Guida per l'amministratore

AWS Client VPN

AWS Client VPN: Guida per l'amministratore

Table of Contents

Che cos'è AWS Client VPN? 1
Caratteristiche di Client VPN 1
Componenti di Client VPN 2
Utilizzo di Client VPN 4
Prezzi per Client VPN 5
Regole e migliori pratiche 6
Requisiti di rete e larghezza di banda 6
Configurazione di sottoreti e VPC 7
Autenticazione e sicurezza 8
Requisiti di connessione e DNS 8
Limitazioni e restrizioni 9
Come funziona Client VPN 10
Scenari ed esempi 11
Autenticazione client 23
Autenticazione Active Directory 24
Autenticazione reciproca 24
Single Sign-On (autenticazione federata basata su SAML 2.0) 30
Autorizzazione client 36
Gruppi di sicurezza 36
Autorizzazione di rete 37
Creare una regola per il gruppo di sicurezza degli endpoint 37
Autorizzazione di connessione 38
Requisiti e considerazioni 38
Interfaccia Lambda 39
Utilizza il gestore client connect per la valutazione della postura 41
Abilita il gestore della connessione del client 42
Ruolo collegato ai servizi 42
Monitora gli errori di autorizzazione della connessione 42
Split-tunnel di Client VPN 43
Vantaggi dello split-tunnel 43
Considerazioni sul routing 44
Abilitare lo split-tunnel 44
Registrazione delle connessioni 44
Voci di log del registro di connessione 45

Considerazioni sul dimensionamento 47
Inizia a usare Client VPN 49
Prerequisiti 50
Fase 1: Generare i certificati e le chiavi server e client 50
Fase 2: Creare un endpoint Client VPN 50
Fase 3: Associazione di una rete target 52
Fase 4: Aggiungere una regola di autorizzazione per il VPC 52
Fase 5: Fornire l'accesso a Internet. 53
Fase 6: Verificare i requisiti del gruppo di sicurezza 54
Fase 7: Scaricare il file di configurazione dell'endpoint Client VPN 54
Fase 8: Connettersi all'endpoint Client VPN 55
Utilizzo di Client VPN 56
accesso self-service al portale 57
Regole di autorizzazione 58
Punti chiave 58
Scenari di esempio 59
Aggiungi una regola di autorizzazione 71
Rimuovere una regola di autorizzazione 72
Visualizzazione delle regole di autorizzazione 73
Elenchi di revoche di certificati client 73
Generazione di un elenco di revoche di certificati client 74
Importazione di un elenco di revoche di certificati client 76
Esportazione di un elenco di revoche di certificati client 76
Connessioni client 77
Visualizzazione delle connessioni client 77
Terminazione di una connessione client 78
banner per il login del cliente 78
Creazione di banner 79
Configura un banner di accesso client per un endpoint esistente 79
Disattiva un banner di accesso client per un endpoint 80
Modifica il testo del banner esistente 80
Visualizza un banner di accesso attualmente configurato 81
Applicazione del percorso del cliente 81
Requisiti 82
Conflitti di routing 82
Considerazioni 83

Attiva Client Route Enforcement 84
Disattiva Client Route Enforcement 85
Risolvi i problemi relativi IPv6 al Client Route Enforcement 85
Endpoints 86
Requisiti per la creazione di endpoint Client VPN 87
Tipi di indirizzi IP 87
Modifica dell'endpoint 88
Creare un endpoint 90
Visualizzazione degli endpoint 95
Modificare un endpoint 95
Eliminazione di un endpoint. 98
Log delle connessioni 99
Abilitazione della registrazione delle connessioni per un nuovo endpoint 100
Abilitare la registrazione delle connessioni per un endpoint esistente 101
Visualizzare i log delle connessioni. 101
Disattivazione della registrazione della connessione 102
esportazione del file di configurazione del client 103
Esportazione del file di configurazione del client 104
Aggiungi il certificato client e le informazioni chiave per l'autenticazione reciproca 104
Route 105
Considerazioni sull'utilizzo dello split-tunnel sugli endpoint Client VPN 106
Creazione di una route dell'endpoint 106
Visualizzazione delle route dell'endpoint 107
Eliminazione di una route dell'endpoint 108
Reti target 108
Requisiti per la creazione di una rete di destinazione 108
Associa una rete di destinazione a un endpoint 110
Applicazione di un gruppo di sicurezza a una rete target 110
Visualizzazione delle reti target 111
Dissocia una rete di destinazione da un endpoint 111
durata massima della sessione VPN 112
Configura la sessione VPN massima durante la creazione di un endpoint 113
Visualizzare la durata massima della sessione VPN corrente 113
Modifica la durata massima della sessione VPN 114
Sicurezza 115
Protezione dei dati 116

Crittografia in transito 117
Riservatezza del traffico Internet 117
Gestione dell'identità e degli accessi 117
Destinatari 118
Autenticazione con identità 119
Gestione dell'accesso con policy 122
Come AWS Client VPN funziona con IAM 125
Esempi di policy basate su identità 131
Risoluzione dei problemi 134
Uso di ruoli collegati ai servizi 136
Resilienza 139
Più reti di destinazione per un'elevata disponibilità 140
Sicurezza dell'infrastruttura 140
Best practice 140
IPv6 considerazioni 141
IPv6 Componenti chiave del supporto 141
IPv6 assegnazione CIDR del client 142
Requisiti di compatibilità 142
Supporto DNS 142
Limitazioni 143
Client Routes Enforcement per IPv6 143
IPv6 prevenzione delle fughe (informazioni precedenti) 143
Monitoraggio di Client VPN 146
CloudWatch metriche 147
Visualizza le metriche CloudWatch 149
Quote 151
Quote Client VPN 151
Quote di utenti e gruppi 152
Considerazioni generali 152
Risoluzione dei problemi 154
Impossibile risolvere il nome DNS dell'endpoint Client VPN 155
Il traffico non viene suddiviso tra sottoreti 155
Regole di autorizzazione per i gruppi di Active Directory non funzionano come previsto 157
I client non possono accedere a un VPC in peering, ad Amazon S3 o a Internet 158
Accesso intermittente a un VPC in peering, ad Amazon S3 o a Internet 161
Il software client restituisce l'errore TLS 162

Il software client restituisce errori relativi al nome utente e alla password: autenticazione Active Directory 163
Il software client restituisce errori relativi al nome utente e alla password: autenticazione federata 164
I client non possono connettersi: autenticazione reciproca 164
Il client restituisce un errore di dimensione superiore alla dimensione massima delle credenziali: autenticazione federata 165
Il client non apre il browser: autenticazione federata 165
Il client non restituisce nessuna porta disponibile, errore: autenticazione federata 166
Connessione VPN interrotta a causa della mancata corrispondenza dell'IP 166
Il routing del traffico verso la LAN non funziona come previsto 167
Verifica il limite di larghezza di banda per un endpoint 167
Connettività tramite tunnel Client VPN 168
Prerequisiti di connettività di rete 168
Verifica lo stato dell'endpoint Client VPN 169
Verifica le connessioni dei client 169
Verifica l'autenticazione del client 170
Controlla le regole di autorizzazione 170
Convalida i percorsi Client VPN 170
Verifica i gruppi di sicurezza e la rete ACLs 171
Verifica la connettività del client 171
Diagnostica il dispositivo client 172
Risoluzione dei problemi relativi alla risoluzione DNS 172
Risolvi i problemi relativi alle prestazioni 173
Monitora le metriche di Client VPN 173
Controlla i log di Client VPN 174
Problemi e soluzioni comuni 174
Cronologia dei documenti 176
..... clxxix

Che cos'è AWS Client VPN?

AWS Client VPN è un servizio VPN gestito basato su client che consente di accedere in modo sicuro alle AWS risorse e alle risorse della rete locale. Con Client VPN, puoi accedere alle risorse da qualsiasi luogo tramite un client VPN basato su OpenVPN.

Argomenti

- Caratteristiche di Client VPN
- Componenti di Client VPN
- Utilizzo di Client VPN
- Prezzi per Client VPN
- Regole e best practice per l'utilizzo AWS Client VPN

Caratteristiche di Client VPN

Client VPN offre le seguenti caratteristiche e funzionalità:

- Connessioni sicure: stabilisce connessioni TLS crittografate da qualsiasi posizione tramite il client OpenVPN, garantendo la privacy e l'integrità dei dati.
- Servizio gestito: elimina l'onere operativo della distribuzione e della manutenzione di soluzioni VPN di accesso remoto di terze parti attraverso la gestione completa di AWS.
- Disponibilità ed elasticità elevate: scalabilità dinamica per soddisfare un numero variabile di utenti che si connettono alle tue risorse AWS e locali senza intervento manuale.
- Autenticazione: supporta diversi metodi di autenticazione tra cui l'integrazione con Active Directory, l'autenticazione federata e l'autenticazione basata su certificati per una gestione flessibile delle identità.
- Controllo granulare: implementa controlli di sicurezza precisi tramite regole di accesso basate sulla rete configurabili a livello di gruppo Active Directory e controllo degli accessi basato sui gruppi di sicurezza.
- Facilità d'uso: fornisce un accesso unificato alle risorse AWS e locali tramite un unico tunnel VPN, semplificando l'esperienza dell'utente finale.

- Gestibilità: offre una visibilità completa attraverso registri di connessione dettagliati e funzionalità di gestione in tempo reale, inclusa la possibilità di monitorare e interrompere le connessioni client attive quando necessario.
- Integrazione profonda: si integra perfettamente con i servizi AWS esistenti, tra cui AWS Directory Service Amazon VPC, migliorando le capacità di connettività dell'infrastruttura cloud.
- IPv6 supporto: consente la IPv6 connettività completa per gli endpoint Client VPN, supportando le connessioni alle IPv6 risorse dell'utente VPCs e dei client sulle IPv6 reti per i requisiti di rete moderni.

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. Per IPv4 il traffico, scegli l'intervallo CIDR del client, ad esempio. `10.2.0.0/16` Per il IPv6 traffico, assegna AWS Client VPN automaticamente l'intervallo CIDR del client.

Porte Client VPN

AWS Client VPN supporta le porte 443 e 1194 sia per TCP che 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. Per il IPv4 traffico, viene applicata la traduzione degli indirizzi di rete di origine (SNAT), in cui l'indirizzo IP di origine dell'intervallo CIDR del client viene tradotto nell'indirizzo IP dell'interfaccia di rete Client VPN. Per IPv6 il traffico, SNAT non viene applicato, garantendo una maggiore visibilità sull'indirizzo IP dell'utente connesso.

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).

Tipo di indirizzo IP dell'endpoint

Il tipo di indirizzo IP per l'endpoint Client VPN, che può essere IPv4 IPv6, o dual-stack (entrambi e). IPv4 IPv6

Tipo di indirizzo IP del traffico

Il tipo di indirizzo IP per il traffico che fluisce attraverso l'endpoint Client VPN, che può essere IPv4 IPv6, o dual-stack (entrambi e). IPv4 IPv6 Ciò determina il tipo di traffico interno (il payload effettivo o il traffico originale trasmesso tramite la connessione VPN), gli intervalli CIDR del client, l'associazione di sottoreti, i percorsi e le regole per endpoint.

Utilizzo di Client VPN

Puoi utilizzare Client VPN in uno dei modi seguenti:

Console di gestione AWS

La console Amazon VPC fornisce un'interfaccia utente basata sul Web per Client VPN. Se ti sei registrato a Account AWS, puoi accedere alla console Amazon VPC e selezionare Client VPN nel pannello di navigazione.

AWS Command Line Interface (AWS CLI)

AWS CLI Fornisce l'accesso diretto al pubblico Client VPN APIs. ed è supportata su Windows, macOS e Linux. Per ulteriori informazioni su come iniziare a usare AWS CLI, consulta la Guida AWS Command Line Interface per l'utente. Per ulteriori informazioni sui comandi per Client VPN, consulta la EC2 sezione di Amazon EC2 Command Line Reference.

AWS Tools for Windows PowerShell

AWS fornisce comandi per un'ampia gamma di AWS offerte per coloro che utilizzano script nell'PowerShell ambiente. 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 Client VPN HTTPS Query ti offre l'accesso programmatico 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. Non sono previsti costi aggiuntivi per l'utilizzo IPv6 degli endpoint dual-stack; vengono addebitati alla stessa tariffa degli endpoint. IPv4 Per ulteriori informazioni, consultare Prezzi di AWS Client VPN.

Ti viene addebitato il costo del trasferimento dei dati da Amazon EC2 a Internet. Per ulteriori informazioni, consulta Data Transfer on the Amazon EC2 On-Demand Pricing.

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, consultare 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 Client VPN (). ENIs Questi indirizzi IP elastici vengono addebitati come indirizzi pubblici in uso. IPv4 Per ulteriori informazioni, consulta la scheda IPv4 Indirizzo pubblico nella pagina dei prezzi VPC.

> **Note**
>
> Gli endpoint Client VPN richiedono indirizzi IP elastici se associati a una sottorete VPC dotata di un Internet Gateway perché consentono la connettività Internet diretta per EIPs i client VPN. Quando si connettono tramite un endpoint Client VPN, hanno bisogno di un indirizzo IP pubblico per comunicare con le risorse Internet. Elastic IPs serve a questo scopo fornendo un endpoint coerente e rivolto al pubblico. Questi EIPs sono collegati alle interfacce di rete elastiche Client VPN (ENIs) e sono essenziali per mantenere un accesso a Internet stabile e sicuro per i client VPN, garantendo al contempo il corretto routing del traffico. Poiché questi indirizzi IP elastici vengono assegnati e utilizzati attivamente per il servizio Client VPN, li AWS

addebita come IPv4 indirizzi pubblici in uso, seguendo il loro modello di prezzo standard per gli indirizzi allocati e associati. EIPs

Regole e best practice per l'utilizzo AWS Client VPN

Le seguenti sezioni descrivono le regole e le migliori pratiche per l'utilizzo AWS Client VPN:

Argomenti

- Requisiti di rete e larghezza di banda
- Configurazione di sottoreti e VPC
- Autenticazione e sicurezza
- Requisiti di connessione e DNS
- Limitazioni e restrizioni

Requisiti di rete e larghezza di banda

- AWS Client VPN è un servizio completamente gestito che si ridimensiona automaticamente per soddisfare ulteriori connessioni utente e requisiti di larghezza di banda. Ogni connessione utente ha una larghezza di banda di base massima di 50 Mbps.

  La larghezza di banda effettiva che si verifica durante la connessione tramite un endpoint Client VPN può variare in base a diversi fattori. Questi fattori includono la dimensione dei pacchetti, la composizione del traffico (mix TCP/UDP), le politiche di rete (configurazione o limitazione) sulle reti intermedie, le condizioni di Internet, i requisiti specifici delle applicazioni e il numero totale di connessioni utente simultanee. Se stai raggiungendo il limite massimo di larghezza di banda, puoi richiedere un aumento tramite AWS Support.
- 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.
- Client VPN supporta IPv4 IPv6 il traffico dual-stack (IPv4 sia IPv6 che). Per ulteriori dettagli sull' IPv6 assistenza, consulta. IPv6 considerazioni per AWS Client VPN
- • L'indirizzo IP di origine viene tradotto nell'indirizzo IP dell'endpoint Client VPN.
  - Il numero di porta di origine originale del client rimane invariato.
- Client VPN esegue Port Address Translation (PAT) solo quando utenti simultanei si connettono alla stessa destinazione. La traduzione delle porte è automatica e necessaria per supportare più connessioni simultanee attraverso lo stesso endpoint VPN.
  - Per la traduzione dell'IP di origine, l'indirizzo IP di origine viene tradotto nell'indirizzo IP del Client VPN.
  - Per la traduzione della porta di origine per le connessioni con un singolo client, il numero di porta di origine originale potrebbe rimanere invariato.
  - Per la traduzione della porta di origine per più client che si connettono alla stessa destinazione (stessa porta e indirizzo IP di destinazione), Client VPN esegue la traduzione delle porte per garantire connessioni uniche.

  Ad esempio, quando due client, il client 1 e il client 2, si connettono allo stesso server e porta di destinazione tramite un endpoint Client VPN:
  - La porta originale per il client 1, ad esempio`9999`, potrebbe essere tradotta in una porta diversa, ad esempio porta`4306`.
  - La porta originale per il client 2, ad esempio`9999`, potrebbe essere tradotta in una porta unica diversa dal client 1, ad esempio porta`63922`.
- Per quanto riguarda il IPv6 traffico, Client VPN non esegue Network Address Translation (NAT). Ciò fornisce una maggiore visibilità dell' IPv6 indirizzo dell'utente connesso.

Configurazione di sottoreti e VPC

- 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.
- Per il traffico dual-stack, le sottoreti associate devono avere intervalli IPv6 CIDR dual-stack. IPv6
- Per gli endpoint dual-stack, non è possibile associare più di una sottorete per zona di disponibilità.

Autenticazione e sicurezza

- Il portale self-service non è disponibile per i client che eseguono l'autenticazione reciproca.
- 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
```

- I certificati utilizzati in AWS Client VPN devono rispettare lo standard RFC 5280: certificato dell'infrastruttura a chiave pubblica Internet X.509 e profilo CRL (Certificate Revocation List), incluse le estensioni di certificato specificate nella sezione 4.2 del memo.
- I nomi utente con caratteri speciali potrebbero causare errori di connessione.

Requisiti di connessione e DNS

- 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.
- 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 utilizzando i client forniti di recente. AWS Questa regola è stata aggiunta per mitigare un attacco IP al server come descritto qui:. TunnelCrack
- È possibile utilizzare un client AWS fornito per connettersi a più sessioni DNS simultanee. Tuttavia, affinché la risoluzione dei nomi funzioni correttamente, i server DNS di tutte le connessioni devono avere record sincronizzati.
- 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`172.16.0.0/12,,192.168.0.0/16, o169.254.0.0/16. 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

- In Windows, quando viene utilizzato un endpoint a tunnel completo, tutto il traffico DNS viene forzato a passare attraverso il tunnel, indipendentemente dal tipo di indirizzo IP dell'endpoint (IPv4 IPv6o dual stack). Affinché il DNS funzioni, un server DNS deve essere configurato e raggiungibile all'interno del tunnel.

Limitazioni e restrizioni

- 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 AWS Managed Microsoft AD risorsa.
- Non è possibile stabilire una connessione VPN da un computer se ci sono più utenti connessi al sistema operativo.
- Client-to-client la comunicazione non è supportata per IPv6 i client. Se un IPv6 client tenta di comunicare con un altro IPv6 client, il traffico verrà interrotto.
- IPv6 e gli endpoint dual-stack richiedono che i dispositivi utente e i provider di servizi Internet (ISPs) supportino la configurazione IP corrispondente.

Come AWS Client VPN funziona

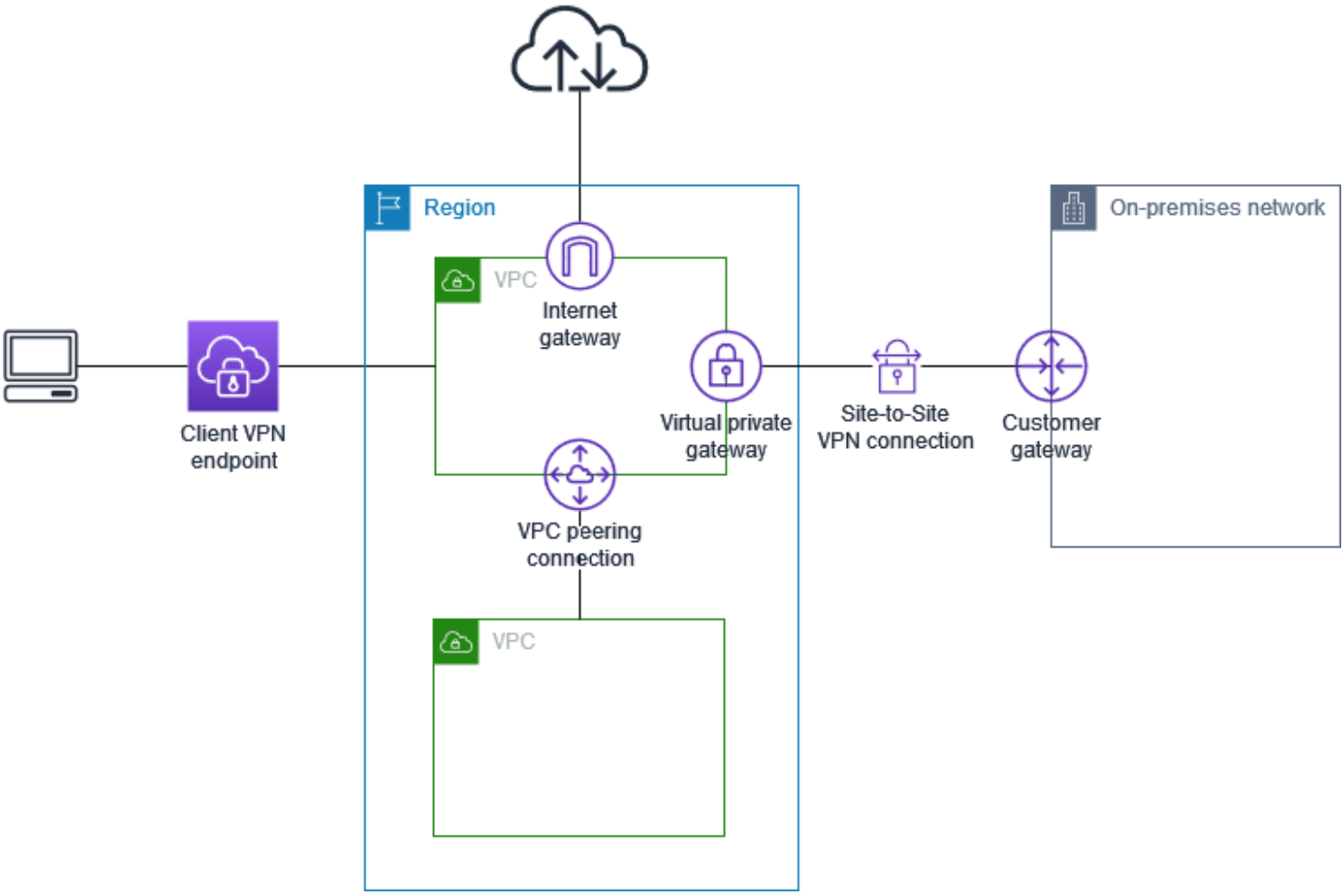
Con AWS Client VPN, esistono due tipi di utenti che interagiscono con l'endpoint Client VPN: amministratori e client.

Client VPN supporta IPv4 e IPv6 connettività dual-stack (entrambi IPv4 e IPv6). Puoi creare endpoint che utilizzano IPv4, o entrambi IPv6, che ti consentono di connetterti alle IPv6 risorse del tuo computer VPCs o di connetterti da client in rete. IPv6 Questa flessibilità aiuta le organizzazioni che hanno già implementato o stanno passando all' IPv6 infrastruttura.

L'amministratore è responsabile dell'impostazione e della configurazione del servizio. Ciò comporta la creazione dell'endpoint Client VPN, l'associazione della rete di destinazione, la configurazione delle regole di autorizzazione e l'impostazione di percorsi aggiuntivi (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 Inizia con 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. Possono anche accedere ad altre risorse in AWS una rete locale o ad 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 la Guida introduttiva nella Guida per l'AWS Client VPN utente.

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



Scenari ed esempi per Client VPN

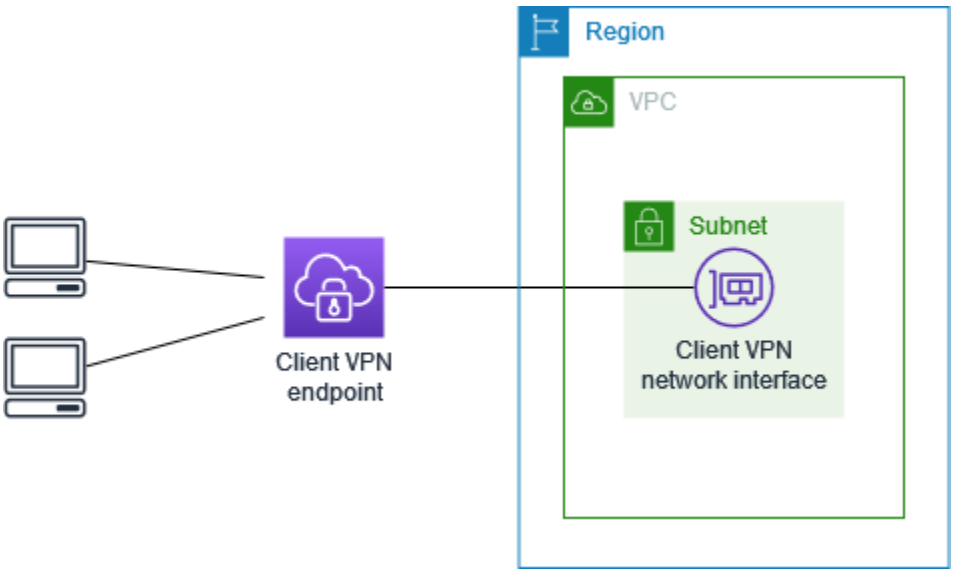
AWS Client VPN è una soluzione VPN di accesso remoto completamente gestita che viene utilizzata per consentire ai client l'accesso sicuro alle risorse sia AWS all'interno della rete locale che a quella locale. Esistono diverse opzioni per la configurazione dell'accesso. In questa sezione vengono forniti gli esempi per la creazione e la configurazione dell'accesso Client VPN per i client.

Scenari

- the section called “Accesso a un VPC”
- the section called “Accesso a un VPC con peering”
- the section called “Accesso a una rete on-premise”
- the section called “Accesso a Internet”
- the section called “lient-to-clientaccesso C”
- the section called “Limitare l'accesso a un VPC in peering”

Accesso a un VPC utilizzando Client VPN

La AWS Client VPN configurazione per questo scenario include un singolo VPC di destinazione. 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 da associare all'endpoint Client VPN e annota IPv4 i relativi intervalli CIDR.
- 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 per l'utilizzo AWS Client VPN.

Per implementare questa configurazione

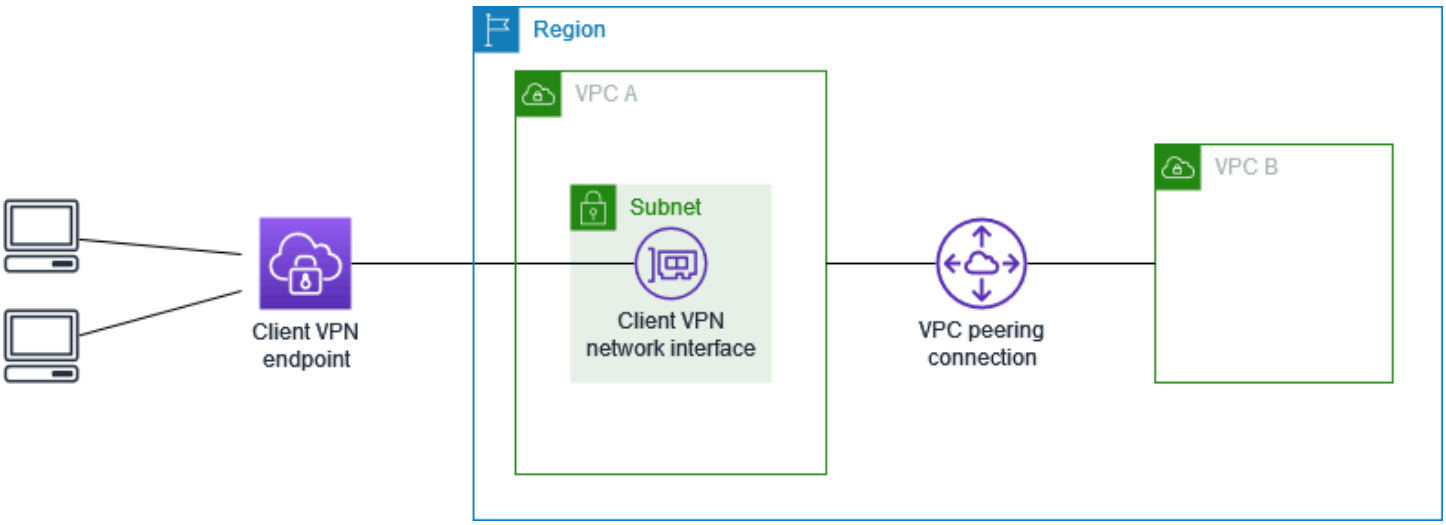
1. Crea un endpoint Client VPN nella stessa regione del VPC. Per eseguire questa operazione, attieniti alla procedura descritta in Creare un AWS Client VPN endpoint.
2. Associa la sottorete all'endpoint Client VPN. Per eseguire questa operazione, attieniti alla procedura descritta in Associare una rete di destinazione a un AWS Client VPN endpoint 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 fare ciò, esegui i passaggi descritti in Aggiungi una regola di autorizzazione e per Rete di destinazione, inserisci l'intervallo IPv4 CIDR 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 Client VPN

La AWS Client VPN configurazione per questo scenario include un VPC di destinazione (VPC A) peerizzato con un VPC aggiuntivo (VPC B). Consigliamo questa configurazione se è necessario consentire ai client l'accesso alle risorse all'interno di un VPC di destinazione e ad altre risorse VPCs che lo utilizzano in peering (come VPC B).

> **Note**
>
> La procedura per consentire l'accesso a un VPC peered (delineata seguendo lo schema di rete) è richiesta 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 da associare all'endpoint Client VPN e annota IPv4 i relativi intervalli CIDR.
- Identificare un intervallo CIDR adatto per gli indirizzi IP client che non si sovrappongono al CIDR VPC.

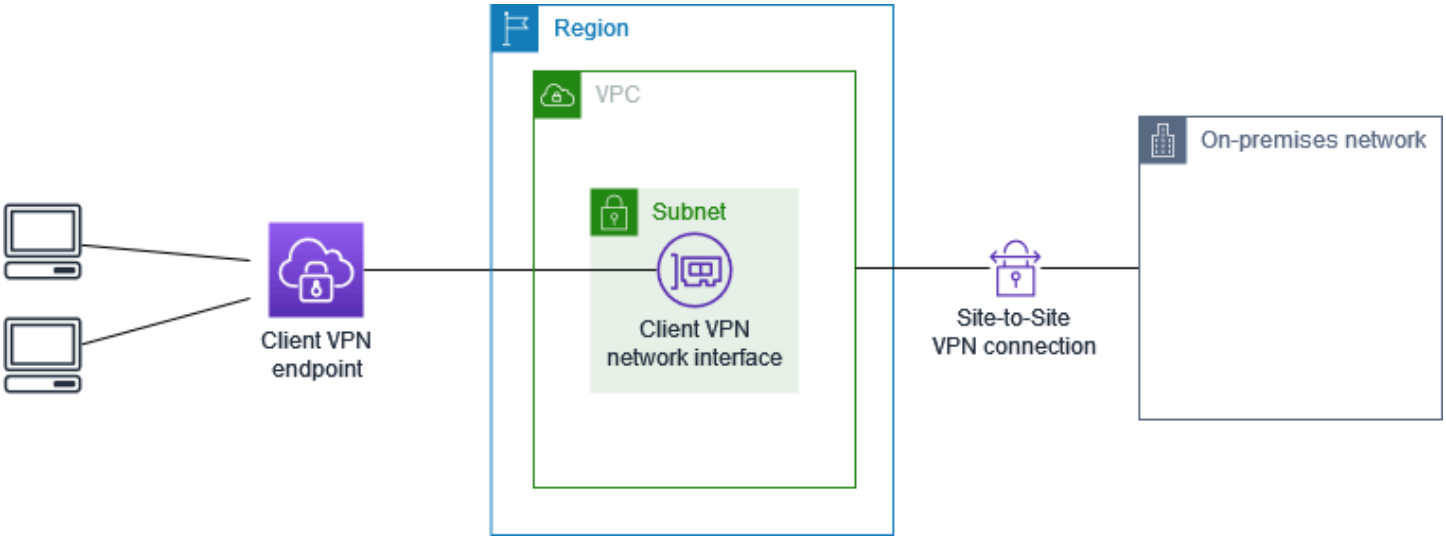
- Esamina le regole e le limitazioni per gli endpoint Client VPN in Regole e best practice per l'utilizzo AWS Client VPN.

Per implementare questa configurazione

1. Stabilire la connessione peering VPC tra. VPCs 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 AWS Client VPN endpoint.
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 AWS Client VPN endpoint 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 Aggiungi una regola di autorizzazione. Per abilitare la rete di destinazione, inserisci l'intervallo IPv4 CIDR 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 inCrea un percorso AWS Client VPN endpoint. Per Route destination, inserisci l'intervallo IPv4 CIDR del VPC peered. 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 Aggiungi una regola di autorizzazione. Per Rete di destinazione, inserisci l'intervallo IPv4 CIDR del VPC peerizzato.
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 Client VPN

La AWS Client VPN configurazione per questo scenario include solo 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 da associare all'endpoint Client VPN e annota IPv4 i relativi intervalli CIDR.
- 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 per l'utilizzo AWS Client VPN.

Per implementare questa configurazione

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

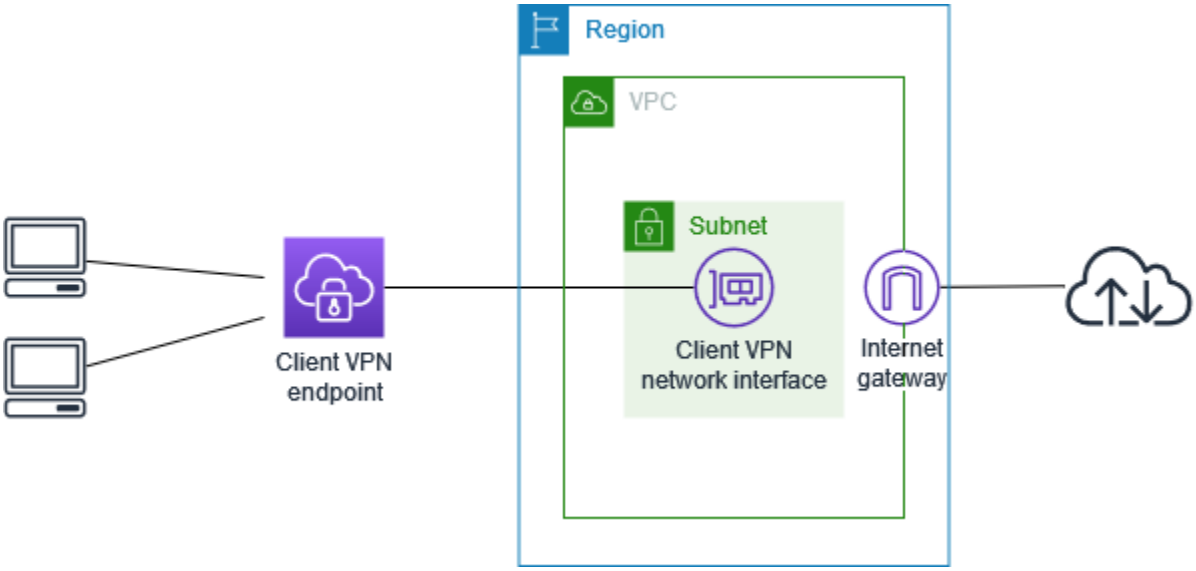
> **Note**
>
> In alternativa, puoi implementare questo scenario utilizzando una Direct Connect connessione tra il tuo VPC e la tua rete locale. Per ulteriori informazioni, consulta la Direct Connect Guida per l'utente di .

2. Prova la connessione AWS Site-to-Site VPN che hai creato nel passaggio precedente. A tale scopo, esegui i passaggi descritti nella sezione Test della connessione Site-to-Site VPN nella Guida per l'AWS Site-to-Site VPN utente. 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 AWS Client VPN endpoint.
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 AWS Client VPN endpoint e seleziona il VPC e la sottorete.
5. Aggiungi un percorso che consenta l'accesso alla connessione AWS Site-to-Site VPN. Per fare ciò, esegui i passaggi descritti inCrea un percorso AWS Client VPN endpoint; per Route destination, inserisci l'intervallo IPv4 CIDR della connessione AWS Site-to-Site VPN e per Target VPC Subnet ID, seleziona la sottorete associata all'endpoint Client VPN.
6. Aggiungi una regola di autorizzazione per consentire ai client di accedere alla connessione VPN. AWS Site-to-Site Per fare ciò, esegui i passaggi descritti inAggiungere una regola di autorizzazione a un AWS Client VPN endpoint; per Rete di destinazione, inserisci l'intervallo IPv4 CIDR della connessione AWS Site-to-Site VPN.

Accesso a Internet utilizzando Client VPN

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

Se hai completato il tutorial Inizia con 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 da associare all'endpoint Client VPN e annota IPv4 i relativi intervalli CIDR.
- 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 per l'utilizzo AWS Client VPN.

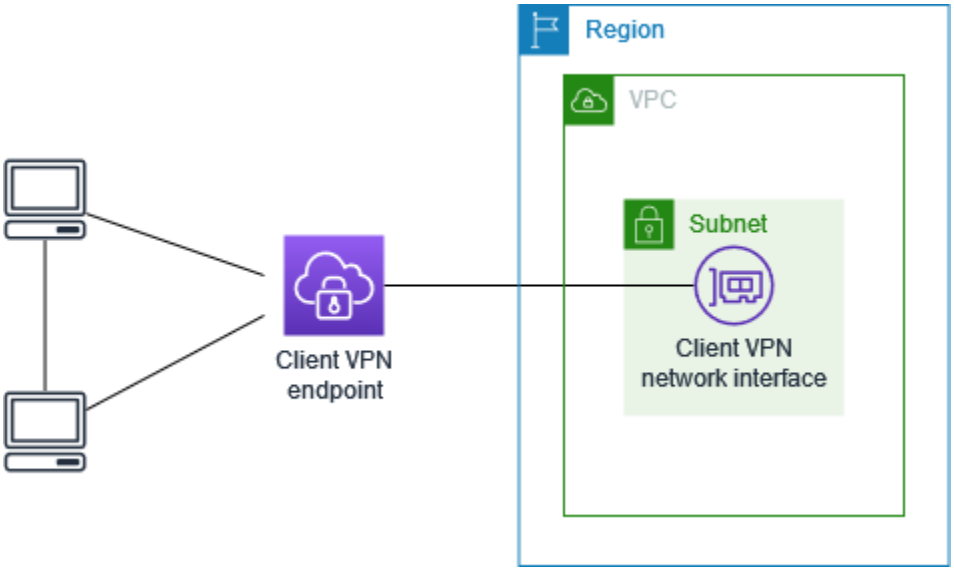
Per implementare questa configurazione

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 AWS Client VPN endpoint.

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 AWS Client VPN endpoint e seleziona il VPC e la sottorete.
6. Aggiungere una regola di autorizzazione per concedere ai client l'accesso al VPC. Per fare ciò, esegui i passaggi descritti inAggiungi una regola di autorizzazione; e per abilitare la rete di destinazione, inserisci l'intervallo IPv4 CIDR del VPC.
7. Aggiungere una route che consenta il traffico verso Internet. Per eseguire questa operazione attieniti alla procedura descritta in Crea un percorso AWS Client VPN 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 Aggiungi una regola di autorizzazione. 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.

Client-to-client accesso tramite Client VPN

La AWS Client VPN configurazione per 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 da associare all'endpoint Client VPN e annota IPv4 i relativi intervalli CIDR.
- 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 per l'utilizzo 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 AWS Client VPN endpoint.
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 AWS Client VPN endpoint 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 Crea un percorso AWS Client VPN 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 Aggiungi una regola di autorizzazione. Per abilitare la rete di destinazione, inserisci l'intervallo IPv4 CIDR 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 Aggiungi una regola di autorizzazione. Per abilitare la rete di destinazione, immettere l'intervallo CIDR del client.

Limitazione dell'accesso alla propria rete utilizzando Client VPN

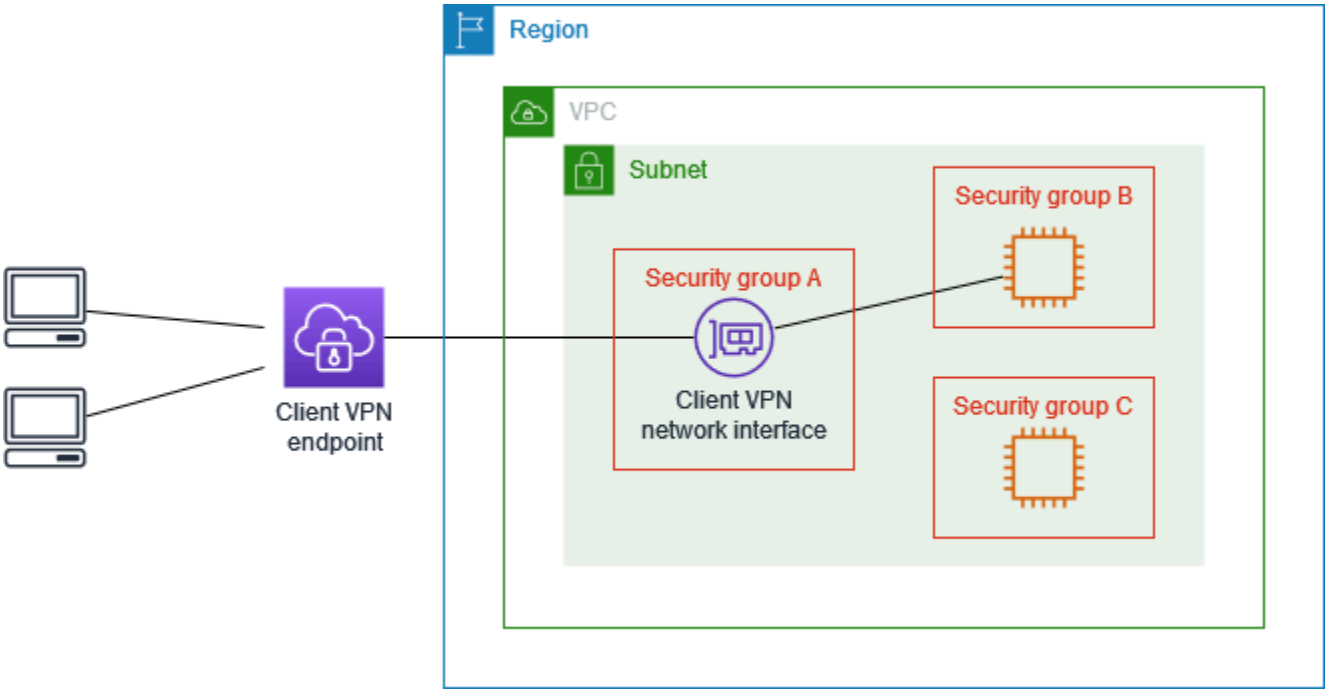
Puoi configurare l' AWS Client VPN endpoint per limitare l'accesso a risorse specifiche nel tuo VPC. Per l'autenticazione basata sull'utente puoi anche limitare l'accesso a parti della rete, in base al gruppo di utenti che accede all'endpoint Client VPN.

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 i Accesso a un VPC utilizzando 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 Client VPN, il gruppo di sicurezza B è associato a un' EC2 istanza e il gruppo di sicurezza C è associato a un' EC2 istanza. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello 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. Configura utenti e gruppi nel Directory Service tuo IdP. Per ulteriori informazioni, consulta i seguenti argomenti:
   - Autenticazione Active Directory in Client VPN
   - 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 AWS Client VPN 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 in AWS Client VPN.
2. Crea un endpoint Client VPN. Per ulteriori informazioni, consulta Creare un AWS Client VPN endpoint.

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 Aggiungi una regola di autorizzazione.

Autenticazione client in AWS Client VPN

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)

Puoi utilizzare solo uno dei metodi precedenti oppure puoi utilizzare 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 in AWS Client VPN.
> - Se si utilizza una combinazione di autenticazione reciproca e autenticazione basata sull'utente, entrambi i metodi devono essere utilizzati per autenticarsi correttamente nella VPN.

Autenticazione Active Directory in Client VPN

Client VPN fornisce supporto per Active Directory mediante l'integrazione con Directory Service. Con l'autenticazione Active Directory, i client vengono autenticati rispetto a gruppi di Active Directory esistenti. Utilizzando 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 in AWS Client VPN

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.

I certificati utilizzati in AWS Client VPN devono rispettare lo standard RFC 5280: certificato dell'infrastruttura a chiave pubblica Internet X.509 e profilo CRL (Certificate Revocation List), incluse le estensioni di certificato specificate nella sezione 4.2 del memo.

> **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 Client VPN vengono aggiornati, tramite la rotazione automatica di ACM, l'importazione manuale di un nuovo certificato o gli aggiornamenti dei metadati su IAM Identity Center, il servizio Client VPN aggiornerà automaticamente l'endpoint Client VPN con il certificato più recente. Si tratta di un processo automatizzato che può richiedere fino a 5 ore.

Attività

- Abilita l'autenticazione reciproca per AWS Client VPN
- Rinnova il certificato del tuo server per AWS Client VPN

Abilita l'autenticazione reciproca per AWS Client VPN

È possibile abilitare l'autenticazione reciproca in Client VPN in uno Linux/MacOS o in Windows.

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
```

10. 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 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.

Rinnova il certificato del tuo server per AWS Client VPN

È possibile rinnovare e reimportare un certificato del server Client VPN scaduto. A seconda della versione di OpenVPN easy-rsa in uso, la procedura può variare. Per maggiori dettagli, consulta la documentazione per il rinnovo e la revoca del certificato Easy-RSA 3.

Per rinnovare il certificato del server

1. Effettua una delle seguenti operazioni:
   - Easy-RSA versione 3.1.x
     - Esecuzione del comando di rinnovo del certificato.

       ```
       $ ./easyrsa renew server nopass
       ```
   - Easy-RSA versione 3.2.x
     a. Esegui il comando expire.

        ```
        $ ./easyrsa expire server
        ```
     b. Firma un nuovo certificato.

```
$ ./easyrsa --san=DNS:server sign-req server server
```

2. 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/
```

3. 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 \
    --certificate-arn
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Single Sign-on — autenticazione federata basata su SAML 2.0 — in Client VPN

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.

Argomenti

- Abilita SAML per AWS Client VPN
- Flusso di lavoro di autenticazione
- Requisiti e considerazioni per l'autenticazione federata basata su SAML
- Risorse di configurazione IdP basate su SAML

Abilita SAML per AWS Client VPN

Puoi abilitare SAML per il single sign-on per Client VPN completando i seguenti passaggi. In alternativa, se hai abilitato il portale self-service per l'endpoint Client VPN, chiedi agli utenti di accedere al portale self-service per ottenere il file di configurazione e il client fornito da AWS . Per ulteriori informazioni, consulta AWS Client VPN accesso al portale self-service.

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 trust tra AWS e il provider di identità.
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 tra IdP AWS e 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.

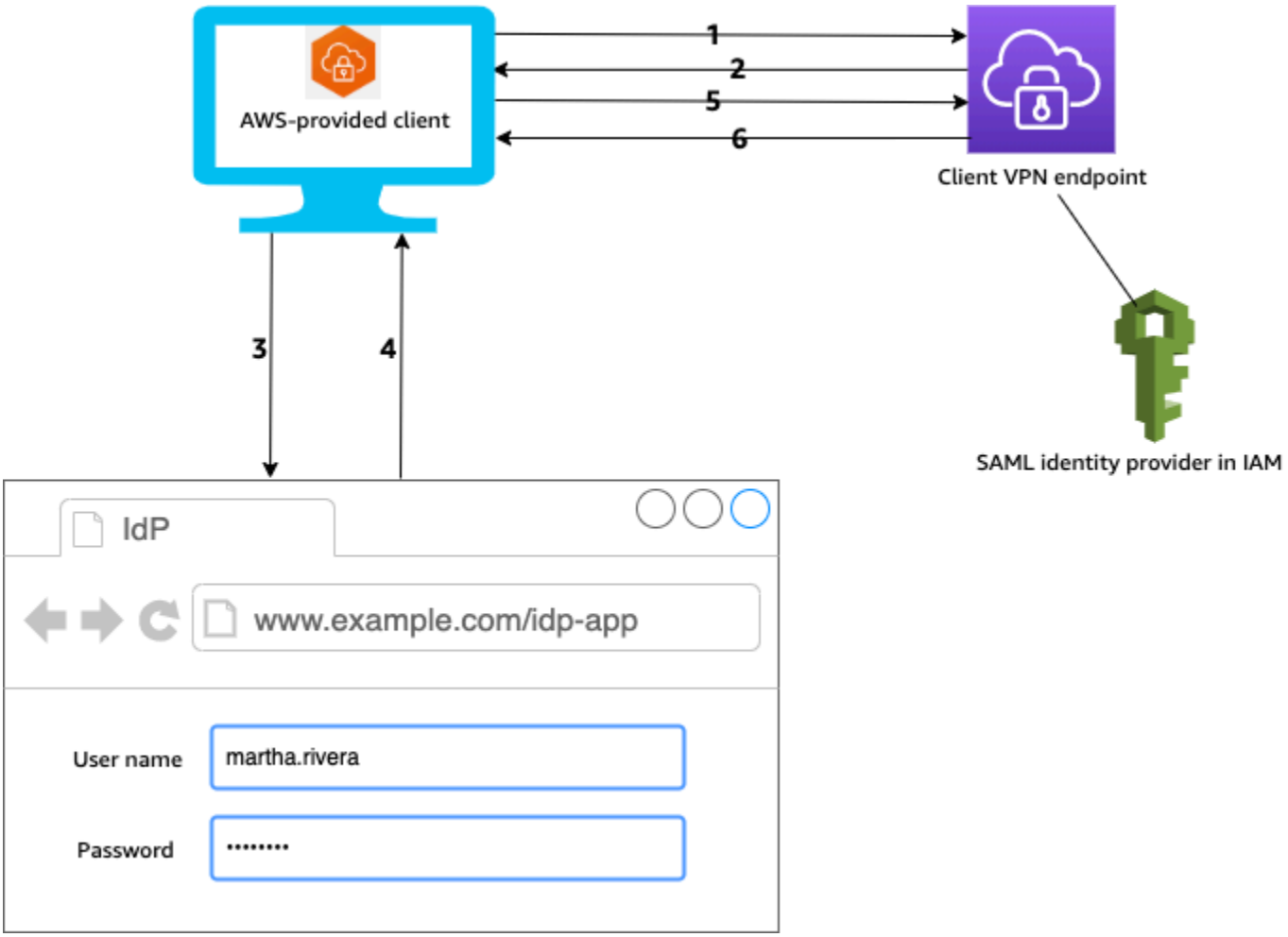
   > **Note**
   >
   > Non è necessario creare un ruolo IAM per utilizzare il provider di identità SAML IAM.
5. Crea un endpoint Client VPN.

   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 AWS Client VPN endpoint.

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.

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 e la risposta SAML devono essere firmate.
- 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`.
- Quando i certificati utilizzati con il servizio Client VPN vengono aggiornati, tramite la rotazione automatica di ACM, l'importazione manuale di un nuovo certificato o gli aggiornamenti dei metadati su IAM Identity Center, il servizio Client VPN aggiornerà automaticamente l'endpoint Client VPN con il certificato più recente. Si tratta di un processo automatizzato che può richiedere fino a 5 ore.

Risorse di configurazione IdP basate su SAML

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

IdP	Risorsa
Okta	Autentica AWS Client VPN gli utenti con SAML
ID Microsoft Entra (in precedenza Azure Active Directory)	Per ulteriori informazioni, vedere Tutorial: integrazione single sign-on (SSO) di Microsoft Entra con AWS ClientVPN sul sito Web di documentazione Microsoft.
JumpCloud	Integrazione 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.
`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 AWS Client VPN 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 IdP supporta più Assertion Consumer Service (ACS) URLs, 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 aggiungerli entrambi. URLs

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

Se il tuo IdP non supporta più ACS URLs, procedi come segue:

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 del cliente in AWS Client VPN

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 Applicare un gruppo di sicurezza a una rete di destinazione in AWS Client VPN. 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.

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 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 AWS Client VPN regole di autorizzazione.

Attività

- Creare una regola del gruppo AWS Client VPN di sicurezza degli endpoint

Creare una regola del gruppo AWS Client VPN di sicurezza degli endpoint

Il gruppo di sicurezza predefinito per il VPC applicato quando si associa una sottorete a un Client VPN potrebbe limitare il traffico proveniente dal traffico del gruppo di sicurezza predefinito che si desidera consentire, consentendo contemporaneamente il traffico che non si desidera. Utilizza i seguenti passaggi per creare una regola del gruppo di sicurezza degli endpoint Client VPN che consenta o limiti il traffico per un gruppo di sicurezza degli endpoint associato a una risorsa o un'applicazione. Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta Security groups for your VPC nella Amazon VPC User Guide.

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

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello 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).

Autorizzazione della connessione in AWS Client VPN

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 Interrompere una connessione AWS Client VPN 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 della limitazione) il seguente messaggio predefinito viene restituito ai client dal servizio Client VPN.

```
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 .

Utilizza il gestore client connect per la valutazione della postura

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 connetterà 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.

Abilita il gestore della connessione del 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 AWS Client VPN endpoint e Modificare un AWS Client VPN endpoint.

Ruolo collegato ai servizi

AWS Client VPN crea automaticamente un ruolo collegato al servizio nel tuo 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 di ruoli collegati ai servizi per AWS Client VPN.

Monitora gli errori di autorizzazione della connessione

Puoi visualizzare lo stato di autorizzazione delle connessioni all'endpoint Client VPN. Per ulteriori informazioni, consulta Visualizza le connessioni AWS Client VPN dei 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 della connessione per un endpoint AWS Client VPN.

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.

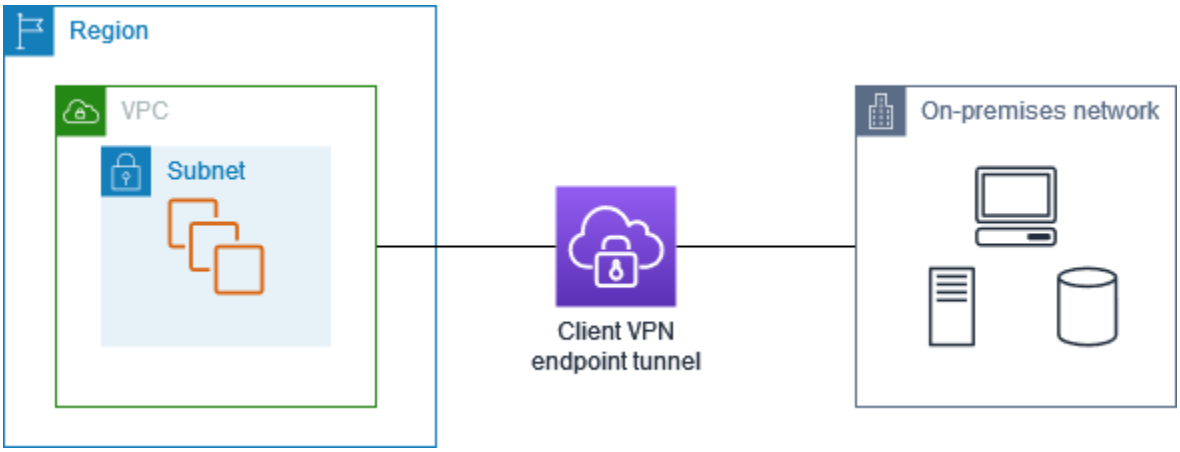
- `client-connect-handler-service-error`: si è verificato un errore sul lato servizio durante il tentativo di connessione.

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 proveniente dai client facendo in modo che solo il traffico AWS destinato 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 si abilita la modalità split-tunnel, tutte le route nella tabella di routing dell'endpoint Client VPN vengono aggiunte alla tabella di route 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**
  >
  > L'aggiunta di una route 0.0.0.0/0 alla tabella di routing dell'endpoint Client VPN quando si utilizza la modalità split-tunnel può causare interruzioni della connettività e non è consigliata

- 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.

Abilitare lo split-tunnel

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

- Creare un AWS Client VPN endpoint
- Modificare un AWS Client VPN endpoint

Registrazione della connessione per un endpoint AWS Client VPN

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

Un registro di connessione contiene voci del registro di connessione che acquisiscono informazioni sugli eventi di connessione, ad esempio 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 AWS Client VPN è disponibile. I registri delle connessioni vengono pubblicati in un gruppo di CloudWatch registri del 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, che viene assegnato dall'intervallo IPv4 CIDR 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 "" e connection-start-time "». connection-end-time

Per ulteriori informazioni sull'abilitazione della registrazione delle connessioni, consulta AWS Client VPN registri di connessione.

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. Dovresti tenere conto del numero di client che attualmente supporti e se il tuo endpoint Client VPN è in grado di scalare per soddisfare la domanda aggiuntiva, se necessario.

I seguenti fattori influiscono sul numero massimo di connessioni VPN simultanee che possono essere supportate su un endpoint Client VPN:

Intervallo dimensioni CIDR cliente

Quando si crea un endpoint Client VPN, è necessario specificare un intervallo CIDR client, che è un blocco IPv4 CIDR compreso tra una netmask /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

Associazioni di sottorete	Numero di connessioni supportate
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 di sottoreti dipende anche dal numero di zone di disponibilità disponibili 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 per l'utilizzo AWS Client VPN.

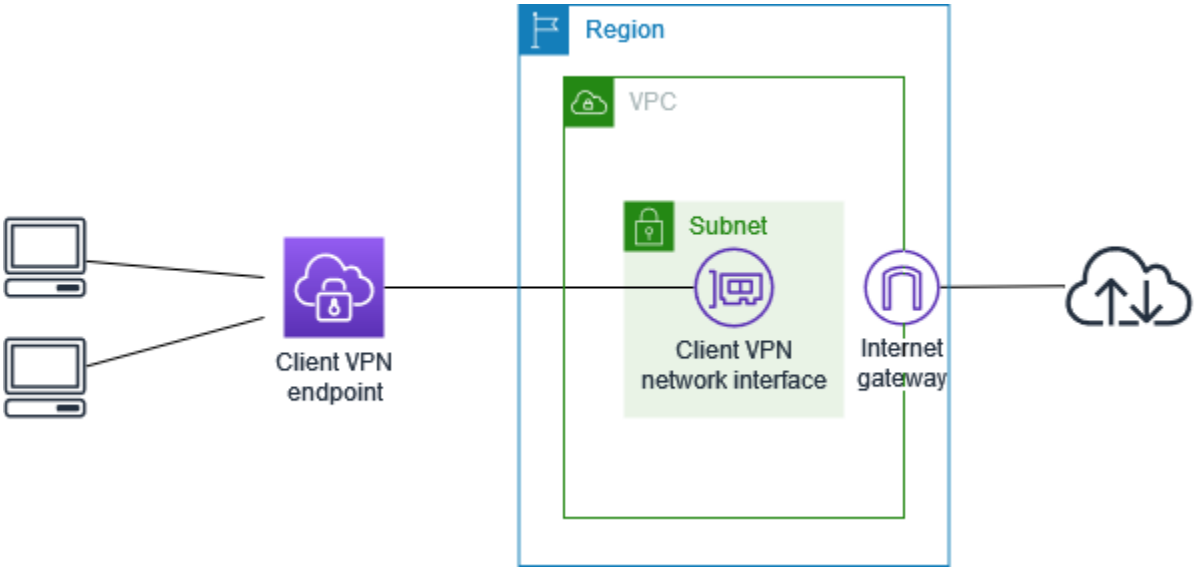
Per ulteriori informazioni sulle quote per l'endpoint VPN client, vedi AWS Client VPN quote.

Inizia con AWS Client VPN

In questo tutorial, creerai un AWS Client VPN endpoint che esegue le seguenti operazioni:

- 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 al momento della creazione dell'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 in AWS Client VPN.

> **Note**
>
> Il certificato del server deve essere fornito o importato in AWS Certificate Manager (ACM) nella stessa AWS regione in cui creerai 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 la 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, specifica un intervallo di indirizzi IP, in notazione CIDR, da 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. (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.

8. 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 AWS Client VPN endpoint.

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. Apri la 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. Apri la 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, specifica il blocco IPv4 CIDR 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.

Puoi fornire l'accesso a reti aggiuntive connesse al VPC, come AWS servizi, reti peered VPCs, locali 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. Apri la 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. Apri la 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 AWS Client VPN esportazione del file di configurazione dell'endpoint.

Fase 8: Connettersi all'endpoint Client VPN

È possibile connettersi all'endpoint Client VPN utilizzando il client AWS fornito 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.

Lavora con AWS Client VPN

I seguenti argomenti spiegano le principali attività amministrative necessarie per lavorare con Client VPN:

- Accedi al portale self-service: configura l'accesso al portale self-service Client VPN in modo che i clienti possano scaricare autonomamente il file di configurazione degli endpoint Client VPN. Per informazioni sull'accesso al portale self-service, consulta. the section called “accesso self-service al portale”
- Regole di autorizzazione: aggiungi regole di autorizzazione per controllare l'accesso dei client a reti specifiche. Per informazioni sull'aggiunta di regole di autorizzazione, vederethe section called “Regole di autorizzazione”.
- Elenchi di revoca dei certificati client: utilizza gli elenchi di revoca dei certificati client per revocare l'accesso a un endpoint Client VPN. Per informazioni sugli elenchi di revoca dei certificati client, consulta. the section called “Elenchi di revoche di certificati client”
- Connessioni client: visualizza o termina una connessione client a un endpoint Client VPN. Per informazioni sulla visualizzazione o l'interruzione di una connessione client, vedere. the section called “Connessioni client”
- Banner di accesso client: aggiungi un banner di testo su un'applicazione desktop Client VPN quando viene stabilita una sessione VPN. Puoi utilizzare il banner di testo per soddisfare le tue esigenze normative e di conformità. Per informazioni sui banner di accesso, consultathe section called “banner per il login del cliente”.
- Client Route Enforcement: applica i percorsi definiti dall'amministratore sui dispositivi collegati tramite la VPN. Per ulteriori informazioni su Client Route Enforcement, consulta. the section called “Applicazione del percorso del cliente”
- Endpoint Client VPN: configura gli endpoint Client VPN per gestire e controllare tutte le sessioni VPN. Per informazioni sulla configurazione degli endpoint, consulta. the section called “Endpoints”
- Registri di connessione: abilita la registrazione delle connessioni per gli endpoint Client VPN nuovi o esistenti per iniziare a catturare i log di connessione. Per informazioni sulla registrazione delle connessioni, vedere. the section called “Log delle connessioni”
- Esportazione del file di configurazione del client: configura il file di configurazione del client di cui i client Client VPN hanno bisogno per stabilire connessioni VPN. Dopo aver configurato il file, scaricalo (esportalo) per la distribuzione ai client. Per ulteriori informazioni sull'esportazione di un file di configurazione del client, vedere. the section called “esportazione del file di configurazione del client”

- Percorsi: configura le regole di autorizzazione per ogni route Client VPN per specificare quali client hanno accesso alla rete di destinazione. Per informazioni sulla configurazione delle regole di autorizzazione, vedere the section called “Regole di autorizzazione”
- Reti di destinazione: associa le reti di destinazione a un endpoint Client VPN per consentire ai client di connettersi ad esso e stabilire una connessione VPN. Per informazioni sulle reti di destinazione, consultathe section called “Reti target”.
- Durata massima della sessione VPN: imposta le opzioni per la durata massima della sessione VPN per soddisfare i requisiti di sicurezza e conformità. Per informazioni sulla durata massima della sessione VPN, consultathe section called “durata massima della sessione VPN”.

AWS Client VPN accesso 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 AWS fornito.

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 che esporti 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, offri ai tuoi clienti una delle seguenti opzioni: URLs

- `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>* l'URL precedente con l'ID del tuo endpoint Client VPN, ad esempio. `cvpn-endpoint-0123456abcd123456`

È inoltre possibile visualizzare l'URL del portale self-service nell'output del comando. describe-client-vpn-endpoints 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.

AWS Client VPN 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 Risoluzione dei problemi AWS Client VPN: le 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.

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.

Argomenti

- Scenari di esempio per le regole di autorizzazione Client VPN
- Aggiungere una regola di autorizzazione a un AWS Client VPN endpoint
- Rimuovere una regola di autorizzazione da un AWS Client VPN endpoint
- Visualizza le regole di AWS Client VPN autorizzazione

Scenari di esempio per le regole di autorizzazione Client VPN

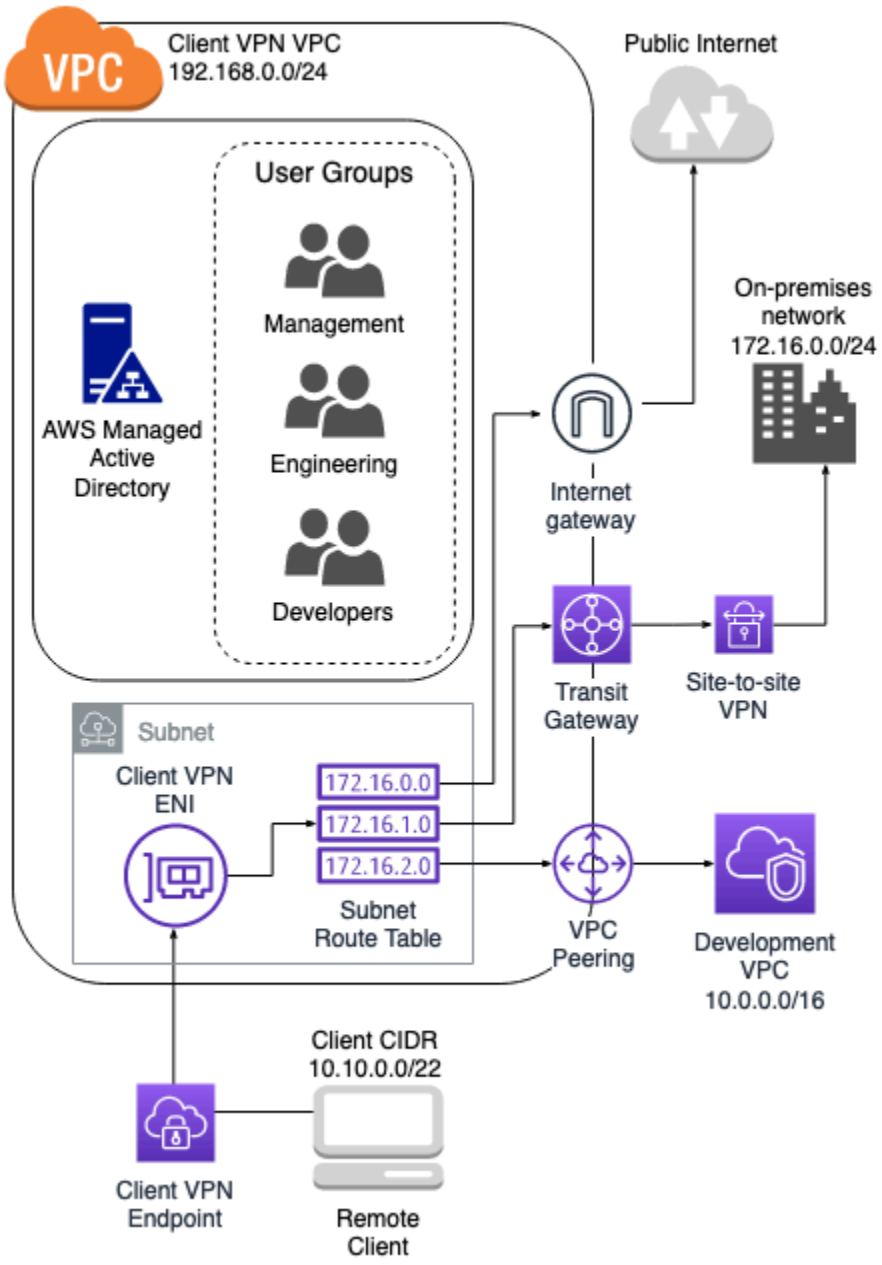
Questa sezione descrive come funzionano le regole di autorizzazione AWS Client VPN. Include punti chiave per comprendere le regole di autorizzazione, un'architettura di esempio e l'illustrazione di scenari di esempio corrispondenti all'architettura di esempio.

Scenari

- the section called “Architettura di esempio”
- the section called “Accesso a un'unica destinazione”
- the section called “Usa qualsiasi destinazione (0.0.0.0/0) CIDR”
- the section called “Corrispondenza del prefisso IP più lunga”
- the section called “CIDR sovrapposto (stesso gruppo)”
- the section called “Regola aggiuntiva 0.0.0.0/0”
- the section called “Aggiungi una regola per 192.168.0.0/24”
- the section called “Autenticazione federata SAML”
- the section called “Accesso per tutti i gruppi di utenti”

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.



Accesso a un'unica destinazione

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

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

Usa qualsiasi destinazione (0.0.0.0/0) CIDR

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

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	CIDR di destinazione
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 `10.0.0/16`.

> **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.

Corrispondenza del prefisso IP più lunga

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	10.0.2.119/32

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`.

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	10.0.2.119/32
Fornisce al gruppo di progettazione l'accesso a una sottorete più piccola	S-xxxxx14	False	172,16,0,128/25

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

Regola aggiuntiva 0.0.0.0/0

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
	S-xxxxx16	False	10.0.2.119/32

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			
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`.

Aggiungi una 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	10.0.2.119/32
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.

Autenticazione federata SAML

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	Engineering (Progettazione)	False	172.16.0.0/24
Fornisce al gruppo di sviluppo l'accesso al VPC di sviluppo	Sviluppatori	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 manager l'accesso al VPC del client VPN	Responsabili	False	192.168.0.0/24

Comportamento risultante

- Solo gli utenti autenticati tramite SAML con l'attributo di gruppo «Engineering» possono accedere. `172.16.0.0/24`
- L'accesso è consentito solo agli utenti autenticati tramite SAML con l'attributo di gruppo «Developers». `10.0.0.0/16`
- L'accesso è consentito solo agli utenti autenticati tramite SAML con l'attributo di gruppo «Managers». `192.168.0.0/24`
- Tutto l'altro traffico viene eliminato dall'endpoint del Client VPN.

> **Note**
>
> Quando si utilizza l'autenticazione federata SAML, il campo ID del gruppo corrisponde al valore dell'attributo SAML che identifica l'appartenenza al gruppo dell'utente. Questo attributo è configurato nel tuo provider di identità SAML e passato a Client VPN durante l'autenticazione.

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

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	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	10.0.2.119/32
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.

Aggiungere una regola di autorizzazione a un AWS Client VPN endpoint

È possibile aggiungere una regola di autorizzazione per concedere o limitare l'accesso a un endpoint Client VPN utilizzando il Console di gestione AWS. È possibile aggiungere una regola di autorizzazione a un endpoint Client VPN utilizzando la console Amazon VPC o utilizzando la riga di comando o l'API.

Per aggiungere una regola di autorizzazione a un endpoint Client VPN utilizzando Console di gestione AWS

1. Apri la 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 Active Directory o il gruppo definito in un provider ID/name di identità (IdP) basato su SAML.

- (Active Directory) Per ottenere il SID, è possibile utilizzare il ADGroup cmdlet Microsoft Powershell Get-, 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) Il gruppo ID/name deve corrispondere alle informazioni sugli attributi di 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.

Rimuovere una regola di autorizzazione da un AWS Client VPN endpoint

È possibile rimuovere le regole di autorizzazione per uno specifico endpoint Client VPN utilizzando la console e il AWS CLI.

Per rimuovere le regole di autorizzazione (console)

1. Apri la 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 il quale è stata aggiunta la regola di autorizzazione, quindi scegli Regole di autorizzazione.
4. Seleziona la regola di autorizzazione da eliminare, scegli Rimuovi regola di autorizzazione, quindi scegli nuovamente Rimuovi regola di autorizzazione per confermare l'eliminazione.

Per rimuovere le regole di autorizzazione (AWS CLI)

Utilizza il comando revoke-client-vpn-ingress.

Visualizza le regole di AWS Client VPN 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. Apri la 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)

Usa il comando describe-client-vpn-authorization-rules.

AWS Client VPN elenchi di revoca dei certificati client

Gli elenchi di revoca dei certificati client Client VPN vengono utilizzati per revocare l'accesso a un endpoint Client VPN per certificati client specifici. È possibile generare un elenco di revoche o importare un elenco esistente. È inoltre possibile esportare l'elenco corrente in un file di elenco delle revoche. La generazione di un elenco viene eseguita utilizzando il software OpenVPN su uno Linux/macOS o su Windows. L'importazione e l'esportazione possono essere eseguite utilizzando la console Amazon VPC o utilizzando la CLI. AWS

Per ulteriori informazioni sulla creazione di certificati e chiavi server e client, consulta Autenticazione reciproca in AWS Client VPN

> **Note**
>
> Se un elenco di revoca dei certificati client è scaduto, non è possibile connettersi all'endpoint Client VPN. Dovrai crearne uno nuovo e importarlo nell'endpoint Client VPN.

È possibile aggiungere solo un numero limitato di voci a un elenco di revoca dei certificati client. Per ulteriori informazioni sul numero di voci che è possibile aggiungere a un elenco di revoca, vedere. Quote Client VPN

Attività

- Generare un elenco di revoca dei certificati AWS Client VPN client
- Importazione di un AWS Client VPN elenco di revoche di certificati client
- Esportazione di un AWS Client VPN elenco di revoche di certificati client

Generare un elenco di revoca dei certificati AWS Client VPN client

È possibile generare un elenco di revoca dei certificati Client VPN su un sistema operativo Linux/macOS o Windows. L'elenco di revoca viene utilizzato per revocare l'accesso a un endpoint Client VPN per certificati specifici. Per ulteriori informazioni sugli elenchi di revoca dei certificati client, vedere. Elenchi 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. Accedere 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
```

Inserisci `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. Esegui il `EasyRSA-Start.bat` file per avviare la shell EasyRSA.

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

3. Nella shell EasyRSA, revocare il certificato client.

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

4. Inserisci `yes` quando richiesto.
5. Generare l'elenco di revoche client.

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

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

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

Per generare un elenco di revoche 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 revoche client.

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

Importazione di un AWS Client VPN elenco di revoche di certificati client

È necessario disporre di un file di elenco di revoca dei certificati del client Client VPN da importare. Per ulteriori informazioni sulla creazione di un elenco di revoche di certificati client, consulta Generare un elenco di revoca dei certificati AWS Client VPN client.

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

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

1. Apri la 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 revoche di certificati client.
4. Scegliere Operazioni, quindi Import Client Certificate CRL (Importa elenco di revoche di certificati client).
5. Per Elenco di revoche di certificati, immettere il contenuto del file con l'elenco di revoche di certificati client e scegliere Import CRL (Importa elenco di revoche di certificati).

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

Usare il certificate-revocation-list comando import-client-vpn-client-.

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

Esportazione di un AWS Client VPN elenco di revoche di certificati client

È possibile esportare gli elenchi di revoca dei certificati dei client Client VPN utilizzando la console e il AWS CLI.

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

1. Apri la 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)

Usare il certificate-revocation-list comando export-client-vpn-client-.

AWS Client VPN connessioni client

AWS Client VPN le connessioni sono sessioni VPN attive che sono state stabilite dai client verso uno specifico endpoint Client VPN, nonché connessioni che sono state interrotte negli ultimi 60 minuti per quell'endpoint. Viene stabilita una connessione quando un client si connette a un endpoint Client VPN. L'interruzione di una sessione interrompe la connessione del client all'endpoint Client VPN.

È possibile visualizzare e terminare le connessioni Client VPN. La visualizzazione delle informazioni di connessione restituisce informazioni come l'indirizzo IP assegnato dall'intervallo di blocchi CIDR del client, l'ID dell'endpoint e il timestamp. L'interruzione di una sessione termina la connessione VPN specificata all'endpoint. La visualizzazione e la chiusura delle sessioni possono essere eseguite utilizzando la console Amazon VPC o la CLI AWS . Se non riesci a connetterti all'endpoint e a seconda dell'errore, consulta le istruzioni da seguire Risoluzione dei problemi per risolvere il problema.

Attività

- Visualizza le connessioni AWS Client VPN dei client
- Interrompere una connessione AWS Client VPN client

Visualizza le connessioni AWS Client VPN dei client

Puoi visualizzare le connessioni Client VPN attive utilizzando la console Amazon VPC o la CLI AWS .

Per visualizzare le connessioni client Client VPN (console)

1. Apri la 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 Client VPN (AWS CLI)

Utilizza il comando describe-client-vpn-connections.

Interrompere una connessione AWS Client VPN client

Puoi interrompere una connessione client Client VPN utilizzando la console Amazon VPC o la CLI AWS .

Per terminare una connessione client Client VPN (console)

1. Apri la 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 Connessioni.
4. Seleziona la connessione da terminare, scegli Termina connessione, quindi scegli nuovamente Termina connessione per confermare la terminazione.

Per terminare una connessione client Client VPN ()AWS CLI

Utilizza il comando terminate-client-vpn-connections.

AWS Client VPN banner di accesso al cliente

AWS Client VPN offre la possibilità di visualizzare un banner di testo sulle applicazioni desktop Client VPN AWS fornite 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 con codifica 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.

Creazione di banner

I banner di accesso vengono inizialmente creati e abilitati durante la creazione dell'endpoint Client VPN. Per i passaggi per abilitare un banner di accesso client durante la creazione di un endpoint Client VPN, vedereCreare un AWS Client VPN endpoint.

Attività

- Configurare un banner di accesso client per un AWS Client VPN endpoint esistente
- Disattiva un banner di accesso client per un endpoint esistente AWS Client VPN
- Modificare il testo del banner esistente su un AWS Client VPN endpoint
- Visualizza un banner di AWS Client VPN accesso attualmente configurato

Configurare un banner di accesso client per un AWS Client VPN endpoint 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. Apri la 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. Per il testo del banner di accesso al client, inserisci il testo che verrà visualizzato in un banner sui client AWS forniti 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.

Disattiva un banner di accesso client per un endpoint esistente AWS Client VPN

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. Apri la 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 AWS Client VPN endpoint

Utilizza i seguenti passaggi per modificare il testo esistente su un banner di accesso al client Client VPN.

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

1. Apri la 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. Per il testo del banner di accesso al Client, sostituisci il testo esistente con il nuovo testo che desideri venga visualizzato in un banner sui client AWS forniti 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.

Visualizza un banner di AWS Client VPN accesso attualmente configurato

Utilizza i seguenti passaggi per visualizzare un banner di accesso al client Client VPN attualmente configurato.

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

1. Apri la 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.

AWS Client VPN Applicazione del percorso del client

Client Route Enforcement aiuta a far rispettare i percorsi definiti dall'amministratore sui dispositivi collegati tramite VPN. Questa funzionalità aiuta a migliorare il livello di sicurezza assicurando che il traffico di rete proveniente da un client connesso non venga inviato inavvertitamente all'esterno del tunnel VPN.

Client Route Enforcement monitora la tabella di routing principale del dispositivo connesso e garantisce che il traffico di rete in uscita vada verso un tunnel VPN, in base ai percorsi di rete configurati nell'endpoint VPN del client. Ciò include la modifica delle tabelle di routing su un dispositivo se vengono rilevate rotte in conflitto con il tunnel VPN. Client Route Enforcement supporta entrambe le famiglie di IPv4 indirizzi IPv6 .

Requisiti

Client Route Enforcement funziona solo con le seguenti versioni Client VPN AWS fornite:

- Windows versione 5.2.0 o successiva (IPv4 supporto)
- macOS versione 5.2.0 o successiva (supporto) IPv4
- Ubuntu versione 5.2.0 o successiva (supporto) IPv4
- Windows versione 5.3.0 o successiva (supporto) IPv6
- macOS versione 5.3.0 o successiva (supporto) IPv6
- Ubuntu versione 5.3.0 o successiva (supporto) IPv6

Per gli endpoint dual-stack, l'impostazione Client Route Enforcement si applica a entrambi gli stack contemporaneamente. IPv4 IPv6 Non è possibile abilitare Client Route Enforcement per un solo stack.

Conflitti di routing

Mentre un client è connesso alla VPN, viene effettuato un confronto tra la tabella delle rotte locali del client e le rotte di rete dell'endpoint. Si verificherà un conflitto di routing in caso di sovrapposizione di rete tra due voci della tabella di routing. Un esempio di reti sovrapposte è:

- `172.31.0.0/16`
- `172.31.1.0/24`

In questo esempio, questi blocchi CIDR costituiscono un conflitto di routing. Ad esempio, `172.31.0.0/16` potrebbe essere il tunnel VPN CIDR. Poiché `172.31.1.0/24` è più specifico perché ha un prefisso più lungo, in genere ha la precedenza e potenzialmente reindirizza il traffico VPN all'interno dell'intervallo `172.31.1.0/24` IP verso un'altra destinazione. Ciò potrebbe portare a comportamenti di routing non intenzionali. Tuttavia, quando Client Route Enforcement è abilitato, quest'ultimo CIDR verrebbe rimosso. Quando si utilizza questa funzionalità, è necessario prendere in considerazione i potenziali conflitti di routing.

Le connessioni VPN a tunnel completo indirizzano tutto il traffico di rete attraverso la connessione VPN. Di conseguenza, i dispositivi collegati alla VPN non saranno in grado di accedere alle risorse della rete locale (LAN), se la funzione Client Route Enforcement è abilitata. Se è necessario l'accesso

alla LAN locale, valuta la possibilità di utilizzare la modalità split-tunnel anziché la modalità full-tunnel. Per ulteriori informazioni su split-tunnel, vedere. Split-tunnel di Client VPN

Considerazioni

Le seguenti informazioni devono essere prese in considerazione prima di attivare Client Route Enforcement.

- Al momento della connessione, se viene rilevato un conflitto di routing, la funzionalità aggiornerà la tabella di routing del client per indirizzare il traffico verso il tunnel VPN. Le rotte che esistevano prima dello stabilimento della connessione e che sono state eliminate da questa funzionalità verranno ripristinate.
- La funzionalità viene applicata solo sulla tabella di routing principale e non si applica ad altri meccanismi di routing. Ad esempio, l'applicazione non viene applicata a quanto segue:
  - routing basato su politiche
  - routing con ambito di interfaccia
- Client Route Enforcement protegge il tunnel VPN mentre è aperto. Non c'è protezione dopo la disconnessione del tunnel o durante la riconnessione del client.

Le direttive OpenVPN hanno un impatto sulla Cloud Route Enforcement

Alcune direttive personalizzate nel file di configurazione OpenVPN hanno interazioni specifiche con Client Route Enforcement:

- Direttiva `route`
  - Quando si aggiungono percorsi a un gateway VPN. Ad esempio, aggiungendo il percorso `192.168.100.0 255.255.255.0` a un gateway VPN.

    Le rotte aggiunte a un gateway VPN vengono monitorate da Client Route Enforcement in modo analogo a qualsiasi altra route VPN. Eventuali percorsi in conflitto al loro interno verranno rilevati e rimossi.
  - Quando si aggiungono percorsi a un gateway non VPN. Ad esempio, aggiungendo il percorso`192.168.200.0 255.255.255.0 net_gateway`.

    Le rotte aggiunte a un gateway non VPN sono escluse da Client Route Enforcement in quanto bypassano il tunnel VPN. Al loro interno sono consentiti percorsi in conflitto. Nell'esempio, il percorso sopra riportato verrà escluso dal monitoraggio da parte di Client Route Enforcement.

- Analogamente alle IPv4 route, le IPv6 route aggiunte a un gateway VPN vengono monitorate da Client Route Enforcement, mentre le route aggiunte a un gateway non VPN sono escluse dal monitoraggio.

Percorsi ignorati

Le rotte verso le seguenti IPv4 reti verranno ignorate da Client Route Enforcement:

- `127.0.0.0/8`— Riservato all'host locale
- `169.254.0.0/16`— Riservato agli indirizzi locali del collegamento
- `224.0.0.0/4`— Riservato al multicast
- `255.255.255.255/32`— Riservato alla trasmissione

Le rotte verso le seguenti IPv6 reti verranno ignorate da Client Route Enforcement:

- `::1/128`— Riservato al loopback
- `fe80::/10`— Riservato agli indirizzi locali del collegamento
- `ff00::/8`— Riservato al multicast

Argomenti

- Attiva Client Route Enforcement per un endpoint AWS Client VPN
- Disattivare Client Route Enforcement da un endpoint AWS Client VPN
- Risolvi i problemi relativi IPv6 al Client Route Enforcement

Attiva Client Route Enforcement per un endpoint AWS Client VPN

È possibile attivare Client Route Enforcement sugli endpoint Client VPN esistenti utilizzando la console o il AWS CLI.

Per attivare Client Route Enforcement utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Endpoint del client VPN.
3. Scegli l'endpoint Client VPN che desideri modificare, scegli Azioni, quindi scegli Modifica endpoint Client VPN.

4. Scorri verso il basso la pagina fino alla sezione Other parameters (Altri parametri).
5. Attiva Client Route Enforcement.
6. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Per attivare Client Route Enforcement utilizzando AWS CLI()

- Utilizza il comando modify-client-vpn-endpoint.

Disattivare Client Route Enforcement da un endpoint AWS Client VPN

È possibile disattivare Client Route Enforcement sugli endpoint Client VPN utilizzando la console o il. AWS CLI

Per disattivare Client Route Enforcement utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Endpoint del client VPN.
3. Scegli l'endpoint Client VPN che desideri modificare, scegli Azioni, quindi scegli Modifica endpoint Client VPN.
4. Scorri verso il basso la pagina fino alla sezione Other parameters (Altri parametri).
5. Disattiva Client Route Enforcement.
6. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Per disattivare Client Route Enforcement utilizzando il AWS CLI

- Utilizza il comando modify-client-vpn-endpoint.

Risolvi i problemi relativi IPv6 al Client Route Enforcement

Se riscontri problemi con IPv6 Client Route Enforcement, considera i seguenti passaggi per la risoluzione dei problemi:

Verifica la versione del client

Assicurati di utilizzare AWS VPN Client versione 5.3.0 o successiva, necessaria per il supporto di IPv6 Client Route Enforcement.

Controlla la configurazione degli endpoint

Verifica che l'endpoint abbia Client Route Enforcement abilitato e che sia configurato per il traffico IPv6 dual-stack.

Esamina i log dei client

Controlla i log del client AWS VPN per eventuali messaggi di errore relativi a IPv6 Client Route Enforcement. Cerca le voci contenenti "IPv6" e «Client Route Enforcement» o «CRM».

Ispeziona la tabella di routing

Utilizzate il comando appropriato per il vostro sistema operativo per visualizzare la tabella di IPv6 routing:

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

Verifica la presenza di percorsi in conflitto

Cerca eventuali IPv6 percorsi che potrebbero entrare in conflitto con i percorsi VPN. Presta particolare attenzione ai percorsi con la stessa destinazione ma gateway diversi.

Verifica il supporto dell'ISP IPv6

Assicurati che il tuo provider di servizi Internet (ISP) supporti correttamente. IPv6

Se continui a riscontrare problemi con IPv6 Client Route Enforcement dopo aver provato questi passaggi per la risoluzione dei problemi, contatta AWS Support per ulteriore assistenza.

AWS Client VPN punti finali

Tutte le AWS Client VPN sessioni stabiliscono la comunicazione con un endpoint Client VPN. È possibile gestire l'endpoint Client VPN per creare, modificare, visualizzare ed eliminare sessioni client VPN con quell'endpoint. Gli endpoint possono essere creati e modificati utilizzando la console Amazon VPC o utilizzando la CLI AWS .

Requisiti per la creazione di endpoint Client VPN

> **Important**
>
> Un endpoint Client VPN deve essere creato nello stesso AWS account in cui viene eseguito il provisioning della rete di destinazione prevista. Dovrai anche generare un certificato server e, se necessario, un certificato client. Per ulteriori informazioni, consulta Autenticazione client in AWS Client VPN.

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

- Esamina le regole e le limitazioni in Regole e best practice per l'utilizzo AWS Client VPN.
- Genera il certificato server e, se necessario, il certificato client. Per ulteriori informazioni, consulta Autenticazione client in AWS Client VPN.

Tipi di indirizzi IP

AWS Client VPN supporta configurazioni IPv4 -only, IPv6 -only e dual-stack sia per la connettività degli endpoint che per il routing del traffico. Le seguenti indicazioni aiutano a selezionare il tipo di indirizzo IP appropriato in base alle funzionalità del dispositivo client, all'infrastruttura di rete e ai requisiti delle applicazioni.

Tipo di indirizzo dell'endpoint

Il tipo di indirizzo dell'endpoint determina i protocolli IP supportati dall'endpoint Client VPN per le connessioni client. Questa impostazione non può essere modificata dopo la creazione dell'endpoint.

Scegli IPv4 -only quando:

- I tuoi dispositivi client supportano solo IPv4 connessioni VPN
- I tuoi strumenti di sicurezza sono ottimizzati per l'ispezione IPv4 del traffico

Scegli IPv6 -only quando:

- Tutti i dispositivi client supportano IPv6 completamente le connessioni
- Ti trovi in reti in cui IPv4 gli indirizzi sono esauriti

Scegli il dual-stack quando:

- Disponi di una combinazione di dispositivi client con diverse funzionalità IP
- Stai gradualmente passando da a IPv4 IPv6

Tipo di indirizzo IP del traffico

Il tipo di indirizzo IP del traffico controlla il modo in cui Client VPN indirizza il traffico tra i client e le risorse VPC, indipendentemente dai protocolli supportati dall'endpoint.

Indirizza il traffico come quando IPv4 :

- Supporta solo le applicazioni target nel tuo VPC IPv4
- Hai gruppi e reti IPv4 di sicurezza complessi ACLs
- Ti stai connettendo a sistemi legacy

Indirizza il traffico come IPv6 quando:

- La tua infrastruttura VPC è principalmente IPv6
- Vuoi rendere la tua architettura di rete a prova di futuro
- Disponi di applicazioni moderne progettate per IPv6

Modifica degli endpoint

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
- Abilita o disabilita la riconnessione automatica al timeout della sessione
- 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 IPv4 CIDR del client, le opzioni di autenticazione, il certificato client o il protocollo di trasporto dopo la creazione dell'endpoint Client VPN.

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

Attività

- Creare un AWS Client VPN endpoint
- Visualizza gli AWS Client VPN endpoint
- Modificare un AWS Client VPN endpoint
- Eliminare un AWS Client VPN endpoint

Creare un AWS Client VPN endpoint

Crea un AWS Client VPN endpoint per consentire ai tuoi clienti di stabilire una sessione VPN utilizzando la console Amazon VPC o AWS CLI la.Client VPN supporta tutte le combinazioni di tipo di endpoint (split-tunnel e full-tunnel) con tipo di traffico (e dual-stack) durante la creazione iniziale. IPv4 IPv6

Prima di creare un endpoint, acquisisci familiarità con i requisiti. Per ulteriori informazioni, consulta the section called “Requisiti per la creazione di endpoint Client VPN”.

Per creare un endpoint Client VPN utilizzando la console

1. Apri la 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 il tipo di indirizzo IP dell'endpoint, scegli il tipo di indirizzo IP per l'endpoint:
   - IPv4: L'endpoint utilizza IPv4 gli indirizzi per il traffico esterno del tunnel VPN.
   - IPv6: L'endpoint utilizza IPv6 indirizzi per il traffico esterno del tunnel VPN.
   - Dual-stack: l'endpoint utilizza sia gli indirizzi che IPv6 gli indirizzi per il traffico IPv4 esterno del tunnel VPN.
5. Per il tipo di indirizzo IP relativo al traffico, scegli il tipo di indirizzo IP per il traffico che attraversa l'endpoint:
   - IPv4: l'endpoint supporta IPv4 solo il traffico.
   - IPv6: L'endpoint supporta solo il IPv6 traffico.
   - Dual-stack: l'endpoint supporta sia il traffico che il traffico. IPv4 IPv6
6. Per Client IPv4 CIDR, specifica un intervallo di indirizzi IP, in notazione CIDR, da cui assegnare gli indirizzi IP del client. Ad esempio, `10.0.0.0/22`. Questo è necessario se hai selezionato IPv4 o Dual-stack per il tipo di indirizzo IP Traffic.

> **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.

- Quando si seleziona IPv6 come tipo di indirizzo IP dell'endpoint, il campo Client IPv4 CIDR è disabilitato. L'endpoint Client VPN alloca IPv6 gli indirizzi dei client da una sottorete associata ed è possibile associare la sottorete dopo aver creato l'endpoint.

> **Note**
>
> Per il IPv6 traffico, non è necessario specificare un intervallo CIDR del client. Amazon assegna automaticamente gli intervalli IPv6 CIDR ai clienti.

7. 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 del server deve essere presente in AWS Certificate Manager (ACM) nella regione in cui si sta creando l'endpoint Client VPN. Il certificato può essere fornito con ACM o importato in ACM.
> Per i passaggi per fornire o importare un certificato in ACM, consulta AWS Certificate Manager Certificati nella Guida per l'AWS Certificate Manager utente.

8. 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 dei certificati, selezionare Usa autenticazione reciproca, quindi per ARN del certificato client, specificare l'ARN del certificato client fornito in (ACM). AWS Certificate Manager

> **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.

9. (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.
10. (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.
11. (Facoltativo) Specificare i server DNS da utilizzare per la risoluzione DNS. Per utilizzare server DNS personalizzati, per l'indirizzo IP DNS Server 1 e l'indirizzo IP DNS Server 2, specifica IPv4 gli indirizzi dei server DNS da utilizzare. Per gli IPv6 endpoint dual-stack, puoi anche specificare gli indirizzi DNS Server 1 e DNS Server 2. IPv6 IPv6 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.

12. (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.

13. (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.
14. (Facoltativo) Per VPC ID (ID VPC) scegli il VPC da associare all'endpoint Client VPN. Per Security Group IDs, scegli uno o più gruppi di sicurezza del VPC da applicare all'endpoint Client VPN.
15. (Facoltativo) Per VPN port (Porta VPN), scegliere il numero di porta VPN. Il valore predefinito è 443.
16. (Facoltativo) Per generare un URL del portale self-service per i client attiva Enable self-service portal (Abilita portale self-service).
17. (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.
18. (Facoltativo) In Disconnetti al timeout della sessione, scegli se desideri terminare la sessione quando viene raggiunto il tempo massimo di sessione. La scelta di questa opzione richiede che gli utenti si riconnettano manualmente all'endpoint quando la sessione scade; in caso contrario, Client VPN proverà automaticamente a riconnettersi.
19. (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.
20. 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.
- Chiedi ai tuoi clienti di utilizzare il client AWS fornito o un'altra applicazione client basata su OpenVPN per connettersi all'endpoint Client VPN. Per ulteriori informazioni, consulta la Guida per l'utente AWS Client VPN.

Per creare un endpoint Client VPN utilizzando AWS CLI

Utilizza il comando create-client-vpn-endpoint.

Esempio di creazione di un IPv4 endpoint:

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

Esempio di creazione di un IPv6 endpoint:

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

Esempio di creazione di un endpoint dual-stack:

```
aws ec2 create-client-vpn-endpoint \
  --endpoint-ip-address-type "dual-stack" \
  --traffic-ip-address-type "dual-stack" \
```

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

Visualizza gli AWS Client VPN endpoint

Puoi visualizzare le informazioni sugli endpoint Client VPN utilizzando la console Amazon VPC o il. AWS CLI

Per visualizzare gli endpoint Client VPN (console)

1. Apri la 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.

Modificare un AWS Client VPN endpoint

Puoi modificare un endpoint Client VPN utilizzando la console Amazon VPC o il. AWS CLI Per ulteriori informazioni sui campi disponibili Campi Client VPN che è possibile modificare, vederethe section called “Modifica dell'endpoint”.

Limitazioni

Le seguenti limitazioni si applicano alla modifica di un endpoint

- 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 IPv4 CIDR del client, le opzioni di autenticazione, il certificato client o il protocollo di trasporto dopo la creazione dell'endpoint Client VPN.
- È possibile modificare gli IPv4 endpoint esistenti in dual-stack sia per l'IP dell'endpoint che per i tipi di IP di traffico. Se hai bisogno di IPv6 -only per l'IP dell'endpoint e l'IP del traffico, devi creare un nuovo endpoint.
- Client VPN non supporta la modifica del tipo di endpoint (IPv4, IPv6, dual-stack) o del tipo di traffico (IPv4 IPv6, dual-stack) dopo la creazione.
- La modifica di un Client VPN con una combinazione specifica di tipo di endpoint e tipo di traffico non è supportata. Non è possibile passare a nessun'altra combinazione. L'endpoint deve essere eliminato e ricreato con la configurazione desiderata.
- Client-to-client la comunicazione per il IPv6 traffico non è supportata.

Modifica un endpoint Client VPN.

È possibile modificare un endpoint Client VPN utilizzando la console o il AWS CLI.

Per modificare un endpoint Client VPN utilizzando la console

1. Apri la 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 il tipo di indirizzo IP dell'endpoint, è possibile modificare un IPv4 endpoint esistente in dual-stack. Questa opzione è disponibile solo per gli endpoint. IPv4
6. Per il tipo di indirizzo IP Traffic, puoi modificare un IPv4 endpoint esistente in dual-stack. Questa opzione è disponibile solo per gli endpoint. IPv4
7. 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 del server deve essere presente in AWS Certificate Manager (ACM) nella regione in cui si sta creando l'endpoint Client VPN. Il certificato può essere fornito con ACM o importato in ACM.

8. 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 connessione 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.

9. 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.
10. Attivare o disattivare Enable DNS servers (Abilita server DNS). Per utilizzare server DNS personalizzati, per l'indirizzo IP DNS Server 1 e l'indirizzo IP DNS Server 2, specifica IPv4 gli indirizzi dei server DNS da utilizzare. Per gli IPv6 endpoint dual-stack, puoi anche specificare gli indirizzi DNS Server 1 e DNS Server 2. IPv6 IPv6 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.

11. Attivare o disattivare Enable split-tunnel (Abilita split-tunnel). Per impostazione predefinita, lo split-tunnel su un endpoint VPN è disabilitato.
12. Per ID VPC, scegli il VPC da associare all'endpoint Client VPN. Per Security Group IDs, scegli uno o più gruppi di sicurezza del VPC da applicare all'endpoint Client VPN.

13. Per VPN port (Porta VPN), scegli il numero di porta VPN. Il valore predefinito è 443.
14. Per generare un URL del portale self-service per i client, attiva Enable self-service portal (Abilita portale self-service).
15. (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.
16. Per Disconnetti al timeout della sessione, scegli se desideri terminare la sessione quando viene raggiunto il tempo massimo di sessione. La scelta di questa opzione richiede che gli utenti si riconnettano manualmente all'endpoint quando la sessione scade; in caso contrario, Client VPN proverà automaticamente a riconnettersi.
17. 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.
18. Scegli Modify Client VPN Endpoint (Modifica l'endpoint del client VPN).

Per modificare un endpoint Client VPN utilizzando AWS CLI

Utilizza il comando modify-client-vpn-endpoint.

Esempio di modifica di un IPv4 endpoint in dual-stack:

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

Eliminare un AWS Client VPN endpoint

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. Apri la 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.

AWS Client VPN registri di connessione

Puoi abilitare la registrazione (logging) delle connessioni per un endpoint Client VPN nuovo o esistente e avviare l'acquisizione dei registri delle connessioni. I log di connessione mostrano la sequenza degli eventi di registro per l'endpoint Client VPN. 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. La registrazione delle connessioni registra quindi le seguenti informazioni: richieste di connessione client, risultati della connessione client (riuscita o meno), motivi dei risultati di connessione non riusciti e ora di terminazione del client dall'endpoint.

Prima di iniziare, devi avere un gruppo di CloudWatch log Logs nel tuo account. Per ulteriori informazioni, consulta Working with Log Groups and Log Streams nella Amazon CloudWatch Logs User Guide. L'utilizzo CloudWatch di Logs comporta dei costi. Per ulteriori informazioni, consulta i CloudWatch prezzi di Amazon.

I log di connessione Client VPN possono essere creati utilizzando la console Amazon VPC o la CLI AWS .

Attività

- Abilitazione della registrazione delle connessioni per un nuovo endpoint AWS Client VPN
- Abilitare la registrazione delle connessioni per un endpoint AWS Client VPN esistente
- Visualizza i registri delle AWS Client VPN connessioni
- Disattiva la registrazione delle AWS Client VPN connessioni

Abilitazione della registrazione delle connessioni per un nuovo endpoint AWS 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. Apri la 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 AWS Client VPN endpoint.
4. In Registrazione delle connessioni, attiva Enable log details on client connections (Abilita i dettagli del registro sulle connessioni client).
5. Per il nome del gruppo di log CloudWatch Logs, scegli il nome del gruppo di CloudWatch log Logs.
6. (Facoltativo) Per il nome del flusso di registro CloudWatch dei registri, scegliete il nome del flusso di registro dei CloudWatch registri.
7. Selezionare Create Client VPN Endpoint (Crea endpoint VPN client).

Per abilitare la registrazione della connessione per un nuovo endpoint Client VPN utilizzando AWS CLI

Utilizzate il create-client-vpn-endpointcomando e specificate il `--connection-log-options` parametro. È possibile specificare le informazioni sui log delle connessioni in formato JSON, come illustrato nell'esempio seguente.

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

Abilitare la registrazione delle connessioni per un endpoint AWS 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. Apri la 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 il nome del gruppo di log CloudWatch Logs, scegli il nome del gruppo di CloudWatch log Logs.
6. (Facoltativo) Per il nome del flusso di registro CloudWatch dei registri, scegliete il nome del flusso di registro dei CloudWatch registri.
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"
}
```

Visualizza i registri delle AWS Client VPN connessioni

È possibile visualizzare i log di connessione Client VPN utilizzando la console CloudWatch Logs.

Per visualizzare i log delle connessioni utilizzando la console

1. Apri la CloudWatch console 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**
>
> La colonna Timestamp mostra l'ora in cui il log di connessione è stato pubblicato in CloudWatch Logs, non l'ora della connessione.

Per ulteriori informazioni sulla ricerca dei dati di log, consulta Search Log Data Using Filter Patterns nella Amazon CloudWatch Logs User Guide.

Disattiva la registrazione delle AWS Client VPN connessioni

Puoi disattivare la registrazione delle connessioni per un endpoint Client VPN utilizzando la console o la riga di comando. Quando si disattiva la registrazione delle connessioni, i registri delle connessioni esistenti in Registri non vengono CloudWatch eliminati.

Per disabilitare la registrazione delle connessioni utilizzando la console

1. Apri la 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 la registrazione delle connessioni utilizzando il AWS CLI

Utilizzate il modify-client-vpn-endpointcomando e specificate il `--connection-log-options` parametro. Assicurarsi che `Enabled` sia impostato su `false`.

AWS Client VPN esportazione del file di configurazione dell'endpoint

Il file di configurazione dell' AWS Client VPN endpoint è il file che i client (utenti) utilizzano 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 hai abilitato il portale self-service per il tuo endpoint Client VPN, i clienti possono accedere al portale e scaricare autonomamente il file di configurazione. Per ulteriori informazioni, consulta AWS Client VPN accesso 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.

Attività

- Esportazione del file di configurazione del AWS Client VPN client
- Aggiungere il certificato AWS Client VPN client e le informazioni chiave per l'autenticazione reciproca

Esportazione del file di configurazione del AWS Client VPN client

È possibile esportare la configurazione del client Client VPN utilizzando la console o il AWS CLI.

Per esportare la configurazione del client (console)

1. Apri la 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)

Utilizzare il comando export-client-vpn-client-configuration e specificare il nome del file di output.

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

Aggiungere il certificato AWS Client VPN client e le informazioni chiave per l'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. Sostituiscilo */path/* con la posizione del certificato e della chiave del client (la posizione è relativa 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 connetterà 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-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

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

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

reneg-sec 0
```

AWS Client VPN percorsi

Ogni AWS Client VPN endpoint dispone di una tabella di routing che descrive le rotte di rete di destinazione disponibili. 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, come le reti peered VPCs locali, la 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 Risoluzione dei problemi AWS Client VPN: l'accesso a un VPC peered, Amazon S3 o Internet è intermittente. Ogni sottorete associata dovrebbe avere un insieme identico di routing.

Considerazioni sull'utilizzo dello split-tunnel sugli 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.

Attività

- Crea un percorso AWS Client VPN endpoint
- Visualizza i AWS Client VPN percorsi degli endpoint
- Eliminare una route AWS Client VPN dell'endpoint

Crea un percorso AWS Client VPN endpoint

Quando si crea una route endpoint Client VPN, si specifica come deve essere indirizzato il traffico per la 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. Apri la 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, specifica l'intervallo IPv4 CIDR per la rete di destinazione. Ad esempio:
   - Per aggiungere una route per il VPC dell'endpoint Client VPN, inserisci l'intervallo CIDR del VPC. IPv4
   - Per aggiungere una route per l'accesso a Internet, immettere `0.0.0.0/0`
   - Per aggiungere una route per un VPC peered, inserisci l'intervallo CIDR del VPC peered. IPv4
   - Per aggiungere un percorso per una rete locale, inserisci l'intervallo CIDR della AWS Site-to-Site connessione VPN. IPv4
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.

Visualizza i AWS Client VPN percorsi degli 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.

Eliminare una route AWS Client VPN dell'endpoint

Puoi eliminare solo le route Client VPN che hai aggiunto 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. Apri la 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.

AWS Client VPN reti di destinazione

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

Per ulteriori informazioni sui tipi di accesso che puoi configurare (ad esempio consentire ai client di accedere a Internet), consultaScenari ed esempi per Client VPN.

Requisiti della rete di destinazione Client VPN

Quando si crea una rete di destinazione, si applicano le seguenti regole:

- 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 Modificare un AWS Client VPN endpoint.

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 ne aggiungi o rimuovi altre CIDRs al tuo VPC collegato, devi eseguire una delle seguenti operazioni per aggiornare la route locale per la tabella di routing degli 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.

Attività

- Associare una rete di destinazione a un AWS Client VPN endpoint
- Applicare un gruppo di sicurezza a una rete di destinazione in AWS Client VPN
- Visualizza le reti AWS Client VPN di destinazione
- Dissociare una rete di destinazione da un endpoint AWS Client VPN

Associare una rete di destinazione a un AWS Client VPN endpoint

Puoi associare una o più reti di destinazione (sottoreti) a un endpoint Client VPN utilizzando la console Amazon VPC o la CLI. AWS Prima di associare una rete di destinazione a un endpoint Client VPN, acquisisci familiarità con i requisiti. Per informazioni, consulta Requisiti per la creazione di una rete di destinazione.

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

1. Apri la 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)

Usa il comando -networkassociate-client-vpn-target.

Applicare un gruppo di sicurezza a una rete di destinazione in AWS Client VPN

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 Client VPN.

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

1. Apri la 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 i gruppi di sicurezza appropriati dal gruppo di sicurezza IDs.
6. Seleziona Apply Security Groups (Applica i gruppi di sicurezza).

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

Usate il client-vpn-target-network comando apply-security-groups-to-.

Visualizza le reti AWS Client VPN di destinazione

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. Apri la 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 di destinazione utilizzando AWS CLI

Utilizzare il comando describe-client-vpn-target-networks.

Dissociare una rete di destinazione da un endpoint AWS 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. Apri la 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)

Usa il comando disassociate-client-vpn-target-network.

AWS Client VPN timeout della durata massima della sessione VPN

AWS Client VPN fornisce diverse opzioni per la durata massima della sessione VPN, che è il tempo massimo consentito per una connessione client all'endpoint Client VPN. È possibile configurare una durata massima della sessione VPN più breve per contribuire a soddisfare i requisiti di sicurezza e conformità. Per impostazione predefinita, la sessione VPN massima dura 24 ore. Una volta impostata la durata massima della sessione, puoi controllare cosa succede con quella sessione quando viene raggiunto il timeout. L'opzione di disconnessione al timeout della sessione consente di terminare la sessione o di tentare automaticamente una riconnessione all'endpoint. L'interruzione di una sessione consente un maggiore controllo sulla sicurezza degli endpoint applicando la durata massima della sessione VPN. Se una sessione è impostata per terminare quando viene raggiunto il tempo massimo, gli utenti dovranno riconnettersi e fornire le proprie credenziali di autenticazione per ristabilire la connessione VPN.

Quando la disconnessione al timeout della sessione è impostata per la riconnessione automatica e viene raggiunto il tempo massimo di sessione,

- viene stabilita automaticamente una nuova sessione nel caso di credenziali utente memorizzate nella cache (Active Directory) o autenticazione basata su certificati (autenticazione reciproca). Per disconnettersi completamente e non riconnettersi automaticamente, questi utenti devono disconnettersi manualmente.
- non viene stabilita automaticamente una nuova sessione nel caso dell'autenticazione federata (SAML). Questi utenti devono autenticarsi nuovamente dopo la scadenza del timeout della sessione per ristabilire la connessione VPN.

> **Note**
>
> - Quando il valore della durata massima della sessione VPN viene ridotto rispetto al valore corrente, tutte le sessioni VPN attive connesse all'endpoint per un periodo di tempo più lungo della durata appena impostata vengono disconnesse.
> - La modifica dell'opzione di disconnessione al timeout della sessione applica la nuova impostazione a tutte le sessioni attualmente aperte.

Configura la sessione VPN massima durante la creazione di un endpoint AWS Client VPN

La durata di una sessione VPN viene configurata durante la creazione di un endpoint Client VPN. Consulta i passaggi Creare un AWS Client VPN endpoint per creare un endpoint Client VPN e impostare la durata massima della sessione.

Attività

- Visualizza la durata massima AWS Client VPN attuale della sessione VPN
- Modifica la durata massima AWS Client VPN della sessione e il comportamento di timeout

Visualizza la durata massima AWS Client VPN attuale della sessione VPN

Utilizzare i seguenti passaggi per visualizzare la durata massima della sessione VPN corrente di Client VPN.

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

1. Apri la 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 la durata massima attuale della sessione VPN accanto alle ore di timeout della sessione e se Disconnect on timeout è abilitato o disabilitato.

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

Utilizza il comando describe-client-vpn-endpoints.

Modifica la durata massima AWS Client VPN della sessione e il comportamento di timeout

Utilizzare i seguenti passaggi per modificare la durata massima di una sessione VPN Client VPN esistente e modificare il comportamento di disconnessione in caso di timeout della sessione.

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

1. Apri la 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. Per Disconnetti al timeout della sessione, scegli se vuoi disconnettere una sessione quando viene raggiunto il timeout massimo della sessione. Per impostazione predefinita, questa opzione è disattivata la prima volta che modifichi un endpoint.
6. 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

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per maggiori informazioni sui programmi di conformità applicabili AWS Client VPN, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

AWS Client VPN fa 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. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Client VPN.

Argomenti

- Protezione dei dati in AWS Client VPN
- Gestione delle identità e degli accessi per AWS Client VPN
- Resilienza in AWS Client VPN
- Sicurezza dell'infrastruttura in AWS Client VPN
- Best practice di sicurezza per AWS Client VPN
- IPv6 considerazioni per AWS Client VPN

Protezione dei dati in AWS Client VPN

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in AWS Client VPN. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. 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 .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Client VPN o altro Servizi AWS utilizzando la console, l'API o AWS SDKs. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log 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 luogo 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 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 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)

Gestione delle identità e degli accessi per AWS Client VPN

AWS Identity and Access Management (IAM) è un servizio Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. 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 software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

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

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in 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 AWS Client VPN di identità e accesso.

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 AWS Client VPN funziona 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 il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al Console di gestione AWS o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo 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)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso 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. Conserva le credenziali dell'utente root e utilizzale 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 IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. 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 un'identità interna 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 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, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in Console di gestione AWS, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente 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 Create a role for a third-party identity provider (federation) nella Guida per l'utente 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 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, con alcuni Servizi AWS, è possibile allegare 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 Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel 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.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei 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 chiama an Servizio AWS, combinate con la richiesta Servizio AWS per

effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

- Ruolo di servizio: 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente 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'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo 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: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come 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 IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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. L'amministratore può quindi 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 dall' Console di gestione AWS AWS CLI, dall'o dall' AWS API.

Policy basate sull'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 Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. 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 IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle 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 utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni 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 su risorse sono policy inline che risiedono in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e 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 funzionalità 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 IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di

Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.

- 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 IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come AWS Client VPN funziona 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 puoi utilizzare con AWS Client VPN

Funzionalità IAM	Supporto per Client VPN
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì

Funzionalità IAM	Supporto per Client VPN
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

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 Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente 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 collegare a una risorsa. Esempi di policy basate sulle 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 utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni 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 il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad 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 Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni di policy per Client VPN

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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 azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni 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 delle azioni Client VPN, consulta Azioni definite da AWS Client VPN nel Service Authorization Reference.

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 AWS JSON per specificare chi ha accesso a cosa. In altre parole, 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). È possibile eseguire questa operazione per operazioni 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 dei tipi di risorse Client VPN e relativi ARNs, consulta Risorse definite da AWS Client VPN nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta Azioni 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 AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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. È possibile 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 si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile 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 del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di Client VPN, consulta Condition keys for AWS Client VPN nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni 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.

ACLs in Client VPN

Supporti ACLs: no

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

ABAC con Client VPN

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. 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 Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente 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 accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi Console di gestione AWS utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente 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 Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee 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 l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei 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 chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Utilizzo dei ruoli collegati ai servizi per Client VPN

Supporta ruoli collegati ai servizi: Sì

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'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo 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.

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 possono eseguire attività utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a 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 (console) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Client VPN, incluso il formato di ARNs per ogni tipo di risorsa, vedere Azioni, risorse e chiavi di condizione per AWS Client VPN nel Service Authorization Reference.

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 azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile 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 IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile 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 anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente 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 alla sintassi 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 il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'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 Protezione dell'accesso API con MFA nella Guida per l'utente 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 cpllegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

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

```
        }
    ]
}
```

Risoluzione dei problemi AWS Client VPN di identità e accesso

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 a persone esterne a me di accedere Account AWS 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`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. 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 passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. 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`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS 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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche 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 AWS Client VPN funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti 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 IAM.

- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Utilizzo di ruoli collegati ai servizi per AWS Client VPN

AWS Client VPN utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a un Client VPN. I ruoli collegati ai servizi sono predefiniti da Client VPN e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Argomenti

- Utilizzo dei ruoli per AWS Client VPN
- Utilizzo dei ruoli per l'autorizzazione della connessione in Client VPN;

Utilizzo dei ruoli per AWS Client VPN

AWS Client VPN utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a un Client VPN. I ruoli collegati ai servizi sono predefiniti da Client VPN e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

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 allegata 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.

Autorizzazioni del ruolo collegato ai servizi per Client VPN

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

Il ruolo collegato al servizio AWSServiceRoleForClientVPN prevede che il seguente servizio assuma il ruolo:

- `clientvpn.amazonaws.com`

Questo ruolo collegato al servizio utilizza la policy gestita Client. VPNService RolePolicy Per visualizzare le autorizzazioni per questa politica, consulta Client VPNService RolePolicy nel AWS Managed Policy Reference.

Creare un ruolo collegato 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 l' Console di gestione AWS, la o l' AWS API AWS CLI, Client VPN crea per te il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile 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.

Modificare un ruolo collegato al servizio per Client VPN

Client VPN non consente di modificare il ruolo collegato al servizio AWSService RoleForClient VPN. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modificare la descrizione di un ruolo collegato al servizio nella Guida per l'utente IAM.

Eliminare un ruolo collegato al servizio per Client VPN

Se non è più necessario utilizzare Client VPN, si consiglia di 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 Eliminare un ruolo collegato al servizio nella Guida per l'utente IAM.

Utilizzo dei ruoli per l'autorizzazione della connessione in Client VPN;

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

ruoli collegati ai servizi sono predefiniti da Client VPN e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

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 allegata 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.

Autorizzazioni del ruolo collegato ai servizi per Client VPN

Client VPN utilizza il ruolo collegato al servizio denominato Service Linked AWSServiceRoleForClientVPNConnectionsRole per le connessioni Client VPN.

Il ruolo AWSService RoleForClient VPNConnections collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `clientvpn-connections.amazonaws.com`

La politica di autorizzazione dei ruoli denominata Client VPNService ConnectionsRolePolicy consente a Client VPN di completare le seguenti azioni 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.

Creare un ruolo collegato 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 l' Console di gestione AWS, la o l' AWS API AWS CLI, Client VPN crea per te il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile 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.

Modificare un ruolo collegato al servizio per Client VPN

Client VPN non consente di modificare il ruolo AWSService RoleForClient VPNConnections collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modificare la descrizione di un ruolo collegato al servizio nella Guida per l'utente IAM.

Eliminare un ruolo collegato al servizio per Client VPN

Se non è più necessario utilizzare Client VPN, si consiglia di eliminare il ruolo AWSServiceRoleForClientVPNConnectionscollegato al servizio.

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 Eliminare un ruolo collegato al servizio nella Guida per l'utente IAM.

Resilienza in AWS Client VPN

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover 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 tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Oltre all'infrastruttura AWS globale, AWS Client VPN offre funzionalità che aiutano a supportare le esigenze di resilienza e backup dei dati.

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 AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Client VPN attraverso la rete. I client 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 di sicurezza per AWS Client VPN

AWS Client VPN fornisce una serie di funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

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.

Disconnettiti al timeout della sessione

Disconnetti una sessione quando viene raggiunto il tempo massimo della sessione Client VPN, applicando una durata massima della sessione VPN. Per ulteriori informazioni, consulta durata massima della sessione VPN.

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 Client VPN.

Gestione dell'identità e degli accessi

Gestisci l'accesso alle risorse Client VPN e APIs utilizza le policy IAM per i tuoi utenti IAM e ruoli IAM. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per AWS Client VPN.

IPv6 considerazioni per AWS Client VPN

Client VPN ora supporta la IPv6 connettività nativa oltre alle IPv4 funzionalità esistenti. Puoi creare endpoint IPv6 -only, IPv4 -only o dual-stack (entrambi IPv4 e IPv6) per soddisfare i tuoi requisiti di rete.

IPv6 Componenti chiave del supporto

Quando si lavora con IPv6 Client VPN, esistono due parametri di configurazione chiave:

Tipo di indirizzo IP dell'endpoint

Questo parametro definisce il tipo di IP di gestione degli endpoint, che determina il tipo di EC2 istanza fornita per l'endpoint. Questo tipo di IP viene utilizzato per gestire il traffico del tunnel VPN esterno (il traffico crittografato che scorre tra il client e il server OpenVPN sulla rete Internet pubblica).

Tipo di indirizzo IP del traffico

Questo parametro definisce il tipo di traffico che attraversa il tunnel VPN. Questo tipo di IP viene utilizzato per gestire il traffico crittografato interno (il payload effettivo), gli intervalli CIDR dei client, l'associazione di sottoreti, i percorsi e le regole per endpoint.

IPv6 assegnazione CIDR del client

Per IPv6 il client CIDR, non è necessario specificare un blocco CIDR. Amazon assegna automaticamente gli intervalli CIDR ai IPv6 clienti. Questa assegnazione automatica consente l'esclusione IPv6 del traffico dal tunnel, fornendo una maggiore visibilità sull'indirizzo dell' IPv6 utente connesso. SNATing

Requisiti di compatibilità

IPv6 e gli endpoint dual-stack dipendono dai dispositivi degli utenti e dai provider di servizi Internet (): ISPs

- I dispositivi utente che eseguono il client CVPN devono supportare la configurazione IP richiesta, come mostrato nella tabella di compatibilità riportata di seguito.
- ISPs devono supportare la configurazione IP richiesta per il corretto funzionamento della connessione.
- Per il traffico dual-stack, le sottoreti VPC associate devono avere intervalli IPv6 CIDR dual-stack. IPv6

Supporto DNS

Il DNS è supportato in tutti i tipi di endpoint e dual-stack. IPv4 IPv6 Per gli IPv6 endpoint, puoi configurare IPv6 i server DNS utilizzando il parametro. `--dns-server-ipv6` I record DNS AAAA sono supportati sia sul lato del servizio che sul lato client.

Limitazioni

Di seguito sono riportate le limitazioni relative a: IPv6

- Client-to-client (C2C) la comunicazione non è supportata per i IPv6 client. Se un IPv6 client tenta di comunicare con un altro IPv6 client, il traffico verrà interrotto.

Client Routes Enforcement per IPv6

Client VPN ora supporta Client Routes Enforcement per IPv6 il traffico. Questa funzionalità aiuta a garantire che il traffico di IPv6 rete proveniente dai client connessi segua i percorsi definiti dall'amministratore e non venga inviato inavvertitamente all'esterno del tunnel VPN.

Aspetti chiave del supporto di IPv6 Client Route Enforcement:

- Il `ClientRouteEnforcementOptions.enforced` flag esistente abilita CRE sia per gli stack che per IPv4 gli IPv6 stack.
- IPv6 Client Route Enforcement esclude determinati IPv6 intervalli per mantenere le funzionalità critiche: IPv6
  - `::1/128`— Riservato al loopback
  - `fe80::/10`— Riservato agli indirizzi locali del collegamento
  - `ff00::/8`— Riservato al multicast
- IPv6 Client Route Enforcement è disponibile nella versione 5.3.0 e successive di AWS VPN Client su Windows, macOS e Ubuntu.

Per informazioni più dettagliate su CRE, incluso come abilitarlo e configurarlo, consulta. the section called “Applicazione del percorso del cliente”

IPv6 prevenzione delle fughe (informazioni precedenti)

Per le configurazioni precedenti che non utilizzano il IPv6 supporto nativo, potrebbe comunque essere necessario prevenire eventuali IPv6 fughe di dati. IPv6 le perdite possono verificarsi quando entrambe IPv4 IPv6 sono abilitate e connesse alla VPN, ma la VPN non instrada il IPv6 traffico nel suo tunnel. In questo caso, quando ti connetti a una destinazione IPv6 abilitata, in realtà continui a connetterti con IPv6 l'indirizzo fornito dal tuo ISP. Ciò farà trapelare il tuo vero IPv6 indirizzo. Le istruzioni riportate di seguito spiegano come indirizzare il IPv6 traffico verso il tunnel VPN.

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

```
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 come indirizzo del dispositivo del tunnel locale `fd15:53b6:dead::2` e come IPv6 indirizzo dell'endpoint IPv6 VPN remoto. `fd15:53b6:dead::1`

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

> **Note**
>
> Ad esempio, per il routing dei dispositivi «TAP» in Windows, il secondo parametro di `ifconfig-ipv6` verrà utilizzato come destinazione del percorso 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 indirizzerà tutto il IPv6 traffico attualmente allocato verso la connessione VPN.

Verifica

L'organizzazione eseguirà probabilmente i propri test. Una verifica di base consiste nel configurare una connessione VPN a tunnel completo, quindi eseguire ping6 su un IPv6 server utilizzando l'indirizzo. IPv6 L' IPv6 indirizzo del server deve essere compreso nell'intervallo specificato dal `route-ipv6` comando. Questo test ping dovrebbe fallire. Tuttavia, ciò potrebbe cambiare se in futuro verrà aggiunto il IPv6 supporto 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. Esistono anche alcuni strumenti disponibili al pubblico.

Monitoraggio AWS Client VPN

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Client VPN altre AWS soluzioni. 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 AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. 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 tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue EC2 istanze Amazon e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

AWS CloudTrail

Acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Tutte le azioni Client VPN vengono registrate CloudTrail e documentate nell'Amazon EC2 API Reference.

CloudWatch Registri Amazon

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 di CloudWatch Logs per registrare i dettagli della connessione. Per ulteriori informazioni, consulta Registrazione della connessione per un endpoint AWS Client VPN la Amazon CloudWatch Logs User Guide.

Argomenti

- CloudWatch Metriche Amazon per AWS Client VPN

CloudWatch Metriche Amazon per AWS Client VPN

AWS Client VPN pubblica le seguenti metriche su Amazon CloudWatch per i tuoi endpoint Client VPN. Le metriche vengono pubblicate su 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.

Parametro	Descrizione
	Unità: numero
SelfServicePortalClientConfigurationDownloads	Numero di download del file di configurazione dell'endpoint Client VPN dal portale self-serv ice. Unità: numero

AWS Client VPN pubblica le seguenti metriche di valutazione della postura 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

Parametro	Descrizione
ClientConnectHandlerDeniedConnections	Numero di connessioni negate dal gestore di connessioni per le connessioni all'endpoint Client VPN. Unità: numero
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 consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. 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 CloudWatch allarme per monitorare una metrica specifica e avviare un'azione (come l'invio di una notifica a un indirizzo e-mail) se la metrica non rientra nell'intervallo che consideri accettabile.

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Attività

- Visualizza le metriche degli endpoint Client VPN in Amazon CloudWatch

Visualizza le metriche degli endpoint Client VPN in Amazon 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 allo spazio dei nomi del servizio e successivamente in base alle diverse combinazioni di dimensioni all'interno di ogni spazio dei nomi.

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

Per visualizzare le metriche utilizzando il 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"
```

AWS Client VPN quote

Il tuo AWS account ha le seguenti quote, precedentemente denominate limiti, relative agli endpoint Client VPN. Salvo diversa indicazione, 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	Predefinita	Adattabile
Regole di autorizzazione per endpoint Client VPN	200 Per gli endpoint dual-stack, questo limite è condiviso tra e route. IPv4 IPv6	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. • 1 – 7.000 • 2 – 36.500 • 3 – 66.500 • 4 – 96.500 • 5 – 126.000 Per gli endpoint dual-stack, questo limite	Sì

Nome	Predefinita	Adattabile
	è condiviso tra e connessioni. IPv4 IPv6	
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
Associazione alla rete di destinazione Routes per Client VPN	100 Per gli endpoint dual-stack, questo limite è condiviso tra e route. IPv4 IPv6	Sì

† Le operazioni includono:

- Associare oppure dissociare sottoreti
- 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 AWS Directory Service risorsa utilizzata per l'autenticazione di Active Directory.
- Se utilizzi l'autenticazione federata basata su SAML per autenticare un utente, l'endpoint Client VPN deve appartenere allo stesso account del provider di identità IAM SAML che crei per definire la relazione tra IdP e trust. AWS Il provider di identità IAM SAML può essere condiviso su più endpoint Client VPN nello stesso AWS account.

Risoluzione dei problemi AWS Client VPN

Le seguenti sezioni possono aiutarti a risolvere i problemi che potresti avere 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

- Risoluzione dei problemi AWS Client VPN: impossibile risolvere il nome DNS dell'endpoint Client VPN
- Risoluzione dei problemi AWS Client VPN: il traffico non viene suddiviso tra le sottoreti
- Risoluzione dei problemi AWS Client VPN: le regole di autorizzazione per i gruppi di Active Directory non funzionano come previsto
- Risoluzione dei problemi AWS Client VPN: i client non possono accedere a un VPC peered, Amazon S3 o Internet
- Risoluzione dei problemi AWS Client VPN: l'accesso a un VPC peered, Amazon S3 o Internet è intermittente
- Risoluzione dei problemi AWS Client VPN: il software client restituisce un errore TLS quando tenta di connettersi a Client VPN
- Risoluzione dei problemi AWS Client VPN: il software client restituisce errori di nome utente e password — Autenticazione Active Directory
- Risoluzione dei problemi AWS Client VPN: il software client restituisce errori di nome utente e password: autenticazione federata
- Risoluzione dei problemi AWS Client VPN: i client non riescono a connettersi: autenticazione reciproca
- Risoluzione dei problemi AWS Client VPN: il client restituisce un errore di dimensioni superiori alla dimensione massima delle credenziali in Client VPN — autenticazione federata
- Risoluzione dei problemi AWS Client VPN: il client non apre il browser per un endpoint — autenticazione federata
- Risoluzione dei problemi AWS Client VPN: il client non restituisce alcun errore sulle porte disponibili: autenticazione federata

- Risoluzione dei problemi AWS Client VPN: una connessione viene interrotta a causa di una mancata corrispondenza IP
- Risoluzione dei problemi AWS Client VPN: il routing del traffico verso la LAN non funziona come previsto
- Risoluzione dei problemi AWS Client VPN: verifica il limite di larghezza di banda per un endpoint Client VPN
- Risoluzione dei problemi AWS Client VPN: problemi di connettività del tunnel a un VPC

Risoluzione dei problemi AWS 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 aggiungi una stringa casuale ad essa in modo che il formato sia. *`random_string.displayed_DNS_name`* Per 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`

Risoluzione dei problemi AWS Client VPN: il traffico non viene suddiviso tra le 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.

Risoluzione dei problemi AWS Client VPN: le 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` autorizzare il traffico per tutte le reti, ma il traffico continua a fallire per una destinazione specifica. CIDRs

Causa

Le regole di autorizzazione sono indicizzate sulla rete. CIDRs Le regole di autorizzazione devono concedere ai gruppi di Active Directory l'accesso a una rete specifica. CIDRs 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

Verifica di creare regole di autorizzazione che consentano esplicitamente ai gruppi di Active Directory di accedere a una rete CIDRs specifica. 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.

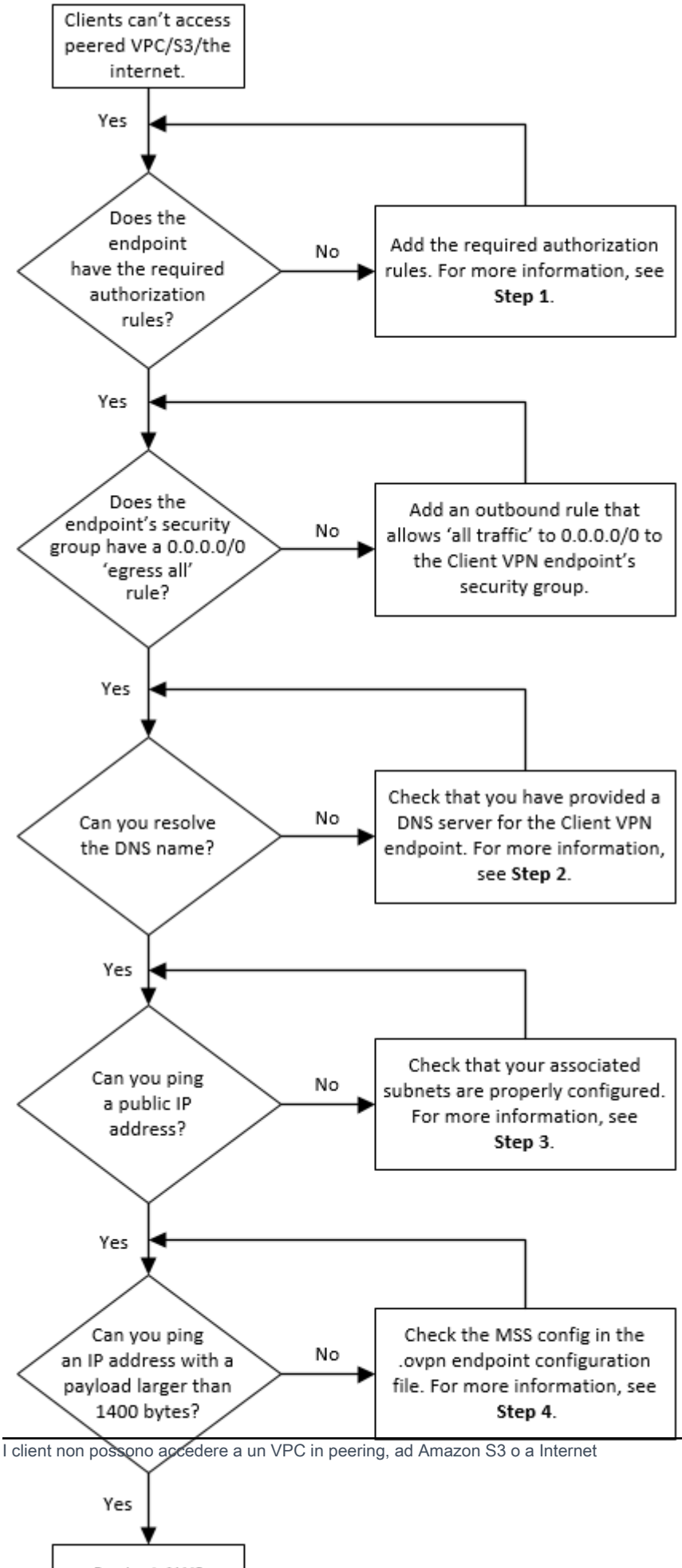
Risoluzione dei problemi AWS Client VPN: i client non possono accedere a un VPC peered, Amazon S3 o Internet

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.


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. Per l'accesso a Internet, aggiungere una regola di autorizzazione per `0.0.0.0/0`.

   Per accedere a un VPC peering, aggiungi 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
```

Risoluzione dei problemi AWS Client VPN: l'accesso a un VPC peered, Amazon S3 o Internet è intermittente

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

Risoluzione dei problemi AWS Client VPN: il software client restituisce un errore TLS quando tenta di connettersi a Client VPN

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 AWS Client VPN elenchi di revoca dei 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 AWS Client VPN.

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 .

Risoluzione dei problemi AWS Client VPN: il software client restituisce errori di nome utente e password — Autenticazione 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 AWS Client VPN esportazione del file di configurazione dell'endpoint. Verifica la configurazione MFA per Active Directory senza utilizzare l'endpoint Client VPN per controllare che MFA funzioni come previsto.

Risoluzione dei problemi AWS Client VPN: il software client restituisce errori di nome utente e password: autenticazione federata

Problema

Tentativo di accesso con nome utente e password con autenticazione federata e viene visualizzato l'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.

Risoluzione dei problemi AWS Client VPN: i client non riescono a 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 AWS Client VPN esportazione del file di configurazione dell'endpoint.

Risoluzione dei problemi AWS Client VPN: il client restituisce un errore di dimensioni superiori alla dimensione massima delle credenziali in Client VPN — 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.

Risoluzione dei problemi AWS Client VPN: il client non apre il browser per un endpoint — 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.

Risoluzione dei problemi AWS Client VPN: il client non restituisce alcun errore sulle porte disponibili: 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.

Risoluzione dei problemi AWS Client VPN: una connessione viene interrotta a causa di una mancata corrispondenza 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 per l'utilizzo AWS Client VPN.

Soluzione

Verifica che non vi sia alcun proxy DNS tra il client AWS fornito e l'endpoint Client VPN.

Risoluzione dei problemi AWS Client VPN: il routing del traffico verso la LAN non funziona come previsto

Problema

Il tentativo di indirizzare 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 per l'utilizzo 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.

Risoluzione dei problemi AWS Client VPN: verifica il 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. È supportata una larghezza di banda minima 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
```

Risoluzione dei problemi AWS Client VPN: problemi di connettività del tunnel a un VPC

In caso di problemi di connettività con la AWS Client VPN connessione, segui questo approccio sistematico alla risoluzione dei problemi per identificare e risolvere il problema. Questa sezione fornisce step-by-step le procedure per diagnosticare i problemi più comuni di connettività Client VPN tra client remoti e risorse Amazon VPC.

Argomenti

- Prerequisiti di connettività di rete
- Verifica lo stato dell'endpoint Client VPN
- Verifica le connessioni dei client
- Verifica l'autenticazione del client
- Controlla le regole di autorizzazione
- Convalida i percorsi Client VPN
- Verifica i gruppi di sicurezza e la rete ACLs
- Verifica la connettività del client
- Diagnostica il dispositivo client
- Risoluzione dei problemi relativi alla risoluzione DNS
- Risolvi i problemi relativi alle prestazioni
- Monitora le metriche di Client VPN
- Controlla i log di Client VPN
- Problemi e soluzioni comuni

Prerequisiti di connettività di rete

Prima di risolvere i problemi di connettività Client VPN, verifica questi prerequisiti di rete:

- Assicurati che la sottorete degli endpoint Client VPN disponga di connettività Internet (tramite Internet Gateway o NAT Gateway).

- Verifica che l'endpoint Client VPN sia associato a sottoreti in diverse zone di disponibilità per un'elevata disponibilità.
- Verifica che il VPC disponga di uno spazio di indirizzi IP sufficiente e che non sia in conflitto con i blocchi CIDR del client.
- Verifica che le sottoreti di destinazione abbiano associazioni corrette tra le tabelle di routing.

Verifica lo stato dell'endpoint Client VPN

Innanzitutto, verifica che l'endpoint Client VPN sia nello stato corretto:

1. Utilizza il AWS CLI per verificare lo stato dell'endpoint Client VPN:

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

2. Cerca lo stato dell'endpoint nell'output. Lo stato dovrebbe essere`available`.
3. Verificare che all'endpoint siano associate reti di destinazione (sottoreti).
4. Se lo stato non lo è`available`, verifica la presenza di messaggi di errore o stati in sospeso che potrebbero indicare problemi di configurazione.

Verifica le connessioni dei client

Controlla lo stato delle connessioni client al tuo endpoint Client VPN:

1. Controlla le connessioni client attive:

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

2. Controlla lo stato della connessione e gli eventuali messaggi di errore nell'output.
3. Controlla i registri di autenticazione del client per i tentativi di autenticazione non riusciti.
4. Verifica che i client ricevano gli indirizzi IP dal blocco CIDR del client configurato.

> **Note**
>
> Se i client non riescono a connettersi, è probabile che il problema riguardi la configurazione dell'autenticazione, le regole di autorizzazione o la connettività di rete.

Verifica l'autenticazione del client

I problemi di autenticazione sono cause comuni dei problemi di connettività Client VPN:

- Per l'autenticazione reciproca, assicurati che i certificati client siano validi e non scaduti.
- Per l'autenticazione Active Directory, verifica le credenziali utente e la connettività del dominio.
- Per l'autenticazione federata basata su SAML, controlla la configurazione IdP e le autorizzazioni utente.
- Controlla i log di autenticazione per informazioni dettagliate sugli errori. CloudWatch
- Verifica che il metodo di autenticazione configurato sull'endpoint corrisponda alla configurazione del client.

Controlla le regole di autorizzazione

Le regole di autorizzazione controllano a quali risorse di rete possono accedere i client:

1. Elenca le regole di autorizzazione correnti:

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

2. Verifica che esistano regole per le reti di destinazione a cui i client devono accedere.
3. Verifica che le regole specifichino i gruppi Active Directory corretti (se utilizzi l'autenticazione AD).
4. Assicurati che le regole di autorizzazione siano `active` valide.

Convalida i percorsi Client VPN

Una corretta configurazione del routing è essenziale per la connettività Client VPN:

1. Controlla i percorsi degli endpoint Client VPN:

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

2. Verifica che esistano percorsi per le reti di destinazione a cui i client devono accedere.

3. Controlla le tabelle di routing di Amazon VPC per assicurarti che il traffico di ritorno possa raggiungere l'endpoint Client VPN:

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

4. Verifica che le associazioni di rete di destinazione siano configurate correttamente.

Verifica i gruppi di sicurezza e la rete ACLs

I gruppi di sicurezza e la rete ACLs possono bloccare il traffico Client VPN:

1. Controlla i gruppi di sicurezza per le EC2 istanze di destinazione:

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

2. Verifica che le regole in entrata consentano il traffico dal blocco CIDR di Client VPN:
   - SSH (porta 22) da Client VPN CIDR: `10.0.0.0/16`
   - HTTP (porta 80) da Client VPN CIDR: `10.0.0.0/16`
   - HTTPS (porta 443) da Client VPN CIDR: `10.0.0.0/16`
   - Porte applicative personalizzate in base alle esigenze
3. Per il gruppo di sicurezza degli endpoint Client VPN (se applicabile), assicurati che consenta:
   - Porta UDP 443 (OpenVPN) da 0.0.0.0/0
   - Tutto il traffico in uscita verso i blocchi CIDR VPC
4. Verifica che la rete non ACLs stia bloccando il traffico. ACLs Le reti sono prive di stato, quindi è necessario configurare sia le regole in entrata che quelle in uscita.
5. Verifica le regole in entrata e in uscita per il traffico specifico che stai tentando di inviare.

Verifica la connettività del client

Verifica la connettività dai client Client VPN alle risorse Amazon VPC:

1. Da un client Client VPN connesso, verifica la connettività alle risorse Amazon VPC:

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

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

2. Verifica la connettività di applicazioni specifiche:

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

3. Verifica la risoluzione DNS se utilizzi nomi DNS privati:

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

4. Verifica la connettività alle risorse Internet se lo split tunneling è abilitato.

Diagnostica il dispositivo client

Esegui questi controlli sul dispositivo client:

1. Verifica che il file di configurazione del client (.ovpn) contenga le impostazioni corrette:
   - URL dell'endpoint del server corretto
   - Certificato client e chiave privata validi
   - Configurazione corretta del metodo di autenticazione
2. Controlla i log del client per verificare la presenza di errori di connessione:
   - Windows: Visualizzatore eventi → Registri applicazioni e servizi → OpenVPN
   - macOS: app per console, cerca «Tunnelblick» o «OpenVPN»
   - Linux: o systemd journal `/var/log/openvpn/`
3. Verifica la connettività di rete di base dal client:

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

Risoluzione dei problemi relativi alla risoluzione DNS

I problemi DNS possono impedire l'accesso alle risorse utilizzando nomi DNS privati:

1. Controlla se i server DNS sono configurati nell'endpoint Client VPN:

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

2. Verifica la risoluzione DNS del client:

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

3. Verifica le regole del Route 53 Resolver se utilizzi una risoluzione DNS personalizzata.
4. Verifica che i gruppi di sicurezza consentano il traffico DNS (porta UDP/TCP 53) dal CIDR Client VPN ai server DNS.

Risolvi i problemi relativi alle prestazioni

Risolvi i problemi di prestazioni con le connessioni Client VPN:

- Monitora l'utilizzo della larghezza di banda utilizzando le CloudWatch metriche per i byte. ingress/egress
- Verifica la perdita di pacchetti utilizzando test ping continui dei client.
- Verifica che l'endpoint Client VPN non stia raggiungendo i limiti di connessione.
- Prendi in considerazione l'utilizzo di più endpoint Client VPN per la distribuzione del carico.
- Esegui test con diverse sedi dei clienti per identificare i problemi di prestazioni regionali.

Monitora le metriche di Client VPN

Monitora le metriche degli endpoint Client VPN utilizzando: CloudWatch

1. Controlla le metriche di connessione attive:

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

2. Rivedi le metriche relative agli errori di autenticazione:

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

3. Esamina altre metriche disponibili come byte e pacchetti in ingresso e uscita.

Controlla i log di Client VPN

I log delle connessioni Client VPN forniscono informazioni dettagliate sui tentativi e sugli errori di connessione:

- Abilita la registrazione della connessione Client VPN se non è già configurata.
- CloudWatch Esamina i log per verificare eventuali tentativi di connessione, errori di autenticazione ed errori di autorizzazione.
- Cerca codici e messaggi di errore specifici che indicano la causa principale dei problemi di connettività.
- Verifica la presenza di schemi nelle connessioni non riuscite che potrebbero indicare problemi di configurazione.

Problemi e soluzioni comuni

Problemi comuni che possono influire sulla connettività Client VPN:

Authentication failures (Errori di autenticazione)

I certificati client sono scaduti o non validi oppure le credenziali di Active Directory non sono corrette. Verifica la configurazione dell'autenticazione e la validità delle credenziali.

Regole di autorizzazione mancanti

I client non possono accedere alle reti di destinazione a causa di regole di autorizzazione mancanti o errate. Aggiungere le regole di autorizzazione appropriate per le reti richieste.

Problemi relativi allo split tunneling

Instradamento del traffico errato a causa della configurazione dello split tunneling. Rivedi e modifica le impostazioni dello split tunneling secondo necessità.

Esaurimento del pool IP del client

Nessun indirizzo IP disponibile nel blocco CIDR del client. Espandi l'intervallo CIDR del client o disconnetti i client non utilizzati.

Problemi MTU

I pacchetti di grandi dimensioni vengono eliminati a causa delle limitazioni delle dimensioni dell'MTU. Prova a impostare l'MTU su 1436 byte o abilita Path MTU Discovery sui dispositivi client.

Problemi di risoluzione DNS

I client non possono risolvere nomi DNS privati. Verifica la configurazione del server DNS e assicurati che il traffico DNS sia consentito attraverso i gruppi di sicurezza.

Intervalli IP sovrapposti

Il CIDR del client blocca i conflitti con gli intervalli della rete locale. Verifica e risolvi eventuali intervalli di indirizzi IP sovrapposti tra il CIDR del client e le reti locali.

Errori di handshake TLS

La connessione non riesce durante la negoziazione TLS. Verifica la validità dei certificati, assicurati che le suite di crittografia siano corrette e verifica che i certificati client e server siano configurati correttamente.

Ritardi di propagazione delle rotte

Nuove rotte non immediatamente disponibili per i clienti. Attendi 1-2 minuti per la propagazione delle rotte dopo aver apportato modifiche alle rotte Client VPN.

Cadute/instabilità della connessione

Disconnessioni frequenti o connessioni instabili. Controlla la congestione della rete, le interferenze del firewall o le impostazioni di gestione dell'alimentazione sui dispositivi client.

Cronologia dei documenti per la Guida per l'utente di Client VPN

La tabella seguente descrive gli aggiornamenti della Administrator Guide AWS Client VPN .

Modifica	Descrizione	Data
IPv6 supporto	Client VPN ora consente la IPv6 connettività completa per gli endpoint Client VPN, supportando le connessioni alle IPv6 risorse dell'utente VPCs e dei client sulle IPv6 reti.	25 agosto 2025
Funzione Client Route Enforcement	Aggiunta della funzionalità Client Route Enforcement.	20 aprile 2025
Quota Client VPN aumentata	Aumentate le regole di autorizzazione per la quota di endpoint Client VPN da 50 a 200.	13 marzo 2025
Support per la disconnes sione in caso di timeout della sessione	Il timeout della sessione ora supporta la disconnes sione quando viene raggiunta la durata massima della sessione.	13 gennaio 2025
Aumento delle quote	Le quote per le regole di autorizzazione per endpoint Client VPN e Routes per endpoint Client VPN sono aumentate da 50 e 10 rispettiv amente a 100.	19 dicembre 2024

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	È possibile abilitare un banner di testo sulle applicazioni desktop Client VPN AWS fornite 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
Client-to-client accesso	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 il tuo AWS Client VPN endpoint.	16 gennaio 2020
Supporto per autenticazione a più fattori	L' AWS Client VPN endpoint supporta l'MFA se è abilitato per Active Directory.	30 settembre 2019
Supporto per split-tunnel	Puoi abilitare lo split-tunnel sul tuo endpoint. AWS Client VPN	24 luglio 2019
Versione iniziale	Questa versione 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.