Endpoint del client VPN e quindi scegli Create Client VPN Endpoint (Crea un endpoint del client VPN).
3. Completa le opzioni fino a raggiungere la sezione Registrazione delle connessioni. Per ulteriori informazioni su queste opzioni, consulta [Creare un endpoint Client VPN](#).
4. In Registrazione delle connessioni, attiva Enable log details on client connections (Abilita i dettagli del registro sulle connessioni client).
5. Per CloudWatch Logs log group name (Nome del gruppo di log di CloudWatch Logs), immetti il nome del gruppo di log di CloudWatch Logs.
6. (Facoltativo) Per CloudWatch Logs log group name (Nome del gruppo di log di CloudWatch Logs) scegli il nome del flusso di log di CloudWatch Logs.
7. Selezionare Create Client VPN Endpoint (Crea endpoint VPN client).

Per abilitare la registrazione delle connessioni per un nuovo endpoint Client VPN utilizzando la AWS CLI

Utilizza il comando [create-client-vpn-endpoint](#) e specifica il parametro `--connection-log-options`. È possibile specificare le informazioni sui log delle connessioni in formato JSON, come illustrato nell'esempio seguente.

```
{
  "Enabled": true,
  "CloudwatchLogGroup": "ClientVpnConnectionLogs",
```



```
"CloudwatchLogStream": "NewYorkOfficeVPN"  
}
```

Abilitazione della registrazione delle connessioni per un endpoint Client VPN esistente

Puoi abilitare la registrazione delle connessioni per un endpoint Client VPN esistente utilizzando la console o la riga di comando.

Per abilitare la registrazione delle connessioni per un endpoint Client VPN esistente utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN, scegli Actions (Operazioni), quindi Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).
4. In Registrazione delle connessioni, attiva Enable log details on client connections (Abilita i dettagli del registro sulle connessioni client).
5. Per CloudWatch Logs log group name (Nome del gruppo di log di CloudWatch Logs), immetti il nome del gruppo di log di CloudWatch Logs.
6. (Facoltativo) Per CloudWatch Logs log group name (Nome del gruppo di log di CloudWatch Logs) scegli il nome del flusso di log di CloudWatch Logs.
7. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Per abilitare la registrazione delle connessioni per un endpoint Client VPN esistente utilizzando la AWS CLI

Utilizza il comando [modify-client-vpn-endpoint](#) e specifica il parametro `--connection-log-options`. È possibile specificare le informazioni sui log delle connessioni in formato JSON, come illustrato nell'esempio seguente.

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

Visualizzare i log delle connessioni.

Puoi visualizzare i log delle connessioni utilizzando la console CloudWatch Logs.

Per visualizzare i log delle connessioni utilizzando la console

1. Aprire la console CloudWatch all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel riquadro di navigazione, scegliere Log groups (Gruppi di log) e selezionare il gruppo di log contenente i log delle connessioni.
3. Seleziona il flusso di log per l'endpoint Client VPN.

Note

Nella colonna Timestamp viene visualizzata l'ora in cui è stato pubblicato il log delle connessioni CloudWatch Logs, non l'ora della connessione.

Per ulteriori informazioni sulla ricerca dei dati dei log, consulta [Ricerca dei dati di log utilizzando i modelli di filtro](#) nella Guida per l'utente di Amazon CloudWatch Logs.

Disattivazione della registrazione della connessione

Puoi disattivare la registrazione delle connessioni per un endpoint Client VPN utilizzando la console o la riga di comando. Quando disattivi la registrazione delle connessioni, i log delle connessioni esistenti in CloudWatch Logs non vengono eliminati.

Per disabilitare la registrazione delle connessioni utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN, scegli Operazioni, quindi Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).
4. In Registrazione delle connessioni, disattiva Enable log details on client connections (Abilita i dettagli del registro sulle connessioni client).
5. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Per disattivare i log di connessione utilizzando AWS CLI

Utilizza il comando [modify-client-vpn-endpoint](#) e specifica il parametro `--connection-log-options`. Assicurarsi che `Enabled` sia impostato su `false`.

Esportazione e configurazione del file di configurazione del client

Il file di configurazione dell'endpoint Client VPN è il file di configurazione utilizzato dai client (utenti) per stabilire una connessione VPN con l'endpoint Client VPN. È necessario scaricare (esportare) questo file e distribuirlo a tutti i client che richiedono l'accesso alla VPN. In alternativa, se è stato abilitato il portale self-service per l'endpoint Client VPN, i client possono accedere al portale e scaricare autonomamente il file di configurazione. Per ulteriori informazioni, consulta [Accedere al portale self-service](#).

Se l'endpoint Client VPN utilizza l'autenticazione reciproca, è necessario [aggiungere il certificato del client e la chiave privata del client al file di configurazione .ovpn](#) che hai scaricato. Dopo aver aggiunto le informazioni, i client possono importare il file .ovpn nel software client OpenVPN.

Important

Se non aggiungi le informazioni sul certificato client e sulla chiave privata del client al file, i client che eseguono l'autenticazione tramite l'autenticazione reciproca non possono connettersi all'endpoint Client VPN.

Per impostazione predefinita, l'opzione «remote-random-hostname» nella configurazione del client OpenVPN abilita il DNS wildcard. Poiché il DNS jolly è abilitato, il client non memorizza nella cache l'indirizzo IP dell'endpoint e non sarà possibile eseguire il ping del nome DNS dell'endpoint.

Se l'endpoint Client VPN utilizza l'autenticazione di Active Directory e abiliti l'autenticazione a più fattori nella directory dopo aver distribuito il file di configurazione del client, devi scaricare un nuovo file e ridistribuirlo ai client. I client non possono utilizzare il file di configurazione precedente per connettersi all'endpoint Client VPN.

Esportazione del file di configurazione del client

Puoi esportare la configurazione del client utilizzando la console o la AWS CLI.

Per esportare la configurazione del client (console)

1. Accedi alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.

2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN per cui scaricare la configurazione del client e scegli Download Client Configuration (Scarica configurazione client).

Per esportare la configurazione del client (AWS CLI)

Usa il comando [export-client-vpn-client-configuration](#) e specifica il nome del file di output.

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

Aggiunta delle informazioni sul certificato del client e la chiave (autenticazione reciproca)

Se l'endpoint Client VPN utilizza l'autenticazione reciproca, è necessario aggiungere il certificato del client e la chiave privata del client al file di configurazione .ovpn che hai scaricato.

Quando si utilizza l'autenticazione reciproca non è possibile modificare il certificato client.

Per aggiungere le informazioni sul certificato del client e la chiave (autenticazione reciproca)

Puoi utilizzare una delle seguenti opzioni.

(Opzione 1) Puoi distribuire il certificato del client e la chiave ai client insieme al file di configurazione dell'endpoint Client VPN. In questo caso, specifica il percorso al certificato e alla chiave nel file di configurazione. Apri il file di configurazione utilizzando l'editor di testo preferito e aggiungi quanto segue alla fine del file. Sostituisci */path/* con il percorso del certificato e della chiave client (il percorso è relativo al client che si connette all'endpoint).

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

(Opzione 2) Puoi aggiungere il contenuto del certificato del client tra i tag `<cert></cert>` e il contenuto della chiave privata tra i tag `<key></key>` al file di configurazione. Se scegli questa opzione, devi distribuire solo il file di configurazione ai client.

Se hai generato certificati client e chiavi distinti per ogni utente che si conatterà all'endpoint Client VPN, ripeti questa fase per ogni utente.

Di seguito è riportato un esempio del formato di un file di configurazione Client VPN che include il certificato client e la chiave.

```
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
```

Route

Ogni endpoint Client VPN ha una tabella di routing che descrive le route disponibili della rete di destinazione. Ogni route della tabella di routing determina dove viene indirizzato il traffico di rete. È necessario configurare le regole di autorizzazione per ciascuna route dell'endpoint Client VPN per specificare quali client hanno accesso alla rete di destinazione.

Quando associ una sottorete da un VPC a un endpoint Client VPN, viene automaticamente aggiunta una route per il VPC alla tabella di routing dell'endpoint Client VPN. Per abilitare l'accesso a reti aggiuntive, ad esempio VPC con peering, reti in locale, rete locale (per consentire ai client di comunicare tra loro) o Internet, è necessario aggiungere manualmente una route alla tabella di routing dell'endpoint Client VPN.

Note

Se stai associando più sottoreti all'endpoint VPN client, assicurati di creare un routing per ogni sottorete come descritto in [Accesso intermittente a un VPC in peering, ad Amazon S3 o a Internet](#). Ogni sottorete associata dovrebbe avere un insieme identico di routing.

Indice

- [Considerazioni per lo split-tunnel su endpoint Client VPN](#)
- [Creazione di una route dell'endpoint](#)
- [Visualizzazione delle route dell'endpoint](#)
- [Eliminazione di una route dell'endpoint](#)

Considerazioni per lo split-tunnel su endpoint Client VPN

Quando utilizzi lo split-tunnel su un endpoint Client VPN, tutte le route presenti nelle tabelle di routing Client VPN vengono aggiunte alla tabella di routing del client quando viene stabilita la VPN. Se aggiungi una route dopo aver stabilito la VPN, è necessario ripristinare la connessione in modo che la nuova route venga inviata al client.

Ti consigliamo di tenere conto del numero di route che il dispositivo client è in grado di gestire prima di modificare la tabella di routing dell'endpoint Client VPN.

Creazione di una route dell'endpoint

Quando crei una route, è necessario specificare il modo in cui viene indirizzato il traffico alla rete di destinazione.

Per consentire ai client di accedere a Internet, aggiungi la route di destinazione `0.0.0.0/0`.

Puoi aggiungere route a un endpoint Client VPN utilizzando la console e la AWS CLI.

Per creare una route endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui aggiungere il routing, scegli Tabella di routing), quindi Create Route (Crea routing).

4. Per Route destination (Destinazione route), specificare l'intervallo CIDR IPv4 della rete di destinazione. Ad esempio:
 - Per aggiungere un routing per il VPC dell'endpoint Client VPN, immettere l'intervallo CIDR IPv4 del VPC.
 - Per aggiungere una route per l'accesso a Internet, immettere `0.0.0.0/0`
 - Per aggiungere una route per un VPC in peering, immettere l'intervallo CIDR IPv4 del VPC in peering,
 - Per aggiungere un routing per una rete on-premise, immetti l'intervallo CIDR IPv4 della connessione AWS Site-to-Site VPN.
5. Per ID sottorete per l'associazione della rete di destinazione) seleziona la sottorete associata all'endpoint Client VPN.

In alternativa, se si aggiunge un routing per la rete dell'endpoint client VPN locale, selezionare `local`.
6. (Facoltativo) In Descrizione, inserire una breve descrizione del routing.
7. Selezionare Create Route (Crea route).

Per creare una route per l'endpoint Client VPN (AWS CLI)

Utilizza il comando [create-client-vpn-route](#).

Visualizzazione delle route dell'endpoint

Puoi visualizzare le route per un determinato endpoint Client VPN utilizzando la console o la AWS CLI.

Per visualizzare le route degli endpoint Client VPN (console)

1. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
2. Seleziona l'endpoint Client VPN per cui visualizzare i routing e scegli Tabella di routing).

Per visualizzare le route per l'endpoint Client VPN (AWS CLI)

Utilizza il comando [describe-client-vpn-routes](#).

Eliminazione di una route dell'endpoint

È possibile eliminare solo le route aggiunte manualmente. Non puoi eliminare le route che vengono aggiunte automaticamente quando viene associata una sottorete all'endpoint Client VPN. Per eliminare una route aggiunta automaticamente, è necessario dissociare la sottorete che ne ha provocato la creazione dall'endpoint Client VPN.

Puoi eliminare una route da un endpoint Client VPN utilizzando la console o la AWS CLI.

Per eliminare una route endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da cui eliminare il routing e scegli Tabella di routing).
4. Selezionare il routing da eliminare, scegliere Elimina routing, quindi Elimina routing.

Per eliminare una route dell'endpoint Client VPN (AWS CLI)

Utilizza il comando [delete-client-vpn-route](#).

Reti target

Una rete target è una sottorete in un VPC. Un endpoint Client VPN deve avere almeno una rete di destinazione per consentire ai client di connettersi e di stabilire una connessione VPN.

Per ulteriori informazioni sui tipi di accesso che è possibile configurare, ad esempio per consentire ai client di accedere a Internet, consulta [Scenari ed esempi per AWS Client VPN](#).

Indice

- [Associare una rete di destinazione a un endpoint Client VPN](#)
- [Applicazione di un gruppo di sicurezza a una rete target](#)
- [Annullare l'associazione di una rete di destinazione da un endpoint Client VPN](#)
- [Visualizzazione delle reti target](#)

Associare una rete di destinazione a un endpoint Client VPN

Puoi associare una o più reti di destinazione (sottoreti) a un endpoint Client VPN.

Si applicano le regole seguenti:

- La sottorete deve disporre di un blocco CIDR con almeno una maschera di bit /27, ad esempio 10.0.0.0/27. La sottorete deve disporre di almeno 20 indirizzi IP disponibili in qualsiasi momento.
- Il blocco CIDR della sottorete non può sovrapporsi all'intervallo CIDR del client dell'endpoint Client VPN.
- Se associ più sottoreti a un endpoint Client VPN, ogni endpoint deve trovarsi in una zona di disponibilità diversa. È consigliabile associare almeno due sottoreti per garantire la ridondanza delle zone di disponibilità.
- Se al momento della creazione dell'endpoint Client VPN è stato specificato un VPC, la sottorete deve trovarsi nello stesso VPC. Se non hai ancora associato un VPC all'endpoint Client VPN, puoi scegliere qualsiasi sottorete in qualsiasi VPC.

Tutte le ulteriori associazioni di sottorete devono provenire dallo stesso VPC. Per associare una sottorete di un VPC diverso, è necessario innanzitutto modificare l'endpoint Client VPN e cambiare il VPC ad esso associato. Per ulteriori informazioni, consulta [Modifica un endpoint Client VPN.](#)

Quando associ una sottorete a un endpoint Client VPN, viene automaticamente aggiunta la route locale del VPC in cui la sottorete associata è assegnata alla tabella di routing dell'endpoint Client VPN.

Note

Dopo aver associato le reti di destinazione, quando aggiungi rimuovi ulteriori CIDR dal VPC collegato, è necessario eseguire una delle seguenti operazioni per aggiornare la route locale per la tabella di routing dell'endpoint Client VPN:

- Annullare l'associazione dell'endpoint Client VPN alla rete di destinazione e quindi associare di nuovo l'endpoint Client VPN alla rete di destinazione.
- Aggiungere manualmente la route o rimuovere la route dalla tabella di routing dell'endpoint Client VPN.

Dopo aver associato la prima sottorete all'endpoint Client VPN, lo stato dell'endpoint Client VPN cambia da `pending-associate` a `available` e i client sono in grado di stabilire una connessione VPN.

Per associare una rete di destinazione a un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui associare la rete di destinazione, scegli Associazioni rete di destinazione, quindi Associa rete di destinazione.
4. Per VPC, scegliere il VPC in cui si trova la sottorete. Se durante la creazione dell'endpoint Client VPN hai specificato un VPC o sono disponibili associazioni sottorete precedenti, questo deve essere lo stesso VPC.
5. Per Sottorete da associare scegli la sottorete da associare all'endpoint Client VPN.
6. Scegli Associa rete tdi destinazione.

Per associare una rete di destinazione a un endpoint Client VPN (AWS CLI)

Utilizza il comando [associate-client-vpn-target-network](#).

Applicazione di un gruppo di sicurezza a una rete target

Quando crei un endpoint Client VPN puoi specificare i gruppi di sicurezza da applicare alla rete di destinazione. Quando associ la prima rete di destinazione a un endpoint Client VPN, viene applicato automaticamente il gruppo di sicurezza predefinito del VPC in cui si trova la sottorete associata. Per ulteriori informazioni, consulta [Gruppi di sicurezza](#).

Puoi modificare i gruppi di sicurezza per l'endpoint Client VPN. Le regole del gruppo di sicurezza richieste dipendono dal tipo di accesso VPN che si desidera configurare. Per ulteriori informazioni, consulta [Scenari ed esempi per AWS Client VPN](#).

Per applicare un gruppo di sicurezza a una rete target (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui applicare i gruppi di sicurezza.
4. Scegli Gruppi di sicurezza e quindi Create Security Group (Crea gruppo di sicurezza).
5. Seleziona il gruppo o i gruppi di sicurezza appropriati da ID gruppo di sicurezza.
6. Seleziona Apply Security Groups (Applica i gruppi di sicurezza).

Per applicare un gruppo di sicurezza a una rete target (AWS CLI)

Utilizza il comando [apply-security-groups-to-client-vpn-target-network](#).

Annullare l'associazione di una rete di destinazione da un endpoint Client VPN

Quando annulli l'associazione una rete di destinazione, vengono eliminati tutti gli instradamenti aggiuntivi aggiunti manualmente alla tabella di routing dell'endpoint Client VPN, così come l'instradamento creato automaticamente quando è stata effettuata l'associazione di rete di destinazione (l'instradamento locale del VPC). Se annulli l'associazione di tutte le reti di destinazione da un endpoint Client VPN, i client non sono più in grado di stabilire una connessione VPN.

Per annullare l'associazione di una rete di destinazione da un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN a cui la rete di destinazione è associata e scegli Associazioni rete di destinazione.
4. Seleziona la rete target da disassociare, scegli Disassociate (Disassocia), quindi Disassociate target network (Disassocia rete di destinazione).

Per annullare l'associazione di una rete di destinazione da un endpoint Client VPN (AWS CLI)

Utilizza il comando [disassociate-client-vpn-target-network](#).

Visualizzazione delle reti target

Puoi visualizzare le reti di destinazione associate a un endpoint Client VPN utilizzando la console o la AWS CLI.

Per visualizzare le reti target (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN e scegli Associazioni rete di destinazione.

Per visualizzare le reti target utilizzando la AWS CLI

Utilizza il comando [describe-client-vpn-target-networks](#).

Durata massima della sessione VPN

AWS Client VPN offre diverse opzioni per la durata massima della sessione VPN. Puoi configurare una durata massima della sessione VPN più breve per soddisfare i requisiti di sicurezza e conformità. Per impostazione predefinita, la sessione VPN massima dura 24 ore.

Note

Quando il valore della durata massima della sessione VPN viene ridotto, le sessioni VPN attive precedenti al nuovo valore di timeout vengono disconnesse.

Consulta [Note di rilascio per il client fornito da AWS](#) nella Guida per l'utente di AWS Client VPN per informazioni dettagliate sulle applicazioni desktop client.

Indice

- [Configurare la sessione VPN massima durante la creazione di un endpoint Client VPN](#)
- [Visualizzare la durata massima della sessione VPN corrente](#)
- [Modificare la durata massima della sessione VPN](#)

Configurare la sessione VPN massima durante la creazione di un endpoint Client VPN

Per la procedura dettagliata per configurare la sessione VPN massima durante la creazione di un endpoint Client VPN, consulta [Creare un endpoint Client VPN](#).

Visualizzare la durata massima della sessione VPN corrente

Utilizza la procedura seguente per visualizzare la durata massima della sessione VPN corrente.

Visualizzare la durata massima della sessione VPN corrente per un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Client VPN Endpoints (Endpoint del client VPN).
3. Seleziona l'endpoint Client VPN da visualizzare.

4. Verifica che la scheda Dettagli sia selezionata.
5. Visualizza la durata massima della sessione VPN corrente accanto a Session timeout hours (Ore di timeout della sessione).

Visualizzare la durata massima della sessione VPN corrente per un endpoint Client VPN (AWS CLI)

Utilizza il comando [describe-client-vpn-endpoints](#).

Modificare la durata massima della sessione VPN

Utilizza la procedura seguente per modificare la durata massima della sessione VPN corrente.

Modificare la durata massima di una sessione VPN esistente per un endpoint Client VPN (console)

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Endpoint del client VPN.
3. Seleziona l'endpoint Client VPN da modificare, scegli Actions (Operazioni), quindi Modify Client VPN Endpoint (Modifica l'endpoint Client VPN).
4. For Session timeout hours (Ore di timeout della sessione), scegli la durata massima desiderata della sessione VPN in ore.
5. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Modificare la durata massima di una sessione VPN esistente per un endpoint Client VPN (AWS CLI)

Utilizza il comando [modify-client-vpn-endpoint](#).

Sicurezza in AWS Client VPN

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il [modello di responsabilità condivisa](#) descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue AWS i servizi nel cloud AWS. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei [Programmi di conformità AWS](#). Per informazioni sui programmi di conformità applicabili a AWS Client VPN, consulta [Servizi AWS coperti dal programma di conformità](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, le leggi e le normative applicabili.

AWS Client VPN è parte del servizio Amazon VPC. Per ulteriori informazioni sulla sicurezza in Amazon VPC, consulta [Sicurezza](#) nella Guida per l'utente di Amazon VPC.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si usa Client VPN. Gli argomenti seguenti illustrano come configurare Client VPN per soddisfare gli obiettivi di sicurezza e compliance. È inoltre illustrato come utilizzare altri servizi AWS che consentono di monitorare e proteggere le risorse Client VPN.

Indice

- [Protezione dei dati in AWS Client VPN](#)
- [Identità e gestione degli accessi per AWS Client VPN](#)
- [Resilienza in AWS Client VPN](#)
- [Sicurezza dell'infrastruttura in AWS Client VPN](#)
- [Best practice relative alla sicurezza di AWS Client VPN](#)
- [Considerazioni IPv6 per AWS Client VPN](#)

Protezione dei dati in AWS Client VPN

Il [modello di responsabilità condivisa](#) di AWS si applica alla protezione dei dati nei Client VPN AWS. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile di mantenere il controllo sui contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della sicurezza e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il suo lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura la creazione di log delle attività di API e utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio un campo Nome. Questo include il lavoro con Client VPN o altri servizi Servizi AWS utilizzando la console, l'API, AWS CLI o gli SDK AWS. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i log di fatturazione o di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia in transito

AWS Client VPN fornisce connessioni sicure da qualsiasi posizione utilizzando Transport Layer Security (TLS) 1.2 o versione successiva.

Riservatezza del traffico Internet

Abilitazione dell'accesso tra reti

Puoi consentire ai client di connettersi al VPC e ad altre reti tramite un endpoint Client VPN. Per maggiori informazioni ed esempi, vedi [Scenari ed esempi per AWS Client VPN](#).

Limitazione dell'accesso alle reti

Puoi configurare l'endpoint Client VPN in modo da limitare l'accesso a risorse specifiche nel VPC. Per l'autenticazione basata sull'utente puoi anche limitare l'accesso a parti della rete, in base al gruppo di utenti che accede all'endpoint Client VPN. Per ulteriori informazioni, consulta [Limitazione dell'accesso alla propria rete utilizzando AWS Client VPN](#).

Autenticazione dei client

L'autenticazione viene implementata nel primo punto di ingresso nel cloud AWS. È utilizzata per determinare se i client sono autorizzati a connettersi all'endpoint Client VPN. Se l'autenticazione va a buon fine, i client si connettono all'endpoint Client VPN e stabiliscono una sessione VPN. Se l'autenticazione ha esito negativo, la connessione viene negata e il client non è in grado di stabilire una sessione VPN.

Client VPN offre i seguenti tipi di autenticazione client:

- [Autenticazione di Active Directory](#) (basata sull'utente)
- [Autenticazione reciproca](#) (basata su certificato)
- [Single Sign-On \(autenticazione federata basata su SAML\)](#) (basata sull'utente)

Identità e gestione degli accessi per AWS Client VPN

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi

può essere autenticato (chi ha effettuato l'accesso) e autorizzato (chi dispone di autorizzazioni) a utilizzare le risorse Client VPN. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona AWS Client VPN con IAM](#)
- [Esempi di policy basate su identità per AWS Client VPN](#)
- [Risoluzione dei problemi di identità e accesso in AWS Client VPN](#)
- [Utilizzo dei ruoli collegati ai servizi per Client VPN](#)

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite nel Client VPN.

Utente del servizio: se utilizzi il servizio Client VPN per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità Client VPN utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Client VPN, consulta [Risoluzione dei problemi di identità e accesso in AWS Client VPN](#).

Amministratore del servizio: se sei il responsabile delle risorse Client VPN presso la tua azienda, probabilmente disponi dell'accesso completo a Client VPN. Il tuo compito è determinare le funzionalità e le risorse di Client VPN a cui gli utenti del servizio possono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Client VPN, consulta [Come funziona AWS Client VPN con IAM](#).

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a Client VPN. Per visualizzare policy basate su identità di Client VPN di esempio che puoi utilizzare in IAM, consulta [Esempi di policy basate su identità per AWS Client VPN](#).

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione [Come accedere al tuo Account AWS](#) nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta [Firma delle richieste AWS](#) nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\) in AWS](#) nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente di IAM.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede a Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono a Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un [utente IAM](#) è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente di IAM.

Un [gruppo IAM](#) è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Quando creare un utente IAM \(invece di un ruolo\)](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità all'interno di Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo [scambio di ruoli](#). È possibile assumere un ruolo chiamando un'operazione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Creazione di un ruolo per un provider di identità di terza parte](#) nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center.
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.
- **Accesso multi-servizio:** alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
 - **Inoltro delle sessioni di accesso (FAS):** quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio

AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).

- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLI o dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWS sotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta [Panoramica delle liste di controllo degli accessi \(ACL\)](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- **Policy di controllo dei servizi (SCP):** le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata degli Account AWS multipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella Guida per l'utente di IAM.

Come funziona AWS Client VPN con IAM

Prima di utilizzare IAM per gestire l'accesso a Client VPN, scopri quali funzionalità IAM sono disponibili all'uso con Client VPN.

Funzionalità IAM che è possibile utilizzare con AWS Client VPN

Funzionalità IAM	Supporto per Client VPN
Policy basate su identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per ottenere un quadro generale del funzionamento di Client VPN e altri servizi AWS con la maggior parte delle caratteristiche di IAM, consulta [Servizi AWS supportati da IAM](#) nella Guida per l'utente di IAM.

Policy basate su identità per Client VPN

Supporta le policy basate su identità Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

Esempi di policy basate su identità per Client VPN

Per visualizzare esempi di policy basate su identità Client VPN, consulta [Esempi di policy basate su identità per AWS Client VPN](#).

Policy basate su risorse all'interno di Client VPN

Supporta le policy basate su risorse No

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

Azioni di policy per Client VPN

Supporta le operazioni di policy

Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le operazioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di operazioni Client VPN, consulta [Operazioni definite da AWSClient VPN](#) in Riferimento per l'autorizzazione del servizio.

Le operazioni delle policy in Client VPN utilizzano il seguente prefisso prima dell'operazione:

```
ec2
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

]

Per visualizzare esempi di policy basate su identità Client VPN, consulta [Esempi di policy basate su identità per AWS Client VPN](#).

Risorse di policy per Client VPN

Supporta le risorse di policy	Sì
-------------------------------	----

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"

```

Per visualizzare un elenco di tipi di risorse Client VPN e dei relativi ARN, consulta [Risorse definite da AWS Client VPN](#) in Riferimento per l'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione [Operazioni definite da AWS Client VPN](#).

Per visualizzare esempi di policy basate su identità Client VPN, consulta [Esempi di policy basate su identità per AWS Client VPN](#).

Chiavi di condizione delle policy per Client VPN

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì
-----------------------------------------------------------------------	----

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione OR logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta [Elementi delle policy IAM: variabili e tag](#) nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta [Chiavi di contesto delle condizioni globali di AWS](#) nella Guida per l'utente di IAM.

Per visualizzare un elenco di chiavi di condizione Client VPN, consulta [Condition Keys \(Chiavi di condizione\) per AWS Client VPN](#) nel Service Authorization Reference (Riferimento per l'autorizzazione del servizio). Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta la sezione [Operazioni definite da AWS Client VPN](#).

Per visualizzare esempi di policy basate su identità Client VPN, consulta [Esempi di policy basate su identità per AWS Client VPN](#).

Liste di controllo degli accessi in Client VPN

Supporta le ACL

No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Client VPN

Supporta ABAC (tag nelle policy)	No
----------------------------------	----

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta [Che cos'è ABAC?](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Client VPN

Supporta le credenziali temporanee	Sì
------------------------------------	----

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta [Servizi AWS supportati da IAM](#) nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo

crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Cambio di un ruolo \(console\)](#) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLI o l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWS consiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

Autorizzazioni del principale tra servizi per Client VPN

Supporta sessioni di accesso diretto (FAS)	Sì
--------------------------------------------	----

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).

Ruoli di servizio per Client VPN

Supporta i ruoli di servizio	Sì
------------------------------	----

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.

Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di Client VPN. Modificare i ruoli del servizio solo quando Client VPN fornisce le indicazioni per farlo.

Utilizzo dei ruoli collegati ai servizi per Client VPN

Supporta i ruoli collegati ai servizi Sì

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta [Servizi AWS supportati da IAM](#). Trova un servizio nella tabella che include un Yes nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate su identità per AWS Client VPN

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Client VPN. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da Client VPN, incluso il formato degli ARN per ogni tipo di risorsa, consulta [Operazioni, risorse e chiavi di condizione per AWS Client VPN](#) in Service Authorization Reference (Guida di riferimento per l'autorizzazione del servizio).

Argomenti

- [Best practice per le policy](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

Best practice per le policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse Client VPN nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS.

Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWS e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWS che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per IAM Access Analyzer](#) nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Configurazione dell'accesso alle API protetto con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLI o l'API AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Risoluzione dei problemi di identità e accesso in AWS Client VPN

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Client VPN e di IAM.

Argomenti

- [Non sono autorizzato a eseguire un'operazione in Client VPN](#)
- [Non sono autorizzato a eseguire iam:PassRole](#)
- [Voglio consentire alle persone esterne al mio account Account AWS di accedere alle mie risorse Client VPN](#)

Non sono autorizzato a eseguire un'operazione in Client VPN

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa `my-example-widget` fittizia ma non dispone di autorizzazioni `ec2:GetWidget` fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa `my-example-widget` utilizzando l'azione `ec2:GetWidget`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a Client VPN.

Alcuni Servizi AWS consentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in Client VPN. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire alle persone esterne al mio account Account AWS di accedere alle mie risorse Client VPN

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Client VPN supporta queste funzionalità, consulta [Come funziona AWS Client VPN con IAM](#).
- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta [Fornire l'accesso agli Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

Utilizzo dei ruoli collegati ai servizi per Client VPN

AWS Client VPN utilizza AWS Identity and Access Management (IAM) [ruoli collegati ai servizi](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a un Client VPN. I ruoli collegati ai servizi sono definiti automaticamente da Client VPN e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per conto dell'utente.

Argomenti

- [Utilizzo dei ruoli per Client VPN](#)
- [Utilizzo dei ruoli per l'autorizzazione della connessione](#)

Utilizzo dei ruoli per Client VPN

AWS Client VPN utilizza AWS Identity and Access Management (IAM) [ruoli collegati ai servizi](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a un Client VPN. I ruoli collegati ai servizi sono definiti automaticamente da Client VPN e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per conto dell'utente.

Un ruolo collegato ai servizi semplifica la configurazione di Client VPN perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Client VPN definisce le autorizzazioni del ruolo associato ai servizi e, salvo diversamente definito, solo Client VPN può assumere il ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Client VPN perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Client VPN

Client VPN utilizza il ruolo collegato ai servizi denominato AWSServiceRoleForClientVPN: consenti a Client VPN di creare e gestire le risorse relative alle tue connessioni VPN.

Il ruolo collegato al servizio AWSServiceRoleForClient VPN considera attendibile il seguente servizio per assumere il ruolo:

- `clientvpn.amazonaws.com`

La policy delle autorizzazioni del ruolo denominata ClientVPNServiceRolePolicy consente ad Client VPN di eseguire le seguenti operazioni sulle risorse specificate:

- Operazione: `ec2:CreateNetworkInterface` su Resource: `"*"`
- Operazione: `ec2:CreateNetworkInterfacePermission` su Resource: `"*"`
- Operazione: `ec2:DescribeSecurityGroups` su Resource: `"*"`
- Operazione: `ec2:DescribeVpcs` su Resource: `"*"`
- Operazione: `ec2:DescribeSubnets` su Resource: `"*"`
- Operazione: `ec2:DescribeInternetGateways` su Resource: `"*"`
- Operazione: `ec2:ModifyNetworkInterfaceAttribute` su Resource: `"*"`
- Operazione: `ec2>DeleteNetworkInterface` su Resource: `"*"`
- Operazione: `ec2:DescribeAccountAttributes` su Resource: `"*"`
- Operazione: `ds:AuthorizeApplication` su Resource: `"*"`
- Operazione: `ds:DescribeDirectories` su Resource: `"*"`
- Operazione: `ds:GetDirectoryLimits` su Resource: `"*"`
- Operazione: `ds:UnauthorizeApplication` su Resource: `"*"`
- Operazione: `logs:DescribeLogStreams` su Resource: `"*"`
- Operazione: `logs:CreateLogStream` su Resource: `"*"`
- Operazione: `logs:PutLogEvents` su Resource: `"*"`
- Operazione: `logs:DescribeLogGroups` su Resource: `"*"`
- Operazione: `acm:GetCertificate` su Resource: `"*"`
- Operazione: `acm:DescribeCertificate` su Resource: `"*"`
- Operazione: `iam:GetSAMLProvider` su Resource: `"*"`
- Operazione: `lambda:GetFunctionConfiguration` su Resource: `"*"`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di ruoli collegati ai servizi per Client VPN

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei il primo endpoint Client VPN nel tuo account con AWS Management Console, AWS CLI o l'API AWS, Client VPN crea il ruolo collegato ai servizi per tuo conto, Client VPN crea il ruolo collegato ai servizi.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Client VPN crea i ruoli collegati al servizio quando crei il primo endpoint Client VPN nel tuo account.

Modifica di un ruolo collegato ai servizi per Client VPN

Client VPN non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForClientVPN`. Dopo aver creato un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Client VPN

Se non occorre più utilizzare Client VPN, è consigliabile eliminare il ruolo collegato al servizio `AWSServiceRoleForClientVPN`.

Devi innanzitutto eliminare le risorse Client VPN correlate. Questo ti impedisce di rimuovere accidentalmente l'autorizzazione ad accedere alle risorse.

Usa la console di IAM, l'interfaccia a riga di comando IAM oppure l'API IAM per eliminare il ruolo collegato ai servizi. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi Client VPN

Client VPN supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni ed endpoint di AWS](#).

Utilizzo dei ruoli per l'autorizzazione della connessione

AWS Client VPN utilizza AWS Identity and Access Management (IAM) [ruoli collegati ai servizi](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a un Client

VPN. I ruoli collegati ai servizi sono definiti automaticamente da Client VPN e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per conto dell'utente.

Un ruolo collegato ai servizi semplifica la configurazione di Client VPN perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Client VPN definisce le autorizzazioni del ruolo associato ai servizi e, salvo diversamente definito, solo Client VPN può assumere il ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Client VPN perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Client VPN

Client VPN utilizza il ruolo collegato ai servizi denominato `AWSServiceRoleForClientVPNConnections`: Role collegato ai servizi per le connessioni Client VPN

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForCodeClientVPNConnections` considera attendibili i seguenti servizi:

- `clientvpn-connections.amazonaws.com`

La policy delle autorizzazioni del ruolo denominata `ClientVPNServiceConnectionsRolePolicy` consente a Client VPN di eseguire le seguenti operazioni sulle risorse specificate:

- Operazione: `lambda:InvokeFunction` su `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di ruoli collegati ai servizi per Client VPN

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei il primo endpoint Client VPN nel tuo account con AWS Management Console, AWS CLI o l'API AWS, Client VPN crea il ruolo collegato ai servizi per tuo conto.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Client VPN crea i ruoli collegati al servizio automaticamente quando crei il primo endpoint Client VPN nel tuo account.

Modifica di un ruolo collegato ai servizi per Client VPN

Client VPN non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForClientVPNConnections`. Dopo aver creato un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Client VPN

Se non occorre più utilizzare Client VPN, è consigliabile eliminare il ruolo collegato al servizio `AWSServiceRoleForClientVPNConnections`.

Devi innanzitutto eliminare le risorse Client VPN correlate. Questo ti impedisce di rimuovere accidentalmente l'autorizzazione ad accedere alle risorse.

Usa la console di IAM, l'interfaccia a riga di comando IAM oppure l'API IAM per eliminare il ruolo collegato ai servizi. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi Client VPN

Client VPN supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni ed endpoint di AWS](#).

Resilienza in AWS Client VPN

L'infrastruttura globale di AWS è basata su regioni e zone di disponibilità AWS. Le regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite

reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle regioni AWS e le zone di disponibilità, consulta [Infrastruttura globale di AWS](#).

Oltre all'infrastruttura globale AWS, AWS Client VPN offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

Più reti di destinazione per un'elevata disponibilità

Puoi associare una rete di destinazione a un endpoint Client VPN per consentire ai client di stabilire sessioni VPN. Le reti di destinazione sono sottoreti nel VPC. Ogni sottorete associata all'endpoint Client VPN deve appartenere a una zona di disponibilità diversa. Puoi associare più sottoreti a un endpoint Client VPN per elevata disponibilità.

Sicurezza dell'infrastruttura in AWS Client VPN

Come servizio gestito, AWS Client VPN è protetto dalla sicurezza di rete globale AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina [Sicurezza del cloud AWS](#). Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina [Protezione dell'infrastruttura](#) nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate all'API pubblicate da AWS per accedere a Client VPN tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Best practice relative alla sicurezza di AWS Client VPN

AWS Client VPN fornisce una serie di caratteristiche di sicurezza che occorre valutare durante lo sviluppo e l'implementazione delle policy di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Dato che queste best practice potrebbero non essere appropriate o sufficienti nel proprio ambiente, si considerino come riflessioni utili più che istruzioni.

Regole di autorizzazione

Utilizza le regole di autorizzazione per limitare gli utenti che possono accedere alla rete. Per ulteriori informazioni, consulta [Regole di autorizzazione](#).

Gruppi di sicurezza

Utilizza i gruppi di sicurezza per controllare le risorse che gli utenti possono accedere nel VPC. Per ulteriori informazioni, consulta [Gruppi di sicurezza](#).

Elenchi di revoche di certificati client

Puoi utilizzare gli elenchi di revoche di certificati client per revocare l'accesso a un endpoint Client VPN per certificati client specifici. Ad esempio, quando un utente lascia l'organizzazione. Per ulteriori informazioni, consulta [Elenchi di revoche di certificati client](#).

Strumenti di monitoraggio

Usa gli strumenti di monitoraggio per tenere traccia della disponibilità e delle prestazioni degli endpoint Client VPN. Per ulteriori informazioni, consulta [Monitoraggio di AWS Client VPN](#).

Identity and Access Management

Gestisci l'accesso alle risorse e alle API Client VPN utilizzando le policy IAM per gli utenti IAM e i ruoli IAM. Per ulteriori informazioni, consulta [Identità e gestione degli accessi per AWS Client VPN](#).

Considerazioni IPv6 per AWS Client VPN

Attualmente il servizio Client VPN non supporta il routing del traffico IPv6 attraverso il tunnel VPN. Tuttavia, ci sono casi in cui il traffico IPv6 deve essere instradato nel tunnel VPN per evitare perdite IPv6. La perdita IPv6 può verificarsi quando sia IPv4 sia IPv6 sono abilitati e connessi alla VPN, ma la VPN non instrada il traffico IPv6 nel suo tunnel. In questo caso, quando ci si connette a una

destinazione abilitata per IPv6, si sta ancora effettuando la connessione con l'indirizzo IPv6 fornito dall'ISP. Questo lascerà trapelare il tuo vero indirizzo IPv6. Le istruzioni riportate di seguito spiegano come instradare il traffico IPv6 nel tunnel VPN.

Le seguenti direttive relative a IPv6 devono essere aggiunte al file di configurazione Client VPN per evitare perdite IPv6:

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

Un esempio potrebbe essere:

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

In questo esempio, `ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` imposterà l'indirizzo IPv6 del dispositivo del tunnel locale su `fd15:53b6:dead::2` e l'indirizzo IPv6 dell'endpoint VPN remoto su `fd15:53b6:dead::1`.

Il comando successivo, `route-ipv6 2000::/4`, instraderà gli indirizzi IPv6 da `2000:0000:0000:0000:0000:0000:0000:0000` a `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` nella connessione VPN.

Note

Per il routing dei dispositivi "TAP" in Windows, ad esempio, il secondo parametro di `ifconfig-ipv6` verrà utilizzato come target di route per `--route-ipv6`.

Le organizzazioni devono configurare i due parametri di `ifconfig-ipv6` in autonomia e possono utilizzare gli indirizzi in `100::/64` (da `0100:0000:0000:0000:0000:0000:0000:0000` a `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) o `fc00::/7` (da `fc00:0000:0000:0000:0000:0000:0000:0000` a `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`). `100::/64` è Blocco di indirizzi di sola lettura, mentre `fc00::/7` è Unico-Locale.

Un altro esempio:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
```

```
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

In questo esempio, la configurazione instraderà tutto il traffico IPv6 attualmente allocato alla connessione VPN.

Verifica

L'organizzazione eseguirà probabilmente i propri test. Una verifica di base consiste nell'impostare una connessione VPN completa del tunnel, quindi eseguire ping6 su un server IPv6 utilizzando l'indirizzo IPv6. L'indirizzo IPv6 del server deve essere compreso nell'intervallo specificato dal comando `route-ipv6`. Questo test ping dovrebbe fallire. Tuttavia, questo potrebbe cambiare se in futuro il supporto IPv6 verrà aggiunto al servizio Client VPN. Se il ping ha esito positivo e si è in grado di accedere a siti pubblici quando si è connessi in modalità tunnel completa, potrebbe essere necessario eseguire ulteriori operazioni di risoluzione dei problemi. Puoi anche eseguire i test utilizzando alcuni strumenti disponibili pubblicamente come ipleak.org.

Monitoraggio di AWS Client VPN

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Client VPN e delle altre soluzioni AWS. Per monitorare gli endpoint Client VPN, analizzare i modelli di traffico e risolvere i problemi relativi agli endpoint Client VPN, puoi utilizzare le seguenti caratteristiche.

Amazon CloudWatch

Monitora in tempo reale le risorse AWS e le applicazioni in esecuzione su AWS. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi impostare CloudWatch perché tenga traccia dell'uso della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la [Guida per l'utente di Amazon CloudWatch](#).

AWS CloudTrail

Acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la [Guida per l'utente AWS CloudTrail](#).

File di log Amazon CloudWatch

Consente di monitorare i tentativi di connessione all'endpoint AWS Client VPN effettuati. Puoi visualizzare i tentativi di connessione e ripristinare le connessioni Client VPN. Per i tentativi di connessione, è possibile visualizzare i tentativi di connessione riusciti e non riusciti. Puoi specificare il flusso di log CloudWatch Logs per registrare i dettagli della connessione. Per ulteriori informazioni, consulta [Registrazione delle connessioni](#) e la [Guida per l'utente di Amazon CloudWatch Logs](#).

Parametri CloudWatch per AWS Client VPN

AWS Client VPN pubblica i seguenti parametri su Amazon CloudWatch per gli endpoint Client VPN. I parametri vengono pubblicati in Amazon CloudWatch ogni cinque minuti.

Parametro	Descrizione
ActiveConnectionsCount	Numero di connessioni attive all'endpoint Client VPN. Unità: numero
AuthenticationFailures	Numero di errori di autenticazione per l'endpoint Client VPN. Unità: numero
CrlDaysToExpiry	Numero di giorni fino alla scadenza dell'elenco di revoche certificati (CRL) configurato sull'endpoint Client VPN. Unità: giorni
EgressBytes	Numero di byte inviati dall'endpoint Client VPN. Unità: byte
EgressPackets	Il numero di pacchetti inviati dall'endpoint Client VPN. Unità: numero
IngressBytes	Il numero di byte ricevuti dall'endpoint Client VPN. Unità: byte
IngressPackets	Il numero di pacchetti ricevuti dall'endpoint Client VPN. Unità: numero
SelfServicePortalClientConfigurationDownloads	Numero di download del file di configurazione dell'endpoint Client VPN dal portale self-service.

Parametro	Descrizione
	Unità: numero

AWS Client VPN pubblica i seguenti parametri di [valutazione dell'assetto](#) per gli endpoint Client VPN.

Parametro	Descrizione
ClientConnectHandlerTimeouts	Numero di timeout all'invocazione del gestore di connessioni all'endpoint Client VPN. Unità: numero
ClientConnectHandlerInvalidResponses	Numero di risposte non valide restituite dal gestore di connessioni per le connessioni all'endpoint Client VPN. Unità: numero
ClientConnectHandlerOtherExecutionErrors	Numero di errori imprevisti durante l'esecuzione del gestore di connessioni all'endpoint Client VPN. Unità: numero
ClientConnectHandlerThrottlingErrors	Numero di errori di limitazione (della larghezza di banda della rete) all'invocazione del gestore di connessioni all'endpoint Client VPN. Unità: numero
ClientConnectHandlerDeniedConnections	Numero di connessioni negate dal gestore di connessioni per le connessioni all'endpoint Client VPN. Unità: numero

Parametro	Descrizione
ClientConnectHandlerFailedServiceErrors	Numero di errori lato server durante l'esecuzione del gestore di connessioni all'endpoint Client VPN. Unità: numero

Puoi filtrare i parametri dell'endpoint Client VPN in base all'endpoint.

CloudWatch ti consente di recuperare le statistiche su quei punti di dati come set ordinato di dati di serie temporali, i cosiddetti parametri. Pensa a una metrica come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. A ogni dato sono associati una marcatura temporale e un'unità di misura facoltativa.

Puoi utilizzare le metriche per verificare che le prestazioni del sistema siano quelle previste. Ad esempio, puoi creare un allarme CloudWatch per monitorare un parametro specificato e avviare un'operazione (come l'invio di una notifica a un indirizzo e-mail) se il parametro non rientra in un intervallo che consideri accettabile.

Per ulteriori informazioni, consulta la [Guida per l'utente di Amazon CloudWatch](#).

Visualizza i parametri CloudWatch

Puoi visualizzare i parametri dell'endpoint Client VPN come segue.

Per visualizzare le metriche utilizzando la console CloudWatch

I parametri vengono raggruppati prima in base al namespace del servizio e successivamente in base alle diverse combinazioni di dimensioni all'interno di ogni namespace.

1. Aprire la console CloudWatch all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel riquadro di navigazione, selezionare Parametri.
3. In All metrics (Tutti i parametri), scegliere il namespace del parametro ClientVPN.
4. Per visualizzare i parametri, seleziona la dimensione del parametro per endpoint.

Visualizzazione dei parametri usando AWS CLI

Al prompt dei comandi, utilizza il comando seguente per elencare i parametri disponibili per il servizio di gateway NAT.

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

Log di CloudTrail per AWS Client VPN

AWS Client VPN è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, da un ruolo o da un servizio AWS in Client VPN. CloudTrail acquisisce tutte le chiamate API per Client VPN come eventi. Le chiamate acquisite includono le chiamate dalla console Client VPN e le chiamate di codice alle operazioni dell'API Client VPN. Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per Client VPN. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella console di CloudTrail in Cronologia eventi. Utilizza le informazioni raccolte da CloudTrail per determinare la richiesta effettuata a Client VPN, l'indirizzo IP da cui è stata effettuata la richiesta, il richiedente, la data della richiesta e altri dettagli.

Per ulteriori informazioni su CloudTrail, consulta la [AWS CloudTrail Guida per l'utente di](#).

Informazioni su Client VPN in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Client VPN, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta [Visualizzazione di eventi nella cronologia degli eventi di CloudTrail](#).

Per una registrazione continua degli eventi nell'account AWS, inclusi gli eventi per Client VPN, crea un trail. Un percorso abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [Servizi e integrazioni CloudTrail supportati](#)

- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di log CloudTrail da più regioni](#) e [Ricezione di file di log CloudTrail da più account](#)

Tutte le operazioni Client VPN vengono registrate da CloudTrail e sono documentate nella [Documentazione di riferimento delle API Amazon EC2](#). Ad esempio, le chiamate alle operazioni `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork` e `AuthorizeClientVpnIngress` generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Informazioni sulle voci dei file di log di Client VPN

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Per maggiori informazioni, consulta [Registrazione delle chiamate API Amazon EC2, Amazon EBS e Amazon VPC con AWS CloudTrail](#) nella Documentazione di riferimento delle API Amazon EC2.

Quote AWS Client VPN

L'account AWS dispone delle seguenti quote, precedentemente definite limiti, correlate agli endpoint Client VPN. Salvo dove diversamente specificato, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per richiedere un aumento delle quote per una quota regolabile, scegli Yes (Sì) nella colonna Adjustable. Per ulteriori informazioni, consulta [Richiesta di un aumento di quota](#) nella Guida per l'utente per Service Quotas.

Quote Client VPN

Nome	Default	Adattabile
Regole di autorizzazione per endpoint Client VPN	50	Sì
Endpoint Client VPN per Regione	5	Sì
Connessioni client simultanee per endpoint Client VPN	Questo valore dipende dal numero di associazioni sottoreti per l'endpoint. <ul style="list-style-type: none"> • 1 – 7.000 • 2 – 36.500 • 3 – 66.500 • 4 – 96.500 • 5 – 126.000 	Sì
Operazioni simultanee per endpoint Client VPN	10	No
Voci in un elenco di revoche di certificati client per gli endpoint Client VPN	20.000	No
Route per endpoint Client VPN	10	Sì

† Le operazioni includono:

- Associare oppure dissociare sottoreti
- Creare oppure eliminare route
- Creare oppure eliminare regole in ingresso e in uscita
- Creare oppure eliminare gruppi di sicurezza

Quote di utenti e gruppi

Quando si configurano utenti e gruppi per Active Directory o un IdP basato su SAML, si applicano le quote seguenti:

- Gli utenti possono appartenere a un massimo di 200 gruppi. Gli eventuali gruppi successivi vengono ignorati.
- La lunghezza massima per l'ID gruppo è di 255 caratteri.
- La lunghezza massima dell'ID nome è di 255 caratteri. I caratteri successivi vengono troncati.

Considerazioni generali

Quando usi gli endpoint Client VPN, prendi in considerazione quanto segue:

- Se si utilizza Active Directory per autenticare l'utente, l'endpoint Client VPN deve appartenere allo stesso account della risorsa AWS Directory Service utilizzata per l'autenticazione di Active Directory.
- Se si utilizza l'autenticazione federata basata su SAML per autenticare un utente, l'endpoint Client VPN deve appartenere allo stesso account del provider di identità SAML IAM creato per definire la relazione di trust tra il provider di identità e AWS. Il provider di identità SAML IAM può essere condiviso tra più endpoint Client VPN nello stesso account AWS.

Risoluzione dei problemi relativi a AWS Client VPN

Nel seguente argomento viene descritto come risolvere i problemi che si possono verificare con un endpoint Client VPN.

Per ulteriori informazioni sulla risoluzione dei problemi relativi al software basato su OpenVPN utilizzato dai client per connettersi a un Client VPN, consulta [Risoluzione dei problemi relativi alla connessione VPN client](#) nella Guida per l'utente di AWS Client VPN .

Problemi comuni

- [Impossibile risolvere il nome DNS dell'endpoint Client VPN](#)
- [Il traffico non viene suddiviso tra sottoreti](#)
- [Regole di autorizzazione per i gruppi di Active Directory non funzionano come previsto](#)
- [I client non possono accedere a un VPC in peering, ad Amazon S3 o a Internet](#)
- [Accesso intermittente a un VPC in peering, ad Amazon S3 o a Internet](#)
- [Il software client restituisce l'errore TLS](#)
- [Il software client restituisce errori di nome utente e password \(autenticazione di Active Directory\)](#)
- [Il software client restituisce gli errori relativi al nome utente e alla password \(autenticazione federata\)](#)
- [I client non sono in grado di connettersi \(autenticazione reciproca\)](#)
- [Client restituisce un errore di superamento delle dimensioni massime delle credenziali \(autenticazione federata\)](#)
- [Il client non apre il browser \(autenticazione federata\)](#)
- [Il client non restituisce un errore nessuna porta disponibile \(autenticazione federata\)](#)
- [Connessione VPN interrotta a causa della mancata corrispondenza dell'IP](#)
- [Il routing del traffico verso la LAN non funziona come previsto](#)
- [Verifica del limite di larghezza di banda per un endpoint Client VPN](#)

Impossibile risolvere il nome DNS dell'endpoint Client VPN

Problema

Impossibile risolvere il nome DNS dell'endpoint Client VPN.

Causa

Il file di configurazione dell'endpoint Client VPN include un parametro chiamato `remote-random-hostname`. Questo parametro impone al client di anteporre una stringa casuale al nome DNS per impedire il caching DNS. Alcuni client non riconoscono questo parametro e, pertanto, non antepongono la stringa casuale richiesta al nome DNS.

Soluzione

Apri il file di configurazione dell'endpoint Client VPN utilizzando l'editor di testo preferito. Individua la riga che specifica il nome DNS dell'endpoint Client VPN e anteponi una stringa casuale in modo che il formato sia *stringa_casuale.nome_DNS_visualizzato*. Ad esempio:

- Nome DNS originale: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nome DNS modificato: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Il traffico non viene suddiviso tra sottoreti

Problema

Sto cercando di suddividere il traffico di rete tra due sottoreti in modo da instradare il traffico privato attraverso una sottorete privata e il traffico Internet attraverso una sottorete pubblica. Tuttavia, pur avendo aggiunto entrambe le route alla tabella di routing dell'endpoint Client VPN, solo una viene utilizzata.

Causa

È possibile associare più sottoreti a un endpoint Client VPN, ma è consentito associare solo una sottorete per zona di disponibilità. L'associazione di più sottoreti ha lo scopo di fornire elevata disponibilità e ridondanza della zona di disponibilità per i client. Tuttavia, Client VPN non consente di suddividere in maniera selettiva il traffico tra le sottoreti associate all'endpoint del Client VPN.

I client si connettono a un endpoint del Client VPN in base all'algoritmo round-robin DNS. Ciò significa che il traffico può essere instradato attraverso una qualsiasi delle sottoreti associate quando

stabiliscono una connessione. Di conseguenza, problemi di connettività si possono verificare se i client si trovano in una sottorete associata che non dispone delle voci route richieste.

Ad esempio, si supponga di configurare le seguenti associazioni di sottorete e route:

- Associazioni di sottorete
 - Associazione 1: Sottorete-A (us-est-1a)
 - Associazione 2: Sottorete-B (us-east-1b)
- Route
 - Route 1: 10.0.0.0/16 instradata a Sottorete-A
 - Route 2: 172.31.0.0/16 instradata a Sottorete-B

In questo esempio, i client che quando si connettono si trovano sulla Sottorete-A, non possono accedere alla Route 2, mentre i client che quando si connettono si trovano sulla Sottorete-B non possono accedere alla Route 1.

Soluzione

Verificare che l'endpoint Client VPN disponga delle stesse voci route con destinazioni per ogni rete associata. Ciò garantisce che i client possano accedere a tutte le route a prescindere dalla sottorete attraverso la quale viene instradato il traffico.

Regole di autorizzazione per i gruppi di Active Directory non funzionano come previsto

Problema

Ho configurato delle regole di autorizzazione per i gruppi di Active Directory, ma il funzionamento non è quello previsto. Ho aggiunto una regola di autorizzazione per `0.0.0.0/0` per autorizzare il traffico per tutte le reti, ma il traffico ancora non va a buon fine per CIDR di destinazione specifici.

Causa

Le regole di autorizzazione sono indicizzate sui CIDR di rete. Le regole di autorizzazione devono concedere ai gruppi di Active Directory l'accesso a CIDR di rete specifici. Le regole di autorizzazione per `0.0.0.0/0` vengono gestite come un caso speciale e pertanto valutate per ultime, a prescindere dal loro ordine di creazione.

Ad esempio, si supponga di creare cinque regole di autorizzazione nel seguente ordine:

- Regola 1: accesso del gruppo 1 a 10.1.0.0/16
- Regola 2: accesso del gruppo 1 a 0.0.0.0/0
- Regola 3: accesso del gruppo 2 a 0.0.0.0/0
- Regola 4: accesso del gruppo 3 a 0.0.0.0/0
- Regola 5: accesso del gruppo 2 a 172.131.0.0/16

In questo esempio, la regola 2, la regola 3 e la regola 4 vengono valutate per ultima. Il gruppo 1 può accedere solo a 10.1.0.0/16 e il gruppo 2 può accedere solo a 172.131.0.0/16. Il gruppo 3 non può accedere a 10.1.0.0/16 o 172.131.0.0/16, ma può accedere a tutte le altre reti. Se si rimuovono le regole 1 e 5, tutti e tre i gruppi possono accedere a tutte le reti.

Durante la valutazione delle regole di autorizzazione, Client VPN utilizza la corrispondenza del prefisso più lungo. Consulta [.Priorità della route](#) nella Guida per l'utente di Amazon VPC per maggiori dettagli.

Soluzione

Verificare di creare regole di autorizzazione che concedono specificatamente ai gruppi di Active Directory l'accesso a CIDR di rete specifici. Se si aggiunge una regola di autorizzazione per 0.0.0.0/0, tenere presente che verrà valutata per ultima e che le regole di autorizzazione precedenti potrebbero limitare le reti a cui viene concesso l'accesso.

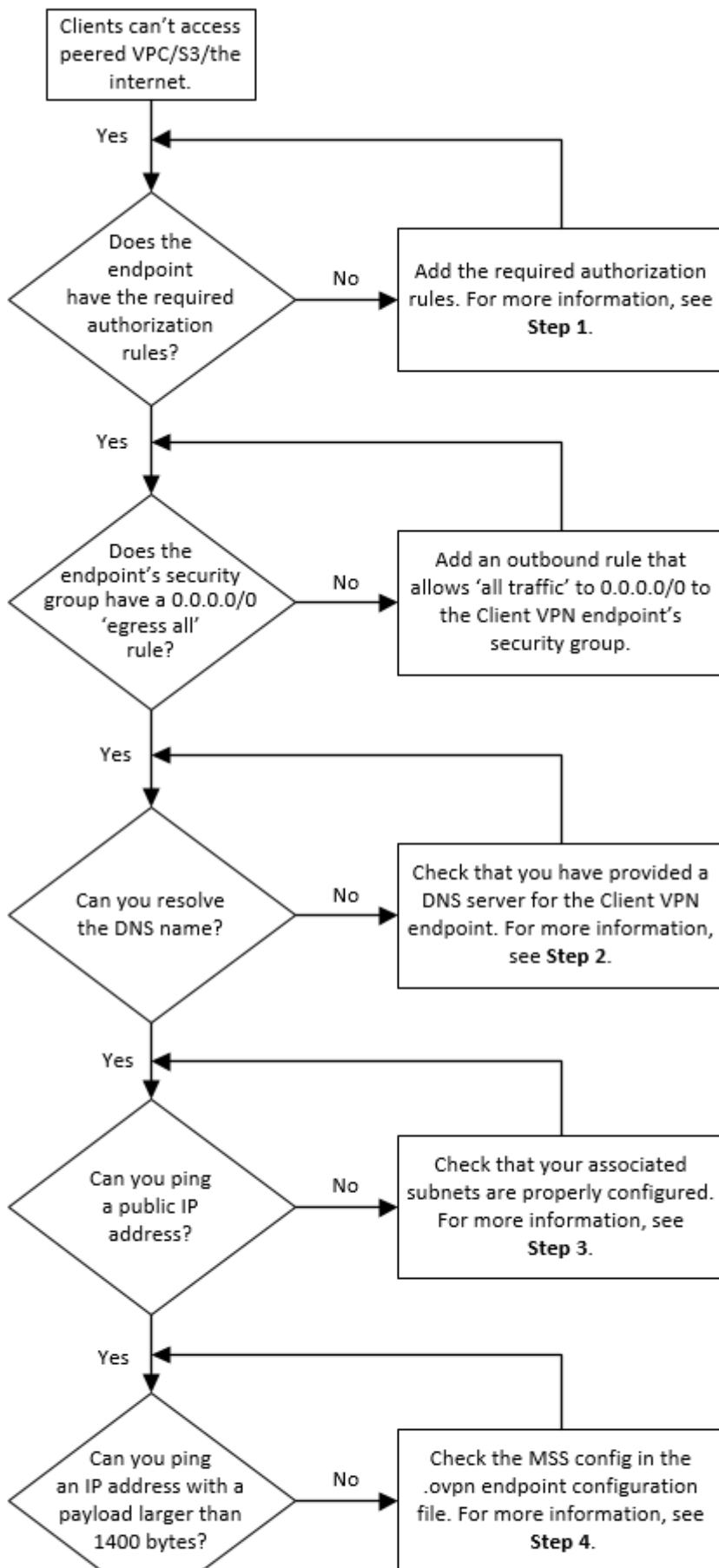
I client non possono accedere a un VPC in peering, ad Amazon S3 o a Internet

Problema

Ho configurato correttamente le route dell'endpoint Client VPN, ma i miei client non possono accedere a un VPC in peering, ad Amazon S3 o a Internet.

Soluzione

Nel seguente diagramma di flusso sono riportate le fasi per la diagnosi dei problemi di connettività Internet, VPC in peering e Amazon S3.



I client non possono accedere a un VPC in peering, ad Amazon S3 o a Internet

1. Per l'accesso a Internet, aggiungere una regola di autorizzazione per `0.0.0.0/0`.

Per l'accesso a un VPC in peering, aggiungere una regola di autorizzazione per l'intervallo CIDR IPv4 del VPC.

Per accedere a S3, specifica l'indirizzo IP dell'endpoint Amazon S3.

2. Verificare se è possibile risolvere il nome DNS.

Se non è possibile risolvere il nome DNS, verificare di aver specificato i server DNS per l'endpoint Client VPN. Se si gestisce il proprio server DNS, specificare l'indirizzo IP. Verificare che il server DNS sia accessibile dal VPC.

Se non si è certi dell'indirizzo IP da specificare per i server DNS, specificare il resolver DNS VPC all'indirizzo IP `.2` del VPC.

3. Per l'accesso a Internet, verificare se è possibile eseguire il ping di un indirizzo IP pubblico o di un sito Web pubblico, ad esempio, `amazon.com`. Se non si riceve una risposta, accertarsi che la tabella di routing per le sottoreti associate disponga di una route predefinita che si rivolge a un Internet gateway o a un gateway NAT. Se la route predefinita è attiva, verificare che la sottorete associata non disponga di regole della lista di controllo accessi di rete che bloccano il traffico in ingresso e in uscita.

Se non è possibile raggiungere un VPC in peering, verificare che la tabella di routing della sottorete associata disponga di una voce route per il VPC in peering.

Se non è possibile raggiungere Amazon S3, verificare che la tabella di routing della sottorete associata disponga di una voce route per l'endpoint VPC del gateway.

4. Verificare se è possibile eseguire il ping di un indirizzo IP pubblico con un payload superiore a 1400 byte. Utilizzare uno dei seguenti comandi:

- Windows

```
C:\> ping 8.8.8.8 -l 1480 -f
```

- Linux

```
$ ping -s 1480 8.8.8.8 -M do
```

Se non è possibile eseguire il ping di un indirizzo IP con un payload superiore a 1400 byte, apri il file di configurazione `.ovpn` dell'endpoint Client VPN utilizzando l'editor di testo preferito e aggiungi quanto segue.

```
mssfix 1328
```

Accesso intermittente a un VPC in peering, ad Amazon S3 o a Internet

Problema

Ho problemi di connettività intermittente durante la connessione a un VPC in peering, ad Amazon S3 o a Internet, ma l'accesso alle sottoreti associate non è influenzato. Per risolvere i problemi di connettività devo eseguire la disconnessione e la riconnessione.

Causa

I client si connettono a un endpoint del Client VPN in base all'algoritmo round-robin DNS. Ciò significa che il traffico può essere instradato attraverso una qualsiasi delle sottoreti associate quando stabiliscono una connessione. Di conseguenza, problemi di connettività si possono verificare se i client si trovano in una sottorete associata che non dispone delle voci route richieste.

Soluzione

Verificare che l'endpoint Client VPN disponga delle stesse voci route con destinazioni per ogni rete associata. Ciò garantisce che i client possano accedere a tutte le route a prescindere dalla sottorete associata attraverso la quale viene instradato il traffico.

Ad esempio, si supponga che l'endpoint Client VPN disponga di tre sottoreti associate (sottorete A, B e C) e che si desideri abilitare l'accesso a Internet per i client. A tale scopo, è necessario aggiungere tre route `0.0.0.0/0`, una per ogni sottorete associata:

- Route 1: `0.0.0.0/0` per sottorete A
- Route 2: `0.0.0.0/0` per sottorete B
- Route 3: `0.0.0.0/0` per sottorete C

Il software client restituisce l'errore TLS

Problema

Ero solito connettere i miei client al Client VPN, ma ora il client basato su OpenVPN restituisce uno dei seguenti errori quando tenta di connettersi:

```
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.
```

Possibile causa #1

Se si utilizza l'autenticazione reciproca e si importa un elenco di revoche di certificati del client, l'elenco di revoche di certificati del client potrebbe essere scaduto. Durante la fase di autenticazione, l'endpoint Client VPN controlla il certificato client rispetto all'elenco di revoche di certificati del client importato. Se l'elenco di revoche di certificati del client è scaduto, non è possibile connettersi all'endpoint Client VPN.

Soluzione #1

Controllare la data di scadenza dell'elenco di revoche di certificati del client utilizzando lo strumento OpenSSL.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

Nell'output vengono visualizzate la data e l'ora di scadenza. Se l'elenco di revoche di certificati del client è scaduto, è necessario crearne uno nuovo e importarlo nell'endpoint Client VPN. Per ulteriori informazioni, consulta [Elenchi di revoche di certificati client](#).

Possibile causa #2

Il certificato del server utilizzato per l'endpoint del Client VPN è scaduto.

Soluzione #2

Controlla lo stato del certificato del tuo server nella AWS Certificate Manager console o utilizzando la AWS CLI. Se il certificato del server è scaduto, crea un nuovo certificato e caricalo in ACM. Per le fasi

dettagliate per generare i certificati e le chiavi server e client utilizzando la [Utility OpenVPN easy-rsa](#) e importarli in ACM vedi [Autenticazione reciproca](#).

In alternativa, potrebbe verificarsi un problema con il software basato su OpenVPN utilizzato dal client per connettersi a Client VPN. Per ulteriori informazioni sulla risoluzione dei problemi relativi al software basato su OpenVPN, consulta [Risoluzione dei problemi relativi alla connessione Client VPN](#) nella Guida per l'utente di AWS Client VPN .

Il software client restituisce errori di nome utente e password (autenticazione di Active Directory)

Problema

Utilizzo l'autenticazione di Active Directory per il mio endpoint Client VPN ed ero in grado di connettere i miei client a Client VPN. Ora, tuttavia, i client ricevono errori di nome utente e password non validi.

Possibili cause

Se si utilizza l'autenticazione di Active Directory e se è stata abilitata l'autenticazione a più fattori dopo aver distribuito il file di configurazione del client, il file non contiene le informazioni necessarie per richiedere agli utenti di immettere il codice MFA. Agli utenti viene richiesto di immettere solo nome utente e password e l'autenticazione non va a buon fine.

Soluzione

Scaricare un nuovo file di configurazione del client e distribuirlo ai client. Verificare che il nuovo file contenga la riga seguente.

```
static-challenge "Enter MFA code " 1
```

Per ulteriori informazioni, consulta [Esportazione e configurazione del file di configurazione del client](#). Verifica la configurazione MFA per Active Directory senza utilizzare l'endpoint Client VPN per controllare che MFA funzioni come previsto.

Il software client restituisce gli errori relativi al nome utente e alla password (autenticazione federata)

Problema

Tentativo di accesso con nome utente e password con autenticazione federata e visualizzazione dell'errore «Le credenziali ricevute non erano corrette. Contatta il tuo amministratore IT».

Causa

Questo errore può essere causato dalla mancata inclusione di almeno un attributo nella risposta SAML dell'IdP.

Soluzione

Assicurati che almeno un attributo sia incluso nella risposta SAML dell'IdP. Per ulteriori informazioni, consulta [Risorse di configurazione IdP basate su SAML](#).

I client non sono in grado di connettersi (autenticazione reciproca)

Problema

Uso l'autenticazione reciproca per il mio endpoint Client VPN. I client ricevono errori di negoziazione della chiave TLS non riuscita ed errori di timeout.

Possibili cause

Il file di configurazione fornito ai client non contiene il certificato client e la chiave privata del client o il certificato e la chiave non sono corretti.

Soluzione

Accertarsi che il file di configurazione contenga il certificato client e la chiave corretti. Se necessario, correggere il file di configurazione e ridistribuirlo ai client. Per ulteriori informazioni, consulta [Esportazione e configurazione del file di configurazione del client](#).

Client restituisce un errore di superamento delle dimensioni massime delle credenziali (autenticazione federata)

Problema

Uso l'autenticazione federata per il mio endpoint Client VPN. Quando i client immettono il nome utente e la password nella finestra del browser del provider di identità (IdP) basato su SAML, viene visualizzato un errore che indica che le credenziali superano le dimensioni massime supportate.

Causa

La risposta SAML restituita dall'IdP supera le dimensioni massime supportate. Per ulteriori informazioni, consulta [Requisiti e considerazioni per l'autenticazione federata basata su SAML](#).

Soluzione

Provare a ridurre il numero di gruppi a cui l'utente appartiene nel provider di identità e provare a connettersi nuovamente.

Il client non apre il browser (autenticazione federata)

Problema

Uso l'autenticazione federata per il mio endpoint Client VPN. Quando i client tentano di connettersi all'endpoint, il software client non apre una finestra del browser e visualizza invece una finestra popup del nome utente e della password.

Causa

Il file di configurazione fornito ai client non contiene il flag `auth-federate`.

Soluzione

[Esporta il file di configurazione più recente](#), importalo nel client AWS fornito e riprova a connetterti.

Il client non restituisce un errore nessuna porta disponibile (autenticazione federata)

Problema

Uso l'autenticazione federata per il mio endpoint Client VPN. Quando i client tentano di connettersi all'endpoint, il software client restituisce il seguente errore:

```
The authentication flow could not be initiated. There are no available ports.
```

Causa

Il client AWS fornito richiede l'uso della porta TCP 35001 per completare l'autenticazione. Per ulteriori informazioni, consulta [Requisiti e considerazioni per l'autenticazione federata basata su SAML](#).

Soluzione

Verificare che il dispositivo del client non stia bloccando la porta TCP 35001 o la stia utilizzando per un processo diverso.

Connessione VPN interrotta a causa della mancata corrispondenza dell'IP

Problema

La connessione VPN è terminata e il software client restituisce il seguente errore: "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."

Causa

Il client AWS fornito richiede che l'indirizzo IP a cui è connesso corrisponda all'IP del server VPN che supporta l'endpoint Client VPN. Per ulteriori informazioni, consulta [Regole e best practice di AWS Client VPN](#).

Soluzione

Verifica che non vi sia alcun proxy DNS tra il client AWS fornito e l'endpoint Client VPN.

Il routing del traffico verso la LAN non funziona come previsto

Problema

Il tentativo di instradare il traffico verso la rete locale (LAN) non funziona come previsto quando gli intervalli di indirizzi IP LAN non rientrano nei seguenti intervalli di indirizzi IP privati standard: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, oppure 169.254.0.0/16.

Causa

Se viene rilevato che l'intervallo di indirizzi LAN del client non rientra negli intervalli standard sopra indicati, l'endpoint Client VPN invierà automaticamente la direttiva OpenVPN «redirect-gateway block-local» al client, forzando tutto il traffico LAN a entrare nella VPN. Per ulteriori informazioni, consulta [Regole e best practice di AWS Client VPN](#).

Soluzione

Se è necessario l'accesso alla LAN durante le connessioni VPN, si consiglia di utilizzare gli intervalli di indirizzi convenzionali sopra elencati per la rete LAN.

Verifica del limite di larghezza di banda per un endpoint Client VPN

Problema

Devo verificare il limite di larghezza di banda per un endpoint Client VPN.

Causa

Il throughput dipende da diversi fattori, ad esempio la capacità della connessione dalla posizione e la latenza di rete tra l'applicazione desktop Client VPN sul computer e l'endpoint VPC. Esiste anche un limite di larghezza di banda di 10 Mbps per connessione utente.

Soluzione

Eseguire i seguenti comandi per verificare la larghezza di banda.

```
sudo iperf3 -s -V
```

Sul client:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Cronologia dei documenti per la Guida per l'utente di Client VPN

Nella tabella seguente sono descritti gli aggiornamenti della Guida per l'amministratore di AWS Client VPN.

Modifica	Descrizione	Data
Esempi di regole di autorizzazione	Aggiunta di scenari di esempio per le regole di autorizzazione.	15 settembre 2022
Durata massima della sessione VPN	Puoi configurare una durata massima della sessione VPN più breve per soddisfare i requisiti di sicurezza e conformità.	20 gennaio 2022
Banner di accesso del client	Puoi abilitare un banner di testo su applicazioni desktop Client VPN fornite da AWS quando viene stabilita una sessione VPN per soddisfare le esigenze normative e di conformità.	20 gennaio 2022
Handler di connessioni client	Puoi abilitare l'handler di connessioni client per l'endpoint Client VPN per eseguire una logica personalizzata che autorizza nuove connessioni.	4 novembre 2020
Portale self-service	Puoi abilitare un portale self-service nell'endpoint Client VPN per i tuoi client.	29 ottobre 2020

Accesso da client a client	Puoi consentire ai client che si connettono a un endpoint Client VPN di connettersi tra loro.	29 settembre 2020
Autenticazione federata basata su SAML 2.0	Puoi autenticare gli utenti Client VPN utilizzando l'autenticazione federata basata su SAML 2.0.	19 maggio 2020
Specifica dei gruppi di sicurezza durante la creazione	Durante la creazione dell'endpoint AWS Client VPN puoi specificare un VPC e gruppi di sicurezza.	5 marzo 2020
Porte VPN configurabili	Puoi specificare un numero di porta VPN supportato per l'endpoint AWS Client VPN.	16 gennaio 2020
Supporto per autenticazione a più fattori	L'endpoint AWS Client VPN supporta l'autenticazione MFA se è abilitata per Active Directory.	30 settembre 2019
Supporto per split-tunnel	Puoi abilitare lo split-tunnel sull'endpoint AWS Client VPN.	24 luglio 2019
Versione iniziale	Questo rilascio introduce AWS Client VPN.	18 dicembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.